APPLICATIONS OF CUBICAL ARRAYS IN THE STUDY OF FINITE SEMIFIELDS

by

KELLY CASIMIR AMAN

Presented to the Faculty of the Graduate School of
The University of Texas at Arlington in Partial Fulfillment
of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON

August 2014

Acknowledgments

I owe thanks to many people for helping me reach this milestone in my life, but I will limit this section to those who have most directly affected the work presented here.

First, I want to thank those who helped with the completion of this dissertation and its defense. Thanks to my advisor, Dr. Minerva Cordero, for her guidance, encouragement, and assistance, as well as allowing me to pursue my interests when conducting the research presented here. I also want to thank the other members of my committee: Dr. Epperson, Dr. Gornet, Dr. Jorgensen, and Dr. Vancliff, for reviewing this work, attending the defense, and providing useful feedback. Lastly, I need to thank Dr. Wene for pointing out some properties of cubical arrays which began the research which led to this dissertation.

I feel it is important to thank the teachers who have most influenced my work as a mathematician. In addition to Dr. Cordero, Dr. Gornet, and Dr. Vancliff, I must also thank Dr. Krueger and David Smith for instilling in me the goal of making my work as rigorous as possible.

Finally, I want to thank my family and friends for their support. In particular, I want to thank my wife, Jackie, for changing her schedule to best suit my needs.

June 23, 2014

Abstract

APPLICATIONS OF CUBICAL ARRAYS IN THE
STUDY OF FINITE SEMIFIELDS

Kelly Casimir Aman, Ph.D.

The University of Texas at Arlington, 2014

Supervising Professor: Minerva Cordero

It is well known that any finite semifield, S, can be viewed as an n-dimensional vector space over a finite field or prime order, $\mathbb{F}_p$, and that the multiplication in S defines and can be defined by an $n \times n \times n$ cubical array of scalars, A. For any element $a \in S$, the matrix, L_a, corresponding to left multiplication by a can be determined from A. In this paper we show that there exists a unique monic polynomial of minimal degree, $f \in \mathbb{F}_p[x]$, such that $f(a) = 0$, and which divides the minimal polynomial of L_a. Furthermore, we show that some properties of f in $\mathbb{F}_p[x]$ correspond to properties of a in S. These results, in turn, help optimize a method we introduce which uses A to determine the automorphism group of S. We show that under certain conditions A can be *inflated* to define a new semifield, $S_{[m]}$, over the field $\mathbb{F}_{p^m}$, and that inflation preserves isotopism and isomorphism between inflated semifields. Finally, we apply our results to the 16-element semifields, and give algebraic constructions for each of these semifields for which no construction currently exists.

Table of Contents

Chapter 1

Introduction

Finite semifields satisfy all of the axioms for finite fields except that their multiplication is not assumed to be associative or commutative. In this paper we study the algebraic properties of finite semifields through the use of cubical arrays. One motivation for semifield research is its applications to the theory of finite geometry, particularly finite translation planes. However, we take an algebraic approach to the work presented here. Nevertheless, we include a brief description of the geometric motivations for the concepts of isotopism and the dual of a semifield.

Chapters 2 and 3 provide background information for our results. They are based on the work of Donald Knuth in [11]. In chapter 2, we provide the formal definition of a finite semifield, and prove that any finite semifield, S, is an n-dimensional vector space over a prime order finite field, $\mathbb{F}_p$. Furthermore, we show that left or right multiplication by each element in S has a corresponding linear transformation. We also describe the relationship between finite semifields and finite projective planes, and introduce the geometrically and algebraically important concept of an isotopism between two semifields. In chapter 3, we show that the multiplication in a semifield defines an $n \times n \times n$ array of scalars known as a cubical array, A, and show the necessary conditions for a cubical array to define a semifield. We will call such cubical arrays *Knuth cubes*. We show how, for any $a \in S$, the matrix corresponding to left multiplication by a, L_a can be determined from A, and show how cubical arrays of isotopic semifields are related.

The remainder of this work is devoted to the results of our research. In chapter

4, we investigate the action of polynomials on elements of finite semifields. Due to the fact that semifield multiplication is nonassociative, we adopt the convention of using two exponential notations to refer to repeated left or right multiplication. Doing so allows us to prove that there exists a unique left minimal polynomial, $f \in \mathbb{F}_p[x]$ such that, when the exponents of f are used for left multiplication, $f(a) = 0$, and proves a number of results regarding the relationship between a, f, and L_a. Analogous results hold if right multiplication is used in place of left multiplication.

In chapter 5, we describe a subgroup, $C(n, p)$, of $GL(n, p)$, and show how $C(n, p)$ can be used to generate the set of all Knuth cubes which define S, $K(S)$. We show necessary and sufficient conditions for matrices in $C(n, p)$ to correspond to automorphisms of S. This allows the automorphism group of S to be determined by testing each matrix in $C(n, p)$, and we use the results of chapter 4 to greatly reduce the number of matrices which need to be tested.

In chapter 6, we outline a number of classical algebraic constructions for finite semifields and describes a Knuth cube generated by each construction. Using these results, it is possible to look at the Knuth cubes in $K(S)$ and see if any is of the proper form for each construction. This provides a method by which cubical arrays can be used to identify whether a particular construction will generate a particular semifield. The primary use of these results is in chapter 8 to identify which of the 16-element semifields can be generated by existing constructions.

The results in chapter 7 were inspired by the work of chapter 6, and follow directly from the results in chapters 2 and 3. We provide necessary and sufficient conditions under which A can define a semifield over $\mathbb{F}_{p^m}$, denoted $S_{[m]}$. We then prove that if $S_{[m]}$ exists, then S and S' are isotopic semifields if and only if $S_{[m]}$ and $S'_{[m]}$ are isotopic semifields.

In chapter 8, we applyin our results to the 16-element semifields. Currently al-

gebraic constructions exist for representatives of the three isotopism classes for these semifields, and we show how the known Knuth cubes can be used to provide algebraic constructions for each of the twenty-four isomorphism classes of these semifields. We conclude with a list of representative for each isomorphism class of the 16-element semifields, and for each representative we provide a Knuth cube, an algebraic construction, a list of automorphisms defined with respect to the algebraic construction, and a list of the elements contained in the most commonly studied semifield subsets.

Chapter 2

Semifields and Their Planes

The term *semifield*, and the definition which follows, were first introduced by Knuth in [11]. Even now, although the term has been widely adopted, these systems are sometimes referred to as "nonassociative division rings" or "distributive quasi-fields". In this chapter we will define what semifields are, describe their general form, and look at the geometries which inspired them. All of the results and proofs in this chapter are taken from [11], and are included here for the sake of completeness. Some of the notation has been altered to help avoid ambiguity and to suit the needs of the results in the later chapters. The proofs have been slightly altered as well to be more rigorous.

2.1 Semifield Basics

Definition 2.1. A finite semifield is a finite set, S, together with two binary operations, denoted $+$ and $*$, which satisfies the following axioms, for all $a, b, c \in S$:

1. $(S, +)$ forms a group, with identity element 0.
2. If $a * b = 0$, then $a = 0$ or $b = 0$.
3. $a * (b + c) = a * b + a * c$ and $(a + b) * c = a * c + b * c$.
4. There exists $e \in S$ such that $a * e = e * a = a$.

In the following work we will use the term semifield to refer to a finite semifield, and, unless otherwise noted, all other sets and systems mentioned will be assumed finite. Notice that any finite field will satisfy this definition, and thus every finite field is a semifield. The key difference is that semifield multiplication is not assumed

to be associative or commutative. By Wedderburn's theorem, associativity will imply commutativity, but the converse is not true. As noted in [7], there exist commutative semifields which are not associative, so the converse is not true.

Many of the results in this work could therefore be applied to the study of finite fields, although there is little need since finite fields are already well understood. Because of this, we will sometimes include examples of results applied to fields in addition to semifields to highlight differences between the systems. And, when it is necessary to emphasize that a semifield is not a field, we will refer to it as a *proper semifield*. In other words, in a proper semifield S, there exist $a, b, c \in S$ such that $a * (b * c) \neq (a * b) * c$.

Associative multiplication is such a common and fundamental assumption in mathematics that the effects of its absence are not always obvious. For example, exponential notation for multiplication is not well defined for powers greater than 2. The term x^2 is unambiguous and stands for $x * x$, but x^3 could mean $x * (x^2)$ or $(x^2) * x$. A similar issue arises with the idea of multiplicative inverses. Consider the following well known lemma.

Lemma 2.2 (Knuth, [11]). Let S be a semifield, and let $a, b \in S$ be nonzero. Then there exist unique x and y in S such that $a * x = b$ and $y * a = b$.

Proof. Let $S = \{0, c_1, c_2, ..., c_q\}$, and consider the set $\{a * c_1, a * c_2, ..., a * c_q\}$. Since S can have no zero divisors, $ac_i \neq 0$ for all i. Suppose there exist i, j such that $a * c_i = a * c_j$. Then $a * (c_i - c_j) = 0$, and $c_i = c_j$. Thus each $a * c_i$ must be distinct, and there must exist a unique i such that $ac_i = b$, thus $x = c_i$. A similar proof shows that there exists a unique y such that $y * a = b$. □

Consider a nonzero element $a \in S$. This lemma shows that there exist $x, y \in S$ such that $a * x = e$ and $y * a = e$. For this reason a finite semifield, like a finite field,

will have no nontrivial ideals. There are still subsets of S which are of particular interest.

Definition 2.3. Let S be a finite semifield. Then the *left nucleus*, *middle nucleus*, and *right nucleus* are the subsets N_l, N_m, and N_r of S defined by

$$N_l = \{a \in S | a * (x * y) = (a * x) * y \ \forall x, y \in S\} \tag{2.1}$$

$$N_m = \{a \in S | x * (a * y) = (x * a) * y \ \forall x, y \in S\} \tag{2.2}$$

$$N_r = \{a \in S | x * (y * a) = (x * y) * a \ \forall x, y \in S\} \tag{2.3}$$

The *nucleus*, N, of S is the intersection of N_l, N_m, and N_r.

The left, middle, and right nucleus of a semifield are sometimes referred to collectively as the *nuclei* of S. This terminology is still not entirely standard, and some authors may use the term *nucleus* to refer to N_l when it is the only nucleus being considered.

Definition 2.4. Let S be a semifield. The *center* of S, denoted Z, is the subset of S defined by

$$Z = \{x \in S | x * y = y * x \ \forall y \in S\} \tag{2.4}$$

It is worth noting that N_l, N_m, N_r, and N are all isomorphic to finite fields, by Wedderburn's theorem. Furthermore, $Z \cap N$ is also isomorphic to a finite field, and is sometimes referred to as the *associative center* of S. But Z may not be isomorphic to a finite field, and there exist cases where $Z = S$ and S is a proper semifield.

2.2 Semifields as Vector Spaces

Another useful consequence of Lemma 2.2 is that $a * 0 = 0 * a = 0$ for all $a \in S$, since $a * b = 0$ implies that a or b is zero. This, coupled with the fact that any semifield is a group under addition, yields the following useful result.

Lemma 2.5 (Knuth, [11]). Let S be a semifield. Then the following are true:

1. The group $(S, +)$ is Abelian.
2. $(S, +)$ has characteristic p, where p is a prime.
3. S is an n-dimensional vector space over the finite field of order p, $\mathbb{F}_p$.
4. $|S| = p^n$ for a prime p and positive integer n.

Proof. Let $a, b \in S$ and let e denote the multiplicative identity of S. By distributivity, we have

$$(a * e + a * e) + (b * e + b * e) = (a + b) * (e + e) = (a * e + b * e) + (a * e + b * e)$$

Since $(S, +)$ is a group, we then have

$$\begin{aligned} (a * e + a * e) + (b * e + b * e) &= (a * e + b * e) + (a * e + b * e) \\ = \quad (a + a) + (b + b) &= (a + b) + (a + b) \\ = \quad a + (a + b) + b &= a + (b + a) + b \\ = \quad a + b &= b + a \end{aligned}$$

Thus $(S, +)$ is Abelian. Now let $a \neq 0$. For any $k \in \mathbb{Z}_+$, let (ka) denote a added to itself k times. Let p denote the smallest integer such that $(pa) = 0$ and suppose there exist $m, n \in \mathbb{Z}_+$ such that $nm = p$. This gives us

$$(ma) * (na) = (m(n(a * a))) = ((mn)(a * a)) = ((mn)a) * a = (pa) * a = 0 * a = 0$$

Then $(ma) = 0$ or $(na) = 0$, which implies $m = p$ or $n = p$. Thus p is prime. Now let $a, b \in S$ and let p_1 and p_2 denote the additive orders of a and b respectively, and let x denote the multiplicative order of $(a + b)$. From the previous argument, x must be prime, but since p_1 and p_2 must both divide x, the only way this can be true is if $p_1 = p_2 = x$. Thus all elements of S have the same additive order. Thus S must be a vector space over the finite field of p elements, $\mathbb{F}_p$, with scalar multiplication

referring to repeated addition. Thus we have $|S| = p^n$, where n is the dimension of S over $\mathbb{F}_p$. □

Definition 2.6. Let S be a semifield where $|S| = p^n$. Then the *order* of S is p^n.

When discussing the number of elements in a semifield we will sometimes specify that S has p^n elements, is a p^n-element semifield, or has order p^n. Since finite fields and vectors over finite fields are also used throughout this work, we will use the notation $\mathbb{F}_p^n$ to denote the set of n-dimensional vectors over $\mathbb{F}_p$, and $\mathbb{F}_{p^n}$ to denote the finite field of p^n elements.

The fact that semifields are vector spaces provides some useful properties. If S and S' are semifields of order p^n, then $(S, +)$ and $(S', +)$ are both isomorphic to $(\mathbb{F}_p^n, +)$. Consider elements $a, b \in S$. Because multiplication is distributive, there exist linear transformations L_a and R_b such that

$$a * b = L_a(b) = R_b(a) \tag{2.5}$$

By Lemma 2.2, these transformations must be bijective. This is a very useful property, since it allows us to view multiplication in terms of linear transformations. For instance, if $R_b(a) = a * b$, then there exists R_b^{-1} such that $R_b^{-1}(a * b) = a$. Some care should be taken when working with these functions though. Consider the differences between the following:

$$\begin{aligned} R_b^2(a) &= (a * b) * b \\ R_{b^2}(a) &= a * (b * b) \end{aligned}$$

The first function is $R_b(R_b(a))$ which is distinct from $R_{b^2}(a)$, and clearly these two functions are distinct.

Finally, we can let 1 denote the multiplicative identity of S without fear of ambiguity. Let $i, j \in \mathbb{F}_p$. Then $(ij)e = (ie)(je)$ and $(i + j)e = ie + je$. Thus there is a subfield of S isomorphic to $\mathbb{F}_p$, and the multiplicative identity of S is isomorphic to

the multiplicative identity of $\mathbb{F}_p$. We will continue to let e denote the multiplicative identity of S for now to keep the notation as clear as possible, but we will switch to 1 in later chapters when it is more convenient.

2.3 Examples

As previously mentioned, every finite field is also a semifield. The following result gives a necessary condition for a semifield to be proper.

Lemma 2.7 (Knuth, [11]). If S is a proper semifield of order p^n, then $n \geq 3$.

Proof. If $|S| = p$, then S must be isomorphic to $\mathbb{F}_p$. If $|S| = p^2$, then S is two-dimensional over $\mathbb{F}_p$, and has a basis of the form $\{e, x\}$. The multiplication in S is therefore determined by $x * x = ax + be$ for $a, b \in \mathbb{F}_p$. Now consider $x^2 - ax - be = 0$. This cannot be factored, otherwise S would contain zero divisors. Thus it is irreducible and $S \cong \mathbb{F}_{p^2}$. □

Knuth also proves in section 6.1 of [11] that if $|S| = 8$, then $S \cong \mathbb{F}_8$. Thus the smallest proper semifields are of order 16. Throughout this work we will use the following three 16-element semifields for examples.

Each of these examples has elements of the form $a + \lambda b$, where $a, b \in \mathbb{F}_4$ and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$. Addition is defined in the usual way, with $(a + \lambda b) + (c + \lambda d) = (a + c) + \lambda(b + d)$, so the only distinguishing feature of these semifields is how multiplication is defined. The names "system V" and "system W" were used by Knuth in [11] as a means of identifying these constructions throughout his work, and

we will do the same here.

(2.6) $\mathbb{F}_{16}$ $(a+\lambda b)*(c+\lambda d) = (ac+bd\omega)+\lambda(bc+ad+bd)$

(2.7) System W $(a+\lambda b)*(c+\lambda d) = (ac+b^2d\omega)+\lambda(bc+a^2d)$

(2.8) System V $(a+\lambda b)*(c+\lambda d) = (ac+b^2d)+\lambda(bc+a^2d+b^2d^2)$

Notice that the multiplication in both system V and system W is very similar to that in $\mathbb{F}_{16}$, yet has been modified in a way which makes it nonassociative. Also, each of these three semifields can be viewed as a right vector space over $\mathbb{F}_4$, or as a vector space over $\mathbb{F}_2$. A valid basis over $\mathbb{F}_2$ for all three of these semifields would be $\{1, \omega, \lambda, \lambda\omega\}$, and, by distributivity, the multiplication in each semifield is determined by the products of the elements of this basis. This is the motivation behind the results in chapter 3.

2.4 Finite Projective Planes

An important application of semifields is in the study of finite projective planes, and a large portion of the existing research on semifields relates to this application. Although the later results in this work were inspired by a purely algebraic motivation, the results in this section will provide a useful tool for classifying semifields.

Definition 2.8. A *finite semifield plane* is a finite set, π, whose elements are called *points*, together with a collection of subsets, called *lines*, which is said to be *coordinatized* by a semifield, S, if the points and lines of π can be expressed in the following way, for $a, b \in S$:

$$\text{points} = \begin{cases} (1,a,b) \\ (0,1,a) \\ (0,0,1) \end{cases} \qquad \text{lines} = \begin{cases} [1,a,b] \\ [0,1,a] \\ [0,0,1] \end{cases}$$

where a point (x_1, x_2, x_3) is contained in a line $[y_1, y_2, y_3]$ if and only if

$$y_1 x_3 = x_2 * y_2 + x_1 y_3 \tag{2.9}$$

The values 0 and 1 used in the definition will be treated as scalar multiples of the semifield elements. The general term for the relationship between the points and lines in a plane is *incidence*, and we will refer to equation 2.9 as the *incidence equation*.

This notation for points and lines is not standard either; Knuth used it in [11] and it is based on a notation used by Albert in [3]. While it does not provide an intuitive view of the geometry of a semifield plane, it does give all of the points a similar form, and provides a simple means of testing whether a point is on a line via equation 2.9.

A finite semifield plane is a special case of the more general definition of a finite projective plane. We include this definition in order to better illustrate the geometric nature of the semifield planes.

Definition 2.9. A *finite projective plane* is a finite set, π, whose elements are called *points*, together with a collection of subsets, called *lines*, which satisfy the following axioms:

1. Two distinct points are contained in one and only one line.
2. The intersection of two distinct lines contains one and only one point.
3. There exist four points, no three of which are contained in the same line.

Standard geometric terms are commonly used when discussing projective planes. If a point is contained on a line it is said to *lie on* that line, and the line is said to *pass through* the point.

A more standard approach to coordinatizing projective planes using the more general ternary rings can be found in the early chapters of "Affine Planes with Tran-

sitive Collineation Groups" by Kallaher (see [9]). It can be proven that a semifield plane satisfies the axioms for a projective plane, and it is easily seen by the definition that a semifield plane contains $q^2 + q + 1$ points and $q^2 + q + 1$ lines, where q is the order of the semifield. This property is true for finite projective planes as well, where q is the number of elements in the ternary ring used to coordinatize the plane.

The following notation will become useful when discussing projective planes. Given points (a_1, a_2, a_3) and (b_1, b_2, b_3), the line passing through them will be denoted $(a_1, a_2, a_3) : (b_1, b_2, b_3)$. Given lines $[y_1, y_2, y_3]$ and $[z_1, z_2, z_3]$, the point where they intersect will be denoted $[y_1, y_2, y_3] \cap [z_1, z_2, z_3]$. Using the incidence equation, we can then derive the following definitions for the points and lines of a plane:

$$\begin{aligned} [0,0,1] &= (0,1,0) : (0,0,1) & (0,0,1) &= [0,1,0] \cap [0,0,1] \\ [0,1,a] &= (0,0,1) : (1,-a,b) & (0,1,a) &= [0,0,1] \cap [1,a,b] \\ [1,a,b] &= (0,1,a) : (1,0,b) & (1,a,b) &= [0,1,-a] \cap [1,0,b] \end{aligned} \tag{2.10}$$

Some definitions, such as $[0,1,a] = (0,0,1) : (1,-a,b)$ may seem ambiguous. Through two distinct points there exists a unique line, so how could $[0,1,a]$ stay constant for any choice of b? The incidence equation verifies this, but a more intuitive answer is that $[0,1,a]$ corresponds to the equation $x = -a$, which is a vertical line. Thus $[0,1,a] = (0,0,1) : (1,-a,b)$ for any choice of b.

2.5 Isotopism

In this section we discuss isotopisms, which can be thought of as a generalization of the concept of isomorphisms. Unlike isomorphisms, isotopisms do not preserve any of the multiplicative properties of a semifield except for nonassociativity. Thus is is possible to have commutative semifields isotopic to noncommutative semifields,

and to even have semifields isotopic to systems which do not posses a multiplicative identity.

Definition 2.10. Let S and S' be semifields of order p^n, with multiplication $*$ and $\star$ respectively. Then S is said to be *isotopic* to S' if there exist nonsingular $\mathbb{F}_p$-linear transformations, F, G, and H, from S to S' such that, for all $a, b \in S$,

$$H(a * b) = F(a) \star G(b) \tag{2.11}$$

The ordered set $\{F, G, H\}$ is said to be an *isotopism* from S to S'.

There are a number of important things to note regarding this definition. First, we could have used a more general definition of isotopism using ternary rings which assumes the functions are bijective but does not assume linearity, and many of the following results could be proven in the more general case. In particular, Theorem 2.13 can be proven without assuming linearity (see Theorem 3.2.3 in [11]), but shows that linearity is sufficient for finding all semifields isotopic to a given semifield. Thus nothing is lost by assuming linearity, and it will make the following results more straightforward.

Second, if $F = G = H$, then an isotopism is an isomorphism. Also, if S and S' are isotopic, with isotopism $\{F, G, H\}$ from S to S', then there is also an isotopism $\{F^{-1}, G^{-1}, H^{-1}\}$ from S' to S. In some cases is is more convenient to define the isotopism going from S' to S, so it is worth noting that this notion is well defined.

Finally, if there are semifields S, S_1, and S_2 such that S is isotopic to S_1, with isotopism $\{F_1, G_1, H_1\}$, and S_1 is isotopic to S_2, with isotopism $\{F_2, G_2, H_2\}$, then S is isotopic to S_2 by the isotopism $\{F_2 \circ F_1, G_2 \circ G_1, H_2 \circ H_1\}$.

Lemma 2.11 (Knuth, [11]). Let $\{F, G, H\}$ be an isotopism from $(S, +, *)$ to $(S', +, \star)$. Then

$$H = R \circ F = L \circ G \tag{2.12}$$

where $L, R : S' \mapsto S$ are defined by $L(x) = F(e) \star x$, $R(x) = x \star G(e)$ and e is the multiplicative identity of S.

Proof. Let $a \in S$. By the definition of isotopism we have

$$\begin{aligned} H(a * e) &= F(a) \star G(e) \\ = \quad H(a) &= R(F(a)) \end{aligned}$$

$$\begin{aligned} H(e * a) &= F(e) \star G(a) \\ = \quad H(a) &= L(G(a)) \end{aligned}$$

□

Theorem 2.12 (Knuth, [11]). Let S be a semifield of order p^n. Then the number of nonisomorphic semifields which are isotopic to S is at most $(p^n - 1)^2$.

Proof. Let $(S_1, +, \star_1)$ and $(S_2, +, \star_2)$ be semifields isotopic to a semifield S, and let $\{F_1, G_1, H_1\}$ and $\{F_2, G_2, H_2\}$ be isotopisms from S_1 to S and S_2 to S respectively. Let e_1 and e_2 denote the multiplicative identity elements of S_1 and S_2 respectively. We will show that if $F_1(e_1) = F_2(e_2) = y$ and $G_1(e_1) = G_2(e_2) = z$, then S_1 is isomorphic to S_2. From there, since there are at most $(p^n - 1)$ possible choices for y and z, there can be at most $(p^n - 1)^2$ nonisomorphic semifields isotopic to S.

Suppose $F_1(e_1) = F_2(e_2) = y$ and $G_1(e_1) = G_2(e_2) = z$, and let L_y and R_z be the linear transformations for left and right multiplication by y and z respectively. Then we have $L_y(x) = y*x = F_1(e_1)*x = F_2(e_x)*x$ and $R_z(x) = x*z = x*G_1(e_1) = x * G_2(e_2)$, and by Lemma 2.11 we get:

$$\begin{aligned} H_1 &= R_z \circ F_1 &= L_y \circ G_1 \\ H_2 &= R_z \circ F_2 &= L_y \circ G_2 \end{aligned}$$

Notice that $(R_z \circ F_2)^{-1} = F_2^{-1} \circ R_z^{-1}$, and thus $(R_z \circ F_2)^{-1} \circ (R_z \circ F_1) = F_2^{-1} \circ F_1$. By equivalence, we can then say

$$H_2^{-1} \circ H_1 = G_2^{-1} \circ G_1 = F_2^{-1} \circ F_1 = \phi$$

Note that since ϕ is a composition of nonsingular linear transformations, it will be bijective and preserve addition. To show it is an isomorphism from S_1 to S_2 we only need to show that it preserves multiplication. By definition, $H_2(\phi(a) \star_2 \phi(b)) = F_2(\phi(a)) * G_2(\phi(b))$. By applying H_2^{-1} to both sides of this equation we get the desired results:

$$\begin{aligned} \phi(a) \star_2 \phi(b) &= H_2^{-1}\left(F_2(\phi(a)) * G_2(\phi(b))\right) \\ &= H_2^{-1}\left(F_1(a) * G_1(b)\right) \\ &= H_2^{-1}\left(H_1(a \star_1 b)\right) \\ &= \phi(a \star_1 b) \end{aligned}$$

□

In general, $(p^n - 1)^2$ is an upper bound which is rarely attained. In the case where S is a finite field, we will later prove that there are no semifields isotopic to S which are not isomorphic to it. In regards to the examples previously given, System V is isotopic to 17 other nonisomorphic semifields, while System W is isotopic to 4 other nonisotopic semifields. The following result gives a specific means of constructing each of the $(p^n - 1)^2$ semifields isotopic to a given semifield.

