4-2016

Finite semifields and their applications

Shamsa Ali Rashed Al Saedi

UAEU

جامعة الإمارات العربية المتحدة
United Arab Emirates University

United Arab Emirates University

College of Science

Department of Mathematical Sciences

FINITE SEMIFIELDS AND THEIR APPLICATIONS

Shamsa Ali Rashed Al Saedi

This thesis is submitted in partial fulfilment of the requirements for the degree of Master of Science in Mathematics

Under the Supervision of Dr. Kanat Abdukhalikov

April 2016

Declaration of Original Work

I, Shamsa Ali Rashed Al Saedi, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled *“Finite Semifields and Their Applications"*, hereby, solemnly declare that this thesis is my own original research work that has been done and prepared by me under the supervision of Dr. Kanat Abdukhalikov, in the College of Science at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student’s Signature ____________________ Date ______________

Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Dr. Kanat Abdukhalikov

   Title: Associate Professor

   Department of Mathematical Sciences

   College of Science

   Signature Abdukhalikov Date 20.04.2016

2) Member: Dr. Adama Diene

   Title: Associate Professor

   Department of Mathematical Sciences

   College of Science

   Signature Adama Diene Date 20/4/2016

3) Member (External Examiner): Dr. Taher Abualrub

   Title: Professor

   Department of Mathematics and Statistics

   Institution: American University of Sharjah

   Signature Taher Date 20/4/2016

This Master Thesis is accepted by:

Dean of the College of Science: Dr. Ahmed Murad

Signature ______________________ Date 18/5/ 2016

Dean of the College of Graduate Studies: Professor Nagi T. Wakim

Signature Nagi Wakim Date 19/5/2016

Copy 10 of 10

Abstract

This thesis is concerned with finite semifields. The objective of this thesis is to give a full description of Knuth orbits of known commutative semifields. We also describe planar functions corresponding to commutative semifields. Results are presented by tables. Nuclei of semifields are studied. Finally we consider applications of semifields, planar functions and spreads to construction of mutually unbiased bases.

Keywords: Finite semifields, isotopism, Knuth orbit, planar functions, spreads, mutually unbiased bases.

Title and Abstract (in Arabic)

شَبَه المجَالَات المحدودة وَ تطبيقَاتهَا

الملخص

تهتم هٰذِهِ الأُطرُوحَة بِشبه المـَجَالَات المحدودة. الهدف من الأُطرُوحَة هو التحديد الكَامل لمدَارَات كنوث لشبه المـَجَالَات التَبَادلية المعروفة. كمَا تم درَاسة الدوَال المستوية المطَابقة لشبه المجَالَاتِ التبَادلية. نقوم بتقديم النتَائِج بَاستخدَام الجدَاول. وَقد تطرقنَا لدرَاسة مجموعَات محتوَاه في شبه المـَجَالَاتِ التي تعرف بـ(نيوكلس). في النهَاية، تم تقديم تطبيقَات لشبه المـَجَالَاتِ وَ الدوَال المستوية لإِنشَاء قوَاعد تَبَادلية غير متحيزة.

مفَاهيم البحث الرئِيسية: شَبَه المجَالَات، مدَارَات كنوث، الدوَال المستوية، قوَاعد تَبَادلية غير متحيزة.

Acknowledgements

I humbly acknowledge all the help and support extended to me by my advisor Dr. Kanat Abdukhalikov. Completion of this thesis would have been impossible without his able guidance and advice. His continued encouragement and direction helped me through difficult times during this thesis and enabled me to fulfill the aimed requirements.

I would also like to thank the chair and all members of the Department of Mathematical Sciences at UAEU for their assistance.

Finally, my deepest gratitude goes to my family for providing me with unfailing support and continuous encouragement throughout my studies.

Dedication

To my beloved parents and family

Table of Contents

List of Tables

Chapter 1: Introduction

Finite semifields satisfy all the axioms for finite fields except that their multiplication is not assumed to be associative or commutative. In this thesis, we review terminologies essential for the understanding of finite semifields. We include a brief description of the geometric motivations for the concepts of isotopism, cubical array, the dual and transpose of a semifield.

The structure of the thesis is as follows. Chapter 2 contains a review of the basic definitions and theory of finite fields. In Chapter 3, we provide the formal definition of finite semifield. Furthermore, we introduce the concept of an isotopism between semifields, and show that the multiplication in a semifield defines an $n \times n \times n$ array of scalars known as a cubical array. We also concentrate on the links between Knuth orbit and each of nuclei, commutative and sympletic semifields. In Chapter 4, we calculate the Knuth orbit of known commutative semifields. To show an example, we also calculate Knuth derivatives of noncommutative Hughes-Kleinfeld semifields. In Chapter 5, we describe the connection between commutative semifields and planar functions in odd and even characteristics. We also find planar functions of known commutative semifields of odd order. In Chapter 6, we compute the middle nucleus and the center for Dickson semifields, Penttila-Williams semifields, Ganley semifields, and Cohen-Ganley semifields. In Chapter 7, we consider applications of planar functions, symplectic spreads, commutative and symplectic semifields to constructions of mutually unbiased bases. Results of our calculations are collected in Tables 7.1 - 7.5.

Chapter 2: Finite Fields

This chapter provides an introduction to abstract algebraic structures, called fields [24, 26]. Our primary interest is in finite fields, i.e., fields with a finite number of elements (also called Galois fields).

A field is a set of elements with two operations, called addition and multiplication, along with a set of properties governing these operations.

2.1 Fields

A field is a set $\mathbb{F}$ with two binary operations + and $*$ such that:

1. ($\mathbb{F}$, $+$) is a commutative group with identity element 0.
2. ($\mathbb{F}^*$, $*$) is a commutative group with identity element 1 (where $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$).
3. The distributive laws holds, $\forall x, y, z \in \mathbb{F}$.

Examples: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$ for p a prime, are fields.

- A field containing only finitely many elements is called a finite field or a Galois field.
- A subfield of a field $\mathbb{F}$ is a subset of $\mathbb{F}$, which is itself a field with respect to operations of $\mathbb{F}$.
- The smallest subfield of a field $\mathbb{F}$ is called the prime subfield.
- If K is a subfield of L, then we say that L is an extension of K.
- The order of a finite field is the number of elements in that field.

2.2 Characteristic of a Field

Definition 2.2.1. The smallest positive integer number n, such that $nx = 0$ for any $x \in \mathbb{F}$ is called the characteristic of the field $\mathbb{F}$, and $\mathbb{F}$ is called a field of characteristic n. If $nx \neq 0$ for any positive integer n, then $\mathbb{F}$ is called a field of characteristic 0.

Theorem 2.2.1. *Let $\mathbb{F}$ be a field. Then the characteristic of $\mathbb{F}$ is either 0 or a prime number p.*

Proof. Let $\mathbb{F}$ be a field and char $\mathbb{F} = n$, $n \neq 0$. Then $\forall x \in \mathbb{F}$, we have $nx = 0$. In particular $ne = 0$ (e is the multiplicative identity). If n is prime, we are done. Otherwise, $n = p_1 p_2$ with $1 < p_1, p_2 < n$. Hence, $0 = ne = (p_1 p_2)e$. Since $e^2 = e$, we have $0 = ne = (p_1 p_2)e = (p_1 e)(p_2 e)$. Thus, $p_1 e = 0$ or $p_2 e = 0$. But $1 < p_1, p_2 < n$, which contradicts to the fact that n is the smallest. □

Note that $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ are fields of characteristic 0, and $\mathbb{Z}_p$ is a field of characteristic p.

Theorem 2.2.2. *Let F be a field of characteristic p, $p \neq 0$, a and b be any two elements of F and n be any positive integer. Then*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}. \tag{2.1}$$

Proof. By induction. For $n = 1$ the equation (2.1) becomes $(a+b)^p = a^p + b^p$. By the binomial theorem, we have

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i,$$

where $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. If $i = 0$, then $\binom{p}{i} a^{p-i} b^i = a^p$, and if $i = p$, then $\binom{p}{i} a^{p-i} b^i = b^p$. For $0 < i < p$ we have $p \nmid i!$ and $p \nmid (p-i)!$. But $p \mid p(p-1)(p-2)\cdots 1 = p!$, hence

$\binom{p}{i} = \frac{p!}{i!(p-i)!} = 0$, since char $\mathbb{F} = p$. So all the coefficients except for the first and for the last are zero. Therefore,

$$(a+b)^p = a^p + b^p.$$

Assume that the equation (2.1) is correct for some n. We will show that the statement (2.1) is correct for $n+1$. Indeed,

$$(a+b)^{p^{n+1}} = ((a+b)^{p^n})^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

Therefore,

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

for any positive integer n. □

Definition 2.2.2. Given a polynomial with coefficients in a field F, the smallest extension of F in which the polynomial can be completely factored into linear factors is called a splitting field for the polynomial.

Theorem 2.2.3. *(Existence and uniqueness of splitting fields). Let $f(x)$ be a polynomial over a field F. There is a splitting field for $f(x)$ over F, and it is unique in the following sense. If E and E' are splitting fields for $f(x)$ over F, then there is an isomorphism between E and E' which is the identity on F.*

Theorem 2.2.4. *(Existence and uniqueness of finite fields). For every prime p and positive integer $n \geq 1$, there is a finite field with p^n elements. Any finite field with p^n elements is isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.*

Proof. First we prove the existence part. Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, and F be a splitting field of $f(x)$ over $\mathbb{F}_p$. Then $f'(x) = p^n x^{p^n - 1} - 1 = -1$. Therefore, $(f, f') = 1$ and f

has p^n distinct roots. Now, Let $S = \{a \in F : f(a) = 0\}$. Then S is a subfield of F since:

- S contains 0.
- $a, b \in S$ implies that $(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b$, so $a - b \in S$.
- For $a, b \in S$ and $b \neq 0$, we have $(ab^{-1})^{p^n} = a^{p^n} b^{-p^n} = ab^{-1}$, so $ab^{-1} \in S$.

On the other hand, $x^{p^n} - x$ must split in S, since S contains all its roots, i.e. the splitting field F is a subfield of S. Thus $F = S$, and since S has p^n elements, F is a finite field with p^n elements.

To prove the uniqueness, let F be a finite field and $|F| = p^n$. Then $\mathbb{F}_p$ is a prime field of F. Since F is a field, we get that $(F^*, \cdot)$ is a multiplicative group with $p^n - 1$ elements. Then, for any $a \in F^*$ we have $a^{p^n - 1} = 1$ if and only if $a^{p^n} = a$. Thus, for all $a \in F^*$, we obtain $a^{p^n} - a = 0$. Therefore, F is a splitting field of $x^{p^n} - x$. Hence, F is the smallest field in which $x^{p^n} - x$ splits completely in linear terms. Since the splitting field of $x^{p^n} - x$ is unique, this implies that there exist a finite field of p^n elements. $\square$

The previous theorem shows that a finite field of a given order is unique up to a field isomorphism. We shall denote this field by $\mathbb{F}_q$, where q denotes a power of the prime characteristic p of $\mathbb{F}_q$.

2.3 Automorphisms

Definition 2.3.1. Let q be a prime power and n a positive integer. The map $\sigma : \alpha \longmapsto \alpha^q$ from $\mathbb{F}_{q^n}$ to itself is an automorphism of $\mathbb{F}_{q^n}$.

- If $\alpha \in \mathbb{F}_q \Rightarrow \sigma(\alpha) = \alpha^q = \alpha$.
- An automorphism of $\mathbb{F}_{q^n}$ which leaves every element of $\mathbb{F}_q$ fixed is called an automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

- The automorphism $\sigma : \mathbb{F}_{q^n} \longmapsto \mathbb{F}_{q^n}$, $\alpha \longmapsto \alpha^q$ is called the Frobenuis Automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

2.4 Characteristic Polynomials and Minimal Polynomials

Let $\alpha \in \mathbb{F}_{q^n}$ and let σ be the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then the polynomial

$$\begin{aligned} g(x) &= (x-\alpha)(x-\sigma(\alpha))(x-\sigma^2(\alpha))...(x-\sigma^{n-1}(\alpha)) \\ &= (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})...(x-\alpha^{q^{n-1}}) \end{aligned}$$

is called the characteristic polynomial of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Related to the characteristic polynomial is the minimal polynomial of α, which is the least degree monic polynomial f over $\mathbb{F}_q$ for which $f(\alpha) = 0$.

Theorem 2.4.1. *Let α be an arbitrary element of $\mathbb{F}_{q^n}$. Then*

1. *The minimal polynomial of α over $\mathbb{F}_q$ exists and it is unique, moreover, it is irreducible over $\mathbb{F}_q$.*
2. *Let $m(x)$ be the minimal polynomial of α over $\mathbb{F}_q$. If $f(x) \in \mathbb{F}_q[x]$ and $f(\alpha) = 0$, then $m(x)|f(x)$.*
3. *Let d be the least positive integer such that $\sigma^d(\alpha) = \alpha$. Then $d|n$.*

Proof. 1. Since the characteristic polynomial $g(x) = (x-\alpha)(x-\sigma(\alpha))...(x-\sigma^{n-1}(\alpha))$ of α is monic and $g(\alpha) = 0$, there exists a monic polynomial $m(x)$ with least degree such that $m(\alpha) = 0$, which implies that the minimal polynomial of α exists. Assume that $m_1(x)$ is another minimal polynomial of α. Then, deg $m(x) =$ deg $m_1(x)$. Assume that $m(x) \neq m_1(x)$. Then, deg $(m(x) - m_1(x)) <$ deg $m(x)$, deg $m_1(x)$. Let c be the leading coefficient of $m(x) - m_1(x)$, then $c^{-1}(m(x) - m_1(x))$ is a monic polynomial over $\mathbb{F}_q$ having α as a root and deg $c^{-1}(m(x)-m_1(x)) <$ deg $m(x)$. This is a contradiction. Therefore, $m(x) = m_1(x)$, and $m(x)$ is unique.

Assume that $m(x)$ is not irreducible. Then we have $m(x) = f_1(x)f_2(x)$, deg $f_1(x), f_2(x) <$ deg $m(x)$ and $m(\alpha) = f_1(\alpha)f_2(\alpha) = 0$. Since $f_1(\alpha), f_2(\alpha) \in \mathbb{F}_{q^n}$ and $\mathbb{F}_{q^n}$ is field (i.e. $\mathbb{F}_{q^n}$ has no zero divisors), $f_1(\alpha)f_2(\alpha) = 0$ implies that $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$. Thus, $m(x)$ doesn't have the lowest degree. Therefore, $m(x)$ is not the minimal polynomial. This is a contradiction. Hence, $m(x) \neq f_1(x)f_2(x)$ and $m(x)$ is irreducible.

2. Given $m(x)$ and $f(x)$, then there exist a unique $q(x)$ and $r(x)$ such that $f(x) = q(x)m(x) + r(x)$, deg $r <$ deg m. Thus, $r(x) = f(x) - q(x)m(x)$. And $r(\alpha) = f(\alpha) - q(\alpha)m(\alpha) = 0 - 0 = 0$. Therefore, $r(\alpha) = 0$, with deg $r <$ deg m. But since m has the lowest degree, we obtain $r \equiv 0$ and $f(x) = q(x)m(x)$. Hence, m divides f.

3. Assume $n = qd + r$ where $0 \leq r < d$. We know $\sigma^n = 1$, thus $\sigma^n(\alpha) = \alpha$. Then $\alpha = \sigma^n(\alpha) = \sigma^r(\sigma^{qd}(\alpha)) = \sigma^r(\alpha)$. Therefore, $\sigma^r(\alpha) = \alpha$. Since d is the lowest integer such that $\sigma^d(\alpha) = \alpha$, and since $r < d$, $\sigma^r(\alpha) = \alpha$, we obtain $r = 0$ and $n = qd$. Thus, d divides n. □

2.5 Trace and Norm

Definition 2.5.1. Let q be a prime power and n be a positive integer. Assume $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^n}$. We define the trace and norm of α as:

$$\begin{aligned} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) &= \alpha + \sigma(\alpha) + \sigma^2(\alpha) + ... + \sigma^{n-1}(\alpha) \\ &= \alpha + \alpha^q + \alpha^{q^2} + ... + \alpha^{q^{n-1}} \end{aligned}$$

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha\sigma(\alpha)\sigma^2(\alpha)...\sigma^{n-1}(\alpha)$$
$$= \alpha\alpha^q\alpha^{q^2}...\alpha^{q^{n-1}}$$
$$= \alpha^{q^n-1/q-1}$$

where $\alpha \in \mathbb{F}_{q^n}$ and σ is the Frobenius Automorphism.

