ON PRIMITIVITY AND DIMENSION OF FINITE SEMIFIELDS AND THEIR PLANES

by

LINLIN CHEN

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
July 2012

Copyright © by Linlin Chen 2012

All Rights Reserved

To my family who set the example and who made me who I am.

ACKNOWLEDGEMENTS

The following is my heartfelt appreciation to all those who gave me inspiration, advice, direction and insight to begin, continue and complete my doctoral studies.

I would like to express my deep gratitude to my advisor, Dr. Minerva Cordero, for her guidance, advice, continuous support, encouragement, patience and understanding in both academics and life throughout my four years of study. It has been a true honor to work with her.

I would like to thank Dr. Ruth Gornet, Dr. David Jorgensen, Dr. Dimitar Grantcharov and Dr. Michaela Vancliff for serving as committee and for their guidance and support throughout the course of this research.

I would like to express my deep gratitude to Dr. Jha and Dr. Wene for the several useful discussions we have had. I also would like to thank my fellow graduate students for making my time at University of Texas at Arlington a great experience.

Finally, I would like to express my deep gratitude to my friends Wei Zhai and Changqi Xu who have encouraged and inspired me for my graduate studies. I am extremely fortunate to be so blessed. I am also extremely grateful to my family for their love, support, and understanding over the years.

July 18, 2012

ABSTRACT

ON PRIMITIVITY AND DIMENSION OF FINITE SEMIFIELDS AND THEIR PLANES

Linlin Chen, Ph.D.

The University of Texas at Arlington, 2012

Supervising Professor: Minerva Cordero

The study of semifields originated from the work of L.E. Dickson in 1905 and was greatly developed in the 1960s by Albert, Knuth, Walker, and Kleinfeld among others. Two problems of interest in this area are the primitivity of semifields and the dimension of semifields over their sub-semifields.

For the first problem, we provide an equivalent condition for the right (or left) primitivity of finite semifields and with this result, we find that the classical Knuth binary semifields of order 2^{15}, 2^{17} and 2^{19} are all right and left primitive; the Albert semifields of order 2^i, where $i = 7, 9, 11, 13$ are all primitive. Also we prove that the number of primitive elements in the classical Knuth binary semifields of order 2^t, $t \in [5, 19]$ odd, is a multiple of t.

For the second problem, we first prove that the classical Knuth binary semifields can not be fractional dimensional. Then we consider two special classes of generalized Knuth binary semifields of order 2^t, t odd. One class is fractional dimensional and contains $GF(2^2)$ as a subfield, when $t \in [5, 31]$. The other class is commutative and does not contain the subfields $GF(2^2)$ or $GF(2^3)$. Finally we show that the Albert semifields $A_n(S)$ do not contain the subfield $GF(2^3)$ when $(n, 3) = 1$.

TABLE OF CONTENTS

Appendix

LIST OF ILLUSTRATIONS

Figure Page

CHAPTER 1

INTRODUCTION AND PRELIMINARIES

1.1 Introduction

In this work, we present a study of primitivity and fractional dimension of finite semifields and semifield planes. A finite semifield is an algebraic structure with two distributive laws, the multiplicative identity, and no zero divisors. If a plane is coordinatized by a finite semifield, then it is called a semifield plane.

A finite semifield is (left) right primitive if its multiplicative group is "(left) right cyclic" in a way to be described later. The study of primitivity was initially raised by G.P. Wene. He provided examples of semifields of order 16, 27, 32, 124, and 343 that have a right primitive element, and according to those sporadic examples, he made the following conjecture

Conjecture 1.1.1. *[16] All finite semifields are right primitive.*

Rúa [15] proved that any finite semifield three-dimensional over its center is both left and right primitive. However, he showed that the classical Knuth binary semifield of order 32 is neither right nor left primitive. Then in 2006, Hentzel and Rúa [8] gave another counterexample to Wene's Conjecture, a semifield of order 64. Although this conjecture is incorrect, people are still interested in this problem since for most semifields it is not known if they are right primitive or not.

Let $F = GF(q)$, where $q = p^n$ for some n and p is a prime number. Suppose E is any subfield of F. Then the order of E must be p^i for some i that is a divisor of n. Hence the dimension of F relative to E is an integer. We now generalize the definition of dimension of finite fields relative to subfields to the case of finite semifields.

Definition 1.1.1. *Let D be a finite semifield and E a sub-semifield. Then $dim_E D := log_{|E|}|D|(= \lambda)$ is the dimension of D relative to E. The semifield D has fractional dimensional, relative to E, if λ is not an integer, and now E is a fractional dimensional sub-semifield of D. In general, D is considered fractional (dimensional) if D is fractional dimensional relative to at least one sub-semifield E.*

The center of a semifield D is a set, composed of all the elements in D that commute with all the elements in D and associate with every element in D from left, right and middle. Notice that the center of a finite semifield is a field and we view the semifield as a vector space over its center. Since the center of a finite semifield is a finite field, and hence has order a power of a prime. Therefore the dimension of D relative to its sub-semifields must be an integer or a proper rational number (not an integer). People are interested in the second case, i.e., when is the dimension of D relative to its sub-semifields a rational number?

Jha and Johnson [9] found that the generalized Knuth binary semifields of order 2^t, where t is divisible by 5 or 7, admit the subfield $GF(2^2)$, so the dimension of those semifields over $GF(2^2)$ is fractional. They also made the following conjectures:

Conjecture 1.1.2. *[9] 1. There exist semifield planes of order 2^r, for any odd integer r that admit Desarguesian subplanes of order 2^2.*

2. There exist semifield planes of order 2^t, for any integers t relatively prime to 3 that admit semifield subplanes of order 2^3.

The first part of Conjecture 1.1.2 was completely solved by V. Jha [19]. However, for the second part of Conjecture 1.1.2, no examples to support it have been found.

This thesis is divided into four chapters. Chapter I contains some basic definitions and results on projective planes and finite semifields. Also, the three types of finite semifields that we are working with will be introduced in this chapter.

In Chapter II, after providing the basic definition of primitivity of finite semifields, we prove the following theorems concerning primitivity.

Theorem 2.2.2 Suppose $\mathcal{S} = (D, +, *)$ is a semifield of order q^n, with center $K = GF(q)$. Let d be a non-zero element in $\mathcal{S}$ and $f(x)$ be its right characteristic polynomial. Then d is a right primitive element if and only if $ord(f(x)) = q^n - 1$.

With this result, we show that

Theorem 2.3.1 The classical Knuth binary semifields of order 2^t, where $t = 15, 17, 19$, are all left and right primitive.

Theorem 2.4.3 For any odd integer $t \in [5, 19]$, if the classical Knuth binary semifield $\mathcal{F}$=$(GF(2^t), +, *)$ is primitive, then the number of primitive elements, N_t of $\mathcal{F}$, is a multiple of t.

Theorem 2.5.1 The Albert Semifields $A_n(S)$ of order 2^n, where $n = 7, 9, 11, 13$, are all right and left primitive.

On Chapter III we provide the results of our study of the dimension of certain finite semifields. In particular, we prove the following theorems.

Corollary 3.2.1 The generalized Knuth binary semifields of order 2^r, for any odd integer $r \in [5, 31]$, contains $GF(4)$. Hence these semifields are fractional dimensional.

Theorem 3.3.1 The classical Knuth binary semifields do not contain any subsemifields.

The generalized Knuth binary semifields and the classical Knuth binary semifields are isotopic, (Lemma 3.3.3), so by Albert's Theorem [1], they coordinatize isomorphic planes. The above two theorems provide evidence that **isomorphic semifield planes may have different coordinatizing theorem**.

Definition 1.1.2. *Let π_1 and π_2 be two isomorphic projective planes with bijection α. Let $\pi_0^{(1)}$ be any subplane of π_1. If there exists $\pi_0^{(2)}$ in π_2 of the same order as $\pi_0^{(1)}$ and α preserves incidence in $\pi_0^{(1)}$ and $\pi_0^{(2)}$, then π_1 and π_2 are called absolutely isomorphic.*

As we just point out, there exist semifield planes which are isomorphic but not absolutely isomorphic. However, two isomorphic Desarguesian planes are absolutely isomorphic, since they are coordinatized by finite fields and there exists a unique finite field for each order up to isomorphism. We raise the question **"when are two projective planes absolutely isomorphic?"**.

On Chapter IV we prove some conclusions that follow from our research and we list two open problems concerning non-associative algebras.

Notice: All the semifields and semifield planes considered in this thesis are finite.

1.2 Preliminaries

1.2.1 Projective Planes and Affine Planes

Definition 1.2.1. *A projective plane is a nonempty set π whose elements are called points and a collection of subsets of π called lines satisfying the following:*

(1) Any two distinct points are contained in one and only one line.

(2) The intersection of two distinct lines contain one and only one point.

(3) There exists four points no three of which are contained in the same line.

If P and Q are two distinct points of a projective plane π, then the line containing P and Q will be denoted by PQ. If the point P is contained in the line ℓ, then P is said to be incident with ℓ.

If one line of a projective plane π contains $n+1$ points, then every line of π contains $n+1$ points and every point of π is incident with $n+1$ lines. Furthermore, π contains n^2+n+1 points and n^2+n+1 lines [10]. In this case, π is said to have order n, denoted by $|\pi| = n$.

Definition 1.2.2. *Let π be a projective plane and π' be the incidence structure whose points (lines) are the lines (points) of π and incidence in π' is given by incidence in π, then π' is a projective plane called the dual plane of π.*

The geometric structure obtained from a projective plane by removing one line and all the points on that line is called an affine plane.

Definition 1.2.3. *An affine plane G is a nonempty set of points and lines together with an incidence relation between the points and lines such that*

(1) Any two distinct points are contained in one and only one line.

(2) Given a point P and a line ℓ with $P \notin \ell$, there exists a unique line m with $P \in m$ and $\ell \cap m = \emptyset$.

(3) There are three points not on the same line

Two lines of an affine plane are parallel if they are equal or if they do not intersect. Parallelism of lines of an affine plane is an equivalence relation; the equivalence classes are called parallel classes.

If an affine plane G is obtained from a projective plane π by deleting a line ℓ of π and all the points of ℓ, then G will be denoted by π_ℓ. Conversely, a projective plane can be obtained from an affine plane G by adjoining an additional point to each parallel class such that the lines of that parallel class intersect in the new point, and adjoining an additional line, denoted by ℓ_∞, consisting precisely of the new points. The projective plane obtained from G in this way will be denoted by $G \cup \ell_\infty$. The extension of an affine plane to a projective plane is unique, but the affine plane obtained from a projective plane by removing a line is not necessarily unique.

The affine plane G is said to have order n, denoted by $|G| = n$, if one (and hence every) line of G has n points.

Coordinates can be introduced in a projective plane π of order n as follows. Choose four points U, V, O, I of π, no three of which are collinear. Let R be a set of n symbols with the two properties:

(1) $0, 1 \in R$;

(2) There exists a 1-1 correspondence α between R and the points in $OI - (UV \cap OI)$ such that $0\alpha = O$ and $1\alpha = I$.

Using the set R, the plane π is coordinatized as follows. (See Figure 1.1)

(a) To a point $P \in OI - (UV \cap OI)$, assign the coordinates (a, a), where $a \in R$ and $a\alpha = P$.

(b) If $P \notin OI$ and $P \notin UV$, assign to P the coordinates (a, b), where $PV \cap OI = (a, a)$ and $PU \cap OI = (b, b)$.

(c) If $P \in UV$ and $P \neq V$, assign to P the coordinates (m), where $OP \cap IV = (1, m)$.

(d) If $P = V$, assign to to P the coordinate (∞), where ∞ is a symbol not in R.

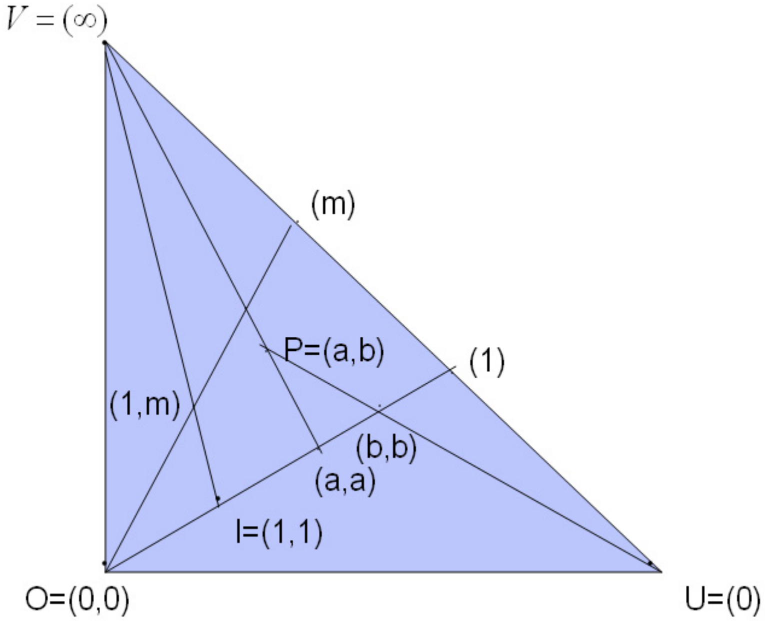

Figure 1.1. Coordinatization of the projective plane π.

Definition 1.2.4. *Let π be a projective plane and R be a set coordinatizing π with respect to the points U, V, O, I. A ternary function F is defined on R as follows:*

if $a, m, k \in R$, $F(a,m,k) = 2^{nd}$ coordinate of the point $(a,0) \cap (m)(0,k)$.

See Figure 1.2.

In terms of the ternary function F, observe that the lines of π, except UV, can be represented by equations as follows:

$$\textit{the line through } (\infty) \textit{ and } (k,0): \; x = k$$

$$\textit{the line through } (m) \textit{ and } (0,k): \; y = F(x,m,k)$$

where x represents the first coordinate and y the second coordinate of a point.

Using the ternary function F, addition and multiplication can be introduced on the coordinate set R as follows:

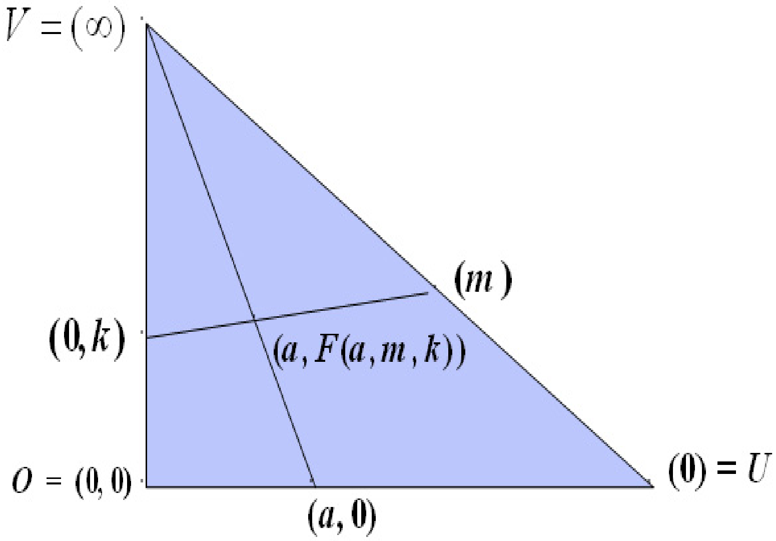

Figure 1.2. Ternary Function.

Definition 1.2.5. *Let π be a projective plane, R be a set coordinatizing π with respect to U, V, O, I, and F the ternary function defined on R. An addition $+$ and a multiplication $\cdot$ are defined on R by*

$$a + b \equiv F(a, 1, b), a \cdot b = ab \equiv F(a, b, 0)$$

for all $a, b \in R$.

The algebraic system on the coordinate set R with operations determined by the ternary function F as above is called a ternary ring and is denoted by $(F, +, \cdot)$ or (R, F).

Definition 1.2.6. *A loop is a set L with a binary operation $*$ satisfying*

(1) There exists an element $e \in L$ such that $a * e = e * a = a$ for all $a \in L$.

(2) Given two of the elements $a, b, c \in L$, the equation $a * b = c$ uniquely determines the third.

Theorem 1.2.1. *[10] If (R, F) is a ternary ring, then $(R, +)$ is a loop with identity 0, and $(R - \{0\}, \cdot)$ is a loop with identity 1.*

We study right quasifields and translation planes.

Definition 1.2.7. *Let Q be a finite set with two binary operations $+$ and $\cdot$ satisfying the following condition:*

(1) $(Q, +)$ is an abelian group with identity 0.

(2) $(Q - \{0\}, \cdot)$ is a loop with identity 1.

(3) For all $a, b, c \in Q$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

(4) For all $a \in Q$, $a \cdot 0 = 0 \cdot a = 0$.

Define a ternary function on the set Q by

(5) For all $a, b, c \in Q$, $F(a, b, c) = a \cdot b + c$.

The quadruple $(Q, F, +, \cdot)$ is called a right quasifield and will be denoted by $(Q, +, \cdot)$

A left quasifield is defined as above by replacing (3) *by* (3′)

(3′) *For all $a, b, c \in Q$, $a \odot (b + c) = a \odot c + a \odot c$*

Definition 1.2.8. *Let π_1 and π_2 be two projective planes (or affine planes). If there exists a bijection α which maps the points of π_1 onto the points of π_2 and the lines of π_1 onto the lines of π_2 and which preserves incidence, then π_1 and π_2 are said to be isomorphic, denoted by $\pi_1 \cong \pi_2$.*

An isomorphism of a plane into itself is called a collineation.

If a collineation α of a projective plane π fixes all the points on a line ℓ and all the lines through a point P of π, then α is called a (P, ℓ)-perspectivity. The point P is called the center of α and ℓ is called the axis. If $P \in \ell$, α is called an elation; if $P \notin \ell$, α is called an homology. The set of all elations of π with a fixed axis ℓ form a group. If this group is transitive on all the points of π not on ℓ, then π is called a translation plane with axis ℓ and the affine plane π_ℓ is called a translation plane. Translation planes are coordinatized by right quasifields.

If the collineation group of a projective plane π contains (P, ℓ)-perspectivities for all points P and all lines ℓ, then π is called a Desarguesian plane. Notice that, all desarguesian planes are coordinatized by finite fields.

1.2.2 Finite Semifields

(I) Basic Results on Semifields

Definition 1.2.9. *A finite semifield $\mathcal{S} = (D, +, *)$ is a finite algebraic system containing at least two elements, which possesses two binary operations, $+$ and $*$ such that*

(1) $(D, +)$ is a group with identity 0.

(2) For every $a, b \in D$, if $a * b = 0$, then either $a = 0$ or $b = 0$.

(3) $a * (b + c) = a * b + a * c$; $(a + b) * c = a * c + b * c$ for every $a, b, c \in D$.

(4) There exists an element 1 in $\mathcal{S}$ such that $1 * a = a * 1 = a$ for every $a \in D$.

Let π be a finite translation plane with axis ℓ_∞. If the group of elations with axis $\ell \neq \ell_\infty$ and center (∞) is transitive on the points of $\ell_\infty - (\infty)$, then π_{ℓ_∞} is called a semifield plane.

If condition (4) is missing, the algebraic system is called a pre-semifield.

If there are n elements in $\mathcal{S}$, then we say the order of $\mathcal{S}$ is n, denoted $|\mathcal{S}| = n$.

Remark 1.2.1. *(1) Every finite field is a semifield.*

(2) The term "proper semifield" refer to a semifield in which the associative law does not hold, i.e., there exist elements $a, b, c \in \mathcal{S}$, such that $(a * b) * c \neq a * (b * c)$.

(3) $(D - \{0\}, *)$ is a loop.

The multiplicative identity 1 does not necessarily exist in a pre-semifield, and the following theorem provides a technique to convert a pre-semifield into a semifield.

Theorem 1.2.2. *[7] Let $\mathcal{P} = (D, +, \circ)$ be a pre-semifield without identity, and let $0 \neq e \in D$. If a new multiplication $*$ is defined on D by the rule*

$$a * b = (a' \circ e) * (e \circ b') = a' \circ b'$$

then with this multiplication $*$ and the given addition, a semifield $(D, +, *)$ is obtained with identity $e \circ e$.