Theorem 2.13 (Knuth, [11]). Let S be a semifield, $y, z \in S$ be nonzero, and L_y, R_z be the linear transformations for left and right multiplication by y and z respectively.

Let $F = R_z^{-1}$ and $G = L_y^{-1}$, and let S' be the additive group of S with multiplication $\star$ defined by

$$a \star b = F(a) * G(b)$$

Then S' is a semifield isotopic to S with multiplicative identity $y * z$. Furthermore, every semifield isotopic to S can be constructed in this way (up to isomorphism).

Proof. We will start by showing that S' satisfies the axioms of a semifield. The first axiom holds, since S' was defined to be the additive group of S with multiplication $\star$. To show S' has no zero divisors, suppose there exist $a, b \in S'$ such that $a \star b = 0$. Then $F(a) * G(b) = 0$, which implies $F(a) = 0$ or $G(b) = 0$. Without loss of generality, suppose $F(a) = 0$. Then $R_z^{-1}(a) = 0$, which is only possible if $a = 0$. Thus S' has no zero divisors. To show that S' is left distributive, consider

$$a \star (b + c) = F(a) * (G(b) + G(c)) = F(a) * G(b) + F(a) * G(c) = a \star b + a \star c$$

A similar argument shows that S' is right distributive. The final axiom to test is whether S' has a multiplicative identity, and we will now show that it will be $y * z$. First we show it is a right identity:

$$\begin{aligned} a \star (y * z) &= F(a) * G(y * z) = R_z^{-1}(a) * L_y^{-1}(y * z) = R_z^{-1}(a) * z \\ &= R_z(R_z^{-1}(a)) = a \end{aligned}$$

Similarly, we show it is a left identity:

$$\begin{aligned} (y * z) * a &= F(y * z) * G(a) = R_z^{-1}(y * z) * L_y^{-1}(a) = y * L_y^{-1}(a) \\ &= L_y(L_y^{-1}(a)) = a \end{aligned}$$

Thus, $(S', +, \star)$ is a semifield isotopic to S with isotopism $\{F, G, I\}$ from S' to S, where I is the identity map.

To show that every semifield isotopic to S can be defined in this way, we will use a result from the proof of the previous theorem. Let $(S_1, +, \star_1)$ be a semifield isotopic

to S, with isotopism $\{F_1, G_1, H_1\}$ from S_1 to S. Let e_1 be the multiplicative identity of S_1, and $F_1(e_1) = y$ and $G_1(e_1) = z$. Now consider the semifield S_2 constructed from S via the isotopism $\{F_2, G_2, H_2\}$ from S_2 to S, where $F_2 = R_z^{-1}$, $G_2 = L_y^{-1}$ and H_2 is the identity map. Then the multiplicative identity, e_2, of S_2 is equal to $y * z$, and we have $F_2(y * z) = y$, $G_2(y * z) = z$. Thus we have $F_1(e_1) = F_2(e_2)$ and $G_1(e_1) = G_2(e_2)$, and as shown in the proof of the previous theorem, S_1 is isomorphic to S_2 via the isomorphism $\phi = F_2^{-1} \circ F_1 = G_2^{-1} \circ G_1$. □

This theorem provides a very useful tool when looking at the isotopisms of semifields. As mentioned at the start of this section, applying an isotopism to a semifield could yield a system lacking a multiplicative identity! But, if the isotopism consists of $F = R_z^{-1}$ and $G = L_y^{-1}$, then the resulting system will be a semifield.

2.6 The Geometric Significance of Isotopisms

This section elaborates on the relationship between semifields and projective planes. In particular, we investigate the relationship between isomorphic projective planes and isotopic semifields.

Definition 2.14. Two projective planes, π and π' are said to be *isomorphic* if there exists a bijection $\phi : \pi \to \pi'$ which preserves incidence, i.e. if point (x_1, x_2, x_3) lies on line $[y_1, y_2, y_3]$ in π, then $\phi(x_1, x_2, x_3)$ lies on $\phi[y_1, y_2, y_3]$. An automorphism of a projective plane is called a *collineation*.

Lemma 2.15 (Knuth, [11]). Let π and π' be isomorphic semifield planes with isomorphism ϕ such that

$$\phi(1,0,0) = (1,0,0) \quad , \quad \phi(0,1,0) = (0,1,0) \quad , \quad \phi(0,0,1) = (0,0,1)$$

Then the semifields which coordinatize π and π' are isotopic.

Proof. We use equation 2.10 to help define the points and lines of π. By hypothesis we have

$$\phi[0,0,1] = \phi(0,1,0) : \phi(0,0,1) = (0,1,0) : (0,0,1) = [0,0,1]$$

Note that $\phi(0,1,a)$ lies on $\phi[0,0,1]$ and thus must lie on $[0,0,1]$. Since $[0,0,1]$ passes through $(0,1,a)$ and $\phi(0,1,a)$, there must exist a linear transformation G such that $\phi(0,1,a) = (0,1,G(a))$. This linear transformation will be the same G as in the isotopism $\{F,G,H\}$, and in a similar way we will define F and H. From the hypothesis we have

$$\phi[0,1,0] = \phi(0,0,1) : \phi(0,1,0) = (0,0,1) : (0,1,0) = [0,1,0]$$

and

$$\phi[1,0,0] = \phi(0,1,0) : \phi(1,0,0) = (0,1,0) : (1,0,0) = [1,0,0]$$

Thus there must exist linear transformations F and H such that $\phi(1,a,0) = (1,F(a),0)$ and $\phi(1,0,b) = (1,0,H(b))$. We can then see that, in general

$$\phi[0,1,a] = \phi(0,0,1) : \phi(1,-a,0) = (0,0,1) : (1,-F(a),b) = [0,1,F(a)]$$
$$\phi[1,a,b] = \phi(0,1,a) : \phi(1,0,b) = (0,1,G(a)) : (1,0,H(b)) = [1,G(a),H(b)]$$
$$\phi(1,a,b) = \phi[0,1,-a] \cap \phi[0,1,b] = [0,1,F(-a)] \cap [0,1,H(b)] = (1,F(a),H(b))$$

We can now show that the incidence relation is preserved. Recall that (x_1,x_2,x_3) lies on $[y_1,y_2,y_3]$ if and only if $y_1x_3 = x_2 * y_2 + x_1y_3$. We also know that $\phi(x_1,x_2,x_3)$ lies on $\phi[y_1,y_2,y_3]$, so we have the following relation, where the symbol "$\Leftrightarrow$" stands for "if and only if":

$$y_1x_3 = x_2 * y_2 + x_1y_3 \Leftrightarrow y_1H(x_3) = F(x_2) * G(y_2) + x_1H(y_3)$$

Without loss of generality, we can let $x_1 = y_1 = 1$, as the cases where they equal zero will be similar. Then, by linearity, we get the following

$$\begin{aligned} & x_3 = x_2 * y_2 + y_3 \quad \Leftrightarrow \quad H(x_3) = F(x_2) * G(y_2) + H(y_3) \\ \Leftrightarrow \quad & x_3 - y_3 = x_2 * y_2 \quad \Leftrightarrow \quad H(x_3 - y_3) = F(x_2) * G(y_2) \end{aligned}$$

By substitution we have $H(x_2 * y_2) = F(x_2) * G(y_2)$, and thus $\{F, G, H\}$ is an isotopism. □

Theorem 2.16 (Knuth, [11]). Let $\{F, G, H\}$ be an isotopism from a semifield S to a semifield S', and let π and π' be the semifield planes coordinatized by S and S' respectively. Then π and π' are isomorphic.

Proof. We define $\phi : \pi \to \pi'$ using the relationships in the previous theorem, i.e.

$$\begin{array}{rclrcl} \phi[0,0,1] & = & [0,0,1] & \phi(0,0,1) & = & (0,0,1) \\ \phi[0,1,a] & = & [0,1,F(a)] & \phi(0,1,a) & = & (0,1,G(a)) \\ \phi[1,a,b] & = & [1,G(a),H(b)] & \phi(1,a,b) & = & (1,F(a),H(b)) \end{array}$$

From the previous lemma we know that $\phi(1, x_2, x_3) \in \phi[1, y_2, y_3]$, but now we need to consider the cases where $x_1 = 0$ or $y_1 = 0$:

$$\begin{aligned} & (0, x_2, x_3) \in [1, y_2, y_3] \Leftrightarrow x_3 = x_2 * y_2 \Leftrightarrow x_2 = 1, y_2 = x_3 \\ \Leftrightarrow \quad & G(y_2) = G(x_2) \Leftrightarrow \phi(0, x_2, x_3) \in \phi[1, y_2, y_3] \end{aligned}$$

$$\begin{aligned} & (1, x_2, x_3) \in [0, y_2, y_3] \Leftrightarrow -y_3 = x_2 * y_2 \Leftrightarrow y_2 = 1, x_2 = -y_3 \\ \Leftrightarrow \quad & F(x_2) = -F(y_3) \Leftrightarrow \phi(1, x_2, x_3) \in \phi[0, y_2, y_3] \end{aligned}$$

$$\begin{aligned} & (0, x_2, x_3) \in [0, y_2, y_3] \Leftrightarrow x_2 = 0 \text{ or } y_2 = 0 \\ \Leftrightarrow \quad & \phi(0, x_2, x_3) \in \phi[0, y_2, y_3] \end{aligned}$$

□

This theorem is sufficient to show that isotopic semifields coordinatize isomorphic projective planes, which is sufficient to show the geometric motivations for studying semifields. The converse is also true, as shown by Albert in [3], but the proof requires developing more geometric tools, and is beyond the scope of this work.

2.7 Autotopisms and Automorphisms

An autotopism of a semifield S is an isotopism, $\{F, G, H\}$, between S and itself, i.e. $H(a * b) = F(a) * G(b)$. The set of all autotopisms of S will clearly form a group under composition, which we will denote $\mathrm{At}(S)$. Furthermore, if S and S' are isotopic, then $|\mathrm{At}(S)| = |\mathrm{At}(S')|$, since each autotopism of S' is determined by applying the isotopism from S to S' to the autotopisms of S.

In the case where $F = G = H$, the autotopism is clearly an automorphism, and if we let $\mathrm{Aut}(S)$ denote the automorphism group of S, then $\mathrm{Aut}(S) \subset \mathrm{At}(S)$.

Lemma 2.17 (Knuth, [11]). Let π be a semifield plane coordinatized by a semifield S. Then all semifields isotopic to S coordinatize π, and the collineations of π which fix $(0, 0, 1)$, $(0, 1, 0)$, and $(1, 0, 0)$ form a group isomorphic to the autotopism group of S.

Proof. This follows directly from Lemma 2.15 and Theorem 2.16. □

This leads to an interesting result which has both algebraic and geometric significance.

Theorem 2.18 (Knuth, [11]). Let S be a semifield of order p^n. Then

$$(p^n - 1)^2 = \sum_{S'} \frac{|\mathrm{At}(S)|}{|\mathrm{Aut}(S')|} \tag{2.13}$$

where S' ranges over all nonisomorphic semifields isotopic to S.

Proof. Let y and z range over the nonzero elements of S and let S' be one of the $(p^n - 1)^2$ semifields isotopic to S determined by a choice of y and z as described in Theorem

2.13. We will show that there are $|\mathrm{At}(S)|/|\mathrm{Aut}(S')|$ such isotopes isomorphic to S', which will prove the theorem.

Let S' be isomorphic and isotopic to S, with isotopism $\{R_z^{-1}, L_y^{-1}, I\}$ from S' to S, where I is the identity map, and isomorphism $\phi : S' \to S$. Then ϕ is an automorphism of S, and $\{\phi \circ R_z, \phi \circ L_y, \phi\}$ is an autotopism of S. Every autotopism of S will have this form and will be determined (up to isomorphism) by y and z. Suppose r choices of y and z yield isomorphic semifields. Then $|\mathrm{At}(S)| = r|\mathrm{Aut}(S)|$.

For any semifield S' which is isotopic to S but not isomorphic to S, we will similarly have $|\mathrm{At}(S')| = r|\mathrm{Aut}(S')|$. Since $|\mathrm{At}(S')| = |\mathrm{At}(S)|$, we have $|\mathrm{At}(S)| = r|\mathrm{Aut}(S')|$. In each case, r is the number of isotopes of S isomorphic to a particular isotope S', and thus the sum of all such r must equal $(p^n-1)^2$. This gives the desired result. □

Chapter 3

Cubical Arrays

In chapter 2, we showed that any semifield S is an n-dimensional vector space over a finite field $\mathbb{F}_p$. Let $\{x_1, x_2, ..., x_n\}$ be a basis of S. Then there is a $n \times n \times n$ set of scalars $A = \{A_{ijk}\}$, defined by

$$x_i * x_j = \sum_{k=1}^{n} A_{ijk} x_k \tag{3.1}$$

This set, A, is an example of a cubical array, and in this chapter we will provide a formal definition for cubical arrays and show how vectors and matrices can act upon them. We will then provide a number of results regarding the relationship between cubical arrays and finite semifields. All of the results and proofs in this chapter are taken from [11] and are included here for the sake of completeness. Some of the notation has been changed to reflect modern conventions and to avoid ambiguity. We have taken a more focused approach to these results than was taken in [11], so many of the proofs in this section have been modified from what appears in [11].

3.1 Cubical Array Basics

Definition 3.1. A *cubical array*, $A =$, of dimension n over a finite field, $\mathbb{F}_q$, is an $n \times n \times n$ ordered set of elements of $\mathbb{F}_q$. The (i, j, K)-th entry of A is denoted A_{ijk} where $1 \leq i, j, k \leq n$.

We will use a notation similar to A_{ijk} for vectors and matrices. Given a vector $\overline{v}$, we will let $\overline{v}_i$ denote the i-th entry of $\overline{v}$, and given a matrix $\overline{M}$, we will let $\overline{M}_{ij}$ denote the (i, j)-th entry of $\overline{M}$. When working with cubical arrays it is often useful

to construct matrices from their entries. Given a cubical array A, we defined the following matrices by fixing an index of A:

$$A_{i**} = \overline{M} \quad \Leftrightarrow \quad A_{ijk} = \overline{M}_{jk} \tag{3.2}$$

$$A_{*j*} = \overline{M} \quad \Leftrightarrow \quad A_{ijk} = \overline{M}_{ik} \tag{3.3}$$

$$A_{**k} = \overline{M} \quad \Leftrightarrow \quad A_{ijk} = \overline{M}_{ij} \tag{3.4}$$

Knuth defines a similar notation in [11] which uses superscripts in place of subscripts. It is important to note that our notation differs slightly though, with $A_{i**} = A^{i**}$ and $A_{**k} = A^{**k}$, but $A_{*j*} = (A^{*j*})^T$, where $(A^{*j*})^T)$ is the transpose of A^{*j*}. We will sometimes wish to construct vectors from the rows and columns of matrices, so we use a similar notation for that as well.

$$M_{i*} = \overline{v} \quad \Leftrightarrow \quad \overline{M}_{ij} = \overline{v}_j \tag{3.5}$$

$$M_{*j} = \overline{v} \quad \Leftrightarrow \quad \overline{M}_{ij} = \overline{v}_i \tag{3.6}$$

Note then that by fixing two of the indices of A, we get a vector. Thus A can be thought of as a three-dimensional array, a set of n square $n \times n$ matrices, or an $n \times n$ matrix whose entries are n-dimensional vectors. This notation also eliminates the need for distinguishing between row and column vectors. For the purposes of this work, all vectors will be assumed to be row vectors, and thus we will have matrices act on vectors by right multiplication, i.e. $\overline{v}\overline{M}$. Finally, we will also define the product of a vector and a cubical as follows:

$$\overline{v}A = \sum_{i=1}^{n} \overline{v}_i A_{i**} \tag{3.7}$$

Definition 3.2. A cubical array, A, is said to be *nonsingular* over a field, $\mathbb{F}_q$, if, for all nonzero $\overline{v} \in \mathbb{F}_q^n$, the matrix

$$\overline{M} = \sum_{i=1}^{n} \overline{v} A_{i**}$$

is nonsingular.

Definition 3.3. A cubical array, A, is said to be in standard form if $A_{1**} = A_{*1*} = \overline{I}$, where $\overline{I}$ is the $n \times n$ identity matrix over $\mathbb{F}_q$.

These two definitions will prove to be of immense value in the following theorem. Consider a semifield, S, of order p^n, let $\mathcal{X} = \{x_1, ..., x_n\}$ be a basis of S over $\mathbb{F}_p$, and let $a, b \in S$. Assuming we know some method for constructing S, such as those given in equations 2.6, 2.7, and 2.8, we then have two ways of viewing a and b: the forms described by the construction and the coordinate vectors with respect to $\mathcal{X}$. Since it will often be necessary to consider both views, we will use $\overline{a}$ and $\overline{b}$ to denote the vector forms of a and b respectively. If A is the cubical array defined by 3.1, we say A is the cubical array *corresponding to* S *generated by* $\mathcal{X}$. Let $c = a * b$. Then, by the distributive property of semifields, we have

$$\overline{c} = \overline{a} * \overline{b} = \left(\sum_{i=1}^{n} \overline{a}_i x_i\right) * \left(\sum_{j=1}^{n} \overline{b}_j x_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{a}_i \overline{b}_j x_i * x_j = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} \overline{a}_i \overline{b}_j A_{ijk} x_k$$

Thus the multiplication in S is completely determined by A. It is also worth noting that addition in S corresponds to standard vector addition in $\mathbb{F}_p^n$, where 0 corresponds to the zero vector. We can now prove the following result, which gives necessary and sufficient conditions for a cubical array to define a semifield.

Theorem 3.4 (Knuth, [11]). Let S be a semifield of order p^n, and let $\mathcal{X} = \{x_1, ..., x_n\}$ be a basis for S over $\mathbb{F}_p$. Then the cubical array A corresponding to S generated by $\mathcal{X}$ will be nonsingular, and will be in standard form if and only if x_1 is the multiplicative identity. Conversely, if A is a nonsingular cubical array in standard form, then equation 3.1 defines an n-dimensional semifield over $\mathbb{F}_p$ using a formal basis $\{x_1, ..., x_n\}$, where x_1 will be the multiplicative identity.

Proof. First, let A be a cubical array corresponding to S generated by $\mathcal{X}$, and let $\overline{v}, \overline{w} \in \mathbb{F}_p^n$ be nonzero. Let $\overline{M} = \overline{v}A$. Then $\overline{M}$ is nonsingular if and only if $\overline{w}\overline{M}$ is

nonzero. There exist nonzero elements $v, w \in S$ corresponding to these vectors. Since S has no zero divisors, $u = v * w$ is nonzero. Then $\overline{w}\overline{M}$ is nonzero by the following:

$$\overline{u} = \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{v}_i \overline{w}_j A_{ij*} = \sum_{j=1}^{n} \overline{w}_j \left(\sum_{i=1}^{n} \overline{v}_i A_{ij*} \right) = \sum_{j=1}^{n} \overline{w}_j \overline{M}_{j*} = \overline{w}\overline{M}$$

Therefore A is nonsingular. Notice in the previous argument that $\overline{v} * \overline{w} = \overline{w}\overline{M}$. Let e be the multiplicative identity of S, and let $\overline{F} = \sum_{i=1}^{n} \overline{e}_i A_{i**}$. Then $\overline{e} * \overline{w} = \overline{w}\overline{F}$, but since $e * w = w$, $\overline{e} * \overline{w} = \overline{w}$, and $\overline{F}$ must be the identity matrix. In a similar way, consider the following:

$$\overline{w} * \overline{e} = \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{w}_i \overline{e}_j A_{ij*} = \sum_{i=1}^{n} \overline{w}_i \left(\sum_{j=1}^{n} \overline{e}_j A_{ij*} \right) = \sum_{i=1}^{n} \overline{w}_i \overline{G}_{i*} = \overline{w}\overline{G}$$

In this case, $\overline{w} * \overline{e} = \overline{w}\overline{G} = \overline{w}$ so $\overline{G}$ must be the identity matrix as well. If $e = x_1$, then $\overline{e}_1 = 1$, and $\overline{e}_i = 0$ for $i > 1$. Plugging this into the definitions of $\overline{F}$ and $\overline{G}$ we have

$$\overline{F} = \textstyle\sum_{i=1}^{n} \overline{e}_i A_{i**} = A_{1**} = \overline{I}$$
$$\overline{G} = \textstyle\sum_{j=1}^{n} \overline{e}_j A_{ij*} = A_{*1*} = \overline{I}$$

Thus A is in standard form. This also shows that the converse is true as well, since the nonsingularity of a cubical array will ensure that no zero divisors exist, and being in standard form ensures the existence of a multiplicative identity. □

Corollary 3.5 (Knuth, [11]). Let S be a semifield of order p^n, $\mathcal{X} = \{x_1, ..., x_n\}$ be a basis of S over $\mathbb{F}_p$, and A be the cubical array corresponding to S generated by $\mathcal{X}$. Let $a, b \in S$. Then the linear transformations L_a and R_b have matrix representations with respect to $\mathcal{X}$, $\overline{L}$ and $\overline{R}$, defined by

$$\overline{L} = \sum_{i=1}^{n} \overline{a}_i A_{i**} = \overline{a}A \qquad \overline{R} = \sum_{j=1}^{n} \overline{b}_j A_{*j*} = \overline{b}A^T \tag{3.8}$$

Notice that we have introduced a new piece of notation in this corollary: the *transpose* of A. To clarify its meaning, and the fact that $\overline{b}A^T$ will still yield a nonsingular matrix, we have the following.

Definition 3.6. Let A be a cubical array. The cubical array B defined by $B_{ijk} = A_{jik}$ is called the *transpose* of A and is denoted A^T.

Lemma 3.7 (Knuth, [11]). Let A be a cubical array. Then A^T is nonsingular and in standard form if and only if A is nonsingular and in standard form.

Proof. If A is nonsingular and in standard form, it defines a semifield, S, as previously discussed. Let $B = A^T$ and let $\overline{v} \in \mathbb{F}_p^n$ be nonzero. Then there exists a nonzero $v \in S$ corresponding to $\overline{v}$, which has a linear transformation R_v with matrix form $\overline{R}$. Since R_v is a linear transformation, $\overline{R}$ is nonsingular, and thus $\sum_{j=1}^{n} \overline{v}_j A_{*j*}$ is nonsingular. By definition, $A_{*j*} = B_{j**}$, and we have $\sum_{j=1}^{n} \overline{v}_j B_{j**}$ is nonsingular, thus B is nonsingular. Further, $\overline{I} = A_{1**} = B_{*1*}$ and $\overline{I} = A_{*1*} = B_{1**}$, so B is in standard form. □

The transpose of a cubical array has further significance. Let π be a semifield plane coordinatized by S. It is well-known that the dual of π is coordinatized by a semifield, S', which is anti-isomorphic to S. This yields the following definition.

Definition 3.8. Let $(S, +, *)$ be a semifield. A semifield $(S', +, \star)$ is said to be the *dual* of S if there exists a nonsingular linear transformation $\phi : S \mapsto S'$ such that $\phi(a * b) = \phi(b) \star \phi(a)$.

Lemma 3.9 (Knuth, [11]). Let A be a cubical array corresponding to a semifield S generated by a basis $\mathcal{X} = \{x_1, ..., x_n\}$, and let S' be the dual of S, with anti-isomorphism $\phi : S \mapsto S'$. Then A^T is the cubical array corresponding to S' generated by $\phi(\mathcal{X}) = \{\phi(x_1), ..., \phi(x_n)\}$.

Proof. Applying ϕ to equation 3.1 gives us

$$\phi(x_i * x_j) = \phi\left(\sum_{k=1} A_{ijk} x_k\right) = \sum_{k=1} A_{ijk} \phi(x_k) = \phi(x_j) \star \phi(x_i)$$

Let $B = A^T$. Then we have

$$\phi(x_j) \star \phi(x_i) = \sum_{k=1} A_{ijk}\phi(x_k) \Leftrightarrow \phi(x_i) \star \phi(x_j) = \sum_{k=1} B_{ijk}\phi(x_k)$$

□

As noted at the beginning of this chapter, these results are all slightly specialized cases of results that Knuth proved in [11]. In honor of his work and the integral role that Theorem 3.4 will play in the following work, we give the following definition.

Definition 3.10. If A is a nonsingular cubical array in standard form, then A will be called a *Knuth cube*. If S is a semifield of order p^n we will let $K(S)$ denote the set of all $n \times n \times n$ Knuth cubes over $\mathbb{F}_p$ which define S.

Note that, since n and p are finite, then there are only a finite number of $n \times n \times n$ cubical arrays over $\mathbb{F}_p$, and thus $K(S)$ must be finite as well. We will further elaborate on this in future chapters, and eventually provide the size of $K(S)$.

3.2 Examples

Recall from section 2.3 that the three examples of 16-element semifields all had elements of the form $a + \lambda b$ where $a, b \in \mathbb{F}_4$ with the convention $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$. The multiplication in the three semifields was defined by

$$\begin{array}{lrcl}
\mathbb{F}_{16} & (a + \lambda b) * (c + \lambda d) & = & (ac + bd\omega) + \lambda(bc + ad + bd) \\
\text{System W} & (a + \lambda b) * (c + \lambda d) & = & (ac + b^2 d\omega) + \lambda(bc + a^2 d) \\
\text{System V} & (a + \lambda b) * (c + \lambda d) & = & (ac + b^2 d) + \lambda(bc + a^2 d + b^2 d^2)
\end{array}$$

All of these semifields are 4-dimensional vector spaces over $\mathbb{F}_2$, and a suitable basis for Knuth cubes for all three of these semifields is $\mathcal{X} = \{1, \omega, \lambda, \lambda\omega\}$. Since the cubical arrays are three-dimensional, we will express them as matrices whose entries

are vectors, i.e. $\overline{M}_{ij} = A_{ij*}$, and we will write the vectors as strings of digits. Then the cubical array generated by $\mathcal{X}$ for each semifield is:

$$\mathbb{F}_{16} \qquad F = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0001 & 0011 \\ 0010 & 0001 & 0110 & 1101 \\ 0001 & 0011 & 1101 & 1011 \end{pmatrix}$$

$$\text{System W} \qquad W = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 0100 & 1100 \\ 0001 & 0011 & 1000 & 0100 \end{pmatrix}$$

$$\text{System V} \qquad V = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 1010 & 0111 \\ 0001 & 0011 & 1111 & 1001 \end{pmatrix}$$

This is how Knuth presented cubical arrays in [11], and this representation has a number of benefits. First, consider the matrices contained in W. In order to construct W_{2**}, we look at the vectors which make up the second row of W. These vectors will form the rows of W_{2**}, and we have

$$W_{2**} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Finding W_{*2*} is also straightforward, as the rows of W_{*2*} will be the vectors which make up the second column of W:

$$W_{*2*} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

To find W_{**k}, we build a matrix whose (i, j)-th entry is the k-th entry of W_{ij*}. For instance, W_{**2} is obtained from the second entry in each vector in W:

$$W_{**2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

This representation also makes the transpose of a cubical array more intuitive, as the matrix form of W^T will be the transpose of the matrix form of W. Notice that $F = F^T$, which corresponds to the fact that $\mathbb{F}_{16}$ is commutative.