Theorem 2.5.1. *For $\alpha, \beta \in \mathbb{F}_{q^n}$, and $a \in \mathbb{F}_q$ we have:*

1. $Tr(\alpha) \in \mathbb{F}_q$.
2. $Tr(\alpha+\beta) = Tr(\alpha)+Tr(\beta)$.
3. $Tr(a\alpha) = aTr(\alpha)$, *and in particular,* $Tr(a) = na$.
4. $Tr(\alpha^q) = Tr(\alpha)$.
5. $N(\alpha) \in \mathbb{F}_q$.
6. $N(\alpha\beta) = N(\alpha)N(\beta)$.
7. $N(a\alpha) = a^nN(\alpha)$, *and in particular,* $N(a) = a^n$.
8. $N(\alpha^q) = N(\alpha)$.

2.6 Bases

Let $\mathbb{F}_{q^n}$ be an extension of $\mathbb{F}_q$, $q = p^e$, p a prime. We can look at $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$ (the field elements are the vectors and the subfield elements are the scalars). Assume $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then any element $\beta \in \mathbb{F}_{q^n}$ can be expressed uniquely as a linear combination of $\alpha_1, \alpha_2, ..., \alpha_n$ with coefficients in $\mathbb{F}_q$: $\beta = b_1\alpha_1 + b_2\alpha_2 + ... + b_n\alpha_n$, where $b_i \in \mathbb{F}_q$ for $i = 1, 2, ..., n$.

Definition 2.6.1. Let $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{F}_{q^n}$. We define the discriminant $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ as:

$$\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \alpha_2, ..., \alpha_n) = \begin{vmatrix} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_1) & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_2) & \cdots & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_n) \\ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_1) & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_2) & \cdots & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_1) & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_2) & \cdots & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_n) \end{vmatrix}$$

The next two results use the discriminant to provide tests that determine whether a given set of vectors forms a basis.

Theorem 2.6.1. *$\{\alpha_1, \alpha_2, ..., \alpha_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the discriminant $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \alpha_2, ..., \alpha_n)$ is nonzero.*

Corollary 1. *$\{\alpha_1, \alpha_2, ..., \alpha_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if*

$$D = \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{vmatrix} \neq 0$$

Proof. Computing D^2, we obtain $D^2 = \Delta(\alpha_1, \alpha_2, ..., \alpha_n)$. And by the previous theorem, $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ is a basis if and only if $D^2 \neq 0$ if and only if $D \neq 0$. □

2.7 Bilinear Forms

Definition 2.7.1. Let V be an n-dimensional vector space over a field F. A bilinear form is a map $\mathbf{H} : V \times V \to F$ such that:

1. $\mathbf{H}(u+v, w) = \mathbf{H}(u, w) + \mathbf{H}(v, w)$;

2. $\mathbf{H}(u, v+w) = \mathbf{H}(u, v) + \mathbf{H}(u, w)$;

3. $\mathbf{H}(\lambda u, v) = \mathbf{H}(u, \lambda v) = \lambda \mathbf{H}(u, v)$

for any $u, v, w \in V$, and $\forall \lambda \in F$.

- A bilinear form **H** is called symmetric if $\mathbf{H}(v, w) = \mathbf{H}(w, v)$ for all $v, w \in V$.
- A bilinear form **H** is called skew-symmetric if $\mathbf{H}(v, w) = -\mathbf{H}(w, v)$ for all $v, w \in V$.
- A bilinear form **H** is called non-degenerate if for all $v \in V$, there exists $w \in V$, such that $\mathbf{H}(w, v) \neq 0$.
- If $\mathbf{H}(v, v) = 0$ for $v \in V$, then v is called isotropic.
- If S is a non-empty set of V, then $S^{\perp} = \{u \in V : \mathbf{H}(u, v) = 0, \forall v \in V\}$ is called **H**-orthogonal of V (i.e. the set of vectors that are **H**-orthogonal to all vectors of S).

It is well known that bilinear form are related to matrices in the following way: Let $\{e_1, ..., e_n\}$ be an F-basis for V. Let u and v be elements of V, and suppose $u = \sum_{i=1}^{n} u_i e_i$, $v = \sum_{i=1}^{n} v_i e_i$ for $u_i, v_i \in F$. Then by the above defining properties of bilinear forms, we have

$$\begin{aligned}\mathbf{H}(u, v) &= \sum_{i,j=1}^{n} u_i v_j \mathbf{H}(e_i, e_j) \\ &= \sum_{i,j=1}^{n} u_i v_j h_{ij}\end{aligned}$$

where $h_{ij} = \mathbf{H}(e_i, e_j)$ for each i, j.

Consider the matrix $H = (h_{ij})_{i,j} \in M_n(F)$. Then

$$\mathbf{H}(u, v) = \mathbf{u}^T H \mathbf{v} = (u_1, u_2 ... u_n) H \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Note that the entries of the matrix H depends on the choice of basis. Hence we refer to H as the matrix representing $\mathbf{H}$ with respect to the basis $\{e_1, ..., e_n\}$.

Chapter 3: Semifields

3.1 Semifields

In this section we recall basic definitions and facts on finite semifields [10, 21, 22]. The study of non-associative division rings were first considered by L.E.Dickson in 1905, and were depply studied by A.A.Albert in 1942, who introduced isotopy of these algebras. The term semifields were introduced by Knuth in 1965 in his PhD thesis. It was his first work in mathematics. Semifields have become an attracting topic in many different areas of mathematics, such as coding theory, finite geometry and cryptography.

Definition 3.1.1. A finite semifield is a finite set $\mathbb{S}$ with at least two distinct elements, and two binary operations + and $\circ$, satisfying the following axioms:

$(S1)$ $(\mathbb{S},+)$ is a group with identity element 0.

$(S2)$ The distributive laws holds, for all $x,y,z \in \mathbb{S}$.

$(S3)$ $x \circ y = 0$ implies $x = 0$ or $y = 0$.

$(S4)$ $\exists 1 \in \mathbb{S}$ such that $1 \circ x = x \circ 1 = x$, for all $x \in \mathbb{S}$.

- A semifield $(\mathbb{S},+,\circ)$ is called commutative if $x \circ y = y \circ x$ for all $x,y \in \mathbb{S}$.

- If $\mathbb{S}$ does not have a multiplicative identity, then it is called a presemifield.

- Any finite semifield can be represented by $\mathbb{S} = (\mathbb{F}_{p^n},+,\circ)$, where p is prime, n is a positive integer.The prime p is called the characteristic of $\mathbb{S}$. A semifield which is not a field is called proper.

- The additive group of a semifield $\mathbb{S}$ is elementary abelian.

Let's prove the last statement. Using the distributive laws we find

$$(a+b)\circ(c+d) = (a\circ c + a\circ d) + (b\circ c + b\circ d)$$
$$= (a\circ c + b\circ c) + (a\circ d + b\circ d).$$

Since $(\mathbb{S},+)$ is a group, we obtain $a\circ d + b\circ c = b\circ c + a\circ d$. Since any two elements $x,y \in \mathbb{S}$ can be written as a product $x = a\circ d$ and $y = b\circ c$ for some $a,b,c,d \in \mathbb{S}$, the additive group is abelian.

To show the elementary abelian part, let $a \neq 0$ and p be the additive order of a. Then p must be a prime number. Hence, $(\mathbb{S},+)$ is elementary abelian.

Theorem 3.1.1. *A two-dimensional finite semifield is a field.*

Proof. Let $\mathbb{S}$ be two dimensional over $\mathbb{F}_p$ and has a basis of the form $\{1,x\}$. Then $|\mathbb{S}| = p^2$. The multiplication in $\mathbb{S}$ is therefore determined by $x*x = ax+b, \quad \forall a,b \in \mathbb{F}_p$. Consider $x^2 - ax - b = 0$. This cannot be factored otherwise $\mathbb{S}$ would contain zero divisors. Thus it is irreducible and $\mathbb{S} \cong \mathbb{F}_{p^2}$. □

Lemma 3.1.2. *(Knuth, [19]). If S is a proper semifield of order p^n, then $n \geq 3$.*

Knuth also proves in [19] that if $|S| = 8$, then $S \cong \mathbb{F}_8$. Thus, the smallest proper semifields are of order 16.

Let $\mathbb{S} = (\mathbb{F}_{q^n},+,\circ)$ be a semifield. The subsets:

$$N_l(\mathbb{S}) = \{a \in \mathbb{S} : (a\circ x)\circ y = a\circ(x\circ y), \forall x,y \in \mathbb{S}\},$$

$$N_m(\mathbb{S}) = \{a \in \mathbb{S} : (x\circ a)\circ y = x\circ(a\circ y), \forall x,y \in \mathbb{S}\},$$

$$N_r(\mathbb{S}) = \{a \in \mathbb{S} : (x\circ y)\circ a = x\circ(y\circ a), \forall x,y \in \mathbb{S}\}$$

are called the left, middle and right nucleus of $\mathbb{S}$ respectively and the set

$$N(\mathbb{S}) = N_l(\mathbb{S}) \cap N_m(\mathbb{S}) \cap N_r(\mathbb{S})$$

is called a (associative) nucleus. The set

$$C(\mathbb{S}) = \{a \in N(\mathbb{S}) : a \circ b = b \circ a, \forall b \in \mathbb{S}\}$$

is called the center of $\mathbb{S}$. All these sets are finite fields, and if $\mathbb{S}$ is commutative then $N_l(\mathbb{S}) = N_r(\mathbb{S}) \subseteq N_m(\mathbb{S})$.

Some further properties of finite semifield:

1. $\mathbb{S}$ is a vector space V over its centre.
2. $\mathbb{S}$ is a left vector space V_l over its left nucleus.
3. $\mathbb{S}$ is a right vector space V_r over its right nucleus.
4. $\mathbb{S}$ is a left and right vector space over its middle nucleus.

Let $\mathbb{F}_q$ denote the finite field of $q = p^e$, p an odd prime, $\mathbb{F}_q^*$ denote the set of nonzero elements of $\mathbb{F}_q$, and $\mathbb{F}_q[x]$ be the ring of polynomials in indeterminate x over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial of $\mathbb{F}_q$ if it induces a bijective mapping on $\mathbb{F}_q$.

A polynomial of the form $L(x) = \sum_{i=0}^{e-1} a_i x^{p^i} = a_0 x + a_1 x^p + \ldots + a_{e-1} x^{p^{e-1}} \in \mathbb{F}_q[x]$ is called a p-polynomial. Such polynomials are also known as linearised polynomials, whose name stems from the properties:

1. $L(x+y) = L(x) + L(y) \quad \text{for all } x, y \in \mathbb{F}_q$.
2. $L(\alpha x) = \alpha x \quad \text{for all } \alpha \in \mathbb{F}_p \text{ and } x \in \mathbb{F}_q$

A Dembowski-Ostrom(DO) polynomial $f \in \mathbb{F}_q[x]$ is a polynomial with the shape

$$f(x) = \sum_{i,j=0}^{e-1} a_{ij} x^{p^i + p^j}.$$

A function from a finite field $\mathbb{F}_q$ to itself is affine, if it is defined by the sum of a constant and a linearized polynomial over $\mathbb{F}_q$.

Let $\mathbb{S} = (\mathbb{S}, +, *)$ and $\mathbb{S}' = (\mathbb{S}, +, \circ)$ be semifields. A semifield homomorphism from $\mathbb{S}$ to $\mathbb{S}'$ is a function $\phi : \mathbb{S} \longmapsto \mathbb{S}'$ such that ϕ satisfies :

1. $\phi(a+b) = \phi(a) + \phi(b) \qquad \forall a, b \in \mathbb{S}$,
2. $\phi(a*b) = \phi(a) \circ \phi(b) \qquad \forall a, b \in \mathbb{S}$.

A homomorphism from a semifield to itself is called endomorphism. Any semifield homomorphism $\phi : \mathbb{S} \longmapsto \mathbb{S}'$ which is bijective is an isomorphism. If $\mathbb{S} = \mathbb{S}'$, we say that the isomorphism ϕ is an automorphism.

Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, *)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \circ)$ be two (pre-)semifields. They are called isotopic if there exist three linear permutations M, N, L of $\mathbb{F}_{p^n}$ such that $L(x*y) = M(x) \circ N(y)$ for any $x, y \in \mathbb{F}_{p^n}$. The triple (M, N, L) is called the isotopism between $\mathbb{S}_1$ and $\mathbb{S}_2$. If $M = N$, then $\mathbb{S}_1$ and $\mathbb{S}_2$ are called strongly isotopic. The set of (pre-)semifields isotopic to a (pre-)semifield S_1 is called the isotopism class of $\mathbb{S}_1$ and is denoted by $[\mathbb{S}_1]$.

- An isotopism from a semifield to itself is called an autotopism.
- In the case where $M = N = L$, the autotopism is clearly an automorphism.

Every commutative presemifield can be transformed into a commutative semifield. Indeed, let $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$ be a commutative presemifield which does not contain an identity. To create a semifield from $\mathbb{S}$ choose any $a \in \mathbb{F}_{p^n}^*$ and define a new multiplication $\circ$ by $(x*a) \circ (a*y) = x*y$ for all $x, y \in \mathbb{F}_{p^n}^*$. Then $\mathbb{S}' = (\mathbb{F}_{p^n}, +, \circ)$ is a commutative semifield isotopic to $\mathbb{S}$ with identity $a*a$. We say $\mathbb{S}'$ is a commutative semifield corresponding to the commutative presemifield S. An isotopism between $\mathbb{S}$ and $\mathbb{S}'$ is a strong isotopism $(L_a(x), L_a(x), x)$ with a linear permutation $L_a(x) = a * x$.

3.2 The Knuth Orbit

If $\mathbb{S} = (S, +, *)$ is a semifield n-dimensional over $\mathbb{F}_p$, and $\{e_1, ..., e_n\}$ is an $\mathbb{F}_p$-basis for $\mathbb{S}$, then the multiplication can be written in terms of the multiplication of the vectors e_i, i.e, if $x = x_1e_1 + ... + x_ne_n$ and $y = y_1e_1 + ... + y_ne_n$ with $x_i, y_j \in \mathbb{F}_p$, then $x * y = \sum_{i,j=1}^n x_iy_j(e_i * e_j) = \sum_{i,j=1}^n x_iy_j(\sum_{k=1}^n a_{ijk}e_k)$ for certain $a_{ijk} \in \mathbb{F}_p$, called the structure constants of $\mathbb{S}$ with respect to the basis $\{e_1, ..., e_n\}$. The set $\{a_{ijk}\}$ is also called a cubical array. We will use this process to define the dual and transpose of a semifield.

The semifield $\mathbb{S}^d$ (the dual of $\mathbb{S}$) can be obtained by reversing the multiplication (i.e., $x \circ y = y * x$). The dualization process in terms of cubical arrays is $a^d_{ijk} = a_{jik}$. Similarly, the semifield $\mathbb{S}^t$ (the transpose of $\mathbb{S}$) can be obtained via exchanging i and k (i.e. $a^t_{ijk} = a_{kji}$).

These processes, dualization and transposition, may be iterated producing six possible semifields, which is equivalent to the action of the symmetric group S_3 on the indices of the cubical array, (i.e., $\mathbb{S}^{(12)} = \mathbb{S}^d$, $\mathbb{S}^{(13)} = \mathbb{S}^t$, $\mathbb{S}^{(23)} = \mathbb{S}^{dtd} = \mathbb{S}^{tdt}$, $\mathbb{S}^{(123)} = \mathbb{S}^{dt}$, $\mathbb{S}^{(132)} = \mathbb{S}^{td}$). These six semifields are called Knuth orbit [19] or Knuth derivatives of a semifeld $\mathbb{S}$.

Taking the transpose of a semifield can also be interpreted geometrically as dualising the semifield spread. The resulting action on the set of nuclei of the isotopism class $\mathbb{S}$ is as follows. The dual of $\mathbb{S}$ fixes the middle nucleus and interchanges the left and right nuclei; while the transpose of $\mathbb{S}$ fixes the left nucleus and interchanges the middle and right nuclei. Summarising, the action of the dual and transpose generate a series of at most six isotopism classes of semifields, with nuclei according to Figure 1.

