On Rank Problems for Subspaces of Matrices over Finite Fields

by

John Sheekey

A dissertation presented to

University College Dublin in partial

fulfillment of the requirements for the degree of

Doctor of Philosophy

in the College of Engineering, Mathematical

and Physical Sciences

August 2011

School of Mathematical Sciences

Head of School: Dr. Mícheál Ó Searcóid

Supervisor of Research: Professor Roderick Gow

Contents

Acknowledgements

This thesis would not have been possible without the help and support of all my family, friends, colleagues and teachers.

Thank you to my parents, Peter and Theresa, for their unwavering and unconditional support. To everyone at UCD, I could not have wished for a better place to spend four years of my life.

To all my teachers, mentors and co-authors, for their willingness to share their wisdom, and for inspiring me to pursue a career in mathematics. In particular to my supervisor, Rod Gow, for his unfailing enthusiasm and patience, and his generosity with his time and knowledge.

Abstract

In this thesis we are concerned with themes suggested by rank properties of subspaces of matrices. Historically, most work on these topics has been devoted to matrices over such fields as the real or complex numbers, where geometric or analytic methods may be applied. Such techniques are not obviously applicable to finite fields, and there were very few general theorems relating to rank problems over finite fields.

In this thesis we are concerned mainly with constant rank subspaces of matrices over finite fields, with particular focus on two subcases: (1) constant rank subspaces of symmetric or hermitian matrices; and (2) constant full rank subspaces of matrices, which correspond to nonassociative algebraic structures known as semifields.

In Chapter 1 we will introduce constant rank subspaces of matrices, and review the known results on the maximum dimension of such a subspace. In Chapter 2 we will recall the definition of a semifield, and illustrate how these algebraic structures are related to constant rank subspaces of matrices.

In Chapter 3 we will prove a general theorem on subspaces of function spaces, and apply the results to obtain new upper bounds on subspaces of matrices, which are sharp in some cases.

In Chapter 4 we will study primitive elements in finite semifields, and prove their existence for a certain family of semifields. In Chapters 5 and 6 we will introduce a construction for semifields using skew-polynomial rings. We will show how they are related to other known constructions, use this representation to obtain new results, and provide elegant new proofs for some known results.

Chapter 1

Introduction to constant rank subspaces

In this chapter we will define constant rank subspaces, establish some notation, survey the known results and applications, and introduce some concepts and results which will be needed in subsequent chapters.

1.1 Constant rank subspaces

1.1.1 Definitions and Notations

Let $\mathbb{F}$ denote an arbitrary field, $M_{m\times n}(\mathbb{F})$ denote the space of $m \times n$ matrices over $\mathbb{F}$, and $M_n(\mathbb{F}) := M_{n\times n}(\mathbb{F})$, where m and n are positive integers. We will assume unless otherwise stated that $m \leq n$. For any non-zero subspace U of $M_{m\times n}(\mathbb{F})$ let $U^{\times}$ denote the subset of non-zero elements in U.

Let V denote a vector space n-dimensional over $\mathbb{F}$. Let $\mathbb{K}$ denote an extension field of $\mathbb{F}$ of degree 2 (assuming such an extension exists), and let W denote a vector space n-dimensional over $\mathbb{K}$.

We denote the space of $n \times n$ *symmetric* matrices over $\mathbb{F}$ by $S_n(\mathbb{F})$. If $\mathbb{F}$ has a degree

2 extension $\mathbb{K}$ admitting an $\mathbb{F}$-automorphism of order 2, we denote the space of $n \times n$ *hermitian* matrices over $\mathbb{K}$ by $H_n(\mathbb{F})$. Note that $H_n(\mathbb{F})$ is not a vector space over $\mathbb{K}$, but is a vector space over $\mathbb{F}$ of dimension n^2. Note that the notation is potentially ambiguous, since such an extension field $\mathbb{K}$ need not be unique. However, in this work we will only be considering hermitian matrices over finite fields, which of course possess a unique degree 2 extension.

Let p be a prime, q a power of p. Let $\mathbb{F}_q$ denote the finite field of q elements.

Definition 1.1. *Let U be a non-zero subspace of $M_{m\times n}(\mathbb{F})$. We say that U is a* constant rank r *subspace if every element of $U^\times$ has rank r.*

Much research has been done to investigate the maximum possible dimension of a constant rank r subspace. The results and techniques differ greatly according to properties of the underlying field.

We will focus on constant rank subspaces of $M_{m\times n}(\mathbb{F})$, $S_n(\mathbb{F})$ and $H_n(\mathbb{F})$, with particular attention to finite fields and constant rank n subspaces.

1.1.2 Existing bounds for the maximum dimension of constant rank subspaces

For any $r \leq m$, there exists an $(n-r+1)$-dimensional constant rank r space for *any* field: Let U be the subspace of $M_{m\times n}(\mathbb{F})$ consisting of elements of the form

$$\left(\begin{array}{cccccccc}
a_1 & a_2 & \dots & \dots & a_{n-r+1} & 0 & \dots & 0 \\
0 & a_1 & \dots & \dots & a_{n-r} & a_{n-r+1} & \dots & 0 \\
\vdots & \vdots & \ddots & & \ddots & & \ddots & \vdots \\
0 & 0 & \dots & a_1 & \dots & \dots & \dots\dots & a_{n-r+1} \\
\hline
0 & 0 & \dots & \dots & \dots & \dots & \dots & 0 \\
\vdots & \vdots & & & & & & \vdots \\
0 & 0 & \dots & \dots & \dots & \dots & \dots & 0
\end{array}\right)$$

for all $a_1, a_2, \dots, a_{n-r+1} \in \mathbb{F}$. Then U is clearly such a subspace.

Westwick [74] showed that over the complex numbers, the maximum dimension of a constant rank r subspace of $M_{m\times n}(\mathbb{C})$ is $m+n-2r+1$. Hence if $r = m$, the above construction is optimal. Ilic and Landsberg [34] showed that the maximum dimension of a constant rank r subspace of $S_n(\mathbb{C})$ is $n-r+1$ if r is *even*, using techniques of complex algebraic geometry. The maximum dimension of a constant rank r subspace of $S_n(\mathbb{C})$ or $S_n(\mathbb{R})$ is 1 if r is *odd*. We will discuss the case where r is odd further in Section 3.3.2. Much study has been dedicated to the problem of constant rank subspaces over $\mathbb{R}$ and $\mathbb{C}$, for example in [5], [12], [48], [57], [74], [75]. Large constant rank spaces can be constructed using division algebras defined over $\mathbb{F}$ (see Corollary 2.8).

Lemma 1.2. Suppose there exist an n-dimensional constant rank n subspace U of $M_n(\mathbb{F})$. Then for any $1 \leq r \leq m \leq n$ there exists an n-dimensional constant rank r subspace U' of $M_{m\times n}(\mathbb{F})$.

Proof. Let A be an arbitrary rank r element of $M_{m\times n}(\mathbb{F})$. Let

$$U' = \{AX : X \in U\}.$$

It is clear that every non-zero element of U' has rank r. It remains to show that $\dim(U') = n$. Suppose $AX = AY$ for some $X, Y \in U$, $X \neq Y$. Then $A(X-Y) = 0$. But $0 \neq X - Y \in U$, and so $X - Y$ is invertible. But then we must have $A = 0$, a contradiction. Hence the map from U to U' defined by $X \mapsto AX$ is injective and surjective, implying $\dim(U') = \dim(U) = n$ and hence proving the result. □

A *presemifield* is a division algebra where multiplication is not assumed to be associative, and a multiplicative identity is not assumed to exist. These structures will be defined and discussed in Chapter 2, and the following theorem is well known and will be proved.

Theorem 1.3. *There exist an n-dimensional constant rank n subspace of $M_n(\mathbb{F})$ if and only if there exists a presemifield n-dimensional over $\mathbb{F}$.*

Note that a field is certainly a presemifield. As every finite field admits an extension field of degree n for all n, we have the following theorem:

Theorem 1.4. *For every $1 \leq r \leq m \leq n$ there exists an n-dimensional constant rank r subspace of $M_{m\times n}(\mathbb{F}_q)$ for all q.*

Beasley and Laffey showed in [5] that this dimension bound is optimal when the conditions $|\mathbb{F}| \geq r+1$ and $n \geq 2r-1$ are imposed. We will see a similar restriction on field size later in Section 3.3. This restriction is imposed to ensure the existence of a non-root of a polynomial of degree r.

Theorem 1.5. *Suppose $|\mathbb{F}| \geq r+1$ and $n \geq 2r-1$. Suppose U is a constant rank r subspace of $M_{m\times n}(\mathbb{F})$. Then* $\dim(U) \leq n$.

In [26] the following upper bound was proved for finite fields:

Theorem 1.6. *Let U be a constant rank r subspace of $M_{m\times n}(\mathbb{F}_q)$. Then* $\dim(U) \leq m+n-r$.

This bound was proved via character theory, using character values calculated by Delsarte in [16]. In Section 3.2.1 we will provide an new proof of this theorem.

The above bounds do not rule out the possibility of constant rank r subspaces of $n \times n$ matrices of dimension larger than n if r is large, or the field size is small. Indeed there exist subspaces which meet the bound of Theorem 1.6 over the field of two elements, as shown in [6], [7], [26].

Theorem 1.7. *There exist d-dimensional constant rank r subspaces of $M_{m\times n}(\mathbb{F}_2)$ for $(m,n,r,d) \in \{(3,3,2,4),(4,4,3,5),(5,5,4,6),(4,5,3,6)\}$.*

The subspace of 3×3 matrices over $\mathbb{F}_2$ with basis

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \right\}$$

is an example of a 4-dimensional constant rank 2 subspace. Note that J-G. Dumas showed by computer calculations that all such subspaces are equivalent to the example above in the sense of Section 1.1.3 below, contrary to Beasley's assertion in [6].

Boston [7] conjectured that constant rank subspaces of $n \times n$ matrices of dimension greater than n exist only for $n \leq 8$. However, this problem remains open.

1.1.3 Equivalence

We consider some linear maps on $M_{m\times n}(\mathbb{F})$ which preserve rank. Let X and Y be invertible elements of $M_m(\mathbb{F})$ and $M_n(\mathbb{F})$ respectively. Then the maps

$$A \mapsto XA$$
$$A \mapsto AY$$

clearly preserve rank.

Let σ be an automorphism of $\mathbb{F}$. For $A \in M_{m\times n}(\mathbb{F})$, define A^σ to be the matrix obtained by applying σ to every entry of A. Then the map $A \mapsto A^\sigma$ is also a linear map which preserves rank.

Clearly these above maps generate a group E of linear maps which preserve rank, consisting of elements of the form $\phi_{X,Y,\sigma} : A \mapsto XA^\sigma Y$.

We can extend these maps to subspaces of matrices. Let $\phi \in E$, and U a subspace of $M_{m\times n}(\mathbb{F})$. Then define

$$U \mapsto U^\phi := \{A^\phi : A \in U\}.$$

Clearly U is a constant rank r subspace if and only if U^ϕ is a constant rank r subspace.

We say that two subspaces U and U' are *equivalent* if there exists an element $\phi \in E$ such that $U' = U^\phi$.

Note that if $m = n$, then the map sending each matrix to its transpose, $A \mapsto A^T$, is another linear map which preserves rank. However, we will exclude these maps from the definition of equivalence of subspaces.

1.2 Symmetric bilinear forms and quadratic forms

In this section we will recall the connections between symmetric matrices, bilinear forms, and quadratic forms, which we will exploit later in this work.

1.2.1 Bilinear forms

Definition 1.8. *Let V be a vector space n-dimensional over a field $\mathbb{F}$. A* bilinear form *is a map $\mathcal{B} : V \times V \to \mathbb{F}$ such that*

$$\begin{aligned}\mathcal{B}(u+v,w) &= \mathcal{B}(u,w)+\mathcal{B}(v,w)\\ \mathcal{B}(u,v+w) &= \mathcal{B}(u,v)+\mathcal{B}(u,w)\\ \mathcal{B}(\lambda u,v) &= \mathcal{B}(u,\lambda v) = \lambda\mathcal{B}(u,v)\end{aligned}$$

for all $u, v, w \in V$, and all $\lambda \in \mathbb{F}$.

Denote the set of all bilinear form on $V \times V$ by $\mathcal{B}_n(\mathbb{F})$. It is well known that bilinear forms are related to matrices in the following way: let $\{e_1, e_2, \dots, e_n\}$ be an $\mathbb{F}$-basis for V. Let u and v be elements of V, and suppose $u = \sum_i u_i e_i$, $v = \sum_i v_i e_i$ for $u_i, v_i \in \mathbb{F}$. Then by the above defining properties of bilinear forms, we have that

$$\mathcal{B}(u,v) = \sum_{i,j=1}^{n} u_i v_j \mathcal{B}(e_i, e_j).$$

Hence the action of $\mathcal{B}$ is completely determined by its action on all pairs of basis elements. Define $b_{ij} := B(e_i, e_j)$ for each i, j. Then the above can be written as

$$\mathcal{B}(u,v) = \sum_{i,j=1}^{n} u_i v_j b_{ij}. \tag{1.1}$$

Consider now the matrix $B := (b_{ij})_{i,j} \in M_n(\mathbb{F})$. Identify each element $u = \sum_i u_i e_i \in V$ with the column vector

$$\mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}.$$

Then it is clear from the definition of matrix multiplication and equation 1.1 that

$$\mathcal{B}(u,v) = \mathbf{u}^T B \mathbf{v}. \tag{1.2}$$

Note that the entries of the matrix B depends on the choice of basis. Hence we refer to B as the matrix representing $\mathcal{B}$ *with respect to the basis* $\{e_1, e_2, \dots, e_n\}$. Suppose $\{e'_1, e'_2, \dots, e'_n\}$ is another $\mathbb{F}$-basis for V, and let B' be the matrix representing $\mathcal{B}$

with respect to this basis. Then if we let X denote the change of basis matrix, it is clear that

$$B' = X^T B X.$$

Conversely, clearly every $n \times n$ matrix over $\mathbb{F}$ defines a bilinear form in the manner of equation 1.2. Hence the $\mathcal{B}_n(\mathbb{F})$ can be identified with $M_n(\mathbb{F})$ through the choice of a basis for V. Similarly, if V' is a vector space m-dimensional vector space over $\mathbb{F}$, we can define $\mathcal{B}_{m\times n}(\mathbb{F})$ to be the set of bilinear forms on $V' \times V$, and identify $\mathcal{B}_{m\times n}(\mathbb{F}) \simeq M_{m\times n}(\mathbb{F})$, where '$\simeq$' denotes $\mathbb{F}$-isomorphism of vector spaces.

1.2.2 Symmetric matrices and quadratic forms

A bilinear form $\mathcal{B}$ is said to be *symmetric* if $\mathcal{B}(u, v) = \mathcal{B}(v, u)$ for all $u, v \in V$. Denote the set of symmetric bilinear forms by $\mathcal{S}_n(\mathbb{F})$. It is clear from the definitions that if B represents $\mathcal{B}$ with respect to some basis, then $\mathcal{B}$ is a symmetric bilinear form if and only if $B = B^T$, i.e. B is a symmetric matrix. Conversely, every symmetric matrix defines a symmetric bilinear form. Hence we can see that

$$\mathcal{S}_n(\mathbb{F}) \simeq S_n(\mathbb{F}).$$

Definition 1.9. *A* quadratic form *is a function $Q : V \to \mathbb{F}$ such that*

$$Q(\lambda u + \mu v) = \lambda^2 Q(u) + \mu^2 Q(v) + \lambda\mu \mathcal{B}_Q(u, v), \tag{1.3}$$

where $\mathcal{B}_Q$ is a bilinear form on $V \times V$.

We call $\mathcal{B}_Q$ the *associated bilinear form* (or *polarization*) of Q. The set of quadratic forms on V forms an $\mathbb{F}$-vector space. We denote this space by $\mathcal{Q}_n(\mathbb{F})$.

Rearranging (1.3) gives us

$$\mathcal{B}_Q(u, v) = Q(u + v) - Q(u) - Q(v).$$

It is clear that this bilinear form is in fact symmetric. Furthermore, if the characteristic of $\mathbb{F}$ is not two, we see that

$$Q(u) = \frac{\mathcal{B}_Q(u, u)}{2},$$

since $4Q(u) = Q(2u) = Q(u+u) = Q(u) + Q(u) + \mathcal{B}_Q(u,u)$. Conversely, when the characteristic of $\mathbb{F}$ is not two, then given a symmetric bilinear form $\mathcal{B}$ we can define a quadratic form $Q_{\mathcal{B}}$ by

$$Q_{\mathcal{B}}(u) := \frac{\mathcal{B}(u,u)}{2}.$$

Hence when $\text{char}(\mathbb{F}) \neq 2$ we have a bijection between the space of quadratic forms and the space of symmetric bilinear forms. It is easily checked that this is in fact a vector space isomorphism, and so

$$\mathcal{Q}_n(\mathbb{F}) \simeq \mathcal{S}_n(\mathbb{F}) \simeq S_n(\mathbb{F}).$$

Remark 1.10. Let $x = (x_1, x_2, \ldots, x_n)$ be a vector of indeterminates. Given a quadratic form Q we can define a polynomial $Q(x) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$. Then $Q(x)$ can be shown to be homogeneous of degree 2. This is sometimes given as the definition of a quadratic form.

1.2.3 Hermitian matrices and hermitian forms

Let $\mathbb{F}$ be a field, and let $\mathbb{K}$ be an field extension of $\mathbb{F}$ of degree 2. There exists an $\mathbb{F}$-automorphism of $\mathbb{K}$ of order 2, i.e. an involution, which we will denote by bar, $a \mapsto \bar{a}$. We can extend the automorphism to an $\mathbb{F}$-linear transformation on a vector space or matrix ring over $\mathbb{K}$: for an element X of a vector or matrix space, denote by $\overline{X}$ the element obtained by applying the bar automorphism to all coefficients or entries of X.

Definition 1.11. *Let W be a vector space n-dimensional over $\mathbb{K}$. A* hermitian form *is a map $\mathcal{H} : W \times W \to \mathbb{F}$ such that*

$$\begin{aligned}
\mathcal{H}(u+v, w) &= \mathcal{H}(u,w) + \mathcal{H}(v,w) \\
\mathcal{H}(u, v+w) &= \mathcal{H}(u,v) + \mathcal{H}(u,w) \\
\mathcal{H}(\lambda u, v) &= \lambda \mathcal{H}(u,v) \\
\mathcal{H}(u,v) &= \overline{\mathcal{H}(v,u)}
\end{aligned}$$

for all $u, v, w \in W$, and all $\lambda \in \mathbb{K}$.

As in the case of bilinear forms, we can define a matrix H representing $\mathcal{H}$ with respect to some $\mathbb{K}$-basis $\{e_i''\}$ of W, by setting $H = (h_{ij})$, where $h_{ij} := \mathcal{H}(e_i'', e_j'')$. Then

$$\mathcal{H}(u, v) = \mathbf{u}H\overline{\mathbf{v}}.$$

The properties in definition 1.11 imply that H is a *hermitian matrix*, i.e.

$$\overline{H}^T = H.$$

We will denote the set of hermitian forms by $\mathcal{H}_n(\mathbb{F})$. Clearly every hermitian matrix defines a hermitian form, and so we have

$$\mathcal{H}_n(\mathbb{F}) \simeq H_n(\mathbb{F}),$$

where $H_n(\mathbb{F})$ is the space of hermitian matrices with entries in $\mathbb{K}$, and $\simeq$ here denotes isomorphism as $\mathbb{F}$-vector spaces. Note that $H_n(\mathbb{F})$ is an $\mathbb{F}$-vector space, but *not* a $\mathbb{K}$-vector space: if H is a hermitian matrix, and $\lambda \in \mathbb{K}$, then λH is hermitian if and only if $\overline{\lambda} = \lambda$, i.e. if and only if $\lambda \in \mathbb{F}$. The dimension of $H_n(\mathbb{F})$ over $\mathbb{F}$ is n^2.

Definition 1.12. *A* quadratic hermitian form *is a map $h : W \to \mathbb{F}$ such that*

$$h(u) = \mathcal{H}(u, u)$$

for some hermitian form $\mathcal{H}$.

We can see that $h(u)$ does indeed lie in $\mathbb{F}$ for all u, as $\overline{h(u)} = \overline{\mathcal{H}(u, u)} = \mathcal{H}(u, u) = h(u)$. Hence h is a map from W to $\mathbb{F}$.

Let $\mathcal{Q}H_n(\mathbb{F})$ denote the space of quadratic hermitian forms defined on W. Then by definition and by the above we have

$$\mathcal{Q}H_n(\mathbb{F}) \simeq \mathcal{H}_n(\mathbb{F}) \simeq H_n(\mathbb{F}).$$

Note that the concepts of hermitian forms, hermitian matrices and quadratic hermitian forms are analogous to symmetric bilinear forms, symmetric matrices and quadratic forms respectively. We say a hermitian matrix represents a quadratic hermitian form in the analogous way.