Notice: if $\circ$ is commutative, so is $*$.

Definition 1.2.10. *Let $(T, +, *)$ and $(T_1, +, \cdot)$ be two ternary rings. An* <u>*isotopism*</u> *from T_1 onto T is a set of three functions (F, G, H), each being a 1-1 correspondence from T_1 to T, such that*

$$(0)H = 0,$$
$$(a * b + c)H = (aF) \cdot (bG) + (cH), \ \ for \ all \ a, b, c \in T.$$

In particular, let $S_1 = (D_1, +, *)$ and $S_2 = (D_2, +, \cdot)$ be two finite semifields. If the triple (F, G, H) consists of additive, 1-1 correspondence mappings from D_1 to D_2, such that

$$for \ any \ x, y \in D_1, \ (xF) \cdot (yG) = (x * y)H$$

then S_1 and S_2 are said to be <u>*isotopic*</u> *and the triple (F, G, H) is called an* <u>*isotopism*</u>*.*

We prove two lemmas that will be used in the future.

Lemma 1.2.1. *The semifield $\mathcal{S} = (D, +, *)$ and pre-semifield $\mathcal{P} = (D, +, \circ)$ in Theorem 1.2.2 are isotopic.*

Proof. Define $R_e : D \longrightarrow D$, $x \mapsto x \circ e$ and $L_e : D \longrightarrow D$, $x \mapsto e \circ x$. Since $(D - \{0\}, \circ)$ is a loop and the two distributive laws hold in $\mathcal{P}$, R_e and L_e are additive bijections. So are R_e^{-1} and L_e^{-1}. Also,

$$a * b = (a' \circ e) * (e \circ b') = a' \circ b' = (aR_e^{-1}) \circ (bL_e^{-1})$$

Hence $\mathcal{S}$ and $\mathcal{P}$ are isotopic with isotopism (R_e^{-1}, L_e^{-1}, I). □

Lemma 1.2.2. *Isotopism of ternary rings is an equivalence relation.*

Proof. T is isotopic to itself, since the triple (F, G, H) can be chosen to be (I, I, I), where I is the identity map of T.

Let T_1 and T_2 be two isotopic ternary rings with isotopism (F, G, H). Since F, G, H are bijective, F^{-1}, G^{-1}, H^{-1} exist and they are bijections. Also, $(0_{T_1})H = 0_{T_2}$ implies $(0_{T_2})H^{-1} = 0_{T_1}$ and for any $x, y, z \in T_2$, there exist elements $a, b, c \in T_1$ such that

$$x = aF,\ \ y = bG,\ \ z = cH$$

Then

$$\begin{aligned}(x \cdot y + z)H^{-1} &= [(aF) \cdot (bG) + cH]H^{-1} = [(a \cdot b)H + cH]H^{-1} \\ &= a \cdot b + c = (xF^{-1}) \cdot (yG^{-1}) + zH^{-1}\end{aligned}$$

So T_2 is isotopic to T_1 with isotopism (F^{-1}, G^{-1}, H^{-1}).

Let T_1 be isotopic to T_2 with isotopism (F, G, H) and T_2 be isotopic to T_3 with isotopism (P, Q, R), then FR, GQ, HR are bijections from T_1 to T_3. For any $a, b, c \in T_1$

$$\begin{aligned}(0_{T_1})(HR) &= (0_{T_1}H)R = (0_{T_2})R = 0_{T_3}, \\ (a \cdot b + c)(HR) &= (aF \cdot bG + cH)R = (aF)P \cdot (bG)Q + (cH)R \\ &= aFP \cdot bGQ + cHR\end{aligned}$$

So T_1 is isotopic to T_3 with isotopism (FR, GQ, HR). □

The importance of isotopisms on semifields is given by the following theorem due to Albert.

Theorem 1.2.3. *[1] Two semifields coordinatize isomorphic planes if and only if they are isotopic.*

(II) Nuclei

Various special subsystems are defined for a semifield $\mathcal{S} = (D, +, *)$, indicating degrees of associativity. The most important of these are the following:

$$\begin{array}{ll} the\ left\ nucleus\ N_l : & \{x \in D | (x * a) * b = x * (a * b),\ for\ all\ a,\ b\ \in D\}, \\ the\ middle\ nucleus\ N_m : & \{x \in D | (a * x) * b = a * (x * b),\ for\ all\ a,\ b\ \in D\}, \\ the\ right\ nucleus\ N_r : & \{x \in D | (a * b) * x = a * (b * x),\ for\ all\ a,\ b\ \in D\}. \end{array}$$

The intersection of these three sets is called the nucleus of the semifield $\mathcal{S}$ and is denoted by N; Knuth [11] showed that each nuclei is a finite field and $\mathcal{S}$ is a vector space over any of its nuclei; it is a left vector space over N_l, N_m and N; it is a right vector space over N_m, N_r and N.

The center of a finite semifield is a set formed by all the elements in N that commute with all the elements in D, denoted by $K = Z(D)$, i.e.,

$$K = \{x \in N | a * x = x * a,\ for\ all\ a \in D\}$$

Obviously, the center of a finite semifield with addition and multiplication forms a finite field. Let $K = GF(q)$, where $q = p^r$, p is the characteristic of D, and $dim_K \mathcal{S} = n$; then $|\mathcal{S}| = q^n$.

In this paper, we consider a finite semifield as a vector space over its center.

(III) Examples of Semifields

(1) Classical Knuth Binary Semifields

First we introduce the construction of the classical binary semifields due to Knuth [12]. Let $F = GF(2^{mn})$ and $F_0 = GF(2^m)$, where m, n are postitive integers and n is odd. Considering F as a vector space over F_0, let f be any nonzero linear functional from F to F_0, i.e.,

$$f(\lambda a + \mu b) = \lambda f(a) + \mu f(b)$$

for all $a, b \in F$ and all $\lambda, \mu \in f_0$.

Define a new multiplication $\circ$ in F as follows:

$$a \circ b = ab + [f(a)b + f(b)a]^2$$

Then $(F, +, \circ)$ is a pre-semifield. Choose a nonzero element e in F and define another multiplication $*$ by

$$x * y = (x' \circ e) * (e \circ y') = x' \circ y', \ \forall x, y \in F$$

then $\mathcal{S} = (F, +, *)$ is a commutative semifield called the classical Knuth binary semifield.

Let $F = GF(2^n)$, $F_0 = GF(2)$, and let T be the trace map from F to F_0, i.e.

$$a^T = a + a^2 + a^{2^2} + \cdots + a^{2^{n-1}}$$

for any $a \in F$. Then the multiplication $\circ$ in (1) is defined by

$$(ComKn) \qquad x \circ y = xy + (x^T y + y^T x)^2$$

Then the multiplication of pre-semifield $(F, +, \circ)$ can be redefined to get a semifield $(F, +, *)$ using Theorem 1.2.2.

(2) Generalized Knuth Binary Semifield

V. Jha and N.L. Johnson [9] generalized the construction of the classical Knuth binary semifields in 2010 as follows:

Let $F = GF(2^n)$, $n \geq 5$ odd, and $F_0 = GF(2)$. Suppose $GL(F, +)$ is the full group of F_0-linear bijections of the vector space F over F_0. Then for any $B, C \in$

$GL(F,+)$, there corresponds a pre-semifield $\mathcal{F}_{B,C}(F) = (F,+,\odot)$, where $\odot$ is defined by

$$(GenKn) \qquad x \odot y = x^B y^C + (x^{BT} y^C + y^{CT} x^B)^2$$

For any choice of $e \in F^*$, redefine the multiplication of the pre-semifield $\mathcal{F}_{B,C}(F) = (F,+,\odot)$ by the following rule

$$(x \odot e) * (e \odot y) = x \odot y, \qquad\qquad \forall\ x,\ y \in F$$

$\mathcal{F}^{(e)}_{B,C}(F) = (F,+,*)_e$ forms a semifield, called a generalized Knuth binary semifield. Notice that $e \odot e$ is the multiplicative identity for $(F,+,*)_e$.

The following proposition is given in [9] without proof; for completeness we provide a proof here.

Proposition 1.2.1. *Let $F = GF(2^n)$, $n \geq 5$ odd. With the addition inherited from the finite field and the multiplication $\odot$ defined above, $(F,+,\odot)$ is a pre-semifield when $B, C \in GL(F,+)$.*

Proof. First, we show there are no zero divisors for $\odot$.

Suppose $x \odot y = 0$ and $x \neq 0$. Then $x^B \neq 0$ since $B \in GF(F,+)$ is a bijection over F and

$$x^B y^C + x^{BT}(y^C)^2 + y^{CT}(x^B)^2 = 0$$

Dividing by $(x^B)^2$ in both sides, we get

$$x^{BT}(\frac{y^C}{x^B})^2 + \frac{y^C}{x^B} + y^{CT} = 0$$

Let $z = \dfrac{y^C}{x^B}$. Then the above equality becomes $x^{BT}z^2 + z + y^{CT} = 0$. Since n is odd, this equation must be reducible, which implies $z \in GF(2)$. Hence

$$x \odot y = x^B y^C + (x^{BT} z x^B + z x^{BT} x^B)^2 = x^B y^C = 0$$

So $y^C = 0$ and then $y = 0$.

Next we show the left distributive law holds in $\mathcal{F}_{B,C}(F)$ and similarly the right distributive law also holds.

Since B, C are additive bijections on F and $T : GF(2^n) \to GF(2)$, n odd, is also additive,

$$\begin{aligned}
x \odot (y+z) &= x^B(y+z)^C + [x^{BT}(y+z)^C + (y+z)^{CT}x^B]^2 \\
&= x^B(y^C+z^C) + [x^{BT}(y^C+z^C) + (y^{CT}+z^{CT})x^B]^2 \\
&= x^By^C + x^Bz^C + x^{BT}(y^C)^2 + x^{BT}(z^C)^2 + y^{CT}(x^B)^2 + z^{CT}(x^B)^2 \\
&= x \odot y + x \odot z
\end{aligned}$$

□

(3) Albert Semifields

This is a class of finite semifields with characteristic 2 due to Albert [17]. He simplified the construction of Knuth for the classical binary semifields. Here is Albert's idea:

Let $F = GF(2^n)$, $n \geq 3$ odd, with multiplication juxtaposition and write $F = S + \omega GF(2)$, where S is a $(n-1)$-dimensional vector space over $GF(2)$ containing 1 and ω is an element not in S. Define

$$s * t = st, s * \omega = \omega * s = s\omega + s^2 + s, \omega * \omega = \omega^2 + 1$$

for any $s, t \in S$. Then the vector space F with multiplication $*$ forms a proper semifield when $n \geq 5$. Wene [17] proved the following theorem.

Theorem 1.2.4. *[17] Let $F = S + \omega GF(2)$, where S is a $(n-1)$-dimensional vector space over $GF(2)$ containing 1. Suppose $\bar{\omega} = \omega + s_0$ for some s_0 in S. Define*

$$s * t = st, s * \bar{\omega} = \bar{\omega} * s = s\bar{\omega} + s^2 + s, \bar{\omega} * \bar{\omega} = \bar{\omega}^2 + 1$$

for any $s, t \in S$. The resulting semifields are isomorphic for all $s_0 \in S$.

The Albert semifield of order 2^n, where $n \geq 5$ is odd, is denoted $A_n(S)$ in this work.

CHAPTER 2

PRIMITIVITY IN FINITE SEMIFIELDS

2.1 Preliminaries

In this section, we are concerned with some basic but helpful tools for the study of primitivity in semifields. Let $\mathcal{S} = (D, +, *)$ be a finite semifield and K be its center, where $K \cong GF(q)$ and q is a prime power. Recall $\mathcal{S}$ is a vector space over K. Suppose $dim_K\mathcal{S} = n$. The slope map of any non-zero element $d \in D$ is T_d, specified by $T_d(x) = x * d$. Since T_d is a non-singular linear transformation on D, it can be identified with a non-singular $n \times n$ K-matrix, which depends on the choice of the basis of $\mathcal{S}$ over K. Also the slope set for $\mathcal{S}$ is denoted by $\tau_D = \{T_d | d \in D\}$, where T_0 is the zero map.

Definition 2.1.1. *Let V be a vector space over a finite field $K \cong GF(q)$, $q = p^r$, with finite dimension n, i.e. $dim_K V = n$. Then a set of linear maps*

$$\tau \subseteq GL(n, K) \cup \{0_n\} := \overline{GL(n, K)}$$

is a spread set on V if

$$|\tau| = |V| = q^n, \ \tau \supset \{0_n, 1_n\}, \ and \ \ A, \ B \in \tau \Rightarrow A - B \in GL(n, K)$$

Definition 2.1.2. *We say that the set τ is additive if it is closed under addition.*

Proposition 2.1.1. *If $\mathcal{S}$ is a semifield, then the slope set τ_D defined above is an additive spread set of $\mathcal{S}$, which is also a vector space over K.*

Proof. We first show $|\tau_D| = |\mathcal{S}| = q^n$. First notice that

$$T_m = T_n \Leftrightarrow xT_m = xT_n \Leftrightarrow x * m = x * n, \ for \ every \ x \in S$$

When $x = 1$, we conclude $m = n$.

The mapping $\mathcal{S} \to \tau_D$ that maps $d \in S$ into $T_d \in \tau_D$, is $1-1$; hence onto. Therefore $|\tau_D| = |\mathcal{S}| = q^n$. For any $T_m,\ T_n \in \tau_D$,

$$x(T_m - T_n) = xT_m - xT_n = x * m - x * n = x * (m - n)$$

so $T_m - T_n = T_{m-n} \in \tau_D$. Since $T_0, T_1 \in \tau_D$, the conclusion holds. □

Suppose $\mathcal{S}$ is a vector space over its center K with basis $\{\varepsilon_1 = 1, \varepsilon_2, \cdots, \varepsilon_n\}$. Then all the elements of S are linear combinations of $\{\varepsilon_1 = 1, \varepsilon_2, \cdots, \varepsilon_n\}$. The additive spread set of $\mathcal{S}$, τ_D, is a vector space over K according to Remark 2.3 [6]. Hence τ_D and $\mathcal{S}$ are isomorphic as vector spaces over K. Therefore $\{T_1, T_{\varepsilon_2}, \cdots, T_{\varepsilon_n}\}$ is a K-basis of τ_D.

Definition 2.1.3. *The $n \times n$ matrix associated with T_d is called the right slope matrix of d and is denoted R_d.*

Remark 2.1.1.

(1) R_d is nonsingular, and so $\det(R_d) \neq 0$.

(2) Knuth [11] introduced two isotopism classes of semifields with 16 elements: system V and system W. Let $F = GF(4)$, so that F has elements $0, 1, \omega, \omega^2 = 1 + \omega$. The elements of system V are of the form $u + \lambda v$, where $u, v \in F$. Addition is defined in an obvious way:

$$(u + \lambda v) + (x + \lambda y) = (u + x) + \lambda(v + y) \tag{2.1}$$

Multiplication is defined by the following rule

$$(u + \lambda v)(x + \lambda y) = (ux + v^2 y) + \lambda(vx + u^2 y + v^2 y^2) \tag{2.2}$$

The set of all the elements in F with addition (2.1) and multiplication (2.2) form a semifield, called system V.

The elements in system W are the same as the elements in system V. But the multiplication in W, defined below (2.3), is different from the multiplication in system V.

$$(u+\lambda v)(x+\lambda y) = (ux+\omega v^2 y) + \lambda(vx+u^2 y) \tag{2.3}$$

By Proposition 2.1.1, since τ_D is an additive spread set, it is closed under addition. Wene [16] proved that system V and system W are both right primitive. In his proof, two special matrices $M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ were used. The characteristic polynomials of M_1 and M_2 are x^4+x+1 and x^4+x^3+1 respectively, which are both irreducible over $GF(2)$ of order 15 by Corollary 3.4 [13].

However, since $\{1, \omega, \lambda, \lambda\omega\}$ is an ordered basis of system V or system W over $GF(2)$, then the set $\{R_1, R_\omega, R_\lambda, R_{\lambda\omega}\}$ is an ordered basis of τ_D over $GF(2)$; so all the slope matrices should be a linear combination of them. But neither M_1 nor M_2 is, which implies there does not exist an element in $\mathcal{S} = (D, +, *)$ with M_1 or M_2 as the right slope matrix.

By Theorem 2.2.2, we found all the right primitive elements in Knuth's system V and system W. In system V, the elements $\omega+\lambda$, $\omega+\lambda\omega$, $1+\omega+\lambda$, $1+\omega+\lambda\omega$, $\omega+\lambda+\lambda\omega$, and $1+\omega+\lambda+\lambda\omega$, have right slope matrices as follows:

$$R_{\omega+\lambda} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad R_{\omega+\lambda\omega} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$R_{1+\omega+\lambda} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \qquad R_{1+\omega+\lambda\omega} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$R_{\omega+\lambda+\lambda\omega} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \quad R_{1+\omega+\lambda+\lambda\omega} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

All the matrices above have right characteristic polynomial $x^4 + x + 1$, which has order 15. So system V has 6 right primitive elements.

Applying the same method we found that system W has 6 right primitive elements too, which are also $\omega + \lambda$, $\omega + \lambda\omega$, $1 + \omega + \lambda$, $1 + \omega + \lambda\omega$, $\omega + \lambda + \lambda\omega$, and $1 + \omega + \lambda + \lambda\omega$.

Before our main results, we list all the theorems and lemmas that are needed in our research.

Result 2.1.1. *(Lemma 3.6, [13]) Let c be a positive integer. Then the polynomial $f \in GF(q)[x]$ with $f(0) \neq 0$ divides $x^c - 1$ if and only if $ord(f)$ divides c.*

Result 2.1.2. *(Theorem 3.8, [13]) Let $g \in GF(q)[x]$ be irreducible over $GF(q)$ with $g(0) \neq 0$ and $ord(g) = e$, and let $f = g^b$ with a positive integer b. Let t be the smallest integer with $p^e \geq b$, where p is the characteristic of F_q. Then $ord(f) = ep^t$.*

Result 2.1.3. *(Theorem 3.9, [13]) Let $g_1, \cdots, g_k$ be pairwise relatively prime nonzero polynomials over $GF(q)$, and let $f = g_1 g_2 \cdots g_k$. Then $ord(f)$ is equal to the least common multiple of $ord(g_1), \cdots, ord(g_k)$, i.e., $ord(f) = [ord(g_1), \cdots, ord(g_k)]$.*

Result 2.1.4. *(Theorem 3.11, [13]) Let $GF(q)$ be a finite field of characteristic p, and let $f \in GF(q)[x]$ be a polynomial of positive degree with $f(0) \neq 0$. Let $f = af_1^{b_1} \cdots f_k^{b_k}$, where $a \in GF(q)$, $b_1, b_2, \cdots, b_k \in N$, and $f_1, \cdots, f_k$ are distinct monic irreducible polynomials in $GF(q)[x]$ be the canonical factorization of f in $GF(q)[x]$. Then $ord(f) = ep^t$, where $e = [ord(f_1), \cdots, ord(f_k)]$ and t is the smallest integer with $p^t \geq$max($b_1, \cdots, b_k$).*

Result 2.1.5. *(Lemma 1, [15]) Let $Z(D) = GF(p^c)$ be the center of a finite semifield D and let $\omega \in D^*$ such that*

$$\omega^{r)} = \lambda_{r-1}\omega^{r-1)} + \cdots + \lambda_1\omega + \lambda_0 e$$

for some $\lambda_0, \cdots, \lambda_{r-1} \in GF(p^c)$. If $t \in N$ is the order of the polynomial $p(x) = x^r - \lambda_{r-1}x^{r-1} - \cdots - \lambda_1 x - \lambda_0 \in GF(p^c)[x]$, i.e., the smallest natural number such that $p(x)|(x^t - e)$, then the element ω satisfies the equation $\omega^{t)} = e$.