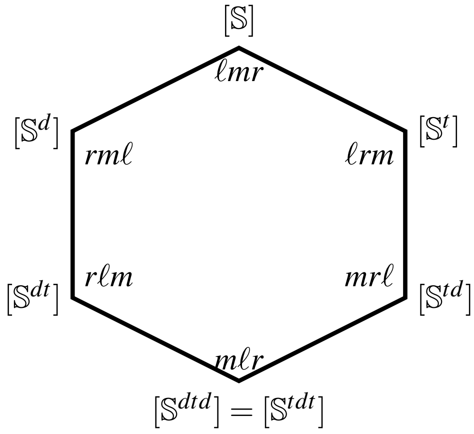

Figure 1: The Knuth orbit $K(S)$ of a semifield $\mathbb{S}$ with nuclei ℓmr

Let $\mathbb{S}$ be an n-dimensional semifield over $\mathbb{F}_p$, i.e. a semifield of order p^n and characteristic p. Define: $x * y = F(x,y) = \sum_{i,j=0}^{n-1} c_{ij} x^{p^i} y^{p^i}$, where $c_{ij} \in \mathbb{F}_{p^n}$. Each $y \in \mathbb{S}$ defines an $\mathbb{F}_p$-endomorphism of $\mathbb{S}$ denote by $R_y(x) = F(x,y)$. We call this the endomorphism of right multiplication by y. Since $\mathbb{S}$ has no zero divisors, R_y is invertible $\forall y \neq 0$, and the set $C = \{R_y : y \in \mathbb{S}\}$ is an $\mathbb{F}_p$-subspace of $\mathbb{F}_p$-endomorphisms of $\mathbb{S}$, where each nonzero element is invertible. We call C the spread set of $\mathbb{S}$. The spread set for $\mathbb{S}^d$ is $C^d = \{L_x : x \in \mathbb{S}\}$.

Define non-degenerate symmetric bilinear form $(x,y) = tr(xy)$. For a $\mathbb{F}_p$-linear map $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, the adjoint map $\overline{\varphi}$ is defined by

$$(\overline{\varphi}(x), y) = (x, \varphi(y)).$$

If $\varphi(x) = \sum_{i=0}^{n-1} \beta_i x^{p^i}$ then $\overline{\varphi}(x) = \sum_{i=0}^{n-1} \beta_i^{p^{n-i}} x^{p^{n-i}}$.

Define $r_i(y) = \sum_j c_{ij} y^{p^j}$, then $R_y(x) = \sum_i (\sum_j c_{ij} y^{p^j}) x^{p^i} = \sum_i r_i(y) x^{p^i}$. The adjoint $\bar{R}_y(x)$ of $R_y(x)$ with respect to $(\cdot,\cdot)$ is $\bar{R}_y(x) = \sum_i (r_{n-i}(y))^{p^i} x^{p^i}$. This implies that the dual and the transpose of $\mathbb{S}$ are defined, respectively, by the following multiplications:

$$x *^d y = F(y,x)$$

and

$$x *^t y = \bar{R}_y(x) = \sum_i (r_{n-i}(y))^{p^i} x^{p^i}.$$

Knuth showed that these operations are well defined up to isotopism. Suppose $\mathbb{S}$ is isotopic to $\mathbb{S}'$, i.e. there exist three linear permutations M, N, L such that $L(x * y) = M(x) \circ N(y)$ for any $x, y \in \mathbb{S}$. Then $L(x *^d y) = L(y * x) = M(y) \circ N(x) = N(x) \circ^d M(y)$. Therefore, $\mathbb{S}^d$ is isotopic to $\mathbb{S}'^d$, with corresponding isotopism (N, M, L).

We have $L(R_y(x)) = L(x * y) = M(x) \circ N(y) = R'_{N(y)} M(x)$, $\forall x, y \in \mathbb{S}$. This implies $L(R_y) = R'_{N(y)} M$, $\forall y \in \mathbb{S}$. Taking the adjoint of both sides, we get $\bar{R}_y(\bar{L}) = (\bar{M})\bar{R}'_{N(y)}$. Hence, $\bar{M}^{-1}(x *^t y) = \bar{M}^{-1}\bar{R}_y(x) = \bar{R}'_{N(y)}\bar{L}^{-1}(x) = \bar{L}^{-1}(x) \circ^t N(y)$. Therefore, $\mathbb{S}^t$ is isotopic to $\mathbb{S}'^t$, with corresponding isotopism $(\bar{L}^{-1}, N, \bar{M}^{-1})$.

Theorem 3.2.1 ([22])**.** *If $\mathbb{S}$ is a semifield, then*

1. $N_r(\mathbb{S}) = N_l(\mathbb{S}^d) = \overline{N_m(\mathbb{S}^t)}$;

2. $N_m(\mathbb{S}) = \overline{N_r(\mathbb{S}^t)} \cong N_m(\mathbb{S}^d)$;

3. $N_l(\mathbb{S}) = N_r(\mathbb{S}^d) \cong N_l(\mathbb{S}^t)$.

Proposition 1. *Let $\mathbb{S}_1 = (S_1, +, \circ)$ and $\mathbb{S}_2 = (S_2, +, *)$ be two presemifields and let C_1 and C_2 be the two corresponding spread sets. Then S_1 and S_2 are isotopic under the isotopism (M, N, L) if and only if $C_2 = LC_1M^{-1} = \{L \circ R_y \circ M^{-1}, y \in S_1\}$.*

Proof. Let $C_1 = \{R_y, y \in S_1\}$ and $C_2 = \{R'_y, y \in S_2\}$. And let (M, N, L) be an isotopism between S_1 and S_2. Then $M(x) * N(y) = L(x \circ y), \forall x, y \in S_1$. It follows that $L(R_y(x)) = R'_{N(y)}(M(x)), \forall x, y \in S_1$. Therefore, $L(R_y(M^{-1}(x))) = R'_{N(y)}(x)$. Hence, $R'_{N(y)} = L \circ R_y \circ M^{-1}, \forall y \in S_1$. Since $C_2 = \{R'_y, y \in S_2\} = \{R'_{N(y)}, y \in S_1\}$, we obtain $C_2 = \{L \circ R_y \circ M^{-1}, y \in S_1\}$.

Conversely, assume that $C_2 = \{L \circ R_y \circ M^{-1}, y \in S_1\}$, where M and L are invertible $\mathbb{F}_p$-linear maps from S_1 to S_2. Then the map N sending each element $y \in S_1$ to unique element $z \in S_2$ such that $R'_z = L \circ R_y \circ M^{-1}$, $(R'_z \in C_2)$ is an invertible $\mathbb{F}_p$-linear map from S_1 to S_2. Therefore, $\forall x, y \in S_1$, we have $R'_{N(y)}(x) = L(R_y(M^{-1}(x)))$. Thus, $x * N(y) = L(M^{-1}(x) \circ y)$. Hence, $M(x') * N(y) = L(x' \circ y)$. □

Lemma 3.2.2. *Let $R = (\mathbb{F}_q, +, *)$ be a commutative presemifield and suppose $R_1 = (\mathbb{F}_q, +, \circ)$ is any presemifield isotopic to R. Any isotopism (M, N, L) from R to R_1 must satisfy $M(x) \circ N(y) = M(y) \circ N(x), \quad \forall x, y \in \mathbb{F}_q$.*

Theorem 3.2.3. *Let $R_1 = (\mathbb{F}_q, +, \circ)$ and $R_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative presemifields. Then there exists an isotopism (M, N, L) between R_2 and R_1 such that either*

1. *$M = N$, or*
2. *$M(x) \neq N(\alpha x) \quad \forall \alpha \in \mathbb{F}_p^*$ and $x \in \mathbb{F}_q^*$.*

Proof. Let (M, N, L) be an isotopism from R_2 to R_1. Suppose $M \neq N$, and that there exist $x_0 \in \mathbb{F}_q^*$ and $\alpha \in \mathbb{F}_p^*$ such that $M(x_0) = N(\alpha x_0)$. As $\alpha \in \mathbb{F}_p^*$, we have $(\alpha x) \circ y = \alpha(x \circ y) = x \circ (\alpha y)$, for all $x, y \in \mathbb{F}_q$. Using the previous lemma, we have $M(x) \circ N(\alpha y) = M(y) \circ N(\alpha x)$, for all $x, y \in \mathbb{F}_q$. Set $y = x_0$, then we get $M(x) \circ N(\alpha x_0) = M(x) \circ M(x_0) = M(x_0) \circ N(\alpha x) = N(\alpha x) \circ M(x_0)$. Since $M(x_0) = N(\alpha x_0)$, we have $M(x) = N(\alpha x)$, for all $x \in \mathbb{F}_q$. Therefore, $M(x) = \alpha N(x)$. Since (M, N, L) are isotopism from R_2 to R_1, we have

$$M(x) \circ N(y) = L(x * y), \forall x, y \in \mathbb{F}_q$$

$$\alpha N(x) \circ N(y) = L(x * y), \forall x, y \in \mathbb{F}_q$$

$$N(x) \circ N(y) = \alpha^{-1} L(x * y), \forall x, y \in \mathbb{F}_q$$

Hence, $(N, N, \alpha^{-1} L)$ is an isotopism between R_2 and R_1. □

Theorem 3.2.4. *Let $R_1 = (\mathbb{F}_q, +, \circ)$ and $R_2 = (\mathbb{F}_q, +, *)$ be isotopic commutative semifields. Then there exists an isotpism (M, N, L) between R_2 and R_1 such that either*

1. *$M = N$, or*

2. *$M(x) = \alpha \circ N(x) \quad$ where $\alpha \in N_m(R_1)$.*

Proof. Suppose $M \neq N$. Let $\alpha = M(b)$ and $N(b) = e$, where e is the identity of R_1. Then $M(x) \circ N(b) = M(x) \circ e = M(x)$ and $M(b) \circ N(x) = \alpha \circ N(x)$. By the previous lemma, we have $M(x) \circ N(b) = M(b) \circ N(x)$. Therefore, $M(x) = \alpha \circ N(x) \quad \forall x \in \mathbb{F}_q$. Now we have to show that $\alpha \in N_m(R_1)$ i.e. $(N(x) \circ \alpha) \circ N(y) = N(x) \circ (\alpha \circ N(y))$. Using the previous lemma, we have $M(x) \circ N(y) = M(y) \circ N(x)$ for all $x, y \in \mathbb{F}_q$. Then

$$\begin{aligned}(\alpha \circ N(x)) \circ N(y) &= (N(x) \circ \alpha) \circ N(y)\\ &= (N(y) \circ \alpha) \circ N(x)\\ &= N(x) \circ (\alpha \circ N(y)).\end{aligned}$$

Hence, $(N(x) \circ \alpha) \circ N(y) = N(x) \circ (\alpha \circ N(y))$ for all $x, y \in \mathbb{F}_q$. Since N is a permutation, we obtain $\alpha \in N_m(R_1)$. □

3.3 Symplectic Semifields and Commutative Semifields

A symplectic semifield is a semifield whose associated semifield spread is symplectic. A spread C of V is called symplectic if there is a nondegenerate alternating bilinear form $(,)$ on V such that $(X, X) = 0$, for each $X \in C$.

Starting from a semifield $\mathbb{S}$, we can construct a family of semifield spreads by an iteration of the construction processes of transpose and dualization [16]. A semifield is commutative if applying dualization to the semifield the original semifield is obtained. That is, if $\{a_{ijk}\} \longmapsto \{a_{jik}\} = \{a_{ijk}\}$. Therefore, the Knuth orbit $K(\mathbb{S})$ of a commutative semifield consists of the following isotopism classes $\{[\mathbb{S}] = [\mathbb{S}^d], [\mathbb{S}^t] = [\mathbb{S}^{dt}], [\mathbb{S}^{td}] = [\mathbb{S}^{dtd}]\}$.

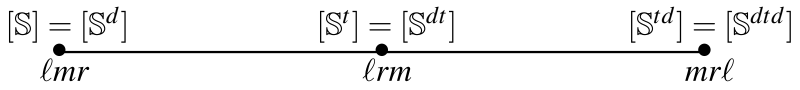
$[\mathbb{S}] = [\mathbb{S}^d]$
ℓmr
$[\mathbb{S}^t] = [\mathbb{S}^{dt}]$
ℓrm
$[\mathbb{S}^{td}] = [\mathbb{S}^{dtd}]$
$mr\ell$

Figure 3.1: The Knuth orbit $K(\mathbb{S})$ of commutative semifield $\mathbb{S}$ with nuclei ℓmr

Similarly, the semifield is symplectic if applying transposition to the semifield, the original semifield is obtained. That is, if $\{a_{ijk}\} \longmapsto \{a_{kji}\} = \{a_{ijk}\}$. Therefore, the Knuth orbit $K(\mathbb{S})$ of a symplectic semifield consists of the following isotopism classes $\{[\mathbb{S}] = [\mathbb{S}^t], [\mathbb{S}^d] = [\mathbb{S}^{td}], [\mathbb{S}^{dt}] = [\mathbb{S}^{tdt}]\}$.

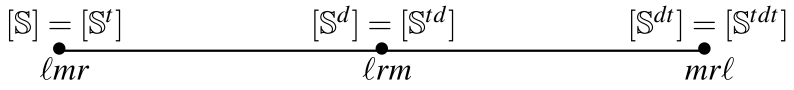
$[\mathbb{S}] = [\mathbb{S}^t]$
ℓmr
$[\mathbb{S}^d] = [\mathbb{S}^{td}]$
ℓrm
$[\mathbb{S}^{dt}] = [\mathbb{S}^{tdt}]$
$mr\ell$

Figure 3.2: The Knuth orbit $K(\mathbb{S})$ of symplectic semifield $\mathbb{S}$ with nuclei ℓmr

Chapter 4: The Knuth Orbit of Semifields

4.1 The Knuth Orbit of Commutative Semifields

4.1.1 Dickson Semifields

Dickson semifields [11] are semifields $(\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}, +, *)$ of order q^{2k}, q odd and $k > 1$ odd, with multiplication defined by

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

where j is a nonsquare in $\mathbb{F}_{q^k}$, σ is an $\mathbb{F}_q-$automorphism of $\mathbb{F}_{q^k}$, $\sigma \neq id$.

In order to obtain the multiplication for $\mathbb{S}^t$ we will use the alternating bilinear form:

$$\langle((a,b),(c,d)),((u,v),(s,t))\rangle = tr[as + bt - cu - dv] \tag{4.1}$$

to find all $((u,v),(s,t))$ such that :

$$\begin{aligned}
0 &= \langle((a,b),(a,b)*(c,d)),((u,v),(s,t))\rangle \\
&= \langle((a,b),(ac + jb^{\sigma}d^{\sigma}, ad + bc)),((u,v),(s,t))\rangle \\
&= tr[as + bt - u(ac + jb^{\sigma}d^{\sigma}) - v(ad + bc)] \\
&= tr[a(s - uc - vd) + bt - u^{\sigma^{-1}} j^{\sigma^{-1}} bd - vbc] \\
&= tr[a(s - uc - vd) + b(t - u^{\sigma^{-1}} j^{\sigma^{-1}} d - vc)]
\end{aligned}$$

Putting $a = 0$ we get the condition $tr[b(t - u^{\sigma^{-1}} j^{\sigma^{-1}} d - vc)] = 0$, for all b. This implies $t = u^{\sigma^{-1}} j^{\sigma^{-1}} d + vc$. Similarly, after putting $b = 0$ we get $s = uc + vd$. Hence after some coordinate transformations, we get the multiplication for $\mathbb{S}^t$:

$$(a,b)\bullet(c,d)=(ac+bd,a^{\sigma^{-1}}j^{\sigma^{-1}}d+bc).$$

Reversing this muliplication we get the semifield $\mathbb{S}^{td}$ by:

$$(a,b)\circ(c,d)=(ac+bd,c^{\sigma^{-1}}j^{\sigma^{-1}}b+ad).$$

We can confirm that $(\mathbb{S}^{td},+,\circ)$ is symplectic. Indeed,

$$\begin{aligned}
&\langle((a,b),(a,b)\circ(c,d)),((u,v),(u,v)\circ(c,d))\rangle\\
&= \langle((a,b),(ac+bd,c^{\sigma^{-1}}j^{\sigma^{-1}}b+ad)),((u,v),(uc+vd,j^{\sigma^{-1}}vc^{\sigma^{-1}}+ud))\rangle\\
&= tr[a(uc+vd)+b(j^{\sigma^{-1}}vc^{\sigma^{-1}}+ud)-u(ac+bd)-v(c^{\sigma^{-1}}j^{\sigma^{-1}}b+ad)]\\
&= tr[auc+avd+bj^{\sigma^{-1}}vc^{\sigma^{-1}}+bud-uac-ubd-vc^{\sigma^{-1}}j^{\sigma^{-1}}b-vad]\\
&= tr[0]\\
&= 0.
\end{aligned}$$