1.2.4 Isotropic vectors

In the following, by "quadratic (hermitian) form" we will mean "quadratic form (resp. quadratic hermitian form)".

Definition 1.13. *Let f be a quadratic (hermitian) form. A vector u is said to be* isotropic *with respect to f if*

$$f(u) = 0.$$

Definition 1.14. *Let f be a quadratic (hermitian) form over a finite field $\mathbb{F}$. Let a be an element of $\mathbb{F}$, and define*

$$N_f(a) := |\{u \in V \mid f(u) = a\}|.$$

The main theorems of Chapter 3 rely on the fact that the number of isotropic vectors with respect to a quadratic (hermitian) form over a finite field is well known and easy to calculate. From the above definition, the number of isotropic vectors is denoted by $N_f(0)$. To illustrate this, we need to introduce the concepts of the *radical* and *rank* of a form.

Let $\mathcal{B}$ be a bilinear form defined on V. Define the *right radical* of $\mathcal{B}$ by

$$\text{rad}_r(\mathcal{B}) := \{v \ : \ \mathcal{B}(u, v) = 0 \text{ for all } u \in V\}.$$

The *left radical* $\text{rad}_l(\mathcal{B})$ is defined similarly. These two subspaces have the same dimension. If $\mathcal{B}$ is symmetric, then clearly $\text{rad}_r(\mathcal{B}) = \text{rad}_l(\mathcal{B}) =: \text{rad}(\mathcal{B})$.

We say that a bilinear form is *non-degenerate* if $\text{rad}_r(\mathcal{B}) = 0$, and *degenerate* otherwise. We define the *rank* of a bilinear form by

$$\text{rank}(\mathcal{B}) := n - \dim(\text{rad}_r(\mathcal{B})) = n - \dim(\text{rad}_l(\mathcal{B})).$$

It is straightforward to see that

$$\text{rank}(\mathcal{B}) = \text{rank}(B),$$

where B is the matrix representing $\mathcal{B}$ with respect to some basis. If B' is the matrix representing $\mathcal{B}$ with respect to some other basis, then we saw that $B' = X^T B X$ for some invertible matrix X. Hence it is clear that the rank does not depend on the choice of basis, and $\mathcal{B}$ is non-degenerate if and only if B is invertible.

Suppose now Q is a quadratic form on V, and $\mathcal{B}_Q$ its associated bilinear form. We say that Q is non-degenerate if $Q(u) \neq 0$ for all $u \in \mathrm{rad}(\mathcal{B}_Q)$, $u \neq 0$. If $\mathrm{char}(\mathbb{F}) \neq 2$, then it is clear that Q is non-degenerate if and only if $\mathcal{B}_Q$ is non-degenerate. We define $\mathrm{rad}(Q) := \mathrm{rad}(\mathcal{B}_Q)$, and $\mathrm{rank}(Q) := \mathrm{rank}(\mathcal{B}_Q)$.

Suppose now $\mathrm{char}(\mathbb{F}) \neq 2$. Suppose $\dim(\mathrm{rad}(Q)) = n - r$, i.e. $\mathrm{rank}(Q) = r$. Let V' be a subspace of V such that $\dim(V') = r$, $V' \bigcap \mathrm{rad}(Q) = 0$ and $V = V' \oplus \mathrm{rad}(Q)$. Then for any $u \in V$ there exist unique $v \in V'$, $w \in \mathrm{rad}(Q)$ such that $u = v + w$. Then we see that $Q(v + w) = 0 \Leftrightarrow Q(v) = 0$, since

$$\begin{aligned} Q(v+w) &= \frac{\mathcal{B}_Q(v+w, v+w)}{2} \\ &= \frac{\mathcal{B}_Q(v,v) + \mathcal{B}_Q(v,w) + \mathcal{B}_Q(w,v) + \mathcal{B}_Q(w,w)}{2} \\ &= \frac{\mathcal{B}_Q(v,v)}{2} \\ &= Q(v). \end{aligned}$$

Consider now $Q' := Q|_{V'}$, the restriction of Q to V'. Then Q' is non-degenerate. For suppose $v' \in \mathrm{rad}(Q')$. Then for any $v \in V'$, $w \in \mathrm{rad}(Q)$, we have

$$\begin{aligned} \mathcal{B}_Q(v', v+w) &= \mathcal{B}_Q(v', v) + \mathcal{B}_Q(v', w) \\ &= \mathcal{B}_{Q'}(v', v) + \mathcal{B}_Q(v', w) \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

But then $v' \in \mathrm{rad}(B_Q)$, and hence $v' = 0$, proving the assertion. Hence we have that

$$\begin{aligned} N_Q(0) &= |\mathrm{rad}(Q)| N_{Q'}(0) \\ &= q^{n-\mathrm{rank}(Q)} N_{Q'}(0) \end{aligned}$$

Suppose now that Q is a non-degenerate quadratic form on V, where V has even dimension $n = 2k$ over a finite field $\mathbb{F}_q$. A subspace V' of V is said to be *totally isotropic* with respect to Q if $Q(v') = 0$ for all $v' \in V'$. We define the *Witt index* of Q to be the maximum dimension of a totally isotropic subspace. It is well known that the Witt index is either k or $k - 1$ over a finite field. For the purposes of this work we will define the *type* of a quadratic form as follows:

Definition 1.15. *Let Q be a non-degenerate quadratic form on V, where V has even dimension $n = 2k$ over $\mathbb{F}_q$. Define the* type $\epsilon(Q)$ *by*

$$\epsilon(Q) := \begin{cases} +1 & \textit{if } Q \textit{ has Witt index } k \\ -1 & \textit{if } Q \textit{ has Witt index } k-1 \end{cases}$$

We say that Q has positive type *or* negative type *respectively. If Q is degenerate, we define*

$$\epsilon(Q) := \epsilon(Q'),$$

where $Q' = Q|_{V'}$ for some V' such that $\dim V' = \operatorname{rank}(Q)$, $V' \bigcap \operatorname{rad}(Q) = 0$.

The following theorem can be found in [54], Theorem 6.26, where the quantity denoted by $\eta((-1)^{n/2}\Delta)$ is the same as our $\epsilon(Q)$:

Theorem 1.16. *Suppose Q is a non-degenerate quadratic form on V, where V is r-dimensional over $\mathbb{F}_q$. Then the number of isotropic vectors with respect to Q is given by*

$$N_Q(0) = \begin{cases} q^{r-1} & \textit{if } r \textit{ is odd} \\ q^{k-1}(q^k + \epsilon(Q)(q-1)) & \textit{if } r = 2k \textit{ is even} \end{cases}$$

Then for an arbitrary quadratic form we get the following corollary:

Corollary 1.17. Suppose Q is a quadratic form on V, where V is n-dimensional over $\mathbb{F}_q$, and suppose $\operatorname{rank}(Q) = r$. Then the number of isotropic vectors with respect to Q is given by

$$N_Q(0) = \begin{cases} q^{n-1} & \text{if } r \text{ is odd} \\ q^{n-k-1}(q^k + \epsilon(Q)(q-1)) & \text{if } r = 2k \text{ is even} \end{cases}$$

Proof. We saw above that the number of isotropic vectors is given by $N_Q(0) = |\operatorname{rad}(Q)|.N_{Q'}(0)$, where Q' is non-degenerate on some r-dimensional vector space V'. As $|\operatorname{rad}(Q)| = q^{n-r}$, the result follows immediately from Theorem 1.16. □

We can similarly calulate the number of isotropic vectors with respect to a quadratic hermitian form, using the number of isotropic vectors with respect to a non-degenerate quadratic hermitian form calculated in [70], Lemma 10.4.

Theorem 1.18. *Suppose h is a quadratic hermitian form on W, where W is n-dimensional over $\mathbb{F}_{q^2}$, and suppose* $\operatorname{rank}(h) = r$. *Then the number of isotropic vectors with respect to Q is given by*

$$N_Q(0) = q^{2n-r-1}(q^r + (-1)^r(q-1)).$$

1.3 Subspaces of matrices as codes

In this section we will discuss two applications of subspaces of matrices to coding theory.

Let $\mathbb{F}$ be a field, and $V \simeq \mathbb{F}^n$ an n-dimensional vector space over $\mathbb{F}$. A *code* is a subset C of V. A code is said to be an $\mathbb{F}$-*linear code* if it is an $\mathbb{F}$-subspace of V. The *length* of a code is given by $n = \dim_{\mathbb{F}} V$. The *cardinality* of a code is defined to be $|C|$, and the *rank* of a linear code is defined to be $\dim_{\mathbb{F}} C$. A code is said to be a $(n, |C|)$-code, and a linear code is said to be an $[n, \dim_{\mathbb{F}} C]$-linear code.

Let $\omega : C \times C \to \mathbb{N}$ be a metric on C. We define the *weight* of a codeword a to be $w(a) := \omega(a, 0)$. The classical example is the *Hamming weight*: if $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}^n$ is a vector, then the Hamming weight $h(v)$ is defined to be the number of non-zero coefficients v_i.

The *weight enumerator* of a linear code C of length with respect to some weight function w is defined to be the polynomial

$$W(x) := \sum_w a_w x^w,$$

where a_w denotes the number of elements of C with weight w.

1.3.1 Rank metric codes

Define a metric on the space of $n \times n$ matrices by

$$\omega(A, B) := \operatorname{rank}(A - B).$$

A subset of matrices $C \subseteq M_n(\mathbb{F})$, together with the weight function arising from this metric, is said to be a *rank metric code.* If C is a subspace of $M_n(\mathbb{F})$, then C is a linear code. These codes were introduced by Delsarte [16], and further studied in for example [69], [28]. In [29] Gabidulin considered symmetric rank codes, corresponding to subspaces of symmetric matrices. Hence we can view a d-dimensional constant rank r subspace of $M_n(\mathbb{F})$ as an $[n, d]$-linear, constant weight r, rank metric code.

1.3.2 Codes from quadratic and hermitian forms

Subspaces of quadratic and hermitian forms have been used to define codes by Goethals [32] and de Boer [14] as follows.

Let U be a d-dimensional subspace of quadratic forms on $V \simeq \mathbb{F}^n$, i.e $U < \mathcal{Q}_n(\mathbb{F})$. Let $\mathbb{P}(V)$ denote the projective space of V. The number of elements of $\mathbb{P}(V)$ is given by $[n]_q := \frac{q^n-1}{q-1}$. For each $f \in U$ define a vector $c_f \in \mathbb{F}^{[n]_q}$ by

$$c_f := [f(u) \ : \ u \in \mathbb{P}(V)],$$

for some fixed ordering of V. Define the set C_U by

$$C_U := \{c_f \ : \ f \in U\}.$$

Then C_U is a subspace of $\mathbb{F}^{[n]_q}$, and $\dim(C_U) = \dim(U) = d$. Therefore C_U is an $[[n]_q, d]$-linear code over $\mathbb{F}$, with weight function being the Hamming weight.

Note that $f(u) = 0 \Leftrightarrow f(\lambda u) = 0$ for all $\lambda \in \mathbb{F}$. Hence the Hamming weight of a codeword c_f is then given by

$$w(c_f) = \frac{q^n - N_f(0)}{q-1}.$$

As we know the value of $N_f(0)$ from Lemma 1.17 above, we can easily calculate the weight enumerator of the code C_U as follows. Define

$$\begin{aligned} A_r^{\epsilon} &:= & |\{f \in U \mid \operatorname{rank}(f) = r \text{ and } \epsilon(f) = \epsilon\}| & \quad \text{if } r \text{ is even;} \\ A_r &:= & |\{f \in U \mid \operatorname{rank}(f) = r\}| & \quad \text{if } r \text{ is odd.} \end{aligned}$$

Lemma 1.19. Let U be a subspace of $\mathcal{Q}_n(\mathbb{F})$, and let C_U be the code as defined above. Then

$$a_w = \begin{cases} A_r^\epsilon & \text{if } w = q^{n-\frac{r}{2}-1}(q^{\frac{r}{2}} - \epsilon), \quad r \text{ even} \\ \sum_{r \text{ odd}} A_r & \text{if } w = q^{n-1} \\ 0 & \text{otherwise} \end{cases}$$

Suppose U is a constant rank r subspace. If r is odd, then the code C_U is a constant weight q^{n-1} code. In fact, if every element of U has odd rank, then C_U is also a constant weight q^{n-1} code. If r is even, then C_U is either a constant weight code, or a *two-weight code*. Two-weight codes have been studied extensively, and if the code is *projective* then it has important connections with strongly regular graphs and partial geometries, dating back to Delsarte [15]. Note that a code being "projective" means that no two columns of its generator matrix are linearly dependent. See for example [10] and [51], Section 2.6. We will see an example of a two-weight code arising from a subspace of quadratic forms in Section 3.2.3.

Similarly, given a d-dimensional subspace of quadratic hermitian forms $U \leq \mathcal{Q}H_n(\mathbb{F})$, we can define a $[[n]_{q^2}, d]$ code C_U over $\mathbb{F}$. If U is a constant rank r subspace, then C_U is a constant weight $q^{2n-k-1}\left(\frac{q^k+(-1)^{k+1}}{q+1}\right)$ code.

Chapter 2

Semifields and constant rank subspaces

In this chapter we introduce semifields, survey some properties, and show how they are related to constant rank subspaces.

2.1 Semifields

Definition 2.1. *A* semifield $(\mathbb{S},+,\circ)$ *is a set with two binary operations,* $+$ *and* $\circ$*, satisfying the following axioms.*

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

(S2) $x\circ(y+z)=x\circ y+x\circ z$ *and* $(x+y)\circ z=x\circ z+y\circ z$*, for all* $x,y,z\in\mathbb{S}$*.*

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

(S4) For all $a,b\in\mathbb{S}$ *there exist unique* $x,y\in\mathbb{S}$ *such that* $a\circ x=b$ *and* $y\circ a=b$*.*

(S5) $\exists 1\in\mathbb{S}$ *such that* $1\circ x=x\circ 1=x$*, for all* $x\in\mathbb{S}$*.*

We call the operations $+$ and $\circ$ *addition* and *multiplication* respectively. Multiplication is not assumed to be associative or commutative. Multiplication is left- and right-distributive over addition, by (S2). Axioms (S3)-(S5) imply that $(S^{\times}, \circ)$ forms a *loop*. If $\mathbb{S}$ is finite, then (S4) is implied by the other axioms.

A *presemifield* is a structure satisfying $(S1) - (S4)$, i.e. a multiplicative identity is not assumed.

It is easily shown that the additive group of a finite (pre)semifield is elementary abelian, and the exponent of the additive group is called the *characteristic* of the semifield.

Contained in a semifield are the following important substructures, relating to the concept of *nucleus*. The *left nucleus* $\mathbb{N}_l(\mathbb{S})$, *the middle nucleus* $\mathbb{N}_m(\mathbb{S})$, and the *right nucleus* $\mathbb{N}_r(\mathbb{S})$ are defined as follows:

$$\mathbb{N}_l(\mathbb{S}) := \{x \ : \ x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall y, z \in \mathbb{S}\}, \tag{2.1}$$

$$\mathbb{N}_m(\mathbb{S}) := \{y \ : \ y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, z \in \mathbb{S}\}, \tag{2.2}$$

$$\mathbb{N}_r(\mathbb{S}) := \{z \ : \ z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, y \in \mathbb{S}\}. \tag{2.3}$$

The intersection $\mathbb{N}(\mathbb{S})$ of the nuclei is called the *associative centre*, and the elements of $\mathbb{N}(\mathbb{S})$ which commute with all other elements of $\mathbb{S}$ form the *centre* $Z(\mathbb{S})$.

It is clear from the definition that the each of the nuclei are associative division algebras, and the centre is a field. The well known Wedderburn-Dickson Theorem [22], [72] states:

Every finite associative division algebra is commutative.

Hence we have the following is a standard result:

Theorem 2.2. *Let $\mathbb{S}$ be a finite semifield. Then $\mathbb{N}_l(\mathbb{S})$, $\mathbb{N}_r(\mathbb{S})$, $\mathbb{N}_m(\mathbb{S})$ and $Z(\mathbb{S})$ are all isomorphic to finite fields.*

If there is no confusion, we denote these substructures by $\mathbb{N}_l$, $\mathbb{N}_m$, $\mathbb{N}_r$ and Z.

Some further properties of finite semifields [46]:

1. $\mathbb{S}$ is a vector space V over its centre.

2. $\mathbb{S}$ is a (not necessarily associative) division algebra over its centre.

3. $\mathbb{S}$ is a left-vector space V_l over its left nucleus.

4. $\mathbb{S}$ is a right-vector space V_r over its right nucleus.

5. $\mathbb{S}$ is a left-vector space V_{lm} and a right-vector space V_{rm} over its middle nucleus.

We denote the dimension of V_l over $\mathbb{N}_l$ by n_l, and define n_m and n_r similarly. We define the *parameters* of $\mathbb{S}$ to be the tuple

$$(\#Z, \#\mathbb{N}_l, \#\mathbb{N}_m, \#\mathbb{N}_r).$$

Note that while Z is clearly a subfield of each of the nuclei, there is no restriction on the orders of the nuclei. See for example [65], where the classification of semifields of order 64 demonstrates the spectrum of possible parameters.

2.1.1 History and examples

All fields and division rings are semifields. We will call a semifield *proper* if multiplication is not associative.

The classical example of a proper semifield over the real numbers is the *octonions*. This was first discovered by Graves in 1843, and independently in 1845 by Cayley. Frobenius and Hurwitz showed that the only *normed* semifields over the real number are the real numbers, the complex numbers, the quaternions, and the octonions. Bott and Milnor [8], and independently Kervaire [45], proved that any semifield over the real numbers must have dimension 1,2,4 or 8.

Finite semifields were first considered by Dickson in 1906 [23]. He constructed the first non-trivial example of a finite semifield, as follows: Let $\mathbb{F}_{q^n}$ be a field for some q odd, and consider the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$. Let addition be vector space addition, and define a multiplication $\circ$ on V by

$$(a, b) \circ (c, d) := (ac + \gamma b^\sigma d^\sigma, ad + bc)$$

for all $a, b, c, d \in \mathbb{F}_{q^n}$, where $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})$, and γ is a non-square in $\mathbb{F}_{q^n}$. Then this defines a commutative semifield.

The following construction is due to Albert [2].

Definition 2.3. *Let $\mathbb{F}$ be a field, and $\mathbb{K}$ an extension field of $\mathbb{F}$ of degree n. Let $\rho, \tau \in \mathrm{Aut}(\mathbb{K} : \mathbb{F})$, and $\gamma \in \mathbb{K}$. Define a multiplication $\circ$ on $\mathbb{K}$ by*

$$x \circ y := xy - \gamma x^{\rho} y^{\tau}.$$

If $\gamma \notin \{x^{\rho-1}y^{\tau-1} : x, y \in \mathbb{K}\}$, then $\mathrm{P}(\mathbb{K}, \rho, \tau, \gamma) := (\mathbb{K}, \circ)$ *is a presemifield. A* generalized twisted field $\mathrm{GT}(\mathbb{K}, \rho, \tau, \gamma)$ *is a semifield isotopic to* $\mathrm{P}(\mathbb{K}, \rho, \tau, \gamma)$.

Note that this construction works for arbitrary fields. In the case where $\mathbb{K} = \mathbb{F}_{q^n}$ is a finite field, and $\mathbb{F} = \mathbb{F}_q$, we have that $\rho = \sigma^k$, $\tau = \sigma^m$ for some k, m, where σ is the Frobenius automorphism $x \mapsto x^q$. We then denote the twisted field by $\mathrm{GT}(\mathbb{F}_{q^n}, k, m, \gamma)$. Then $\mathrm{GT}(\mathbb{F}_{q^n}, k, m, \gamma)$ is a semifield if

$$N_{\mathbb{F}_{q^n}:\mathbb{F}_q}(\gamma) = \gamma\gamma^{\sigma} \dots \gamma^{\sigma^{n-1}} \neq 1.$$

We will study these semifields further in Chapter 4.

There are many families and constructions known for finite semifields. See [43], [53] for an overview of the available constructions. In Chapter 5 we will consider an important family known as *cyclic semifields*.

The classification of finite semifields is far from complete, and probably infeasible. Full classification by computer search has to date only been achieved up to order 243: see [21], [65], [66], [67]. The majority of semifields of small order have no known algebraic or geometric construction: for example, in [65] classification for order 64 found 332 *isotopy classes* (see Section 2.1.3 below), while only 35 were previously known. Similarly, there exist 80 *Knuth orbits* (see Section 2.2.2 below) of order 64, while only 13 were previously known.