Result 2.1.6. *(Lemma 3.1, [13]) If $f(x) \in GF(q)[x]$ is a polynomial of degree $n \geq 1$ with $f(0) \neq 0$, then there exists a positive integer $e \leq q^n - 1$, such that $f(x)|x^e - 1$.*

The following well-known fact is used in the proof of the main result of this chapter; we include a proof for completeness.

Lemma 2.1.1. *Suppose p is a prime number. Then $(p^{n_1} - 1)(p^{n_2} - 1) \cdots (p^{n_t} - 1) < p^{n_1 + \cdots + n_t} - 1$, where all the $n_i's$ are positive integers and $t > 1$.*

Proof. Induction is applied to prove this result. First,

$$\begin{aligned}(p^{n_1} - 1)(p^{n_2} - 1) &= p^{n_1+n_2} - p^{n_1} - p^{n_2} + 1 \\ &= p^{n_1+n_2} - 1 - p^{n_1} - p^{n_2} + 2\end{aligned}$$

Let $\Delta = -p^{n_1} - p^{n_2} + 2$. Since p is a prime number, and $n_i \geq 1$, then

$$p^{n_1} + p^{n_2} \geq 2^1 + 2^1 = 4 > 2$$

Therefore $\Delta < 0$ and $(p^{n_1} - 1)(p^{n_2} - 1) < p^{n_1+n_2} - 1$.

Second, suppose $(p^{n_1} - 1)(p^{n_2} - 1) \cdots (p^{n_k} - 1) < p^{n_1+\cdots+n_k} - 1$. Then

$$\begin{aligned}&(p^{n_1} - 1) \cdots (p^{n_k} - 1)(p^{n_{k+1}} - 1) \\ &< (p^{n_1+\cdots+n_k} - 1)(p^{n_{k+1}} - 1) \\ &= p^{n_1+\cdots+n_k+n_{k+1}} - p^{n_1+\cdots+n_k} - p^{n_{k+1}} + 1 \\ &= p^{n_1+\cdots+n_k+n_{k+1}} - 1 - p^{n_1+\cdots+n_k} - p^{n_{k+1}} + 2\end{aligned}$$

Let $\Delta = -p^{n_1+\cdots+n_k} - p^{n_{k+1}} + 2$. Then $\Delta < 0$ and

$$(p^{n_1} - 1)\cdots(p^{n_k} - 1)(p^{n_{k+1}} - 1) < p^{n_1+\cdots+n_k+n_{k+1}} - 1$$

□

2.2 Equivalent Condition for Right Primitivity

Let $\mathcal{S} = (\mathcal{D}, +, *)$ be a finite semifield with order q^n. The element $\omega \in \mathcal{S}$ is said to be a right (left) primitive element of $\mathcal{S}$ if each element in D^* can be represented as some right (left) power of ω. Note:

$$\omega^{1)} = \omega,\ \omega^{2)} = \omega * \omega, \cdots, \omega^{n)} = \omega^{n-1)} * \omega$$

$$(\omega^{(1} = \omega,\ \omega^{(2} = \omega * \omega, \cdots, \omega^{(n} = \omega * \omega^{(n-1})$$

If $K = Z(D)$, the center of $\mathcal{S}$, has order q, then $\mathcal{S}$ is right primitive if and only if there exists at least one element $\omega \in \mathcal{S}$ such that $\omega^{q^n-1)} = 1$, where $q^n - 1$ is the least positive integer satisfying the above condition. We also say $\mathcal{S}$ is primitive if $\mathcal{S}$ is right and left primitive.

Theorem 2.2.1. *Let $d \in \mathcal{S}$. Then*

$$a_0 + a_1 d + a_2 d^{2)} + \cdots + a_n d^{n)} = 0,\ a_i \in K$$

if and only if

$$a_0 I_n + a_1 R_d + a_2 R_d^2 + \cdots + a_n R_d^n = 0,\ a_i \in K$$

where R_d is the right slope matrix of d.

Proof. First we show $ad^{k)} = aR_d^k$, $a \in K,\ d \in D$, for all positive integers k.
If $k = 1$, $ad = a * d = T_d(a) = aR_d$. Suppose $ad^{i)} = aR_d^i$, for some $i > 1$. Then

$$ad^{i+1)} = a * d^{i+1)} = a * \left(d^{i)} * d\right) = (a * d^{i)}) * d = (aR_d^i) * d = (aR_d^i)R_d = aR_d^{i+1}.$$

Hence,

$$a_0 + a_1 d + a_2 d^{2)} + \cdots + a_n d^{n)} = 0 \Leftrightarrow a_0 I_n + a_1 R_d + a_2 R_d^2 + \cdots + a_n R_d^n = 0$$

$\square$

Note: If $a_0 + a_1 d + a_2 d^{2)} + \cdots + a_n d^{n)} = 0,\ a_i \in K$, we say that d is a right root of $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0,\ a_i \in K$.

Remark 2.2.1. *When Theorem 2.2.1 is applied, the semifield $\mathcal{S}$ must be considered as a vector space over its center; otherwise it is not necessarily true.*

For example, let $K = GF(3)$. In [18] Jha-Cordero observed that the semifield $D_N = (K^5, +, *)$ has an ordered basis $\{E_1, E_2, E_3, E_4, E_5\}$ over K, where

$$E_1 = (0,0,0,1,0), E_2 = (1,1,2,0,1), E_3 = (0,0,0,0,2),$$
$$E_4 = (0,1,0,2,0), E_5 = (2,2,0,1,1)$$

Let $d = E_2$ and M denote the slope map of d in the semifield $D_N = (K^5, +, *)$. Then $M = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 1 & 2 & 0 & 2 & 2 \\ 1 & 1 & 2 & 0 & 1 \\ 2 & 2 & 2 & 1 & 0 \end{pmatrix}$. *Obviously, $2d^{3)} + 2d^{4)} + d^{5)} = 0$, but $2M^3 + 2M^4 + M^5 \neq 0$.*

Theorem 2.2.1 is not true for this example, since K is not the center of the semifield D_N and then $\{E_1, E_2, E_3, E_4, E_5\}$ is not a basis over its center. In D_N, $E_3 = (0,0,0,0,2)$, is not in the center, because $E_2 * E_3 \neq E_3 * E_2$. Here is a copy of the table of the multiplication in D_N as given in [18].

*	E_1	E_2	E_3	E_4	E_5
E_1	*3*	*127*	*2*	*33*	*220*
E_2	*127*	*130*	*37*	*168*	*207*
E_3	*2*	*123*	*50*	*154*	*27*
E_4	*33*	*175*	*97*	*2*	*64*
E_5	*220*	*70*	*64*	*55*	*2*

Corollary 2.2.1. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, $a_i \in K$, be the characteristic polynomial of R_d. Then d is a right root of f; that is,*

$$d^{n)} + a_{n-1}d^{n-1)} + \cdots + a_1d + a_0 = 0$$

Proof. Since $f(x)$ is the characteristic polynomial of R_d, then R_d is a root of $f(x)$. i.e.,

$$R_d^n + a_{n-1}R_d^{n-1} + \cdots + a_1R_d + a_0I_n = 0$$

The result is easily obtained from Theorem 2.2.1. □

Definition 2.2.1. *The characteristic polynomial of R_d is called the right characteristic polynomial of d.*

Remark 2.2.2. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be the right characteristic polynomial of $d \in \mathcal{S}$. Suppose f is reducible over $K = Z(D)$; say $f(x) = f_1(x)f_2(x)$, where*

$$f_1(x) = x^m + \sum_{i=0}^{m-1} b_ix^i, \;\; f_2(x) = x^k + \sum_{i=0}^{k-1} c_ix^i$$

$m, k > 0$, and $m + k = n$. By Corollary 2.2.1, $d^{n)} + a_{n-1}d^{n-1)} + \cdots + a_1d + a_0 = 0$. However, it is possible for d not to be a right root of either factor, as the following example shows.

Example 2.2.1. *In system W, the right characteristic polynomial of λ is x^4+x^2+1; so $\lambda^{4)}+\lambda^{2)}+1 = 0$. Over $GF(2)$ we have $x^4+x^2+1 = (x^2+x+1)^2$, but $\lambda^{2)}+\lambda+1 = \omega + \lambda + 1 \neq 0$.*

Note: $f(d))$ equals $f_1(d))f_2(d))$ if and only if d associates with every element in S; so most often $f(d)) \neq f_1(d))f_2(d))$.

Lemma 2.2.1. *Let $f(x)$ be the right characteristic polynomial of $d \in D^*$ over $K = GF(q)$. Then $ord(f(x)) \leq q^n - 1$.*

Proof. $f(x)$ is a polynomial over K with degree n, and $f(0) \neq 0$, since $f(0) = \det(-R_d)$ and R_d is nonsingular. By Result 2.1.6 and the definition of order we get $ord(f(x)) \leq q^n - 1$. □

Now we give the main result of this chapter.

Theorem 2.2.2. *Suppose $\mathcal{S} = (D, +, *)$ is a semifield of order q^n, with center $K = GF(q)$. Let d be a non-zero element in $\mathcal{S}$ and $f(x)$ be its right characteristic polynomial. Then d is a right primitive element if and only if $ord(f(x)) = q^n - 1$.*

Proof. The proof follows from the following three lemmas. □

Lemma 2.2.2. *Let $f(x)$ be the right characteristic polynomial of $d \in D^*$. Suppose f is irreducible over K. If $ord(f(x)) = q^n - 1$, d is a right primitive element; if $ord(f(x)) < q^n - 1$, d is not a primitive element.*

Proof. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,\ a_i \in K$. Then

$$R_d^n + a_{n-1}R_d^{n-1} + \cdots + a_1R_d + a_0I_n = 0$$

i.e., R_d is a root of $f(x)$. By Theorem 2.2.1, $d^{n)} + a_{n-1}d^{n-1)} + \cdots + a_1d + a_0 = 0$. If $ord(f(x)) = q^n - 1$, by Result 2.1.5, $d^{q^n-1)} = 1$.

In order to show d is a right primitive element, we also need to show $d^{i)} \neq 1$, for all i such that $0 < i < q^n - 1$.

Suppose $d^{k)} = 1$ for some k, $0 < k < q^n - 1$. Then $d^{k)} - 1 = 0$, and so $R_d^k - I_n = 0$, i.e., R_d is a root of $x^k - 1$. By hypothesis, $f(x)$ is the characteristic polynomial of d, so it is monic and irreducible over K. Hence $f(x)$ is the minimal polynomial of R_d and $f(x)|x^k - 1$. If $ord(f(x)) = q^n - 1$, then by Result 2.1.1, $q^n - 1|k$. But this never happens since $0 < k < q^n - 1$. Therefore, $q^n - 1$ is the least positive integer satisfying $d^{q^n-1)} = 1$; hence d is a right primitive element of $\mathcal{S}$, i.e., $\mathcal{S}$ is right primitive.

If $ord(f(x)) = m < q^n - 1$, then $f(x) | x^m - 1$. Now $d^{n)} + a_{n-1}d^{n-1)} + \cdots + a_1 d + a_0 = 0$ implies $d^{m)} = 1$ by Result 2.1.5. But $m < q^n - 1$, so d can't be a right primitive element of $\mathcal{S}$. □

Notice that if all the nonzero elements of $\mathcal{S}$ have characteristic polynomial with order less that $q^n - 1$, then $\mathcal{S}$ is not right primitive. This argument was used by I.F. Rúa [15], when he showed that the Knuth binary semifield of order 32 is neither right nor left primitive. In the proof he showed that any nonzero element ω of trace 0 satisfy $\omega^{5)} + \omega + 1 = 0$, and any nonzero element ω of trace 1 satisfy $\omega^{5)} + \omega^{4)} + 1 = 0$. The characteristic polynomial of each nonzero element is either $x^5 + x + 1$ or $x^5 + x^4 + 1$; each of them have order 21, which is less than $31(= 2^5 - 1)$.

Lemma 2.2.3. *If $\omega \in D^*$ is a right primitive element of $\mathcal{S}$, then the right characteristic polynomial of ω has order $q^n - 1$.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_i \in K$, be the right characteristic polynomial of ω. Then $f(R_\omega) = 0$, i.e.,

$$R_\omega^n + a_{n-1}R_\omega^{n-1} + \cdots + a_1 R_\omega + a_0 I_n = 0$$

By Theorem 2.2.1,

$$\omega^{n)} + a_{n-1}\omega^{n-1)} + \cdots + a_1\omega + a_0 = 0$$

Let $m = ord(f(x))$, so $\omega^{m)} = 1$. We need to show $m = q^n - 1$. Since ω is a right primitive element of $\mathcal{S}$ we have $q^n - 1$ is the least positive integer such that $\omega^{q^n-1)} = 1$. Hence $m \geq q^n - 1$. But $ord(f(x)) \leq q^n - 1$ according to Lemma 2.1, so $m = q^n - 1$, i.e., $ord(f(x)) = q^n - 1$. □

Lemma 2.2.4. *Let $f(x)$ be the characteristic polynomial of $d \in D^*$, and suppose f is reducible over K, where $K = GF(q) = GF(p^r)$ for some r, and p is the characteristic of $\mathcal{S}$. Then $ord(f(x)) < q^n - 1$.*

Proof. Suppose $f = f_1^{b_1} \cdots f_k^{b_k}$ is the canonical factorization of f over K, where $f_1, \cdots, f_k$ are distinct monic irreducible polynomials in $K[x]$ and $b_i \geq 1$. By Result 2.1.4, $ord(f(x)) = ep^t$, where $e = [ord(f_1), \cdots, ord(f_k)]$, and t is the smallest integer with $p^t \geq max(b_1, \cdots, b_k)$.

Case 1: If there is one b_i greater than 1, then $p^t \geq max(b_1, \cdots, b_k) > 1$ implies $t > 0$. If $ord(f(x)) = q^n - 1$, then $ord(f(x)) = p^{rn} - 1 = ep^t$, so $p|p^{rn} - 1$. This is obviously impossible, so $ord(f(x)) \neq q^n - 1$ and $ord(f(x)) < q^n - 1$ by Lemma 2.1.

Case 2: If all the b_i are 1, then $f(x) = f_1(x)f_2(x) \cdots f_k(x)$, and $\mathrm{ord}(f(x)) = [ord(f_1(x)), \cdots, ord(f_k(x))]$. Suppose $deg(f_i(x)) = n_i$, then $deg(f(x)) = n_1 + n_2 + \cdots + n_k = n$ and

$$\begin{aligned} ord(f(x)) &= [ord(f_1(x)), \cdots, ord(f_k(x))] \\ &\leq [q^{n_1} - 1, \cdots q^{n_k} - 1] \leq (q^{n_1} - 1) \cdots (q^{n_k} - 1) \\ &< q^{n_1 + q_2 + \cdots + n_k} - 1 = q^n - 1. \ (\textit{by Lemma } 2.1.1) \end{aligned}$$

□

Remark 2.2.3. *In [8], Hentzel and Rúa provided a proof of Theorem 2.2.2 using the technique of linear recurring sequences. Also Gow and Sheekey [14] gave a different proof for this result using slope matrices.*

2.3 Primitivity of Classical Knuth Binary Semifields of order 2^{15}, 2^{17}, 2^{19}

Let $F = GF(2^t)$, t odd, with multiplication juxtaposition. The following defines a multiplication for a commutative pre-semifield $(F, +, \circ)$ due to D.E. Knuth [12]. For any $x, y \in F$, define

$$x \circ y = xy + (xy^T + yx^T)^2$$

where $T : GF(2^t) \longrightarrow GF(2)$ is the trace function. Choose a nonzero element e in F and define another multiplication $*$ by

$$x * y = (x' \circ e) * (e \circ y') = x' \circ y', \ \forall x, y \in F.$$

Then $(F, +, *)$ is a commutative semifield called a classical Knuth binary semifield.

Rúa [15] indicated that from his computations it follows that this semifield with $F = GF(2^t)$, $t = 7, 9, 11, 13$ is primitive. We investigate primitivity of the classical Knuth binary semifields of order 2^{15}, 2^{17}, and 2^{19} in this section.

In the following, R_1 represents the mapping $x \to x \circ 1$. Also e is chosen to be 1, the identity of the finite field.

Theorem 2.3.1. *The classical Knuth binary semifields of order* 2^t*, where* $t = 15, 17, 19$*, are left and right primitive.*

Proof. Suppose $f(x)$ is an irreducible polynomial over $GF(2)$ associated with the field extension $GF(2^t)$ over $GF(2)$. Then $\{1, \theta, \cdots, \theta^{t-1}\}$ forms a basis of $GF(2^t)$ over $GF(2)$, where θ is a root of $f(x)$. The set $\{1, \theta, \cdots, \theta^{t-1}\}$ is also a basis of the classical Knuth binary semifield $\mathcal{F} = (GF(2^t), +, *)$ and $\{T_1, T_\theta, \cdots, T_{\theta^{t-1}}\}$ is a basis of the spread set τ_D of $\mathcal{F}$. By Theorem 2.2.2, if there exists an element $d \in \mathcal{F}$, whose right characteristic polynomial has order $2^t - 1$, then $\mathcal{F}$ is primitive. Next we study each of the cases under discussion.

When $t = 15$, choose $f(x) = x^{15} + x + 1$ and let θ be a root of $f(x)$. Then

$$\{1, \theta, \theta^2, \cdots, \theta^{14}\}$$

is a basis of $GF(2^{15})$ over $GF(2)$. By Lemma 1 [2], $(\theta^i)^T = 0$ for all $0 < i < 15$.

First we compute $R_1(\theta^i)$, for $0 \leq i < 15$. Since

$$R_1(\theta^i) = \theta^i \circ 1 = \theta^i + (\theta^i)^2 + (\theta^i)^T$$

we have

$$\begin{aligned}
R_1(1) &= 1\\
R_1(\theta) &= \theta+\theta^2\\
R_1(\theta^2) &= \theta^2+\theta^4\\
R_1(\theta^3) &= \theta^3+\theta^6\\
R_1(\theta^4) &= \theta^4+\theta^8\\
R_1(\theta^5) &= \theta^5+\theta^{10}\\
R_1(\theta^6) &= \theta^6+\theta^{12}\\
R_1(\theta^7) &= \theta^7+\theta^{14}\\
R_1(\theta^8) &= \theta+\theta^2+\theta^8\\
R_1(\theta^9) &= \theta^3+\theta^4+\theta^9\\
R_1(\theta^{10}) &= \theta^5+\theta^6+\theta^{10}\\
R_1(\theta^{11}) &= \theta^7+\theta^8+\theta^{11}\\
R_1(\theta^{12}) &= \theta^9+\theta^{10}+\theta^{12}\\
R_1(\theta^{13}) &= \theta^{11}+\theta^{12}+\theta^{13}\\
R_1(\theta^{14}) &= \theta^{13}
\end{aligned}$$

Second we find $R_1^{-1}(\theta^i)$, for $0 \leq i < 15$. Since $R_1^{-1}(\theta^i)$ is the element such that $R_1^{-1}(\theta^i) \circ 1 = \theta^i$, we have

$$\begin{aligned}
R_1^{-1}(1) &= 1\\
R_1^{-1}(\theta) &= \theta^2+\theta^4+\theta^8\\
R_1^{-1}(\theta^2) &= \theta+\theta^2+\theta^4+\theta^8\\
R_1^{-1}(\theta^3) &= \theta^3+\theta^5+\theta^{10}
\end{aligned}$$

$$
\begin{aligned}
R_1^{-1}(\theta^4) &= \theta + \theta^4 + \theta^8 \\
R_1^{-1}(\theta^5) &= \theta + \theta^3 + \theta^4 + \theta^5 + \theta^6 + \theta^8 + \theta^9 + \theta^{12} \\
R_1^{-1}(\theta^6) &= \theta^5 + \theta^{10} \\
R_1^{-1}(\theta^7) &= \theta + \theta^5 + \theta^6 + \theta^8 + \theta^{10} + \theta^{11} + \theta^{13} + \theta^{14} \\
R_1^{-1}(\theta^8) &= \theta + \theta^8 \\
R_1^{-1}(\theta^9) &= \theta + \theta^3 + \theta^4 + \theta^5 + \theta^8 + \theta^9 + \theta^{10} \\
R_1^{-1}(\theta^{10}) &= \theta + \theta^3 + \theta^4 + \theta^6 + \theta^8 + \theta^9 + \theta^{12} \\
R_1^{-1}(\theta^{11}) &= \theta^5 + \theta^6 + \theta^{10} + \theta^{13} + \theta^{14} \\
R_1^{-1}(\theta^{12}) &= \theta^5 + \theta^6 + \theta^{10} \\
R_1^{-1}(\theta^{13}) &= \theta^{14} \\
R_1^{-1}(\theta^{14}) &= \theta + \theta^5 + \theta^6 + \theta^7 + \theta^8 + \theta^{10} + \theta^{11} + \theta^{13} + \theta^{14}
\end{aligned}
$$

Next we find the basic slope matrices $R_i = T_{\theta^i}$, for $0 \leq i < 15$.