4.1.2 Ganley Semifields

These semifields $(\mathbb{F}_{3^r}\times\mathbb{F}_{3^r},+,*)$ are defined in [13] with

$$(a,b)*(c,d)=(ac-b^9d-bd^9,ad+bc+b^3d^3),$$

where $r \geq 3$ odd. We will apply the equation (4.1) :

$$\begin{aligned}
0 &= \langle ((a,b),(a,b)*(c,d)),((u,v),(s,t))\rangle \\
&= \langle ((a,b),(ac-b^9d-bd^9,ad+bc+b^3d^3)),((u,v),(s,t))\rangle \\
&= tr[as+bt-u(ac-b^9d-bd^9)-v(ad+bc+b^3d^3)] \\
&= tr[a(s-uc-vd)+bt+u^{3^{-2}}bd^{3^{-2}}+ubd^9-vbc-v^{3^{-1}}bd] \\
&= tr[a(s-uc-vd)+b(t+u^{\frac{1}{9}}d^{\frac{1}{9}}+ud^9-vc-v^{\frac{1}{3}}d]
\end{aligned}$$

Putting $a=0$ we get the condition $tr[b(t+u^{\frac{1}{9}}d^{\frac{1}{9}}+ud^9-vc-v^{\frac{1}{3}}d]=0$, for all b. This implies $t=vc+v^{\frac{1}{3}}d-ud^9-u^{\frac{1}{9}}d^{\frac{1}{9}}$. Similarly, after putting $b=0$ we get $s=uc+vd$. Hence after some coordinate transformations, we get the multiplication for S^t:

$$(a,b)\bullet(c,d)=(ac+bd,bc+b^{\frac{1}{3}}d-ad^9-a^{\frac{1}{9}}d^{\frac{1}{9}}).$$

Reversing this muliplication we get the multiplication for $\mathbb{S}^{td}$:

$$(a,b)\circ(c,d)=(ac+bd,ad+bd^{\frac{1}{3}}-b^9c-b^{\frac{1}{9}}c^{\frac{1}{9}}).$$

We have that $(\mathbb{S}^{td},+,\circ)$ is symplectic since:

$$\begin{aligned}
&\langle ((a,b),(a,b)\circ(c,d)),((u,v),(u,v)\circ(c,d))\rangle \\
&= \langle ((a,b),(ac+bd,ad+bd^{\frac{1}{3}}-b^9c-b^{\frac{1}{9}}c^{\frac{1}{9}})),((u,v), \\
&\quad (uc+vd,ud+vd^{\frac{1}{3}}-v^9c-v^{\frac{1}{9}}c^{\frac{1}{9}}))\rangle \\
&= tr[a(uc+vd)+b(ud+vd^{\frac{1}{3}}-v^9c-v^{\frac{1}{9}}c^{\frac{1}{9}}) \\
&\quad -u(ac+bd)-v(ad+bd^{\frac{1}{3}}-b^9c-b^{\frac{1}{9}}c^{\frac{1}{9}})] \\
&= tr[auc+avd+bud+bvd^{\frac{1}{3}}-bv^9c-bv^{\frac{1}{9}}c^{\frac{1}{9}} \\
&\quad -uac-ubd-vad-vbd^{\frac{1}{3}}+vb^9c+vb^{\frac{1}{9}}c^{\frac{1}{9}}] \\
&= tr[0] \\
&= 0.
\end{aligned}$$

4.1.3 The Penttila-Williams Semifield

This semifield [25] is given by $(\mathbb{F}_{3^5} \times \mathbb{F}_{3^5}, +, *)$, with

$$(a,b) * (c,d) = (ac + (bd)^9, ad + bc + (bd)^{27}).$$

Using equation(4.1), we will find all $((u,v),(s,t))$ such that :

$$\begin{aligned}
0 &= \langle((a,b),(a,b)*(c,d)),((u,v),(s,t))\rangle \\
&= \langle((a,b),(ac+(bd)^9, ad+bc+(bd)^{27})),((u,v),(s,t))\rangle \\
&= tr[as + bt - u(ac + (bd)^9) - v(ad + bc + (bd)^{27})] \\
&= tr[a(s - uc - vd) + bt - u^{3^3}bd - vbc - v^{3^2}bd] \\
&= tr[a(s - uc - vd) + b(t - u^{27}d - vc - v^9 d)]
\end{aligned}$$

If we put $b = 0$ then $tr[a(s - uc - vd)] = 0$, for all a and hence $s = uc + vd$. If we put $a = 0$ then $tr[b(t - u^{27}d - vc - v^9 d)] = 0$, for all b and hence $t = vc + v^9 d + u^{27} d$. By a straightforward change of coordinates we get the multiplication for $\mathbb{S}^t$:

$$(a,b) \bullet (c,d) = (ac + bd, bc + b^9 d + a^{27} d).$$

Swap a with c and b with d in the product formula for $\mathbb{S}^t$ to get the product for $\mathbb{S}^{td}$:

$$(a,b) \circ (c,d) = (ac + bd, ad + bd^9 + bc^{27}).$$

Note that $(\mathbb{S}^{td},+,\circ)$ is symplectic since:

$$\begin{aligned}
&\langle((a,b),(a,b)\circ(c,d)),((u,v),(u,v)\circ(c,d))\rangle\\
&= \langle((a,b),(ac+bd,ad+bd^9+bc^{27})),((u,v),(uc+vd,ud+vd^9+vc^{27}))\rangle\\
&= tr[a(uc+vd)+b(ud+vd^9+vc^{27})-u(ac+bd)-v(ad+bd^9+bc^{27})]\\
&= tr[auc+avd+bud+bvd^9+bvc^{27}-uac-ubd-vad-vbd^9-vbc^{27}]\\
&= tr[0]\\
&= 0.
\end{aligned}$$

4.1.4 Cohen-Ganley Semifields

Assume that $s \geq 3$ and j is a nonsquare in $\mathbb{F}_{3^s}$. The Cohen-Ganley [6] semifields $(\mathbb{F}_{3^s}\times\mathbb{F}_{3^s},+,*)$ are defined by

$$(a,b)*(c,d)=(ac+jbd+j^3(bd)^9,ad+bc+j(bd)^3).$$

To determine the product formula for $\mathbb{S}^t$, we will use equation (4.1) :

$$\begin{aligned}
0 &= \langle((a,b),(a,b)*(c,d)),((u,v),(s,t))\rangle\\
&= \langle((a,b),(ac+jbd+j^3(bd)^9,ad+bc+j(bd)^3)),((u,v),(s,t))\rangle\\
&= tr[as+bt-u(ac+jbd+j^3(bd)^9)-v(ad+bc+j(bd)^3)]\\
&= tr[a(s-uc-vd)+bt-ujbd-u^{3^{-2}}j^{3^{-1}}bd-vbc-v^{3^{-1}}j^{3^{-1}}bd]\\
&= tr[a(s-uc-vd)+b(t-ujd-u^{\frac{1}{9}}j^{\frac{1}{3}}d-vc-v^{\frac{1}{3}}j^{\frac{1}{3}}d)].
\end{aligned}$$

This implies that $s=uc+vd$ and $t=ujd+u^{\frac{1}{9}}j^{\frac{1}{3}}d+vc+v^{\frac{1}{3}}j^{\frac{1}{3}}d$. Therefore, $\mathbb{S}^t$ is defined by

$$(a,b)\bullet(c,d)=(ac+bd,ajd+a^{\frac{1}{9}}j^{\frac{1}{3}}d+bc+b^{\frac{1}{3}}j^{\frac{1}{3}}d).$$

Reversing this muliplication we get the semifield $\mathbb{S}^{td}$:

$$(a,b)\circ(c,d)=(ac+bd, cjb+c^{\frac{1}{9}}j^{\frac{1}{3}}b+ad+d^{\frac{1}{3}}j^{\frac{1}{3}}b).$$

Note that $(\mathbb{S}^{td},+,\circ)$ is symplectic since:

$$\begin{aligned}
&\langle((a,b),(a,b)\circ(c,d)),((u,v),(u,v)\circ(c,d))\rangle\\
&= \langle((a,b),(ac+bd, cjb+c^{\frac{1}{9}}j^{\frac{1}{3}}b+ad+d^{\frac{1}{3}}j^{\frac{1}{3}}b)),\\
&\quad ((u,v),(uc+vd, cjv+c^{\frac{1}{9}}j^{\frac{1}{3}}v+ud+d^{\frac{1}{3}}j^{\frac{1}{3}}v))\rangle\\
&= tr[a(uc+vd)+b(cjv+c^{\frac{1}{9}}j^{\frac{1}{3}}v+ud+d^{\frac{1}{3}}j^{\frac{1}{3}}v)\\
&\quad -u(ac+bd)-v(cjb+c^{\frac{1}{9}}j^{\frac{1}{3}}b+ad+d^{\frac{1}{3}}j^{\frac{1}{3}}b)]\\
&= [auc+avd+bcjv+bc^{\frac{1}{9}}j^{\frac{1}{3}}v+bud+bd^{\frac{1}{3}}j^{\frac{1}{3}}v\\
&\quad -uac-ubd-vcjb-vc^{\frac{1}{9}}j^{\frac{1}{3}}b-vad-vd^{\frac{1}{3}}j^{\frac{1}{3}}b]\\
&= tr[0]\\
&= 0.
\end{aligned}$$

4.1.5 Coulter-Henderson-Kosick Presemifield

This presemifield $\mathbb{S}=(\mathbb{F}_{3^8},+,*)$ is defined in [8, 9] by

$$x*y=xy+L(xy^9+x^9y-xy-x^9y^9)+x^{243}y^3+x^{81}y-x^9y+x^3y^{243}+xy^{81}-xy^9,$$

where $L(x)=x^{3^5}+x^{3^2}$.

In order to obtain the multiplication for $\mathbb{S}^t$ we will use the alternating bilinear form:

$$\langle(x,y),(u,v)\rangle=tr[xv-yu] \tag{4.2}$$

to find all (u,v) such that:

$$\begin{aligned}
0 &= \langle((x,x*y),(u,v))\rangle \\
&= tr[xv-uxy-ux^{3^5}y^{3^7}-ux^{3^7}y^{3^5}+ux^{3^5}y^{3^5}+ux^{3^7}y^{3^7}-ux^{3^2}y^{3^4}-ux^{3^4}y^{3^2} \\
&\quad +ux^{3^2}y^{3^2}+ux^{3^4}y^{3^4}-ux^{3^5}y^{3}-ux^{3^4}y+ux^{3^2}y-ux^{3}y^{3^5}-uxy^{3^4}+uxy^{3^2}] \\
&= tr[xv-uxy-u^{3^3}xy^{3^2}-u^{3}xy^{3^6}+u^{3^3}xy+u^{3}xy-u^{3^6}xy^{3^2}-u^{3^4}xy^{3^6} \\
&\quad +u^{3^6}xy+u^{3^4}xy-u^{3^3}xy^{3^4}-u^{3^4}xy^{3^4}+u^{3^6}xy^{3^6}-u^{3^7}xy^{3^4}-uxy^{3^4}+uxy^{3^2}] \\
&= tr[x(v-uy-u^{3^3}y^{3^2}-u^{3}y^{3^6}+u^{3^3}y+u^{3}y-u^{3^6}y^{3^2}-u^{3^4}y^{3^6}+u^{3^6}y \\
&\quad +u^{3^4}y-u^{3^3}y^{3^4}-u^{3^4}y^{3^4}+u^{3^6}y^{3^6}-u^{3^7}y^{3^4}-uy^{3^4}+uy^{3^2})].
\end{aligned}$$

This implies that $v=uy+u^{3^3}y^{3^2}+u^{3}y^{3^6}-u^{3^3}y-u^{3}y+u^{3^6}y^{3^2}+u^{3^4}y^{3^6}-u^{3^6}y-u^{3^4}y+u^{3^3}y^{3^4}+u^{3^4}y^{3^4}-u^{3^6}y^{3^6}+u^{3^7}y^{3^4}+uy^{3^4}-uy^{3^2}$. By a straightforward change of coordinates we get the multiplication for $\mathbb{S}^t$:

$$\begin{aligned}
x\bullet y &= xy+x^{3^3}y^{3^2}+x^{3}y^{3^6}-x^{3^3}y-x^{3}y+x^{3^6}y^{3^2}+x^{3^4}y^{3^6}-x^{3^6}y \\
&\quad -x^{3^4}y+x^{3^3}y^{3^4}+x^{3^4}y^{3^4}-x^{3^6}y^{3^6}+x^{3^7}y^{3^4}+xy^{3^4}-xy^{3^2}
\end{aligned}$$

Swap x with y in the product formula S^t to get the product for $\mathbb{S}^{td}$:

$$\begin{aligned}
x\circ y &= xy+y^{3^3}x^{3^2}+y^{3}x^{3^6}-y^{3^3}x-y^{3}x+y^{3^6}x^{3^2}+y^{3^4}x^{3^6}-y^{3^6}x-y^{3^4}x \\
&\quad +y^{3^3}x^{3^4}+y^{3^4}x^{3^4}-y^{3^6}x^{3^6}+y^{3^7}x^{3^4}+yx^{3^4}-yx^{3^2}.
\end{aligned}$$

4.1.6 Generalized Twisted Fields

A semifield $(\mathbb{F}_{q^t},+,*)$ of order $\mathbb{F}_{q^t}$, q odd and $t>1$ odd, with multiplication [3] defined by

$$x*y=x^{\alpha}y+xy^{\alpha},$$

where $\alpha : x \to x^{q^n}$ is automorphism of F_{q^t}. Then

$$x * y = x^{q^n} y + x y^{q^n}.$$

Using the alternating bilinear form (4.2), we will find all (u,v) such that:

$$\begin{aligned}
0 &= \langle((x, x*y),(u,v))\rangle \\
&= tr[xv - u(x^{q^n} y + x y^{q^n})] \\
&= [xv - u^{q^{t-n}} x y^{q^{t-n}} - u x y^{q^n}] \\
&= tr[x(v - u^{q^{t-n}} y^{q^{t-n}} - u y^{q^n})].
\end{aligned}$$

Therefore, $v = u^{q^{t-n}} y^{q^{t-n}} + u y^{q^n}$. After some coordinate transformations, we get the multiplication for $\mathbb{S}^t$:

$$x \bullet y = x^{q^{t-n}} y^{q^{t-n}} + x y^{q^n}.$$

Reversing this multiplication, we have multiplication for $\mathbb{S}^{td}$:

$$x \circ y = x^{q^{t-n}} y^{q^{t-n}} + x^{q^n} y.$$

4.1.7 Coulter-Matthews/Ding-Yuan Presemifields

These presemifields [7, 12] are given by $\mathbb{S} = (\mathbb{F}_{3^e}, +, *)$ with

$$x * y = x^9 y + x y^9 \mp x^3 y^3 + xy,$$

where $e \geq 3$ odd.

Using equation (4.2), we have

$$\begin{aligned}
0 &= \langle((x, x*y),(u,v))\rangle \\
&= tr[xv - u(x^9y + xy^9 \mp x^3y^3 + xy)] \\
&= [xv - u^{3^{-2}}xy^{3^{-2}} - uxy^9 \pm u^{3^{-1}}xy - uxy] \\
&= tr[x(v - u^{3^{-2}}y^{3^{-2}} - uy^9 \pm u^{3^{-1}}y - uy)].
\end{aligned}$$

Therefore, $v = u^{3^{-2}}y^{3^{-2}} + uy^9 \mp u^{3^{-1}}y + uy$.

By a straightforward change of coordinates, we get the multiplication for $\mathbb{S}^t$:

$$x \bullet y = x^{3^{-2}}y^{3^{-2}} + xy^9 \mp x^{3^{-1}}y + xy.$$

Interchanging x and y, we get the multiplication for $\mathbb{S}^{td}$:

$$x \circ y = x^{3^{-2}}y^{3^{-2}} + x^9y \mp xy^{3^{-1}} + xy.$$

4.1.8 Budaghyan-Helleseth Presemifields

Assume that p is odd prime, $m > 1$ and $0 < s < 2m$. The Budaghyan-Helleseth presemifields [5] $(\mathbb{F}_{p^{2m}}, +, *)$ are defined by

$$x * y = xy^{p^m} + x^{p^m}y + [\beta(xy^{p^s} + x^{p^s}y) + \beta^{p^m}(xy^{p^s} + x^{p^s}y)^{p^m}]\omega,$$

where ω is an element of $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ with $\omega^{p^m} = -\omega$.