2.1.2 Projective planes

Finite semifields are of interest in finite geometry due to their connection with projective planes:

Definition 2.4. *A* projective plane *is a set of* points $\mathcal{P}$*, a set of* lines $\mathcal{L}$ *and an incidence relation $\mathcal{I}$ on $\mathcal{P} \times \mathcal{L}$ such that*

- *for every pair of distinct points $p_1, p_2 \in \mathcal{P}$, there exists a unique line $l \in \mathcal{L}$ such that $(p_1, l), (p_2, l) \in \mathcal{I}$;*

- *for every pair of distinct lines $l_1, l_2 \in \mathcal{L}$, there exists a unique point $p \in \mathcal{P}$ such that $(p, l_1), (p, l_2) \in \mathcal{I}$;*
- *there exist four points, no three of which are incident with the same line.*

Every semifield coordinatizes a projective plane. See [17]. A semifield coordinatizes a *translation plane* which is also a *dual translation plane.* Conversely, every translation plane which is also a dual translation plane defines a semifield.

2.1.3 Isotopy

Let $(\mathbb{S}, \circ)$ and $(\mathbb{S}', \circ')$ be semifields n-dimensional over their centre $\mathbb{F}$. We say that $\mathbb{S}$ and $\mathbb{S}$ are *isotopic* if there exists a triple (F, G, H) of non-singular $\mathbb{F}$-linear transformations from $\mathbb{S}$ to $\mathbb{S}'$ such that

$$x^F \circ' y^G = (x \circ y)^H$$

for all $x, y \in \mathbb{S}$. Isotopy is an equivalence relation on the set of semifields, and the equivalence class of a semifield $\mathbb{S}$ under this relation is called the *isotopy class* of $\mathbb{S}$, denoted by $[\mathbb{S}]$.

The concept of isotopy was introduced by Albert [1]. Semifields are classified up to isotopy in part due the following important theorem of Albert [3]:

Theorem 2.5. *Two semifields are isotopic if and only if the planes they coordinatize are isomorphic.*

The following is also a standard result [39], [46]:

Theorem 2.6. *The parameters $(\#Z, \#\mathbb{N}_l, \#\mathbb{N}_m, \#\mathbb{N}_r)$ of a semifield are invariant under isotopy.*

It is well known that every presemifield is isotopic to a semifield. This can be shown by the so-called Kaplansky trick: Let $(\mathbb{P}, \circ)$ be a presemifield. Choose some $0 \neq e \in \mathbb{P}$. Define a new multiplication $\circ'$ by

$$(x \circ e) \circ' (e \circ y) = x \circ y$$

for all $x, y \in \mathbb{P}$. Then $(\mathbb{P}, \circ')$ is a semifield with identity element $e \circ e$.

2.2 Semifields as subspaces of matrices

Suppose $\mathbb{S}$ is a presemifield, n-dimensional over its centre $\mathbb{F}$. For each $x \in \mathbb{S}$, left multiplication by x defines an endomorphism $L_x \in \mathrm{End}(V)$ as follows:

$$L_x(y) := x \circ y$$

for each $y \in \mathbb{S}$. As $\mathbb{S}$ contains no zero divisors, L_x is invertible for each $0 \neq x \in \mathbb{S}$. Moreover, L_x is $\mathbb{F}$-linear and

$$L_{\lambda x+y} = \lambda L_x + L_y$$

for all $x, y \in \mathbb{S}$, $\lambda \in \mathbb{F}$. Hence the set

$$L_{\mathbb{S}} := \{L_x : x \in \mathbb{S}\}$$

forms an n-dimensional constant rank n $\mathbb{F}$-subspace of $\mathrm{End}(V) \simeq M_n(\mathbb{F})$. The set $L_{\mathbb{S}}$ is called the *semifield spread set* corresponding to $\mathbb{S}$.

In fact, as $\mathbb{S}$ is a right-vector space over $\mathbb{N}_r$, left-multiplication is an invertible $\mathbb{N}_r$-linear transformation of $\mathbb{S}$. Hence $L_{\mathbb{S}}$ can be viewed as a subset of $\mathrm{End}(V_r) \simeq M_{n_r}(\mathbb{N}_r)$. Similarly, $R_{\mathbb{S}}$ can be viewed as a subset of $\mathrm{End}(V_l) \simeq M_{n_l}(\mathbb{N}_l)$.

However, $L_{x \circ a}$ does not necessarily equal aL_x for all $a \in \mathbb{N}_r$. Hence the space $L_{\mathbb{S}}$ is not a $\mathbb{N}_r$-subspace of $M_{n_r}(\mathbb{N}_r)$. It is however an $\mathbb{F}$-subspace of $M_{n_r}(\mathbb{N}_r)$.

Similarly, the set of transformations of right-multiplication, denoted by $R_{\mathbb{S}} := \{R_x : x \in \mathbb{S}\}$, is an $\mathbb{F}$-subspace of $M_{n_l}(\mathbb{N}_l)$.

Conversely, suppose we have an n-dimensional constant rank n subspace U of $\mathrm{End}(V)$. As U and V both have dimension n over $\mathbb{F}$, there exists an $\mathbb{F}$-isomorphism $\phi : V \to U$. Now define a multiplication '$\circ$' on V by

$$x \circ y := \phi(x)y.$$

Then clearly $\mathbb{S}_U := (V, \circ)$ is a presemifield, and $L_{\mathbb{S}_U} = U$ by definition. Hence we get the standard result:

Theorem 2.7. *There exists an n-dimensional constant rank n subspace U of $M_n(\mathbb{F})$ if and only if there exists a presemifield $\mathbb{S}$ which is n-dimensional over $\mathbb{F}$.*

This theorem together with Lemma 1.2 gives the following corollary:

Corollary 2.8. Suppose there exists a presemifield $\mathbb{S}$ which is n-dimensional over its centre $\mathbb{F}$. Then for any $1 \leq r \leq m \leq n$, there exists a constant rank r subspace of $M_{m\times n}(\mathbb{F})$ of dimension n.

2.2.1 Isotopy and semifield spread sets

Let $\mathbb{S}$ and $\mathbb{S}'$ be isotopic via (F, G, H). Let L_x and L'_x denote left multiplication by x in $\mathbb{S}$ and $\mathbb{S}'$ respectively. Then we see that

$$\begin{aligned} L_x(y) &= x \circ y \\ &= (x^F \circ' y^G)^{H^{-1}} \\ &= (L'_{x^F}(y^G))^{H^{-1}} \\ &= (H^{-1}L'_{x^F}G)(y) \end{aligned}$$

for all $x, y \in \mathbb{S}$. Hence

$$L_{\mathbb{S}} = H^{-1}L_{\mathbb{S}'}G.$$

Note that F, G, H are invertible $\mathbb{F}$-linear transformations of V. Hence if we view $L_{\mathbb{S}}$ as a subspace of $\mathrm{End}(V)$, then we can view G, H as invertible elements of $\mathrm{End}(V)$. If we view $L_{\mathbb{S}}$ as a subspace of $\mathrm{End}(V_r)$ however, G and H do not necessarily lie in $\mathrm{End}(V_r)$. Nonetheless, we do have the following result, which can be found in [53], where the authors credit the result to Maduram [55]:

Theorem 2.9. *Two semifields $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if there exist invertible elements $X, Y \in \mathrm{End}(V_r)$ and $\sigma \in \mathrm{Aut}(\mathbb{N}_r)$ such that*

$$L_{\mathbb{S}} = XL^{\sigma}_{\mathbb{S}'}Y.$$

Note that this theorem says that $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if $L_{\mathbb{S}}$ and $L_{\mathbb{S}'}$ are equivalent in the sense of Section 1.1.3.

2.2.2 Knuth cubical array and Knuth orbit

Let $\mathcal{A}$ be an n-dimensional (not necessarily associative) algebra over a field $\mathbb{F}$, and let $\{e_0, e_1, \dots, e_{n-1}\}$ be an $\mathbb{F}$-basis for $\mathcal{A}$. Then for each i, j we have

$$e_i \circ e_j = \sum_{i,j,k=0}^{n-1} \alpha_{ijk} e_k \tag{2.4}$$

for some $a_{ijk} \in \mathbb{F}$. We call the coefficients a_{ijk} the *structure constants* of $\mathcal{A}$. We form the 3-dimensional (hyper)cube $T_{\mathcal{A}} := (a_{ijk})_{i,j,k}$. Conversely, given any hypercube T we can define an algebra $\mathcal{A}_T$ by defining a multiplication on $\mathbb{F}^n$ as in (2.4).

We can see how this hypercube is related to the endomorphisms of multiplication as follows:

$$\begin{aligned} L_{e_i} &= (a_{ijk})_{j,k} \\ R_{e_j} &= (a_{ijk})_{i,k} \\ L_v &= \sum_{i=0}^{n-1} v_i L_{e_i} = \sum_{i=0}^{n-1} v_i (a_{ijk})_{j,k} \\ R_v &= \sum_{i=0}^{n-1} v_i R_{e_i} = \sum_{i=0}^{n-1} v_j (a_{ijk})_{i,k} \end{aligned}$$

Given a vector $v \in \mathbb{F}^n$, we can define three maps $\phi_1^v, \phi_2^v, \phi_3^v$ from the set of hypercubes of order 3 to $M_n(\mathbb{F})$, which act on a hypercube $T = (a_{ijk})_{i,j,k}$ by:

$$\begin{aligned} \phi_1^v(T) &= (\sum_{i=0}^{n-1} v_i a_{ijk})_{j,k} \\ \phi_2^v(T) &= (\sum_{j=0}^{n-1} v_j a_{ijk})_{i,k} \\ \phi_3^v(T) &= (\sum_{k=0}^{n-1} v_k a_{ijk})_{i,j}. \end{aligned}$$

We call ϕ_m^v a *projection* of T. If $v \neq 0$ we say this projection is non-trivial.

Definition 2.10. *A hypercube is said to be be* non-singular *if every non-trivial projection is a non-singular matrix.*

Note that these definitions are a special case of the larger theory of *tensors*, but we will not need this theory for the purposes of this work. See [52] for more on this.

We can see now from the definitions above that $L_v = \phi_1^v(T_{\mathcal{A}})$ and $R_v = \phi_w^v(T_{\mathcal{A}})$, and hence

$$L_{\mathcal{A}} = \{\phi_1^v(T_{\mathcal{A}}) : v \in \mathbb{F}^n\}$$
$$R_{\mathcal{A}} = \{\phi_2^v(T_{\mathcal{A}}) : v \in \mathbb{F}^n\}.$$

Knuth [46] showed that $\mathcal{A}$ is a semifield if and only if $T_{\mathcal{A}}$ is *non-singular*. Knuth also showed that there is an action of the symmetric group S_3 on hypercubes which preserves nonsingularity: given an element $\pi \in S_3$ and a hypercube $T = (a_{ijk})_{i,j,k}$, define

$$T^\pi := (a_{\pi(ijk)})_{i,j,k}.$$

Then by ([46] Theorem 4.3.1), T^π is non-singular if and only if T is non-singular. Hence given a semifield $\mathbb{S}$ with associated hypercube T, we can define up to six semifields $\{\mathbb{S}^\pi\}$ with associated hypercubes $\{T^\pi\}$. We define the *Knuth orbit* of a semifield to be the set of isotopy classes

$$\mathcal{K}(\mathbb{S}) := \{[\mathbb{S}^\pi] : \pi \in S_3\}.$$

If two semifields lie in the same Knuth orbit, we say that they are *Knuth derivatives* of each other. The semifield $\mathbb{S}^{(23)}$ is usually called the *transpose* of $\mathbb{S}$, and the semifield $\mathbb{S}^{(12)}$ is usually called the *dual* of $\mathbb{S}$. The dual of $\mathbb{S}$ is equal to the opposite algebra of $\mathbb{S}$.

2.2.3 Commutative semifields and symmetric matrices

Let $\mathbb{S}$ be a semifield, and let $T = (a_{ijk})_{i,j,k}$ be the associated hypercube. Then it is clear that $\mathbb{S}$ is commutative if and only if $a_{ijk} = a_{jik}$ for all i, j, k. Consider then the semifield $\mathbb{S}^{(132)}$, and its spread set

$$L_{\mathbb{S}^{(132)}} = \{\phi_3^v(T) : v \in V\} \subset M_n(\mathbb{F}).$$

As T is non-singular, every element of this set is an invertible matrix. Moreover, as it is the spread set of a semifield, it is an n-dimensional constant rank n subspace of $M_n(\mathbb{F})$. We can see that every element of this set is symmetric, since

$$\begin{aligned}[\phi_3^v(T)]^T &= (\sum_{k=0}^{n-1} v_k a_{jik})_{i,j} \\ &= (\sum_{k=0}^{n-1} v_k a_{jik})_{i,j} \\ &= \phi_3^v(T)\end{aligned}$$

Hence we get the following known result [42]:

Theorem 2.11. *Let $\mathbb{F}$ be a field. Then there exists an n-dimensional constant rank n subspace of $S_n(\mathbb{F})$ if and only if there exists a commutative semifield n-dimensional over $\mathbb{F}$.*

This gives us the following simple corollary on constant rank subspaces of symmetric matrices over finite fields:

Corollary 2.12. Let $\mathbb{F}_q$ be any finite field. Then there exists an r-dimensional constant rank r subspace of $S_n(\mathbb{F}_q)$.

Proof. We know that every finite field has an extension field of degree r for all r. Hence by Theorem 2.11 there exists an r-dimensional constant rank r subspace of $S_r(\mathbb{F}_q)$, and for $r \leq n$ we can embed this space into $S_n(\mathbb{F}_q)$ simply by addending the appropriate zero matrices. This clearly does not affect the dimension or the rank, proving the claim. □

Remark 2.13. Commutative semifields have important applications in areas such as cryptography, due to their connection with so-called *Dembowski-Ostrom polynomials.* See for example [18] for more on this.

Chapter 3

Constant rank subspaces of symmetric and hermitian matrices

In this chapter we will investigate constant rank subspaces of symmetric and hermitian matrices over finite fields. We provide optimal bounds in the hermitian case, and bounds in the symmetric case that are optimal in some cases. We will then consider some constant rank subspaces of symmetric matrices over arbitrary fields.

3.1 Counting theorem for subspaces of function spaces

Let $\mathbb{F}$ be a field, and Ω some non-empty set. The *$\mathbb{F}$-valued function space on Ω* is the set of functions from Ω to $\mathbb{F}$, and is denoted by $\mathbb{F}^{\Omega}$. We can easily impose a vector space structure on $\mathbb{F}^{\Omega}$ as follows: given an element $\alpha \in \mathbb{F}$ and a function $f \in \mathbb{F}^{\Omega}$, define the function αf by

$$(\alpha f)(\omega) := \alpha(f(\omega))$$

for all $\omega \in \Omega$.

Example 3.1. Let V, V' be n, m-dimensional vector spaces over $\mathbb{F}$ respectively, and let W be an n-dimensional vector space over $\mathbb{K}$, where $\mathbb{K}$ is a degree two extension of $\mathbb{F}$. Recall that we are assuming $m \leq n$ throughout.

- A bilinear form $\mathcal{B}$ is an element of the function space $\mathbb{F}^{V' \times V}$, and the set of all bilinear forms is a subspace of $\mathbb{F}^{V' \times V}$.

- A quadratic form Q is an element of the function space $\mathbb{F}^{V}$, and the set of all quadratic forms is a subspace of $\mathbb{F}^{V}$.

- A hermitian form $\mathcal{H}$ is an element of the function space $\mathbb{K}^{W \times W}$, and the set of all hermitian forms is an $\mathbb{F}$-subspace of $\mathbb{K}^{W \times W}$, but *not* a $\mathbb{K}$-subspace.

- A quadratic hermitian form h is an element of the function space $\mathbb{F}^{W}$, and the set of all quadratic hermitian forms is a subspace of $\mathbb{F}^{W}$.

By the above correspondence, we can also consider

$$\begin{array}{lll} M_{m\times n}(\mathbb{F}) & \simeq \mathcal{B}_{m\times n}(\mathbb{F}) & \leq \mathbb{F}^{V' \times V}; \\ H_n(\mathbb{F}) & \simeq h_n(\mathbb{F}) & \leq \mathbb{F}^{W}, \end{array}$$

and if q is odd,

$$S_n(\mathbb{F}) \ \simeq \mathcal{Q}_n(\mathbb{F}) \ \leq \mathbb{F}^{V}.$$

As in Section 1.2.4, we denote by $N_f(\alpha)$ the number of elements $\omega \in \Omega$ such that $f(\omega) = \alpha$.

Let U be an $\mathbb{F}$-subspace of $\mathbb{F}^{\Omega}$. We define

$$N_U(0) := |\{\omega \in \Omega \mid f(\omega) = 0 \ \forall f \in U\}|.$$

We will call such an element a *common zero* of U. In this section we will prove a general expression for $N_U(0)$, which we will then apply to subspaces of bilinear, quadratic and quadratic hermitian forms, eventually leading to our main result of this section on constant rank subspaces. The proof is a generalization of a result of Fitzgerald and Yucas [27].

Theorem 3.2. *Let $\mathbb{F}_q$ be a finite field, Ω a finite set, and U a d-dimensional subspace of $\mathbb{F}_q^{\Omega}$. Then*

$$N_U(0) = \frac{\left(\sum_{f \in U} N_f(0)\right) - q^{d-1}|\Omega|}{q^{d-1}(q-1)} \tag{3.1}$$

Proof. Let $\{f_1, f_2, \dots, f_d\}$ be an $\mathbb{F}_q$-basis for U. Define a map $\mu : \Omega \to \mathbb{F}_q^d$ by

$$\mu(\omega) := (f_1(\omega), f_2(\omega), \dots, f_d(\omega))$$

for $\omega \in \Omega$. Then

$$N_U(0) = |\{\omega \in \Omega | \mu(\omega) = (0, 0, \dots, 0)\}|.$$

For each $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_d) \in \mathbb{F}_q^d$, define $f_\lambda \in U$ by

$$f_\lambda := \lambda_1 f_1 + \lambda_2 f_2 + \ldots + \lambda_d f_d.$$

Then given $\omega \in \Omega$, we have

$$f_\lambda(\omega) = \sum_{i=1}^{d} \lambda_i f_i(\omega) = \lambda \cdot \mu(\omega),$$

where the dot denotes the usual dot product. Denote $\lambda^\perp = \{v \in \mathbb{F}_q^d \mid \lambda \cdot v = 0\}$. Then $f_\lambda(\omega) = 0$ if and only if $\mu(\omega) \in \lambda^\perp$.

Hence the number of zeros of f_λ is given by

$$N_{f_\lambda}(0) = \sum_{v \in \lambda^\perp} |\{\omega \mid \mu(\omega) = v\}|.$$

We now sum this equation over all $\lambda \in \mathbb{F}_q^d$, giving

$$\sum_{f \in U} N_f(0) = \sum_{\lambda \in \mathbb{F}_q^d} N_{f_\lambda}(0) = \sum_{\lambda \in \mathbb{F}_q^d} \sum_{v \in \lambda^\perp} |\{\omega \mid \mu(\omega) = v\}|.$$

Next we reverse the order of summation, exploiting the fact that $v \in \lambda^\perp$ if and only if $\lambda \in v^\perp$, giving

$$\sum_{f \in U} N_f(0) = \sum_{v \in \mathbb{F}_q^d} \sum_{\lambda \in v^\perp} |\{\omega \mid \mu(\omega) = v\}|.$$

Now $|v^\perp|$ is equal to q^d if $v = 0$, and q^{d-1} otherwise. Hence

$$\sum_{f \in U} N_f(0) = q^d |\{\omega \mid \mu(\omega) = 0\}| + q^{d-1} \sum_{0 \neq v \in \mathbb{F}_q^d} |\{\omega \mid \mu(\omega) = v\}|.$$

But we know that $|\{\omega \mid \mu(\omega) = 0\}| = N_U(0)$, and

$$\sum_{0 \neq v \in \mathbb{F}_q^d} |\{\omega \mid \mu(\omega) = v\}| = |\Omega| - N_U(0).$$

Therefore

$$\sum_{f\in U} N_f(0) = q^d N_U(0) + q^{d-1}(|\Omega| - N_U(0)).$$

Rearranging and solving for $N_U(0)$ gives

$$N_U(0) = \frac{\left(\sum_{f\in U} N_f(0)\right) - q^{d-1}|\Omega|}{q^{d-1}(q-1)},$$

as claimed. □

3.2 Bounds for constant rank subspaces

3.2.1 Bilinear forms

We now apply Theorem 3.2 to subspaces of bilinear forms, and use the resulting formula to obtain new proof for Theorem 1.6.