Since 1 is the identity of the classical Knuth binary semifield, $R_0 = I_{15}$, the identity matrix of size 15×15.

To compute R_1, we first calculate $\theta^i * \theta$ and represent the result by a vector with basis $\{1, \theta, \theta^2, \cdots, \theta^{14}\}$. Then R_1 is composed of the following vectors.

$$
\begin{aligned}
1 * \theta &= \theta = (01000, 00000, 00000) \\
\theta * \theta &= R_1^{-1}(\theta) \circ R_1^{-1}(\theta) = \theta + \theta^2 + \theta^4 + \theta^8 \\
&= (01101, 00010, 00000) \\
\theta^2 * \theta &= R_1^{-1}(\theta^2) \circ R_1^{-1}(\theta) = \theta + \theta^2 + \theta^3 + \theta^4 + \theta^5 + \theta^8 + \theta^9 \\
&= (01111, 10011, 00000)
\end{aligned}
$$

$$
\begin{aligned}
\theta^3 * \theta &= R_1^{-1}(\theta^3) \circ R_1^{-1}(\theta) = \theta^3 + \theta^4 + \theta^5 + \theta^9 + \theta^{11} + \theta^{12} + \theta^{13} + \theta^{14} \\
&= (00011, 10001, 01111) \\
\theta^4 * \theta &= R_1^{-1}(\theta^4) \circ R_1^{-1}(\theta) = \theta + \theta^2 + \theta^3 + \theta^5 + \theta^6 + \theta^8 + \theta^9 + \theta^{10} \\
&= (01110, 11011, 10000) \\
\theta^5 * \theta &= R_1^{-1}(\theta^5) \circ R_1^{-1}(\theta) = \theta^2 + \theta^5 = (00100, 10000, 00000) \\
\theta^6 * \theta &= R_1^{-1}(\theta^6) \circ R_1^{-1}(\theta) = \theta^3 + \theta^4 + \theta^7 + \theta^9 + \theta^{12} + \theta^{13} + \theta^{14} \\
&= (00011, 00101, 00111) \\
\theta^7 * \theta &= R_1^{-1}(\theta^7) \circ R_1^{-1}(\theta) = \theta^2 + \theta^4 + \theta^6 + \theta^7 = (00101, 01100, 00000) \\
\theta^8 * \theta &= R_1^{-1}(\theta^8) \circ R_1^{-1}(\theta) = \theta + \theta^2 + \theta^3 + \theta^5 + \theta^9 + \theta^{10} + \theta^{12} \\
&= (01110, 10001, 10100) \\
\theta^9 * \theta &= R_1^{-1}(\theta^9) \circ R_1^{-1}(\theta) = \theta + \theta^3 + \theta^4 + \theta^6 + \theta^8 + \theta^{10} + \theta^{12} + \theta^{14} \\
&= (01011, 01010, 10101) \\
\theta^{10} * \theta &= R_1^{-1}(\theta^{10}) \circ R_1^{-1}(\theta) = \theta^2 + \theta^5 + \theta^7 + \theta^9 + \theta^{13} \\
&= (00100, 10101, 00010) \\
\theta^{11} * \theta &= R_1^{-1}(\theta^{11}) \circ R_1^{-1}(\theta) = 1 + \theta^3 + \theta^6 + \theta^7 + \theta^9 + \theta^{10} + \theta^{12} + \theta^{13} \\
&= (10010, 01101, 10110) \\
\theta^{12} * \theta &= R_1^{-1}(\theta^{12}) \circ R_1^{-1}(\theta) = \theta^3 + \theta^4 + \theta^7 + \theta^8 + \theta^9 + \theta^{10} + \theta^{12} + \theta^{13} \\
&= (00011, 00111, 10110) \\
\theta^{13} * \theta &= R_1^{-1}(\theta^{13}) \circ R_1^{-1}(\theta) = \theta + \theta^2 + \theta^3 + \theta^4 + \theta^7 + \theta^8 \\
&= (01111, 00110, 00000) \\
\theta^{14} * \theta &= R_1^{-1}(\theta^{14}) \circ R_1^{-1}(\theta) = 1 + \theta + \theta^2 + \theta^4 + \theta^6 + \theta^7 + \theta^9 + \theta^{11} \\
&= (11101, 01101, 01000)
\end{aligned}
$$

So

$$R_1 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Similarly, we found the other slope matrices $R_2, R_3, \cdots, R_{14}$.

$$R_2 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1
\end{pmatrix}$$

$$R_3 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

$$R_4 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1
\end{pmatrix}$$

$$R_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$R_6 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$R_7 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}$$

$$R_8 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0
\end{pmatrix}$$

$$R_9 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$R_{10} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$R_{11} = \begin{pmatrix}
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1
\end{pmatrix}$$

$$R_{12} = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}$$

$$R_{13} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$R_{14} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

The program given in Appendix A is used to compute the different right characteristic polynomials of all the elements in $\mathcal{S} = (GF(2^{15}), +, *)$.

Finally to find a primitive polynomial. We checked all the above polynomials and found that the matrix $R_3 + R_9$, corresponding to the element $\theta^3 + \theta^9$, has right characteristic polynomial

$$F(x) = x^{15} + x^6 + x^4 + x^3 + x^2 + x + 1$$

We now show that $F(x)$ is a primitive polynomial over $GF(2)$, i.e., the order of $F(x)$ is $2^{15}-1$.

Let α be a root of $F(x)$. We need to show the order of α is $2^{15}-1$. Now $2^{15}-1 = 7 \times 31 \times 151$ and

$$\begin{aligned}
&\alpha^{15} = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \\
&\alpha^{31} = \alpha^{13} + \alpha^9 + \alpha^7 + \alpha^5 + \alpha^3 + \alpha \\
&\alpha^{151} = \alpha^{13} + \alpha^{12} + \alpha^{10} + \alpha^9 + \alpha^6 + \alpha^5 + \alpha \\
&\alpha^{7\times 31} = \alpha^{14} + \alpha^{13} + \alpha^{11} + \alpha^{10} + \alpha^9 + \alpha^8 + \alpha^4 + 1 \\
&\alpha^{7\times 151} = \alpha^{12} + \alpha^{11} + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 \\
&\alpha^{31\times 151} = \alpha^{14} + \alpha^{13} + \alpha^{12} + \alpha^{11} + \alpha^4 + \alpha^3 + \alpha \\
&\alpha^{2^{15}-1} = 1
\end{aligned}$$

Therefore the order of $F(x)$ is $2^{15}-1$.

For the case when $t = 17$, we choose $f(x) = x^{17} + x^3 + 1$. Then using Matlab and GAP we found that the element $\theta + \theta^3$ has right characteristic polynomial

$$F(x) = x^{17} + x^{13} + x^{11} + x^7 + x^4 + x + 1$$

which is irreducible over $GF(2)$. Since $2^{17}-1$ is a Mersenne prime number, the order of $F(x)$ must be $2^{17}-1$.

When $t = 19$, we choose $f(x) = x^{19} + x^9 + x^7 + x + 1$. Then again by using Matlab and GAP we found that the element θ^9 has right characteristic polynomial

$$F(x) = x^{19} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{11} + x^{10} + x^7 + x^3 + x^2 + x + 1$$

which is irreducible over $GF(2)$. Since $2^{19}-1$ is also a Mersenne prime number,then the order of $F(x)$ is $2^{19}-1$. □

2.4 Primitive Elements in The Classical Knuth Binary Semifields

In this section, we are concerned with the number of primitive elements in the classical Knuth binary semifields. Knuth [12] proved that for any element $d \in F$, the mapping $d \to d^2$ is an automorphism of the classical Knuth binary semifield. Hence d and d^2 have the same right characteristic polynomial. Let r be the smallest integer such that $d^{2^r} = d$. Then obviously $d, d^2, d^{2^2}, \cdots, d^{2^{r-1}}$ have the same right characteristic polynomial.

Definition 2.4.1. *We call r the length of d and $\{d, d^2, d^{2^2}, \cdots, d^{2^{r-1}}\}$ the family of d.*

Proposition 2.4.1. *For any nonzero $d \in \mathcal{S}$, the length r of d is a divisor of t.*

Proof. Let $d \neq 1$, otherwise the result is obviously true, and $t = qr + a$, where $0 \leq a < r$. If $a \neq 0$, since $d \in F$ and $d^{2^r} = d$, then

$$d = d^{2^t} = d^{2^{qr+a}} = d^{2^{qr}} d^{2^a}$$

and $d^{2^a} = 1$. Hence the order of d must be a divisor of $(2^r - 1, 2^a) = 1$, and so $d = 1$. Hence $a = 0$ and then r is a divisor of t. □

Remark 2.4.1. *Some right characteristic polynomials with degree t have more than t matrices as their roots.*

For example, in the classical Knuth binary semifield of order 32, x^5+x+1 is the right characteristic polynomial of each of the following fifteen elements: ζ, ζ^2, ζ^4, $\zeta + \zeta^3 + \zeta^4$, $\zeta^2 + \zeta^3$, ζ^3, $\zeta + \zeta^4$, $\zeta + \zeta^2 + \zeta^3 + \zeta^4$, $\zeta^2 + \zeta^3 + \zeta^4$, $\zeta + \zeta^2 + \zeta^3$, $\zeta + \zeta^2$, $\zeta^2 + \zeta^4$, $\zeta + \zeta^3$, $\zeta + \zeta^2 + \zeta^4$, $\zeta + \zeta^2 + \zeta^3$. Hence all the matrices associated with these fifteen elements are the roots of $x^5 + x + 1$.

In any semifield t-dimensional over its center, 0 is the unique element with right characteristic polynomial x^t and 1 is the unique element with right characteristic polynomial $(x-1)^t$. Since 0 and 1 can never be primitive elements, these two polynomials are excluded from all the subsequent proofs of this section.

For every right characteristic polynomial $f(x)$, where $f(x) \neq x^t$ and $f(x) \neq (x-1)^t$, let $N(f)$ indicate the number of elements in $\mathcal{F}$ whose right characteristic polynomial is $f(x)$. Then $N(f) = \sum\limits_{i|t, 1<i\leq t} i \cdot n_{i,f}$, where i = length of a family, and $n_{i,f}$ = the number of families of length i whose elements have $f(x)$ as their right characteristic polynomial.

For example, in Remark 2.4, there are 3 families of length 5 whose elements have right characteristic polynomial $x^5 + x + 1$ in the Knuth binary semifield of order 32. In this case $i = 5$ and $n_i = 3$.

Notice that by the arguments given above, Part (1) of the following result follows.

Theorem 2.4.1. *Let $\mathcal{F} = (GF(2^t), +, *)$, t odd, be the classical Knuth binary semifield and $f_1(x), f_2(x), \cdots, f_n(x)$ be all the distinct primitive right characteristic polynomials of $\mathcal{F}$. Let N_t be the number of primitive elements in $\mathcal{F}$. Then*

(1) $N_t = \sum\limits_{i|t,1<i\leq t} i \cdot n_i$, where i = length of a family, $n_i = \sum\limits_{k=1}^{n} n_{i,k}$, $n_{i,k}$ = the number of families of length i whose elements have $f_k(x)$ as their right characteristic polynomial.

(2) $n_i \leq [\frac{2^i-2}{i}]$.

Proof. We prove Part (2).

Let d be a primitive element with length i; then $d^{2^i-1} = 1$. Suppose θ is a generator of the finite field $GF(2^t)$, and $d = \theta^m$ for some m. Then $(\theta^m)^{2^i-1} = \theta^{m(2^i-1)} = 1$. Hence $2^t - 1 | m(2^i - 1)$. Let $s(2^t-1) = m(2^i-1)$ for some s; hence $m = s(\dfrac{2^t-1}{2^i-1})$. There are at most $2^i - 2$ choices for m, which means d has at most 2^i-2 possibilities. The set of conjugates of d contains i elements, so the number of families with length i must be less than or equal to $[\dfrac{2^i-2}{i}]$. □

Theorem 2.4.2. *With the hypothesis of Theorem 2.4.1, if t is an odd prime number, then N_t is a multiple of t.*

Proof. Let $d \neq 0$ be a primitive element in $\mathcal{F}$ with length i. Then $i|t$, and so $i = 1$ or t. If $i = 1$, then we have $d^2 = d$, which implies $d = 1$; hence the length of d must be t and so N_t is a multiple of t. □

The following well-known result follows easily from Theorem 2.4.1.

Corollary 2.4.1. *If t is an odd prime number, then $t|(2^{t-1} - 1)$*

Proof. If t is a prime number, there are $2^t - 2$ nonzero, nonidentity elements in the Knuth binary semifield $\mathcal{F} = (GF(2^t), +, *)$, t odd. All these elements can be separated into several families; each family has t elements, so $t|(2^{t-1} - 1)$. □

Theorem 2.4.3. *For an odd integer $t \in [5, 19]$, the number of primitive elements, N_t, in the classical Knuth binary semifield $\mathcal{F}$=$(GF(2^t), +, *)$ is a multiple of t.*

Proof. This result is true for prime numbers t by Theorem 2.4.2. When $t = 9$, choose the irreducible polynomial $f(x) = x^9 + x^4 + x^3 + x + 1$ over $GF(2)$. Let θ be a root of $f(x)$. Since $f(x)$ is a primitive polynomial over the finite field $GF(2^9)$, then θ is a generator of the multiplicative group of this field. Let d be an element in $\mathcal{F} = (GF(2^9), +, *)$ of length 3. Then there are 6 possibilities for d in $\mathcal{F}$, which are

$$\theta^{73}, \theta^{146}, \theta^{292}$$

$$\theta^{219}, \theta^{438}, \theta^{365}$$

With the help of Matlab and GAP, we found the right characteristic polynomial of each family is,

$$P_1(x) = x^9 + x^8 + x^3 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)(x^4 + x^3 + 1)$$

$$P_2(x) = x^9 + x^3 + x^2 + x + 1 = (x^2 + x + 1)(x^3 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

respectively, which are both reducible over $GF(2)$. So those d are not primitive elements in $\mathcal{F} = (GF(2^9), +, *)$, which implies that the number of primitive elements in $\mathcal{F} = (GF(2^9), +, *)$ is a multiple of 9.

The only case left is $t = 15$. Now we prove all the right characteristic polynomials of all the elements of length r, where r is a proper divisor of 15, are reducible over $GF(2)$.

Let $f(x) = x^{15} + x + 1$ be an irreducible polynomial for the field extension from $GF(2)$ to $GF(2^{15})$. It is easily shown that $f(x)$ has order $2^{15} - 1$, which implies that $f(x)$ is primitive. Let θ be a root of $f(x)$. Then θ is a generator of the multiplicative group of the finite field $GF(2^{15})$. Suppose d is an element in $\mathcal{F} = (GF(2^{15}), +, *)$ of length r. Then $d = \theta^m$ for some m.

1. If $r = 3$, there are $2^3 - 2 = 6$ choices for d, and those elements are separated into 2 families.

$$\begin{aligned} &(1.1) \quad \theta^{\Delta}, \theta^{2\Delta}, \theta^{4\Delta} \\ &(1.2) \quad \theta^{3\Delta}, \theta^{6\Delta}, \theta^{5\Delta} \end{aligned}$$

where $\Delta = 31 \times 151$. With the help of Matlab and GAP, we found that the right characteristic polynomials of (1.1) and (1.2) are

$$\begin{aligned} F_1(x) &= x^{15} + x^{13} + x^{12} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x + 1 \\ &= (x^3 + x + 1)(x^{12} + x^6 + x^5 + x^3 + 1) \\ F_2(x) &= x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^2 + 1 \\ &= (x^3 + x^2 + 1)(x^{12} + x^8 + x^6 + x^5 + x^4 + x^3 + 1), \end{aligned}$$

respectively; notice these are both reducible over $GF(2)$. So these d are not primitive elements in $\mathcal{F}$.

2. If $r = 5$, there are $2^5 - 2 = 30$ choices for d, and those elements are separated into 6 families.

$$\begin{aligned}
&(2.1) \quad \theta^{\delta}, \theta^{2\delta}, \theta^{4\delta}, \theta^{8\delta}, \theta^{16\delta} \\
&(2.2) \quad \theta^{3\delta}, \theta^{6\delta}, \theta^{12\delta}, \theta^{24\delta}, \theta^{17\delta} \\
&(2.3) \quad \theta^{5\delta}, \theta^{10\delta}, \theta^{20\delta}, \theta^{9\delta}, \theta^{18\delta} \\
&(2.4) \quad \theta^{7\delta}, \theta^{14\delta}, \theta^{28\delta}, \theta^{25\delta}, \theta^{19\delta} \\
&(2.5) \quad \theta^{11\delta}, \theta^{22\delta}, \theta^{13\delta}, \theta^{26\delta}, \theta^{21\delta} \\
&(2.6) \quad \theta^{15\delta}, \theta^{30\delta}, \theta^{29\delta}, \theta^{27\delta}, \theta^{23\delta}
\end{aligned}$$

where $\delta = 7 \times 151$. With the help of Matlab and GAP, we found that the right characteristic polynomials of (2.1)–(2.6) are

$$\begin{aligned}
G_1(x) &= x^{15} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x + 1 \\
&= (x^2 + x + 1)^2 (x^3 + x^2 + 1)(x^8 + x^7 + x^3 + x + 1) \\
G_2(x) &= x^{15} + x^{14} + x^{13} + x^9 + x^8 + x^6 + x^5 + x^3 + 1 \\
&= (x^2 + x + 1)^2 (x^3 + x + 1)(x^8 + x^7 + x^6 + x^5 + x^4 + x + 1) \\
G_3(x) &= x^{15} + x^{13} + x^9 + x^8 + x^7 + x + 1 \\
&= (x^2 + x + 1)(x^3 + x^2 + 1)(x^{10} + x^8 + x^6 + x^5 + 1) \\
G_4(x) &= x^{15} + x^{14} + x^{11} + x^{10} + x^9 + x^5 + x^4 + x + 1 \\
&= (x^2 + x + 1)(x^3 + x + 1)(x^{10} + x^6 + x^5 + x + 1) \\
G_5(x) &= x^{15} + x^{13} + x^{12} + x^{11} + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
&= (x^2 + x + 1)^2 (x^3 + x^2 + 1)(x^8 + x^7 + x^6 + x^5 + x^2 + x + 1) \\
G_6(x) &= x^{15} + x^{14} + x^{10} + x^8 + x^7 + x^5 + x^3 + x + 1 \\
&= (x^2 + x + 1)(x^3 + x^2 + 1)(x^{10} + x^9 + x^6 + x^5 + x^4 + x^3 + 1)
\end{aligned}$$

respectively. Again these are all reducible over $GF(2)$. So these d are not primitive elements in $\mathcal{F} = (GF(2^{15}), +, *)$. □

Conjecture 2.4.1. *In the classical Knuth binary semifield $\mathcal{F} = (GF(2^t), +, *)$, t odd, any right characteristic polynomial $f(x)$ of an element d, whose length is a proper divisor of t, is reducible over $GF(2)$; so the number of primitive elements in $\mathcal{F}$ is always a multiple of t.*

Remark 2.4.2.