3.3 The Triple Product

So far we have only defined the product of a vector and a cubical array. In [11], Knuth devotes a great deal of work to defining a general class of products between arrays of arbitrary dimension, and the vector and cubical array product is a special case of this. For our purposes there is only one other case of Knuth's products which we will need.

Definition 3.11. Let A be an $n \times n \times n$ cubical array over $\mathbb{F}_q$, and let $\overline{F}$, $\overline{G}$, and $\overline{H}$ be $n \times n$ matrices over $\mathbb{F}_q$. Then the *triple product* of $[\overline{F}, \overline{G}, \overline{H}]$ and A is the cubical array B defined by

$$B_{ijk} = \sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \overline{F}_{ir} \overline{G}_{js} \overline{H}_{kt} A_{rst}$$

and is denoted $B = [\overline{F}, \overline{G}, \overline{H}] \times A$

Lemma 3.12 (Knuth, [11]). Let A be a cubical array of dimension n over $\mathbb{F}_q$, and let $\overline{B}$, $\overline{C}$, $\overline{D}$, $\overline{F}$, $\overline{G}$, and $\overline{H}$ be $n \times n$ matrices over $\mathbb{F}_q$. Then the following equation is true:

$$[\overline{B}, \overline{C}, \overline{D}] \times ([\overline{F}, \overline{G}, \overline{H}] \times A) = [\overline{BF}, \overline{CG}, \overline{DH}] \times A \tag{3.9}$$

Proof. The proof is straightforward, based on the definition of the triple product and matrix multiplication. First, recall that $(\overline{BF})_{xy} = \sum_{z=1}^{n} \overline{B}_{xz} \overline{F}_{zy}$. Let $B = [\overline{F}, \overline{G}, \overline{H}] \times A$ and $C = [\overline{B}, \overline{C}, \overline{D}] \times B$. Then

$$\begin{aligned}
C_{ijk} &= \sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \overline{B}_{ir} \overline{C}_{js} \overline{D}_{kt} B_{rst} \\
&= \sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \overline{B}_{ir} \overline{C}_{js} \overline{D}_{kt} \left(\sum_{x=1}^{n} \sum_{y=1}^{n} \sum_{z=1}^{n} \overline{F}_{rx} \overline{G}_{sy} \overline{H}_{tz} A_{xyz} \right) \\
&= \sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \sum_{x=1}^{n} \sum_{y=1}^{n} \sum_{z=1}^{n} \overline{B}_{ir} \overline{F}_{rx} \overline{C}_{js} \overline{G}_{sy} \overline{D}_{kt} \overline{H}_{tz} A_{xyz} \\
&= \sum_{x=1}^{n} \sum_{y=1}^{n} \sum_{z=1}^{n} (\overline{BF})_{ix} (\overline{CG})_{jy} (\overline{DH})_{kz} A_{xyz} \\
&= [\overline{BF}, \overline{CG}, \overline{DH}] \times A
\end{aligned}$$

□

Lemma 3.13 (Knuth, [11]). Let A be a cubical array of dimension n over $\mathbb{F}_q$, let $\overline{F}$, $\overline{G}$, and $\overline{H}$ be $n \times n$ matrices over $\mathbb{F}_q$, and let $B = [\overline{F}, \overline{G}, \overline{H}] \times A$. Then the following formulas are true

$$B_{i**} = \overline{G} \left(\sum_{r=1}^{n} F_{ir} A_{r**} \right) \overline{H}^T \tag{3.10}$$

$$B_{*j*} = \overline{F} \left(\sum_{s=1}^{n} G_{js} A_{*s*} \right) \overline{H}^T \tag{3.11}$$

$$B_{**k} = \overline{F} \left(\sum_{t=1}^{n} H_{kt} A_{**t} \right) \overline{G}^T \tag{3.12}$$

Proof. These formulas are also a direct consequence of the definition of the triple product and matrix multiplication. For example, to derive the first equation we start with

$$B_{ijk} = \sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \overline{F}_{ir} \overline{G}_{js} \overline{H}_{kt} A_{rst} \Leftrightarrow B_{i**} = \sum_{r=1}^{n} \overline{F}_{ir} \left(\sum_{s=1}^{n} \sum_{t=1}^{n} \overline{G}_{*s} A_{rst} \overline{H}_{*t} \right)$$

For any particular r we will let $\overline{M} = A_{r**}$, and note that $\overline{G}_{s*} \overline{H}_{*t} = (\overline{GH})_{st}$. Now consider $(\overline{GM})\overline{H}^T$. By the definition of matrix multiplication we have

$$(\overline{GM})_{xy} = \sum_{s=1}^{n} \overline{G}_{xs} \overline{M}_{sy}$$

Then

$$((\overline{GM})\overline{H}^T)_{xy} = \sum_{t=1}^{n} (\overline{GM})_{xt} \overline{H}^T_{ty} = \sum_{t=1}^{n} \sum_{s=1}^{n} \overline{G}_{xs} \overline{M}_{st} \overline{H}_{yt}$$

And thus

$$((\overline{GM})\overline{H}^T) = \sum_{t=1}^{n} \sum_{s=1}^{n} \overline{G}_{*s} \overline{M}_{st} \overline{H}_{*t}$$

Recall that $\overline{M} = A_{r**}$, so $\overline{M}_{st} = A_{rst}$, which gives the desired result, by substitution:

$$B_{i**} = \sum_{r=1}^{n} \overline{F}_{ir} \left(\sum_{s=1}^{n} \sum_{t=1}^{n} \overline{G}_{*s} A_{rst} \overline{H}_{*t} \right) = \sum_{r=1}^{n} \overline{F}_{ir} (\overline{G} A_{r**} \overline{H}^t) = \overline{G} \left(\sum_{r=1}^{n} F_{ir} A_{r**} \right) \overline{H}^T$$

The other formulas can be derived in a similar way. □

Throughout this work we will use nonsingular $n \times n$ matrices over $\mathbb{F}_p$, and the following definition provides a useful shorthand for such matrices.

Definition 3.14. The group $GL(n, q)$ is the set of all $n \times n$ invertible matrices with entries in $\mathbb{F}_q$ together with standard matrix multiplication.

Theorem 3.15 (Knuth, [11]). Let A be a nonsingular cubical array of dimension n over $\mathbb{F}_q$, and let $\overline{F}, \overline{G}, \overline{H} \in GL(n, q)$. Then $B = [\overline{F}, \overline{G}, \overline{H}] \times A$ is also nonsingular.

Proof. Let $\overline{v} \in \mathbb{F}_q^n$ be nonzero. We need to show that $\overline{v}B$ is nonsingular. By equation 3.10, we have

$$\overline{v}B = \sum_{i=1}^{n} \overline{v}_i B_{i**} = \sum_{i=1}^{n} \overline{v}_i \left(\overline{G} \left(\sum_{r=1}^{n} F_{ir} A_{r**} \right) \overline{H}^T \right) = \overline{G} \left(\sum_{i=1}^{n} \sum_{r=1}^{n} \overline{v}_i \overline{F}_{ir} A_{r**} \right) \overline{H}^T$$

Since both $\overline{G}$ and $\overline{H}$ are nonsingular, the only way $\overline{v}B$ is singular is if $\sum_{i=1}^{n} \sum_{r=1}^{n} \overline{v}_i \overline{F}_{ir} A_{r**}$ is singular. Note that $\overline{v}\overline{F} = \sum_{i=1}^{n} \overline{v}_i \overline{F}_{i*}$, so if $\overline{w} = \overline{v}\overline{F}$, then $\overline{w}_r = \sum_{i=1}^{n} \overline{v}_i \overline{F}_{ir}$. Since $\overline{F}$ is nonsingular and $\overline{v}$ is nonzero, $\overline{w}$ is nonzero. Since A is nonsingular, $\overline{w}A$ is nonsingular, and thus B is nonsingular since

$$\sum_{i=1}^{n} \sum_{r=1}^{n} \overline{v}_i \overline{F}_{ir} A_{r**} = \sum_{r=1}^{n} \overline{w}_r A_{r**}$$

□

3.4 Isotopism

In this section we present a few crucial theorems which show how the cubical arrays of isotopic semifields are related.

Theorem 3.16 (Knuth, [11]). Let S and S' be isotopic semifields of order p^n with isotopism $\{F, G, H\}$ from S' to S. Let A be a cubical array corresponding to S generated by a basis $\mathcal{X} = \{x_1, ..., x_n\}$. Let $\overline{F}, \overline{G}, \overline{H} \in GL(n, p)$ be the matrix forms of F, G, and H with respect to $\mathcal{X}$. Then $B = [\overline{F}, \overline{G}, \overline{H}^{-T}] \times A$ is a cubical array corresponding to B generated by $\mathcal{X}$.

Proof. Note that $\overline{F}$, $\overline{G}$, and $\overline{H}$ are defined by the following:

$$F(x_i) = \sum_{r=1}^{n} \overline{F}_{ir} x_r \qquad G(x_j) = \sum_{s=1}^{n} \overline{G}_{sj} x_s \qquad H(x_k) = \sum_{t=1}^{n} \overline{H}_{kt} x_t$$

Let $\star$ denote the multiplication in S', and let B be the cubical array corresponding to S' generated by $\mathcal{X}$, i.e.

$$x_i \star x_j = \sum_{k=1}^{n} B_{ijk} x_k$$

By the definition of isotopism, we also have

$$H(x_i \star x_j) = F(x_i) * G(x_j)$$

Then we have

$$\begin{aligned}
x_i \star x_j &= H^{-1}(F(x_i) * G(x_j)) \\
&= H^{-1}\left(\left(\textstyle\sum_{r=1}^{n} \overline{F}_{ir} x_r\right) * \left(\textstyle\sum_{s=1}^{n} \overline{G}_{js} x_s\right)\right) \\
&= H^{-1}\left(\textstyle\sum_{r=1}^{n} \sum_{s=1}^{n} \overline{F}_{ir} \overline{G}_{js} x_r * x_s\right) \\
&= H^{-1}\left(\textstyle\sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \overline{F}_{ir} \overline{G}_{js} A_{rst} x_t\right) \\
&= \textstyle\sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \sum_{k=1}^{n} \overline{F}_{ir} \overline{G}_{js} \overline{H}^{-1}_{tk} A_{rst} x_k
\end{aligned}$$

Then $B = [\overline{F}, \overline{G}, \overline{H}^{-T}] \times A$. □

Lemma 3.17 (Knuth, [11]). Let S be a semifield of order p^n and let $\mathcal{X} = \{x_1, ..., x_n\}$ and $\mathcal{Y} = \{y_1, ..., y_n\}$ be bases of S over $\mathbb{F}_p$. Let A and B be the cubical arrays generated by $\mathcal{X}$ and $\mathcal{Y}$ respectively, and let $\overline{C}$ be the change of basis matrix from $\mathcal{X}$ to $\mathcal{Y}$. Then

$$B = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times A$$

Proof. Note that $\overline{C}$ satisfies the following equations

$$y_i = \sum_{j=1}^{n} \overline{C}_{ij} x_j \qquad x_i = \sum_{j=1}^{n} \overline{C}^{-1}_{ij} y_j$$

From this we have

$$\begin{aligned} y_i * y_j &= \left(\textstyle\sum_{r=1}^{n} \overline{C}_{ir} x_r\right) * \left(\textstyle\sum_{s=1}^{n} \overline{C}_{js} x_s\right) \\ &= \textstyle\sum_{r=1}^{n} \sum_{s=1}^{n} \overline{C}_{ir} \overline{C}_{js} x_r * x_s \\ &= \textstyle\sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \overline{C}_{ir} \overline{C}_{js} A_{rst} x_t \\ &= \textstyle\sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{t=1}^{n} \sum_{k=1}^{n} \overline{C}_{ir} \overline{C}_{js} A_{rst} \overline{C}^{-1}_{tk} y_k \\ &= \textstyle\sum_{k=1}^{n} B_{ijk} y_k \end{aligned}$$

where, by definition of the triple product, $B = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times A$. □

We now have the means to construct a Knuth cube for any isotope of a semifield.

Theorem 3.18 (Knuth, [11]). Let S and S' be isotopic semifields, and let $A \in K(S)$. Then there exists $B \in K(S')$ such that

$$B = [\overline{C}\overline{R}^{-1}, \overline{C}\overline{L}^{-1}, \overline{C}^{-T}] \times A \tag{3.13}$$

where $\overline{R}$, $\overline{L}$, and $\overline{C}$ are the matrices corresponding to R_z, L_y, and L_{y*z} respectively for some nonzero $y, z \in S$.

Proof. This is a direct consequence of a number of previous theorems. By Theorem 2.13 there exist nonzero $y, z \in S$ such that $\{R_z^{-1}, L_y^{-1}, I\}$ is an isotopism between S and S'. Let $\mathcal{X} = \{x_1, ..., x_n\}$ be the basis which generates A, and let $\overline{R}$, $\overline{L}$, and $\overline{I}$ be the matrices corresponding to R_z, L_y and I with respect to $\mathcal{X}$. Then

$D = [\overline{R}^{-1}, \overline{L}^{-1}, \overline{I}^{-T}] \times A$ will be a cubical array corresponding to S' by Theorem 3.16. Note that D may not be in standard form, so we need to apply a change of basis from $\mathcal{X}$ to an ordered basis whose first element is the multiplicative identity of S'. By Theorem 2.13, the multiplicative identity of S' is $y * z$, so the matrix corresponding to L_{y*z} would be a suitable choice. Let $\overline{C}$ be the matrix corresponding to L_{y*z} with respect to $\mathcal{X}$. Since A is in standard form, x_1 is the multiplicative identity of S. Let $\mathcal{Y} = \{y_1, ..., y_n\}$ be defined by

$$y_i = \sum_{j=1}^{n} C_{ij} x_j$$

Since $L_{y*z}(x_1) = y * z$, $\overline{C}_{1*}$ is the vector corresponding to $y * z$ with respect to $\mathcal{X}$, which in turn is equal to y_1. Now let $B = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times D$ will be a nonsingular cubical array in standard form corresponding to S'. Then $B \in K(S')$ and

$$B = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times ([\overline{R}^{-1}, \overline{L}^{-1}, \overline{I}^{-T}] \times A) = [\overline{C}\overline{R}^{-1}, \overline{C}\overline{L}^{-1}, \overline{C}^{-T}] \times A$$

□

Chapter 4

The Relationship Between S and $\mathbb{F}_p[x]$

There does not yet exist a strong theory regarding polynomials and semifields, and the use of polynomials in the study of semifields has been limited to the minimal and characteristic polynomials of the matrices for left and right multiplication by semifield elements. Albert, [3], was probably the first to utilize the minimal polynomials of these matrices, which he used to prove the existence of a cyclic basis for semifields of order 16 and 32. Oehmke, [14], used both the minimal and characteristic polynomials to prove commutativity of a specific class of semifields. More recently, two independent proofs of the following result were presented by Rúa, Cambarro, and Ranilla in [18], and Gow and Sheekey in [6].

Theorem. Let S be a semifield, $a \in S$, and $\overline{L}$ be the matrix associated with left multiplication by a. Then a is a left primitive element of S if and only if the characteristic polynomial of $\overline{L}$ is primitive.

The work in this chapter is an attempt to build a foundation for the study of the relationship between elements of a finite semifield and the polynomial ring over an appropriate finite field. The overall structure and motivation for this work comes from Chapter 3 of *Finite fields and their applications* [12], which discusses the properties of polynomials over finite fields. And, as a direct consequence of these investigations, we provide a new proof for the previously mentioned theorem.

4.1 Exponents, Primitive Elements, and Cyclic Bases

As we mentioned in chapter 2, standard exponential notation is not well defined for semifield elements due to the nonassociativity of multiplication. A common way of addressing this issue is to define two new exponential notations which refer to repeated multiplication on the left or right. For example, if $a \in S$, we use the following inductive definition.

$$a^{(1} = aa^{(i+1} = a * a^{(i} \tag{4.1}$$

$$a^{1)} = aa^{i+1)} = a^{i)} * a \tag{4.2}$$

Due to the fact that semifields are both left and right distributive, it is common practice to present results using only the left or right multiplication. We will do the same, and focus entirely on left multiplication. The primary reason for choosing left multiplication instead of right is simply because, if $A \in K(S)$ and $\overline{a}$ is the vector form of a with respect to A, then the matrix for left multiplication by a is $\overline{a}A$. From this point on, all of the definitions and results presented will be based on left multiplication by an element. We will continue to use the term *left* in order to emphasize this choice and the fact that similar results would hold if right multiplication were used.

Definition 4.1. Let S be a semifield of order p^n. An element $a \in S$ is said to be *left primitive* if, for all nonzero $b \in S$, there exists $1 \leq i \leq p^n - 1$ such that $a^{(i} = b$.

It is well known that finite fields contain primitive elements, but finite semifields are a different matter altogether. First, note that we have defined *left* primitive elements, and similarly we could define right primitive elements. As will be illustrated in chapter 8, the left and right primitive elements of a semifield can be different. Wene conjectured in [22] that every semifield contained a right primitive element, but a counterexample was provided by Rúa, [17], of a semifield which was neither left nor right primitive. Thus we cannot assume a semifield contains left primitive

elements, but the existence of left primitive elements in semifields is common enough to warrant study.

Definition 4.2. Let S be a semifield of order p^n. Let $a \in S$ be nonzero, and let $\mathcal{L}_a$ be the set of left powers of a from 0 to $n-1$, i.e.

$$\mathcal{L}_a = \{1, a^{(1}, ..., a^{(n-1}\} \tag{4.3}$$

If $\mathcal{L}_a$ is a basis of S over $\mathbb{F}_p$, then $\mathcal{L}_a$ is called the *left cyclic basis* generated by a.

Currently, there is no proof that such a basis exists for every semifield, but there has not yet been a semifield found which does not possess such a basis. Oehmke provides a possible partial proof that such a basis exists in [14], by showing that, for a semifield, S, of order p^n the indeterminate vector $\overline{x} = (x_1, ..., x_n)$ generates a right cyclic basis of the algebra $S \otimes \mathbb{F}_p[x_1, ..., x_n]$. Thus, the matrix $\overline{M}$ whose i-th row is the $(i+1)$-st right power of $\overline{x}$ is nonsingular, and if we substitute $\overline{v} \in \mathbb{F}_p^n$ for $\overline{x}$ in $\overline{M}$, then we will get a matrix whose rows correspond to the vector form of the first $n-1$ right powers of some element of S. Note that, if there exists a $\overline{v}$ for which $\overline{M}$ remains nonsingular, then that would prove the existence of a right cyclic basis for S. By taking the determinant of $\overline{M}$, we get a polynomial $f(x_1, ..., x_n)$, which may not be homogeneous, and we would need to show that there exists $\overline{v} \in \mathbb{F}_p^n$ such that $f(\overline{v}) \neq 0$.

4.2 Left Order and Minimal Polynomial

We begin by defining properties of semifield elements analogous to those of elements of finite fields. It is useful to consider the matrices for left multiplication by semifield elements, so we will introduce a new notation which works well with our existing vector notation. Consider a semifield S of order p^n and $A \in K(S)$ defined by a basis $\mathcal{A} = \{1, x_2, ..., x_n\}$. For any $a \in S$, $\overline{a}$ is the vector corresponding to a

with respect to $\mathcal{A}$, and we will let L_a denote the matrix for left multiplication by a with respect to $\mathcal{A}$. Note that $\overline{1}$ is the first vector of the standard basis, $(1, 0, 0, ..., 0)$, which is commonly denoted e_1. Then we also have $\overline{a}A = L_a$ and

$$\overline{a} = \overline{a * 1} = \overline{a} * \overline{1} = \overline{1}L_a = e_1 L_a$$

We can now begin investigating the left multiplicative properties of semifield elements.

Lemma 4.3. For any $a \in S$, there exists an integer $k \leq p^n - 1$ such that $a^{(k} = 1$.

Proof. Consider the set $(a) = \{a^{(i}; i \in \mathbb{Z}_+\}$ of all positive left powers of a. As noted lemma 2.2, for any $a^{(i}$, there exists b_i such that $b_i a^{(i} = a$. There are, at most, $p^n - 1$ distinct b_i. If this is the case, then for some i we have $aa^{(i} = a$, in which case $a^{(i} = 1$. If there are fewer than $p^n - 1$ distinct b_i, then there exists $j < i < p^n - 1$ such that $b_i a^{(i} = b_i a^{(j}$, which gives $b_i(a^{(i} - a^{(j}) = 0$, which forces $a^{(i} - a^{(j} = 0$ and $a^{(i-j} = 1$. □

Definition 4.4. For $a \in S$, the smallest integer k such that $a^{(k} = 1$ is called the *left order* of a and denoted $\text{ord}^l(a)$.

Lemma 4.5. Let $a \in S$. Then there is a positive integer $k \leq p^n - 1$ such that $L_a^k = \overline{I}$, where $\overline{I}$ is the identity matrix.

Proof. Let $f(x)$ be the characteristic polynomial of L_a, i.e. $f(x) = |L_a - x\overline{I}|$. Since L_a is nonsingular, we have $\deg(f) = n$. Note that, by the Cayley-Hamilton theorem, $f(L_a) = 0$ and $f(0) \neq 0$. By lemma 3.1 in [12], there exists a positive integer $k \leq p^n - 1$ such that $f(x)|(x^k - 1)$. Thus $L_a^k - \overline{I} = 0$, and $L_a^k = \overline{I}$. □

Definition 4.6. The smallest integer k such that $L_a^k = \overline{I}$ is called the order of L_a, and denoted $\text{ord}(L_a)$.

Lemma 4.7. Let $a \in S$. Then $\text{ord}^l(a)|\text{ord}(L_a)$.

Proof. Let $\text{ord}^l(a) = k$. Then we have the following

$$\overline{a^{(k}} = \overline{1} = e_1 L_a^k = e_1$$

So the first row of L_a^k is e_1. Now consider $\overline{a^{(k+1}} = e_1 L_a^{k+1} = \overline{a}$. In other words, the first row of L_a^{k+1} is $\overline{a}$. In general, the first row of L_a^{k+i} will be $\overline{a^{(i}}$. Thus, the first row of L_a^j is e_1 if and only if j is a multiple of k. And so $\text{ord}^l(a)|\text{ord}(L_a)$. □

Notice that, in the case of finite fields, these results are trivial. If $a \in \mathbb{F}_{p^n}$, then $\text{ord}^l(a) = \text{ord}(a)$, and if $\text{ord}(a) = k$, then $(L_a)^k = L_{a^k} = \overline{I}$. Thus $\text{ord}(a) = \text{ord}(L_a)$.

These lemmas provide a strong foundation regarding the exponential properties of the elements of semifields. Given a polynomial $f \in \mathbb{F}_p[x]$ and $a \in S$, we define $f(a)$ in the natural way. More explicitly, for $c_i \in \mathbb{F}_p$, we have

$$f(x) = c_0 + \sum_{i=1}^{j} c_i x^i \Rightarrow f(a) = c_0(1) + \sum_{i=1}^{j} c_i a^{(i} \tag{4.4}$$

The nonassociative multiplication in S causes some trouble when evaluating polynomials, since polynomial multiplication assumes the indeterminate is self-associative. Some polynomials can be factored into a product of lesser degree polynomials, and this could cause $f(a)$ to not be well defined. For example, consider the polynomial $f(x) = x^4+x^2+1$ in $\mathbb{F}_2[x]$, and the element λ in system W. Recall that multiplication in system W is defined by

$$(a + \lambda b) * (c + \lambda d) = (ac + b^2 d\omega) + \lambda(bc + a^2 d)$$

So $\lambda^2 = \omega$, $\lambda^{(3} = \lambda\omega$, and $\lambda^{(4} = 1 + \omega$. Then $f(\lambda) = (1 + \omega) + \omega + 1 = 0$. But $f(x) = (x^2 + x + 1)^2$, and

$$(\lambda^2 + \lambda + 1)^2 = (1 + \omega + \lambda)^2 = \omega + \omega + \lambda(1 + \omega + \omega) = \lambda$$

Thus, it is worth emphasizing that when a polynomial is evaluated at a semifield element, it is evaluated in its fully expanded form as written in equation 4.4. We can now define when a semifield element is a root of a polynomial, and begin looking at the relationship between polynomials and semifield elements.

Definition 4.8. Let $f \in \mathbb{F}_p[x]$, $a \in S$, and $f(a)$ be defined by equation 4.4. If $f(a) = 0$, then a is called a *left root* of f.

Lemma 4.9. Let $a \in S$ and $f, g, h \in \mathbb{F}_q[x]$ such that $f + g = h$. Then $f(a) + g(a) = h(a)$.

Proof. Let d be the degree of h. Then, there exist $b_i, c_i \in \mathbb{F}_p$, such that

$$f(x) = \sum_{i=0}^{d} b_i x^i \qquad g(x) = \sum_{i=0}^{d} c_i x^i \qquad h(x) = \sum_{i=0}^{n} (b_i + c_i) x^i$$

Since S is distributive, we have

$$f(a) + g(a) = \left(\sum_{i=0}^{d} b_i a^{(i} \right) + \left(\sum_{i=0}^{d} c_i a^{(i} \right) = \sum_{i=0}^{d} (b_i + c_i) a^{(i} = h(a)$$

□

Lemma 4.10. Let $a \in S$ and $f, g, h \in \mathbb{F}_p[x]$ such that $fg = h$ and a is a left root of f or g. Then a is a left root of h.

Proof. This proof is not as simple as at may at first appear. As already mentioned we must look at the final form of h and show that a is a left root of that form. First, let f and g have the following forms:

$$f(x) = \sum_{i=0}^{j} b_i x^i \qquad g(x) = \sum_{i=0}^{k} c_i x^i$$

Without loss of generality, suppose a is a left root of f. Note that $h(x) = \sum_{i=0}^{k} c_i x^i f(x)$, and, by the previous lemma, a is a left root of h if and only if a is a left root of the expanded form of $c_i x^i f(x)$ for all i. Now consider

$$f_i(x) = c_i x^i f(x) = c_i b_0 x^i + c_i b_1 x^{i+1} + \cdots + c_i b_j x^{i+j}$$

By un-distributing multiples of a we obtain the desired result:

$$\begin{aligned} f_i(a) &= c_i b_0 a^{(i} + c_i b_1 a^{(i+1} + \cdots + c_i b_j a^{(i+j} \\ &= c_i a(b_0 a^{(i-1} + b_1 a^{(i} + \cdots + b_j a^{(i+j-1}) \\ &\vdots \\ &= c_i a(a(\cdots a(b_0 + b_1 a + \cdots + b_j a^{(j}) \cdots) \\ &= c_i a(a(\cdots a(0) \cdots) \\ &= 0 \end{aligned}$$

Thus $f_i(a) = 0$ for all i and $h(a) = 0$. □

Lemma 4.11. Let $a \in S$. Then there exists a unique monic polynomial of minimal degree $f \in \mathbb{F}_p[x]$ such that a is a left root of f.