Lemma 3.3. Let $\mathcal{B}$ be a bilinear form defined on $V' \times V$, where V', V is m, n-dimensional over $\mathbb{F}_q$ respectively, and $m \leq n$. Suppose $\mathcal{B}$ has rank r. Then the number of zeros of $\mathcal{B}$ is given by

$$N_{\mathcal{B}}(0) = q^{m+n-r-1}\left(q^r + q - 1\right).$$

Proof. Define $v^\perp = \{u \mid \mathcal{B}(u,v) = 0\}$. Then $N_{\mathcal{B}}(0) = \sum_v |v^\perp|$. Now if $v \in \mathrm{rad}_r(\mathcal{B})$, then $|v^\perp| = q^m$. If $v \notin \mathrm{rad}_r(\mathcal{B})$, then $|v^\perp| = q^{m-1}$. Hence

$$\begin{aligned} N_{\mathcal{B}}(0) &= q^m|\mathrm{rad}_r(\mathcal{B})| + q^{m-1}(q^n - |\mathrm{rad}_r(\mathcal{B})|) \\ &= q^m.q^{n-r} + q^{m-1}(q^n - q^{n-r}) \\ &= q^{m+n-r-1}\left(q^r + q - 1\right). \end{aligned}$$

as claimed. □

Theorem 3.4. *Let U be a d-dimensional subspace of $M_{m\times n}(\mathbb{F}_q)$. Let A_r denote the number of elements of U of rank r. Then*

$$N_U(0) = \sum_{r=0}^{m} A_r q^{m+n-d-r}.$$

Proof. We will view U as a subspace of $\mathbb{F}^{V'\times V}$. We know from Lemma 3.3 that the number of zeros of a bilinear form depends only on rank, and so

$$\begin{aligned}\sum_{f\in U} N_f(0) &= \sum_{r=0}^{n} A_r q^{m+n-r-1}\left(q^r+q-1\right)\\ &= q^{m+n-1}(\sum_{r=0}^{n} A_r) + \sum_{r=0}^{n} A_r q^{m+n-r-1}(q-1).\end{aligned}$$

Now $\sum_r A_r = q^d$, and $|\Omega| = |V'\times V| = q^{m+n}$. Hence

$$\left(\sum_{f\in U} N_f(0)\right) - q^{d-1}|\Omega| = \sum_{r=0}^{n} A_r q^{m+n-r-1}(q-1).$$

Applying Theorem 3.2 gives us

$$\begin{aligned}N_U(0) &= \frac{\sum_{r=0}^{n} A_r q^{m+n-r-1}(q-1)}{q^{d-1}(q-1)}\\ &= \sum_{r=0}^{n} A_r q^{m+n-d-r},\end{aligned}$$

as claimed. □

We can now provide a new proof to Theorem 1.6:

Theorem 3.5. *Let U be a constant rank r subspace of $M_{m\times n}(\mathbb{F}_q)$. Then*

$$\dim(U) \leq m+n-r.$$

Proof. As above, view U as a subspace of $\mathbb{F}^{V'\times V}$. Let $d = \dim(U)$. Then $A_0 = 1$, $A_r = q^d - 1$, and $A_i = 0$ otherwise. Hence Theorem 3.4 gives us

$$\begin{aligned}N_U(0) &= q^{m+n-d} + (q^d-1)q^{m+n-d-r}\\ &= q^{m+n-d-r}(q^r+q^d-1).\end{aligned}$$

But $N_U(0)$ is a positive integer, and q^r+q^d-1 is a positive integer relatively prime to q, and hence $q^{m+n-d-r}$ must be a positive integer. This implies that $d \leq m+n-r$, as claimed. □

Note that elements of the form $(u, 0)$ and $(0, v)$ are zeros of every bilinear form. We will call these 'trivial', and see that we have $q^m + q^n - 1$ of these. Suppose $m = n = d = r$, i.e. suppose we have an n-dimensional subspace of $n \times n$ invertible matrices. Then $N_U(0) = 2q^n - 1$, implying that U has no non-trivial common zeros.

Suppose $m = n$, $r = n - 1$, and $d = n + 1$. Then $N_U(0) = q^{n+1} + q^{n-1} - 1 = (2q^n - 1) + q^{n-1}(q-1)^2$, implying that U has $q^{n-1}(q-1)^2$ non-trivial common zeros.

3.2.2 Hermitian forms

We now apply Theorem 3.2 to subspaces of hermitian forms, and use the resulting formula to obtain an upper bound for the dimension of a constant rank subspace of hermitian forms. This bound will be shown to be sharp.

Theorem 3.6. *Let U be a d-dimensional subspace of quadratic hermitian forms on W, where W be a vector space n-dimensional over $\mathbb{F}_{q^2}$. Let A_r denote the number of elements of U of rank r. Then*

$$N_U(0) = \sum_{r=0}^{n} (-1)^r A_r q^{2n-d-r}.$$

Proof. Consider U as a subspace of $\mathbb{F}_q^W$. By Theorem 1.18 we know that if $h \in U$ has rank r, then $N_h(0) = q^{2n-1} + (-1)^r q^{2n-r-1}(q-1)$. Hence

$$\begin{aligned}\sum_{h \in U} N_h(0) &= \sum_{r=0}^{n} A_r(q^{2n-1} + (-1)^r q^{2n-r-1}(q-1)) \\ &= q^{2n+d-1} + \sum_{r=0}^{n} A_r(-1)^r q^{2n-r-1}(q-1),\end{aligned}$$

using the fact that $\sum_r A_r = q^d$. We know that $|\Omega| = |W| = q^{2n}$, and so

$$\left(\sum_{h \in U} N_h(0)\right) - q^{d-1}|\Omega| = \sum_{r=0}^{n} (-1)^r A_r q^{2n-r-1}(q-1).$$

Inputting this formula into equation 3.1 gives us

$$\begin{aligned} N_U(0) &= \frac{\sum_{r=0}^{n}(-1)^r A_r q^{2n-r-1}(q-1)}{q^{d-1}(q-1)} \\ &= \sum_{r=0}^{n}(-1)^r A_r q^{2n-r-d}, \end{aligned}$$

as claimed. □

The number $N_U(0)$ is a positive integer, as the zero vector is clearly isotropic with respect to every form. The above Theorem 3.6 leads to the following result in the spirit of the Chevalley-Warning Theorem (see for example [54], Theorem 6.5):

Corollary 3.7. Suppose we have d quadratic hermitian forms defined on $W \simeq \mathbb{F}_{q^2}^n$. Then if $n > d$, the forms have a non-trivial common zero. More precisely, the number of common zeros is divisible by q^{n-d}.

Proof. We may suppose that the forms are linearly independent over $\mathbb{F}_q$. Let U be the $\mathbb{F}_q$-subspace spanned by these forms. We have that

$$N_U(0) = q^{n-d}\left(\sum_{r=0}^{n}(-1)^r A_r q^{n-r}\right).$$

Each A_r is an integer, and as $r \leq n$, q^{n-r} is also an integer for all r. Hence the expression inside the brackets above is an integer, proving the claim. □

In fact we can improve this divisibility property further. Let $r_{\max}$ denote the maximum rank of elements of U, i.e. the largest r such that $A_r \neq 0$. Then

$$N_U(0) = q^{2n-d-r_{\max}}\left(\sum_{r=0}^{n}(-1)^r A_r q^{r_{\max}-r}\right),$$

and so the number of common zeros is divisible by $q^{2n-d-r_{\max}}$.

We are now ready to prove our main theorem on the maximum dimension of a constant rank subspace of hermitian matrices, or equivalently, subspaces of (quadratic) hermitian forms.

Theorem 3.8. *Let U be an $\mathbb{F}_q$-subspace of $H_n(\mathbb{F}_q)$ of constant rank r and dimension d. Then*

$$d \leq \begin{cases} r & \text{if } r \text{ is odd} \\ 2n-r & \text{if } r \text{ is even} \end{cases}$$

Proof. Following the notation above, we have that $A_r = q^d - 1$, $A_0 = 1$ and $A_i = 0$ otherwise. Inserting these values into the formula from Theorem 3.6 gives us that

$$N_U(0) = q^{2n-d} + (-1)^r (q^d - 1) q^{2n-r-d}.$$

If r is odd, we have

$$N_U(0) = q^{2n-r-d}(q^r - q^d + 1).$$

But $N_U(0)$ must be a positive integer, and hence $q^r - q^d + 1$ must be a positive integer, implying $d \leq r$ as claimed.

If r is even, we have

$$N_U(0) = q^{2n-r-d}(q^r + q^d - 1).$$

Now $q^r + q^d - 1$ is a positive integer, and is relatively prime to q. Hence q^{2n-r-d} must also be a positive integer, implying $d \leq 2n - r$ as claimed. □

We now show that these bounds are sharp.

Lemma 3.9. Suppose there exists a constant rank k subspace U of $M_{m \times (n-m)}(\mathbb{K})$ which is d-dimensional over $\mathbb{K}$. Then there exists a constant rank $2k$ subspace U' of $H_n(\mathbb{F})$ which is $2d$-dimensional over $\mathbb{F}$.

Proof. Let U' be the set of elements of the form

$$\begin{pmatrix} 0_m & A \\ \overline{A}^T & 0_{n-m} \end{pmatrix},$$

for all $A \in U$. Then it is straightforward to see that each element of U' is hermitian and has rank $2k$. Furthermore, U' is clearly a subspace of dimension $2d$ over $\mathbb{F}$. □

Hence we have our main theorem of this section:

Theorem 3.10. *The maximum dimension of a constant rank r subspace of $H_n(\mathbb{F}_q)$ is precisely r if r is odd, and $2n - r$ if r is even.*

Proof. We know from Corollary 2.12 that there exists an r-dimensional constant rank r subspace of $S_n(\mathbb{F}_q) \leq H_n(\mathbb{F}_q)$ for all r. Let $r = 2m$ be even. We know from Theorem 1.4 that there exists a constant rank $n-m$ subspace of $M_{m\times(n-m)}(\mathbb{F}_{q^2})$ which has dimension $n-m$ over $\mathbb{F}_{q^2}$. Hence by Lemma 3.9 there exists a constant rank r subspace of $H_n(\mathbb{F}_q)$ which has dimension $2(n-m) = 2n-r$ over $\mathbb{F}_q$. These two constructions, together with the bound proved in Theorem 3.8 prove the assertion. □

3.2.3 Quadratic forms

We now obtain similar formulae for subspaces of quadratic forms.

Theorem 3.11. *Let U be a d-dimensional subspace of quadratic forms on $V \times V$, where V is a vector space n-dimensional over $\mathbb{F}_q$. When $0 \neq r$ is even, let A_r^ϵ denote the number of elements of U of rank r and type ϵ. When r is odd, let A_r denote the number of elements of U of rank r, and define $A_0^+ = 1$, $A_0^- = 0$ for ease of notation. Then*

$$N_U(0) = \sum_{r \text{ even}} (A_r^+ - A_r^-) q^{n-d-\frac{r}{2}}.$$

Proof. By Theorem 1.17, and using $\sum_{r \text{ odd}} A_r + \sum_{r \text{ even}} (A_r^+ + A_r^-) = q^d$, we have that

$$\begin{aligned}\sum_{Q\in U} N_Q(0) &= \sum_{r \text{ odd}} A_r q^{n-1} + \sum_{r \text{ even}} \Big((A_r^+ + A_r^-) q^{n-1} + (A_r^+ - A_r^-) q^{n-\frac{r}{2}-1}(q-1) \Big) \\ &= q^{n+d-1} + \sum_{r \text{ even}} (A_r^+ - A_r^-) q^{n-\frac{r}{2}-1}(q-1).\end{aligned}$$

Now $|\Omega| = |V| = q^n$, and so

$$\left(\sum_{Q\in U} N_Q(0) \right) - q^{d-1}|\Omega| = \sum_{r \text{ even}} (A_r^+ - A_r^-) q^{n-\frac{r}{2}-1}(q-1).$$

Hence by Theorem 3.2 we have

$$\begin{aligned} N_U(0) &= \frac{\sum_{r \text{ even}} (A_r^+ - A_r^-) q^{n-\frac{r}{2}-1}(q-1)}{q^{d-1}(q-1)} \\ &= \sum_{r \text{ even}} (A_r^+ - A_r^-) q^{n-d-\frac{r}{2}},\end{aligned}$$

as claimed. □

Consider now constant rank subspaces of $\mathcal{Q}_n(\mathbb{F}_q)$. We know that $\mathcal{Q}_n(\mathbb{F}_q)$ is an $\mathbb{F}_q$-subspace of $\mathcal{H}_n(\mathbb{F}_q)$. Hence we know from 3.8 that if U is a constant rank r subspace, where r is *odd*, then U has dimension at most r, and by Corollary 2.12 there exists a subspace meeting this bound. The results for constant rank r subspaces of $\mathcal{Q}_n(\mathbb{F}_q)$ are not as complete for r *even*, due to the fact that the distribution amongst positive and negative type element is required. However, we can make some progress with some assumptions on the distribution.

Theorem 3.12. *Let U be a d-dimensional constant rank r subspace of $\mathcal{Q}_n(\mathbb{F}_q)$, where r is even. Then*

$$d \leq n - \frac{r}{2}$$

if $\epsilon(Q) = 1$ for all non-zero $Q \in U$,

$$d \leq \frac{r}{2}$$

if $\epsilon(Q) = -1$ for all non-zero $Q \in U$, and

$$d \leq n$$

if U contains equal number of non-zero elements of each type.

Proof. Suppose $\epsilon(Q) = \epsilon$ for all $Q \in U$. Then $A_0 = 1$, $A_r^{\epsilon} = q^d - 1$, and $A_i, A_i^{\pm} = 0$ otherwise. Hence by Theorem 3.11 we have

$$N_U(0) = q^{n-d} + \epsilon(q^d - 1)q^{n-d-\frac{r}{2}}.$$

If $\epsilon = 1$, then

$$N_U(0) = q^{n-d-\frac{r}{2}}(q^{\frac{r}{2}} + q^d - 1).$$

But $N_U(0)$ is a positive integer, and the number inside the brackets above is a positive integer relatively prime to q, implying that $d \leq n - \frac{r}{2}$, as claimed.

If $\epsilon = -1$ then

$$N_U(0) = q^{n-d-\frac{r}{2}}(q^{\frac{r}{2}} - q^d - 1),$$

implying that $d \leq \frac{r}{2}$.

If U contains equal number of non-zero elements of each type, then $A_0 = 1$, $A_r^+ = A_r^- = \frac{q^d-1}{2}$, and $A_i, A_i^{\pm} = 0$ otherwise. Hence

$$N_U(0) = q^{n-d},$$

implying $d \leq n$, as claimed. □

We can construct subspaces meeting the bound for cases (1) and (2) for q odd. We start with case (1):

Lemma 3.13. Suppose $\mathrm{char}(\mathbb{F}) \neq 2$, and suppose there exists a constant rank m subspace U of $M_{m\times(n-m)}(\mathbb{F})$ which is d-dimensional over $\mathbb{F}$. Then there exists a constant rank $2m$ subspace U' of $S_n(\mathbb{F})$ which is d-dimensional over $\mathbb{F}$, and in which every non-zero element has positive type.

Proof. Let U' be the set of elements of the form

$$\begin{pmatrix} 0_m & A \\ A^T & 0_{n-m} \end{pmatrix},$$

for all $A \in U$. Then it is straightforward to see that each element of U' is symmetric and has rank $2k$. Furthermore, U' is clearly a subspace of dimension d over $\mathbb{F}$.

Now an element $X \in S_n(\mathbb{F})$ of rank $2m$ has positive type if and only if there exists an $(n-m)$-dimensional subspace of V which is totally isotropic with respect to Q_X. It is clear that the subspace of vectors of the form $(0, 0, \ldots, 0, v_{m+1}, \ldots, v_n)$ forms such a subspace, proving the claim. □

Corollary 3.14. Suppose $r = 2m$ is even and q is odd. Then the maximum dimension of a constant rank r subspace of $S_n(\mathbb{F}_q)$ where every non-zero element has positive type, is precisely $n - m$.

Proof. We know from Theorem 1.4 that there exists a constant rank m subspace of $M_{m\times(n-m)}(\mathbb{F}_q)$ which has dimension $n - m$ over $\mathbb{F}_q$. Hence by Lemma 3.13 there exists a constant rank r subspace of $S_n(\mathbb{F}_q)$ which has dimension $n-m$ over $\mathbb{F}_q$. This construction, together with the bound proved in Theorem 3.12 prove the assertion. □

We now show that the bound described in Theorem 3.12, case (2) is sharp. To do this, we begin by recalling some facts about the embedding of a field into a matrix ring.

Suppose that we embed the field $\mathbb{F}_{q^{2m}}$ into $M_{2m}(\mathbb{F}_q)$ by its regular representation over $\mathbb{F}_q$. Then we obtain an $2m$-dimensional subspace, U, say, of $M_{2m}(\mathbb{F}_q)$ in which each non-zero element is invertible. Given $S \in U$, we have

$$\det S = N(S),$$

where we identify S with an element of $\mathbb{F}_{q^{2m}}$ and N denotes the norm mapping from $\mathbb{F}_{q^{2m}}^\times$ to $\mathbb{F}_q^\times$.

Theorem 3.15. *Let m be a positive integer. Then there exists an m-dimensional subspace of $S_{2m}(\mathbb{F}_q)$ in which each non-zero element has rank $2m$ and negative type.*

Proof. We first recall that an invertible symmetric matrix S in $S_{2m}(\mathbb{F}_q)$ satisfies $w(S) = -1$ if and only if $\det S$ is a non-square in $\mathbb{F}_q^\times$, except when m is odd and $q \equiv 3 \mod 4$, in which case the condition is that $\det S$ is a square.

We consider the field $\mathbb{F}_{q^{2m}}$ and its subfield $\mathbb{F}_{q^m}$. Let

$$N : \mathbb{F}_{q^{2m}}^\times \to \mathbb{F}_q^\times$$

be the norm mapping, which is well known to be a surjective homomorphism. We claim that each element $x \in \mathbb{F}_{q^m}^\times$ is a square in $\mathbb{F}_{q^{2m}}^\times$. To prove this, we must show that

$$x^{(q^{2m}-1)/2} = 1.$$

This is clear, however, since $x^{q^m-1} = 1$ and hence

$$x^{(q^{2m}-1)/2} = x^{(q^m-1)(q^m+1)/2} = 1,$$

as required. Thus, since N is a homomorphism, $N(x)$ is a square in $\mathbb{F}_q^\times$.

Finally, consider an embedding of $\mathbb{F}_{q^{2m}}$ into $S_{2m}(\mathbb{F}_q)$ by symmetric matrices. Let U be the image of $\mathbb{F}_{q^m}$ under this embedding. U is a subspace of dimension m in which each non-zero element has rank $2m$ and square determinant, by what we have proved above. Thus if m is odd and $q \equiv 3 \mod 4$, U is a subspace of $S_{2m}(\mathbb{F}_q)$ with the required property. In all other cases, let w be an element of $\mathbb{F}_{q^{2m}}$ with $N(w)$ a non-square in $\mathbb{F}_q^\times$. Then Uw is a subspace with the required property (here, we think of w as a symmetric matrix in the embedding of $\mathbb{F}_{q^{2m}}$ into $S_{2m}(\mathbb{F}_q)$).

□

Hence we have:

Corollary 3.16. Suppose $r = 2m$ is even and q is odd. Then the maximum dimension of a constant rank r subspace of $S_n(\mathbb{F}_q)$ where every non-zero element has negative type, is precisely m.

It is not clear how many elements of each type occur in a constant rank subspace. In general, they do not always fall into one of the above categories. For example, consider the 5-dimensional subspace U of $S_5(\mathbb{F}_3)$ consisting of the linear span of the matrices

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

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

A computer calculation shows that U is a 5-dimensional constant rank 4 subspace, containing 220 elements of positive type and 22 elements of negative type.

Remark 3.17. As stated in Section 1.3.2, a constant even rank space of quadratic forms (or equivalently for q odd, symmetric matrices) gives rise to a two-weight code, and, if the code is projective, a strongly regular graph. This example above leads to a $(243, 220, 199, 200)$-strongly regular graph. While a strongly regular graph with these parameters was already known, it is not known if this graph is isomorphic to a previously known graph. It is possible that large constant even rank subspaces of symmetric matrices could lead to interesting strongly regular graphs.

Remark 3.18. While Theorem 3.12 holds for subspaces of quadratic forms over fields of even characteristic, it does not give any information about subspaces of symmetric matrices over these fields. This remains a topic for future investigation.

3.3 Constant rank 3 spaces of symmetric matrices over arbitrary fields

In this section we will consider constant *odd* rank subspaces of symmetric matrices over different fields, with particular focus on constant rank 3 subspaces.

3.3.1 Constant odd rank subspaces over $\mathbb{R}$

Recall the definition of the *order* of a polynomial $f = \sum_i f_i y^i$:

$$\operatorname{ord}(f) := \inf\{i \mid f_i \neq 0\}$$

Lemma 3.19. Let A be an element of $S_n(\mathbb{R})$, and let $\operatorname{char}(A) = \sum_{i=0}^n a_i y^i$. Then $\operatorname{rank}(A) = n - \operatorname{ord}(\operatorname{char}(A))$.