Let $GF(q)$ be the finite field of order q. Cohen and Mullen [5] proved four conjectures made by Golomb for finite fields as follows:

Conjecture A: If $q > 2$ then $GF(q)$ contains two primitive elements α and β (not necessarily distinct) with $\alpha + \beta = 1$.

Conjecture B: If $q > 3$ then $GF(q)$ contains two primitive elements α and β with $\alpha + \beta = -1$.

Conjecture C: For all $q > q_0$, every non-zero element ε has at least one representation of the form $\varepsilon = \alpha + \beta$, where α and β are primitive elements of $GF(q)$.

Conjecture D: There exists a primitive quadratic of trace 1 over every $GF(q)$.

By direct cooperation, see appendices C and D, we found that Conjectures A and C also hold in the classical Knuth binary semifields of order 2^7 and 2^9. Conjecture A also holds in Knuth's system V and system W, but Conjecture C fails in them. Notice that in our context, Conjectures B and A are the same; Conjecture D is not applicable in the classical Knuth binary semifields.

Conjecture 2.4.2. *Golomb's conjectures A and C hold in all the primitive classical Knuth binary semifields.*

2.5 Primitivity of Albert Semifields of order 2^7, 2^9, 2^{11}, 2^{13}

Albert semifields $A_n(S)$, where $n \geq 5$ is odd, is a class of commutative semifields with characteristic 2. The Albert semifield of order 32 is both right and left primitive and it contains 22 primitive elements [17]. We are concerned with the primitivity of Albert Semifields $A_n(S)$, when $n = 7, 9, 11, 13$.

Theorem 2.5.1. *The Albert Semifields $A_n(S)$, where $n = 7, 9, 11, 13$, are all right and left primitive.*

Proof. When $n = 7$, suppose $f(x) = x^7 + x + 1$ is the irreducible polynomial over $GF(2)$ used to construct the finite field $GF(2^7)$ and θ is a root of $f(x)$. Then $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6\}$ is a $GF(2)$-basis of the vector space $GF(2^7)$.

Let $S = GF(2) + GF(2)\theta + GF(2)\theta^2 + GF(2)\theta^3 + GF(2)\theta^4 + GF(2)\theta^5$ and $\omega = \theta^6$. By the definition of multiplication in Albert semifields,

$$s * t = st, \quad s * \omega = \omega * s = s\omega + s^2 + s, \quad \omega * \omega = \omega^2 + 1$$

for any $s, t \in S$. We calculate all the right slope matrices $\{T_1, T_\theta, \cdots, T_{\theta^6}\}$. Let R_i be the right slope matrix T_{θ^i}, $0 \leq i < 7$.

Obviously, $R_0 = I_7$, the identity matrix of size 7×7. Next we compute R_1:

$$\begin{aligned}
1 * \theta &= \theta = (01000, 00) \\
\theta * \theta &= \theta^2 = (00100, 00) \\
\theta^2 * \theta &= \theta^3 = (00010, 00) \\
\theta^3 * \theta &= \theta^4 = (00001, 00) \\
\theta^4 * \theta &= \theta^5 = (00000, 10) \\
\theta^5 * \theta &= \theta^6 = (00000, 01) \\
\theta^6 * \theta &= \theta^7 + \theta^2 + \theta = 1 + \theta^2 = (10100, 00)
\end{aligned}$$

So $$R_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Similarly, we found

$$R_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \ R_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$R_4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \ R_5 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$R_6 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Using the program given in Appendix B, we can get all the different right characteristic polynomials of all the elements in the Albert Semifield $A_7(S)$.

Finally we checked all the polynomials above and found that the matrix R_1+R_2, corresponding to the element $\theta + \theta^2$, has right characteristic polynomial $F(x) = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$, which has order $2^7 - 1$. So $\theta + \theta^2$ is a right primitive element, which implies $A_7(S)$ is both right and left primitive.

When $n = 9, 11, 13$, similarly by our computation, the Albert semifields A_n are all all right and left primitive.

□

2.6 Automorphisms of Right Primitive Semifields

If ω is a right primitive element of $\mathcal{S} = (D, +, *)$ and σ is any automorphism of $\mathcal{S}$, then $\sigma(\omega)$ must be a right primitive element and $\sigma(\omega^{i)}) = \sigma(\omega)^{i)}$ for any integer i. Now we consider sort of a converse of this problem, namely, if $\mathcal{S} = (D, +, *)$ is a right primitive semifield of order q^n, and σ is a bijection from $\mathcal{S}$ to $\mathcal{S}$ with $\sigma(\omega^{i)}) = d^{i)}$, where ω and $d = \sigma(\omega)$ are both right primitive elements, must σ be an automorphism of $\mathcal{S}$? Certainly if ω and d have different characteristic polynomials, σ is not an automorphism of $\mathcal{S}$; however, if ω and d have the same characteristic polynomial, what happens?

We give two examples in which σ is defined by $\sigma(\omega^{i)}) = \sigma(\omega)^{i)}$, where ω and d are right primitive elements with the same right characteristic polynomial, but σ is not an automorphism of $\mathcal{S}$.

Example 1 Knuth's system W. In W, which is a noncommutative semifield, there are 6 right primitive elements who possess the same right characteristic polynomial $x^4 + x + 1$, and all the bijections can be represented by $\sigma_{ij}(u + \lambda v) = u^i + \lambda\omega^j v$, $i = 1, 2,\ j = 0, 1, 2$, [11]. We show that exactly 3 of them are automorphisms in system W, namely $\sigma_{10}(u + \lambda v) = u + \lambda v$, $\sigma_{11}(u + \lambda v) = u + \lambda\omega v$, and $\sigma_{12}(u + \lambda v) = u + \lambda\omega^2 v$.

Proof. σ_{10} is the identity map of system W, so it is obviously an automorphism. Now, for addition,

$$\sigma_{11}((u + \lambda v) + (x + \lambda y))$$

$$= \sigma_{11}((u + x) + \lambda(v + y))$$

$$= (u + x) + \lambda\omega(v + y)$$

$$= (u + \lambda\omega v) + (x + \lambda\omega y)$$

$$= \sigma_{11}(u + \lambda v) + \sigma_{11}(x + \lambda y)$$

For multiplication, we have on the one hand,

$$\sigma_{11}((u + \lambda v)(x + \lambda y))$$

$$= \sigma_{11}((ux + \omega v^2 y) + \lambda(vx + u^2 y))$$

$$= (ux + \omega v^2 y) + \lambda\omega(vx + u^2 y)$$

On the other hand,

$$\sigma_{11}(u + \lambda v)\sigma_{11}(x + \lambda y)$$

$$= (u + \lambda\omega v)(x + \lambda\omega y)$$

$$= (ux + \omega(\omega v)^2 \omega y) + \lambda(\omega vx + u^2 \omega y)$$

$$= (ux + \omega v^2 y) + \lambda\omega(vx + u^2 y)$$

$$= \sigma_{11}((u + \lambda v)(x + \lambda y))$$

Hence σ_{11} is an automorphism of system W. Similarly, we can prove that σ_{12} is an automorphism of system W.

But σ_{20}, σ_{21}, and σ_{22} are not automorphisms of system W, because

$$\sigma_{20}((\omega + \lambda)(\omega + \lambda)) = 1 + \lambda \neq \lambda = \sigma_{20}(\omega + \lambda)\sigma_{20}(\omega + \lambda),$$

$$\sigma_{21}((\omega + \lambda)(\omega + \lambda)) = 1 + \lambda\omega = \lambda\omega = \sigma_{21}(\omega + \lambda)\sigma_{21}(\omega + \lambda),$$

$$\sigma_{22}((\omega + \lambda)(\omega + \lambda)) = 1 + \lambda\omega^2 = \lambda\omega^2 = \sigma_{22}(\omega + \lambda)\sigma_{21}(\omega + \lambda).$$

□

Example 2 Let $GF(2^7) = GF(2)(\theta)$, where θ is a root of the irreducible polynomial $f(x) = x^7 + x + 1$ over $GF(2)$. Then $\{1, \theta, \theta^2, \cdots, \theta^6\}$ is a $GF(2)$-basis of

$GF(2^7)$. Now consider the elements $\theta+\theta^6$ and $\theta^4+\theta^5$ in the classical Knuth binary semifield $\mathcal{F} = (GF(2^7), +, *)$. They are primitive elements and the characteristic polynomial of both elements is x^7+x+1. Suppose σ is the bijection of $\mathcal{F}$ given by $\sigma((\theta+\theta^6)^{i)}) = (\theta^4+\theta^5)^{i)}$; we show that σ is not an automorphism of $\mathcal{F}$.

By direct computation, we know

$$\begin{array}{ll} R_1(1) = 1 & R_1(\theta) = \theta+\theta^2 \\ R_1(\theta^2) = \theta^2+\theta^4 & R_1(\theta^3) = \theta^3+\theta^6 \\ R_1(\theta^4) = \theta+\theta^2+\theta^4 & R_1(\theta^5) = \theta^3+\theta^4+\theta^5 \\ R_1(\theta^6) = \theta^5 & \end{array}$$

and

$$\begin{array}{ll} R_1^{-1}(1) = 1, & R_1^{-1}(\theta) = \theta^2+\theta^4 \\ R_1^{-1}(\theta^2) = \theta+\theta^2+\theta^4, & R_1^{-1}(\theta^3) = \theta+\theta^4+\theta^5+\theta^6 \\ R_1^{-1}(\theta^4) = \theta+\theta^4, & R_1^{-1}(\theta^5) = \theta^6 \\ R_1^{-1}(\theta^6) = \theta+\theta^3+\theta^4+\theta^5+\theta^6 & \end{array}$$

Also

$$\begin{array}{ll} \theta = (\theta+\theta^6)^{44)} & 1+\theta+\theta^2+\theta^3+\theta^4 = (\theta^4+\theta^5)^{44)} \\ \theta+\theta^2+\theta^4 = (\theta+\theta^6)^{82)} & 1+\theta^2+\theta^6 = (\theta^4+\theta^5)^{82)} \end{array}$$

Hence

$$\theta * \theta = R_1^{-1}(\theta) \circ R_1^{-1}(\theta) = \theta+\theta^2+\theta^4 = (\theta+\theta^6)^{82)}$$

$$\sigma(\theta * \theta) = (\theta^4+\theta^5)^{82)} = 1+\theta^2+\theta^6$$

But

$$\begin{aligned} \sigma(\theta) * \sigma(\theta) &= \sigma((\theta+\theta^6)^{44)}) * \sigma((\theta+\theta^6)^{44)}) \\ &= (\theta^4+\theta^5)^{44)} * (\theta^4+\theta^5)^{44)} \\ &= (1+\theta+\theta^2+\theta^3+\theta^4) * (1+\theta+\theta^2+\theta^3+\theta^4) \\ &= (1+R_1^{-1}(\theta)+R_1^{-1}(\theta^2)+R_1^{-1}(\theta^3)+R_1^{-1}(\theta^4))^2 \\ &= 1+\theta^2+\theta^3+\theta^4+\theta^5+\theta^6 \end{aligned}$$

$\sigma(\theta * \theta) \neq \sigma(\theta) * \sigma(\theta)$, so σ is not an automorphism of $\mathcal{F}$.

CHAPTER 3

DIMENSION of FINITE SEMIFIELDS

3.1 Introduction

In this chapter we are concerned with the dimension of a finite semifield over its sub-semifields. We know the dimension of the finite field $F = GF(q^n)$ over a subfield $K = GF(q^m)$ is specified by $log_{q^m} q^n = \frac{n}{m}$, which is always an integer. One may more generally defined the dimension of an arbitrary finite ternary ting with respect to any sub-ternary ring.

Definition 3.1.1. *Let D be a ternary ring of order n with a sub-ternary ring E of order m. Then the dimension of D relative to E is specified by $dim_E D := log_m n$; D is transcendental, fractional, or integer dimensional, relative to E, according to whether $dim_E D$ is transcendental, rational (but not an integer), or an integer.*

Similarly, if π is an affine plane of order n, with an affine subplane π_0 of order m, the dimension of π relative to π_0 is specified by $log_m n$. In particular, π has transcendental, fractional, or integer dimensional, relative to π_0, according to whether $log_m n$ is transcendental, rational (but not an integer), or an integer.

In this paper, we focus on finite semifields and finite semifield planes. Suppose $\mathcal{S} = (D, +, *)$ is a finite semifield, n-dimensional over its center $K \cong GF(q)$, where q is a prime power. Then the order of $\mathcal{S}$ must be q^n. Let E be any sub-semifield of $\mathcal{S}$; then the order of E must be q^m for some positive integer m. Hence $dim_E D = log_{q^m} q^n = \frac{n}{m}$, which is either an integer or a proper rational number. Therefore, finite semifields can never have transcendental dimension.

Definition 3.1.2. *Let $\mathcal{S} = (D, +, *)$ be a finite semifield of order n, with a sub-semifield E of order m. Then the dimension of $\mathcal{S}$ relative to E, is specified by $d := dim_E D = log_m n$; the semifield $\mathcal{S}$ is fractional dimensional relative to E if d is a proper rational number.*

A semifield $\mathcal{S}$ is considered fractional if it is fractional dimensional relative to some sub-semifield E.

In this chapter we show that some semifields can be fractional dimensional and some other semifields can never be fractional dimensional. If E is a sub-semifield of D such that $dim_E D$ is a proper rational number, we consider the case when E has small order, i.e., $|E| = q^2$ or $|E| = q^3$.

Let π be a projective (affine) plane of order n with a subplane π_0 of order m. Then either $n = m^2$ or $n \geq m^2 + m$ [p10, 10].

Definition 3.1.3. *If π is a projective (affine) plane of order n, a Baer subplane of π is a subplane of order m with $n = m^2$.*

By the Baer condition, it is obvious that a fractional dimensional semifield D must have order $|D| \geq 32$. Examples of semifields of order 32 containing the finite field $GF(4)$ are given in [2], [9], and [15] . G.P. Wene also found several sporadic semifields of order 2^j, for $j = 5, 7, 9, 11$, that admit a subplane of order 2^2. On the other hand, V.Jha and N.L.Johnson [9] pointed out a sufficient condition for the generalized Knuth binary semifields to admit a subfield of order 2^2.

Let $F = GF(2^t)$, the finite field of order 2^t, and $GL(F, +)$ be the full group of $GF(2)$-linear bijections of the vector space F. We first point out the notation to be used in this chapter.

Notation 3.1.1. *(1) $T : F \to \{0, 1\}, x \to x^T$, is the trace map, and $\Gamma = Ker(T)$.*
(2) The stabilizer of Γ in $GL(F, +)$ is denoted by $GL(F, +)_\Gamma$.

In this chapter first we list some finite semifields that are fractional dimensional relative to the finite field $GF(2^2)$, and then we prove that the classical Knuth binary semifields do not admit any sub-semifields; hence this class of semifields can never be fractional dimensional. Finally, we show that a special class of the generalized Knuth binary semifields are commutative and do not admit subfields $GF(2^2)$ or $GF(2^3)$. We also prove that the Albert semifields can never contain $GF(2^3)$.

3.2 Generalized Knuth Binary Semifields with Fractional Dimension

The classical binary Knuth pre-semifield associated with the finite field $F = GF(2^t)$, $t \geq 5$ odd, is a commutative pre-semifield $(F, +, \circ)$ with product:

$$(ComKn) \qquad x \circ y = xy + (x^T y + y^T x)^2$$

V. Jha and N.L. Johnson [9] generalized the construction of the classical Knuth binary semifields as follows.

Let $F = GF(2^t)$, $t \geq 5$ odd. Then for any $B, C \in GL(F, +)$, there corresponds a pre-semifield $\mathcal{F}_{B,C}(F) = (F, +, \odot)$, where $\odot$ is defined by

$$(GenKn) \qquad x \odot y = x^B y^C + (x^{BT} y^C + y^{CT} x^B)^2$$

For any choice of $e \in F^*$. The product in the pre-semifield $\mathcal{F}_{B,C}(F) = (F, +, \odot)$ can be redefined so that $\mathcal{F}^{(e)}_{B,C}(F) = (F, +, *)_e$ becomes a semifield called a generalized Knuth binary semifield. The new product is given by

$$(x \odot e) * (e \odot y) = x \odot y, \ for \ every \ x, \ y \in F$$

Notice that $e \odot e$ is the multiplicative identity for $(F, +, *)_e$.

Let $B = R_b$ and $C = R_c$ be multiplication from the right by elements $b, c \in F$. V. Jha and N.L. Johnson [9] also pointed out that if there exist $b, c \in F$ such that

$$(ec)^T = b^T = (eb)^T = 0, \quad c^T = 1, \quad and \quad \frac{e^2}{e+1} = 1 + \frac{b}{c} \tag{3.1}$$

then there exists a subfield isomorphic to $GF(4)$ in $(F, +, *)_e$.

The corresponding semifield plane is the commutative binary Knuth semifield plane, which has order 2^t, and would then admit a subsemifield plane of order 2^2.

When $t = 5$ or 7 there are subplanes of order 4 in the commutative binary Knuth semifield planes of order 2^t, c.f. Corollary 1 [9].

In this section we present a family of irreducible polynomials, where all the x-divisible monomials (i.e., all the monomials of the form x^i, where $i \geq 1$) have trace zero, and then use them to show that there are semifields of order 2^r, for any odd integer $r \in [5, 31]$, containing $GF(4)$. Hence these semifields are fractional dimensional.

Lemma 3.2.1. *Suppose $F = GF(2^t)$, where t is an odd positive integer. Let $t = 2N+1$ for some positive integer N. Suppose $x^t + f(x) + 1$ is an irreducible polynomial for the field extension over $GF(2)$, where $f(x)$ is any x-divisible polynomial (i.e., the constant of $f(x)$ is 0) of degree$< t$, in which all even degree monomials have coefficient zero. Then $T(x^i) = 0$ for $0 < i < t$.*

Proof. For any x^i, $0 < i < t$,

$$T(x^i) = \sum_{j=0}^{t-1} (x^i)^{2^j} = x^i + (x^i)^2 + (x^i)^{2^2} + \cdots + (x^i)^{2^{t-1}}$$

Let $Gal(F)$=\{all the distinct automorphisms of $GF(2^t)$ over $GF(2)$\} and σ be any element of $Gal(F)$. Then $\sigma(x) = x^{2^m}$, for any $m = 0, 1, \cdots, t-1$. Since t is odd, $\sigma(x)$ is x-divisible, and so is $T(x^i)$. Hence $T(x^i) = 0$, because the trace function is onto $GF(2)$. □

Lemma 3.2.2. *If an irreducible polynomial in Lemma 3.2.1 exists with $a_{2N-1} = 0$, i.e., $a_{t-2} = 0$, then $T(x^{t+2}) = 0$.*

Proof. Let $f(x) = \sum_{k=1}^{N} a_{2k-1}x^{2k-1}$. Then $x^t = 1 + \sum_{k=1}^{N} a_{2k-1}x^{2k-1}$, and

$$x^{t+2} = x^2x^t = x^2 + a_1x^3 + \cdots + a_{2t-3}x^{2N-1} + a_{2N-1}x^t$$

By Lemma 3.2.1, $T(x^i) = 0$, $0 < i < t$, so

$$T(x^{t+2}) = 0 + a_{2N-1}T(x^t) = 0 + 0 = 0$$

□

Theorem 3.2.1. *Suppose an irreducible polynomial in Lemma 3.2.2 exists and let*

$$e = 1 + x, \quad b = x^{t+1} + x^{t-2}, \quad c = x^t + x^{t-1}$$

Then the generalized Knuth binary semifield $(F, +, *)_e$ admits a subfield isomorphic to $GF(4)$.