Proof. Since there exists $k \leq p^n - 1$ with $a^{(k} = 1$, a is a left root of $x^k - 1$. Thus a is a left root of a monic polynomial in $\mathbb{F}_p[x]$. Let n be the lowest degree of polynomial in $\mathbb{F}_p[x]$ for which a is a left root. Suppose f and g are monic polynomials of degree n with a as a left root, with

$$f(x) = x^n + \sum_{i=0}^{n-1} b_i x^i \qquad g(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$$

Since $f(a) = g(a) = 0$, we have the following:

$$\begin{aligned} a^{(n} + \textstyle\sum_{i=0}^{n-1} b_i a^{(i} &= a^{(n} + \textstyle\sum_{i=0}^{n-1} c_i a^{(i} \\ \Rightarrow \quad \textstyle\sum_{i=0}^{n-1} b_i a^{(i} &= \textstyle\sum_{i=0}^{n-1} c_i a^{(i} \\ \Rightarrow \quad \textstyle\sum_{i=0}^{n-1} (b_i - c_i) a^{(i} &= 0 \end{aligned}$$

Let $h(x) = \sum_{i=0}^{n-1} (b_i - c_i) x^i$. Note that, since h has degree less than n, a cannot be a left root of h unless $h(x) = 0$. Thus $b_i = c_i$ for all i. □

Definition 4.12. Let $a \in S$. The unique monic polynomial of minimal degree in $\mathbb{F}_p[x]$ for which a is a left root will be called the *left minimal polynomial* of a.

As mentioned in chapter 2, if S is a semifield of order p^n, then S contains a subfield isomorphic to $\mathbb{F}_p$ consisting of scalar multiples of the multiplicative identity. It is sometimes useful to identify the elements of S which are *not* in this subfield, and we will refer to such elements as being *nonscalar*. The following lemma and corollary present some useful properties of the left minimal polynomial of a nonscalar semifield element.

Lemma 4.13. Let $a \in S$ be nonscalar, and let $f \in \mathbb{F}_p[x]$ be a monic polynomial for which a is a left root. If there exist polynomials $g, h \in \mathbb{F}_p[x]$ such that $f = gh$ and $h(x) = x - c$, then a is a left root of g.

Proof. Note that g can be written as $g(x) = \sum_{i=0}^{n-1} b_i x^i$, with $b_{n-1} = 1$. Then, f has the form

$$f(x) = \sum_{i=0}^{n-1} b_i x^i (x - c) = \left(\sum_{i=0}^{n} b_i x^{i+1} \right) + \left(\sum_{i=0}^{n-1} (-c) b_i x^i \right)$$

Since a is a left root of f, we then have

$$f(a) = \left(\sum_{i=0}^{n} b_i a^{(i+1} \right) + \left(\sum_{i=0}^{n-1} (-c) b_i a^{(i} \right) = (a - c) \left(\sum_{i=0}^{n-1} b_i a^{(i-1} \right) = 0$$

Note that $a - c \neq 0$ so $g(a) = 0$, and a is a left root of g. □

Corollary 4.14. Let $a \in S$ be nonscalar, and let $f \in \mathbb{F}_p[x]$ be the left minimal polynomial of a. Then f has no linear factors, $f(c) \neq 0$ for all $c \in \mathbb{F}_p$, and $\deg(f) < \mathrm{ord}(f)$. Consequently, f is either irreducible or the product of irreducible polynomials of at least second degree.

4.3 Determining the Left Minimal Polynomial

The left minimal polynomial of a semifield element can be determined using a method similar to the one used in [12] to find the minimal polynomial of a finite field element. Let S be a semifield of order p^n, $a \in S$, and let f be the left minimal polynomial of a. Clearly $\deg f \leq n$, otherwise S would contain a set of more than n linearly independent elements. Then f has the following form, for $c_i \in \mathbb{F}_p$, assuming some trivial c_i,

$$f(x) = c_n x^n + \cdots + c_1 x + c_0$$

Then a is a left root of f if and only if

$$\sum_{i=0}^{n} c_i \overline{a^{(i}} = 0$$

Let $\overline{M}$ be the $(n+1) \times n$ matrix whose i-th row is $\overline{a^{(i-1}}$. Let r be the rank of $\overline{M}$. Then, if $\overline{c} = (c_0, c_1, ..., c_n)$, $\overline{f(a)} = \overline{c}\overline{M}$. By the Rank-Nullity theorem, if the rank of $\overline{M}$ is r and dimension of the set of solutions is s, then $s = n+1-r$. Since $1 \leq r \leq n$, $1 \leq s \leq n$. Thus, if s coordinates of c are prescribed, the other coordinates are uniquely determined. If $s = 1$, set $c_n = 1$. If $s > 1$, set $c_n = c_{n-1} = \cdots = c_{n-s+1} = 0$, and $c_{n-s} = 1$. This remaining values of c_i will define f, and the degree of f will be r.

For example, consider the element λ in system W. We will look at the vector coordinates of the powers of λ with respect to the basis $\{1, \omega, \lambda, \lambda\omega\}$. As we've previously mentioned, $\lambda^2 = \omega$, $\lambda^{(3} = \lambda\omega$, and $\lambda^{(4} = 1+\omega$. Then, $\overline{M}$ has the following form:

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

Then we have $r = 4$ and $s = 1$. Let $\overline{c} = (c_0, c_1, c_2, c_3, 1)$, and set $\overline{c}\overline{M} = 0$. This gives $(c_0 + 1, c_2 + 1, c_1, c_3) = (0, 0, 0, 0)$, which gives $c_0 = c_2 = 1$ and $c_1 = c_3 = 0$. Thus, the left minimal polynomial for λ is $f(x) = x^4 + x^2 + 1$.

4.4 Consequences of the Left Minimal Polynomial

The existence of the left minimal polynomial has many applications. As previously mentioned, if a is a left root of a polynomial f, then a may not be a left root of any factor of f. The following lemma shows how the left minimal polynomial helps address this issue.

Lemma 4.15. Let $a \in S$ and let $f, g \in \mathbb{F}_p[x]$ with f the left minimal polynomial of a. Then $f|g$ if and only if a is a left root of g.

Proof. If $f|g$, then, by lemma 4.10, $g(a) = 0$. Suppose a is a left root of g. If $\deg(f) = \deg(g)$, then g is a scalar multiple of f and thus a is clearly a left root of g. Suppose $\deg(f) < \deg(g)$. By the division algorithm, there exist $h, r \in \mathbb{F}_p[x]$ such that $g = hf + r$, with $\deg(r) < \deg(f)$. Let $q = hf$. By lemmas 4.9 and 4.10, $q(a) = 0$, $g(a) = q(a) + r(a)$, and we have $0 = r(a)$. But $\deg(r) < \deg(f)$ and f is the minimal polynomial of a, so $r(x) = 0$. Thus $f|g$. □

Since $L_a \in GL(n, p)$, it is well known that there exists a minimal polynomial for L_a which must divide its characteristic polynomial. And since $\overline{f(a)} = e_1 f(L_a)$, a will be a left root of both the minimal and characteristic polynomials of L_a. The following lemma provides a sufficient condition for the minimal polynomials of a and L_a to be equal.

Lemma 4.16. Let $a \in S$. Let f be the minimal polynomial of a and let g be the minimal polynomial of L_a. Then $f|g$, and $f = g$ if and only if $\text{ord}^l(a) = \text{ord}(L_a)$.

Proof. As mentioned, $g(a) = 0$, so, by lemma 4.15, $f|g$. Thus there exists $h \in \mathbb{F}_p[x]$ such that $g = hf$. Since $g(L_a) = 0$, either $f(L_a) = 0$ or $h(L_a) = 0$. Note that the degrees of f and h must be less than or equal to the degree of g, but that g is the minimal polynomial of L_a. Thus f or h must be trivial. Since f is not trivial, h must be, and we have $f = g$. Conversely, if $f = g$, then clearly $\text{ord}^l(a) = \text{ord}(L_a)$. □

Note that an element $a \in S$ will define a cyclic basis if and only if its left minimal polynomial has degree n. This yields the following.

Corollary 4.17. Let $a \in S$, and let L_a be the matrix for left multiplication by a with respect to some basis. If the characteristic polynomial of L_a is irreducible, then a defines a cyclic basis.

Recall that, for $f \in \mathbb{F}_p[x]$, the order of f, denoted $\text{ord}(f)$, is the smallest integer k such that $f|(x^k - 1)$. For $a \in S$, if f is the left minimal polynomial of a, and $k = \text{ord}^l(a)$, then by definition $a^{(k} = 1$, a is a left root of $x^k - 1$, and we have $f|(x^k - 1)$. This yields the following important result.

Theorem 4.18. Let $a \in S$ and let f be the left minimal polynomial of a. Then $\text{ord}^l(a) = \text{ord}(f)$.

This rather straightforward result allows us to study the algebraic properties of a semifield element by studying its left minimal polynomial. The following theorem summarizes a number of results that follow directly from the previous theorem and results from [12] regarding the order of a polynomial.

Theorem 4.19. Let $a \in S$, let f be the left minimal polynomial of a, and let $\text{ord}^l(a) = k$. Then the following are true:

1. If f is irreducible and $\deg(f) = n$, then $k|(p^n - 1)$.
2. Let c be a positive integer. Then $f|(x^c - 1)$ if and only if $k|c$.

3. If $f = g^b$ where b is a positive integer and $g \in \mathbb{F}_p[x]$ is irreducible with $g(0) \neq 0$ and $\text{ord}(g) = c$. Then $k = cp^t$, where t is the smallest integer such that $p^t \geq b$.
4. If $g_1, ..., g_n \in \mathbb{F}_p[x]$ are pairwise relatively prime, and $f = g_1 \cdots g_n$, then $k = \text{lcm}(\text{ord}(g_1), ..., \text{ord}(g_n))$.
5. If $f = bf_1^{c_1} \cdots f_n^{c_n}$, where $b \in \mathbb{F}_p$, $c_1, ..., c_n$ are positive integers, and $f_1, ..., f_n \in \mathbb{F}_p[x]$ are distinct monic irreducible polynomials, then $k = dp^t$ where $d = \text{lcm}(\text{ord}(f_1), ..., \text{ord}(f_n))$, t is the smallest positive integer greater than or equal to $\max(c_1, ..., c_n)$.
6. f is a primitive polynomial of degree n over $\mathbb{F}_p$ if and only if $k = p^n - 1$.

This theorem provides some useful tools for studying semifield elements. For example, if the left minimal polynomial of a is irreducible, then $a^{(p^n} = a$. In the case of a finite field this is always true, but in a semifield, the order of an element may not divide $p^n - 1$.

We conclude by proving the result from the beginning of this chapter, which follows almost directly from the previous results.

Corollary 4.20. Let $a \in S$ and let f be the left minimal polynomial of a. Then a is left primitive if and only if f is a left primitive polynomial of degree n over $\mathbb{F}_p$.

Theorem 4.21. An element $a \in S$ is left primitive if and only if the characteristic polynomial of L_a is primitive.

Proof. Let f be the left minimal polynomial of a and g the characteristic polynomial of L_a. First, suppose a is left primitive. Then f is primitive, which implies that f is irreducible and $\deg(f) = n$. Also, f must divide the minimal polynomial of L_a, which must divide g, so $f|g$. Since L_a is an $n \times n$ matrix, $\deg(g) = n$ as well, so $f = g$. Thus the characteristic polynomial of L_a is primitive. Now, suppose g is

primitive. Then g is irreducible and f must divide g. Thus $f = g$ and f is a primitive polynomial of degree n over $\mathbb{F}_p$. Thus a is left primitive. $\square$

Chapter 5

Determining Aut(S)

Presently, all of the results regarding the automorphism groups of semifields have been found for very specific cases. Wene ([23], [24]) has determined the automorphism groups of semifields following particular constructions. Al-ali, [1], has determined the automorphism group of semifields of order q^4 which admit $\mathbb{Z}_2 \times \mathbb{Z}_2$ as an automorphism group which acts freely on the semifield, where $q > 3$ is a prime power. The main results in this chapter provide a tool which can be used to determine the automorphism group of any semifield using a brute-force approach.

5.1 Investigating $K(S)$

Theorem 3.4 states that any Knuth cube of dimension n over $\mathbb{F}_p$ can define a semifield using a formal basis, $\mathcal{X} = \{x_1, ..., x_m\}$. Note that the coordinate vector for x_i with respect to $\mathcal{X}$ will be e_i, the i-th standard basis vector. For this reason, rather than using a Knuth cube to define a semifield over a formal basis, it is more convenient to simply define a semifield product on $\mathbb{F}_p^n$ by using the Knuth cube to define the products of the elements of the standard basis.

Definition 5.1. Let S be a semifield of order p^n, $A \in K(S)$, and let $\{e_1, ..., e_n\}$ denote the standard basis of $\mathbb{F}_p^n$. Then $*_A$ denotes the semifield product on $\mathbb{F}_p^n$ defined by

$$e_i *_A e_j = \sum_{k=1}^{n} A_{ijk} e_k \tag{5.1}$$

In this case, $S = (\mathbb{F}_p^n, +, *_A)$, where $+$ denotes standard vector addition, and e_1 is the multiplicative identity. Note that, viewing S in this way, any other cube in $K(S)$ must be defined by an ordered basis of $\mathbb{F}_p^n$, $\mathcal{Y} = \{y_1 = e_1, y_2, ..., y_n\}$. The

change of basis matrix, $\overline{C}$, from the standard basis to $\mathcal{Y}$ will have the form $\overline{C}_{1*} = y_i$. This leads us to the following results.

Lemma 5.2. Let $C(n,p)$ denote the set of all $\overline{X} \in GL(n,p)$ whose first row is e_1. Then $C(n,p)$ is a subgroup of $GL(n,p)$.

Proof. Clearly the identity matrix, $\overline{I}$, is in $C(n,p)$. Let $\overline{X}, \overline{Y} \in C(n,p)$. Since $\overline{Y} \in GL(n,p)$, $\overline{Y}^{-1}$ exists, and $\overline{YY}^{-1} = \overline{I}$. By assumption $\overline{Y}_{1*} = e_1$, so $e_1\overline{Y}^{-1} = \overline{I}_{1*} = e_1$, and thus $\overline{Y}_{1*}^{-1} = e_1$, and $\overline{Y}^{-1} \in C(n,p)$. If $\overline{Z} = \overline{XY}^{-1}$, then $\overline{Z} \in C(n,p)$ by the following

$$\overline{Z}_{1*} = \overline{X}_{1*}\overline{Y}^{-1} = e_1\overline{Y}^{-1} = e_1$$

□

Theorem 5.3. Let S be a semifield of order p^n, $A \in K(S)$, and $\overline{C} \in C(n,p)$. Then $[\overline{C}, \overline{C}, \overline{C}^{-T}] \times A$ defines a group action of $C(n,p)$ on $K(S)$.

Proof. By Lemma 3.17 we know that $B = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times A$ defines S. We now show that B is in standard form. From equation 3.10, , we have

$$B_{1**} = \overline{C}\left(\sum_{i=1}^{n} \overline{C}_{1i} A_{i**}\right)\overline{C}^{-1} = \overline{CIC}^{-1}$$

Similarly, by equation 3.11,

$$B_{*1*} = \overline{C}\left(\sum_{j=1}^{n} \overline{C}_{1j} A_{*j*}\right)\overline{C}^{-1} = \overline{CIC}^{-1} = \overline{I}$$

Thus B is in standard form, and we have $B \in K(S)$. Finally, for $\overline{C}, \overline{D} \in C(n,p)$, we need

$$[\overline{C}, \overline{C}, \overline{C}^{-T}] \times ([\overline{D}, \overline{D}, \overline{D}^{-T}] \times A) = [\overline{CD}, \overline{CD}, (\overline{CD})^{-T}] \times A$$

Note that $\overline{C}^{-T}\overline{D}^{-T} = (\overline{D}^{-1}\overline{C}^{-1})^T = (\overline{CD})^{-T}$. Then this is true by Theorem 3.12.

□

Consider the results of this theorem in terms of building semifields from $\mathbb{F}_p^n$. Let $\mathcal{A}$ and $\mathcal{B}$ be distinct bases of S over $\mathbb{F}_p$, and $A, B \in K(S)$ the Knuth cubes defined by $\mathcal{A}$ and $\mathcal{B}$ respectively. Let $*_A$ and $*_B$ denote the multiplication defined by A and B acting on the standard basis. Then, there is a linear transformation C corresponding to the matrix $\overline{C} \in C(n,p)$ satisfying $B = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times A$, such that $\forall a, b \in S$,

$$C(a *_A b) = C(a) *_B C(b)$$

And we have $C : (\mathbb{F}_p^n, +, *_A) \mapsto (\mathbb{F}_p^n, +, *_B)$ is an isomorphism. Note that $(\mathbb{F}_p^n, +, *_A) = (\mathbb{F}_p^n, +, *_B)$ if and only if $A = B$. Thus we have proven the following result.

Theorem 5.4. Let S be a semifield of order p^n, $A \in K(S)$, and $S = (\mathbb{F}_p^n, +, *_A)$. Then $\overline{C} \in C(n,p)$ is an automorphism of S if and only if $A = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times A$.

In practice, suppose we have a semifield S of order p^n. We first generate a Knuth cube A for S, and give S the form $(\mathbb{F}_p^n, +, *_A)$. Then, $\mathrm{Aut}(S)$ is the subgroup of $C(n,p)$ which fixes A, i.e. the stabilizer of A. This fact allows us to determine the size of $K(S)$.

Lemma 5.5. $|C(n,p)| = \prod_{i=1}^{n-1}(p^n - p^i)$.

Proof. This is a straightforward result due to the fact that, if $\overline{C} \in C(n,p)$, then $\overline{C}_{1*} = e_1$ and the remaining rows must be linearly independent. □

Corollary 5.6.

$$|K(S)| = \frac{|C(n,p)|}{|\mathrm{Aut(S)}|} = \frac{\prod_{i=1}^{n-1}(p^n - p^i)}{|\mathrm{Aut}(S)|}$$

Proof. As noted in Lemma 5.5, each matrix in $C(n,p)$ corresponds to one of the possible bases which define a Knuth cube for S. Let $\mathcal{A}$ be a basis which defines $A \in K(S)$. Then, for each $\phi \in \mathrm{Aut}(S)$, $\phi(\mathcal{A})$ is a distinct basis which also defines A. □

5.2 Utilizing Properties of Automorphisms

Clearly $C(n,p)$ can be quite large, and, even with computer assistance, a brute force approach to determining $\mathrm{Aut}(S)$ from $C(n,p)$ could take an impractically long time. The work in this section aims to address this problem by significantly reducing the number of matrices which need to be tested. Recall that, for $z \in S$, the notation $z^{(i}$ refers to repeated *left* multiplication.

Lemma 5.7. Let S be a semifield of order p^n, $z \in S$, and $\phi \in \mathrm{Aut}(S)$. Then $\phi(z^{(i}) = \phi(z)^{(i}$. Also, if $\mathcal{L}_z$ is a basis of S, then so is $\mathcal{L}_{\phi(x)}$.

Proof. By definition of the left powers of z and of automorphisms, we have

$$\phi(z^{(i}) = \phi(z * z^{(i-1}) = \phi(z) * \phi(z^{(i-1}) = \phi(z) * (\phi(z) * \cdots * (\phi(z) * \phi(z)) \cdots) = \phi(z)^{(i}$$

□

Corollary 5.8. Let $z \in S$, $\phi \in \mathrm{Aut}(S)$. Then the following are true.

1. If f is the left minimal polynomial of z, then f is the left minimal polynomial of $\phi(z)$.
2. If z is left primitive, then $\phi(z)$ is left primitive.
3. If $\mathcal{L}_z$ is a basis of S, then $\mathcal{L}_{\phi(z)}$ is also a basis of S.

This corollary provides a means by which we can reduce the number of matrices which need to be tested. Consider a semifield, S, of order p^n and $A \in K(S)$. First, determine the characteristic polynomial, f_z, of $\overline{z}A$ for all nonzero $z \in S$. Make a list, $\mathcal{P}$, of all z for which f_z is primitive, and a list, $\mathcal{I}$, of all z for which f_z is irreducible. Note that, as mentioned in chapter 4, there is no guarantee that $\mathcal{P}$ or $\mathcal{I}$ will actually contain any elements, but the empirical evidence suggests that $\mathcal{I}$ should not be empty. Suppose $\mathcal{P}$ is not empty. Then pick a particular $z \in \mathcal{P}$ with left minimal polynomial f and make a new list $\mathcal{P}'$ of all $y \in \mathcal{P}$ which also have f as their

left minimal polynomial. Let $\overline{C}$ be defined by $\overline{C}_{i*} = \overline{z^{(i-1)}}$, and construct the cubical array $B = [\overline{C}, \overline{C}, \overline{C}^{-T}] \times A$. At this point B is the cubical array for S generated by $\mathcal{L}_z$. For all $y \in \mathcal{P}'$, $\overline{y}\overline{C}$ will be the vector for y with respect to $\mathcal{L}_z$. Thus, for each $y \in \mathcal{P}'$, let $\overline{D}$ be the matrix defined by $\overline{D}_{i*} = (\overline{y^{(i-1}}\overline{C})_{i*}$. Then, determine which $\overline{D}$ satisfy $B = [\overline{D}, \overline{D}, \overline{D}^{-T}] \times B$. These matrices will be the automorphisms of S with respect to $\mathcal{L}_z$. If $\mathcal{P}$ is empty, then a similar approach using $\mathcal{J}$ will yield similar results. If both $\mathcal{P}$ and $\mathcal{J}$ are empty, then some other means of reducing the number of matrices to test must be found.

We provide an application of this method in section 5.4. For now, note that it should reduce the number of matrices to check from $|C(n,p)|$ to $p^n - p$. The only case where this may not work is if the semifield in question does not have a cyclic basis.

5.3 Automorphisms of System V

System V is an interesting example because it has 6 automorphisms, which is more than any other 16-element semifield, including $\mathbb{F}_{16}$. Recall that the elements in system V have the form $a + \lambda b$, where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$. Addition is defined in the standard way, and multiplication is defined by

$$(a + \lambda b) * (c + \lambda d) = ac + b^2 d + \lambda(bc + a^2 d + b^2 d^2)$$

Then $\mathcal{A} = \{1, \omega, \lambda, \lambda\omega\}$ is a basis for system V over $\mathbb{F}_2$ which generates the following Knuth cube:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 1010 & 0111 \\ 0001 & 0011 & 1111 & 1001 \end{pmatrix}$$

Since $|C(4,2)| = 1,344$, it is a simple matter to find all $\overline{C}$ in $C(4,2)$ such that $[\overline{C}, \overline{C}, \overline{C}^{-T}] \times A = A$. By computation, the following matrices were found:

$$1.\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad 2.\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad 3.\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$4.\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad 5.\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad 6.\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

If we view system V as $(\mathbb{F}_2^4, +, *_A)$, then each of these matrices is actually an automorphism. Additionally, we can use these matrices to find more algebraically significant definitions of the automorphisms. We will let ϕ_i denote the automorphism corresponding to the i-th matrix listed above. Recall that the rows of these matrices are the vectors of the images of the basis elements under the automorphisms. For example, the second matrix gives the following information about ϕ_2:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \Rightarrow \begin{array}{lcl} \phi_2(1) & = & 1 \\ \phi_2(\omega) & = & \omega \\ \phi_2(\lambda) & = & \lambda\omega \\ \phi_2(\lambda\omega) & = & \lambda + \lambda\omega \end{array}$$

Since $\lambda+\lambda\omega = \lambda(1+\omega) = \lambda\omega^2$, we can see that ϕ_2 is defined as $\phi_2(a+\lambda b) = a+\lambda(b\omega)$. In a similar fashion, all of the automorphisms of system V can be found:

$$\phi_1(a+\lambda b) = a+\lambda b \qquad \phi_2(a+\lambda b) = a+\lambda(b\omega) \qquad \phi_3(a+\lambda b) = a+\lambda(b\omega^2)$$
$$\phi_4(a+\lambda b) = a^2+\lambda(b^2) \quad \phi_5(a+\lambda b) = a^2+\lambda(b^2\omega) \quad \phi_6(a+\lambda b) = a^2+\lambda(b^2\omega^2)$$

5.4 Automorphisms of Sandler's Construction of order 3^{3^2}

This is a specific case of a general construction discovered by Sandler, [20]. In this case, S consists of elements of the form $a_0 + \lambda a_1 + \lambda^2 a_2$, where $a_i \in \mathbb{F}_{27}$, with addition defined in the standard way and multiplication defined by

$$\begin{aligned} (\lambda^{(i} x) * (\lambda^{(j} y) &= \lambda^{(i+j} x^{3^j} y \\ \lambda^{(3} &= \omega \\ \lambda^{(4} &= \lambda\omega \end{aligned}$$

where ω is a primitive element of $\mathbb{F}_{27}$ satisfying $\omega^3 + 2\omega + 1 = 0$. This semifield will be 9 dimensional over $\mathbb{F}_3$, and an obvious choice of basis would be

$$\mathcal{A} = \{1, \omega, \omega^2, \lambda, \lambda\omega, \lambda\omega^2, \lambda^2, \lambda^2\omega, \lambda^2\omega^2\}$$

We will let A denote the Knuth cube defined by this basis. Note that $|C(9,3)| \approx 1.3 \times 10^{34}$, so testing each $\overline{C} \in C(9,3)$ would be unfeasible even with the aid of a computer. On the other hand $|S| = 19,683$, so we can use the results from section 5.2 to find the automorphisms of S. First we determine whether S has any left primitive elements. To do this we check the matrix for left multiplication by each element of S with respect to $\mathcal{B}$ and find its characteristic polynomial. By Theorem 4.21 such a polynomial will be primitive of degree 9 over $\mathbb{F}_3$. Let R be the set of all $z \in S$ for which the characteristic polynomial of the matrix for left multiplication by z is $x^9 + 2x^6 + x^2 + 2x + 1$. By computation, $|R| = 39$, and one of the elements in R is $2\omega^2 + \lambda$. Let $\overline{P}$ be the matrix whose i-th row is the vector corresponding to $(2\omega^2 + \lambda)^{(i-1}$, and let $B = [\overline{P}, \overline{P}, \overline{P}^{-T}] \times A$. Note that B is generated by $\mathcal{L}_{(2\omega^2+\lambda)}$, and any other basis which generates B must equal $\mathcal{L}_z$ for some $z \in R$. Thus, to find $\overline{Q}$ such that $B = [\overline{Q}, \overline{Q}, \overline{Q}^{-T}] \times B$, we need only consider matrices where i-th row is the vector corresponding to the i-th term of $\mathcal{L}_z$ with respect to $\mathcal{L}_{(2\omega^2+\lambda)}$.