Proof. It is well known that every real symmetric matrix is similar to a diagonal matrix. Hence A is similar to $\operatorname{diag}(b_1, b_2, \ldots, b_n)$ for some $b_i \in \mathbb{R}$, and $\operatorname{rank}(A) = \#\{i \mid b_i \neq 0\}$. Therefore $\operatorname{char}(A) = \prod_{i=1}^n (y - b_i)$, and hence the largest power of y dividing $\operatorname{char}(A)$ is $\#\{i \mid b_i = 0\} = n - \operatorname{rank}(A)$. Hence $\operatorname{ord}(\operatorname{char}(A)) = n - \operatorname{rank}(A)$, proving the claim. □

Hence we have the following result, which is not assumed to be new:

Lemma 3.20. Suppose U is a constant rank r subspace of $S_n(\mathbb{R})$, where r is *odd*. Then $\dim(U) \leq 1$.

Proof. Suppose U has dimension d, and let $\{E_1, E_2, \ldots, E_d\}$ be a basis of U. Then

$$\operatorname{char}(\sum_{i=1}^d x_i E_i) = \det(y - \sum_{i=1}^d x_i E_i) = y^d + \sum_{i=0}^n f_i(x_1, x_2, \ldots, x_d) y^{n-i}$$

where f_i is a homogeneous polynomial of degree i in $\mathbb{R}[x_1, x_2, \ldots, x_d]$. By Lemma 3.19, $f_i \equiv 0$ for $i \leq r$, and f_r has no non-trivial zeros (for otherwise U would contain elements of rank not equal to r). But it is well known that any homogeneous polynomial of odd degree in $\mathbb{R}[x_1, x_2, \ldots, x_d]$ has a non-trivial zero unless $d = 1$, proving the result. □

Note that the same result holds for any real closed field, as the proof only relies on the fact that every symmetric matrix is diagonalizable, and the fact that every homogeneous polynomial of odd degree has a non-trivial zero, both of which hold true for real closed fields.

3.3.2 Constant rank 3 subspaces of symmetric matrices over arbitrary fields

It seems reasonable to ask if a constant rank r subspace of symmetric matrices over an arbitrary field has dimension at most r when r is odd. We have proved this is true for a finite field, and an application of the Kronecker pair theory, discussed below, shows that over an algebraically closed field, the maximum dimension of an odd constant rank subspace of symmetric matrices is 1. As an indication that a general result for all fields might be true, we shall present a proof that, over an arbitrary field, the maximum dimension of a constant rank 3 subspace of symmetric matrices is 3.

Let V be a finite dimensional vector space over the field $\mathbb{F}$ and let f and g be symmetric bilinear forms defined on $V \times V$. A basic result in the theory of bilinear forms, due essentially to Kronecker, shows that there is a decomposition

$$V = V_1 \perp V_2 \perp V_3$$

of V into subspaces V_1, V_2 and V_3. This decomposition is *orthogonal* with respect to both f and g: that is, $f(v_i, v_j) = 0$ for all $v_i \in V_i \neq V_j \ni v_j$, and the same holds true for g. See for example [71], Theorem 3.1.

We may choose the notation so that f is non-degenerate on V_1, g is non-degenerate on V_2, and V_3 is the orthogonal direct sum (with respect to f and g) of *basic singular subspaces*. We allow the possibility that any of the V_i is a zero subspace and also that g is non-degenerate on V_1, or f is non-degenerate on V_2.

A basic singular subspace U, say, with respect to f and g, has odd dimension, $2k+1$, say, and the restriction of each of f and g to $U \times U$ has even rank $2k$. In fact, the subspace spanned by the restrictions of f and g forms a constant rank $2k$ subspace.

Hence the restrictions of f and g to the subspace V_3 above span a constant rank $2s$ subspace for some s.

If f and g each have rank r, then the restrictions of f and g to $V_1 \perp V_2$ each have rank $r - 2s$. If $s = 0$, then V_3 is clearly contained in the radical of both f and g.

We wish to show that if f and g span a constant rank 3 subspace, then we must have $s = 0$ and $\dim(V_3) = n - 3$, and hence f and g have the same radical.

Lemma 3.21. Let f and g be symmetric bilinear forms of rank r defined on $V \times V$. Suppose there exists a decomposition $V = V_1 \perp V_2$ such that f is non-degenerate on V_1 and g is non-degenerate on V_2, and the decomposition is orthogonal with respect to both f and g. If $|\mathbb{F}| > r + 1$, then there exist $a, b \in \mathbb{F}$ such that $af + bg$ is non-degenerate on V.

Proof. We can assume that

$$f = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \quad g = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix},$$

where A_1 and B_1 are $n_1 \times n_1$ symmetric matrices, and A_1 is invertible, and A_2 and B_2 are $n_2 \times n_2$ symmetric matrices, and B_2 is invertible. Furthermore, we may take

$$A_2 = \begin{pmatrix} A_2' & 0 \\ 0 & 0 \end{pmatrix}, \quad B_1 = \begin{pmatrix} B_1' & 0 \\ 0 & 0 \end{pmatrix},$$

where A_2' is an $(r - n_1) \times (r - n_1)$ invertible symmetric matrix, and B_1' is an $(r - n_2) \times (r - n_2)$ invertible symmetric matrix. Consider then

$$\begin{aligned} F(x,y) &:= \det(xf + yg) && (3.2) \\ &= \det(xA_1 + yB_1)\det(xA_2 + yB_2) && (3.3) \\ &=: F_1(x,y)F_2(x,y). && (3.4) \end{aligned}$$

We want to show that F is not identically zero over $\mathbb{F}$. Then we can see that F_1 is homogeneous of degree n_1, and has degree $r - n_2$ in y. Hence F_1 is divisible by $x^{n_1+n_2-r}$. Similarly F_2 is divisible by $y^{n_1+n_2-r}$, and so

$$F(x,y) = (xy)^{n_1+n_2-r}F'(x,y),$$

where F' is homogeneous of degree r, which is not divisible by x or y. Define a polynomial G in x by

$$\begin{aligned} G(x) &:= F(x,1) \\ &= x^{n_1+n_2-r}F'(x,1). \end{aligned}$$

Then $G(a)=0$ if and only if $a=0$ or a is a root of a polynomial of degree r. If $|\mathbb{F}|>r+1$, there exists some a such that $G(a)\neq 0$, and hence $af+g$ is non-degenerate on V, as claimed. □

Corollary 3.22. Let f and g be symmetric bilinear forms defined on $V\times V$ such that $\operatorname{rank}(af+bg)=r$ for all $a,b\in\mathbb{F}$, a and b not both zero. Suppose there exists a decomposition $V=V_1\perp V_2$ such that f is non-degenerate on V_1 and g is non-degenerate on V_2, and the decomposition is orthogonal with respect to both f and g. If $|\mathbb{F}|>r+1$, then $\dim(V)=r$.

Proof. From Lemma 3.21 we know that there exists $a,b\in\mathbb{F}$ such that $af+bg$ is non-degenerate on V. But as $\operatorname{rank}(af+bg)=r$ for all $(a,b)\neq(0,0)$, we have that $\dim(V)=r$, as claimed. □

This implies that f and g span a two-dimensional constant rank r subspace of symmetric bilinear forms on an r-dimensional space.

Corollary 3.23. Let f and g be symmetric bilinear forms defined on $V\times V$ such that $\operatorname{rank}(af+bg)=3$ for all $a,b\in\mathbb{F}$, a and b not both zero. Then if $|\mathbb{F}|>4$, f and g have the same radical.

Proof. Let $V=V_1\perp V_2\perp V_3$ be the decomposition as above. Suppose f and g have rank $2s$ on V_3, and hence rank $r-2s$ on $V_1\perp V_2$. Clearly we must have $s\in\{0,1\}$. Denote the restriction of f and g to $V_1\perp V_2$ by f' and g' respectively. Then f' and g' satisfy the conditions of the previous corollary, and so we must have $\dim(V_1\perp V_2)=r-2s$. If $s=1$, then $\dim(V_1\perp V_2)=1$. But then f' and g' span a two-dimensional constant rank 1 subspace of 1×1 symmetric matrices, which is not possible. Hence $s=0$, and so V_3 is contained in the radical of both f and g, and V_3 has co-dimension 3 in V, implying that $\operatorname{rad}(f)=\operatorname{rad}(g)$ $(=V_3)$, as claimed. □

The following example shows that the hypothesis on the size of the field is necessary. Suppose that $|\mathbb{F}| \leq 3$ and f and g are respectively represented by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

All non-trivial linear combinations of f and g have rank 3, yet f and g have different radicals.

Corollary 3.24. Let U be a subspace of symmetric bilinear forms defined on $V \times V$, where V is a finite dimensional vector space over the field $\mathbb{F}$. Suppose that each non-zero element of U has rank 3. Then if $|\mathbb{F}| > 4$, we have

$$\dim U \leq 3$$

and each non-zero element of U has the same radical.

Proof. It follows from Lemma 3.23 that each non-zero element of U has the same radical, R, say, when $|\mathbb{F}| > 4$. Let N be a complement of R in V. Then $\dim N = 3$ and it is clear that the restriction of U to $N \times N$ defines a subspace U', say, of symmetric bilinear forms on $N \times N$ with

$$\dim U = \dim U'.$$

Each element of U' is non-degenerate so U' is a constant rank 3 subspace of 3×3 matrices, and it follows that

$$\dim U' \leq 3.$$

This is what we wanted to prove. □

Theorem 3.8 and Corollary 3.24 imply the following result.

Corollary 3.25. Let U be a subspace of $S_n(\mathbb{F})$. Suppose that each element of $U^\times$ has rank 3. Then $\dim U \leq 3$.

Remark 3.26. In this chapter we have seen that the dimension of a constant rank 3 subspace of $S_n(\mathbb{F})$ is at most 3 for *any* field $\mathbb{F}$, and also that the dimension of a constant rank r subspace of $S_n(\mathbb{F}_q)$ at most r for any odd r and any *finite* field $\mathbb{F}_q$. This suggests that result may hold true for any odd r and any field $\mathbb{F}$. However, this question remains open at this time.

Chapter 4

Primitive elements in finite semifields

In this chapter, we prove the existence of left and right primitive elements in semifields of prime degree over their centre $\mathbb{F}_q$, for q large enough. For this chapter, by *semifield* we will always mean *finite semifield.*

4.1 Primitive elements

Let $\mathbb{S}$ be a (pre)semifield n-dimensional over $\mathbb{F}_q$, and a an element of $\mathbb{S}$. For this chapter we will denote multiplication in $\mathbb{S}$ by juxtaposition. We recursively define the left powers of a by

$$\begin{aligned} a^{(1} &= a; \\ a^{(i} &= aa^{(i-1} \end{aligned}$$

for all $i > 1$. We define the right powers $a^{i)}$ of a similarly. The left and right powers do not coincide in general.

Definition 4.1. *A (pre)semifield $\mathbb{S}$ is said to be* left primitive *if there exists some $a \in \mathbb{S}$ such that*

$$\mathbb{S}^\times = \{a^{(i} : i = 1, \ldots, q^{n-1}\}.$$

If such an a exists, we say that a is a left primitive element of $\mathbb{S}$.

We define *right primitive* similarly.

It is well known that every finite field is left and right primitive ([54], Theorem 2.8). Wene [73] considered the existence of primitive elements of finite semifields, and showed that they exist in many small semifields. Rúa [64] showed that Knuth's *binary semifield* [47] of order 32 does not contain a left or right primitive element. Knuth's binary semifields consist of elements of the field $\mathbb{F}_{q^n}$ for q even, n odd, with multiplication defined by

$$x \star y = xy + (\mathrm{Tr}(x)y + \mathrm{Tr}(y)x)^2.$$

(Note: for $q = 2$, n up to 23, all others have primitive elements by computer calculation.)

Rúa and Hentzel [33] showed that for order 32 and 64 there exist semifields which are left primitive but not right primitive (and vice-versa), and also semifields which are neither left nor right primitive. No other examples of non-primitive semifields are known.

In this chapter we will prove the following theorem:

Theorem 4.2. *Let $\mathbb{S}$ be a semifield, n-dimensional over its centre $\mathbb{F}_q$. Then*

(a) if $n = 3$, for any q, $\mathbb{S}$ is both left and right primitive;

(b) if n is prime and q is large enough, $\mathbb{S}$ is both left and right primitive.

4.1.1 Primitive elements as invertible matrices

Let $\mathbb{S}$ be a (pre)semifield n-dimensional over its centre $\mathbb{F}_q$. We saw in section 2.2 that the set of endomorphisms of left (resp. right) multiplication $L_{\mathbb{S}}$ (resp. $R_{\mathbb{S}}$) can be represented as an n-dimensional constant rank n subspace of $M_n(\mathbb{F}_q)$.

Given a matrix $A \in M_n(\mathbb{F}_q)$, the *characteristic polynomial* of A is defined as

$$\mathrm{char}(A) := \det(yI - A) \in \mathbb{F}_q[y].$$

Let $\mathbb{F}_q(A)$ denote the $\mathbb{F}_q$-subspace of $M_n(\mathbb{F}_q)$ spanned by the powers of A. Then it is well known ([54] Section 2.5) that

- $\mathbb{F}_q(A)$ is a field isomorphic to $\mathbb{F}_{q^n}$ if and only if $\mathrm{char}(A)$ is irreducible.
- A is a primitive element of $\mathbb{F}_q(A)$ if and only if $\mathrm{char}(A)$ is primitive.

Hence $\mathrm{char}(A)$ is primitive if and only if $A^i \neq A^j$ for $0 \leq i < j < q^n - 1$.

We can exploit this using the following important lemma. An alternative proof of the result can be found in [33].

Lemma 4.3. Let $\mathbb{S}$ be a (pre)semifield. Then x is left primitive if and only if L_x has primitive characteristic polynomial. Similarly, x is right primitive if and only if R_x has primitive characteristic polynomial over $\mathbb{F}_q$.

Proof. By definition,

$$x^{(i} = L_x^{i-1}x.$$

Then for any $0 < i < j \leq q^n - 1$, we have $x^{(i} = x^{(j}$ if and only if $(L_x^{i-1} - L_x^{j-1})x = 0$. Suppose x is left primitive in $\mathbb{S}$. Then $L_x^{i-1} \neq L_x^{j-1}$ for $0 < i < j \leq q^n - 1$. Hence L_x has primitive characteristic polynomial.

Conversely, suppose L_x has primitive characteristic polynomial. Then $(L_x^{i-1} - L_x^{j-1})$ is an invertible matrix for $0 < i < j \leq q^n - 1$. Hence $(L_x^{i-1} - L_x^{j-1})x \neq 0$, and so $x^{(i} \neq x^{(j}$ for $0 < i < j \leq q^n - 1$, implying x is left primitive and thus proving the claim.

The proof for right primitive elements is similar. □

For the binary semifield of order 32 described above, one can check that the set of characteristic polynomials is given by $\{\mathrm{char}(L_x)\} = \{y^5 + y + 1, y^5 + y^4 + y + 1, y^5 + y^4 + 1\}$, none of which is primitive, as expected.

Note that if a (pre)semifield $\mathbb{S}$ has a left identity element, i.e. an element e such that $ex = x$ for all x, if and only if $I \in L_{\mathbb{S}}$, where I denotes the identity matrix. Similarly, $\mathbb{S}$ has a right identity element if and only if $I \in R_{\mathbb{S}}$.

Hence to prove that every semifield of prime dimension n over its centre $\mathbb{F}_q$ contains a left and right primitive element, it suffices to show that every n-dimensional constant rank n subspace of $M_n(\mathbb{F}_q)$ containing the identity matrix has an element with primitive characteristic polynomal.

4.1.2 Homogeneous polynomials over finite fields

In this section, we investigate certain homogeneous polynomials defined in terms of n-dimensional constant rank n subspaces of $M_n(\mathbb{F}_q)$. We begin with a general definition.

Let $\mathbb{F}$ be a field, $\mathbb{K}$ be an extension field of $\mathbb{F}$, and let $g \in \mathbb{K}[x_1, \dots, x_n]$ be a polynomial with coefficients in $\mathbb{K}$. Let σ be an automorphism of $\mathbb{K}$ fixing $\mathbb{F}$. Then we let g^σ denote the polynomial obtained by applying σ to each coefficient of g.

Definition 4.4. *Let $\mathbb{K}$ be a cyclic extension of degree n of the field $\mathbb{F}$ and let σ generate the Galois group of $\mathbb{K}$ over $\mathbb{F}$. Let f be a non-zero homogeneous polynomial of degree n in $\mathbb{F}[x_1, \dots, x_n]$. We say that f is a* norm form *(with respect to $\mathbb{K}$) if there exists a basis $a_1, \dots, a_n$ for $\mathbb{K}$ over $\mathbb{F}$ with*

$$f = gg^\sigma \cdots g^{\sigma^{n-1}},$$

where

$$g = a_1x_1 + \cdots + a_nx_n \in \mathbb{K}[x_1, \dots, x_n].$$

Suppose that f is a norm form, as above, and the coefficient of x_1^n in f is 1. Then it follows that

$$1 = a_1a_1^\sigma \cdots a_1^{\sigma^{n-1}}.$$

We set

$$b_i = a_1^{-1}a_i, \quad 1 \leq i \leq n.$$

It is clear that $b_1 = 1$, $b_2, \dots, b_n$ is a basis for $\mathbb{K}$ over $\mathbb{F}$ and we may write

$$f = hh^\sigma \cdots h^{\sigma^{n-1}},$$

where

$$h = x_1 + b_2x_2 + \cdots + b_nx_n.$$

Thus, under the given hypothesis that the coefficient of x_1^n in f is 1, we may represent the norm form f as a product of Galois conjugate linear polynomials in which the coefficient of x_1 in each is 1.

Note that when we state that $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a norm form of degree n, it can only be such with respect to $\mathbb{F}_{q^n}$ and then we may take σ to be the Frobenius automorphism $\lambda \to \lambda^q$ of $\mathbb{F}_{q^n}$.

4.1.3 Associated polynomial of semifields

Let U be an n-dimensional constant rank n subspace of $M_n(\mathbb{F}_q)$, containing the identity. Let $B = \{E_1, \ldots, E_n\}$ be an ordered $\mathbb{F}_q$-basis for U. We know from Section 2.2 that every such U is the semifield spread set $L_{\mathbb{S}}$ of some (pre)semifield $\mathbb{S}$.

Definition 4.5. *Let U and B be as above. Then the* associated polynomial of U with respect to B *is the polynomial given by*

$$f_{U,B}(x_1, x_2, \ldots, x_n) := \det(x_1E_1 + \cdots + x_nE_n).$$

If we use a different basis B_1, say, of U, the corresponding polynomial f_{U,B_1} is obtained from $f_{U,B}$ by making an invertible linear transformation on the variables and is thus an equivalent polynomial.

It follows that such properties of the associated polynomials as being irreducible or a norm form are independent of the choice of basis and depend only on the subspace.

By abuse of language, we shall henceforth talk of the *associated polynomial* of U to be that obtained for an arbitrary choice of ordered basis B in which the first basis element E_1 is the identity matrix and we shall write f_U in place of $f_{U,B}$.

We note the following properties of f_U.

(1) f_U is a homogeneous polynomial of degree n.

(2) f_U has no non-trivial zeros over $\mathbb{F}_q$, as all non-zero elements of U are invertible.

(3) The coefficient of x_1^n is 1 (since $E_1 = I$).

(4) If $X = \lambda_1 E_1 + \lambda_2 E_2 + \ldots + \lambda_n E_n$, $\lambda_i \in \mathbb{F}_q$, and $\mathrm{char}(X)$ is the characteristic polynomial of X, then

$$\mathrm{char}(X) = \det(yI - X) = f_U(y - \lambda_1, -\lambda_2, \ldots, -\lambda_n) \ \in \mathbb{F}_q[y].$$

Following the notation introduced in Section 2.2, let

$$L_{\mathbb{F}_{q^n}} = \{L_z \mid z \in \mathbb{F}_{q^n}\}$$

be the semifield spread set of $\mathbb{F}_{q^n}$, an n-dimensional subspace of $M_n(\mathbb{F}_q)$. Given $z \in \mathbb{F}_{q^n}$, the eigenvalues of L_z are

$$z, z^q, \ldots, z^{q^{n-1}}$$

and consequently the characteristic polynomial of L_z is

$$\prod_{i=0}^{n-1} (y - z^{q^i}).$$

Theorem 4.6. *Let U be an n-dimensional constant rank n subspace of $M_n(\mathbb{F}_q)$, containing the identity matrix. Let $\{E_1 = I, \ldots, E_n\}$ be an ordered $\mathbb{F}_q$-basis for U and let f_U be the associated polynomial of U with respect to this basis. Suppose that f_U is a norm form, with*

$$f = gg^\sigma \cdots g^{\sigma^{n-1}},$$

where $g = x_1 + a_2 x_2 + \cdots + a_n x_n$ and 1, a_2, $\ldots$, a_n is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$. Given elements λ_1, $\ldots$, λ_n of $\mathbb{F}_q$, let

$$A = \lambda_1 E_1 + \lambda_2 E_2 + \cdots + \lambda_n E_n, \quad z = \lambda_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$$

be corresponding elements in U and $\mathbb{F}_{q^n}$, respectively. Then A and L_z have the same characteristic polynomial.