We will apply the equation (4.2), to find the product formula for $\mathbb{S}^t$:

$$\begin{aligned} 0 &= \langle((x, x*y),(u,v))\rangle \\ &= tr[xv - uxy^{p^m} - ux^{p^m}y - \beta\omega uxy^{p^s} - \beta\omega ux^{p^s}y \\ &\quad - \beta^{p^m}\omega ux^{p^m}y^{p^{s+m}} - \beta^{p^m}\omega ux^{p^{s+m}}y^{p^m}] \\ &= tr[x(v - uy^{p^m} - u^{p^m}y^{p^m} - \beta\omega uy^{p^s} - \beta^{p^{-s}}\omega^{p^{-s}}u^{p^{-s}}y^{p^{-s}} \\ &\quad - \beta\omega^{p^m}u^{p^m}y^{p^s} - \beta^{p^{-s}}\omega^{p^{m-s}}u^{p^{m-s}}y^{p^{-s}}]. \end{aligned}$$

Therefore,

$$v = uy^{p^m} + u^{p^m}y^{p^m} + \beta\omega uy^{p^s} + \beta^{p^{-s}}\omega^{p^{-s}}u^{p^{-s}}y^{p^{-s}} + \beta\omega^{p^m}u^{p^m}y^{p^s} + \beta^{p^{-s}}\omega^{p^{m-s}}u^{p^{m-s}}y^{p^{-s}}.$$

So the multiplication for S^t is

$$\begin{aligned} x \bullet y &= xy^{p^m} + x^{p^m}y^{p^m} + \beta\omega xy^{p^s} + \beta^{p^{-s}}\omega^{p^{-s}}x^{p^{-s}}y^{p^{-s}} \\ &\quad + \beta\omega^{p^m}x^{p^m}y^{p^s} + \beta^{p^{-s}}\omega^{p^{m-s}}x^{p^{m-s}}y^{p^{-s}} \end{aligned}$$

Swap x with y in the product formula $\mathbb{S}^t$ to get the product for $\mathbb{S}^{td}$:

$$x \circ y = x^{p^m}y + x^{p^m}y^{p^m} + \beta\omega x^{p^s}y + \beta^{p^{-s}}\omega^{p^{-s}}x^{p^{-s}}y^{p^{-s}} + \beta\omega^{p^m}x^{p^s}y^{p^m} + \beta^{p^{-s}}\omega^{p^{m-s}}x^{p^{-s}}y^{p^{m-s}}$$

In a similar way, we calculate the Knuth orbit of other known semifields.

4.1.9 Zha-Kyureghyan-Wang Presemifields

Let u be a primitive element of $\mathbb{F}_{p^{3s}}$ and let $0 < t < 3s$. The Zha-Kyureghyan-Wang presemifields [27] $(\mathbb{F}_{p^{3s}}, +, *)$ are defined by

$$x * y = y^{p^t}x + yx^{p^t} - u^{p^s-1}(y^{p^{s+t}}x^{p^{2s}} + y^{p^{2s}}x^{p^{s+t}}).$$

Then for $\mathbb{S}^t$ we have

$$x \bullet y = y^{p^t}x + y^{p^{3s-t}}x^{p^{3s-t}} - u^{p^s(p^s-1)}y^{p^{2s+t}}x^{p^s} - u^{p^{2s-t}(p^s-1)}y^{p^{s-t}}x^{p^{2s-t}},$$

and for $\mathbb{S}^{td}$ we have

$$x \circ y = yx^{p^t} + y^{p^{3s-t}}x^{p^{3s-t}} - u^{p^s(p^s-1)}y^{p^s}x^{p^{2s+t}} - u^{p^{2s-t}(p^s-1)}y^{p^{2s-t}}x^{p^{s-t}}.$$

4.1.10 Bierbrawer Presemifields

These presemifields $(\mathbb{F}_{p^{4s}}, +, *)$ are defined [4] with

$$x * y = y^{p^t}x + yx^{p^t} - u^{p^s-1}(y^{p^{s+t}}x^{p^{3s}} + y^{p^{3s}}x^{p^{s+t}}),$$

where u is a primitive element of $\mathbb{F}_{p^{4s}}$. Then for $\mathbb{S}^t$ we have

$$x \bullet y = y^{p^t}x + y^{p^{4s-t}}x^{p^{4s-t}} - u^{p^s(p^s-1)}y^{p^{2s+t}}x^{p^s} - u^{p^{3s-t}(p^s-1)}y^{p^{2s-t}}x^{p^{3s-t}},$$

and for $\mathbb{S}^{td}$ we have

$$x \circ y = yx^{p^t} + y^{p^{4s-t}}x^{p^{4s-t}} - u^{p^s(p^s-1)}y^{p^s}x^{p^{2s+t}} - u^{p^{3s-t}(p^s-1)}y^{p^{3s-t}}x^{p^{2s-t}}.$$

4.1.11 Knuth's Binary Semifields

Knuth's binary semifields [20] consist of elements of the field $\mathbb{F}_{q^n}$ for q even, $n > 1$ odd and trace map $T : \mathbb{F}_{q^n} \to \mathbb{F}_q$ with multiplication defined by

$$\begin{aligned} x * y &= xy + (T(x)y + T(y)x)^2 \\ &= xy + T(x)^2y^2 + T(y)^2x^2. \end{aligned}$$

Then

$$\begin{aligned}
0 &= \langle((((x,x*y),(u,v))\rangle \\
&= \langle((xv-u(xy+T(x)^2y^2+T(y)^2x^2))\rangle \\
&= tr[xv+uxy+\sqrt{u}y\sum_{i=0}^{n-1}x^{q^i}+\sqrt{u}x\sum_{i=0}^{n-1}y^{q^i}] \\
&= tr[xv+uxy+x\sum_{i=0}^{n-1}(\sqrt{u}y)^{q^{-i}}+\sqrt{u}x\sum_{i=0}^{n-1}y^{q^i}] \\
&= tr[x(v+uy+\sum_{i=0}^{n-1}(\sqrt{u}y)^{q^{-i}}+\sqrt{u}\sum_{i=0}^{n-1}y^{q^i})].
\end{aligned}$$

Therefore, $v = uy+\sum_{i=0}^{n-1}(\sqrt{u}y)^{q^{-i}}+\sqrt{u}\sum_{i=0}^{n-1}y^{q^i}$ and the multiplication for $\mathbb{S}^t = (\mathbb{S}^t,+,\bullet)$ is given by:

$$x\bullet y = xy+\sum_{i=0}^{n-1}(\sqrt{x}y)^{q^{-i}}+\sqrt{x}\sum_{i=0}^{n-1}y^{q^i}.$$

Furthermore, the multiplication of $\mathbb{S}^{td} = (\mathbb{S}^{td},+,\circ)$ is

$$\begin{aligned}
x\circ y &= y\bullet x \\
&= xy+\sum_{i=0}^{n-1}(\sqrt{y}x)^{q^{-i}}+\sqrt{y}\sum_{i=0}^{n-1}x^{q^i} \\
&= xy+T(x\sqrt{y})+\sqrt{y}T(x).
\end{aligned}$$

4.1.12 The Kantor-Williams Presemifields

Assume that we have a chain of fields $F = F_0 \supset F_1 \supset \ldots \supset F_n \supseteq K = \mathbb{F}_2, n \geq 1$ with $F = \mathbb{F}_{2^m}$, $m > 1$ odd, $\zeta \in F$ and $T_i : F \to F_i$ are the trace functions. Then the multiplication

$$\begin{aligned}
x*y &= xy+(x\sum_1^n T_i(\zeta_i y)+y\sum_1^n T_i(\zeta_i x))^2 \\
&= xy+x^2\sum_1^n T_i(\zeta_i y)^2+y^2\sum_1^n T_i(\zeta_i x)^2
\end{aligned}$$

defines the Kantor commutative presemifields [16]. We calculate now corresponding symplectic presemifield (which are called Kantor-Williams presemifields [17]).

$$\begin{aligned}
0 &= \langle((x, x*y),(u,v))\rangle \\
&= \langle(xv - u(xy + x^2\sum_1^n T_i(\zeta_i y)^2 + y^2\sum_1^n T_i(\zeta_i x)^2))\rangle \\
&= tr[xv + uxy + x^2u\sum_1^n T_i(\zeta_i y)^2 + y^2u\sum_1^n T_i(\zeta_i x)^2] \\
&= tr[xv + uxy + xu^{\frac{1}{2}}\sum_1^n T_i(\zeta_i y) + yu^{\frac{1}{2}}\sum_1^n T_i(\zeta_i x)] \\
&= tr[xv + xuy + xu^{\frac{1}{2}}\sum_1^n T_i(\zeta_i y) + x\sum_1^n \zeta_i T_i(u^{\frac{1}{2}}y)] \\
&= tr[x(v + uy + u^{\frac{1}{2}}\sum_1^n T_i(\zeta_i y) + \sum_1^n \zeta_i T_i(u^{\frac{1}{2}}y))].
\end{aligned}$$

Therefore, $v = uy + u^{\frac{1}{2}}\sum_1^n T_i(\zeta_i y) + \sum_1^n \zeta_i T_i(u^{\frac{1}{2}}y)$ and the multiplication of $\mathbb{S}^t = (\mathbb{S}^t, +, \bullet)$ is

$$x \bullet y = xy + x^{\frac{1}{2}}\sum_1^n T_i(\zeta_i y) + \sum_1^n \zeta_i T_i(x^{\frac{1}{2}}y),$$

and the multiplication of $\mathbb{S}^{td} = (\mathbb{S}^{td}, +, \circ)$ is

$$x \circ y = y \bullet x = xy + y^{\frac{1}{2}}\sum_1^n T_i(\zeta_i x) + \sum_1^n \zeta_i T_i(y^{\frac{1}{2}}x).$$

4.2 The Knuth Orbit of Noncommutative Semifields

Suppose $a = x^{1+\theta} + xb$ has no solution for $x \in \mathbb{F}_q$. Then ***Hughes-Kleinfeld Semifields*** [15] are semifields $(\mathbb{F}_q \times \mathbb{F}_q, +, *)$ of order q^2, q odd, with multiplication defined by

$$(x,y)*(z,t) = (xz + aty^\theta, yz + x^\theta t + y^\theta bt).$$

In order to obtain the multiplication for $\mathbb{S}^t$, we have to find all $((u,v),(c,d))$ for which:

$$\begin{aligned}
0 &= \langle((x,y),(x,y)*(z,t)),((u,v),(c,d))\rangle \\
&= \langle((x,y),((xz+aty^{\theta}),(yz+x^{\theta}t+y^{\theta}bt))),((u,v),(c,d))\rangle \\
&= tr[xc+yd-u(xz+aty^{\theta})-v(yz+x^{\theta}t+y^{\theta}bt)] \\
&= tr[x(c-uz-v^{\theta^{-1}}t^{\theta^{-1}})+y(d-u^{\theta^{-1}}a^{\theta^{-1}}t^{\theta^{-1}}-vz-v^{\theta^{-1}}b^{\theta^{-1}}t^{\theta^{-1}}]
\end{aligned}$$

Putting $x=0$ we get the condition $tr[y(d-u^{\theta^{-1}}a^{\theta^{-1}}t^{\theta^{-1}}-vz-v^{\theta^{-1}}b^{\theta^{-1}}t^{\theta^{-1}})]$, for all $y\in\mathbb{F}_q$. This implies $d=vz+u^{\theta^{-1}}a^{\theta^{-1}}t^{\theta^{-1}}+v^{\theta^{-1}}b^{\theta^{-1}}t^{\theta^{-1}}$. Similarly, after putting $y=0$ we get $c=uz+v^{\theta^{-1}}t^{\theta^{-1}}$. Hence, after some coordinate transformations, we get the multiplication for $\mathbb{S}^t=(\mathbb{S}^t,+,\bullet)$:

$$(x,y)\bullet(z,t)=(xz+y^{\theta^{-1}}t^{\theta^{-1}},yz+x^{\theta^{-1}}a^{\theta^{-1}}t^{\theta^{-1}}+y^{\theta^{-1}}b^{\theta^{-1}}t^{\theta^{-1}}).$$

Reversing this multiplication we get the multiplication for $\mathbb{S}^{td}=(\mathbb{S}^{td},+,\circ)$:

$$(x,y)\circ(z,t)=(xz+t^{\theta^{-1}}y^{\theta^{-1}},xt+z^{\theta^{-1}}a^{\theta^{-1}}y^{\theta^{-1}}+t^{\theta^{-1}}b^{\theta^{-1}}y^{\theta^{-1}}).$$

To find the product formula for $\mathbb{S}^{tdt}$, we will use the alternating bilinear form (4.1) such that:

$$\begin{aligned}
0 &= \langle((x,y),(x,y)*(z,t)),((u,v),(c,d))\rangle \\
&= \langle((x,y),(xz+t^{\theta^{-1}}y^{\theta^{-1}},xt+z^{\theta^{-1}}a^{\theta^{-1}}y^{\theta^{-1}}+t^{\theta^{-1}}b^{\theta^{-1}}y^{\theta^{-1}})),((u,v),(c,d))\rangle \\
&= tr[xc+yd-u(xz+t^{\theta^{-1}}y^{\theta^{-1}})-v(xt+z^{\theta^{-1}}a^{\theta^{-1}}y^{\theta^{-1}}+t^{\theta^{-1}}b^{\theta^{-1}}y^{\theta^{-1}})] \\
&= tr[x(c-uz-vt)+y(d-tu^{\theta}-zav^{\theta}-tbv^{\theta})].
\end{aligned}$$

This implies that $c = uz + vt$, $d = tu^{\theta} + zav^{\theta} + tbv^{\theta}$. Therefore, multiplication for $\mathbb{S}^{tdt} = (\mathbb{S}^{tdt}, +, \times)$ is

$$(x,y) \times (z,t) = (xz + yt, tx^{\theta} + zay^{\theta} + tby^{\theta}).$$

Swap x with z and y with t in the product formula for S to get the product for $\mathbb{S}^{d} = (\mathbb{S}^{d}, +, \diamond):$

$$(x,y) \diamond (z,t) = (z,t) * (x,y) = (xz + ayt^{\theta}, xt + z^{\theta}y + t^{\theta}by).$$

Using equation(4.1), we will find all $((u,v),(c,d))$ such that:

$$\begin{aligned}
0 &= \langle((x,y),(x,y) \diamond (z,t)),((u,v),(c,d))\rangle \\
&= \langle((x,y),(xz + ayt^{\theta}, xt + z^{\theta}y + t^{\theta}by)),((u,v),(c,d))\rangle \\
&= tr[xc + yd - u(xz + ayt^{\theta}) - v(xt + z^{\theta}y + t^{\theta}by)] \\
&= tr[x(c - uz - vt) + y(d - uat^{\theta} - vz^{\theta} - vt^{\theta}b)].
\end{aligned}$$

This implies that $c = uz + vt$, $d = uat^{\theta} + vz^{\theta} + vt^{\theta}b$. Therefore, $\mathbb{S}^{dt} = (\mathbb{S}^{dt}, +, \star)$ is given by:

$$(x,y) \star (z,t) = (xz + yt, xat^{\theta} + yz^{\theta} + yt^{\theta}b).$$

Chapter 5: Planar Function

5.1 Planar Functions In Odd Characteristic

Let $q = p^n$, where p is an odd prime and n is a positive integer. A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is called a planar function if for each nonzero $a \in \mathbb{F}_q$, $f(x+a) - f(x)$ is a bijection on $\mathbb{F}_q$. There is a one to one correspondence between commutative semifields of odd orders and planar functions. Given a commutative semifields $S = (\mathbb{F}_q, +, *)$ of odd order, the function given by $F(x) = x * x$ is a planar function [10]. Conversely, given a planar function $f(x) \in \mathbb{F}_q[x]$, q is odd, then $S = (\mathbb{F}_q, +, *)$ with $x * y = \frac{1}{2}(f(x+y) - f(x) - f(y))$ for any $x, y \in \mathbb{F}_q$, is a commutative semifield.

We calculated the planar functions of known commutative semifields.