By computation, 13 such matrices were found; hence there are 13 automorphisms. For each such $\overline{Q}$, we can determine the automorphism with respect to $\mathcal{A}$ by looking at $\overline{P}^{-1}\overline{QP}$. Since $|\mathrm{Aut}(S)| = 13$, we know $\mathrm{Aut}(S) \cong \mathbb{Z}_{13}$, and we thus only need to determine one non-trivial automorphism to generate the group. We make the following choice for $\overline{P}^{-1}\overline{QP}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Let $z \in S$ have the form $z_0 + \lambda z_1 + \lambda^2 z_2$. Then the automorphisms of S will clearly preserve z_0 and act on λz_1 and $\lambda^2 z_2$ independently. Consider $\phi(\lambda z_1)$, with $z_1 = b_0 + b_1\omega + b_2\omega^2$ where $b_i \in \mathbb{F}_3$. The center block of the matrix then tells us $\phi(\lambda z_1) = \lambda(b_2 + (2b_0 + 2b_2)\omega + 2b_1\omega^2$. Note that

$$\begin{aligned} 2\omega(b_0 + b_1\omega + b_2\omega^2) &= 2b_0\omega + 2b_1\omega^2 + 2b_2\omega^3 \\ &= 2b_0\omega + 2b_1\omega^2 + 2b_2(2 + \omega) \\ &= b_2 + (2b_0 + 2b_2)\omega + 2b_1\omega^2 \end{aligned}$$

Thus $\phi(\lambda z_1) = \lambda(2z_1\omega)$. Similarly, $\phi(\lambda^2 z_2) = \lambda^2(2z_2\omega + z_2\omega^2)$. Since ω is primitive, we can define these mappings as powers of ω to get

$$\phi(z_0 + \lambda z_1 + \lambda^2 z_2) = z_0 + \lambda(z_1\omega^{14}) + \lambda^2(z_2\omega^4)$$

As previously noted, this automorphism generates the automorphism group, and therefore any automorphism of this semifield will have the form

$$\phi_i(z_0 + \lambda z_1 + \lambda^2 z_2) = z_0 + \lambda(z_1\omega^{14i}) + \lambda^2(z_2\omega^{4i})$$

for some positive integer $1 \leq i \leq 13$, with the identity automorphism corresponding to $i = 13$.

Chapter 6

Constructions and Enumerations

In this chapter we address the enumeration and construction of semifields. We will start by discussing the orders for which all semifields have been found (enumerated), and then give a brief description of the classical algebraic constructions. The methods used to enumerate semifields are all equivalent to determining Knuth cubes for all such semifields, but this yields little information about the algebraic structure of those semifields. For this reason, when we discuss the algebraic constructions we will also investigate what form a Knuth cube corresponding to each construction would have. Knowing this we can then determine which constructions corresponds to a semifield with a given set of Knuth cubes.

6.1 Early Enumeration - Kleinfeld and Walker

As mentioned in chapter 2, the smallest proper semifields are of order 16. It is only fitting then that these were the first semifields to be completely determined. In 1960, Kleinfeld, [10], determined all 16-element Veblen-Wedderburn systems, which satisfy all of the semifield axioms except for left distributivity, i.e. $a * (b + c)$ was not assumed to equal $a * b + a * c$. The lack of zero divisors causes the multiplication table for the nonzero elements of a Veblen-Wedderburn system to be a Latin square. Kleinfeld used this fact and some linear algebra to show that the entire multiplication table could be determined once a small number of entries were determined. He then used a computer to generate and sort all of the possible multiplication tables for

Veblen-Wedderburn systems. Since semifields are a special case of these systems, this list includes all of the 16-element semifields as well. There are 24 such semifields, up to isomorphism, in three isotopism classes. The first class consists only of $\mathbb{F}_{16}$. The second consists of system W and 4 other semifields. The third consists of system V and 17 other semifields.

Shortly after this, in 1963, Walker, [21], determined all of the 32-element semifields. In [3], Albert proved that any 32-element semifield is isotopic to a 32-element semifield which has a right cyclic basis $\mathcal{B} = \{1, b, b^2, b^2 * b, (b^2 * b) * b\}$, where $(b^2 * b) * b$ was either equal to b^2+1 or $b+1$. Walker noted that the multiplication in the semifield is entirely determined by the products of the elements of $\mathcal{B}$, so he used a computer to determine all of the possible products of the basis elements. Note that this is essentially equivalent to finding all of the cubical arrays determined by such a basis. Walker then computed all of the possible isotopes of these semifields using a result similar to Theorem 2.13. Walker discovered that there were 6 isotopism classes for the 32 element semifields, and provided a representative from each class.

6.2 Recent Enumerations by Rúa, Combarro, and Ranilla

For about 45 years after Walker's work no further enumerations were attempted, which is likely due to a lack of computing power. The semifields of order 27 could likely have been computed, but there was no need due to Menichetti, [13], proving that all semifields of dimension 3 are Albert twisted fields (see section 6.12).

By Theorem 3.4, every semifield of order p^n is defined by an n-dimensional Knuth cube over $\mathbb{F}_p$. Suppose we wanted to enumerate the semifields of order 64. We would consider all cubical arrays, A, of dimension 6 over $\mathbb{F}_2$ which are in standard form. Then $A_{1**} = A_{*1*} = \overline{I}$, and $A_{ij*} \neq (0,0,0,0,0,0)$ otherwise A would not be nonsingular. Thus, for $1 < i, j \leq 6$, A_{ij*} has $2^6 - 1 = 63$ possible values. This results

in $63^{25} \approx 9.6 \times 10^{44}$ possible choices for A which would each then need to be tested for nonsingularity. This would be a straightforward method which would take far too long to be practical. And, as the dimension of the semifields increases, so too does the number of cubical arrays which would need to be tested. For the 81-element semifields only $80^9 \approx 1.3 \times 10^{17}$ would need to be tested, while for the 243-element semifields, $242^{16} \approx 1.3 \times 10^{38}$ would need to be tested.

Thus the developments in enumerating semifields based on cubical arrays are based on finding ways to reduce the number which need to be tested. Results such as that used by Walker can help quite a bit, as simply knowing that only two possible cyclic bases exist reduces the number of cubical arrays from 31^{16} to 31^{11}. This number can be further reduced by building the cubical arrays to be nonsingular. Though it may seem like it would be slower, it is actually far quicker to make successive choices of A_{ij*} by removing linear combinations of previous choices. For example, in a 4-dimensional cubical array, if $A_{22*} = (0, 1, 1, 0)$, then A_{2j*} and A_{i2*} cannot equal any scalar multiple $(0, 1, 1, 0)$. Similarly, A_{42*} cannot be a linear combination of A_{12*}, A_{22*} and A_{32*}.

This is essentially the approach taken by Rúa, Combarro, and Ranilla in [18], which enumerates all of the 64 element semifields and was published in 2009. Since then, they have continued to refine their search algorithm to enumerate the semifields of order 3^5 and 7^4 in [19] and [4] respectively. It is interesting to note that the problem has shifted more towards the realm of computer science, as the major advancement in [4] was in a more efficient implementation of their search algorithm which allowed for parallel processing.

6.3 Reverse Decimal Matrix Notation

In this section we introduce a useful notation for discussing the properties of Knuth cubes. For a cubical array, A, of dimension n over $\mathbb{F}_p$, we will construct a matrix, $\overline{A}$, where $\overline{A}_{ij}$ is a number representing the vector A_{ij*}. To ensure that this notation is well-defined, we will use a variant of changing from base p to base 10.

First, let us identify the standard basis vectors of $\mathbb{F}_p^n$ as follows: $\widehat{p^0} = \hat{1} = e_1$, $\hat{p} = e_2$, $\cdots$, $\widehat{p^{n-1}} = e_n$. Then, define the sums of vectors (modulo p) as

$$\sum_{k=1}^{n} a_k \widehat{p^{k-1}} = \sum_{k=1}^{n} a_k e_k = \widehat{\sum_{k=1}^{n} a_k p^{k-1}} \tag{6.1}$$

Thus, given a vector $\overline{v} \in \mathbb{F}_p^n$, we treat the coordinates of $\overline{v}$ as the reversed digits of a number in base p. By reversing these digits and converting the number to base 10, we get the reverse decimal form of $\overline{v}$.For example, in $\mathbb{F}_2^4$, the basis vectors are $\hat{1} = (1,0,0,0)$, $\hat{2} = (0,1,0,0)$, $\hat{4} = (0,0,1,0)$ and $\hat{8} = (0,0,0,1)$. Addition is modulo 2, so $\hat{2} + \hat{2} = 0$. To find the reverse decimal form of the vector $(0,1,1,1)$ we would consider the base 10 value of the binary number 1110, which is 14, so the reverse decimal form of $(0,1,0,1)$ is $\widehat{14}$. Alternatively, we could use the definition of the standard basis and equation 6.1 to get

$$(0,1,1,1) = e_2 + e_3 + e_4 = \hat{2} + \hat{4} + \hat{8} = \widehat{14}$$

Next, we apply this to a cubical array by converting the vectors A_{ij*}. That is, given a cubical array A, we define the matrix $\overline{A}$ as

$$\overline{A}_{ij} = \sum_{k=1}^{n} \widehat{p^{k-1}} A_{ijk} \tag{6.2}$$

We will call $\overline{A}$ the *reverse decimal matrix* of A, and denote their relationship by $A \sim \overline{A}$. Similarly, if $\hat{v}$ is the reverse decimal form of $\overline{v}$, then we will write $\overline{v} \sim \hat{v}$. The hat notation is used in this section to emphasize that the digits used are representing

vectors and not numbers. The hat is not necessary once the notation is understood, and for this reason the results in the following sections will not have it.

This notation has many benefits. First, it is easier to present than a cubical array, but can easily be converted into a cubical array using (6.2). Second, the matrices for left and right multiplication by various basis elements can be computed. To find the matrix $\overline{R}$ for right multiplication by e_j, consider the column $\overline{A}_{*j}$. Then for each $\overline{A}_{ij}$ in that column, and each $\overline{v}$ associated with it by 6.1, $\overline{R}_{i*} = \overline{v}$. Similarly, to find the matrix $\overline{L}$ for left multiplication by e_i, consider the row $\overline{A}_{i*}$. Then, for each $\overline{A}_{ij}$ in that row, and each $\overline{v}$ corresponding to it, $\overline{L}_{j*} = \overline{v}$.

A third benefit of the reverse decimal matrix is that it can easily be used as a multiplication table for the basis elements of S. Given basis elements $\widehat{p^a}$, $\widehat{p^b}$, with $0 \leq a, b < n$, the product $\widehat{p^a} \cdot \widehat{p^b}$ is $\overline{A}_{(a-1),(b-1)}$. Since the first row and column of $\overline{A}$ represent multiplication by the identity element, to find $\widehat{p^a} \cdot \widehat{p^b}$ one simply finds the intersection of the row starting with $\widehat{p^a}$ and the column starting with $\widehat{p^b}$. Finally, the following result regarding cubical arrays becomes far simpler when it is used with reverse decimal matrices.

Theorem 6.1. A semifield, S, of dimension n over $\mathbb{F}_p$ has a subsemifield, S', of dimension m over $\mathbb{F}_p$ if and only if there exists $A \in K(S)$ such that the cubical array A' consisting of the first $m \times m \times m$ entries of A is nonsingular, and $A_{ijk} = 0$ for all $i, j \leq m$, $k > m$.

Proof. First suppose S has a subsemifield S' of dimension m. Then there exists a basis $\{1 = x_1, x_2, ..., x_m\}$ of S' over $\mathbb{F}_p$ which generates a Knuth cube A'. Further, S

must have a basis of the form $\{1, x_2, ..., x_m, y_{m+1}, ..., y_{n-1}\}$ which generates a Knuth cube $A \in K(S)$. Then we have

$$x_i * x_j = \sum_{k=1}^{n} A_{ijk} x_k = \sum_{k=1}^{m} A'_{ijk} x_k + \sum_{k=m+1}^{n} A_{ijk} x_k = \sum_{k=1}^{m} A'_{ijk}$$

Thus $A_{ijk} = 0$ when $i, j \leq m$ and $k > m$.

Now suppose the converse is true, that there exists $A \in K(S)$ such that the cubical array A' consisting of the first $m \times m \times m$ entries of A is nonsingular, and $A_{ijk} = 0$ for all $i, j \leq m$, $k > m$. Note that A' will clearly be in standard form as well. Thus, if $\{1 = x_1, x_2, ..., x_m\}$ is the basis which generates A', then it is also the basis of a semifield of dimension m over $\mathbb{F}_p$, where multiplication is defined by

$$x_i * x_j = \sum_{k=1}^{n} A'_{ijk} x_k$$

□

Corollary 6.2. A semifield, S, of dimension n over $\mathbb{F}_p$ has a subsemifield, S', of dimension m over $\mathbb{F}_p$ if and only if there exists a reverse decimal matrix $\overline{A}$ for S where $\overline{A}_{ij} < p^m$ for all $1 \leq i, j \leq m$

6.4 Examples

To further illustrate the use of the reverse decimal matrix, consider the reverse decimal matrices associated with the Knuth cubes already given for $\mathbb{F}_{16}$, system V, and system W.

$$\mathbb{F}_{16} \qquad F \sim \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 8 & 12 \\ 4 & 8 & 6 & 11 \\ 8 & 12 & 11 & 13 \end{pmatrix}$$

$$\text{System W} \qquad W \sim \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 2 & 12 & 4 \\ 4 & 8 & 2 & 3 \\ 8 & 12 & 1 & 2 \end{pmatrix}$$

$$\text{System V} \qquad V \sim \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 12 & 4 \\ 4 & 8 & 5 & 14 \\ 8 & 12 & 15 & 9 \end{pmatrix}$$

This notation makes a few things very clear. Notice that the matrix for $\mathbb{F}_{16}$ is symmetric, which is due to the commutativity of its multiplication. Also notice that the upper left 2×2 entries of these matrices are all less than 4. This means that each of these semifields contains a subsemifield of dimension 2 over $\mathbb{F}_2$. Since there are no proper 4-element semifields, this means that each of these subsemifields is isomorphic to $\mathbb{F}_4$. The reason for this is due to the fact that in all three of these semifields $(a+\lambda 0)*(c+\lambda 0) = ac$, and $a, c \in \mathbb{F}_4$. Furthermore, the fact that the second columns

of these matrices are all equal is due to the fact that $(0 + \lambda b) * (c + \lambda 0) = \lambda(bc)$ in all three of these semifields.

6.5 Knuth Cubes and Constructions

Suppose we have a Knuth cube A of dimension n over $\mathbb{F}_p$, and suppose we have a semifield S of order p^n generated by some algebraic construction. Then A will correspond to S if and only if $A \in K(S)$. Thus, we construct a Knuth cube B for S, and, using $C(n, p)$ or the results from section 5.2, we can generate $K(S)$ and see if A is in $K(S)$. Alternatively, we could use A to construct a semifield S' and investigate all of the cubes in $K(S')$ to see if any of them correspond to a cube for a given construction.

The key to constructing a Knuth cube for a semifield S generated by a given construction is the determination of an appropriate basis to generate the cube. Since $K(S)$ will contain the Knuth cubes generated by all appropriate bases, we can choose a basis of the most convenient form. For some constructions, such as those used for system V and system W, there is an obvious choice of basis. But there are constructions where it is not clear what a valid basis would be. Thus, most of the work in the following sections is devoted to determining an appropriate basis for a construction. Once a basis is found, general products of the basis elements are determined, and the general form of a reverse decimal matrix generated by this basis is given.

6.6 Albert Binary Semifields

According to Wene, [25], this construction came from an investigation by Albert of the Knuth binary semifields described in the following section. We introduce it

first due to it's straightforward construction.

Consider the vector space $U = \mathbb{F}_2^n$, for an odd $n \geq 3$. Let $U = V + \omega\mathbb{F}_2$, with $1 \in V$. In other words, if U has a basis $\{x_1, ..., x_n\}$ and $\omega = x_i$, then V is the span of $\{x_1, ..., x_{i-1}, x_{i+1}, ..., x_n\}$. Then we construct a semifield $S = (U, +, *)$ where, for $a, b \in V$,

$$\begin{aligned} a * b &= ab \\ a * \omega &= \omega * a = a\omega + a^2 + a \\ \omega * \omega &= \omega^2 + 1 \end{aligned}$$

Due to the many possible choices of ω, it is not clear what form a basis for an Albert binary semifield would have. However, in the case where $n = 2^k+1$, we will be able to determine such a basis. Wene, [25], proved that ω is a defining element of $\mathbb{F}_2^n$ over $\mathbb{F}_2$, i.e. $U = \mathbb{F}_2[\omega]$, and that if σ is an automorphism of $\mathbb{F}_2^n$, then $\sigma(U) = \sigma(V) + \sigma(\omega)\mathbb{F}_2$ will define an isomorphic semifield. This leads to the following lemma.

Lemma 6.3. Let S be an Albert binary semifield of order 2^n, where $n = 2^k+1$ for some k. Then S is isomorphic to an Albert binary semifield with a basis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1} = \omega\}$, where α is a defining element of $\mathbb{F}_2^n$ over $\mathbb{F}_2$, .

Proof. Let α be a defining element of $\mathbb{F}_2^n$. By assumption, $\alpha^{n-1} = \alpha^{2^k}$, and clearly $k < n - 1$. Thus α^{n-1} is a conjugate of α. By Theorem 2.21 in [12], there is an automorphism which maps α to α^{2^k}. Thus, S is isomorphic to a semifield with a basis $\{1, \alpha, ..., \alpha^{n-1} = \omega\}$. □

By Theorem 3.33 in [12], if $m(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ is the minimal polynomial of α, then it is also the minimal polynomial of α^{2^k}, and it is irreducible. Thus the number of possible Albert binary semifields of order 2^{2^k+1} is less than or equal to the number of irreducible polynomials of order $2^k + 1$ over $\mathbb{F}_2$.

Now consider the reverse decimal matrices $\overline{A}$ for an Albert binary semifield with

basis $\{1, \alpha, ..., \alpha^{n-1} = \omega\}$, and $\overline{B}$ for $\mathbb{F}_2^n$ with basis $\{1, \alpha, ..., \alpha^{n-1}\}$. Then $\overline{A}_{ij} = \overline{B}_{ij}$ for $1 \leq i, j < n$, since these entries correspond to multiplication in the field.

To determine whether a given $(2^k + 1) \times (2^k + 1)$ reverse decimal matrix $\overline{B}$ defines an Albert binary semifield, check that the first $2^k \times 2^k$ entries match a reverse decimal matrix $\overline{A}$ for $\mathbb{F}_2^{2^k+1}$. Then, consider $a = \overline{A}_{3,2^k}$, and $\overline{a} \in \mathbb{F}_2^{2^k+1}$ such that $a \sim \overline{a}$. Then, the minimal polynomial of α over $\mathbb{F}_2$ will be

$$m(x) = x^{2^k+1} + \overline{a}_{2^k} x^{2^k} + \cdots + \overline{a}_1 x + \overline{a}_0$$

This can then be used to determine whether the last column of $\overline{B}$ satisfies the structure of an Albert binary semifield.

6.7 Knuth Binary Semifields

This construction was introduced by Knuth in [11], and is called "binary" due to the fact that the semifields resulting from this construction are vector spaces over $\mathbb{F}_2$.

Let $\{1, \alpha, ..., \alpha^{n-1}\}$ be a basis for $\mathbb{F}_2^{mn}$ over $\mathbb{F}_2^m$, where n is odd and $nm > 3$. Let $f : \mathbb{F}_2^{mn} \mapsto \mathbb{F}_2^m$ be a linear function defined by $f(\alpha^{n-1}) = 1$ and $f(\alpha^i) = 0$ for $0 \leq i \leq n-2$. Then, define two products $\circ$ and $*$ on $\mathbb{F}_2^{mn}$

$$\begin{aligned} a \circ b &= ab + (f(a)b + f(b)a)^2 \\ a \circ b &= (1 \circ a) * (1 \circ b) \end{aligned}$$

Then $(\mathbb{F}_2^{mn}, +, \circ)$ is a presemifield (it has no multiplicative identity) and $(\mathbb{F}_2^{nm}, +, *)$ is a semifield.

To find a basis, we start with the case where $m = 1$. This gives us

$$\begin{aligned}
1 \circ 1 &= 1 \\
1 \circ \alpha^i &= \alpha^i & 0 \le i \le n-2 \\
1 \circ \alpha^{n-1} &= \alpha^{n-1} + 1 \\
\alpha^i \circ \alpha^j &= \alpha^{i+j} & 0 \le i, j \le n-2 \\
\alpha^i \circ \alpha^{n-1} &= \alpha^{i+n-1} + \alpha^{2i} & 0 \le i \le n-2 \\
\alpha^{n-1} \circ \alpha^{n-1} &= \alpha^{2n-2} \\
1 \circ (\alpha^{n-1} + 1) &= \alpha^{n-1}
\end{aligned}$$

This defines the following products, for $0 \le i, j \le n-2$

$$\begin{aligned}
1 * 1 &= (1 \circ 1) * (1 \circ 1) &&= 1 \\
1 * \alpha^i &= (1 \circ 1) * (1 \circ \alpha^i) &&= \alpha^i \\
1 * \alpha^{n-1} &= (1 \circ 1) * (1 \circ (\alpha^{n-1} + 1)) &&= \alpha^{n-1} \\
\alpha^i * \alpha^j &= (1 \circ \alpha^i) * (1 \circ \alpha^j) &&= \alpha^{i+j} \\
\alpha^i * \alpha^{n-1} &= (1 \circ \alpha^i) * (1 \circ (\alpha^{n-1} + 1)) &&= \alpha^i(\alpha^{n-1} + \alpha^i + 1) \\
\alpha^{n-1} * \alpha^{n-1} &= (1 \circ (\alpha^{n-1} + 1)) * (1 \circ (\alpha^{n-1} + 1)) &&= \alpha^{2n-2} + 1
\end{aligned}$$

More simply

$$\begin{aligned}
1 * 1 &= 1 \\
1 * \alpha^i &= \alpha^i \\
1 * \alpha^{n-1} &= \alpha^{n-1} \\
\alpha^i * \alpha^j &= \alpha^{i+j} \\
\alpha^i * \alpha^{n-1} &= \alpha^i \alpha^{n-1} + (\alpha^i)^2 + \alpha^i \\
\alpha^{n-1} * \alpha^{n-1} &= (\alpha^{n-1})^2 + 1
\end{aligned}$$

This is exactly the case of an Albert binary semifield with $\omega = \alpha^{n-1}$. Now suppose $m > 1$. Let $\{1, \beta, ..., \beta^{m-1}\}$ be a basis for $\mathbb{F}_2^m$. Then $f(\beta^i \alpha^{n-1}) = \beta^i$. This causes

some slight changes to the multiplication, giving the more general results, for $0 \leq k \leq m-1$

$$\begin{aligned}
\beta^b * \beta^k &= \beta^{b+k} \\
\beta^b * \beta^k\alpha^i &= \beta^{b+k}\alpha^i \\
\beta^b * \beta^k\alpha^{n-1} &= \beta^{b+k}\alpha^{n-1} \\
\beta^b\alpha^i * \beta^k\alpha^j &= \beta^{b+k}\alpha^{i+j} \\
\beta^b\alpha^i * \beta^k\alpha^{n-1} &= (\beta^{b+k}\alpha^i)\alpha^{n-1} + (\beta^{b+k}\alpha^i)^2 + \beta^{b+k}\alpha^i \\
\beta^b\alpha^{n-1} * \beta^k\alpha^{n-1} &= \beta^{b+k}(\alpha^{n-1})^2 + \beta^{b+k}
\end{aligned}$$

This is similar to the case of the Albert binary semifields where $\omega = \alpha^{n-1}$. In this case, there is a basis of the form

$$\{1, \beta, ..., \beta^{m-1}, \alpha, ..., \beta^{m-1}\alpha, ..., \alpha^{n-1}, ..., \beta^{m-1}\alpha^{m-1}\}$$

If $\overline{B}$ is the reverse decimal matrix for S generated by this basis, then there is a reverse decimal matrix $\overline{A}$ for $\mathbb{F}_2^{mn}$ such that $\overline{B}_{ij} = \overline{A}_{ij}$ for all $1 \leq i, j \leq m(n-1)$. To find $\overline{B}_{ij}$ where $i, j > m(n-1)$, we need to determine the value of α^n. This can be done using the fact that the reverse decimal form of $\overline{\alpha^n}$ is located in the $m(n-1)+1$ column and $m+1$ row. Once that is determined, the remaining entries of $\overline{B}$ can be checked.

6.8 Sandler's Construction

A Sandler semifield, S, has p^{nm^2} elements, where $m > 1$, of the form

$$a_0 + \lambda a_1 + \lambda^2 a_2 + \cdots + \lambda^{m-1} a_{m-1}; \qquad a_i \in \mathbb{F}_p^{nm}$$

Multiplication is defined by

$$\begin{aligned}
(\lambda^{(i}x)(\lambda^{(j}y) &= \lambda^{(i+j}x^{(p^n)^j}y \\
\lambda^{(m} &= \delta
\end{aligned}$$

where δ is a root of an irreducible polynomial of degree m over $\mathbb{F}_p^n$, and the exponential notation refers to repeated left multiplication. Let $\mathbb{F}_p^{nm} = \mathbb{F}_p[\alpha]$ for some α. We can now construct a reverse decimal matrix, $\overline{B}$ for S in a straightforward manner. First, we choose a basis of the form

$$\{1, \alpha, ..., \alpha^{nm-1}, \lambda, \lambda\alpha, ..., \lambda\alpha^{nm-1}, ..., \lambda^{(m-1}, \lambda^{(m-1}\alpha, ..., \lambda^{(m-1}\alpha^{nm-1}\}$$

Then $\overline{B}$ will have a block structure corresponding to which power of λ is multiplied by the basis of $\mathbb{F}_p^{nm}$. The notation $\overline{B}_{[x,y]}$ will denote the $nm \times nm$ submatrix whose upper-left corner is $\overline{B}_{xm+1,ym+1}$. Here's a graphic to help visualize $\overline{B}$

$$\begin{array}{c} \\ 1 \\ \lambda \\ \vdots \\ \lambda^{(m-1} \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \lambda & \cdots & \lambda^{(m-1} \end{array} \\ \left(\begin{array}{c|c|c|c} & & & \\ \hline & & & \\ \hline & & & \\ \hline & & & \end{array}\right) \end{array}$$

Then $\overline{B}_{[1,1]}$ will be the reverse decimal matrix for $\mathbb{F}_p^{nm}$ generated by the basis $\{1, \alpha, ..., \alpha^{nm-1}\}$. Similarly, the entries in $\overline{B}_{[i,1]}$ will equal the entries of $\overline{B}_{[1,1]}$ times $\lambda^{(i} \sim p^{(i+1)nm}$. The rest of $\overline{B}$ is less straightforward and depends on the powers of α.