Proof. By property 4, after Definition 4.5 above,

$$\begin{aligned}\mathrm{char}(A) = \det(yI - A) &= f_U(y - \lambda_1, -\lambda_2, \ldots, -\lambda_n) \\ &= \prod_{i=0}^{n-1} (y - \lambda_1 - \lambda_2 a_2 - \ldots - \lambda_n a_n)^{\sigma^i} \\ &= \prod_{i=0}^{n-1} (y - z)^{\sigma^i} = \prod_{i=0}^{n-1} (y - z^{q^i}).\end{aligned}$$

As we observed earlier, this is the characteristic polynomial of L_z.

□

Corollary 4.7. Let U be an n-dimensional constant rank n subspace of $M_n(\mathbb{F}_q)$, containing the identity matrix. Suppose that the associated polynomial f_U is a norm form. Then each monic irreducible polynomial of degree n in $\mathbb{F}_q[y]$ occurs as the characteristic polynomial of exactly n elements of U.

Hence we have the following immediate consequence of Corollary 4.7 and Lemma 4.3:

Corollary 4.8. Let $\mathbb{S}$ be a semifield n-dimensional over $\mathbb{F}_q$. Suppose that the associated polynomial $f_{L_\mathbb{S}}$ is a norm form. Then $\mathbb{S}$ contains a left primitive element. Similarly, if $f_{R_\mathbb{S}}$ is a norm form, then $\mathbb{S}$ contains a right primitive element.

4.2 Primitive element theorems

We now apply some known results on norm forms to obtain the main results of this chapter on primitive elements.

Recall the definition of a generalized twisted field $\mathrm{GT}(\mathbb{F}_{q^n}, k, m, \gamma)$ from Definition 2.3. Menichetti ([56], Corollaries 29,32) proved the following theorem:

Theorem 4.9. *Let $\mathbb{S}$ be a semifield n-dimensional over $\mathbb{F}_q$. Then $f_{L_\mathbb{S}}$ (resp. $f_{R_\mathbb{S}}$) is a norm form if and only if $\mathbb{S}$ is isotopic to a generalized twisted field* $\mathrm{GT}(\mathbb{F}_{q^n}, k, m, \gamma)$ *for* $\gcd(n, k) = \gcd(n, m)$.

Hence Theorem 4.9 and Corollary 4.8 give us the following theorem:

Theorem 4.10. *Let $\mathbb{S}$ be a generalized twisted field* $\mathrm{GT}(\mathbb{F}_{q^n}, k, m, \gamma)$*, where* $\gcd(n,k) = \gcd(n,m)$*. Then $\mathbb{S}$ contains both a left and right primitive element.*

Remark 4.11. Note that our theorem does not apply to all twisted fields. However, this does not preclude the possibility that all twisted fields contain left and right primitive elements.

Remark 4.12. Rúa proved the above theorem for $n = 3$ in [64], by explicitly considering the multiplication in a twisted field. Our above proof does not require any knowledge of the multiplication, as it depends only on the fact that the associated polynomial is a norm form.

For some values of q and n, all semifields of size q^n with centre $\mathbb{F}_q$ have associated polynomials which are norm forms, as shown by Menichetti, and hence are both left and right primitive. We will discuss these cases now, beginning with the well known *Lang-Weil bound*:

Theorem 4.13 (Lang-Weil)**.** *Let f be an absolutely irreducible homogeneous polynomial in $\mathbb{F}_q[x_1, \dots, x_n]$ of degree d. Let N be the number of zeros of f over $\mathbb{F}_q$. Then N satisfies*

$$|N - q^{n-1}| \leq (d-1)(d-2)q^{n-\frac{3}{2}} + Cq^{n-2}$$

for some C which does not depend on q.

When originally proved, the Lang-Weil theorem, [50], was ineffective, as explicit bounds for C were not available. More recently, explicit bounds for C have been proven. See, for example, [30]. As far as we know, the best bound currently available was proved by Cafure and Matera, [9], Theorem 5.2.

Theorem 4.14 (Cafure and Matera)**.** *Let f be as above. Then*

$$|N - q^{n-1}| \leq (d-1)(d-2)q^{n-\frac{3}{2}} + 5d^{\frac{13}{3}}q^{n-2}$$

Hence if q is large enough, a homogeneous polynomial f of degree n in $\mathbb{F}_q[x_1, \dots, x_n]$ which has no non-trivial zeroes cannot be absolutely irreducible. If n is prime, this implies that f must be a norm form. Here "q is large enough" means that q satisfies the equation

$$q^{n-1} - 1 > (n-1)(n-2)q^{n-\frac{3}{2}} + 5n^{\frac{13}{3}}q^{n-2}.$$

The above sketches the proof of the following theorem:

Theorem 4.15. *Let f be a homogeneous polynomial of degree n in $\mathbb{F}_q[x_1, \dots, x_n]$. Suppose f has no non-trivial zero in $\mathbb{F}_q$. Then*

(a) if $n = 3$, for any q, f is a norm form;

(b) if n is prime and q is large enough, f is a norm form.

Case (a) was essentially known to Dickson, [24], whose proof was later corrected by Carlitz, [11]. Case (b) is due to [56], Proposition 17 (where the theorem is stated in terms of hypersurfaces in projective spaces). Hence Theorem 4.15 and Corollary 4.8 give us:

Theorem 4.16. *Let $\mathbb{S}$ be a semifield, n-dimensional over its centre $\mathbb{F}_q$. Then*

(a) if $n = 3$, for any q, $\mathbb{S}$ is both left and right primitive;

(b) if n is prime and q is large enough, $\mathbb{S}$ is both left and right primitive.

Remark 4.17. As an example, if we take $n = 5$, the condition "q large enough" becomes $q > 6296$, i.e. any semifield 5-dimensional over its centre $\mathbb{F}_q$ for $q > 6296$ has both a left and right primitive element. For $q < 6296$, we only know that the theorem does not hold for $q = 2$, and does hold for $q = 3$.

Remark 4.18. Note that Corollary 4.7 implies that if the associated polynomial of a semifield $\mathbb{S}$ which is n-dimensional over its centre $\mathbb{F}_q$ is a norm form, then every monic irreducible polynomial of degree dividing n occurs as the characteristic polynomial of an element of $L_{\mathbb{S}}$.

However, this is not a necessary condition for a semifield to be left primitive. For example, Knuth's binary semifield $\mathbb{S}$ of order 2^7 contains left (and right) primitive elements, but not every irreducible polynomial of degree 7 over $\mathbb{F}_2$ occurs as the characteristic polynomial of an element of $L_{\mathbb{S}}$. Furthermore, the $L_{\mathbb{S}}$ contains (non-identity) elements whose characteristic polynomial is not irreducible.

Remark 4.19. It is well known that every finite field contains a primitive element. Little is known about the existence of primitive elements in other families of semifields. See for example [13], [73].

Chapter 5

Semifields from skew-polynomial rings

In this chapter we will introduce a particular construction for semifields using skew-polynomial rings. We will show that these are isotopic to *cyclic semifields* as defined by Jha and Johnson in [40], and use this representation to obtain new results. We will also discuss this construction over arbitrary fields, and show how it is connected to some classical constructions of algebras.

In this chapter $\mathbb{F}$ will denote a field, $\mathbb{K}$ an extension field of $\mathbb{F}$ of degree n, σ an $\mathbb{F}$-automorphism of $\mathbb{K}$ fixing precisely $\mathbb{F}$, and V a vector space of dimension d over $\mathbb{K}$ (and hence dimension nd over $\mathbb{F}$).

5.1 Skew-polynomial rings

Let $\mathbb{F}$ be a field, $\mathbb{K}$ an extension field, σ an $\mathbb{F}$-automorphism of $\mathbb{K}$. We define a σ-derivation to be an $\mathbb{F}$-linear map $\delta : \mathbb{K} \to \mathbb{K}$ such that

$$(ab)^{\delta} = a^{\sigma} b^{\delta} + a^{\delta} b$$

for all $a, b \in \mathbb{K}$. The following definition is due to Ore [61]:

Definition 5.1. *The* skew polynomial ring $R = \mathbb{K}[t;\sigma,\delta]$ *is defined to be the set of polynomials in t with coefficients in $\mathbb{K}$, where addition is defined termwise, and multiplication is defined by $ta = a^{\sigma}t + a^{\delta}$ for all $a \in \mathbb{K}$.*

Note that the definition in [61] actually allows the coefficient ring $\mathbb{K}$ to be a division ring rather than a field. However, for the purposes of this work we will restrict to the case where $\mathbb{K}$ is a field.

Furthermore, we will restrict to the case where $\delta = 0$, because of the following theorem of Jacobson [38] Prop 1.2.20:

Theorem 5.2. *Let $R = \mathbb{K}[t;\sigma,\delta]$ be a skew-polynomial ring over a field $\mathbb{K}$, and suppose $\sigma \neq \mathrm{id}$. Then R is isomorphic to $\mathbb{K}[t;\sigma',0]$ for some σ'.*

We will denote $\mathbb{K}[t;\sigma,0]$ by $\mathbb{K}[t;\sigma]$. We will denote the fixed field of σ by $\mathbb{F}$, and the order of σ by n. We define *degree* in the usual way, and say that an element f is *irreducible* in R if there do not exist any $a, b \in R$ with $\deg(a), \deg(b) < \deg(f)$ such that $f = ab$. The following important properties of skew-polynomial rings will be needed in this chapter:

Theorem 5.3 (Ore [61])**.** *Let $R = \mathbb{K}[t;\sigma]$ be a skew-polynomial ring. Then*

1. *multiplication in R is associative and R satisfies both distributive laws;*

2. *multiplication in R is not commutative unless σ is the identity automorphism;*

3. *R is left- and right-Euclidean;*

4. *R is a left- and right-principal ideal domain;*

5. *the centre of R is $\mathbb{F}[t^n;\sigma] \simeq \mathbb{F}[y]$, where $\mathbb{F}$ is the fixed field of σ and the isomorphism maps t^n to y;*

6. *if $f_1, f_2, \ldots, f_r, g_1, g_2, \ldots, g_s$ are irreducible elements of R, and*

$$f_1 f_2 \ldots f_r = g_1 g_2 \ldots g_s$$

then $r = s$ and there is a permutation $\pi \in S_r$ such that $\deg(f_i) = \deg(g_{\pi(i)})$ for all i.

Note that properties (1),(3),(4) and (6) also hold for $R = \mathbb{K}[t;\sigma,\delta]$.

Hence we can define a semifield as follows:

Theorem 5.4. *Let V be the vector space consisting of elements of R of degree strictly less than d. Let $f \in R$ be an irreducible of degree d. Define a multiplication $\circ_f$ on V by*

$$a \circ_f b := ab \mod {}_r f$$

where juxtaposition denotes multiplication in R, and ' $\mod {}_r$*' denotes remainder on right division by f. Then $\mathbb{S}_f = (V, \circ_f)$ is semifield of dimension nd over $\mathbb{F}$.*

Proof. This multiplication is well defined, as R is right-Euclidean. We check that $\mathbb{S}_f$ has no zero divisors. Suppose $a, b \in \mathbb{S}_f$, and $a \circ_f b = 0$. This implies $\exists h \in \mathbb{S}_f$ such that $ab = hf$. Comparing degrees, part (6) of Theorem 5.3 gives a contradiction unless a or b is the zero polynomial. The other properties of a semifield are easily verified. Obviously $\mathbb{S}_f$ has dimension d over $\mathbb{K}$, and hence dimension nd over $\mathbb{F}$. □

This construction was considered by Ore [60] and Jacobson [35] in order to define a class of associative algebras, known as *cyclic algebras.* Though they did not consider non-associative structures, the fact that the above construction leads to a multiplication with no zero divisors was essentially known to them. Petit [63] then explicitly constructed non-associative algebras in this manner. This point will be further discussed in Section 5.2 below.

Remark 5.5. Note that for any $0 \neq \alpha \in \mathbb{K}$, the polynomials f and αf define the same semifield.

Remark 5.6. Note that defining the multiplication using remainder on *left* division by f also defines a semifield. However, in Section 5.1.2 we will show that the semifields obtained are Knuth derivatives of each other.

For the rest of this chapter we will write *mod* for *mod$_r$* unless otherwise stated, and write *divides* for *right divides.*

5.1.1 Eigenring and nuclei

Definition 5.7. *Let f be an irreducible element of R of degree d. Define the* eigenring *of f by*

$$E(f) = \{u \in R \mid \deg(u) < d, \ f \text{ divides } fu\}$$

Theorem 5.8. *[63] Let f be a* monic *irreducible element of R of degree d, and let $\mathbb{S}_f$ be the semifield as defined above. Then*

$$N_r(\mathbb{S}_f) = E(f)$$

and

$$E(f) = \mathbb{S}_f \Leftrightarrow f \in Z(R)$$

where $Z(R)$ denotes the centre of R.

Proof. First we will prove the second assertion. Suppose $E(f) = \mathbb{S}_f$. Let

$$f = \sum_{i=0}^{d} f_i t^i$$

where $f_i \in \mathbb{K}$, and $f_d = 1$ as f is monic. As $t \in E(f)$ by assumption, we must have $ft \equiv 0 \mod f$. But then

$$\begin{aligned} ft \mod f &= ft - tf \\ &= \sum_{i=0}^{d} (f_i - f_i^\sigma) t^i \\ &= 0, \end{aligned}$$

implying that $f_i = f_i^\sigma$ for all i, and so $f_i \in \mathbb{F}$ for all i. Now as $\alpha \in E(f)$ for all $\alpha \in \mathbb{K}$, we have

$$\begin{aligned} fa \mod f &= f\alpha - \alpha^{\sigma^d} f \\ &= \sum_{i=0}^{d} (\alpha^{\sigma^i} - \alpha^{\sigma^d}) f_i t^i \\ &= 0, \end{aligned}$$

implying that for each i we have $f_i = 0$ or $\alpha^{\sigma^i} = \alpha^{\sigma^d}$ for all $a \in \mathbb{K}$. As f is irreducible, we must have $f_0 \neq 0$ (for otherwise t would divide f). Hence if $f_i \neq 0$, we have $\alpha^{\sigma^i} = \alpha$ for all $\alpha \in \mathbb{K}$, and so $\sigma^i = \mathrm{id}$. Hence if $f_i \neq 0$ then n divides i. Therefore $f \in \mathbb{F}[t^n; \sigma] = Z(R)$, as claimed.

Conversely, if $f \in Z(R)$ then clearly $fu = uf$ is divisible by f for all u, and so $E(f) = \mathbb{S}_f$.

We now show that $\mathbb{N}_r(\mathbb{S}_f) = E(f)$. For any $a, b, c \in F$ of degree less than $d = \deg(f)$ we can find unique $u, v, w, z \in R$ of degree less than d such that

$$ab = uf + v, \text{ and}$$

$$bc = wf + z,$$

i.e. $a \circ_f b = v$, $b \circ_f c = z$. Then

$$(a \circ_f b) \circ_f c = v \circ_f c = vc \mod f,$$

while

$$a \circ_f (b \circ_f c) = a \circ_f z = az \mod f.$$

But as R is associative, we have that

$$ufc + vc = (ab)c = a(bc) = awf + az,$$

and hence

$$az = ufc + vc \mod f.$$

Therefore

$$(a \circ_f b) \circ_f c = a \circ_f (b \circ_f c) \Leftrightarrow ufc = 0 \mod f.$$

Let c be in the right nucleus. One can choose a, b such that $u = 1$. Then $fc = 0 \mod f$, implying that $c \in E(f)$. Conversely, if $c \in E(f)$ then $ufc = 0 \mod f$ for all u, and hence c is in the right nucleus, as claimed. □

Hence we get the following corollary:

Corollary 5.9. [63] $\mathbb{S}_f$ is associative if and only if $f \in Z(R)$.

We will see in Lemma 6.7 that if $\mathbb{K}$ is a finite field, then every element of $Z(R)$ is reducible. This is also implied by the Wedderburn-Dickson theorem, for otherwise we would obtain a non-commutative finite division algebra. We will see in Section 5.2 however that such elements can exist over infinite fields.

Theorem 5.10. *[63] Suppose f is a monic irreducible element of $R = \mathbb{K}[t;\sigma]$ such that $f \notin Z(R)$. The left and middle nuclei of $\mathbb{S}_f$ are given by*

$$\mathbb{N}_l(\mathbb{S}_f) = \mathbb{N}_m(\mathbb{S}_f) = (\mathbb{K}).1$$

i.e. they are the set of constant polynomials, and the centre is

$$Z(\mathbb{S}_f) = (\mathbb{F}).1.$$

Proof. Let $a, b, c \in R$, and u, v, w, z be as defined in the proof of Theorem 5.8. We saw that $(a \circ_f b) \circ_f c = a \circ_f (b \circ_f c) \Leftrightarrow ufc = 0 \mod f$.

We show that an element is in the left nucleus if and only if it has degree zero. First suppose a has degree zero. Then for any b, ab has degree strictly less than d, and hence $u = 0$ for all b. Therefore $ufc = 0 \mod f$ for all b, c, and so $a \in \mathbb{N}_l$.

Suppose now $\deg(a) = r > 0$, and let a_r be the leading coefficient of a. Let $b = \frac{1}{a_r^{-\sigma^r}} t^{d-r}$. Then ab is monic, and has degree d, and so $u = 1$. Let c be some element not in $E(f)$, i.e. $fc \neq 0 \mod f$. We know that such an element exists as $f \notin Z(R)$. Then $ufc = fc \neq 0 \mod f$, and so $a \notin \mathbb{N}_l$.

The proof for $\mathbb{N}_m$ is similar.

The centre is a subfield of $\mathbb{N}_l$, and so consists of all constant polynomials which commute with t. Since $ta = a^\sigma t$ for all $a \in \mathbb{K}$, the centre is therefore equal to the fixed field of σ, which is $\mathbb{F}$.

□

The nuclei of $\mathbb{S}_f$ were calculated in a different way by Dempwolff in [20], when he calculated the nuclei of cyclic semifields, which we will show in Section 5.2.4 to be equivalent to this construction.

5.1.2 Semifields from different skew-polynomial rings

In this section, we consider the isotopism problem for semifields constructed from different skew polynomial rings.

Consider the more general skew polynomial ring of the form $\mathbb{K}[t;\sigma,\delta]$. As noted above, Jacobson showed that if $\mathbb{K}$ is a field, then this ring is isomorphic to $\mathbb{K}[t;\sigma']$ for some σ'. We will now illustrate this for finite fields.

For any $x \in K$ the map

$$\delta_x : a \mapsto x(a - a^\sigma)$$

is a σ-derivation. It is easily verified that for a finite field, every σ-derivation is of this form. The following theorem shows, $\mathbb{K}[t;\sigma,\delta_x]$ is isomorphic to $\mathbb{K}[t;\sigma]$ for all x, and hence the semifields obtained are isotopic.

Theorem 5.11. *Let $R = \mathbb{K}[t;\sigma]$ and $R' = \mathbb{K}[t;\sigma,\delta_x]$ be skew-polynomial rings. Denote the multiplication in R and R' by $\circ$ and $\circ'$ respectively. Then R and R' are isomorphic via the map $\phi : R \to R'$ defined by*

$$a(t) \mapsto a(t-x),$$

where the evaluation of $a(t-x)$ occurs in R' (i.e. $\phi(t^2) = (t-x) \circ' (t-x)$). The map ϕ is linear and

$$\phi(a \circ b) = \phi(a) \circ' \phi(b)$$

for all $a, b \in R$

Proof. Clearly by the definition of ϕ, $\phi(t^i \circ t^j) = \phi(t^i) \circ' \phi(t^j)$ for all i, j, and $\phi(\alpha \circ \beta t^i) = \phi(\alpha) \circ' \phi(\beta t^i)$ for all $\alpha, \beta \in K$ and all i. Hence it suffices to show that

$$\phi(t \circ \alpha) = \phi(t) \circ' \phi(\alpha)$$

for all $\alpha \in K$. Now

$$\phi(t \circ \alpha) = \phi(\alpha^\sigma t) = \phi(\alpha^\sigma) \circ' \phi(t) = \alpha^\sigma \circ' (t-x) = \alpha^\sigma t - x\alpha^\sigma$$

while

$$\phi(t) \circ' \phi(\alpha) = (t-x) \circ' \alpha = \alpha^\sigma t + x(\alpha - \alpha^\sigma) - x\alpha = \alpha^\sigma t - x\alpha^\sigma$$

and the result holds. □

Note that defining the multiplication using remainder on *left* division by f also defines a semifield. Denote this semifield by ${}_f\mathbb{S}$, and the multiplication by '${}_f\circ$'. The following theorems show that the semifields obtained are Knuth derivatives of each other.