Generalized twisted fields: Assume that q odd and $t > 1$ odd. The Generalized twisted fields $(\mathbb{F}_{q^t}, +, *)$ are defined by

$$x * y = x^{\alpha} y + x y^{\alpha},$$

where $\alpha : x \to x^{q^n}$ is automorphism of $\mathbb{F}_{q^t}$. Then , $f(x) = x * x$ is expressed as the following :

$$f(x) = x^{q^n} \cdot x + x \cdot x^{q^n} = 2x^{q^n+1}.$$

Coulter-Matthews/Ding-Yuan presemifields: Consider presdemifield $(\mathbb{F}_{3^e}, +, *)$, where $e \geq 3$ odd. A multiplication is defined as

$$x * y = x^9 y + x y^9 \mp x^3 y^3 + xy$$

Then, we have

$$\begin{aligned} f(x) &= 2x^{10} \mp x^6 + x^2 \\ &= -x^{10} \mp x^6 + x^2 \end{aligned}$$

Coulter-Henderson-Kosick presemifield: This presemifield $(\mathbb{F}_{3^8}, +, *)$ is defined by

$$x * y = xy + L(xy^9 + x^9y - xy - x^9y^9) + x^{243}y^3 + x^{81}y - x^9y + x^3y^{243} + xy^{81} - xy^9,$$

where $L(x) = x^{3^5} + x^{3^2}$. Then we have

$$\begin{aligned} f(x) &= x^2 + L(2x^{10} - x^2 - x^{18}) + 2x^{246} + 2x^{82} - 2x^{10} \\ &= x^2 + (2x^{10} - x^2 - x^{18})^{3^5} + (2x^{10} - x^2 - x^{18})^{3^2} + 2x^{246} + 2x^{82} - 2x^{10} \\ &= x^2 + (x^{243} + x^9)(2x^{10} - x^2 - x^{18}) + 2x^{246} + 2x^{82} - 2x^{10}. \end{aligned}$$

Zha-Kyureghyan-Wang presemifields: Consider $(\mathbb{F}_{p^{3s}}, +, *)$. A multiplication is defined by

$$x * y = y^{p^t}x + yx^{p^t} - u^{p^s-1}(y^{p^{s+t}}x^{p^{2s}} + y^{p^{2s}}x^{p^{s+t}}),$$

where u be a primitive element of $\mathbb{F}_{p^{3s}}$ and $0 < t < 3s$.

Then we have

$$f(x) = 2x^{p^t+1} - u^{p^s-1}(2x^{p^{2s}+p^{s+t}}).$$

Bierbrawer presemifields: These presemifields $(\mathbb{F}_{p^{4s}}, +, *)$ are defined with

$$x * y = y^{p^t}x + yx^{p^t} - u^{p^s-1}(y^{p^{s+t}}x^{p^{3s}} + y^{p^{3s}}x^{p^{s+t}}),$$

where u is a primitive element of $\mathbb{F}_{p^{4s}}$

Then we have

$$f(x) = 2x^{p^t+1} - u^{p^s-1}(2x^{p^{3s}+p^{s+t}}).$$

For the other known commutative semifields, we follow the method described in [23].

Cohen-Ganley semifields. A multiplication in $(\mathbb{F}_{q^2}, +, *)$ is defined as

$$(a+\lambda b)*(c+\lambda d) = (ac+\alpha bd+\alpha^3(bd)^9)+\lambda(ad+bc+\alpha(bd)^3)$$

with $q = 3^n$ $(n \geq 2)$ and α is nonsquare in $\mathbb{F}_q$ and $\{1, \lambda\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, where $\lambda^2 = \alpha$.

Let $X = x+\lambda y \in \mathbb{F}_{q^2}$. We consider planar functions of quadratic polynomials and express them in the finite field.

1. $f : X \to X*X = (x+\lambda y)*(x+\lambda y) = (x^2+\alpha y^2+\alpha^3 y^{18})+\lambda(2xy+\alpha y^6)$
2. $g_1 : X \to X^2 = x^2+\alpha y^2+2\lambda xy$
3. $g_2 : X \to X^{1+3^n} = (x+\lambda y)^{1+3^n} = (x+\lambda y)(x-\lambda y) = x^2-\alpha y^2$
4. $g_3 : X \to X^{2\cdot 3^n} = (x+\lambda y)^{2\cdot 3^n} = (x-\lambda y)^2 = x^2+\alpha y^2-2\lambda xy$

We use the expression $(g_1+g_3-2g_2)(X)$ to find y^2:

$$(g_1+g_3-2g_2)(X) = X^2+X^{2\cdot 3^n}-2X^{1+3^n} = 4\alpha y^2,$$

$$X^2+X^{2\cdot 3^n}+X^{1+3^n} = \alpha y^2.$$

Therefore, $y^2 = \alpha^{-1}(X^2 + X^{2\cdot 3^n} + X^{1+3^n})$. On the other hand,

$$\begin{aligned}(f-g_1)(X) &= X * X - X^2\\ &= (x^2 + \alpha y^2 + \alpha^3 y^{18}) + \lambda(2xy + \alpha y^6) - x^2 - \alpha y^2 - 2\lambda xy\\ &= \alpha^3 y^{18} + \lambda \alpha y^6\\ &= \alpha^3 \alpha^{-9}(X^{18} + X^{2\cdot 3^{n+2}} + X^{9+3^{n+2}}) + \lambda \alpha \alpha^{-3}(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}})\\ &= \alpha^{-6}(X^{18} + X^{2\cdot 3^{n+2}} + X^{9+3^{n+2}}) + \lambda \alpha^{-2}(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}})\end{aligned}$$

We find $f(X)$ using the equation $(f-g_1)(X) = f(X) - g_1(X)$:

$$\begin{aligned}f(X) &= g_1(X) + (f-g_1)(X)\\ &= X^2 + \alpha^{-6}(X^{18} + X^{2\cdot 3^{n+2}} + X^{9+3^{n+2}}) + \lambda \alpha^{-2}(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}}).\end{aligned}$$

The Penttila-Williams semifield. A multiplication in $(\mathbb{F}_{q^2}, +, *)$ is defined as

$$(a + \lambda b) * (c + \lambda d) = (ac + (bd)^9) + \lambda(ad + bc + (bd)^{27})$$

with $q = 3^5$ and α is nonsquare in $\mathbb{F}_{3^5}$ and $\{1, \alpha\}$ is a basis over $\mathbb{F}_{3^5}$ where $\lambda^2 = \alpha$. We find the equations of the following functions:

$$f(x) = X * X = (x + \lambda y) * (x + \lambda y) = (x^2 + y^{18}) + \lambda(2xy + y^{54}),$$

$$g_1(X) = X^2 = (x + \lambda y)^2 = x^2 + 2\lambda xy + \alpha y^2,$$

$$g_2(X) = X^{1+3^5} = (x + \lambda y)^{1+3^5} = x^2 - \alpha y^2,$$

$$g_3(X) = X^{2\cdot 3^5} = (x + \lambda y)^{2\cdot 3^5} = x^2 + \alpha y^2 - 2\lambda xy.$$

Then, we find y^2 using the expression $(g_1+g_3-2g_2)(X)$:

$$(g_1+g_3-2g_2)(X)=X^2+X^{2\cdot 3^5}-2X^{1+3^5}=4\alpha y^2,$$

$$X^2+X^{2\cdot 3^5}+X^{1+3^5}=\alpha y^2.$$

Therefore, $y^2=\alpha^{-1}(X^2+X^{2\cdot 3^5}+X^{1+3^5})$. Furthermore,

$$\begin{aligned}(f-g_1)(X) &= X*X-X^2\\ &= (x^2+y^{18})+\lambda(2xy+y^{54})-x^2-\alpha y^2-2\lambda xy\\ &= y^{18}+\lambda y^{54}-\alpha y^2\\ &= \alpha^{-9}(X^{18}+X^{2\cdot 3^7}+X^{9+3^7})+\lambda\alpha^{-27}(X^{54}+X^{2\cdot 3^8}+X^{27+3^8})\\ &\quad -(X^2+X^{2\cdot 3^5}+X^{1+3^5}).\end{aligned}$$

Thus,

$$\begin{aligned}f(X) &= g_1(X)+(f-g_1)(X)\\ &= X^2+\alpha^{-9}(X^{18}+X^{2\cdot 3^7}+X^{9+3^7})+\lambda\alpha^{-27}(X^{54}+X^{2\cdot 3^8}+X^{27+3^8})\\ &\quad -(X^2+X^{2\cdot 3^5}+X^{1+3^5})\end{aligned}$$

Ganley semifields. A multiplication in $(\mathbb{F}_{q^2},+,*)$ is defined as

$$(a+\lambda b)*(c+\lambda d)=(ac-b^9d-bd^9)+\lambda(ad+bc+b^3d^3)$$

with $q=3^n$ $(n\geq 3)$ and α is nonsquare in $\mathbb{F}_q$ and $\{1,\lambda\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, where $\lambda^2=\alpha$.

We first consider planar functions of quadratic polynomials and express them in the finite field:

1. $f:X\rightarrow X*X=(x+\lambda y)*(x+\lambda y)=(x^2-2y^{10})+\lambda(2xy+y^6)$.
2. $g_1:X\rightarrow X^2=x^2+\alpha y^2+2\lambda xy$.

3. $g_2 : X \to X^{1+3^n} = (x+\lambda y)^{1+3^n} = x^2 - \alpha y^2$.

4. $g_3 : X \to X^{2\cdot 3^n} = (x+\lambda y)^{2\cdot 3^n} = x^2 + \alpha y^2 - 2\lambda xy$.

Accordingly,

$$(g_1+g_3-2g_2)(X) = X^2 + X^{2\cdot 3^n} - 2X^{1+3^n} = 4\alpha y^2,$$

$$X^2 + X^{2\cdot 3^n} + X^{1+3^n} = \alpha y^2,$$

Therefore,

$$y^2 = \alpha^{-1}(X^2 + X^{2\cdot 3^n} + X^{1+3^n}).$$

On the other hand,

$$\begin{aligned}
(f-g_1)(X) &= X * X - X^2 \\
&= (x^2 - 2y^{10}) + \lambda(2xy + y^6) - x^2 - \alpha y^2 - 2\lambda xy \\
&= y^{10} + \lambda y^6 - \alpha y^2 \\
&= \lambda^{-10}[X^{10} - X^{9+3^n} - X^{1+9\cdot 3^n} + X^{10\cdot 3^n}] \\
&\quad + \lambda[\alpha^{-1}(X^2 + X^{2\cdot 3^n} + X^{1+3^n})]^3 - \alpha[\alpha^{-1}(X^2 + X^{2\cdot 3^n} + X^{1+3^n})] \\
&= \lambda^{-10}[X^{10} - X^{9+3^n} - X^{1+9\cdot 3^n} + X^{10\cdot 3^n}] \\
&\quad + \lambda\alpha^{-3}(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}}) - (X^2 + X^{2\cdot 3^n} + X^{1+3^n}).
\end{aligned}$$

Hence,

$$\begin{aligned}
f(X) &= g_1(X) + (f-g_1)(X) \\
&= X^2 + \lambda^{-10}[X^{10} - X^{9+3^n} - X^{1+9\cdot 3^n} + X^{10\cdot 3^n}] \\
&\quad + \lambda\alpha^{-3}(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}}) - (X^2 + X^{2\cdot 3^n} + X^{1+3^n}).
\end{aligned}$$

In similar way, we find the planar function of Dickson semifields.

Dickson semifields. Assume that $q = p^n$, where p is an odd prime, $n > 1$ and let α be any element of $\mathbb{F}_q$ which is not square. A multiplication is defined as

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

with $\{1,\lambda\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, $\lambda^2 = \alpha$ and σ is an automorphism of $\mathbb{F}_q$ given by $x^{\sigma} = x^{p^r}, 1 \leq r < n$. Then , $f(X) = X*X$ is expressed as the following:

$$f(X) = X^2 + 4^{-1}\alpha^{1-p^r}(X^{2p^r} + X^{2p^{n+r}} - 2X^{p^r+p^{n+r}}) - 4^{-1}(X^2 + X^{2p^n} - 2X^{1+p^n}).$$

5.2 Pseudo-Planar Functions

In this section, we introduce an analog of planar functions in even characteristic. Let $F = \mathbb{F}_q$ be a finite field of even order q. Planar functions cannot exist in characteristic two since, if q is even and x is a solution to $f(x+a) - f(x) = b$, then so $x+a$. This implies that x and $x+a$ are both mapped to b. Therefore, f is not a bijection on $\mathbb{F}_q$. Recently, a new notion of planar functions in even characteristic was proposed by Zhou [29]. However, the term "pseudo-planar" was first used by Abdukhalikov [1].

Definition 5.2.1. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called a pseudo-planar if for each nonzero $a \in \mathbb{F}_{2^n}$, $f(x+a) - f(x) + ax$ is a bijection on $\mathbb{F}_{2^n}$

The following theorem illustrates the relationship between pseudo-planar functions and commutative presemifields.

Theorem 5.2.1. *If $(F,+,*)$ is a commutative presemifield with multiplication given by*

$$x*y = xy + \sum_{i<j} a_{ij}(x^{2^i}y^{2^j} + x^{2^j}y^{2^i})$$

then $f(x) = \sum_{i<j} a_{ij}x^{2^i+2^j}$ is a pseudo-planar function and $x*y = xy + f(x+y) + f(x) + f(y)$.

Example. *The Kantor presemifields.* Assume that we have a chain of fields $F = F_0 \supset$

$F_1 \supset ... \supset F_n \supseteq K = \mathbb{F}_2, n \geq 1$ with $F = \mathbb{F}_{2^m}$, $m > 1$ odd and $T_i : F \to F_i$ is the trace function. The multiplication is defined as:

$$x * y = xy + x^2 \sum_1^n T_i(y)^2 + y^2 \sum_1^n T_i(x)^2.$$

Then $f(x) = (x \sum_1^n T_i(x))^2$ is *pseudo-planar* [29].

Note that this semifield is a generalization of Knuth's binary semifields, on which the multiplication is defined as:

$$x * y = xy + x^2 T(y)^2 + y^2 T(x)^2.$$

The pseudo-planar function derived from Knuth's semifields is

$$\begin{aligned} f(x) &= x^2 T(x)^2 \\ &= x^2 \sum_{i=0}^{m-1} (x^{2^i})^2 \\ &= x^2 (x^2 + x^{2^2} + x^{2^3} + ... + x^{2^{m-1}} + x^{2^m}) \\ &= \sum_{j=0}^{m-1} x^{2+2^j}. \end{aligned}$$

Chapter 6: The Nuclei of Commutative Semifields

In this chapter, we compute the middle nucleus and the center for some known commutative semifields.

6.1 Dickson Semifields

Consider $(\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}, +, *)$ where q odd and $k > 1$ odd. A multiplication is defined as

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

where j is a nonsquare in $\mathbb{F}_{q^k}$, σ is an $\mathbb{F}_q-$automorphism of $\mathbb{F}_{q^k}$, $\sigma \neq id$. We have

$$(a,b)*(1,0) = (1,0)*(a,b) = (a,b).$$

This implies that the identity of $\mathbb{S}$ is $(1,0)$. Assume $(x,0) \in N_m(\mathbb{S})$. Then we have

$$[(a,b)*(x,0)]*(c,d) = (a,b)*[(x,0)*(c,d)],$$

$$[(a,b)*(x,0)]*(c,d) = (xa,xb)*(c,d) = (xac + j(xb)^{\sigma}d^{\sigma}, xad + xbc),$$

$$(a,b)*[(x,0)*(c,d)] = (a,b)*(xc,xd) = (axc + jb^{\sigma}(xd)^{\sigma}, xad + xbc).$$

Since $[(a,b)*(x,0)]*(c,d) = (a,b)*[(x,0)*(c,d)]$ for all $a,b,c,d \in \mathbb{F}_{q^k}$, we have that the middle nucleus contains all the elements of the form $(x,0)$, $x \in \mathbb{F}_{q^k}$. Furthermore, $\mathbb{S}$ can be viewed as a vector space over its middle nucleus $N_m(\mathbb{S})$. Let $N = \{(x,0) : x \in \mathbb{F}_{q^k}\}$, $N \cong \mathbb{F}_{q^k}$. Since $N \subseteq N_m(\mathbb{S})$ and $\mathbb{S}$ is a vector space over N of dimension 2, we obtain that $N_m(\mathbb{S}) = N$ or $N_m(\mathbb{S}) = \mathbb{S}$. But $\mathbb{S}$ is a semifield in which multiplication is not associative, and $N_m(S)$ is a field. Therefore, $N_m(\mathbb{S}) \neq \mathbb{S}$. We conclude that the middle nucleus of $\mathbb{S}$ is $N_m(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_{q^k}\}$.