To tell if a particular $nm^2 \times nm^2$ reverse decimal matrix corresponds to a Sandler semifield, first determine whether $\overline{B}_{[1,1]}$ corresponds to a reverse decimal matrix for $\mathbb{F}_p^{nm}$, and then check whether $\overline{B}_{[i,1]}$ will equal the entries of $\overline{B}_{[1,1]}$ times $p^{(i+1)m}$. From there, determine which basis generated $\overline{B}_{[1,1]}$ and then check the remaining blocks of $\overline{B}$.

6.9 Petit's Construction

This construction was introduced by Petit, [15], [16], and is based on factor rings of skew polynomial rings over finite fields. We do not give a formal definition

of these rings or their properties, but instead simply provide sufficient information to derive the construction.

Let $\mathbb{F}_{p^n}[X;\sigma]$ denote the skew polynomial ring over $\mathbb{F}_{p^n}$, and σ is an automorphism of $\mathbb{F}_{p^n}$, i.e. $a^\sigma = a^{p^i}$ for some i. Multiplication is defined as usual on the left, but $Xa = a^{p^i}X$. Wene, [25], cites theorems that show that $\mathbb{F}_{p^n}[X;\sigma]$ has a division algorithm, and thus can be factored by ideals. Let $M(X) \in \mathbb{F}_{p^n}[X,\sigma]$ be an irreducible polynomial of degree m, and let $F_M = \mathbb{F}_{p^n}[X;\sigma]/M(X)$. Addition is defined on F_M as normal, but multiplication is defined by $A(X) * B(X) = R(X)$ where $A(X)B(X) = Q(X)M(X)+R(X)$ in $\mathbb{F}_{p^n}[X;\sigma]$. Then $(F_M, +, *)$ is a semifield of order p^{nm} .

Note that $\{1, X, ..., X^{m-1}\}$ forms a basis of F_M over $\mathbb{F}_{p^n}$, and if $n > 1$, and $\{1, \alpha, ..., \alpha^{n-1}\}$ is a basis of F, then a basis for S over F would be

$$\{1, \alpha, ..., \alpha^{n-1}, X, ..., \alpha^{n-1}X, ..., X^{m-1}, ..., \alpha^{n-1}X^{m-1}\}$$

Let $\overline{B}$ be a reverse decimal matrix for S with respect to this basis. Then there is a reverse decimal matrix $\overline{A}$ for $\mathbb{F}_{p^{nm}}$ such that $\overline{B}_{i*} = \overline{A}_{i*}$ for $1 \leq i \leq m-1$. From there, it should be easy to determine if there exists a fixed σ such that $X \cdot a = a^\sigma X$.

6.10 Dickson's Even-Dimensional Semifields

The study of finite semifields began with the work of Dickson in the early 1900s. This particular construction was introduced in [5].

Let p be odd, $n > 1$, and let $f \in \mathbb{F}_{p^m}$ be a nonsquare element. Then, the Dickson semifield S is a two dimension vector space over $\mathbb{F}_{p^n}$ with basis $\{1, \lambda\}$, and multiplication defined by

$$(a + \lambda b)(c + \lambda d) = (ac + f(bd)^\theta) + \lambda(ad + bc)$$

where θ is an automorphism of $\mathbb{F}_{p^n}$, i.e. $x^\theta = x^{p^r}$ for some $1 \leq r < n$.

Let $\{1, \alpha, ..., \alpha^{n-1}\}$ be a basis of $\mathbb{F}_p^n$. Then S has a basis of the form $\{1, ..., \alpha^{n-1}, \lambda, ..., \lambda\alpha^{n-1}\}$, and its corresponding reverse decimal matrix will have the form

$$\overline{A} = \left(\begin{array}{ccccc|ccc} 1 & & p & \cdots & p^{n-1} & p^n & \cdots & p^{2n-1} \\ p & & & & & & & \\ \vdots & & & & & & & \\ p^{n-1} & & & & & & & \\ \hline p^n & & & & & & & \\ \vdots & & & & & & & \\ p^{2n-1} & & & & & & & \end{array}\right)$$

We will let $\overline{A}_{[x,y]}$ denote the $n \times n$ submatrix of $\overline{A}$ whose upper left corner is located at $\overline{A}_{(nx,ny)}$. Then $\overline{A}_{[1,1]}$ corresponds to a reverse decimal matrix for $\mathbb{F}_p^n$, $\overline{A}_{[2,1]} = \overline{A}_{[1,2]} = p^n\overline{A}_{[1,1]}$. The entries in $\overline{A}_{[2,2]}$ require a bit more work. First, note that $\overline{A}_{nn} \sim \lambda^2 = f$, and $\overline{A}_{(n,n+1)} = \overline{A}_{(n+1,n)} \sim f(\alpha)^\theta$. Thus, it is possible to determine what f and θ must be, which can then be used to determine whether this is a Dickson semifield.

6.11 Quadratic Over a Weak Nucleus

This construction was given by Knuth in [11], and both system V and system W are special cases of this construction. A *weak* nucleus is a subset N of a semifield S such that, for $a, b, c \in S$, $a*(b*c) = (a*b)*c$ is true whenever any two of the elements is in N. Knuth constructs S as a two-dimensional vector space over a finite field $\mathbb{F}_{p^n}$, and assumes that $\mathbb{F}_{p^n}$ will be a weak nucleus of S. The elements of S have the form $(a + \lambda b)$, for $a, b \in \mathbb{F}_{p^n}$. Knuth proves that this forces $(0 + \lambda b) * (c + \lambda 0) = \lambda(bc)$,

and $(a+\lambda 0)*(0+\lambda d)=\lambda(a^{\sigma}d)$ where σ is an automorphism of $\mathbb{F}_{p^n}$, i.e. $a^{\sigma}=a^{p^i}$ for $1\leq i\leq n$. From here we have the general product

$$(a+\lambda b)*(c+\lambda d)=ac+\lambda(bc+a^{\sigma}d)+(\lambda b)*(\lambda d)$$

Knuth then considers the results for when $p\neq 2$ or $p=2$, but we will only present the results of this investigation here. In both cases, S will be a two dimensional vector space over $\mathbb{F}_{p^n}$, so, if $\{1,x,...,x^{n-1}\}$ is a basis of $\mathbb{F}_{p^n}$, then $\{1,...,x^{n-1},\lambda,...,\lambda x^{n-1}\}$ will be a basis for S, such that $\lambda^2\notin\mathbb{F}_{p^n}$. Let $\overline{A}$ be the reverse decimal matrix for this basis, and let $\overline{A}_{[x,y]}$ denote the $n\times n$ submatrix whose upper left order is at $\overline{A}_{(nx,ny)}$. Then $\overline{A}_{[1,1]}$ will be a reverse decimal matrix for $\mathbb{F}_{p^n}$.

In the first case, suppose $p\neq 2$, $\alpha,\beta,\sigma\in \mathrm{Aut}(\mathbb{F}_{p^n}$ not all trivial, $f\in\mathbb{F}_{p^n}$ nonsquare, multiplication in S is defined by

$$(a+\lambda b)(c+\lambda d)=(ac+b^{\alpha}d^{\beta}f)+\lambda(a^{\sigma}d+bc)$$

Then $\overline{A}_{[2,1]}=p^n\overline{A}_{[1,1]}$. To determine σ, note that $\overline{A}_{(2,n+1)}\sim(x)(\lambda)=\lambda(x^{\sigma})$, and σ will determine all of $\overline{A}_{[1,2]}$. For $\overline{A}_{[2,2]}$, note the following

$$\begin{array}{lcll}\overline{A}_{(n+1,n+1)} & \sim & \lambda^2 & = f\\ \overline{A}_{(n+1,n+2)} & \sim & \lambda(\lambda x) & = x^{\beta}f\\ \overline{A}_{(n+2,n+1)} & \sim & (\lambda x)\lambda & = x^{\alpha}F\end{array}$$

These can be used to determine f, α, and σ, and then verify the rest of $\overline{A}$.

Now suppose $p=2$. Let $\sigma\in\mathrm{Aut}(\mathbb{F}_{p^n})$ be nontrivial, $\tau=\sigma^{-1}$, and let $f,g\in\mathbb{F}_{p^n}$ such that

$$y^{\sigma+1}+gy-f\neq 0;\quad \text{for all } y\in\mathbb{F}_{p^n}$$

Then the multiplication $(a+\lambda b)(c+\lambda d)$ has one of four forms

$$(1) \qquad (ac + b^\sigma d^{\tau^2} f) + \lambda(bc + a^\sigma d + b^\sigma d^\tau g)$$

$$(2) \qquad (ac + b^\sigma df) + \lambda(bc + a^\sigma d + b^\sigma dg)$$

$$(3) \qquad (ac + b^\tau d^{\tau^2} f) + \lambda(bc + a^\sigma d + bd^\tau g)$$

$$(4) \qquad (ac + b^\tau df) + \lambda(bc + a^\sigma d + bdg)$$

Rather than look at each of these four separately, We will describe the general method for determination. The entries in $\overline{A}_{[2,1]}$ correspond to products of the form $(\lambda b)(c) = \lambda(bc)$, so $\overline{A}_{[2,1]} = p^n \overline{A}_{[2,1]}$. The entries in $\overline{A}_{[1,2]}$ correspond to products of the form $(a)(\lambda d) = \lambda(a^\sigma d)$. In particular, $\overline{A}_{(2,n+1)} \sim (x)(\lambda) = \lambda(x^\sigma)$. From this it is possible to determine σ and τ, and consequently all of $\overline{A}_{[1,2]}$. Determining which of the four types the semifield has depends on $\overline{A}_{[2,2]}$. Let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \{1, \sigma, \tau, \tau^2\}$. Then the following can be used to determine f, α_i, β_i:

$$\begin{aligned}
\overline{A}_{(n+1,n+1)} &\sim (\lambda)(\lambda) &&= f + \lambda g \\
\overline{A}_{(n+1,n+2)} &\sim (\lambda)(\lambda x) &&= x^{\beta_1} f + \lambda(x^{\beta_2} g) \\
\overline{A}_{(n+2,n+1)} &\sim (\lambda x)(\lambda) &&= x^{\alpha_1} f + \lambda(x^{\alpha_2} g)
\end{aligned}$$

6.12 Albert's Twisted Fields

This construction was introduced by Albert in [2], and gets its name due to the fact that it defines a new product on the elements of a finite field by "twisting" the existing finite field product.

Let $n > 2$ and $\sigma, \theta \in \mathrm{Aut}(\mathbb{F}_{p^n}$. Let F_σ and F_θ denote the subfields of $\mathbb{F}_{p^n}$ which are fixed by σ and θ, and let $F = F_\sigma \cap F_\theta$. Let $c \in F$ such that

$$c \neq \frac{xy}{x^\theta y^\sigma}$$

for any nonzero $x, y \in F$. Define linear transformations L and R over F by

$$L(x) = x - cx^\theta \qquad R(y) = y - cy^\sigma$$

The Albert twisted semifield, S is constructed from F with standard addition and multiplication $*$ defined by

$$L(x) * R(y) = xy - cx^{\theta}y^{\sigma}$$

The complexity of this construction makes it difficult to determine what form a Knuth cube would have if generated by this construction. There is one specific case where it is actually somewhat straightforward. Menichetti, [13], proved that every semifield of dimension 3 over a finite field will be an Albert twisted field, and determined a set of structure constants which would correspond to such a semifield. Since the Knuth cubes are equivalent to the set of structure constants, we can easily adapt his results.

If S is three dimensional over a field, then it will have a Knuth cube whose reverse decimal matrix has the form

$$\overline{A} = \left(\begin{array}{c|c|c} \begin{array}{cccc} 1 & p & \cdots & p^{k-1} \\ p & & & \\ \vdots & & & \\ p^{k-1} & & & \end{array} & \begin{array}{ccc} p^k & \cdots & p^{2k-1} \\ & & \\ & & \\ & & \end{array} & \begin{array}{ccc} p^{2k} & \cdots & p^{3k-1} \\ & & \\ & & \\ & & \end{array} \\ \hline \begin{array}{cccc} p^k & & & \\ \vdots & & & \\ p^{2k-1} & & & \end{array} & & \\ \hline \begin{array}{cccc} p^{2k} & & & \\ \vdots & & & \\ p^{3k-1} & & & \end{array} & & \end{array}\right)$$

where $\overline{A}_{[1,1]}$ is a reverse decimal matrix for $GF(p)^k$, $\overline{A}_{[1,i]} = \overline{A}_{[i,1]} = p^{(i-1)k}\overline{A}_{[1,1]}$ for $i = 2, 3$, and $\overline{A}_{[2,2]} = p^{2k}\overline{A}_{[1,1]}$.

Chapter 7

Extending a Subfield of a Semifield

As mentioned in chapter 6, cubical arrays have been used to find all of the semifields of orders 2^4, 2^5, 2^6, 3^4, 3^5, and 7^4. Also, a number of the known constructions yield block reverse decimal matrices where many of the blocks are related to a reverse decimal matrix for a finite field. This helped inspire the results in this chapter, which provide a method for constructing new semifields by using the Knuth cubes of known semifields over $\mathbb{F}_p$ to define new semifields over extensions of $\mathbb{F}_p$.

7.1 Cubical Arrays Over Extension of $\mathbb{F}_p$

The crux of these results is based on the natural embedding of a finite field into any of its extension fields. Because of this, we will use the following notation: for $\overline{M} \in GL(n,p)$, $[\overline{M}]_{p^m}$ will denote the matrix in $GL(n,p^m)$ whose entries are the natural embedding of the entries of $\overline{M}$ into $\mathbb{F}_{p^m}$.

Lemma 7.1. Let $\overline{M} \in GL(n,p)$. Then $[\overline{M}]_{p^m} \in GL(n,p^m)$.

Proof. Because $\overline{M}$ is invertible, $\det(\overline{M}) \neq 0$. Let σ denote the natural embedding of $\mathbb{F}_p$ into $\mathbb{F}_{p^m}$. Note that σ is an injective homomorphism, thus $\det(\overline{M}) = \det([\overline{M}]_{p^m})$, and thus $[\overline{M}]_{p^m}$ is nonsingular. □

We will use a similar notation for cubical arrays, with $[A]_{p^m}$ signifying that we wish to view the entries of A as elements of $\mathbb{F}_{p^m}$ in the natural way. Unlike with matrices, nonsingularity of cubical arrays is not necessarily preserved under this embedding.

In the proof of Theorem 3.4, we showed how the properties of a cubical array

translated to the algebra which it defined. If the cubical array is in standard form, then the resulting construction will have a multiplicative identity. If the cubical array is nonsingular, then the resulting construction will have no zero divisors. These facts inspire the following result.

Lemma 7.2. Let S be a semifield of order p^n and $A \in K(S)$. Then $[A]_{p^m}$ defines an n-dimensional semifield over $\mathbb{F}_{p^m}$, if and only if $[A]_{p^n}$ is nonsingular over $\mathbb{F}_{p^m}$.

Proof. Let $\overline{I}$ denote the $n \times n$ identity matrix. By definition, $A_{1**} = A_{*1*} = I$, so $[A_{1**}]_{p^n} = [A_{*1*}]_{p^n} = \overline{I}$ as well. Thus $[A]_{p^m}$ is in standard form, and $[A]_{p^m}$ will define a semifield over $\mathbb{F}_{p^m}$ if and only if it is nonsingular. □

Let $S_{[m]}$ denote the system defined by A over $\mathbb{F}_{p^m}$. By the Lemma above, $S_{[m]}$ is a semifield if and only if $[A]_{p^m}$ is nonsingular. If $S_{[m]}$ is a semifield, then there exists an $nm \times nm \times nm$ cubical array for $S_{[m]}$ over $\mathbb{F}_p$. In particular, suppose A is defined by a basis $\{1, \alpha_2, ..., \alpha_n\}$, and let $\mathcal{B} = \{1, \beta_2, ..., \beta_m\}$ be a basis for $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. If $[A]_{p^m}$ is nonsingular, then the cubical array B defined by the basis

$$\{1, \beta_2, ..., \beta_m, \alpha_2, \alpha_2\beta_2, ..., \alpha_2\beta_m, ..., \alpha_n, \alpha_n\beta_2, ..., \alpha_n\beta_m\}$$

will also be nonsingular, and we say that B is the *inflation* of A by $\mathcal{B}$. Similarly, we will say $S_{[m]}$ is the m-inflation of S.

Inflation does more than simply allow a cubical array to define multiple semifields. It also provides a nesting structure to semifields over the same prime subfield, as is demonstrated by the following results.

Theorem 7.3. Let S and S' be isotopic semifields of order p^n. Then $S_{[m]}$ is a semifield if and only if $S'_{[m]}$ is a semifield. Further, if $S_{[m]}$ is a semifield, it is isotopic to $S'_{[m]}$.

Proof. Let $A \in K(S)$, $B \in K(S')$. By Theorem 3.16, there exist $\overline{F}, \overline{G}, \overline{H} \in GL(n,p)$ such that $B = [\overline{F}, \overline{G}, \overline{H}^{-T}] \times A$ and

$$B_{i**} = \sum_{j=1}^{n} \overline{F}_{ij} \overline{G} A_{i**} \overline{H}^T = \overline{G} \left(\sum_{j=1}^{n} \overline{F}_{ij} A_{i**} \right) \overline{H}^T$$

Let $\overline{v} \in \mathbb{F}_{p^m}^n$ and $\overline{w} = \overline{v}[\overline{F}]_{p^n}$. Then, using the equation above and embedding into $\mathbb{F}_{p^m}$, we get

$$\begin{aligned} \textstyle\sum_{i=1}^{n} \overline{v}_i [B_{i**}]_{p^m} &= [\overline{G}]_{p^m} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \overline{v}_i [\overline{F}_{ij}]_{p^m} [A_{j**}]_{p^m} \right) [\overline{H}^T]_{p^m} \\ &= [\overline{G}]_{p^m} \left(\sum_{j=1}^{n} \overline{w}_j [A_{j**}]_{p^m} \right) [\overline{H}^T]_{p^m} \end{aligned}$$

By Lemma 7.1, $[\overline{G}]_{p^m}$ and $[\overline{H}^T]_{p^m}$ are nonsingular. Thus $\sum_{i=1}^{n} \overline{v}_i [B_{i**}]_{p^m}$ is singular if and only if $\sum_{j=1}^{n} \overline{w}_j [A_{j**}]_{p^m}$ is singular, which implies $S_{[m]}$ is a semifield if and only if $S'_{[m]}$ is a semifield. And if $S_{[m]}$ is a semifield, it is isotopic to $S'_{[m]}$ with isotopism $\{[\overline{F}]_{p^m}, [\overline{G}]_{p^m}, [\overline{H}]_{p^m}\}$. □

Corollary 7.4. Let S and S' be isomorphic semifields of order p^n. Then $S_{[m]}$ is a semifield if and only if $S'_{[m]}$ is a semifield. Further, if $S_{[m]}$ is a semifield, it is isomorphic to $S'_{[m]}$.

Now we address the obvious question of how to determine if $[A]_{p^m}$ is nonsingular. By definition, the only method to determine whether $[A]_{p^m}$ is nonsingular is to check $\sum_{i=1}^{n} \overline{v}_i A_{i**}$ for all $\overline{v} \in \mathbb{F}_{p^m}^n$. Consider the following, equivalent, method. Let $x = (x_1, ..., x_n)$ be a vector of indeterminates, and define $f \in \mathbb{F}_p[x_1, ..., x_n]$ by

$$f(x_1, ..., x_n) = \det(xA) = \det \left(\sum_{i=1}^{n} x_i A_{i**} \right)$$

We will call f the *inflation polynomial* of A. Then $[A]_{p^m}$ is nonsingular if and only if f contains no nontrivial zeroes in $\mathbb{F}_{p^m}^n$. Note that f is a homogeneous polynomial

of degree n in n unknowns. While this does not make it easier to show that $[A]_m$ is nonsingular, the inflation polynomial can make it much easier to show that $[A]_m$ is singular for some given m.

7.2 Determining Valid Extension Fields

We will use the 16-element semifields to illustrate these results. As we mentioned in chapter 2, there are three isotopism classes for these semifields. Class 1 consists of $\mathbb{F}_{16}$, class 2 contains the semifields isotopic to system W, and class 3 contains the semifields isotopic to system V. Consider the following Knuth cubes, A and B which correspond to semifields in classes 2 and 3 respectively.

$$A = \begin{pmatrix} 1000 & 0100 & 00010 & 0001 \\ 0100 & 1100 & 0001 & 0011 \\ 0010 & 0011 & 1010 & 1101 \\ 0001 & 0010 & 0101 & 1011 \end{pmatrix} \qquad B = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 1110 \\ 0010 & 0001 & 0100 & 1100 \\ 0001 & 0011 & 1000 & 0111 \end{pmatrix}$$

Let $\overline{x} = (a, b, c, d)$ be a vector of indeterminates. Then we get the following matrices, whose determinants will give us the inflation polynomials.

$$\overline{x}A = \begin{pmatrix} a & b & c & d \\ b & a+b & c+d & c \\ c & d & a+c & b+d \\ c+d & c & b+d & a+b+c+d \end{pmatrix}$$

$$\overline{x}B = \begin{pmatrix} a & b & c & d \\ b & a+b & d & c+d \\ d & c & a+b & b \\ b+c & b+c+d & b+d & a+d \end{pmatrix}$$

It turns out that these matrices have the same determinant, so we have the following inflation polynomial for both A and B:

$$\begin{aligned} f(a,b,c,d) &= a^4 + a^3d + a^2b^2 + a^2bc + a^2bd + a^2c^2 + a^2cd + a^2d^2 + ab^2c + ab^2d \\ &\quad + abc^2 + abcd + abd^2 + ac^2d + acd^2 + ad^3 + b^4 + b^3c + b^2c^2 \\ &\quad + b^2cd + b^2d^2 + bc^3 + bc^2d + bcd^2 + c^4 + c^2d^2 + d^4 \end{aligned}$$

Without loss of generality, let S denote the semifield defined by A. We can find some m for which $S_{[m]}$ is not a semifield by setting all but one of the inputs equal to elements of $\mathbb{F}_2$:

$$\begin{aligned} f(x,1,1,1) &= x^4 + x^3 + 1 \\ f(x,1,1,0) &= x^4 + x^2 + 1 = (x^2 + x + 1)^2 \end{aligned}$$

The first polynomial is a primitive polynomial of $\mathbb{F}_{16}$, and thus has a root in $\mathbb{F}_{16}$, implying that $S_{[4]}$ is not a semifield. The second polynomial is the square of the primitive polynomial of $\mathbb{F}_4$ and thus $S_{[2]}$ is not a semifield. In fact, the second polynomial also implies that $S_{[4]}$ is not a semifield, since $\mathbb{F}_4$ is isomorphic to a subfield of $\mathbb{F}_{16}$. This can be generalized into the following lemma.

Lemma 7.5. Let S be a semifield of order p^n. If $S_{[m]}$ is not a semifield and $m|r$, then $S_{[r]}$ is not a semifield.

Proof. $S_{[r]}$ is not a semifield if for some $A \in K(S)$ and $\overline{v} \in \mathbb{F}_{p^r}^n$, $\sum_{i=1}^n \overline{v}_i A_{i**}$ is singular. Since $S_{[m]}$ is not a semifield, there exists $\overline{w} \in \mathbb{F}_{p^m}^n$ such that $\sum_{i=1}^n \overline{w}_i A_{i**}$ is singular. Since $m|r$, $\mathbb{F}_{p^m}$ is isomorphic to a subfield of $\mathbb{F}_{p^r}$, and $[\overline{w}]_{p^r} \in \mathbb{F}_{p^r}^n$. Thus $S_{[r]}$ is not a semifield. □

Corollary 7.6. If $a \in \mathbb{F}_{p^m}$ is a root of the characteristic polynomial of L_z for some $z \in S$, then $S_{[m]}$ is not a semifield.

Corollary 7.7. If $a \in \mathbb{F}_{p^m}$ is a root of the left minimal polynomial of any element of S, then $S_{[m]}$ is not a semifield.

Returning to the 16-element semifields, we now know that $S_{[2k]}$ is not a semifield for all $k \in \mathbb{Z}^+$. By direct computation, f was found to have no nontrivial zeroes in $\mathbb{F}_8^4$, $\mathbb{F}_{32}^4$, or $\mathbb{F}_{128}^4$. Thus $S_{[3]}$, $S_{[5]}$, and $S_{[7]}$ are all semifields. Furthermore, we know there exist at least three isotopism classes for semifields of order 2^{12}, 2^{20}, and 2^{28}.

A key problem that remains is a general method for determining which extension fields will not contain roots of the inflation polynomial. Based on Lemma 7.5, as well as the properties of finite fields, the following conjecture may be the case.

Conjecture 7.8. Let S be a semifield of order q^n, where q is the order of the largest subfield of S over which S can be viewed as a vector space. Then $S_{[m]}$ is a semifield if and only if m and n are relatively prime.

7.3 Results of Extension

The results in this chapter have focused on extending the prime subfield of a semifield, since every finite semifield can be viewed as a vector space over its prime subfield. But, through inflation, we have shown that there exist semifields which can be viewed as vector spaces over extensions of their prime subfield. All of the results presented in chapters 4 and 5 have been proven viewing S as a vector space over its prime subfield, but it is worth mentioning that similar results will hold if a different view of S is taken. To illustrate this, we will let S be the semifield of order 2^{12} defined by $[A]_8$ in the previous section. Then S can either be viewed as a 12-dimensional vector space over $\mathbb{F}_2$ or a 4-dimensional vector space over $\mathbb{F}_8$.

First we consider the properties of left minimal polynomials of elements of S. If $z \in S$ is left primitive, then, as we've defined it, the left minimal polynomial of z will be a primitive polynomial of degree 12 in $\mathbb{F}_2[x]$. But, if we consider the characteristic polynomial of $\overline{z}[A]_8$, where $\overline{z}$ is the vector form of z over $\mathbb{F}_8$, then this polynomial will be a primitive degree 4 polynomial in $\mathbb{F}_8[x]$.