Theorem 5.12. *Let $R = \mathbb{K}[t;\sigma]$ and $R'' = \mathbb{K}[t;\sigma^{-1}]$ be skew-polynomial rings. Denote the multiplication in R and R'' by $\circ$ and $\circ''$ respectively. Then R and R' are anti-isomorphic via the map $\psi : R \to R'$ defined by*

$$\psi\left(\sum a_i t^i\right) = \sum a_i^{\sigma^{-i}} t^i,$$

i.e.

$$\psi(a \circ b) = \psi(b) \circ'' \psi(a)$$

Proof. For any a, b,

$$\begin{aligned}
\psi(a \circ b) &= \psi\left(\sum_{i,j} a_i b_j^{\sigma^i} t^{i+j}\right) \\
&= \sum_{i,j} a_i^{\sigma^{-i-j}} (b_j^{\sigma^i})^{\sigma^{-i-j}} t^{i+j} \\
&= \sum_{i,j} (b_j^{\sigma^{-j}})(a_i^{\sigma^{-i}})^{\sigma^{-j}} t^{i+j} \\
&= \sum_{i,j} \psi(b)_j (\psi(a)_i)^{\sigma^{-j}} t^{i+j} \\
&= \psi(b) \circ'' \psi(a),
\end{aligned}$$

as claimed. □

Corollary 5.13. Let R, R'' and ψ be as above. Let f be irreducible in R. Then

1. $\psi(f)$ is irreducible in R';
2. If $\mathbb{S}_f = R \mod Rf$, and ${}_{\psi(f)}\mathbb{S}'' = R'' \mod \psi(f)R'$, then $\mathbb{S}_f$ and ${}_{\psi(f)}\mathbb{S}''$ are anti-isomorphic (and hence Knuth derivatives of each other).

Proof. (1) Clear, for if $\psi(f) = \psi(a) \circ'' \psi(b)$, then by the previous theorem, $f = b \circ a$. But then a or b must be a unit, and as ψ preserves degrees, $\psi(a)$ or $\psi(b)$ must be a unit.

(2) We claim that ψ is an anti-isomorphism from $\mathbb{S}_f$ to ${}_{\psi(f)}\mathbb{S}''$. Clearly ψ is a bijective linear map. We need to show that

$$\psi(a \circ_f b) = \psi(b)_{\psi(f)} \circ'' \psi(a),$$

where

$$a \circ_f b = a \circ b \mod{}_r\ f, \text{ and}$$
$$\psi(b)_{\psi(f)} \circ'' \psi(a) = \psi(b) \circ'' \psi(a) \mod{}_l\ \psi(f).$$

Let $a \circ b = u \circ f + v$, where $\deg(v) < d = \deg(f)$. Then using the above theorem we obtain

$$\begin{aligned}\psi(a \circ_f b) &= \psi(v)\\ &= \psi(a \circ b - u \circ f) = \psi(a \circ b) - \psi(u \circ f)\\ &= \psi(b) \circ'' \psi(a) - \psi(f) \circ'' \psi(u) = \psi(b) \circ'' \psi(a) \mod{}_l\ \psi(f)\\ &= \psi(b)_{\psi(f)} \circ'' \psi(a),\end{aligned}$$

as claimed. □

Hence we have

$$\{\mathcal{K}(\mathbb{S}_f) : f \text{ irreducible in } \mathbb{K}[t;\sigma]\} = \{\mathcal{K}({}_f\mathbb{S}) : f \text{ irreducible in } \mathbb{K}[t;\sigma^{-1}]\}.$$

Remark 5.14. It is not clear when different skew polynomial rings $R = \mathbb{K}[t;\sigma]$ and $R' = \mathbb{K}[t;\sigma']$ define isotopic semifields. It is a necessary condition that σ and σ' have the same order.

We will see in Section 5.2.4 that a result of Kantor and Liebler implies that every semifield $\mathbb{S}_f$ for $f \in \mathbb{K}[t;\sigma]$ is isotopic to $\mathbb{S}_{\bar{f}}$ for some $\bar{f} \in \mathbb{K}[t;\sigma^{-1}]$. Hence we have that

$$\{[\mathbb{S}_f] : f \text{ irreducible in } \mathbb{K}[t;\sigma]\}\} = \{[\mathbb{S}_f] : f \text{ irreducible in } \mathbb{K}[t;\sigma^{-1}]\}\}.$$

Therefore combining this with the above result, we have

$$\{\mathcal{K}(\mathbb{S}_f) : f \text{ irreducible in } \mathbb{K}[t;\sigma]\} = \{\mathcal{K}({}_f\mathbb{S}) : f \text{ irreducible in } \mathbb{K}[t;\sigma]\}.$$

5.2 Connections with known constructions

5.2.1 Knuth semifields

We will now explicitly calculate the multiplication in $\mathbb{S}_f$ when f has degree 2 for illustrative purposes and for later comparison with previously known constructions.

Suppose $f \in \mathbb{K}[t;\sigma]$ has degree d. Then it has been shown by Ore ([62] Theorem 3) that $f = \sum_i f_i t^i$ has a linear right divisor if and only if there exists an element $\alpha \in \mathbb{K}$ such that

$$f_0 + f_1\alpha + f_2\alpha^{1+\sigma} + f_3\alpha^{1+\sigma+\sigma^2} + \ldots + f_d\alpha^{1+\sigma+\ldots+\sigma^{d-1}} = 0.$$

Hence if $f = t^2 - xt - y$, then f is irreducible if and only if

$$\alpha^{\sigma+1} - x\alpha - y = 0$$

has no solutions $\alpha \in \mathbb{K}$.

Suppose now $f = t^2 - xt - y$ is irreducible. Write elements $a + bt \in \mathbb{S}_f$ as a tuple $(a, b) \in \mathbb{K}^2$. Then

$$\begin{aligned}(a+bt)(c+dt) &= ac + (bc^\sigma + ad)t + bd^\sigma t^2\\ &= ac + (bc^\sigma + ad)t + bd^\sigma(f + xt + y)\\ &\equiv (ac + xbd^\sigma) + (bc^\sigma + ad + ybd^\sigma)t \mod {}_r f\end{aligned}$$

Hence

$$(a, b) \circ_f (c, d) = (ac + xbd^\sigma, ad + bc^\sigma + ybd^\sigma). \tag{5.1}$$

Similarly, if we let ${}_f\mathbb{S}$ denote the semifield obtained by taking remainder on left division by f, then

$$(a, b)_f \circ (c, d) = (ac + xb^{\sigma^{-1}}d^{\sigma^{-2}}, a^\sigma d + bc + ybd^{\sigma^{-1}}). \tag{5.2}$$

In [46], section 7.4, Knuth defined four classes of semifields two-dimensional over $\mathbb{K}$. We will denote them by $(K1) - (K4)$. The multiplications are defined by

$$\begin{array}{lll} (K1) & (ac + xb^\sigma d^{\sigma^{-2}}, & bc + a^\sigma d + yb^\sigma d^{\sigma^{-1}}) \\ (K2) & (ac + xb^\sigma d, & bc + a^\sigma d + yb^\sigma d) \\ (K3) & (ac + xb^{\sigma^{-1}}d^{\sigma^{-2}}, & bc + a^\sigma d + ybd^{\sigma^{-1}}) \\ (K4) & (ac + xb^{\sigma^{-1}}d, & bc + a^\sigma d + ybd) \end{array}$$

where we assume that $\alpha^{\sigma+1} + x\alpha - y = 0$ has no solutions $\alpha \in \mathbb{K}$.

Then comparing these with equations 5.1 and 5.2 gives us:

Theorem 5.15. *Let f be an irreducible polynomial of degree 2 in $\mathbb{K}[t;\sigma]$. Then*

- *$\mathbb{S}_f^{op}$ is a semifield of type $(K2)$.*
- *${}_f\mathbb{S}$ is a semifield of type $(K3)$.*

Note that the condition that $\alpha^{\sigma+1}+x\alpha-y=0$ has no solutions $\alpha \in \mathbb{K}$ is equivalent to the condition that $f'=t^2+xt-y$ is irreducible. But as we will see in the next section, the map $t \mapsto -t$ is an isomorphism of $\mathbb{K}[t;\sigma]$, and so $f=t^2-xt-y$ is irreducible if and only if f' is irreducible.

Hence we can see that these two families can be thought of as a special case of the construction using skew-polynomial rings. Knuth implicitly showed that these families are Knuth derivatives of each other, as noted in [4]. We see from Section 5.1.2 that that this is a special case of the more general fact that the families $\{\mathbb{S}_f : f \text{ irreducible}\}$ and $\{{}_f\mathbb{S} : f \text{ irreducible}\}$ are Knuth derivatives of each other.

5.2.2 Cyclic algebras

Given a field $\mathbb{K}$, an automorphism σ of $\mathbb{K}$ with fixed field $\mathbb{F}$, and a non-zero element γ of $\mathbb{F}$, we define the *cyclic algebra* $(\mathbb{K},\sigma,\gamma)$ as follows: Let $\{e_0,e_1,\dots,e_{d-1}\}$ be a $\mathbb{K}$-basis for the vector space $\mathbb{K}^d$. Define a multiplication on $\mathbb{K}^d$ by

$$e_i\alpha = \alpha^{\sigma^i}e_i$$

for all $\alpha \in \mathbb{K}$, and

$$e_ie_j = \begin{cases} e_{i+j} & \text{if } i+j<d \\ \gamma e_{i+j-d} & \text{if } i+j \geq d \end{cases}$$

As can be seen in ([38], Section 1.4), if we identify $e_i \leftrightarrow t^i$, then

$$(\mathbb{K},\sigma,\gamma) \simeq \frac{\mathbb{K}[t;\sigma]}{\langle t^n-\gamma\rangle} \simeq \mathbb{S}_{t^n-\gamma}.$$

Hence this construction is a special case of the above construction using skew-polynomial rings. As shown in Theorem 5.8, given a skew-polynomial ring R and an element f, the algebra $\mathbb{S}_f$ is associative if and only if f is in the centre of R, and $\mathbb{S}_f$ is a division algebra if and only if f is irreducible in R. Hence the cyclic algebra $(\mathbb{K},\sigma,\gamma)$ is always associative, and is a division algebra if and only if $f \in Z(R)$. We will see in Lemma 6.7 that for skew-polynomial rings over finite fields, every central element is reducible. However, over many fields this is not true, and much study has been done on the problem of deciding when a cyclic algebra is a division algebra. Cyclic division algebras have been used in space-time coding, e.g. in [59].

It is not clear whether irreducible elements must exist for all degrees in an arbitrary skew-polynomial ring. This remains a problem for future research.

5.2.3 Nonassociative analogues of cyclic algebras

Ore and Jacobson, when studying cyclic algebras, each considered structures obtained from the vector space of residue classes of $R = \mathbb{K}[t;\sigma]$ modulo a left ideal Rf. As they were interested only in associative algebras, they restricted to a substructure, the eigenring $E(f)$. They each proved (in different ways) the following theorem ([60], p. 242 and [35], p. 201-202):

Theorem 5.16. *If f is irreducible in R, then $E(f)$ is a[n associative] division algebra.*

As we have seen in the previous sections, if we choose a specific representative of each residue class (the unique element of degree less than $\deg(f)$), then the structure $\mathbb{S}_f$ obtained is a non-associative algebra. The theorem then extends to:

Theorem 5.17. *If f is irreducible in R, then $\mathbb{S}_f$ is a division algebra.*

The proof relies only on the theorem of Ore (Theorem 5.3 above). Hence it is perhaps fair to say that the construction of the semifields $\mathbb{S}_f$ was, in essence, known to Ore and Jacobson.

Petit [63] explicitly constructed the semifields $\mathbb{S}_f$ in 1966, and calculated the nuclei. This work was brought to the author's attention by W.M. Kantor subsequent to the original submission of this thesis.

Sandler [68] considered non-associative generalizations of cyclic algebras over finite fields. These can be seen to be precisely algebras of the form $\mathbb{S}_f$, where $f = t^n - \gamma \in \mathbb{K}[t;\sigma]$ and $\gamma \notin \mathbb{F}$. He showed that this defines a semifield if and only if γ does not lie in any proper subfield of $\mathbb{K}$.

Jha and Johnson further generalized this by defining *cyclic semifields*, using the theory of semilinear transformations. We will now show that these semifields are precisely the semifields (isotopic to) semifields of the form $\mathbb{S}_f$, $f \in R$.

5.2.4 Equivalence with cyclic semifields

Definition 5.18. *A* semilinear transformation *on a vector space* $V = \mathbb{K}^d$ *is an additive map* $T : V \to V$ *such that*

$$T(\alpha v) = \alpha^\sigma T(v)$$

for all $\alpha \in \mathbb{K}$, $v \in V$, *for some* $\sigma \in \mathrm{Aut}(\mathbb{K})$. *The set of invertible semilinear transformations on* V *form a group called the* general semilinear group, *denoted by* $\Gamma\mathrm{L}(d, \mathbb{K})$.

Note that choosing a basis for V gives us

$$T(v) = A(v^\sigma)$$

where A is some invertible $\mathbb{K}$-linear transformation from V to itself, σ is an automorphism of $\mathbb{K}$, and v^σ is the vector obtained from v by applying the automorphism σ to each coordinate of v with respect to this basis.

Definition 5.19. *An element* T *of* $\Gamma\mathrm{L}(d, \mathbb{K})$ *is said to be* irreducible *if the only* T*-invariant subspaces of* V *are* V *and* $\{0\}$.

In [40] Jha and Johnson defined a semifield as follows.

Theorem 5.20. *Let* T *be an irreducible element of* $\Gamma\mathrm{L}(d, \mathbb{K})$. *Fix a* K*-basis* $\{e_0, e_1, \dots, e_{d-1}\}$ *of* V. *Define a multiplication on* V *by*

$$a \circ b = a(T)b = \sum_{i=0}^{d-1} a_i T^i(b)$$

where $a = \sum_{i=0}^{d-1} a_i e_i$. *Then* $\mathbb{S}_T = (V, \circ)$ *defines a semifield.*

We call a semifield $\mathbb{S}_T$ a *cyclic semifield.* It is clear that the spread set of endomorphisms of left multiplication of $\mathbb{S}_T$ is given by

$$L_{\mathbb{S}_T} = \{\sum_{i=0}^{d} a_i T^i : a_i \in \mathbb{K}\}.$$

We will show that these semifields are isotopic to the semifields constructed in the previous section.

Theorem 5.21. *Let $\mathbb{S}_f$ be a semifield defined by an irreducible $f = t^d - \sum_{i=0}^{d-1} f_i t^i$ in R, and let L_t denote left multiplication by t in $\mathbb{S}_f$. Then the following properties hold.*

1. *L_t is an element of $\Gamma\mathrm{L}(d, \mathbb{K})$ with accompanying automorphism σ.*

2. *If we write elements $v = \sum_{i=0}^{d-1} v_i t^i$ of $\mathbb{S}_f$ as column vectors $(v_0, v_1, \ldots, v_{d-1})^t$, then*
$$L_t(v) = A_f(v^\sigma)$$
where
$$A_f = \begin{pmatrix} 0 & 0 & \ldots & 0 & f_0 \\ 1 & 0 & \ldots & 0 & f_1 \\ 0 & 1 & \ldots & 0 & f_2 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & f_{d-1} \end{pmatrix}.$$

3. *If $a = \sum_{i=0}^{d-1} a_i t^i$, then*
$$L_a = a(L_t) = \sum_{i=0}^{d-1} a_i L_t^i.$$

4. *The semilinear transformation L_t is irreducible.*

Proof. (1) Clearly L_t is linear, as multiplication is distributive. Let v be any vector. If $tv = uf + w$ for some unique u, w, $\deg(w) < d$, then $L_t(v) = w$. Let α be any non-zero element of $\mathbb{K}$. Then

$$\begin{aligned} L_t(\alpha v) &= t(\alpha v) \mod f = (\alpha^\sigma tv) \mod f \\ &= \alpha^\sigma(uf + w) \mod f = (\alpha^\sigma uf + \alpha^\sigma w) \mod f \\ &= \alpha^\sigma w = \alpha^\sigma L_t(v). \end{aligned}$$

(2) The action of L_t is as follows:

$$L_t : 1 \mapsto t \mapsto t^2 \mapsto \ldots \mapsto t^{d-1} \mapsto (t^d \mod f) = \sum_{i=0}^{d-1} f_i t^i$$

and so $L_t(v) = A_f(v^\sigma)$ as claimed.

(3) By definition,

$$L_a(b) = a \circ_f b = \left(\sum_{i=0}^{d-1} a_i t^i\right) b \mod f = \sum_{i=0}^{d-1} a_i (t^i b \mod f) = \sum_{i=0}^{d-1} a_i L_{t^i}(b)$$

while

$$a(L_t)(b) := \sum_{i=0}^{d-1} a_i L_t^i(b).$$

Hence it suffices to show that $L_t^i(b) = L_{t^i}(b)$ for all i. Suppose $L_t^i(b) = (t^i b) \mod f$ for some i. Let $L_t^i(b) = b'$. Then $t^i b = cf + b'$ for some c, and

$$\begin{aligned} L_t^{i+1}(b) &= L_t(L_t^i(b)) = L_t(b') \\ &= L_t(t^i b - cf) = t(t^i b - cf) \mod f \\ &= (t^{i+1} b - tcf) \mod f = (t^{i+1} b) \mod f \\ &= L_{t^{i+1}}(b). \end{aligned}$$

Hence the result follows by induction.

(4) Let W be a L_t-invariant subspace of V such that $0 < r := \dim(W) < d$. Choose some non-zero $w \in W$. Then the set

$$\{w, L_t w, L_t^2 w, \ldots, L_t^r w\} \subset W$$

is linearly dependent. Hence there exist elements $a_0, a_1, \ldots, a_d$ in $\mathbb{K}$, not all zero, such that

$$\sum_{i=0}^{d-1} a_i (L_t^i w) = 0.$$

Let $a = \sum_{i=0}^{d-1} a_i t^i$. Then

$$\left(\sum_{i=0}^{d-1} a_i L_t^i\right) w = a(L_t) w = 0.$$

By part (3) of this theorem, $a(L_t) = L_a$, and so

$$a \circ_f w = 0.$$

But $a \circ_f w = 0$ implies $a = 0$ or $w = 0$, a contradiction. Hence L_t is irreducible. □

Corollary 5.22. The spread set of endomorphisms of left multiplication of elements in $\mathbb{S}_f$ is $\{a(L_t) \mid a \in \mathbb{S}_f\}$.

The following theorem is an immediate consequence of the definition of $\mathbb{S}_T$ and Theorem 5.21.

Theorem 5.23. *If f is irreducible in R, and $L_{t,f}$ denotes the semilinear transformation $v \mapsto tv \mod f$, then $\mathbb{S}_f = \mathbb{S}_{L_{t,f}}$.*

Kantor and Liebler [44] noted that conjugate semilinear transformations define isotopic semifields.

Lemma 5.24. Suppose $T = \phi^{-1}U\phi$ for some $\phi \in \Gamma\mathrm{L}(d, \mathbb{K})$, and let $\rho \in \mathrm{Aut}(\mathbb{K})$ be the accompanying automorphism of ϕ. Let $\mathbb{S}_T = (V, \circ)$, $\mathbb{S}_U = (V, \star)$. Then

$$\phi(a \circ b) = a^\rho \star \phi(b).$$

Hence to show that

$$\{[\mathbb{S}_T]\} = \{[\mathbb{S}_f]\},$$

where T runs through all irreducible elements of $\Gamma\mathrm{L}(d, \mathbb{K})$ and f runs through all irreducible elements of $\mathbb{K}[t; \sigma]$ of degree d, it suffices to show that T is $\Gamma\mathrm{L}(d, \mathbb{K})$-conjugate to $L_{t,f}$ for some f irreducible of degree d in $\mathbb{K}[t; \sigma]$.