Proof. We just need to check e, b and c satisfy (3.1):
Now $\frac{e^2}{1+e} = \frac{(1+x)^2}{x} = \frac{1+x^2}{x}$, and

$$\frac{b}{c} = \frac{x^{t+1} + x^{t-2}}{x^t + x^{t-1}} = \frac{x^{t-2}(x^3+1)}{x^{t-1}(x+1)} = \frac{x^2+x+1}{x}$$

So $\frac{e^2}{1+e} = 1 + \frac{b}{c}$. Also

$$T(b) = T(x^{t+1}) + T(x^{t-2}) = 0 + 0 = 0,$$

$$T(c) = T(x^t) + T(x^{t-1}) = 1 + 0 = 1,$$

$$T(ec) = T((1+x)(x^t + x^{t-2})) = T(x^{t+1}) + T(x^{t-1}) = 0.$$

By Lemma 3.2.2,

$$T(eb) = T(x^{t+1}) + T(x^{t-2}) + T(x^{t+2}) + T(x^{t-1}) = 0.$$

□

Theorem 3.2.1 works for some particular orders of generalized Knuth binary semifield. The following corollary lists $f(x)$ in the irreducible polynomials of $x^t + f(x) + 1$ associated with $GF(2^t)$, t odd.

Corollary 3.2.1. *If $f(x)$ in Lemma 3.2.2 exists, then the semifield $(F, +, *)_e$ with e, b, and c as given above is a fractional semifield of order 2^t for each odd $t \geq 1$. Examples of such $f(x)$ include:*

$t = 7, 9, 15,$	$f(x) = x + 1$
$t = 11,$	$f(x) = x^5 + x^3 + x + 1$
$t = 13,$	$f(x) = x^7 + x^3 + x + 1$
$t = 17, 25, 31,$	$f(x) = x^3 + 1$
$t = 19,$	$f(x) = x^9 + x^7 + x + 1$
$t = 21,$	$f(x) = x^7 + 1$
$t = 23,$	$f(x) = x^5 + 1$
$t = 27,$	$f(x) = x^9 + x^5 + x^3 + 1$
$t = 29,$	$f(x) = x^{27} + x + 1$

In fact, everything won't be lost even if $f(x)$ has at least one monomial with even degree. For example, for $F = GF(2^{13})$ we can choose the irreducible polynomial $x^{13} + x^4 + x^3 + x + 1$ over $GF(2)$ to generate F, and choose

$$e = 1 + x^{11},\ b = 1 + x + x^7 + x^9,\ c = x^7 + x^9$$

The corresponding generalized Knuth semifield of order 2^{13} also admits a subfield of order 4.

3.3 The Classical Knuth Binary Semifields without Fractional Dimension

In this section, we prove the following main result:

Theorem 3.3.1. *Let $\mathcal{F} = (GF(2^t), +, *)$ be the classical Knuth binary semifield, t odd. Then for any k, $1 < k < t$, there does not exist a subsemifield of order 2^k in $\mathcal{F}$.*

Proof. The proof of this theorem utilizes the following two lemmas. □

Lemma 3.3.1. *$R_1^{-1}(d^2) = (R_1^{-1}(d))^2$ for any $d \in GF(2^t)$.*

Proof. Let $x = R_1^{-1}(d)$ and $y = R_1^{-1}(d^2)$. We need to show $y = x^2$, where x^2 is the product in the field.

$$\begin{aligned} x = R_1^{-1}(d) &\Rightarrow x \circ 1 = d \\ &\Rightarrow x + (x^T + 1^T x)^2 = d \\ &\Rightarrow x + x^2 + x^T = d \ \ ((x^T)^2 = (x^2)^T = x^T) \\ &\Rightarrow x^2 + x^4 + x^T = d^2 \end{aligned}$$

Since $y = R_1^{-1}(d^2)$, we have

$$y + (y^T + y)^2 = d^2 \textit{ and } y + y^2 + y^T = d^2$$

So $y + y^2 + y^T = x^2 + x^4 + x^T$ and $(y + x^2) + (y + x^2)^2 = x^T + y^T$

Let $a = y + x^2$; then $a + a^2 = x^T + y^T \in GF(2)$.

If $x^T + y^T = 1$, then $a + a^2 = 1$, which implies that a is a root of the polynomial $x^2 + x + 1$. So there is a subfield $GF(2^2)$ in $GF(2^t)$ generated by $x^2 + x + 1$. But t is odd, so this is impossible. Hence $x^T + y^T = 0$, and $a + a^2 = 0$. So either $a = 0$ or $a = 1$. If $a = 1$, then

$$a^T = (y + x^2)^T = y^T + (x^2)^T = y^T + x^T = 0.$$

But this contradicts the fact that $a^T = 1^T = 1$. Hence $a = 0$, which implies $y + x^2 = 0$ and $y = x^2$. □

Lemma 3.3.2. *In the classical Knuth semifield $\mathcal{F} = (GF(2^t), +, *)$, t odd, let d be any element in $GF(2^t)$, not in $GF(2)$. Then for any k*

$$\{1, x_1, x_2, x_3, \cdots, x_k\}$$

where

$$x_1 = d,\ x_2 = d * d,\ x_3 = x_2 * x_2,\ \cdots,\ x_i = x_{i-1} * x_{i-1}$$

is a linearly independent set over $GF(2)$.

Proof. Suppose $d_1 = R_1^{-1}(d)$ and $d_n = R_1^{-1}(d_{n-1})$. Then

$$d = d_1 \circ 1 = d_1 + (d_1^T + 1^T d_1)^2 = d_1 + d_1^2 + d_1^T \tag{3.2}$$

$$d_n = d_{n-1} \circ 1 = d_{n-1} + (d_{n-1}^T + 1^T d_{n-1})^2 = d_{n-1} + d_{n-1}^2 + d_{n-1}^T \tag{3.3}$$

Note: $d^T = d_1^T = d_2^T = \cdots = d_i^T$, for any i.

<u>Claim 1</u> : $x_i = d_{i-1}^{2^{i-1}}$, $i = 2, 3, \cdots, k$.

Proof: If $i = 2$, then

$$\begin{aligned} x_2 &= d * d = R_1^{-1}(d) \circ R_1^{-1}(d) = d_1 \circ d_1 \\ &= d_1^2 + (d_1^T d_1 + d_1^T d_1)^2 = d_1^2 \end{aligned}$$

Suppose $x_{i-1} = d_{i-2}^{2^{i-2}}$, then for i,

$$\begin{aligned} x_i &= x_{i-1} * x_{i-1} = R_1^{-1}(x_{i-1}) \circ R_1^{-1}(x_{i-1}) \\ &= R_1^{-1}(d_{i-2}^{2^{i-2}}) \circ R_1^{-1}(d_{i-2}^{2^{i-2}}) \\ &= (R_1^{-1}(d_{i-2}))^{2^{i-2}} \circ (R_1^{-1}(d_{i-2}))^{2^{i-2}} \\ &= (d_{i-1})^{2^{i-2}} \circ (d_{i-1})^{2^{i-2}} = (d_{i-1})^{2^{i-1}} \end{aligned}$$

<u>Claim 2</u> : $\{1, d, x_2, x_3, \cdots, x_k\}$ is linearly independent over $GF(2)$.

Suppose $a_0 * 1 + a_1 * d + a_2 * x_2 + \cdots + a_k * x_k = 0$, $a_i \in GF(2)$. Then by Claim 1, we have

$$a_0 + a_1 * d + a_2 * (d_1^2) + a_3 * (d_2^4) + \cdots + a_k * (d_{k-1}^{2^{k-1}}) = 0 \tag{3.4}$$

Simplify the left hand side of Equality (3.4) as follows.

First by Equality (3.2), replace d by d_1 and we get the left hand side of Equality (3.4) to be

$$a_0 + a_1 * d_1^T + *a_1 * d_1 + (a_1 + a_2) * d_1^2 + a_3 * d_2^4 + + \cdots + a_k * x_k \tag{3.5}$$

Let $P_1 = a_0 + a_1 * d^T + *a_1 * d_1 + (a_1 + a_2) * d_1^2$.

Next by Equality (3.3), replace d_1 by d_2 and we get the left hand side of Equality (3.4) to be

$$a_0 + (a_1 + a_2) * d^T + a_1 * d_2 + a_2 * d_2^2 + (a_1 + a_2 + a_3) * d_2^4 + a_4 * d_3^8 + \cdots + a_k * x_k \tag{3.6}$$

Let $P_2 = a_0 + (a_1 + a_2) * d^T + a_1 * d_2 + a_2 * d_2^2 + (a_1 + a_2 + a_3) * d_2^4$

Repeating the same procedure and replacing d_{i-1} by d_i according to Equality (3.3), we get the left hand side of Equality (3.4) to be

$$P_i + a_{i+2} * d_{i+1}^{2^{i+1}} + a_{i+3} * d_{i+2}^{2^{i+2}} + \cdots + a_k * x_k \tag{3.7}$$

where

$$P_i = a_0 + (m_{1,i}) * d^T + a_1 * d_i + (m_{2,i}) * d_i^2 + (m_{4,i}) * d_i^4 + \cdots + (m_{2^i,i}) * d_i^{2^i}$$

and

$$\begin{aligned} m_{1,i} &= \ a\ linear\ function\ of\ a_1,\ a_2, \cdots, a_i \\ m_{2,i} &= \ a\ linear\ function\ of\ a_1\ and\ a_2 \\ m_{4,i} &= \ a\ linear\ function\ of\ a_1, a_2,\ and\ a_3 \\ &\vdots \\ m_{2^i,i} &= \ a\ linear\ function\ of\ a_1, a_2, \cdots, a_{i+1} \end{aligned} \tag{3.8}$$

Now we prove that Equation (3.8) is true for any i, where $1 \leq i \leq k$.

Obviously, if $i = 1$ or 2, the above result is true. Suppose it's also true for i; then for $i + 1$, we have

$$\begin{aligned}
P_{i+1} &= a_0 + (m_{1,i}) * d^T + a_1 * (d_{i+1} + d_{i+1}^2 + d^T) \\
&\quad + (m_{2,i}) * (d_{i+1} + d_{i+1}^2 + d^T)^2 + (m_{4,i}) * (d_{i+1} + d_{i+1}^2 + d^T)^4 \\
&\quad + \cdots + (m_{2^i,i}) * (d_{i+1} + d_{i+1}^2 + d^T)^{2^i} + a_{i+2} * d_{i+1}^{2^{i+1}} \\
&= a_0 + (m_{1,i} + a_1 + m_{2,i} + m_{4,i} + \cdots + m_{2^i,i}) * d^T \\
&\quad + a_1 * d_{i+1} + (a_1 + m_{2,i}) * d_{i+1}^2 + (m_{2,i} + m_{4,i}) * d_{i+1}^4 \\
&\quad + \cdots + (m_{2^{i-1},i} + m_{2^i,i}) * d_{i+1}^{2^i} + (m_{2^i,i} + a_{i+2}) * d_{i+1}^{2^{i+1}}
\end{aligned}$$

So

$$\begin{aligned}
m_{1,i+1} &= m_{1,i} + a_1 + m_{2,i} + m_{4,i} + \cdots + m_{2^i,i} \\
&= a\ linear\ function\ of\ a_1,\ a_2, \cdots, a_{i+1} \\
m_{2,i+1} &= a_1 + m_{2,i} = \ a\ linear\ function\ of\ a_1\ and\ a_2 \\
&\vdots
\end{aligned}$$

$$\begin{aligned}
m_{2^i,i+1} &= m_{2^{i-1},i} + m_{2^i,i} = \ a\ linear\ function\ of\ a_1, a_2, \cdots, a_{i+1} \\
m_{2^{i+1},i+1} &= m_{2^i,i} + a_{i+2} = \ a\ linear\ function\ of\ a_1, a_2, \cdots, a_{i+2}
\end{aligned}$$

Also, for all j between 1 and $i+1$, by the construction of $m_{2^j,i+1}$, the term a_{j+1} occurs in $m_{2^j,i+1}$.

Hence, the left hand side of Equality (3.4) can be represented as a polynomial of d_{k-1}, so

$$a_0 * 1 + a_1 * d + a_2 * x_2 + \cdots + a_k * x_k = 0,\ a_i \in GF(2)$$

is equivalent to $P_{k-1} = 0$. Therefore, all the coefficients of P_{k-1} must be 0. Then we get

$$\begin{aligned}
&a_0 + m_{1,k-1}(a_1, a_2, \cdots, a_{k-1}) = 0\\
&a_1 = 0\\
&m_{2,k-1}(a_1, a_2) = 0\\
&m_{4,k-1}(a_1, a_2, a_3) = 0\\
&\vdots\\
&m_{2^{k-1},k-1}(a_1, a_2, \cdots, a_k) = 0
\end{aligned}$$

This linear system has a unique solution $a_0 = a_1 = \cdots = a_k = 0$. □

Now we can prove Theorem 3.3.1.

Proof. Suppose for some $1 < k < t$, the classical Knuth binary semifield $\mathcal{F}$ admits a sub-semifield S_k of order 2^k. Let $d \in S_k$, but $d \notin GF(2)$. Then by Lemma 3.3.2,

$$\{1, x_1, x_2, x_3, \cdots, x_{k-1}\}$$

is linearly independent and

$$\begin{aligned}
&x_1 = d \in S_k\\
&x_2 = x_1 * x_1 \in S_k\\
&\vdots\\
&x_{k-1} = x_{k-2} * x_{k-2} \in S_k
\end{aligned}$$

So $\{1, x_1, x_2, x_3, \cdots, x_{k-1}\}$ can be viewed as a basis of S_k over $GF(2)$. Therefore,

$$x_k = x_{k-1} * x_{k-1} \in S_k$$

which implies that x_k should be a linear combination of $\{1, x_1, x_2, x_3, \cdots, x_{k-1}\}$. This is a contradiction to Lemma 3.3.2. □

Corollary 3.3.1. *For the classical Knuth binary semifield $\mathcal{F} = (GF(2^t), +, *)$, t odd, which is a vector space over $GF(2)$, $N_l = N_r = N_m = GF(2)$.*

It is uncommon for a semifield to admit no sub-semifields; we give a special name for such a semifield.

Definition 3.3.1. *Suppose $\mathcal{S} = (D, +, *)$ is a semifield. Then $\mathcal{S}$ is said to be simple if $\mathcal{S}$ has no any proper sub-semifield.*

Rúa [15] showed that a semifield, 3-dimensional over its center, is both right and left primitive; obviously, a 3-dimensional semifield over its center is never fractional dimensional. V.Jha and M. Cordero [6] proved that a 5-dimensional semifield over its center $GF(q)$, which is not fractional dimensional, is both right and left primitive if q is large enough. Following Theorem 3.3.1, we have the following conjecture.

Conjecture 3.3.1. *Let $\mathcal{S}$ be a simple semifield, n-dimensional over its center $GF(q)$. When q is large enough, $\mathcal{S}$ is both left and right primitive.*

Lemma 3.3.3. *The classical Knuth binary semifield $S_1 = (F, +, *)$ and the generalized Knuth binary semifield $S_2 = (F, +, *')$, where $F = GF(2^t)$, $t \geq 5$ odd, are isotopic.*

Proof. By Lemma 1.2.1 and Lemma 1.2.2, we just need to show that the classical Knuth binary pre-semifield $P_1 = (F, +, \circ)$ and the generalized Knuth binary pre-semifield $P_2 = (F, +, \odot)$ are isotopic. Let B, C be any two mappings in $GL(F, +)$. By the definition of $\odot$,

$$x \odot y = x^B y^C + (x^{BT} y^C + y^{CT} x^B)^2 = (x^B) \circ (y^C)$$

We get that P_1 and P_2 are isotopic with isotopism (B, C, I). □

By Albert's Theorem, the classical Knuth binary semifield S_1, which is commutative, and the generalized Knuth binary semifield S_2, which is not commutative, coordinatize isomorphic planes, π_1 and π_2, respectively. Theorem 3.3.1 tells us π_1 is never fractional dimensional, but π_2, by Theorem 3.2.1, contains $GF(2^2)$ when $t \in [5, 31]$. In fact, V. Jha [19] proved that for any odd integer t, the generalized Knuth binary semifields always contain $GF(2^2)$, so π_2 is always fractional dimensional.

Notice that we have found two isotopic semifields, one commutative and not fractional dimensional, and the other noncommutative and fractional dimensional that coordinatize isomorphic planes. Hence **isomorphic semifield planes may have very different algebraic structures coordinating them**.

3.4 The Generalized Knuth Binary Semifields Without Fractional Dimension

In this section, we prove that a special subclass of generalized Knuth binary semifields, where B, C leave the trace kernel Γ invariant, do not contain the subfields $GF(2^2)$ or $GF(2^3)$.

Definition 3.4.1. *If $(F, +, \circ)$ is an arbitrary pre-semifield, then the twister of any $e \in F^*$ is the unique function $\nu_e : F \to F$ specified by*

$$f \circ e = e \circ f^{\nu_e}, \ for\ every\ f \in F$$

Result 3.4.1. *[19 Remark 4.1] For any pre-semifield $(F, +, \circ)$, the twister ν_e belong to $GL(F, +)$.*

For the generalized Knuth pre-semifield $\mathcal{F}_{B,C}(F) = (F, +, \odot)$, where $B, C \in GL(F, +)_\Gamma$, the corresponding twister is sometimes denoted by $\nu_e^{(B,C)}$, to emphasize the dependency of ν_e on the choice of (B, C).

If the choice of (B, C) is clear from the context, we just write ν_e instead of $\nu_e^{(B,C)}$.

Result 3.4.2. *[19 Corollary 4.3] Suppose $e \in \Gamma^*$ and $e^B = e^C$, $B, C \in GL(F,+)_\Gamma$. Then the left and right multiplication by e in the generalized Knuth pre-semifield $\mathcal{F}_{B,C}(F)$ are specified as follows.*

$$(1)\ For\ all\ f \in F,\ f^{\nu_e^{(B,C)}} = f^{BC^{-1}}.$$

$$(2)\ For\ all\ f \in F,\ e \circ f = f^{CB^{-1}} \circ e.$$

In this section, we prove that the generalized Knuth binary semifield $\mathcal{F}^{(e)}_{B,C}(F) = (F,+,*)_e$ is commutative when $e \in \Gamma^*$ and $e^B = e^C$, for $B, C \in GL(F,+)_\Gamma$. We also show that it does not admit $GF(2^2)$ or $GF(2^3)$.

Lemma 3.4.1. *Suppose $e \in \Gamma^*$ and $e^B = e^C$, $B, C \in GL(F,+)_\Gamma$. Then the generalized Knuth binary semifield $\mathcal{F}^{(e)}_{B,C}(F) = (F,+,*)_e$ is commutative.*

Proof. For any $f, g \in F$, we show $(e \odot f) * (e \odot g) = (e \odot g) * (e \odot f)$.

$$\begin{aligned}
(e \circ f) * (e \circ g) &= (f^{CB^{-1}} \circ e) * (e \circ g)\ (by\ Result\ 3.4.2)\\
&= f^{CB^{-1}} \circ g\\
&= (f^{CB^{-1}})^B g^C + ((f^{CB^{-1}})^{BT} g^C + g^{CT} f^{CB^{-1}})^2\\
&= f^C g^C + (f^{CT} g^C + g^{CT} f^C)^2
\end{aligned}$$

On the other hand,

$$\begin{aligned}
(e \circ g) * (e \circ f) &= (g^{CB^{-1}} \circ e) * (e \circ f)\ (by\ Result\ 3.4.2)\\
&= g^{CB^{-1}} \circ f\\
&= (g^{CB^{-1}})^B f^C + ((g^{CB^{-1}})^{BT} f^C + f^{CT} g^{CB^{-1}})^2\\
&= g^C f^C + (g^{CT} f^C + f^{CT} g^C)^2
\end{aligned}$$

Obviously, $f^C g^C = g^C f^C$, which implies $(e \circ f) * (e \circ g) = (e \circ g) * (e \circ f)$. □

Theorem 3.4.1. *For any odd integer n, with the hypothesis of Lemma 3.4.1, the generalized Knuth binary semifield $\mathcal{F}^{(e)}_{B,C}(F) = (F, +, *)_e$ does not contain the finite field $GF(2^2)$.*

Proof. Since $(F^*, \odot)$ is a loop, for any $d \neq 0$, there is a unique $f \in F^*$ such that $d = f \odot e$. If $\{1, d\}$ is a basis of $GF(2^2)$, then

$$d \notin GF(2) \text{ and } d * d = d + 1 \tag{3.9}$$

where $1 = e \odot e$ is the identity of the generalized Knuth binary semifield $\mathcal{F}^{(e)}_{B,C}(F) = (F, +, *)_e$.