If $p^n = q^m$, where q is some power of p, we could have proven the theorems in chapter 4 in terms of $\mathbb{F}_q^m$ instead of $\mathbb{F}_p^n$, but it is more convenient to consider S as a vector space over the prime subfield. The results in chapter 5 could similarly be changed, looking at $C(m, q)$ in place of $C(n, p)$. If this is the case, then $|C(m, q)|$ will be less than $|C(n, p)|$, but will likely still be too large to test.

Chapter 8

Determining Constructions of the Semifields of Order 16

In this chapter we will derive algebraic constructions for each of the 16-element semifields (up to isomorphism). As mentioned in chapter 6, the 16-element semifields were first enumerated by Kleinfeld in [10]. In his work, Kleinfeld essentially provided a Knuth cube for each isomorphism class of these semifields. We start by verifying these results, and in the process develop a database of Knuth cubes for the 16-element semifields. From there we determine which of the 16-element semifields correspond to known constructions in chapter 6. We then investigate the remaining semifields for which there is no known construction and develop a construction for each based on its Knuth cubes. We conclude with a full list of the 16-element semifields along with all of the information which can be determined for each based on the results from chapters 4 and 5.

8.1 Verifying Kleinfeld's Results

We verified Kleinfeld's results using a desktop PC and Wolfram Mathematica by determining all nonsingular Knuth cubes of dimension 4 over $\mathbb{F}_2$ using the following method.

As Kleinfeld proved in Theorem 3 of [10], given any 16 element semifield S, there exists $a \in S$ such that $\{1, a, a^2, a(a^2)\}$ forms a basis for S over $\mathbb{F}_2$. The reverse

decimal matrix of a Knuth cube generated by this basis will then have the following form:

$$\overline{A} = \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 4 & 8 & b_1 \\ 4 & b_2 & b_3 & b_4 \\ 8 & b_5 & b_6 & b_7 \end{pmatrix}$$

The unknowns, b_i, $1 \leq i \leq 7$, can each have values ranging from 1 to 15, subject to the fact that no value can correspond to a vector which is a linear combination of the vectors corresponding to the other values in that row or column. For example, b_1 must be odd, since any even value between 1 and 15 would be a linear combination of the vectors corresponding to 2, 4, and 8. We had Mathematica construct reverse decimal matrices of this form by trying all of the possible values in $\overline{A}$ starting with the choice of b_1, then b_2, b_5, b_3, b_4, b_6, and finally b_7. Once $\overline{A}$ was completed, the cubical array A corresponding to $\overline{A}$ was constructed and tested for nonsingularity. If A was nonsingular, it was added to a list, $\mathcal{L}$.

Once all of the possible matrices had been constructed and their cubical arrays tested, we then needed to sort out the isomorphism and isotopism classes. For each $A \in \mathcal{L}$ we construct a list $\mathcal{L}_A$ of Knuth cubes generated by left cyclic bases generated by elements of the semifield S defined by A. Each of these cubes will also be in $\mathcal{L}$, so we remove them from $\mathcal{L}$ to save time. We continue in this way until we have 24 lists of cubical arrays corresponding to the 24 isomorphism classes of the 16-element semifields. Then, using the results from Theorem 3.18, we construct Knuth cubes for all of the semifields isotopic to a Knuth cube from each isomorphism class. We then sort these into the three isotopism classes. Finally, we use $C(4, 2)$ to generate all of the distinct Knuth cubes for each isomorphism class.

For each isomorphism class we assign a pair of numbers $\{t, m\}$, where t refers to

which isotopism class the semifield is included in, and m refers to which isomorphism class it is within that isotopism class. In the database, $\{t, m\}$ is a list of up to 1344 reverse decimal matrices corresponding to the Knuth cubes for that isomorphism class. The choices of t and m are arbitrary and merely used as a convenient way of referencing the semifields as we investigate then. The following list identifies each isomorphism class in our database, DB, with the designation given by Kleinfeld, KD, with the exception of $\mathbb{F}_{16}$, which he did not include. System V is in $\{3, 71\}$, and system W is in $\{2, 5\}$.

DB	KD	DB	KD	DB	KD	DB	KD
$\{1,1\}$	$\mathbb{F}_{16}$	$\{3,1\}$	V(5)	$\{3,8\}$	V(7)	$\{3,74\}$	V(4)
$\{2,1\}$	T(24)	$\{3,2\}$	V(9)	$\{3,9\}$	V(18)	$\{3,75\}$	V(8)
$\{2,5\}$	T(45)	$\{3,4\}$	V(1)	$\{3,11\}$	V(11)	$\{3,85\}$	V(15)
$\{2,6\}$	T(50)	$\{3,5\}$	V(3)	$\{3,70\}$	V(10)	$\{3,88\}$	V(2)
$\{2,13\}$	T(25)	$\{3,6\}$	V(12)	$\{3,71\}$	V(13)	$\{3,89\}$	V(14)
$\{2,15\}$	T(35)	$\{3,7\}$	V(17)	$\{3,73\}$	V(16)	$\{3,90\}$	V(6)

8.2 Eliminating Known Constructions

Using the results from chapter 6 we look at all of the semifields which can be generated using these known constructions. Rather than looking at each isomorphism class individually and determining whether it corresponds to a known construction, we instead simply construct the Knuth cubes for all possible constructions and find their locations in the database. First, note that many of the constructions do not allow for a 16-element case. There are clearly no Albert binary or Knuth binary semifields of order 16. There are also no proper Albert twisted fields of order 16, but this is not easily seen and would require a considerable amount of work to show. Instead we simply note that this is a consequence of proposition 10.14 in [8].

By building all of the possible Knuth cubes for the other constructions we find that the following semifields are defined by the noted constructions, with QWN referring to the semifields which are quadratic over a weak nucleus.

Database	Constructions
$\{2,1\}$	QWN
$\{2,6\}$	QWN
$\{2,13\}$	Petit, QWN
$\{2,15\}$	System W, Petit, QWN
$\{3,70\}$	QWN
$\{3,71\}$	System V, QWN

This leaves 17 isomorphism classes for which there is no known construction. Giving a detailed description of the derivation of constructions for each of the 17 unknown semifields would be quite lengthy. For that reason we will limit the work presented here to a few noteworthy examples, and exclude the others that are derived in similar ways. The full results will be listed in section 8.6.

8.3 Determining Constructions Part 1: Quadratic Over $\mathbb{F}_4$

If the elements of a semifield of order 16 can be viewed as a two-dimensional left or right vector space over $\mathbb{F}_4$, then we will say such a semifield is left or right *quadratic* over $\mathbb{F}_4$. Let S be a semifield which is right quadratic over $\mathbb{F}_4$, and let S^D be its dual. Note that S^D would be left quadratic over $\mathbb{F}_4$, and, once a construction is found for S, it will be a simple matter to find S^D in the database and define its product through the use of an anti-isomorphism. For this reason we will focus only on semifields which are right vector spaces over $\mathbb{F}_4$ in this section and the next.

Suppose a 16-element semifield was right quadratic over $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 =$

$1+\omega\}$ and had a basis $\{1, \omega, \lambda, \lambda\omega\}$ over $\mathbb{F}_2$, where $(0+\lambda b)*(c+\lambda 0) = \lambda(bc)$. Then a reverse decimal matrix corresponding to this basis would have the following form:

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & & \\ 4 & 8 & & \\ 8 & 12 & & \end{pmatrix}$$

The unknown semifields corresponding to $\{2,5\}$, $\{3,1\}$, $\{3,2\}$, and $\{3,85\}$ have reverse decimal matrices of this form. We will focus on $\{2,5\}$. There are 12 such matrices in $\{2,5\}$:

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 9 & 14 \\ 4 & 8 & 5 & 10 \\ 8 & 12 & 15 & 5 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 9 & 14 \\ 4 & 8 & 5 & 10 \\ 8 & 12 & 14 & 7 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 11 & 13 \\ 4 & 8 & 9 & 14 \\ 8 & 12 & 7 & 9 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 11 & 13 \\ 4 & 8 & 10 & 15 \\ 8 & 12 & 7 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 10 & 15 \\ 4 & 8 & 13 & 6 \\ 8 & 12 & 11 & 13 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 10 & 15 \\ 4 & 8 & 15 & 5 \\ 8 & 12 & 9 & 14 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 9 & 15 \\ 4 & 8 & 5 & 11 \\ 8 & 12 & 15 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 9 & 15 \\ 4 & 8 & 5 & 10 \\ 8 & 12 & 14 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 11 & 14 \\ 4 & 8 & 3 & 9 \\ 8 & 12 & 5 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 11 & 14 \\ 4 & 8 & 2 & 9 \\ 8 & 12 & 5 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 10 & 13 \\ 4 & 8 & 3 & 14 \\ 8 & 12 & 6 & 9 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 10 & 13 \\ 4 & 8 & 2 & 15 \\ 8 & 12 & 7 & 9 \end{pmatrix}$$

Let A be the cubical array corresponding to the first of these matrices:

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 9 & 14 \\ 4 & 8 & 5 & 10 \\ 8 & 12 & 15 & 5 \end{pmatrix} \sim A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 1001 & 0111 \\ 0010 & 0001 & 1010 & 0101 \\ 0001 & 0011 & 1111 & 1010 \end{pmatrix}$$

To determine the result of $(a + \lambda b) * (c + \lambda d)$ we use the properties of cubical arrays mentioned in chapter 3. Let $\overline{u} = \langle a_1, a_2, b_1, b_2 \rangle$ and $\overline{v} = \langle c_1, c_2, d_1, d_2 \rangle$ be the vector forms of $(a+\lambda b)$ and $(c+\lambda d)$ over $\mathbb{F}_2$. Also note that, for example, that $a = a_1 + a_2\omega$. Let $\overline{w} = \overline{v}(\overline{u}A)$, which means $\overline{w}$ is the3 vector form of $(a + \lambda b) * (c + \lambda d)$. We get the following result:

$$\begin{aligned} \overline{w} = \langle \quad & a_1c_1 + a_2c_2 + b_2d_2 + a_2d_1 + b_1d_1 + b2d_1 && , \\ & a_2c_1 + a_1c_2 + a_2c_2 + b_2d_1 + a_2d_2 + b_1d_2 && , \\ & b_1c_1 + b_2c_2 + a_1d_1 + b_1d_1 + b_2d_1 + a_2d_2 + b_2d_2 && , \\ & b_2c_1 + b_1c_2 + b_2c_2 + a_2d_1 + b_2d_1 + a_1d_2 + a_2d_2 + b_1d_2 && \rangle \end{aligned}$$

Note that the first two coordinates of $\overline{w}$ are the coefficients of 1 and ω respectively. Thus we take $\overline{w}_1 + \omega\overline{w}_2$ to find the first part of the product:

$$
\begin{aligned}
(1) \qquad & a_1c_1 + a_2c_2 + b_2d_2 + a_2d_1 + b_1d_1 + b2d_1 \\
& +\omega(a_2c_1 + a_1c_2 + a_2c_2 + b_2d_1 + a_2d_2 + b_1d_2)
\end{aligned}
$$

$$
\begin{aligned}
(2) \quad = \quad & a_1c_1 + a_2c_2 + b_2d_2 + a_2d_1 + b_1d_1 + b2d_1 + a_2c_1\omega + a_1c_2\omega + a_2c_2\omega \\
& +b_2d_1\omega + a_2d_2\omega + b_1d_2\omega
\end{aligned}
$$

$$
\begin{aligned}
(3) \quad = \quad & (a_1c_1 + a_2c_2 + a_2c_1\omega + a_1c_2\omega + a_2c_2\omega) + (a_2d_1 + a_2d_2\omega) \\
& +(b_2d_2 + b_1d_2\omega + b_1d_1 + b_2d_1 + b_2d_1\omega)
\end{aligned}
$$

$$
\begin{aligned}
(4) \quad = \quad & (c_1(a_1 + a_2\omega) + a_1c_2\omega + a_2c_2\omega^2) + (a_2(d_1 + d_2\omega)) \\
& +(b_2d_2 + b_1(d_1 + d_2\omega) + b_2d_1\omega^2)
\end{aligned}
$$

$$
\begin{aligned}
(5) \quad = \quad & (c_1(a_1 + a_2\omega) + (c_2\omega)(a_1 + a_2\omega)) + (a + a^2)d \\
& +(b_2d_2 + b_1(d_1 + d_2\omega) + b_2d_1\omega^2 + b_2d_2\omega + b_2d_2\omega)
\end{aligned}
$$

$$
\begin{aligned}
(6) \quad = \quad & ((c_1 + c_2\omega)(a_1 + a_2\omega)) + (a + a^2)d \\
& +(b_1(d_1 + d_2\omega) + b_2d_1 + b_2d_1\omega + b_2d_2\omega^2 + b_2d_2\omega)
\end{aligned}
$$

$$
\begin{aligned}
(7) \quad &= \quad ac + (a + a^2)d + (b_1(d_1 + d_2\omega) + (b_2\omega)(d_1 + d_2\omega) + b_2(d_1 + d_2\omega)) \\
(8) \quad &= \quad ac + (a + a^2)d + ((b_1 + b_2\omega)(d_1 + d_2\omega) + b_2(d_1 + d_2\omega)) \\
(9) \quad &= \quad ac + (a + a^2)d + bd + (b + b^2)d \\
(10) \quad &= \quad ac + (a + a^2)d + b^2d
\end{aligned}
$$

On line 4 we have a_2 isolated from a. The fact that $a_2 = a + a^2$ comes from the trace function acting on a. We now determine the second part of the product by looking at $\overline{w}_3 + \omega\overline{w}_4$, which we will multiply on the left by λ when we are finished.

$$\begin{aligned}
(1) \qquad & b_1c_1 + b_2c_2 + a_1d_1 + b_1d_1 + b_2d_1 + a_2d_2 + b_2d_2 \\
& +\omega(b_2c_1 + b_1c_2 + b_2c_2 + a_2d_1 + b_2d_1 + a_1d_2 + a_2d_2 + b_1d_2)
\end{aligned}$$

$$\begin{aligned}
(2) \quad = \quad & b_1c_1 + b_2c_2 + a_1d_1 + b_1d_1 + b_2d_1 + a_2d_2 + b_2d_2 \\
& +b_2c_1\omega + b_1c_2\omega + b_2c_2\omega + a_2d_1\omega + b_2d_1\omega + a_1d_2\omega + a_2d_2\omega + b_1d_2\omega
\end{aligned}$$

$$\begin{aligned}
(3) \quad = \quad & (b_1c_1 + b_2c_2 + b_2c_1\omega + b_1c_2\omega + b_2c_2\omega) \\
& +(a_1d_1 + a_2d_2 + a_2d_1\omega + a_1d_2\omega + a_2d_2\omega) \\
& +(b_1d_1 + b_2d_1 + b_2d_2 + b_2d_1\omega + b_1d_2\omega)
\end{aligned}$$

$$(4) \quad = \quad bc + ad + b^2d$$

This gives the final result, where $T : \mathbb{F}_4 \mapsto \mathbb{F}_2$ is the standard trace function $T(x) = x + x^2$:

$$(a + \lambda b) * (c + \lambda d) = ac + T(a)d + b^2d + \lambda(bc + ad + b^2d)$$

Notice that this is very similar to the QWN construction, with the only difference being the term $T(a)d$. This is the result from looking at only the first matrix, and it would be prudent to list products defined by the other matrices:

(2) $ac + T(a)d + bd + \lambda(bc + ad + b^2d)$

(3) $ac + T(a)d\omega^2 + b^2d + \lambda(bc + ad + b^2d\omega)$

(4) $ac + T(a)d\omega^2 + bd\omega + \lambda(bc + ad + b^2d\omega)$

(5) $ac + T(a)d\omega + b^2d + \lambda(bc + ad + b^2d\omega^2)$

(6) $ac + T(a)d\omega + bd\omega^2 + \lambda(bc + ad + b^2d\omega^2)$

(7) $ac + T(a)d^2 + b^2d^2 + \lambda(bc + ad + b^2d + T(b)T(d))$

(8) $ac + T(a)d^2 + bd + \lambda(bc + ad + b^2d + T(b)T(d))$

(9) $ac + T(a)d^2\omega^2 + bd\omega^2 + \lambda(bc + ad + T(b)R(d) + R(b)T(d)\omega)$

(10) $ac + T(a)d^2\omega^2 + b^2d^2\omega + \lambda(bc + ad + T(b)R(d) + R(b)T(d)\omega)$

(11) $ac + T(a)d^2\omega + b^2d^2\omega^2 + \lambda(bc + ad + b^2d\omega + R(b)R(d)\omega)$

(12) $ac + T(a)d^2\omega + bd\omega + \lambda(bc + ad + b^2d\omega + R(b)R(d)\omega)$

where $R(a) = a_1 + a_2 + a_1a_2$. The initial choice is still one of the simplest representations (due to the lack of R or products including ω), so that is the one which is listed in section 8.6. For now we will also note that $\{3, 1\}$, $\{3, 2\}$, and $\{3, 85\}$ yield formulas similar to (7) or (8) on the list.

In fact, $\{3, 1\}$ will be useful to illustrate another approach to deriving constructions. First, note that the product formula for $\{3, 1\}$ is

$$(a + \lambda b) * (c + \lambda d) = ac + T(a)T(d)\omega^2 + b^2d\omega + \lambda(bc + a^2d + T(b)T(d)\omega^2)$$

Let A be the cubical array which yielded this product. The transpose of A corresponds to a reverse decimal matrix located in $\{3, 74\}$ meaning that these two semifields are

duals of each other. Thus we simply swap a with c and b with d in the product formula for $\{3,1\}$ to get the product for $\{3,74\}$. This gives

$$(a+\lambda b)*(c+\lambda d) = ac + T(b)T(c)\omega^2 + bd^2\omega + \lambda(ad + bc^2 + T(b)T(d)\omega^2)$$

This also means that the assumption $(\lambda b)*c = \lambda(bc)$ will not be true for $\{3,74\}$, and, instead $b*(\lambda c) = \lambda(bc)$. Rather than describe the multiplication in this way, we will instead use the basis $\{1,\omega,X,\omega X\}$ since this behavior is similar to Petit's construction. This changes the product in $\{3,74\}$ to

$$(a+bX)*(c+dX) = ac + T(b)T(c)\omega^2 + bd^2\omega + (ad + bc^2 + T(b)T(d)\omega^2)X$$

This is how this semifield is described in section 8.6. And using this method, we can find $\{3,73\}$ and $\{3,75\}$, which are the duals of $\{3,85\}$ and $\{3,2\}$ respectively.

8.4 Determining Constructions Part 2: Almost Quadratic Over $\mathbb{F}_4$

We will say a semifield of order 16 is *almost right quadratic* over $\mathbb{F}_4$ if it a basis of the form $\{1,\omega,\lambda,\lambda\omega\}$ where $\lambda*\omega = \lambda\omega$, but $(\lambda\omega)*\omega \neq \lambda(\omega^2)$. The semifields corresponding to $\{3,7\}$, $\{3,9\}$, $\{3,11\}$, $\{3,88\}$, and $\{3,89\}$ are all almost right quadratic over $\mathbb{F}_4$ are are the dual of such a semifield.

We will only show the derivation for $\{3,7\}$ here. First, we choose the cubical array A corresponding to the following reverse decimal matrix:

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 2 & 3 & 14 & 4 \\ 4 & 8 & 6 & 3 \\ 8 & 13 & 9 & 2 \end{pmatrix} \sim A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0111 & 0010 \\ 0010 & 0001 & 0110 & 1100 \\ 0001 & 1011 & 1001 & 0100 \end{pmatrix}$$

We let $\overline{u}$ and $\overline{v}$ be the vector forms of $(a+\lambda b)$ and $(c+\lambda d)$ over $\mathbb{F}_2$, and $\overline{w} = \overline{v}(\overline{u}A)$. This gives

$$\begin{aligned}\overline{w} = \langle \quad & a_1c_1 + a_2c_2 + b_2c_2 + b_2d_1 + b_1d_2 && , \\ & a_2c_1 + a_1c_2 + a_2c_2 + a_2d_1 + b_1d_1 + b_1d_2 + b_2d_2 && , \\ & b_1c_1 + b_2c_2 + a_1d_1 + a_2d_1 + b_1d_1 + a_2d_2 && , \\ & b_2c_1 + b_1c_2 + b_2c_2 + a_2d_1 + b_2d_1 + a_1d_2 && \rangle\end{aligned}$$

Then the first part of the product is $\overline{w}_1 + \omega\overline{w}_2$:

$$\begin{aligned}(1) \qquad & a_1c_1 + a_2c_2 + b_2c_2 + b_2d_1 + b_1d_2 \\ & +\omega(a_2c_1 + a_1c_2 + a_2c_2 + a_2d_1 + b_1d_1 + b_1d_2 + b_2d_2)\end{aligned}$$

$$\begin{aligned}(2) \quad = \quad & a_1c_1 + a_2c_2 + b_2c_2 + b_2d_1 + b_1d_2 \\ & +(a_2c_1\omega + a_1c_2\omega + a_2c_2\omega + a_2d_1\omega + b_1d_1\omega + b_1d_2\omega + b_2d_2\omega)\end{aligned}$$

$$\begin{aligned}(3) \quad = \quad & (a_1c_1 + a_2c_2 + a_2c_1\omega + a_1c_2\omega + a_2c_2\omega) + (b_2c_2) + (a_2d_1\omega) \\ & +(b_2d_1 + b_1d_2 + b_1d_1\omega + b_1d_2\omega + b_2d_2\omega)\end{aligned}$$

$$\begin{aligned}(4) \quad = \quad & ac + (b_2c_2) + (a_2d_1\omega) + b^2d\omega \\ (5) \quad = \quad & ac + T(b)T(c) + T(a)R(d)\omega + b^2d\omega\end{aligned}$$

where $R(a_1 + \omega a_2) = a_1$. There is no standard function for R like there was for T, so we will leave it as is. Then we compute $\overline{w}_3 + \omega\overline{w}_4$:

$$\begin{aligned}
(1) \qquad & b_1c_1 + b_2c_2 + a_1d_1 + a_2d_1 + b_1d_1 + a_2d_2 \\
& +\omega(b_2c_1 + b_1c_2 + b_2c_2 + a_2d_1 + b_2d_1 + a_1d_2) \\
(2) \quad = \quad & b_1c_1 + b_2c_2 + a_1d_1 + a_2d_1 + b_1d_1 + a_2d_2 \\
& +(b_2c_1\omega + b_1c_2\omega + b_2c_2\omega + a_2d_1\omega + b_2d_1\omega + a_1d_2\omega) \\
(3) \quad = \quad & (b_1c_1 + b_2c_2 + b_2c_1\omega + b_1c_2\omega + b_2c_2\omega) \\
& +(a_1d_1 + a_2d_1 + a_2d_2 + a_2d_1\omega + a_1d_2\omega) + (b_1d_1 + b_2d_1\omega) \\
(4) \quad = \quad & bc + a^2d + R(d)b
\end{aligned}$$

And we get the following product:

$$(a + \lambda b) * (c + \lambda d) = ac + T(b)T(c) + T(a)R(d)\omega + b^2d\omega + \lambda(bc + a^2d + R(d)b)$$

This method, and the use of duals, yields similar formulas for $\{3, 9\}$, $\{3, 11\}$, $\{3, 88\}$, and $\{3, 89\}$.

8.5 Determining Constructions Part 3: Not Quadratic Over $\mathbb{F}_4$

All of the semifields mentioned thus far have contained a subfield isomorphic to $\mathbb{F}_4$. The remaining unknown semifields, $\{3, 4\}$, $\{3, 5\}$, $\{3, 6\}$, $\{3, 8\}$ and $\{3, 90\}$ do not posses this feature, and thus will not be quadratic or almost quadratic over $\mathbb{F}_4$. Rather than giving a product formula for such semifields, we will instead attempt to find a basis of the form $\{1, a, b, c\}$ for these semifields over $\mathbb{F}_2$ which will posses similar properties in each of these semifields. By investigation, all of these semifields

have such a basis where $a^2 = b$, $b^2 = c$, and c^2 is some linear combination of 1, a, and b. In section 8.6, for each of these semifields we provide a multiplication table of the nontrivial basis elements in place of a product formula.

8.6 A Catalog Of The 16-Element Semifields

In this section we provide as much pertinent information as possible for each of the finite semifields of order 16. Each semifield, S, is given an entry in a similar format. First we list any names which have been given for S. Beneath the name, we provide a Knuth cube, A, which was used to define the other results in the entry. To the right of A we list the database numbers for S, "DB", the designation for S given by Kleinfeld, "KD", the database numbers for the dual of S, "Dual DB", the designation for the dual of S given by Kleinfeld, "Dual KD". Below the Knuth cube, we list which known constructions yield S, "Construction:", we describe what form the elements may have, "Elements", and below that provide a product formula or multiplication table. This is followed by the left, middle, and right nuclei, the center, and the left and right primitive elements of S with respect to the given construction, denoted N_l, N_m, N_r, Z, P_l and P_r respectively. This is followed by the lists of with respect to this construction, denoted P_l and P_r respectively. Finally, the automorphisms of S are listed, denoted ϕ_i unless there is only the trivial automorphism.

For each semifield which can be constructed using a known construction, we list the necessary information for that construction to be used. In the case where multiple variations of the same construction can be used, e.g. choices of f qand g in the QWN construction, we only provide one possible set of values. And in the case where multiple constructions yield the same semifield (up to isomorphism), the

construction used to define the product is presented last.

The results of chapters 4 and 5 were used to determine the primitive elements and automorphisms of each semifield. The center and nuclei of each semifield were determined by direct computation with the aid of a computer.

Name: $GF(16)$, $\mathbb{F}_{16}$

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0001 & 0011 \\ 0010 & 0001 & 0110 & 1101 \\ 0001 & 0011 & 1101 & 1011 \end{pmatrix}$$

DB: $\{1, 1\}$

Dual DB: $\{1, 1\}$

KD: None

Dual KD: None

Construction: The field $\mathbb{F}_4[\lambda]$, where λ is a root of $x^2 + x + \omega$.

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + bd\omega + \lambda(bc + ad + bd)$

$$\begin{aligned} N_l &= \mathbb{F}_{16} \\ N_m &= \mathbb{F}_{16} \\ N_r &= \mathbb{F}_{16} \\ Z &= \mathbb{F}_{16} \\ P_l &= \{a + \lambda | a \in \mathbb{F}_4\} \cup \{1 + \lambda\omega, \omega + \lambda\omega, \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \\ P_r &= \{a + \lambda | a \in \mathbb{F}_4\} \cup \{1 + \lambda\omega, \omega + \lambda\omega, \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b & \qquad \phi_3(a + \lambda b) &= (a + \lambda b)^4 \\ \phi_2(a + \lambda b) &= (a + \lambda b)^2 & \qquad \phi_4(a + \lambda b) &= (a + \lambda b)^8 \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 1010 & 0101 \\ 0001 & 0011 & 1101 & 1011 \end{pmatrix}$$

DB: $\{2, 1\}$

Dual DB: $\{2, 1\}$

KD: T(24)

Dual KD: T(24)

Construction: QWN: case 2, type 4, $f = g = 1$.