To show that the left nucleus of $\mathbb{S}$ is $N_\ell(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_q\}$, we need to have

$$[(x,0)*(a,b)]*(c,d) = (x,0)*[(a,b)*(c,d)],$$

$$[(x,0)*(a,b)]*(c,d) = (xa,xb)*(c,d) = (xac+j(xb)^\sigma d^\sigma, xad+xbc),$$

$$(x,0)*[(a,b)*(c,d)] = (x,0)*(ac+jb^\sigma d^\sigma, ad+bc) = (xac+jxb^\sigma d^\sigma, xad+xbc).$$

Then $[(x,0)*(a,b)]*(c,d) = (x,0)*[(a,b)*(c,d)]$ if and only if $xac+j(xb)^\sigma d^\sigma = xac+jxb^\sigma d^\sigma$, which means $x^\sigma = x$. Thus,

$$N(\mathbb{S}) = N_\ell(\mathbb{S}) = N_r(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_q\}.$$

It is clear that

$$C(\mathbb{S}) = N(\mathbb{S}).$$

6.2 Penttila-Williams Semifield

This semifield [25] is given by $(\mathbb{F}_{3^5} \times \mathbb{F}_{3^5}, +, *)$, with

$$(a,b)*(c,d) = (ac+(bd)^9, ad+bc+(bd)^{27}).$$

The identity of $\mathbb{S}$ is $(1,0)$, since $(a,b)*(1,0) = (1,0)*(a,b) = (a,b)$. Assume $(x,0) \in N_m(\mathbb{S})$. Then we have

$$[(a,b)*(x,0)]*(c,d) = (a,b)*[(x,0)*(c,d)],$$

$$[(a,b)*(x,0)]*(c,d) = (xa,xb)*(c,d) = (xac+(xbd)^9, xad+xbc+(xbd)^{27}),$$

$$(a,b)*[(x,0)*(c,d)] = (a,b)*(xc,xd) = (xac+(xbd)^9, xad+xbc+(xbd)^{27}).$$

This implies that $[(a,b)*(x,0)]*(c,d)=(a,b)*[(x,0)*(c,d)]$ for all $a,b,c,d\in\mathbb{F}_{3^5}$ We derive that the middle nucleus contains all the elements of the form $(x,0)$, $x\in\mathbb{F}_{3^5}$. On the other hand, $\mathbb{S}$ can be viewed as a vector space over its middle nucleus $N_m(\mathbb{S})$. Let $N=\{(x,0):x\in\mathbb{F}_{3^5}\}$, $N\cong\mathbb{F}_{3^5}$. Since $N\subseteq N_m(\mathbb{S})$ and $\mathbb{S}$ is a vector space over N of dimension 2, we obtain $N_m(\mathbb{S})=N$ or $N_m(\mathbb{S})=\mathbb{S}$. But $\mathbb{S}$ is a semifield in which multiplication is not associative, and $N_m(\mathbb{S})$ is a field. Therefore, $N_m(\mathbb{S})\neq\mathbb{S}$. Thus, the middle nucleus of $\mathbb{S}$ is $N_m(\mathbb{S})=\{(x,0):x\in\mathbb{F}_{3^5}\}$.

We show the nucleus and center of $\mathbb{S}$ is $N(\mathbb{S})=\{(x,0):x\in\mathbb{F}_3\}$. Indeed,

$$[(x,0)*(a,b)]*(c,d)=(x,0)*[(a,b)*(c,d)],$$

$$\begin{aligned}[(x,0)*(a,b)]*(c,d)&=(xa,xb)*(c,d)\\&=(xac+(xbd)^9,xad+xbc+(xbd)^{27}),\end{aligned}$$

$$\begin{aligned}(x,0)*[(a,b)*(c,d)]&=(x,0)*(ac+(bd)^9,ad+bc+(bd)^{27})\\&=(xac+x(bd)^9,xad+xbc+x(bd)^{27}).\end{aligned}$$

Then $[(x,0)*(a,b)]*(c,d)=(x,0)*[(a,b)*(c,d)]$ if and only if

$$(xbd)^9=x(bd)^9 \tag{6.1}$$

and

$$(xbd)^{27}=x(bd)^{27}. \tag{6.2}$$

From (6.1) and (6.2) we get $N(\mathbb{S})=F_3$.

6.3 Ganley Semifields

Assume $r \geq 3$ odd. The Ganley [13] semifields $(\mathbb{F}_{3^r} \times \mathbb{F}_{3^r}, +, *)$ are defined by

$$(a,b)*(c,d) = (ac - b^9d - bd^9, ad + bc + b^3d^3).$$

We have $(a,b)*(1,0) = (1,0)*(a,b) = (a,b)$. Therefore, the identity of $\mathbb{S}$ is $(1,0)$.

Let $(x,y) \in N_m(\mathbb{S})$. Then we have,

$$[(0,b)*(x,y)]*(0,1) = (0,b)*[(x,y)*(0,1)],$$

$$\begin{aligned} [(0,b)*(x,y)]*(0,1) &= (-b^9y - by^9, bx + b^3y^3)*(0,1) \\ &= (-b^9x^9 - b^{27}y^{27} - bx - b^3y^3, -b^9y - by^9 + b^3x^3 + b^9y^9), \end{aligned}$$

$$\begin{aligned} (0,b)*[(x,y)*(0,1)] &= (0,b)*(-y^9 - y, x + y^3) \\ &= (-b^9x - b^9y^3 - bx^9 - by^{27}, -by^9 - by + b^3x^3 + b^3y^9). \end{aligned}$$

Comparing the second components, we have

$$-b^9y + b^9y^9 = -by + b^3y^9,$$

$$(y^9 - y)b^9 - y^9b^3 + yb = 0$$

for any $b \in \mathbb{F}_{3^r}$. This means that the polynomial $f(X) = (y^9 - y)X^9 - y^9X^3 + yX$ has 3^r zeroes unless it is equal to 0. Therefore, $y = 0$.

Assume $(x,0) \in N_m(\mathbb{S})$. Then we have

$$[(a,b)*(x,0)]*(c,d) = (a,b)*[(x,0)*(c,d)],$$

$$[(a,b)*(x,0)]*(c,d) = (xa,xb)*(c,d) = (xac-(bx)^9d-bxd^9, xad+xbc+(xbd)^3),$$

$$(a,b)*[(x,0)*(c,d)] = (a,b)*(xc,xd) = (xac-b^9xd-b(xd)^9, xad+xbc+(xbd)^3).$$

Then $[(a,b)*(x,0)]*(c,d) = (a,b)*[(x,0)*(c,d)]$ if and only if

$$\begin{aligned} xac-(bx)^9d-bxd^9 &= xac-b^9xd-b(xd)^9, \\ x^9(bd^9-b^9d) &= x(bd^9-b^9d), \\ x^9 &= x. \end{aligned}$$

Since r is odd, we have $x \in \mathbb{F}_3$. Thus, the middle nucleus of S is $N_m(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_3\}$. Since $\mathbb{F}_3$ is a prime field, we have

$$N(\mathbb{S}) = N_\ell(\mathbb{S}) = N_r(\mathbb{S}) = N_m(\mathbb{S}) = C(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_3\}.$$

6.4 Cohen-Ganley Semifields

Let $s \geq 3$ and let j be a nonsquare in $\mathbb{F}_{3^s}$. The Cohen-Ganley [6] semifields $(\mathbb{F}_{3^s} \times \mathbb{F}_{3^s}, +, *)$ are defined by

$$(a,b)*(c,d) = (ac+jbd+j^3(bd)^9, ad+bc+j(bd)^3).$$

We have $(a,b)*(1,0) = (1,0)*(a,b) = (a,b)$. Therefore, the identity of $\mathbb{S}$ is $(1,0)$. Assume $(x,0) \in N_m(\mathbb{S})$. Then we have,

$$[(a,b)*(x,0)]*(c,d) = (a,b)*[(x,0)*(c,d)],$$

$$[(a,b)*(x,0)]*(c,d) = (xa,xb)*(c,d) = (xac+jbxd+j^3(bxd)^9, xad+xbc+j(xbd)^3),$$

$$(a,b)*[(x,0)*(c,d)] = (a,b)*(xc,xd) = (xac+jbxd+j^3(bxd)^9, xad+xbc+j(xbd)^3).$$

Therefore, $[(a,b)*(x,0)]*(c,d) = (a,b)*[(x,0)*(c,d)]$ for all $a,b,c,d,x \in F_{3^s}$. Thus, the middle nucleus contains all the elements of the form $(x,0)$, $x \in \mathbb{F}_{3^s}$. Furthermore, $\mathbb{S}$ can be viewed as a vector space over its middle nucleus $N_m(\mathbb{S})$. Let $N = \{(x,0) : x \in \mathbb{F}_{3^s}\}$, $N \cong \mathbb{F}_{3^s}$. Since $N \subseteq N_m(\mathbb{S})$ and $\mathbb{S}$ is a vector space over N of dimension 2, we obtain $N_m(\mathbb{S}) = N$ or $N_m(\mathbb{S}) = \mathbb{S}$. But $\mathbb{S}$ is a semifield in which multiplication is not associative , and $N_m(\mathbb{S})$ is a field. Therefore, $N_m(\mathbb{S}) \neq \mathbb{S}$. Hence, the middle nucleus of $\mathbb{S}$ is $N_m(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_{3^s}\}$.

The nucleus of $\mathbb{S}$ is $N(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_3\}$ since

$$[(x,0)*(a,b)]*(c,d) = (x,0)*[(a,b)*(c,d)],$$

$$[(x,0)*(a,b)]*(c,d) = (xa,xb)*(c,d) = (xac+jxbd+j^3(xbd)^9, xad+xbc+j(xbd)^3),$$

$$\begin{aligned} (x,0)*[(a,b)*(c,d)] &= (x,0)*(ac+jbd+j^3(bd)^9, ad+bc+j(bd)^3) \\ &= (xac+jxbd+j^3x(bd)^9, xad+xbc+jxb^3d^3). \end{aligned}$$

Then $[(x,0)*(a,b)]*(c,d) = (x,0)*[(a,b)*(c,d)]$ if and only if

$$xac+jxbd+j^3(xbd)^9 = xac+jxbd+j^3x(bd)^9,$$

$$x^9 = x \tag{6.3}$$

and

$$xad+xbc+j(xbd)^3 = xad+xbc+jxb^3d^3$$

$$x^3 = x \tag{6.4}$$

From (6.3) and (6.4) we get $N(\mathbb{S}) = \mathbb{F}_3$. Therefore, $C(\mathbb{S}) = \mathbb{F}_3$.

Nuclei for remaining known commutative semifields can be found in [22].

Chapter 7: Mutually Unbiased Bases

7.1 Definitions

Mutually unbiased bases (MUBs) are a structure first defined in a quantum physics context in 1960 by Schwinger. Then in 1981 Ivanovic provided a construction of MUBs in odd prime power dimensions. In 1989 Wootters and Fields extended the Ivanovic construction to all odd prime powers and provided a construction for even prime powers. In 2003 Klappenecker and Rotteler published a summary of known constructions which included the sets of MUBs and descirbed by Wootters and Fields and Ivanovic. Recently it was discovered that MUBs are very closely related or even equivalent to other problems in various parts of mathematics, such as algebraic combinatorics, finite geometry, discrete mathematics, coding theory, metric geometry, sequences, and spherical codes [1, 2].

Let $\mathbb{C}^n$ be a vector space of dimension n over the field $\mathbb{C}$ of complex numbers. A basis for $\mathbb{C}^n$ is orthonormal if all basis vectors are orthogonal and of unit length. A pair of orthonormal bases $\{e_1,...,e_n\}$ and $\{f_1,...,f_n\}$ are said to be mutually unbiased if the square of the absolute value of the inner product of any two vectors from distinct bases is equal to $1/n$. (i.e $\left|\langle e_i, f_j\rangle\right|^2 = \frac{1}{n}$ for $1 \leq i, j \leq n$). A set $\{B_0, B_1, ..., B_r\}$ of orthonormal bases in $\mathbb{C}^n$ is said to be mutually unbiased bases (MUBs) if each pair of orthonormal bases is mutually unbiased.

The maximum number of mutually unbiased bases in $\mathbb{C}^n$ is $n+1$. A set of $n+1$ MUBs is called complete. While constructions of complete sets of MUBs in $\mathbb{C}^n$ are known when n is a prime power, it is unknown if such complete sets exist in non-prime power dimensions.

7.2 Constructions

We introduce several constructions of MUBs. The first construction is based on ***planar functions over fields of odd characteristic***. Let $q = p^r$, $F = \mathbb{F}_{p^r}$ and let $\varepsilon \in \mathbb{C}$ be a primitive pth root of unity. Let $\{e_w, w \in F\}$ be the standard basis of $\mathbb{C}^q$.

Theorem 7.2.1. *Let F be a finite field of odd order q and f be a planar function on F. Then the following forms a complete set of MUBs:*

$$B_\infty = \{e_w, w \in F\}, \quad B_m = \{b_{m,v}, v \in F\},\ m \in F,$$

$$b_{m,v} = \frac{1}{\sqrt{q}} \sum_{w \in F} \varepsilon^{tr(\frac{1}{2}mf(w)+vw)} e_w.$$

Let $S = (F, +, *)$ be a commutative semifield of odd order. Then $f(x) = x * x$ is a planar function. Therefore, from the previous Theorem we get the construction of MUBs based on ***finite commutative semifields of odd order***.

Theorem 7.2.2. *Let $S = (F, +, *)$ be a commutative semifield of odd order. Then the following forms a complete set of MUBs:*

$$B_\infty = \{e_w, w \in F\}, \quad B_m = \{b_{m,v}, v \in F\},\ m \in F,$$

$$b_{m,v} = \frac{1}{\sqrt{q}} \sum_{w \in F} \varepsilon^{tr(\frac{1}{2}m(w*w)+vw)} e_w.$$

Let $f(x) = \sum_{i \le j} a_{ij} x^{p^i + p^j}$ be a quadratic planar polynomial. Then, $S = (F, +, *)$ with $x * y = \frac{1}{2}(f(x+y) - f(x) - f(y)) = \frac{1}{2}\sum_{i \le j} a_{ij}(x^{p^i} y^{p^j} + x^{p^j} y^{p^i})$ is a commutative pre-semifield. We follow the method described in chapter 4 to find the product formula for corresponding symplectic semifield S^{td}:

$$x \circ y = \frac{1}{2} \sum_{i \le j} a_{ij}^{p^{r-i}} x^{p^{j-i}} y^{p^{r-i}} + \frac{1}{2} \sum_{i \le j} a_{ij}^{p^{r-j}} u^{p^{i-j}} y^{p^{r-j}}.$$

Then we have

$$
\begin{aligned}
tr(\frac{1}{2}w(w\circ m)) &= tr(\frac{1}{4}\sum_{i\leq j} wa_{ij}^{p^{r-i}} w^{p^{j-i}} m^{p^{r-i}} + \frac{1}{4}\sum_{i\leq j} wa_{ij}^{p^{r-j}} w^{p^{r+i-j}} m^{p^{r-j}}) \\
&= tr(\frac{1}{4}\sum_{i\leq j} w^{p^i} a_{ij} w^{p^j} m + \frac{1}{4}\sum_{i\leq j} w^{p^j} a_{ij} w^{p^i} m) \\
&= tr(\frac{1}{2}m(w * w)).
\end{aligned}
$$

Therefore, we get the construction of MUBs based on ***finite symplectic semifields of odd order***:

Theorem 7.2.3. *Let $(F,+,\circ)$ be a finite symplectic presemifield of odd characteristic. Then the following set forms a complete set of MUBs:*

$$B_\infty = \{e_w, w \in F\}, \quad B_m = \{b_{m,v}, v \in F\},\ m \in F,$$

$$b_{m,v} = \frac{1}{\sqrt{q}} \sum_{w\in F} \varepsilon^{tr(\frac{1}{2}w(w\circ m)+vw)} e_w.$$

Where $q = p^r$, and $\varepsilon \in \mathbb{C}$ is a primitive pth root of unity.

This construction can be generalized to any ***symplectic spreads*** [1].

Theorem 7.2.4. *Let F be a finite field of odd characteristic. Consider symplectic spread of F^2 whose elements are subspaces of the form $\{(x, h_m(x)) \mid x \in F\}$, where for every $m \in F$ the functions h_m is linear, and the subspace $\{(0, y \mid y \in F\}$. Then the following set forms a complete set of MUBs:*

$$B_\infty = \{e_w, w \in F\}, \quad B_m = \{b_{m,v}, v \in F\},\ m \in F,$$

$$b_{m,v} = \frac{1}{\sqrt{q}} \sum_{w\in F} \varepsilon^{tr(\frac{1}{2}w\cdot h_m(w)+vw)} e_w.$$

The previous constructions can be generalized for even characteristic cases, using commutative and symplectic semifields, symplectic spreads and pseudo-planar functions, see for details [1]. They use special technique called the Teichmüller lift.