We prove

$$d^2 = d + 1, \text{ i.e., } (f \odot e)^{2)} = f \odot e + e \odot e \tag{3.10}$$

where $(f \odot e)^{2)} = (f \odot e) * (f \odot e)$, never has a solution in the generalized Knuth binary semifield $\mathcal{F}^{(e)}_{B,C}(F) = (F, +, *)_e$.

$$\begin{aligned}
(f \odot e)^{2)} &= (f \odot e) * (e \odot f^{\nu_e}) \;=\; f \odot f^{\nu_e} \\
&= f^B f^{\nu_e C} + (f^{BT} f^{\nu_e C} + f^{\nu_e CT} f^B)^2 \\
&= f^B (f^{BC^{-1}})^C + (f^{BT} f^{BC^{-1}C} + f^{BC^{-1}CT} f^B)^2 \\
&= f^B f^B = (f^B)^2 \\
f \odot e + e \odot e &= f^B e^C + (f^{BT} e^C + e^{CT} f^B)^2 + e^B e^C + (e^{BT} e^C + e^{CT} e^B)^2 \\
&= f^B e^C + f^{BT} (e^C)^2 + e^B e^C \\
&= f^B e^B + f^{BT} (e^B)^2 + (e^B)^2
\end{aligned}$$

Case 1: When $f \in \Gamma$. If (3.10) is true, then $(f^B)^2 + f^B e^B + (e^B)^2 = 0$. Since n is odd, the above equation never has a solution in the finite field $F = GF(2^n)$.

Case 2: When $f \notin \Gamma$. Then $f \odot e + e \odot e = f^B e^B + (e^B)^2 + (e^B)^2 = f^B e^B$. If (3.10) is true, then $(f^B)^2 = f^B e^B$, and so $f^B = 0$ or $f^B = e^B$. Hence $f = 0$ or $f = e$, since $B \in GL(F, +)$, and then implies $d = 0$ or $d = e \odot e$. □

Lemma 3.4.2. *Suppose $e \in \Gamma^*$ and $e^B = e^C$, $B, C \in GL(F,+)_\Gamma$. For any $f \in F$, let $f_1 \odot e = f$. Then*

$$f_1 = \begin{cases} (\frac{f}{e^C})^{B^{-1}}, & if\ f_1 \in \Gamma, \\ (\frac{f}{e^C})^{B^{-1}} + e, & if\ f_1 \notin \Gamma. \end{cases}$$

Proof. If $f_1 \odot e = f$, then

$$\begin{aligned} f &= f_1^B e^C + (f_1^{BT} e^C + e^{CT} f_1^B)^2 \\ &= f_1^B e^C + f_1^{BT} (e^C)^2 \end{aligned}$$

<u>Case 1</u>: if $f_1 \in \Gamma$, then $f = f_1^B e^C$ and $f_1^B = \frac{f}{e^C}$. So $f_1 = (\frac{f}{e^C})^{B^{-1}}$.

<u>Case 2</u>: if $f_1 \notin \Gamma$, then $f = f_1^B e^C + (e^C)^2$ and $f_1^B = \frac{f + (e^C)^2}{e^C}$. So

$$f_1 = (\frac{f}{e^C})^{B^{-1}} + (e^C)^{B^{-1}} = (\frac{f}{e^C})^{B^{-1}} + e.$$

□

Theorem 3.4.2. *For any odd integer n, with the hypothesis of Lemma 3.4.1, the generalized Knuth binary semifield $\mathcal{F}_{B,C}^{(e)}(F) = (F, +, *)_e$ does not contain the finite field $GF(2^3)$ when $(n, 3) = 1$.*

Proof. By Theorem 3.4.1, for any $d \in F - GF(2)$, $\{1, d, d^{2)}\}$ is linearly independent, so this set can be viewed as a basis of $GF(2^3)$ over $GF(2)$. Any finite field $GF(q^n)$, q is a prime power, can be constructed by an irreducible polynomial over $GF(q)$. For the finite field $GF(2^3)$, there are only 2 irreducible polynomials over $GF(2)$:

$$x^3 + x + 1 \quad and \quad x^3 + x^2 + 1.$$

Without lost of generality, let d be a root of $g(x) = x^3 + x + 1$, which is the irreducible polynomial for the field extension from $GF(2)$ to $GF(2^3)$.

For any $d \in F - GF(2)$, let $d = f \odot e$. In order to prove this theorem, we just need to show that the equation

$$(f \odot e)^{3)} + f \odot e + e \odot e = 0 \tag{3.11}$$

has no solution in $F = GF(2^n)$, when $(n, 3) = 1$.

By the computation in Theorem 3.4.1,

$$f \odot e + e \odot e = f^B e^B + f^{BT}(e^B)^2 + (e^B)^2 \tag{3.12}$$

and

$$(f \odot e)^{2)} = (f^B)^2 \tag{3.13}$$

<u>Case 1</u>: if $f \in \Gamma$, then $f \odot e + e \odot e = f^B e^B + (e^B)^2$. Let $f_1 \odot e = (f \odot e)^{2)}$. If $f_1 \in \Gamma$, then by Lemma 3.4.2, $f_1 = (\frac{(f^B)^2}{e^B})^{B^{-1}}$ and

$$\begin{aligned}(f \odot e)^{3)} &= (f \odot e)^{2)} * (f \odot e) \\ &= (f_1 \odot e)^{2)} * (e \odot f^{\nu_e}) \ = \ f_1 \odot f^{\nu_e} \\ &= f_1^B f^{\nu_e C} + (f_1^{BT} f^{\nu_e C} + f^{\nu_e CT} f_1^B)^2 \\ &= (\frac{(f^B)^2}{e^B}) f^B \ = \ \frac{(f^B)^3}{e^B}\end{aligned}$$

So if (3.11) is true, then

$$\frac{(f^B)^3}{e^B} + f^B e^B + (e^B)^2 = 0 \tag{3.14}$$

and

$$(f^B)^3 + f^B(e^B)^2 + e^B)^3 = 0 \tag{3.15}$$

Let $z = \frac{f^B}{e^B}$. Since $e \neq 0$ and B is a bijection on F, $e^B \neq 0$. Then dividing by $(e^B)^3$ in both sides of equation (3.15), we get $z^3 + z + 1 = 0$. This equation has no solution in F because $(n, 3) = 1$.

If $f_1 \notin \Gamma$, then by Lemma 3.4.2, $f_1 = (\frac{(f^B)^2}{e^B})^{B^{-1}} + e$ and

$$\begin{aligned}(f \odot e)^{3)} &= (f \odot e)^{2)} * (f \odot e) \ = \ f_1 \odot f^{\nu_e} \\ &= f_1^B f^{\nu_e C} + (f_1^{BT} f^{\nu_e C} + f^{\nu_e CT} f_1^B)^2\end{aligned}$$

$$\begin{aligned}
&= (f_1^B)f^B + (f^{\nu_e C})^2 \ = \ (f_1^B)f^B + (f^B)^2 \\
&= (\frac{(f^B)^2}{e^B} + e^B)f^B + (f^B)^2 \\
&= \frac{(f^B)^3}{e^B} + e^B f^B + (f^B)^2
\end{aligned}$$

So if equation (3.11) is true, then

$$\frac{(f^B)^3}{e^B} + e^B f^B + (f^B)^2 + f^B e^B + (e^B)^2 = 0 \tag{3.16}$$

and

$$\frac{(f^B)^3}{e^B} + (f^B)^2 + (e^B)^2 = 0 \tag{3.17}$$

Hence $(\frac{f^B}{e^B})^3 + (\frac{f^B}{e^B})^2 + 1 = 0$. This equation has no solution in F because $(n, 3) = 1$.

Case 2: if $f \notin \Gamma$, then $f \odot e + e \odot e = f^B e^B$. Let $f_1 \odot e = (f \odot e)^{2)}$.

If $f_1 \in \Gamma$, then by Lemma 3.4.2, $f_1 = (\frac{(f^B)^2}{e^B})^{B^{-1}}$ and so

$$\begin{aligned}
(f \odot e)^{3)} &= f_1 \odot f^{\nu_e} \\
&= f_1^B f^{\nu_e C} + (f_1^{BT} f^{\nu_e C} + f^{\nu_e CT} f_1^B)^2 \\
&= (f_1^B)f^B + (f_1^B)^2 \\
&= (\frac{(f^B)^2}{e^B})f^B + (\frac{(f^B)^2}{e^B})^2 \\
&= \frac{(f^B)^3 e^B + (f^B)^4}{(e^B)^2}
\end{aligned}$$

So if equation (3.11) is true, then

$$\frac{(f^B)^3 e^B + (f^B)^4}{(e^B)^2} + f^B e^B = 0 \tag{3.18}$$

and

$$f^B[(f^B)^3 + e^B(f^B)^2 + (e^B)^3] = 0 \tag{3.19}$$

Since $f \neq 0$ and B is a bijection on F, then $f^B \neq 0$. Hence equation (3.19) can be simplified as

$$(f^B)^3 + e^B(f^B)^2 + (e^B)^3 = 0 \tag{3.20}$$

However, equation (3.20) has no solution in F because $(n,3)=1$.

If $f_1 \notin \Gamma$, then by Lemma 3.4.2, $f_1 = (\frac{(f^B)^2}{e^B})^{B^{-1}} + e$ and

$$\begin{aligned}(f \odot e)^{3)} &= f_1 \odot f^{\nu_e} \\ &= f_1^B f^{\nu_e C} + (f_1^{BT} f^{\nu_e C} + f^{\nu_e CT} f_1^B)^2 \\ &= (f_1^B) f^B + (f^B)^2 + (f_1^B)^2 \\ &= (\frac{(f^B)^2}{e^B} + e^B) f^B + (f^B)^2 + (\frac{(f^B)^2}{e^B} + e^B)^2 \\ &= \frac{(f^B)^3}{e^B} + \frac{(f^B)^4}{(e^B)^2} + f^B e^B + (f^B)^2 + (e^B)^2\end{aligned}$$

If (3.11) is true, then

$$\begin{aligned}&\frac{(f^B)^3}{e^B} + \frac{(f^B)^4}{(e^B)^2} + (f^B)^2 + (e^B)^2 = 0 \\ \Rightarrow &(f^B)^3 e^B + (f^B)^4 + (e^B)^4 + (f^B)^2 (e^B)^2 = 0 \\ \Rightarrow &(f^B + e^B)[(f^B)^3 + f^B (e^B)^2 + (e^B)^3] = 0\end{aligned}$$

Since B is a bijection on F and $f^B \neq e^B$, then we have $f^B + e^B \neq 0$, and

$$(f^B)^3 + f^B (e^B)^2 + (e^B)^3 = 0 \tag{3.21}$$

Similarly the equation above has no solution in F. □

3.5 The Albert Semifields Without Fractional Dimension

Wene [17] proved that any Albert semifield $A_n(S)$, n odd, where S is a $(n-1)$-dimensional vector space over $GF(2)$ containing 1, never contains a field of order 4. We have the following result:

Theorem 3.5.1. *For any odd integer n, where $(n,3)=1$, it's impossible for the Albert semifield $A_n(S)$, where S is a $(n-1)$-dimensional vector space over $GF(2)$ containing 1, to contain the finite field $GF(2^3)$.*

Proof. Since $GF(4)$ is not contained in any Albert semifield $A_n(S)$, for any $d \notin GF(2)$, $\{1, d, d * d\}$ is linearly independent. Hence this set can be viewed as a $GF(2)$-basis of the finite field $GF(2^3)$. Suppose the finite field $GF(2^3)$ is generated by the irreducible polynomial $f(x) = x^3 + x + 1$ over $GF(2)$ and d is a zero of $f(x)$.

We show all the elements d in the Albert semifield A_n, when $(n, 3) = 1$, can not be a root of the equation $x^3 + x + 1 = 0$.

There are a total of 4 cases to consider:

$$(i)\ d, d * d \in S; \qquad (ii)\ d \in S, d * d \notin S;$$

$$(iii)\ d \notin S, , d * d \in S; \qquad (iv)\ d, d * d \notin S$$

Case i: If $d, d * d \in S$, then $\{1, d, d * d\} \subseteq S$, so a subfield $GF(2^3)$ is contained in $GF(2^n)$. But this is impossible since $(n, 3) = 1$.

Case ii: If $d \in S$, but $d * d = d^2 \notin S$. Suppose $d * d = \omega + t$ for some $t \in S$, then

$$\begin{aligned} d^{3)} &= (\omega + t) * d = \omega * d + t * d \\ &= \omega d + d^2 + d + td \end{aligned}$$

If $d^{3)} = d + 1$, then

$$\begin{aligned} \omega d + d^2 + d + td = d + 1 &\Rightarrow \omega d + d^2 + td + 1 = 0 \\ &\Rightarrow d^2 + (\omega + t)d + 1 = 0 \\ &\Rightarrow d^2 + (d^2)d + 1 = 0,\ \textit{i.e.},\ d^3 + d^2 + 1 = 0 \end{aligned}$$

Hence d is a root of the irreducible polynomial $g(x) = x^3 + x^2 + 1$ over $GF(2)$, which implies $GF(2^3)$ is in $GF(2^n)$. But this contradicts the fact that $(n, 3) = 1$.

If $d \notin S$, suppose $d = \omega + d_1$ for some $d_1 \in S$, then

$$d * d = (\omega + d_1) * (\omega + d_1) = \omega^2 + d_1^2 + 1$$

Case iii: If $d \notin S$, but $d * d \in S$. Then

$$\begin{aligned} d^{3)} &= d^{2)} * d = (\omega^2 + d_1^2 + 1) * (\omega + d_1) \\ &= (\omega^2 + d_1^2 + 1)\omega + (\omega^2 + d_1^2 + 1)^2 + (\omega^2 + d_1^2 + 1) + (\omega^2 + d_1^2 + 1)d_1 \\ &= (\omega^2 + d_1^2 + 1)[(\omega^2 + d_1^2 + 1) + (\omega + d_1 + 1)] \end{aligned}$$

If $d^{3)} = d + 1$, then

$$(\omega^2 + d_1^2 + 1)[(\omega^2 + d_1^2 + 1) + (\omega + d_1 + 1)] = \omega + d_1 + 1$$

Since $d \notin GF(2)$, $d + 1 = \omega + d_1 + 1 \neq 0$ and then

$$\begin{aligned} &(\omega + d_1 + 1)[(\omega^2 + d_1^2 + 1) + (\omega + d_1 + 1)] = 1 \\ &\Rightarrow (\omega + d_1 + 1)[(\omega + d_1 + 1)(\omega + d_1)] = 1 \\ &\Rightarrow (d + 1)[(d + 1)d] = 1, \ \textit{i.e.}, \ d^3 + d + 1 = 0 \end{aligned}$$

The equation above implies that $GF(2^3)$ is contained in $GF(2^n)$. But this contradicts the fact that $(n, 3) = 1$.

Case iv: If $d, d * d \notin S$. Then $d * d = (\omega + d_1) * (\omega + d_1) = \omega^2 + d_1^2 + 1$. Let $d * d = \omega + p$ for some $p \in S$; so $p = \omega^2 + \omega + d_1^2 + 1$ and then

$$\begin{aligned} d^{3)} &= d^{2)} * d = (\omega + p) * (\omega + d_1) \\ &= \omega * \omega + \omega * (p + d_1) + p * d_1 \\ &= \omega^2 + 1 + (p + d_1)\omega + (p + d_1)^2 + (p + d_1) + pd_1 \end{aligned}$$

If $d^{3)} = d + 1$, then

$$\begin{aligned} &\omega^2 + (p + d_1)\omega + (p + d_1)^2 + (p + d_1) + pd_1 = \omega + d_1 \\ &\Rightarrow \omega^2 + (\omega^2 + \omega + d_1^2 + 1 + d_1)\omega + (\omega^2 + \omega + d_1^2 + 1 + d_1)^2 + (\omega^2 + \omega + d_1^2 + 1 + d_1) \\ &+ (\omega^2 + \omega + d_1^2 + 1)d_1 = \omega + d_1 \end{aligned}$$

$$\Rightarrow \omega^4+\omega^3+\omega(d_1^2+d_1+1)+(d_1^2+d_1+1)^2+(d_1^2+d_1+1)+(\omega^2+\omega)d_1+d_1^3=0$$

$$\Rightarrow (\omega^4+d_1^4)+(\omega^3+\omega d_1^2+\omega^2 d_1+d_1^3)+(\omega+d_1)=0$$

$$\Rightarrow (\omega+d_1)^4+(\omega+d_1)^3+(\omega+d_1)=0$$

Since $d=\omega+d_1\neq 0$,then the equation above is $d^3+d^2+1=0$, which implies that $GF(2^3)$ is contained in $GF(2^n)$. But again this is impossible because $(n,3)=1$. □

CHAPTER 4

CONCLUSIONS AND FUTURE WORK

4.1 Conclusions

In Chapter II, we focused on the the problem of right primitivity for finite semifields. After providing the basic definition of primitivity of finite semifields, we proved the main theorem of the chapter, which provided an equivalent condition for right primitivity of finite semifields (Section 2.2). With this result, we investigated the primitivity of the classical Knuth binary semifields of order 2^n, where $n = 15, 17, 19$ (Section 2.3), and the Albert semifields of order 2^n, where $n = 7, 9, 11, 13$ (Section 2.5). Also for the primitive classical Knuth binary semifields we exhibited a formula to describe the number of primitive elements (Section 2.4). Finally, we investigated some properties of automorphisms of right primitive semifields (Section 2.6).

In Chapter III, we provided some new results on the dimension of finite semifields. Let $F = GF(2^n)$, where n is an odd positive integer. First, the classical Knuth binary semifields $\mathcal{F} = (F, +, *)$, which is an n-dimensional vector space over $GF(2)$, does not contain any sub-semifields (Section 3.3). Next, we considered two special classes of the generalized Knuth binary semifields $\mathcal{F}^{(e)}_{B,C}(F) = (F, +, *)_e$, where $B, C \in GL(F, +)$ and e is a nonzero element in F. Each semifield in the first class contains the subfield $GF(2^2)$, when $n \in [5, 31]$; hence this class is fractional dimensional(Section 3.2). The semifield in the second class do not contain the subfield $GF(2^2)$ or $GF(2^3)$ (Section 3.4). Finally, we proved that the Albert semifields do not contain subfields $GF(2^3)$ either (Section 3.5).

4.2 Future Work

Until now, all semifields that do not admit the finite fields $GF(2^2)$ or $GF(2^3)$ are commutative. Some interesting problems to explore are the following.