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + b^2 d + \lambda(bc + a^2 d + bd)$

$$\begin{aligned} N_l &= \{0, 1, \omega, \omega^2\} \\ N_m &= \{0, 1, \lambda, \lambda^2\} \\ N_r &= \{0, 1, \omega, \omega^2\} \\ Z &= \{0, 1\} \\ P_l &= \{1 + \lambda\omega, \lambda^2(\omega), \omega^2 + \lambda, \lambda^2(\omega^2)\} \\ P_r &= \{1 + \lambda\omega, \omega^2 + \lambda\omega, \omega^2 + \lambda, \omega + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a^2 + \lambda(b^2) \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 1001 & 0111 \\ 0010 & 0001 & 1010 & 0101 \\ 0001 & 0101 & 1111 & 1010 \end{pmatrix}$$

DB: $\{2, 5\}$

Dual DB: $\{2, 5\}$

KD: T(45)

Dual KD: T(45)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + T(a)d + b^2d + \lambda(bc + ad + b^2d)$,

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$N_l = \{0, 1, \omega + \lambda, \omega^2 + \lambda\}$

$N_m = \{0, 1, \lambda, \lambda^2\}$

$N_r = \{0, 1, \omega, \omega^2\}$

$Z = \{0, 1\}$

$P_l = \{1 + \lambda\omega, \omega^2 + \lambda\omega, 1 + \lambda(\omega^2), \omega + \lambda(\omega^2)\}$

$P_r = \{1 + \lambda\omega, \omega^2 + \lambda\omega, 1 + \lambda(\omega^2), \omega + \lambda(\omega^2)\}$

Automorphisms:

$\phi_1(a + \lambda b) = a + \lambda b$

$\phi_2(a + \lambda b) = a + \lambda^2(b)$

$\phi_3(a + \lambda b) = a^2 + \lambda(b^2)$

$\phi_4(a + \lambda b) = a^2 + \lambda^2(b^2)$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 1010 & 0101 \\ 0001 & 0011 & 1111 & 1010 \end{pmatrix}$$

DB: $\{2, 6\}$

Dual DB: $\{2, 13\}$

KD: T(50)

Dual KD: T(25)

Construction: QWN: case 2, type 2, $f = g = 1$.

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + b^2 d + \lambda(bc + a^2 d + b^2 d)$

$$\begin{aligned} N_l &= \{0, 1, \lambda, \lambda^2\} \\ N_m &= \{0, 1, \omega, \omega^2\} \\ N_r &= \{0, 1, \omega, \omega^2\} \\ Z &= \{0, 1\} \\ P_l &= \{1 + \lambda\omega, \omega^2 + \lambda\omega, 1 + \lambda(\omega^2), \omega + \lambda(\omega^2)\} \\ P_r &= \{\omega + \lambda, \omega^2 + \lambda, \lambda^2(\omega), \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \lambda^2(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a^2 + \lambda(b^2) \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 1010 & 0111 \\ 0001 & 0011 & 1101 & 1010 \end{pmatrix}$$

DB: $\{2, 13\}$

Dual DB: $\{2, 6\}$

KD: T(25)

Dual KD: T(50)

Construction: Petit: $M(X) = X^2 + X + 1$.

QWN: case 2, type 3, $f = g = 1$.

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + b^2 d + \lambda(bc + a^2 d + bd^2)$

$$\begin{aligned} N_l &= \{0, 1, \omega, \omega^2\} \\ N_m &= \{0, 1, \omega, \omega^2\} \\ N_r &= \{0, 1, \lambda, \lambda^2\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + \lambda, \omega^2 + \lambda, \lambda^2(\omega), \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \lambda^2(\omega^2)\} \\ P_r &= \{1 + \lambda\omega, \lambda^2(\omega), 1 + \lambda(\omega^2), \lambda^2(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a^2 + \lambda(b^2) \end{aligned}$$

Name: System W

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 0100 & 1100 \\ 0001 & 0011 & 1000 & 0100 \end{pmatrix}$$

DB: $\{2, 15\}$

Dual DB: $\{2, 15\}$

KD: T(35)

Dual KD: T(35)

Construction: Petit: $M(X) = X^2 + \omega$.

QWN: case 2, any type, $f = \omega$, $g = 0$.

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + b^2 d\omega + \lambda(bc + a^2 d)$

$$\begin{aligned} N_l &= \{0, 1, \omega, \omega^2\} \\ N_m &= \{0, 1, \omega, \omega^2\} \\ N_r &= \{0, 1, \omega, \omega^2\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + \lambda, \omega^2 + \lambda, \omega + \lambda\omega, \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \\ P_r &= \{\omega + \lambda, \omega^2 + \lambda, \omega + \lambda\omega, \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a + \lambda(b\omega) \\ \phi_3(a + \lambda b) &= a + \lambda(b\omega^2) \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 1110 \\ 0010 & 0001 & 0100 & 1100 \\ 0001 & 0011 & 1000 & 0111 \end{pmatrix}$$

DB: $\{3, 1\}$

Dual DB: $\{3, 74\}$

KD: V(5)

Dual KD: V(4)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + \lambda b) * (c + \lambda d) = ac + T(a)T(d)\omega^2 + b^2 d\omega + \lambda(bc + a^2 d + T(b)T(d)\omega^2)$,

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{1 + \lambda\omega, \omega^2 + \lambda\omega, 1 + \lambda(\omega^2), \omega + \lambda(\omega^2) \\ P_r &= \{\omega + \lambda, \omega^2 + \lambda, \lambda\omega, 1 + \lambda\omega, \lambda(\omega^2), 1 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\phi(a + \lambda b) = a + \lambda b$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0110 \\ 0010 & 0001 & 0100 & 1111 \\ 0001 & 0011 & 1000 & 0100 \end{pmatrix}$$

DB: $\{3, 2\}$

Dual DB: $\{3, 75\}$

KD: V(9)

Dual KD: V(8)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + \lambda b) * (c + \lambda d) = ac + T(a)T(d)\omega + b^2 d\omega + \lambda(bc + a^2 d + R(b)T(d)\omega^2)$,

where $T(a) = a + a^2$, $R(a) = a + T(a)\omega$;

equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$, $R(a) = a_1$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{1 + \lambda, \omega + \lambda, 1 + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \\ P_r &= \{\omega + \lambda, \omega^2 + \lambda, \lambda\omega, 1 + \lambda\omega, \lambda(\omega^2), 1 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a^2 + b^2\omega + \lambda(b^2\omega^2) \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 0010 & 0101 & 1000 \\ 0010 & 1111 & 0001 & 0100 \\ 0001 & 0101 & 1111 & 0110 \end{pmatrix}$$

DB: $\{3, 4\}$

Dual DB: $\{3, 90\}$

KD: V(1)

Dual KD: V(6)

Construction:

Elements: $(a + bi + cj + dk)$, where $a, b, c, d \in \mathbb{F}_2$

Product: Let $z = 1 + i + j + k$. The products of i, j, and k are:

$*$	i	j	k
i	j	$i + k$	1
j	z	k	i
k	$i + k$	z	$i + j$

$N_l = \{0, 1\}$

$N_m = \{0, 1\}$

$N_r = \{0, 1\}$

$Z = \{0, 1\}$

$P_l = \{1 + j, i + j, j + k, i + j + k\}$

$P_r = \{i, 1 + i, k, 1 + k, j + k, 1 + j + k\}$

Automorphisms:

$\phi(a + bi + cj + dk) = a + bi + cj + dk$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 0010 & 1001 & 1110 \\ 0010 & 1111 & 0001 & 0100 \\ 0001 & 0011 & 0100 & 1100 \end{pmatrix}$$

DB: $\{3, 5\}$

Dual DB: $\{3, 8\}$

KD: V(3)

Dual KD: V(7)

Construction:

Elements: $(a + bi + cj + dk)$, where $a, b, c, d \in \mathbb{F}_2$

Product: Let $z = 1 + i + j + k$. The products of i, j, and k are:

$*$	i	j	k
i	j	$1 + k$	$1 + i + j$
j	z	k	i
k	$j + k$	i	$1 + i$

$N_l = \{0, 1\}$

$N_m = \{0, 1\}$

$N_r = \{0, 1\}$

$Z = \{0, 1\}$

$P_l = \{1 + j, i + j, 1 + j + k, 1 + i + j + k\}$

$P_r = \{k, i + k, j + k, 1 + i + j + k\}$

Automorphisms:

$\phi(a + bi + cj + dk) = a + bi + cj + dk$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 0010 & 1001 & 0101 \\ 0010 & 0101 & 0001 & 1111 \\ 0001 & 1000 & 1101 & 0110 \end{pmatrix}$$

DB: $\{3, 6\}$

Dual DB: $\{3, 6\}$

KD: V(12)

Dual KD: V(12)

Construction:

Elements: $(a + bi + cj + dk)$, where $a, b, c, d \in \mathbb{F}_2$

Product: Let $z = 1 + i + j + k$. The products of i, j, and k are:

$*$	i	j	k
i	j	$1 + k$	$i + k$
j	$i + k$	k	z
k	1	$1 + i + k$	$i + j$

$N_l = \{0, 1\}$

$N_m = \{0, 1\}$

$N_r = \{0, 1\}$

$Z = \{0, 1\}$

$P_l = \{i, 1 + i + j, i + k, i + j + k\}$

$P_r = \{1 + j, 1 + i + j, 1 + j + k, i + j + k\}$

Automorphisms:

$\phi(a + bi + cj + dk) = a + bi + cj + dk$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0111 & 0010 \\ 0010 & 0001 & 0110 & 1100 \\ 0001 & 1011 & 1001 & 0100 \end{pmatrix}$$

DB: $\{3, 7\}$

Dual DB: $\{3, 7\}$

KD: V(17)

Dual KD: V(17)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + \lambda b) * (c + \lambda d) = ac + T(b)T(c) + T(a)R(d)\omega + b^2 d\omega + \lambda(bc + a^2 d + R(d)b)$,

where $T(a) = a + a^2$, $R(a) = a + T(a)\omega$;

equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$, $R(a) = a_1$.

$N_l = \{0, 1\}$

$N_m = \{0, 1\}$

$N_r = \{0, 1\}$

$Z = \{0, 1\}$

$P_l = \{1 + \lambda, \omega^2 + \lambda, 1 + \lambda(\omega^2), \omega + \lambda(\omega^2)\}$

$P_r = \{\lambda, \omega^2 + \lambda, \lambda(\omega^2), \omega + \lambda(\omega^2)\}$

Automorphisms:

$\phi(a + \lambda b) = a + \lambda b$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 0010 & 1111 & 0011 \\ 0010 & 1001 & 0001 & 0100 \\ 0001 & 1110 & 0100 & 1100 \end{pmatrix}$$

DB: $\{3, 8\}$

Dual DB: $\{3, 5\}$

KD: V(7)

Dual KD: V(3)

Construction:

Elements: $(a + bi + cj + dk)$, where $a, b, c, d \in \mathbb{F}_2$

Product: Let $z = 1 + i + j + k$. The products of i, j, and k are:

$*$	i	j	k
i	j	z	$j + k$
j	$1 + k$	k	i
k	$1 + i + j$	i	$1 + i$

$N_l = \{0, 1\}$

$N_m = \{0, 1\}$

$N_r = \{0, 1\}$

$Z = \{0, 1\}$

$P_l = \{k, i + k, j + k, 1 + i + j + k\}$

$P_r = \{1 + j, i + j, 1 + j + k, 1 + i + j + k\}$

Automorphisms:

$$\phi(a + bi + cj + dk) = a + bi + cj + dk$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 1011 & 1110 \\ 0010 & 0001 & 1010 & 1101 \\ 0001 & 1011 & 1111 & 0110 \end{pmatrix}$$

DB: $\{3, 9\}$

Dual DB: $\{3, 9\}$

KD: V(18)

Dual KD: V(18)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + \lambda b) * (c + \lambda d) = ac + T(b)T(c) + T(a)d^2 + b^2d^2 + \lambda(bc + a^2d + b^2d)$,

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{1 + \lambda\omega, \omega + \lambda\omega, 1 + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \\ P_r &= \{\lambda\omega, \omega + \lambda\omega, \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a^2 + \lambda(b^2) \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & & & \\ 0010 & & & \\ 0001 & & & \end{pmatrix}$$

DB: $\{3, 11\}$

Dual DB: $\{3, 89\}$

KD: V(11)

Dual KD: V(14)

Construction:

Elements: $(a + bX)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + bX) * (c + dX) = ac + T(a)T(d)\omega^2 + T(c)b\omega + bd^2\omega + (bc + ad + T(b)T(d)\omega)X,$

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1, \omega + \omega X, \omega^2 + \omega X\} \\ P_l &= \{X, \omega^2 + X, (\omega^2)X, \omega + (\omega^2)X\} \\ P_r &= \{\omega X, 1 + \omega X, (\omega^2)X, 1 + (\omega^2)X, \omega + (\omega^2 X), \omega^2 + (\omega^2)X\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + bX) &= a + bX & \phi_3(a + \lambda b) &= \\ \phi_2(a + bX) &= a + b\omega^2 + bX & \phi_4(a + \lambda b) &= \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 1001 & 0110 \\ 0001 & 0011 & 1110 & 1011 \end{pmatrix}$$

DB: $\{3, 70\}$

Dual DB: $\{3, 70\}$

KD: V(10)

Dual KD: V(10)

Construction: QWN: case 2, type 1, $f = 1$, $g = \omega$.

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + b^2 d + \lambda(bc + a^2 d + b^2 d^2 \omega)$

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + \lambda, \omega^2 + \lambda, \omega + \lambda\omega, \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \\ P_r &= \{\omega + \lambda, \omega^2 + \lambda, \omega + \lambda\omega, \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a + \lambda(b\omega) \\ \phi_2(a + \lambda b) &= a + \lambda(b\omega^2) \end{aligned}$$

Name: System V

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0011 & 0010 \\ 0010 & 0001 & 1010 & 0111 \\ 0001 & 0011 & 1111 & 1001 \end{pmatrix}$$

DB: $\{3, 71\}$

Dual DB: $\{3, 71\}$

KD: V(13)

Dual KD: V(13)

Construction: QWN: case 2, type 1, $f = g = 1$.

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product: $(a + \lambda b) * (c + \lambda d) = ac + b^2 d + \lambda(bc + a^2 d + b^2 d^2)$

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + \lambda, \omega^2 + \lambda, \lambda^2(\omega), \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \lambda^2(\omega^2)\} \\ P_r &= \{\omega + \lambda, \omega^2 + \lambda, \lambda^2(\omega), \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \lambda^2(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b & \qquad \phi_4(a + \lambda b) &= a^2 + \lambda(b^2) \\ \phi_2(a + \lambda b) &= a + \lambda(b\omega) & \qquad \phi_5(a + \lambda b) &= a^2 + \lambda(b^2\omega) \\ \phi_3(a + \lambda b) &= a + \lambda(b\omega^2) & \qquad \phi_6(a + \lambda b) &= a^2 + \lambda(b^2\omega^2) \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0001 & 0011 \\ 0010 & 1011 & 1010 & 1101 \\ 0001 & 1110 & 0111 & 1010 \end{pmatrix}$$

DB: $\{3, 73\}$

Dual DB: $\{3, 85\}$

KD: V(16)

Dual KD: V(15)

Construction:

Elements: $(a + bX)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + bX) * (c + dX) = ac + T(c)b^2 + bd^2 + (ad + bc^2 + b^2d)X$

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + X, \omega^2 + X, \omega X, 1 + \omega X, (\omega^2)X, 1 + (\omega^2)X\} \\ P_r &= \{\omega + X, \omega^2 + X, \omega + \omega X, \omega^2 + \omega X, \omega + (\omega^2)X, \omega^2 + (\omega^2)X\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + bX) &= a + bX \\ \phi_2(a + bX) &= a^2 + (b^2)X \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0001 & 0011 \\ 0010 & 0011 & 0100 & 1000 \\ 0001 & 1110 & 1100 & 0111 \end{pmatrix}$$

DB: $\{3, 74\}$

Dual DB: $\{3, 1\}$

KD: V(4)

Dual KD: V(5)

Construction:

Elements: $(a + bX)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + bX) * (c + dX) = ac + T(b)T(c)\omega^2 + bd^2\omega + (ad + bc^2 + T(b)T(d)\omega^2)X$

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + X, \omega^2 + X, \omega X, 1 + \omega X, (\omega^2)X, 1 + (\omega^2)X\} \\ P_r &= \{1 + \omega X, \omega^2 + \omega X, 1 + (\omega^2)X, \omega + (\omega^2)X\} \end{aligned}$$

Automorphisms:

$$\phi(a + bX) = a + bX$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0001 & 0011 \\ 0010 & 0011 & 0100 & 1000 \\ 0001 & 0110 & 1111 & 0100 \end{pmatrix}$$

DB: $\{3, 75\}$

Dual DB: $\{3, 2\}$

KD: V(8)

Dual KD: V(9)

Construction:

Elements: $(a + bX)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + bX) * (c + dX) = ac + T(b)T(c)\omega + bd^2\omega + (ad + bc^2 + T(b)R(d)\omega^2)X$

where $T(a) = a + a^2$, $R(a) = a + T(a)\omega$;

equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$, $R(a) = a_1$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + X, \omega^2 + X, \omega X, 1 + \omega X, (\omega^2)X, 1 + (\omega^2)X\} \\ P_r &= \{1 + X, \omega + X, 1 + (\omega^2)X, \omega^2 + (\omega^2)X\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + bX) &= a + bX \\ \phi_2(a + bX) &= a^2 + b^2\omega + (b^2\omega^2)X \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 1011 & 1110 \\ 0010 & 0001 & 1010 & 0111 \\ 0001 & 0011 & 1101 & 1010 \end{pmatrix}$$

DB: $\{3, 85\}$

Dual DB: $\{3, 73\}$

KD: V(15)

Dual KD: V(16)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + \lambda b) * (c + \lambda d) = ac + T(a)d^2 + b^2 d + \lambda(bc + a^2 d + bd^2)$,

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{\omega + \lambda, \omega^2 + \lambda, \omega + \lambda\omega, \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \\ P_r &= \{\omega + \lambda, \omega^2 + \lambda, \lambda\omega, 1 + \lambda\omega, \lambda(\omega^2), 1 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a^2 + \lambda(b^2) \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 1101 & 1011 \\ 0010 & 0001 & 1100 & 1000 \\ 0001 & 1111 & 0111 & 1100 \end{pmatrix}$$

DB: $\{3, 88\}$

Dual DB: $\{3, 88\}$

KD: V(2)

Dual KD: V(2)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + \lambda b) * (c + \lambda d) = ac + T(b)T(c)\omega^2 + T(a)d\omega^2 + b^2 d\omega^2 + \lambda(bc + ad + T(b)R(d)\omega^2)$,

where $T(a) = a + a^2$, $R(a) = a + T(a)\omega$;

equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$, $R(a) = a_1$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1\} \\ P_l &= \{\lambda\omega, 1 + \lambda\omega, \omega + \lambda\omega, \omega^2 + \lambda\omega, \lambda(\omega^2), 1 + \lambda(\omega^2)\} \\ P_r &= \{\lambda\omega, 1 + \lambda\omega, \omega + \lambda\omega, \omega^2 + \lambda\omega, \omega + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a + b\omega + \lambda b \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 1100 & 0101 & 1111 \\ 0010 & 0001 & 0100 & 1100 \\ 0001 & 1111 & 1000 & 0101 \end{pmatrix}$$

DB: $\{3, 89\}$

Dual DB: $\{3, 11\}$

KD: V(14)

Dual KD: V(11)

Construction:

Elements: $(a + \lambda b)$ where $a, b \in \mathbb{F}_4$, and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$

Product:

$(a + \lambda b) * (c + \lambda d) = ac + T(b)T(c)\omega^2 + T(a)d\omega + b^2 d\omega + \lambda(bc + ad + T(b)T(d)\omega)$,

where $T(a) = a + a^2$; equivalently, if $a = a_1 + a_2\omega$, $T(a) = a_2$.

$$\begin{aligned} N_l &= \{0, 1\} \\ N_m &= \{0, 1\} \\ N_r &= \{0, 1\} \\ Z &= \{0, 1, \omega + \lambda\omega, \omega^2 + \lambda\omega\} \\ P_l &= \{\lambda\omega, 1 + \lambda\omega, \lambda(\omega^2), 1 + \lambda(\omega^2), \omega + \lambda(\omega^2), \omega^2 + \lambda(\omega^2)\} \\ P_r &= \{\lambda, \omega^2 + \lambda, \lambda(\omega^2), \omega + \lambda(\omega^2)\} \end{aligned}$$

Automorphisms:

$$\begin{aligned} \phi_1(a + \lambda b) &= a + \lambda b \\ \phi_2(a + \lambda b) &= a + b\omega^2 + \lambda b \end{aligned}$$

Name:

$$A = \begin{pmatrix} 1000 & 0100 & 0010 & 0001 \\ 0100 & 0010 & 1111 & 0101 \\ 0010 & 0101 & 0001 & 1111 \\ 0001 & 1000 & 0100 & 0110 \end{pmatrix}$$

DB: $\{3, 90\}$

Dual DB: $\{3, 4\}$

KD: V(6)

Dual KD: V(1)

Construction:

Elements: $(a + bi + cj + dk)$, where $a, b, c, d \in \mathbb{F}_2$

Product: Let $z = 1 + i + j + k$. The products of i, j, and k are:

$*$	i	j	k
i	j	z	$i + k$
j	$i + k$	k	z
k	1	i	$i + j$

$N_l = \{0, 1\}$

$N_m = \{0, 1\}$

$N_r = \{0, 1\}$

$Z = \{0, 1\}$

$P_l = \{i, 1 + i, k, 1 + k, j + k, 1 + j + k\}$

$P_r = \{1 + j, i + j, j + k, i + j + k\}$

Automorphisms:

$$\phi(a + bi + cj + dk) = a + bi + cj + dk$$

References

[1] M. I. M. Al-Ali. The automorphism group of a semifield of order q^4. *Comm. Algebra*, 36(9):3347–3352, 2008.

[2] A. A. Albert. On nonassociative division algebras. *Trans. Amer. Math. Soc.*, 72:296–309, 1952.

[3] A. A. Albert. Finite division algebras and finite planes. *Proc. Sympos. Appl. Math.*, 10:53–70, 1960.

[4] E. F. Combarro, I. F. Rúa, and J. Ranilla. Finite semifields with 7^4 elements. *Int. J. Comput. Math.*, 89(13-14):1865–1878, 2012.

[5] L. E. Dickson. Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, 7(3):370–390, 1906.

[6] R. Gow and J. Sheekey. On primitive elements in finite semifields. *Finite Fields Appl.*, 17:194–204, 2011.

[7] V. Jha and N. L. Johnson. The dimension of a subplane of a translation plane. *Bull. Belg. Math. Soc. Simon Stevin*, 17(3):463–477, 2010.

[8] Norman L. Johnson, Vikram Jha, and Mauro Biliotti. *Handbook of Finite Translation Planes*. Taylor and Francis Group, LLC, 2007.

[9] Michael J. Kallaher. *Affine Planes With Transitive Collineation Groups*. Elsevier North Holland Inc., 1982.

[10] E. Kleinfeld. Techniques for enumerating veblen-wedderburn systems. *J. Assoc. Comput. Math.*, 7:330–337, 1960.

[11] D. E. Knuth. Finite semifields and projective planes. *J. Algebra*, 2:182–217, 1965.

[12] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, revised edition, 1986.

[13] G. Menichetti. On a kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J. Algebra*, 47(2):400–410, 1977.

[14] R. H. Oehmke. On finite division rings. *Proc. Amer. Math. Soc.*, 79(2):174–176, 1980.

[15] J. Petit. Quasi-corps gènèralisant un type d'anneau quotient. *C. R. Acad. Sci. Paris Sér A-B*, 265:A708–A711, 1967.

[16] J. Petit. Sur les quasi-corps distributifs à base monogéne. *C. R. Acad. Sci. Paris Sér A-B*, 266:A402–A404, 1968.

[17] I. F. Rúa. Primitive and non primitive finite semifields. *Comm. Algebra*, 32(2):793–803, 2004.

[18] I. F. Rúa, E. F. Combarro, and J. Ranilla. Classification of semifields of order 64. *J. Algebra*, 322(11):4011–4029, 2009.

[19] I. F. Rúa, E. F. Combarro, and J. Ranilla. Determination of division algebras with 243 elements. *Finite Fields Appl.*, 18(6):1148–1155, 2012.

[20] R. Sandler. Autotopism groups of some finite non-associative algebras. *Amer. J. Math.*, 84:239–264, 1962.

[21] R. J. Walker. Determination of division algebras with 32 elements. *Proc. Sympos. Appl. Math.*, Vol. XV:83–85, 1963.

[22] G. P. Wene. On the multiplicative structure of finite division rings. *Aequationes Math.*, 41(2-3):222–233, 1991.

[23] G. P. Wene. Automorphisms of type i semifields quadratic over a weak nucleus. *Algebras Groups Geom.*, 23(4):375–386, 2006.

[24] G. P. Wene. Inner automorphism of finite semifields. *Note Mat.*, 29:231–242, 2009. suppl. 1.

[25] G. P. Wene. Semifields: Two constructions. *Lecture at UT Arlington*, 2012.

Biographical Statement

Kelly C. Aman was born in Moorhead, Minnesota, in 1983. He earned a B.A. in Mathematics from the University of Texas at Arlington in the spring of 2008. That summer he married his wife, Jacqueline, and that fall he began the Ph.D. program in the Department of MAthematics at UT Arlington. Kelly worked as a Graduate Teaching Assistant from the fall of 2008 to the spring of 2012. From the fall of 2012 through the spring of 2014, he was awarded a GK-12 Fellowship, which gave him the unique experience of teaching aspects of his research to middle-school and high-school students.

The research which culminated in this dissertation began in 2011, and began to take focus in the spring of 2012. Kelly presented his first results at Combinatorics 2012 in Perugia, Italy, and he went on to attend many more conferences throughout his final two years in graduate school. Upon the completion of this dissertation, Kelly has had one paper published, along with three papers under review. The results in this dissertation are intended to be the groundwork for further research, and he plans to further investigate the topics in chapters 4 and 7.

His time as a GTA and GK-12 Fellow have inspired Kelly to become a teacher. He believes that anyone can learn mathematics if they have the desire to learn, so part of a teacher's duty is to share their passion for the subject with their students. To that end, teaching will always be an important part of his life from this point forward.