Table 7.1: The Knuth orbit of a commutative semifields

Type		*Knuth orbit*
D	$(\mathbb{S},+,*)$	$(a,b)*(c,d)=(ac+jb^{\sigma}d^{\sigma},ad+bc)$
	$(\mathbb{S}^{t},+,\bullet)$	$(a,b)\bullet(c,d)=(ac+bd,a^{\sigma^{-1}}j^{\sigma^{-1}}d+bc)$
	$(\mathbb{S}^{td},+,\circ)$	$(a,b)\circ(c,d)=(ac+bd,c^{\sigma^{-1}}j^{\sigma^{-1}}b+ad)$
PW	$(\mathbb{S},+,*)$	$(a,b)*(c,d)=(ac+(bd)^{9},ad+bc+(bd)^{27})$
	$(\mathbb{S}^{t},+,\bullet)$	$(a,b)\bullet(c,d)=(ac+bd,bc+b^{9}d+a^{27}d)$
	$(\mathbb{S}^{td},+,\circ)$	$(a,b)\circ(c,d)=(ac+bd,ad+bd^{9}+bc^{27})$
G	$(\mathbb{S},+,*)$	$(a,b)*(c,d)=(ac-b^{9}d-bd^{9},ad+bc+b^{3}d^{3})$
	$(\mathbb{S}^{t},+,\bullet)$	$(a,b)\bullet(c,d)=(ac+bd,bc+b^{\frac{1}{3}}d-ad^{9}-a^{\frac{1}{9}}d^{\frac{1}{9}})$
	$(\mathbb{S}^{td},+,\circ)$	$(a,b)\circ(c,d)=(ac+bd,ad+bd^{\frac{1}{3}}-b^{9}c-b^{\frac{1}{9}}c^{\frac{1}{9}})$
CG	$(\mathbb{S},+,*)$	$(a,b)*(c,d)=(ac+jbd+j^{3}(bd)^{9},ad+bc+j(bd)^{3})$
	$(\mathbb{S}^{t},+,\bullet)$	$(a,b)\bullet(c,d)=(ac+bd,ajd+a^{\frac{1}{9}}j^{\frac{1}{3}}d+bc+b^{\frac{1}{3}}j^{\frac{1}{3}}d)$
	$(\mathbb{S}^{td},+,\circ)$	$(a,b)\circ(c,d)=(ac+bd,cjb+c^{\frac{1}{9}}j^{\frac{1}{3}}b+ad+d^{\frac{1}{3}}j^{\frac{1}{3}}b)$
CHK	$(\mathbb{S},+,*)$	$x*y=xy+L(xy^{9}+x^{9}y-xy-x^{9}y^{9})+x^{243}y^{3}+x^{81}y-x^{9}y+x^{3}y^{243}+xy^{81}-xy^{9}$
	$(\mathbb{S}^{t},+,\bullet)$	$x\bullet y=xy+x^{3^{3}}y^{3^{2}}+x^{3}y^{3^{6}}-x^{3^{3}}y-x^{3}y+x^{3^{6}}y^{3^{2}}+x^{3^{4}}y^{3^{6}}-x^{3^{6}}y-x^{3^{4}}y+x^{3^{3}}y^{3^{4}}$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y=xy+y^{3^{3}}x^{3^{2}}+y^{3}x^{3^{6}}-y^{3^{3}}x-y^{3}x+y^{3^{6}}x^{3^{2}}+y^{3^{4}}x^{3^{6}}-y^{3^{6}}x-y^{3^{4}}x+y^{3^{3}}x^{3^{4}}+y^{3^{4}}x^{3^{4}}-y^{3^{6}}x^{3^{6}}+y^{3^{7}}x^{3^{4}}+yx^{3^{4}}-yx^{3^{2}}$
GT	$(\mathbb{S},+,*)$	$x*y=x^{\alpha}y+xy^{\alpha}$
	$(\mathbb{S}^{t},+,\bullet)$	$x\bullet y=x^{q^{t-n}}y^{q^{t-n}}+xy^{q^{n}}$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y=x^{q^{t-n}}y^{q^{t-n}}+x^{q^{n}}y$

Table 7.2**:** The Knuth orbit of a commutative semifields, cont.

Type		*Knuth orbit*
CM	$(\mathbb{S},+,*)$	$x*y=x^9y+xy^9-2x^3y^3-2xy$
	$(\mathbb{S}^t,+,\bullet)$	$x\bullet y=x^{3^{-2}}y^{3^{-2}}+xy^9+x^{3^{-1}}y+xy$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y=x^{3^{-2}}y^{3^{-2}}+x^9y+xy^{3^{-1}}+xy$
BH	$(\mathbb{S},+,*)$	$x*y=xy^{p^m}+x^{p^m}y+[\beta(xy^{p^s}+x^{p^s}y)+\beta^{p^m}(xy^{p^s}+x^{p^s}y)^{p^m}]\omega$
	$(\mathbb{S}^t,+,\bullet)$	$x\bullet y = xy^{p^m}+x^{p^m}y^{p^m}+\beta\omega xy^{p^s}+\beta^{p^{-s}}\omega^{p^{-s}}x^{p^{-s}}y^{p^{-s}}+\beta\omega^{p^m}x^{p^m}y^{p^s}+\beta^{p^{-s}}\omega^{p^{m-s}}x^{p^{m-s}}y^{p^{-s}}$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y = x^{p^m}y+x^{p^m}y^{p^m}+\beta\omega x^{p^s}y+\beta^{p^{-s}}\omega^{p^{-s}}x^{p^{-s}}y^{p^{-s}}+\beta\omega^{p^m}x^{p^s}y^{p^m}+\beta^{p^{-s}}\omega^{p^{m-s}}x^{p^{-s}}y^{p^{m-s}}$
ZKW	$(\mathbb{S},+,*)$	$x*y=y^{p^t}x+yx^{p^t}-u^{p^s-1}(y^{p^{s+t}}x^{p^{2s}}+y^{p^{2s}}x^{p^{s+t}})$ where u is a primitive element of $\mathbb{F}_{3^s}$
	$(\mathbb{S}^t,+,\bullet)$	$x\bullet y = y^{p^t}x+y^{p^{3s-t}}x^{p^{3s-t}}-u^{p^s(p^s-1)}y^{p^{2s+t}}x^{p^s}-u^{p^{2s-t}(p^s-1)}y^{p^{s-t}}x^{p^{2s-t}}$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y = yx^{p^t}+y^{p^{3s-t}}x^{p^{3s-t}}-u^{p^s(p^s-1)}y^{p^s}x^{p^{2s+t}}-u^{p^{2s-t}(p^s-1)}y^{p^{2s-t}}x^{p^{s-t}}$
B	$(\mathbb{S},+,*)$	$x*y=y^{p^t}x+yx^{p^t}-u^{p^s-1}(y^{p^{s+t}}x^{p^{3s}}+y^{p^{3s}}x^{p^{s+t}})$ where u is a primitive element of $\mathbb{F}_{4^s}$
	$(\mathbb{S}^t,+,\bullet)$	$x\bullet y = y^{p^t}x+y^{p^{4s-t}}x^{p^{4s-t}}-u^{p^s(p^s-1)}y^{p^{2s+t}}x^{p^s}-u^{p^{3s-t}(p^s-1)}y^{p^{2s-t}}x^{p^{3s-t}}$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y = yx^{p^t}+y^{p^{4s-t}}x^{p^{4s-t}}-u^{p^s(p^s-1)}y^{p^s}x^{p^{2s+t}}-u^{p^{3s-t}(p^s-1)}y^{p^{3s-t}}x^{p^{2s-t}}$
K	$(\mathbb{S},+,*)$	$x*y=xy+(T(x)y+T(y)x)^2\ F=GF(q^n)$, with q even and $n>1$ odd , $T:F\to GF(q)$
	$(\mathbb{S}^t,+,\bullet)$	$x\bullet y=xy+\sum_{i=0}^{n-1}(\sqrt{x}y)^{q^{-i}}+\sqrt{x}\sum_{i=0}^{n-1}y^{q^i}$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y=y\bullet x=xy+\sum_{i=0}^{n-1}(\sqrt{y}x)^{q^{-i}}+\sqrt{y}\sum_{i=0}^{n-1}x^{q^i}$
KW	$(\mathbb{S},+,*)$	$x*y=xy+(x\sum_1^n T_i(\zeta_iy)+y\sum_1^n T_i(\zeta_ix))^2$
	$(\mathbb{S}^t,+,\bullet)$	$x\bullet y=xy+x^{\frac{1}{2}}\sum_1^n T_i(\zeta_iy)+\sum_1^n\zeta_iT_i(x^{\frac{1}{2}}y)$
	$(\mathbb{S}^{td},+,\circ)$	$x\circ y=y\bullet x=xy+y^{\frac{1}{2}}\sum_1^n T_i(\zeta_ix)+\sum_1^n\zeta_iT_i(y^{\frac{1}{2}}x)$

Table 7.3**:** The Knuth orbit of Hughes-Kleinfeld semifields

Type	*Knuth orbit*
$\mathbb{S}$	$(x,y)*(z,t)=(xz+aty^{\theta},yz+x^{\theta}t+y^{\theta}bt)$
$\mathbb{S}^{t}$	$(x,y)\bullet(z,t)=(xz+y^{\theta^{-1}}t^{\theta^{-1}},yz+x^{\theta^{-1}}a^{\theta^{-1}}t^{\theta^{-1}}+y^{\theta^{-1}}b^{\theta^{-1}}t^{\theta^{-1}})$
$\mathbb{S}^{td}$	$(x,y)\circ(z,t)=(xz+t^{\theta^{-1}}y^{\theta^{-1}},xt+z^{\theta^{-1}}a^{\theta^{-1}}y^{\theta^{-1}}+t^{\theta^{-1}}b^{\theta^{-1}}y^{\theta^{-1}})$
$\mathbb{S}^{tdt}$	$(x,y)\times(z,t)=(xz+yt,tx^{\theta}+zay^{\theta}+tby^{\theta})$
$\mathbb{S}^{d}$	$(x,y)\diamond(z,t)=(z,t)*(x,y)=(xz+ayt^{\theta},xt+z^{\theta}y+t^{\theta}by)$
$\mathbb{S}^{dt}$	$(x,y)\star(z,t)=(xz+yt,xat^{\theta}+yz^{\theta}+yt^{\theta}b)$

Table 7.4**:** Planar functions of commutative semifields

Type	*Planar Function*
GTF	$f(x) = x^{q^n} \cdot x + x \cdot x^{q^n} = 2x^{q^n+1}$
CMP	$f(x) = -x^{10} - x^6 + x^2$
CHP	$f(x) = x^2 + (x^{243} + x^9)(2x^{10} - x^2 - x^{18}) + 2x^{246} + 2x^{82} - 2x^{10}$
ZWP	$f(x) = 2x^{p^t+1} - u^{p^s-1}(2x^{p^{2s}+p^{s+t}})$
BP	$f(x) = 2x^{p^t+1} - u^{p^s-1}(2x^{p^{3s}+p^{s+t}})$
CG	$f(X) = X^2 + \alpha^{-6}(X^{18} + X^{2\cdot 3^{n+2}} + X^{9+3^{n+2}}) + \lambda\alpha^{-2}(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}})$
PW	$f(X) = X^2 + \alpha^{-9}(X^{18} + X^{2.3^7} + X^{9+3^7}) + \lambda\alpha^{-27}(X^{54} + X^{2.3^8} + X^{27+3^8}) - (X^2 + X^{2.3^5} + X^{1+3^5})$
G	$f(X) = X^2 + \alpha^{-6}(X^{18} + X^{2\cdot 3^{n+2}} + X^{9+3^{n+2}}) + \lambda\alpha^{-2}(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}})$
D	$f(X) = X^2 + 4^{-1}\alpha^{1-p^r}(X^{2p^r} + X^{2p(n+r)} - 2X^{p^r+p^{(n+r)}}) - 4^{-1}(X^2 + X^{2p^n} - 2X^{1+p^n})$

Table 7.5**:** The nuclei of commutative semifields

Type	*The nucleus of* $\mathbb{S}$	*The middle nucleus of* $\mathbb{S}$
D	$N_r(\mathbb{S}) = N_\ell(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_q\}$	$N_m(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_{q^k}\}$
PW	$N_r(\mathbb{S}) = N_\ell(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_3\}$	$N_m(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_{3^5}\}$
G	$N_r(\mathbb{S}) = N_\ell(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_3\}$	$N_m(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_3\}$
CG	$N_r(\mathbb{S}) = N_\ell(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_3\}$	$N_m(\mathbb{S}) = \{(x,0) : x \in \mathbb{F}_{3^s}\}$

Bibliography

[1] K. Abdukhalikov, Symplectic spreads, planar functions and mutually unbiased bases, *Journal of Algebraic Combinatorics* 41 (2015), 1055–1077.

[2] K. Abdukhalikov, E. Bannai and S. Suda, Association schemes related to universally optimal configurations, Kerdock codes and extremal Euclidean line-sets, *Journal of Combinatorial Theory* Ser. A 116 (2009), 434–448.

[3] A. A. Albert, Generalized twisted fields, *Pacific Journal of Mathematics* 11 (1961), 1–8.

[4] J. Bierbrauer, New semifields, PN and APN functions, *Designs, Codes and Cryptography* 54(3) (2010), 189–200.

[5] L. Budaghyan and T. Helleseth, New perfect nonlinear multinomials over $F_{p^{2k}}$ for any odd prime p. In: SETA âĂŹ08: Proceedings of the 5th International Conference on Sequences and their Applications, 403–414. Springer, Berlin, Heidelberg (2008).

[6] S. D. Cohen, M. J. Ganley, Commutative semifields, two-dimensional over their middle nuclei, *Journal of Algebra* 75 (1982), 373–385.

[7] R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II. Commutative presemifields and semifields, *Designs, Codes and Cryptography* 10 (1997), 167–184.

[8] R. S. Coulter and M. Henderson, Commutative presemifields and semifields, *Advances in Mathematics* 217 (2008), 282–304.

[9] R. S. Coulter and P. Kosick, Commutative semifields of order 243 and 3125, in: Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 129–136 (2010).

[10] P. Dembowski, Finite geometries, Springer, Berlin (1968).

[11] L. E. Dickson, On commutative linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society* 7 (1906), 514–522.

[12] C. Ding and J. Yuan, A family of skew Hadamard difference sets. *Journal of Combinatorial Theory Ser. A* 113 (2006), 1526–1535.

[13] M. J. Ganley, Central weak nucleus semifields, *European Journal of Combinatorics* 2 (1981), 339–347.

[14] N. L. Johnson, V. Jha and M. Biliotti, Handbook of finite translation planes. Pure and Applied Mathematics (Boca Raton), 289. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[15] D. R. Hughes and E. Kleinfeld, Seminuclear extensions of Galois fields, *American Journal of Mathematics* 82 (1960), 389–392.

[16] W. M. Kantor, Commutative semifields and symplectic spreads, *Journal of Algebra* 270 (2003), 96–114.

[17] W. M. Kantor and M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes, *Transactions of the American Mathematical Society* 356 (2004), 895–938.

[18] W. M. Kantor, Finite semifields. Finite geometries, groups, and computation, 103–114, Walter de Gruyter, Berlin, 2006.

[19] D. E. Knuth, Finite semifields and projective planes, *Journal of Algebra* 2 (1965), 182–217.

[20] D. E. Knuth, A class of projective planes, *Transactions of the American Mathematical Society* 115 (1965), 541–549.

[21] M. Lavrauw and O. Polverino, Finite semifields and Galois geometry, Current Research Topics in Galois Geometry, 129–157, Nova Science Publishers, 2011.

[22] G. Marino and O. Polverino, On the nuclei of a finite semifield. Theory and applications of finite fields, 123–141, Contemp. Math., 579, Amer. Math. Soc., 2012.

[23] K. Minami and N. Nakagawa, On planar functions of elementary abelian p-group type, *Hokkaido Mathematical Journal* 37 (2008), 531–544 .

[24] G. L. Mullen and C Mummert, Finite Fields and Applications, 2007.

[25] T. Penttila and B. Williams, Ovoids of parabolic spaces. *Geometriae Dedicata* 82 (2000), 1–19.

[26] Z.-X. Wan, Lectures on finite fields and Galois rings, World Scientific, Singapore, 2003.

[27] Z. Zha, G. M. Kyureghyan and X. Wang, Perfect nonlinear binomials and their semifields, *Finite Fields and Their Applications* 15 (2009), 125–133.

[28] Z. Zha and X. Wang, New families of perfect nonlinear polynomial functions, *Journal of Algebra* 322 (2009), 3912–3918.

[29] Y. Zhou, $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations, *Journal of Combininatorial Designs* 21 (12) (2013), 563–584.