- Let S be a commutative semifield. Is it possible for S to be fractional dimensional?
- If π_1 and π_2 are two semifield planes coordinatized by 2 commutative finite semifields, can π_1 and π_2 be absolutely isomorphic? (See Definition 1.1.2)

APPENDIX A

MATLAB PROGRAM FOR $\mathcal{F} = (GF(2^{15}), +, *)$

In this appendix, we present a Matlab program to get all the distinct right characteristic polynomials of all the elements in the classical Knuth binary semifield $\mathcal{F} = (GF(2^{15}), +, *)$.

```
B = [ ];j = 0;
for i0 = 0 : 1
for i1 = 0 : 1
for i2 = 0 : 1
for i3 = 0 : 1
for i4 = 0 : 1
for i5 = 0 : 1
for i6 = 0 : 1
for i7 = 0 : 1
for i8 = 0 : 1
for i9 = 0 : 1
for i10 = 0 : 1
for i11 = 0 : 1
for i12 = 0 : 1
for i13 = 0 : 1
for i14 = 0 : 1
j = j + 1;
p = poly(i0 * A0 + i1 * A1 + i2 * A2 + i3 * A3 + i4 * A4 + i5 * A5 + i6 * A6 + i7 * A7 +
i8 * A8 + i9 * A9 + i10 * A10 + i11 * A11 + i12 * A12 + i13 * A13 + i14 * A14);
p = round(p);
r = abs(mod(p, 2));
B(j, :) = r;
```

```
unique(B, ‘rows’)
end
end
end
end
end
end
end
end
end
end
end
end
end
end
end
```

APPENDIX B

MATLAB PROGRAM FOR $A_7(S)$

In this appendix, we present a Matlab program to get all the distinct right characteristic polynomials of all the elements in the Albert semifield $A_7(S)$.

```
for i0 = 0 : 1
for i1 = 0 : 1
for i2 = 0 : 1
for i3 = 0 : 1
for i4 = 0 : 1
for i5 = 0 : 1
for i6 = 0 : 1
A = i0 * R0 + i1 * R1 + i2 * R2 + i3 * R3 + i4 * R4 + i5 * R5 + i6 * R6;
p = poly(rem(A, 2));
r = round(rem(p, 2))
end
end
end
end
end
end
end
```

APPENDIX C

PRIMITIVE ELEMENTS IN $\mathcal{F} = (GF(2^7), +, *)$

In this appendix, we present all the primitive elements in the Knuth binary semifield $\mathcal{F} = (GF(2^7), +, *)$. The irreducible polynomial $f(x) = x^7 + x + 1$ is chosen to be the polynomial associated with the field extension over $GF(2)$. Let ζ be a root of $f(x)$. Then $\{1, \zeta, \zeta^2, \cdots, \zeta^6\}$ is a $GF(2)$-basis of $GF(2^7)$.

Primitive elements in the Knuth binary semifield of order 2^7

ζ

$1 + \zeta$

ζ^2

$\zeta + \zeta^2$

$1 + \zeta^2$

$1 + \zeta + \zeta^2$

ζ^4

$1 + \zeta^4$

$\zeta + \zeta^4$

$1 + \zeta + \zeta^4$

$\zeta^2 + \zeta^4$

$\zeta + \zeta^2 + \zeta^4$

$1 + \zeta^2 + \zeta^4$

$1 + \zeta + \zeta^2 + \zeta^4$

$\zeta^3 + \zeta^4$

$1 + \zeta^3 + \zeta^4$

$\zeta + \zeta^3 + \zeta^4$

$1 + \zeta + \zeta^3 + \zeta^4$

$\zeta^2 + \zeta^3 + \zeta^4$

$\zeta + \zeta^2 + \zeta^3 + \zeta^4$

$1 + \zeta^2 + \zeta^3 + \zeta^4$

$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$

ζ^5

$1 + \zeta^5$

$\zeta + \zeta^5$

$1 + \zeta + \zeta^5$

$\zeta^2 + \zeta^3 + \zeta^5$

$\zeta + \zeta^2 + \zeta^3 + \zeta^5$

$1 + \zeta^2 + \zeta^3 + \zeta^5$

$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^5$

$\zeta^4 + \zeta^5$

$1 + \zeta^4 + \zeta^5$

$\zeta + \zeta^4 + \zeta^5$

$1 + \zeta + \zeta^4 + \zeta^5$

$\zeta^3 + \zeta^4 + \zeta^5$

$1 + \zeta^3 + \zeta^4 + \zeta^5$

$\zeta + \zeta^3 + \zeta^4 + \zeta^5$

$1 + \zeta + \zeta^3 + \zeta^4 + \zeta^5$

$\zeta + \zeta^6$

$1 + \zeta + \zeta^6$

$\zeta + \zeta^2 + \zeta^6$

$1 + \zeta + \zeta^2 + \zeta^6$

$\zeta^3 + \zeta^6$

$1 + \zeta^3 + \zeta^6$

$\zeta^2 + \zeta^3 + \zeta^6$

$1 + \zeta^2 + \zeta^3 + \zeta^6$

$\zeta + \zeta^4 + \zeta^6$

$1 + \zeta + \zeta^4 + \zeta^6$

$\zeta + \zeta^2 + \zeta^4 + \zeta^6$

$1 + \zeta + \zeta^2 + \zeta^4 + \zeta^6$

$\zeta + \zeta^3 + \zeta^4 + \zeta^6$

$1 + \zeta + \zeta^3 + \zeta^4 + \zeta^6$

$\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^6$

$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^6$

$\zeta + \zeta^5 + \zeta^6$

$1 + \zeta + \zeta^5 + \zeta^6$

$\zeta^2 + \zeta^5 + \zeta^6$

$1 + \zeta^2 + \zeta^5 + \zeta^6$

$\zeta^3 + \zeta^5 + \zeta^6$

$1 + \zeta^3 + \zeta^5 + \zeta^6$

$\zeta + \zeta^2 + \zeta^3 + \zeta^5 + \zeta^6$

$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^5 + \zeta^6$

$\zeta + \zeta^4 + \zeta^5 + \zeta^6$

$1 + \zeta + \zeta^4 + \zeta^5 + \zeta^6$

$\zeta^2 + \zeta^4 + \zeta^5 + \zeta^6$

$1 + \zeta^2 + \zeta^4 + \zeta^5 + \zeta^6$

$\zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$

$1 + \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$

$\zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$

$1 + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$

APPENDIX D

PRIMITIVE ELEMENTS IN $\mathcal{F} = (GF(2^9), +, *)$

In this appendix, we present all the primitive elements in the Knuth binary semifield $\mathcal{F} = (GF(2^9), +, *)$. The irreducible polynomial $f(x) = x^9 + x + 1$ is chosen to be the polynomial associated with the field extension over $GF(2)$. Let ζ be a root of $f(x)$. Then $\{1, \zeta, \zeta^2, \cdots, \zeta^8\}$ is a $GF(2)$-basis of $GF(2^9)$.

Primitive elements in the Knuth binary semifield of order 2^9

$\zeta^8, \zeta^7+\zeta^8, \zeta^5+\zeta^6+\zeta^8, \zeta^5+\zeta^6+\zeta^7+\zeta^8, \zeta^4, \zeta^4+\zeta^7, \zeta^4+\zeta^5+\zeta^8, \zeta^4+\zeta^5+\zeta^7, \zeta^4+\zeta^5+\zeta^7+\zeta^8, \zeta^4+\zeta^5+\zeta^6+\zeta^8, \zeta^3+\zeta^6, \zeta^3+\zeta^6+\zeta^7, \zeta^3+\zeta^5+\zeta^6+\zeta^7, \zeta^3+\zeta^5+\zeta^6+\zeta^7+\zeta^8, \zeta^3+\zeta^4+\zeta^6, \zeta^3+\zeta^4+\zeta^6+\zeta^8, \zeta^3+\zeta^4+\zeta^6+\zeta^7, \zeta^3+\zeta^4+\zeta^5, \zeta^3+\zeta^4+\zeta^5+\zeta^8, \zeta^2, \zeta^2+\zeta^6+\zeta^7+\zeta^8, \zeta^2+\zeta^5, \zeta^2+\zeta^5+\zeta^7, \zeta^2+\zeta^5+\zeta^7+\zeta^8, \zeta^2+\zeta^4+\zeta^8, \zeta^2+\zeta^4+\zeta^7, \zeta^2+\zeta^4+\zeta^6+\zeta^7+\zeta^8, \zeta^2+\zeta^4+\zeta^5, \zeta^2+\zeta^4+\zeta^5+\zeta^8, \zeta^2+\zeta^4+\zeta^5+\zeta^7, \zeta^2+\zeta^4+\zeta^5+\zeta^6, \zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^8, \zeta^2+\zeta^3+\zeta^7+\zeta^8, \zeta^2+\zeta^3+\zeta^6, \zeta^2+\zeta^3+\zeta^5+\zeta^6, \zeta^2+\zeta^3+\zeta^4+\zeta^7, \zeta^2+\zeta^3+\zeta^4+\zeta^7+\zeta^8, \zeta^2+\zeta^3+\zeta^4+\zeta^6+\zeta^8, \zeta, \zeta+\zeta^6+\zeta^8, \zeta+\zeta^5, \zeta+\zeta^5+\zeta^6+\zeta^8, \zeta+\zeta^4+\zeta^6+\zeta^8, \zeta+\zeta^4+\zeta^5+\zeta^7, \zeta+\zeta^3+\zeta^8, \zeta+\zeta^3+\zeta^7, \zeta+\zeta^3+\zeta^7+\zeta^8, \zeta+\zeta^3+\zeta^5+\zeta^7, \zeta+\zeta^3+\zeta^5+\zeta^6, \zeta+\zeta^3+\zeta^5+\zeta^6+\zeta^7, \zeta+\zeta^3+\zeta^4+\zeta^7+\zeta^8, \zeta+\zeta^3+\zeta^4+\zeta^6, \zeta+\zeta^3+\zeta^4+\zeta^5, \zeta+\zeta^2+\zeta^7, \zeta+\zeta^2+\zeta^6+\zeta^8, \zeta+\zeta^2+\zeta^6+\zeta^7, \zeta+\zeta^2+\zeta^5+\zeta^6+\zeta^8, \zeta+\zeta^2+\zeta^5+\zeta^6+\zeta^7, \zeta+\zeta^2+\zeta^4, \zeta+\zeta^2+\zeta^4+\zeta^8, \zeta+\zeta^2+\zeta^4+\zeta^7, \zeta+\zeta^2+\zeta^4+\zeta^5+\zeta^6, \zeta+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^8, \zeta+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^7+\zeta^8, \zeta+\zeta^2+\zeta^3+\zeta^8, \zeta+\zeta^2+\zeta^3+\zeta^7, \zeta+\zeta^2+\zeta^3+\zeta^6, \zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^7, \zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^7+\zeta^8, \zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5, \zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^7+\zeta^8, \zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6+\zeta^7+\zeta^8, 1+\zeta^8, 1+\zeta^7, 1+\zeta^7+\zeta^8, 1+\zeta^6, 1+\zeta^6+\zeta^8, 1+\zeta^6+\zeta^7, 1+\zeta^5, 1+\zeta^5+\zeta^7, 1+\zeta^5+\zeta^6, 1+\zeta^5+\zeta^6+\zeta^8, 1+\zeta^5+\zeta^6+\zeta^7+\zeta^8, 1+\zeta^4, 1+\zeta^4+\zeta^8, 1+\zeta^4+\zeta^7, 1+\zeta^4+\zeta^6, 1+\zeta^4+\zeta^5, 1+\zeta^4+\zeta^5+\zeta^8, 1+\zeta^4+\zeta^5+\zeta^7, 1+\zeta^4+\zeta^5+\zeta^7+\zeta^8, 1+\zeta^4+\zeta^5+\zeta^6+\zeta^8, 1+\zeta^4+\zeta^5+\zeta^6+\zeta^7, 1+\zeta^3, 1+\zeta^3+\zeta^7, 1+\zeta^3+\zeta^6, 1+\zeta^3+\zeta^6+\zeta^7, 1+\zeta^3+\zeta^6+\zeta^7+\zeta^8, 1+\zeta^3+\zeta^5, 1+\zeta^3+\zeta^5+\zeta^7+\zeta^8, 1+\zeta^3+\zeta^5+\zeta^6, 1+\zeta^3+\zeta^5+\zeta^6+\zeta^7, 1+\zeta^3+\zeta^5+\zeta^6+\zeta^7+\zeta^8, 1+\zeta^3+\zeta^4, 1+\zeta^3+\zeta^4+\zeta^8, 1+\zeta^3+\zeta^4+\zeta^7+\zeta^8, 1+\zeta^3+\zeta^4+\zeta^6, 1+\zeta^3+\zeta^4+\zeta^6+\zeta^8, 1+\zeta^3+\zeta^4+\zeta^6+\zeta^7, 1+\zeta^3+\zeta^4+\zeta^5, 1+\zeta^3+\zeta^4+\zeta^5+\zeta^8, 1+\zeta^3+\zeta^4+\zeta^5+\zeta^7+\zeta^8, 1+\zeta^3+\zeta^4+\zeta^5+\zeta^6, 1+\zeta^2, 1+\zeta^2+\zeta^6, 1+\zeta^2+\zeta^6+\zeta^7, 1+\zeta^2+\zeta^6+\zeta^7+\zeta^8, 1+\zeta^2+\zeta^5, 1+\zeta^2+\zeta^5+\zeta^7, 1+\zeta^2+\zeta^5+\zeta^7+\zeta^8, 1+\zeta^2+\zeta^4, 1+\zeta^2+\zeta^4+\zeta^8, 1+\zeta^2+\zeta^4+\zeta^7, 1+\zeta^2+\zeta^4+\zeta^7+\zeta^8, 1+\zeta^2+\zeta^4+\zeta^6+$

$\zeta^8, 1+\zeta^2+\zeta^4+\zeta^6+\zeta^7+\zeta^8, 1+\zeta^2+\zeta^4+\zeta^5, 1+\zeta^2+\zeta^4+\zeta^5+\zeta^8, 1+\zeta^2+\zeta^4+\zeta^5+\zeta^7, 1+\zeta^2+\zeta^4+\zeta^5+\zeta^6, 1+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^8, 1+\zeta^2+\zeta^3, 1+\zeta^2+\zeta^3+\zeta^7, 1+\zeta^2+\zeta^3+\zeta^7+\zeta^8, 1+\zeta^2+\zeta^3+\zeta^6, 1+\zeta^2+\zeta^3+\zeta^6+\zeta^8, 1+\zeta^2+\zeta^3+\zeta^6+\zeta^7, 1+\zeta^2+\zeta^3+\zeta^6+\zeta^7+\zeta^8, 1+\zeta^2+\zeta^3+\zeta^5+\zeta^6, 1+\zeta^2+\zeta^3+\zeta^4+\zeta^7, 1+\zeta^2+\zeta^3+\zeta^4+\zeta^7+\zeta^8, 1+\zeta^2+\zeta^3+\zeta^4+\zeta^6+\zeta^8, 1+\zeta^2+\zeta^3+\zeta^4+\zeta^5, 1+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6, 1+\zeta, 1+\zeta+\zeta^6+\zeta^8, 1+\zeta+\zeta^6+\zeta^7, 1+\zeta+\zeta^5, 1+\zeta+\zeta^5+\zeta^6+\zeta^8, 1+\zeta+\zeta^4+\zeta^6+\zeta^8, 1+\zeta+\zeta^4+\zeta^5+\zeta^7, 1+\zeta+\zeta^4+\zeta^5+\zeta^6, 1+\zeta+\zeta^4+\zeta^5+\zeta^6+\zeta^7+\zeta^8, 1+\zeta+\zeta^3, 1+\zeta+\zeta^3+\zeta^8, 1+\zeta+\zeta^3+\zeta^7, 1+\zeta+\zeta^3+\zeta^7+\zeta^8, 1+\zeta+\zeta^3+\zeta^6+\zeta^7, 1+\zeta+\zeta^3+\zeta^5+\zeta^7, 1+\zeta+\zeta^3+\zeta^5+\zeta^6, 1+\zeta+\zeta^3+\zeta^5+\zeta^6+\zeta^7, 1+\zeta+\zeta^3+\zeta^4+\zeta^8, 1+\zeta+\zeta^3+\zeta^4+\zeta^7+\zeta^8, 1+\zeta+\zeta^3+\zeta^4+\zeta^6, 1+\zeta+\zeta^3+\zeta^4+\zeta^5, 1+\zeta+\zeta^3+\zeta^4+\zeta^5+\zeta^8, 1+\zeta+\zeta^3+\zeta^4+\zeta^5+\zeta^6+\zeta^7, 1+\zeta+\zeta^2, 1+\zeta+\zeta^2+\zeta^8, 1+\zeta+\zeta^2+\zeta^7, 1+\zeta+\zeta^2+\zeta^6, 1+\zeta+\zeta^2+\zeta^6+\zeta^8, 1+\zeta+\zeta^2+\zeta^6+\zeta^7, 1+\zeta+\zeta^2+\zeta^5+\zeta^7, 1+\zeta+\zeta^2+\zeta^5+\zeta^7+\zeta^8, 1+\zeta+\zeta^2+\zeta^5+\zeta^6, 1+\zeta+\zeta^2+\zeta^5+\zeta^6+\zeta^8, 1+\zeta+\zeta^2+\zeta^5+\zeta^6+\zeta^7, 1+\zeta+\zeta^2+\zeta^4, 1+\zeta+\zeta^2+\zeta^4+\zeta^8, 1+\zeta+\zeta^2+\zeta^4+\zeta^7, 1+\zeta+\zeta^2+\zeta^4+\zeta^6+\zeta^8, 1+\zeta+\zeta^2+\zeta^4+\zeta^5+\zeta^6, 1+\zeta+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^8, 1+\zeta+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^7+\zeta^8, 1+\zeta+\zeta^2+\zeta^3+\zeta^8, 1+\zeta+\zeta^2+\zeta^3+\zeta^7, 1+\zeta+\zeta^2+\zeta^3+\zeta^6, 1+\zeta+\zeta^2+\zeta^3+\zeta^6+\zeta^8, 1+\zeta+\zeta^2+\zeta^3+\zeta^4, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^7, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^7+\zeta^8, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^6, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^6+\zeta^8, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^7+\zeta^8, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6+\zeta^8, 1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6+\zeta^7+\zeta^8$

REFERENCES

[1] A. A. Albert, “Finite division algebra and finite planes”, Proceedings of symposia in applied mathematics, vol. 10, pp. 53-70, 1960.

[2] L. L. Chen and M. Cordero, “New Examples of Fractional Dimensional Semifield Planes”, Note di Matematica, accepted, 2011.

[3] L. L. Chen and M. Cordero, “Primitivity in Finite Semifields”, in progress.

[4] S. D. Cohen, “Pairs of primitive roots”, Mathematika, 32, pp. 276-285, 1985.

[5] S. D Cohen and G. L. Mullen, “Primitive elements in finite fields and costas arrays”, AAECC, 2, pp. 45-53, 1991.

[6] M. Cordero and V. Jha, “Primitive semifields and fractional planes of order q^5”, Rendiconti Di Matematica, Serie VII, vol. 30, Roma, pp. 1-21, 2010.

[7] P. Dembowski, Finite geometries, Springer, New York, N.Y., 1968.

[8] I. R. Hentzel and I. F. Rúa, “Primitivity of Finite Semifields with 64 and 81 Elements”, International Journal of Algebra and Computation, vol. 17, No. 7, pp. 1411-1429, 2007.

[9] V. Jha and N. L. Johnson, “The dimension of a subplane of a translation plane”, Bull. Belg. Math. Soc. Simon Stevin, 17, n. 3, pp. 523-535, 2010.

[10] M. J. Kallaher, Affine planes with transitive collineation groups, Elsevier North Holland, Inc., New York 10017, 1982.

[11] D. E. Knuth, “Finite semifields and projective planes”, J. Algebra, 2, pp. 182-217, 1965a.

[12] D. E. Knuth, “A class of projective planes”, Trans. Amer. Math. Soc., 115, pp. 541-549, 1965b.

[13] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1986.

[14] R. Gow and J. Sheekey, “On primitive elements in finite semifields”, Finite Fields and Their Applications, 17, pp. 194-204, 2011.

[15] I. F. Rúa, “Primitive and non primitive finite semifields”, Communications in Algebra, 22, pp. 791–803, 2004.

[16] G. P. Wene, “On the multiplicative structure of finite division rings”, Aequationes Math., 41, pp. 463-477, 1991.

[17] G. P. Wene, “Semifields: Two Constructions”, Presented to Students and Faculty of The University of Texas at Arlington, 2012.

[18] M. Cordero and V. Jha, “Fractional dimensions in semifields of odd order”, Des. Codes Cryptogr., 61, pp. 197-221, 2011.

[19] V. Jha, “The Ubiquity of the orders of frational semifields of even characteristic”, personal communication.

BIOGRAPHICAL STATEMENT

Linlin Chen was born in Shandong, China, in 1982. She received her B.S. degree from Liaocheng University, China, in 2004 and her M.S. degree from Zhongshan University, China, in 2006. In 2008, she joined the doctoral program in the Department of Mathematics at the University of Texas at Arlington. She is a very passionate teacher and encourages young people to study science and mathematics. Her current research interests are in non-associative algebra, finite geometry, and the application of polynomials over finite fields.