Theorem 5.25. *Let T be any irreducible element of $\Gamma\mathrm{L}(d, \mathbb{K})$ with automorphism σ. Then T is $\mathrm{GL}(d, \mathbb{K})$-conjugate to $L_{t,f}$ for some $f \in R = \mathbb{K}[t; \sigma]$, and hence $\mathbb{S}_T$ is isotopic to $\mathbb{S}_f$.*

Proof. Identify V with the set of polynomials of degree $\leq d - 1$ in R and choose some non-zero element $v \in V$. Consider the basis

$$\{v, Tv, T^2v, \dots, T^{d-1}v\},$$

and define a transformation $\phi \in \mathrm{GL}(d, \mathbb{K})$ by

$$\phi(t^i) := T^i v,$$

for $i = 0, 1, \dots, d - 1$. Then there exist $f_i \in \mathbb{K}$ such that

$$T^d v = \sum_{i=0}^{d-1} f_i T^i v.$$

We claim that

$$T\phi = \phi L_{t,f},$$

with

$$f = t^d - \sum_{i=0}^{d-1} f_i t^i \in R.$$

It suffices to show that these transformations coincide on t^i for all i. Suppose first that $i < d-1$. Then

$$T\phi(t^i) = T(T^i v) = T^{i+1} v,$$

while

$$\phi L_{t,f}(t^i) = \phi(t^{i+1} \mod f) = \phi(t^{i+1}) = T^{i+1} v,$$

as claimed. Suppose now $i = d-1$. Then

$$T\phi(t^{d-1}) = T(T^{d-1} v) = T^d v = \sum_{i=0}^{d-1} f_i T^i v,$$

while

$$\phi L_{t,f}(t^{d-1}) = \phi(t^d \mod f) = \phi\left(\sum_{i=0}^{d-1} f_i t^i\right) = \sum_{i=0}^{d-1} f_i T^i v,$$

and so

$$T\phi = \phi L_{t,f}$$

as claimed. □

Note that the polynomial f depends on the choice of v, and hence T may be $\Gamma\mathrm{L}(d, \mathbb{K})$-conjugate to $L_{t,g}$ for some other $g \in \mathbb{K}[t;\sigma]$. We will see in the Chapter 6 when two semilinear transformations $L_{t,g}$ and $L_{t,f}$ are $\Gamma\mathrm{L}(d, \mathbb{K})$-conjugate.

Remark 5.26. The following observation of Kantor and Liebler (in [44]), together with the above theorems, allow us to prove the assertion in Remark 5.14.

If T is an irreducible semilinear transformation with automorphism σ, then T^{-1} is an irreducible semilinear transformation with automorphism σ^{-1}, and $\mathbb{S}_T$ and $\mathbb{S}_{T^{-1}}$ are isotopic. (See [44], Remark 4.1, where the statement is made in terms of projective planes.)

This implies that every semifield $\mathbb{S}_f$ for $f \in \mathbb{K}[t;\sigma]$ is isotopic to $\mathbb{S}_{\bar{f}}$ for some $\bar{f} \in \mathbb{K}[t;\sigma^{-1}]$. In fact it can be shown that $\bar{f}$ is the reciprocal of f. Hence we have that

$$\{[\mathbb{S}_f] : f \text{ irreducible in } K[t;\sigma]\} = \{[\mathbb{S}_f] : f \text{ irreducible in } K[t;\sigma^{-1}]\}.$$

5.2.5 Quaternion algebras and Cayley-Dickson algebras

In this section we will recall the well-known construction of quaternion algebras and Cayley-Dickson algebras, and show that they can be constructed using skew-polynomial rings.

Definition 5.27. *Let $\mathbb{F}$ be a field with* $\mathrm{char}(\mathbb{F}) \neq 2$*, and let a, b be non-zero elements of $\mathbb{F}$. Define the* quaternion algebra $Q(a,b)_{\mathbb{F}}$ *to be the set of elements of the form*

$$\alpha + \beta i + \gamma j + \delta k$$

for all $\alpha, \beta, \gamma, \delta \in \mathbb{F}$, with multiplication defined by the relations

$$i^2 = a,\ j^2 = b,\ ij = -ji = k.$$

Note that these algebras are sometimes denoted in the literature by $\left(\frac{a,b}{\mathbb{F}}\right)$. These algebras are generalizations of Hamilton's quaternions, $\mathbb{H} = Q(-1,-1)_{\mathbb{R}}$.

If a is a non-square in $\mathbb{F}$, we see that $\mathbb{F}(i) = \mathbb{F}(\sqrt{a})$ is a field extension of $\mathbb{F}$ of degree 2. It is easily seen that there exists an automorphism σ on $\mathbb{F}(i)$ defined by

$$(\alpha + \beta i)^\sigma = \alpha - \beta i.$$

Then we can write elements of $Q(a,b)_{\mathbb{F}}$ in the form

$$\lambda + \mu j,$$

for $\lambda, \mu \in \mathbb{F}(i)$. Then the multiplication is determined by

$$\begin{aligned} j\lambda &= j(\alpha + \beta i) \\ &= \alpha j + \beta j i \\ &= \alpha j - \beta i j \\ &= (\alpha - \beta i) j \\ &= \lambda^\sigma j, \end{aligned}$$

for all $\lambda \in \mathbb{F}$, and $j^2 = b$.

Consider now the skew-polynomial ring $R = \mathbb{F}(i)[t;\sigma]$, and the polynomial $f = t^2 - b$. Constructing the division algebra $\mathbb{S}_f$ as in Section 5.1, we can see that by identifying j with t, these two constructions coincide precisely, and so if σ is the automorphism of $\mathbb{F}(\sqrt{a})$ sending $\sqrt{a}$ to $-\sqrt{a}$ then

$$Q(a,b)_{\mathbb{F}} \simeq \frac{\mathbb{F}(\sqrt{a})[t;\sigma]}{\langle t^2 - b\rangle} = \mathbb{S}_f.$$

Definition 5.28. *Let $\mathbb{F}$ be a field, and $\mathbb{K}$ a separable quadratic field extension of $\mathbb{F}$ with non-trivial Galois automorphism σ. Let b be a non-zero element of $\mathbb{K}$. Define a multiplication on $\mathbb{K} \times \mathbb{K}$ by*

$$(\alpha,\beta)(\gamma,\delta) := (\alpha\gamma + b\delta\beta^{\sigma}, \alpha^{\sigma}\delta + \gamma\beta)$$

for $\alpha,\beta,\gamma,\delta \in \mathbb{K}$. The algebra obtained is called the Cayley-Dickson double *of $\mathbb{K}$ with scalar b, and is denoted by* $\mathrm{Cay}(\mathbb{K}, b)$.

The algebra $\mathrm{Cay}(\mathbb{K}, b)$ is associative if and only if $b \in \mathbb{F}$, as implied by Corollary 5.9. These were originally defined for $b \in \mathbb{F}$, and extended to $b \in \mathbb{K}$ by Dickson [25]. If we take $\mathbb{K} = \mathbb{F}(\sqrt{a})$, then we have

$$\mathrm{Cay}(\mathbb{K}, b) \simeq Q(a,b)_{\mathbb{F}}.$$

Comparing this definition with equation 5.1, we see that the Cayley-Dickson double of a field, and hence the quaternion algebras, are special cases of the construction from skew-polynomial rings.

For the case of Hamilton's quaternions, we have

$$\mathbb{H} = \frac{\mathbb{C}[t;\sigma]}{\langle t^2 + 1\rangle} = \mathbb{S}_{t^2+1},$$

where σ denotes complex conjugation.

It can be shown that if $R = \mathbb{K}[t;\sigma]$ is a skew-polynomial ring, then there exists an anti-automorphism of R if and only if $\sigma^2 = 1$, and all anti-automorphisms are of the form

$$\sum a_k t^k \mapsto \sum a_k^{\sigma^{-k+m}} (\lambda t)^k,$$

where $0 \neq \lambda \in \mathbb{K}$ and $m \in \{0, 1\}$. The proof of this is similar to the proofs of Theorem 5.12 and Lemma 6.1 in the next chapter, and so is omitted here. If f is irreducible in R and lies in the centre of R, then the restriction of this map to $\mathbb{S}_f$ is an anti-automorphism of $\mathbb{S}_f$. Choosing $m = 1$, $\lambda = -1$, we see that we obtain the usual quaternion conjugation: if $a = \alpha + \beta i \in \mathbb{C}$, $b = \gamma + \delta i \in \mathbb{C}$, then

$$\begin{aligned}\overline{(a + bj)} &= a^{\sigma} - bj \\ &= (\alpha + \beta i)^{\sigma} - (\gamma + \delta i)j \\ &= \alpha - \beta i - \gamma j - \delta ij.\end{aligned}$$

Note that the Cayley-Dickson doubling process can also be applied to a division algebra D. This does not, in general, coincide with residue algebras obtained from $D[t; \sigma]$, as the Cayley-Dickson process uses this anti-automorphism above rather than an automorphism, and the order of multiplication of elements of D do not match.

Chapter 6

Isotopy classes of semifields from skew-polynomial rings

In this chapter we will consider the problem of deciding when two semifields $\mathbb{S}_f$ and $\mathbb{S}_g$ are isotopic. We will then apply these results to obtain an improved upper bound on the number of isotopy classes over a finite field.

6.1 Isotopy relations

We begin by considering automorphisms of skew-polynomial rings. The following lemma is not assumed to be new, but a proof is included for lack of convenient reference.

Lemma 6.1. Let ϕ be an automorphism of $R = \mathbb{K}[t;\sigma]$, where σ is not the identity automorphism. Then

$$\phi(f) = f^{\rho}(\alpha t)$$

where $\rho \in \mathrm{Aut}(\mathbb{K})$ and $\alpha \in \mathbb{K}^{\times}$.

Proof. As ϕ is bijective, it preserves the degree of elements of R. Let ρ be the field automorphism obtained by the restriction of ϕ to $\mathbb{K}$, and assume $\phi(t) = \alpha t + \beta$,

$\alpha, \beta \in \mathbb{K}$, $\alpha \neq 0$. Choose $\gamma \in \mathbb{K}$ such that $\gamma^\sigma \neq \gamma$. Computing $\phi(t)\phi(\gamma) = \phi(t\gamma) = \phi(\gamma^\sigma t) = \phi(\gamma^\sigma)\phi(t)$, we see that $\beta = 0$, and the assertion follows.

□

Automorphisms of R can be used to define isomorphisms between semifields.

Theorem 6.2. *Let f be a monic irreducible of degree d in R. Let ϕ be an automorphism of R. Define $g = \phi(f)$. Then $\mathbb{S}_f$ and $\mathbb{S}_g$ are isomorphic, and*

$$\phi(a \circ_f b) = \phi(a) \circ_g \phi(b).$$

Proof. For any $a, b \in R$ of degree less than d, there exist unique $u, v \in R$ such that $\deg(u), \deg(v) < d$ and

$$ab = uf + v.$$

Then $a \circ_f b = v = ab - uf$. As ϕ is an automorphism of R, we have that

$$\phi(a \circ_f b) = \phi(ab - uf) = \phi(a)\phi(b) - \phi(u)\phi(f) = \phi(a) \circ_g \phi(b)$$

as claimed. □

We now consider another type of isotopism between these semifields.

Definition 6.3. *Let f and g be monic irreducibles of degree d in R. We say that f and g are* similar *if there exists a non-zero element u of R of degree less than d such that*

$$gu \equiv 0 \mod f.$$

Theorem 6.4. *Suppose f and g are similar. Then $\mathbb{S}_f$ and $\mathbb{S}_g$ are isotopic, and*

$$(a \circ_g b)^H = a \circ_f b^H$$

where $b^H = b \circ_f u$, $gu \equiv 0 \mod f$.

Proof. Let $a \circ_g b = ab - vg$. Then

$$\begin{aligned} (a \circ_g b)^H &= (ab - vg)^H \\ &= (ab - vg)u \mod f \\ &= (abu - vgu) \mod f \\ &\equiv abu \mod f, \end{aligned}$$

as $gu \equiv 0 \mod f$.

Let $b \circ_f u = bu - wf$. Then

$$\begin{aligned} a \circ_f b^H &= a \circ_f (b \circ_f u) \\ &= a \circ_f (bu - wf) \\ &= a(bu - wf) \mod f \\ &\equiv abu \mod f, \end{aligned}$$

and the result holds. □

In [36] Jacobson investigated when two skew polynomials are similar. In the next section we will include a proof for skew polynomial rings over finite fields for the sake of completeness, and because some of the concepts introduced will be of use later in this chapter for counting isotopy classes.

6.2 Counting isotopy classes for finite semifields

For this section we will assume $\mathbb{K} = \mathbb{F}_{q^n}$, $\mathbb{F} = \mathbb{F}_q$ are finite fields, although some of the concepts introduced remain valid for arbitrary fields.

Let $A(q, n, d)$ denote the number of isotopy classes of semifields of order q^{nd} defined by the skew polynomial ring $\mathbb{F}_{q^n}[t; \sigma]$, with

$$(\#Z, \#N_l, \#N_m, \#N_r) = (q, q^n, q^n, q^d),$$

i.e.

$$A(q, n, d) := |\{[\mathbb{S}_f] : f \text{ irreducible in } \mathbb{F}_{q^n}[t; \sigma], \deg(f) = d\}|.$$

In this section we will apply the isotopy relations outlined in the previous section to obtain a new upper bound for $A(q, n, d)$.

Definition 6.5. *Let $f \in R$ be irreducible of degree d. Define the* minimal central left multiple *of f, denoted by $mzlm(f)$, as the monic polynomial of minimal degree in the centre $Z \simeq \mathbb{F}_q[t^n; \sigma] \simeq \mathbb{F}_q[y]$ that is right-divisible by f.*

In [31] Giesbrecht showed that $mzlm(f)$ exists, is unique, has degree d and is irreducible when viewed as an element of $\mathbb{F}_q[y]$ (the proof of which is included in the next lemma). Note that this is related to the *bound* of f: if t does not divide f, then $R.mzlm(f)$ is the largest two-sided ideal of R contained in the left ideal $R.f$. See for example [37].

Lemma 6.6. Let $f \in R$ be irreducible of degree d. Let $mzlm(f) = \hat{f}(t^n)$ for some $\hat{f} \in \mathbb{F}_q[y]$. Then $\hat{f}$ is irreducible.

Proof. Suppose $\hat{f} = \hat{g}\hat{h}$ for some $\hat{g}, \hat{h} \in \mathbb{F}_q[y]$, with $\deg(\hat{g}) < \deg(\hat{f})$. As f does not divide $\hat{g}(t^n)$, and f is irreducible, we must have that $gcrd(f, \hat{g}(t^n)) = 1$. By Theorem 5.3 (3) R is right-Euclidean, and hence there exist $a, b \in R$ such that

$$af + b\hat{g}(t^n) = 1.$$

Right multiplying by $\hat{h}(t^n)$, we get $af\hat{h}(t^n) + b\hat{g}(t^n)\hat{h}(t^n) = \hat{h}(t^n)$. But as $\hat{h}(t^n)$ commutes with f, and as f divides $\hat{f}(t^n) = \hat{g}(t^n)\hat{h}(t^n)$, there exists some $c \in R$ such that

$$a\hat{h}(t^n)f + bcf = (a\hat{h}(t^n) + bc)f = \hat{h}(t^n).$$

But then f divides $\hat{h}(t^n)$, and by definition of minimal central left multiple, we must have $\deg(\hat{h}) = \deg(\hat{f})$, and so $\hat{f}$ is irreducible in $\mathbb{F}_q[y]$. □

Lemma 6.7. Let h be an element of R such that $h = \hat{h}(t^n)$, where $\hat{h} \in \mathbb{F}_q[y]$ is monic, irreducible and has degree d in y and $\hat{h} \neq y$. Then

(1)
$$\frac{R}{Rh} \simeq M_n(\mathbb{F}_{q^d});$$

(2) any irreducible divisor f of $h = \hat{h}(t^n)$ has degree d;

(3) if A denotes the isomorphism of part (1), and f is an irreducible (right) divisor of h, then the matrix $A(f + Rh)$ has rank $n - 1$.

By abuse of notation we will write $A(a) = A(a + Rh)$ for $a \in R$.

Proof. (1) First we show that Rh is a maximal two-sided ideal in R. For suppose there exists some $g \in R$ such that Rg is a two-sided ideal, $\deg(g) < \deg(h)$ and

$Rh \subset Rg$. Then

$$g = \hat{g}(t^n)t^s$$

for some $\hat{g} \in \mathbb{F}_q[y]$ (see for example [38] Theorem 1.2.22). As t does not divide h, we must have that $s = 0$, and

$$h = ag$$

for some $a \in R$. As h and g are in the centre of R, a must also be in the centre of R, and so $a = \hat{a}(t^n)$ for some $\hat{a} \in \mathbb{F}_q[y]$. But then

$$\hat{h}(y) = \hat{a}(y)\hat{g}(y)$$

As $\hat{h}$ is irreducible in $\mathbb{F}_q[y]$, we must have $\hat{g} \in \mathbb{F}_q$, and so $g \in \mathbb{F}_q$. Therefore $Rg = R$, proving that Rh is maximal.

It follows that $\frac{R}{Rh}$ is a finite simple algebra and hence isomorphic to a full matrix algebra over its centre ([49] Chapter 17). It is easily shown (see for example [31], proof of Theorem 4.3) that the centre $Z\left(\frac{R}{Rh}\right)$ is the image of the centre of R, and is given by

$$Z\left(\frac{R}{Rh}\right) = \frac{Z(R) + Rh}{Rh} \simeq \frac{\mathbb{F}_q[y]}{\mathbb{F}_q[y]\hat{h}(y)} \simeq \mathbb{F}_{q^d}$$

as $\hat{h}$ is a degree d irreducible in $\mathbb{F}_q[y]$.

As the dimension of $\frac{R}{Rh}$ as a vector space over $\mathbb{F}_q$ is n^2d, we see that

$$\frac{R}{Rh} \simeq M_n(\mathbb{F}_{q^d})$$

as claimed.

(2) Let f be an irreducible divisor of h, and let $r = \deg(f)$. Then f generates a maximal left ideal in R, and also in $\frac{R}{Rh}$. This maximal left ideal $\left(\frac{R}{Rh}\right) f$ is then $(n^2d - nr)$-dimensional over $\mathbb{F}_q$.

By part (1), we know that $\frac{R}{Rh}$ is isomorphic to $M := M_n(\mathbb{F}_{q^d})$. It is well known that maximal left ideals in M are all of the form $Ann_M(U)$ for some 1-dimensional space $U < (\mathbb{F}_{q^d})^n$, and are $(n^2 - n)$-dimensional over $\mathbb{F}_{q^d}$, and hence $(n^2 - n)d$-dimensional over $\mathbb{F}_q$. Therefore $r = d$, as claimed.

(3) The left ideal $M.A(f)$ is equal to $Ann_M(Ker(A(f)))$, and so $A(f)$ has rank $n-1$ as claimed. □

Remark 6.8. The number of monic irreducible elements of degree d in R can be seen to be

$$N(q,d)\left(\frac{q^{nd}-1}{q^d-1}\right).$$

This was calculated by Odoni [58], and is an upper bound for $A(q,n,d)$. However, we will see that this is far from optimal.

We can now calculate the size of the eigenring, and hence the right nucleus of $\mathbb{S}_f$.

Lemma 6.9. If $f \in R$ is irreducible of degree d, then $|E(f)| = q^d$.

Proof. Let u have degree less than nd, and let $u = af + u'$ for $\deg(u') < f$. Then $fu \equiv 0 \mod f$ if and only if $u' \in E(f)$, as

$$fu = f(af+u') \equiv fu' \mod f.$$

Let $h = mzlm(f)$.

Let E' be the set of all $u+Rh \in R/Rh$ such that $(f+Rh)(u+Rh) = (v+Rh)(f+Rh)$ for some $v + Rh \in R/Rh$. Then $u + Rh \in E'$ if and only if there exists some $v \in R$ such that $fu+Rh = vf+Rh$, which occurs if and only if there exists $v \in R$ such that $fu \equiv vf \mod h$. But then as f divides h, we have $fu \equiv vf \mod f \equiv 0 \mod f$. Hence we have that

$$\begin{aligned} E' &= \{(af+u') + Rh : a \in R, \deg(a) < d(n-1), u' \in E(f)\} \\ &= \frac{(E(f)+Rf)+Rh}{Rh}. \end{aligned}$$

Hence we have that $|E'| = q^{dn(n-1)}|E(f)|$.

By part (1) of Lemma 6.7, $\frac{R}{Rh} \simeq M_n(\mathbb{F}_{q^d}) = M$. If A denotes this isomorphism, then by part (3) of Lemma 6.7, $A(f) := A(f+Rh)$ has rank $n-1$. Let $Ker(A(f)) =< v >$ for $0 \neq v \in (\mathbb{F}_{q^d})^n$. Then

$$u + Rh \in E' \Leftrightarrow A(f)A(u) \in M.A(f) \Leftrightarrow A(u)v = \lambda v$$

for some $\lambda \in \mathbb{F}_{q^d}$. Then $A(u) - \lambda I \in Ann_M(v)$, and so

$$|E'| = q^d|Ann_M(v)| = q^{d(n^2-n+1)}.$$

Hence from the two expressions for $|E'|$ we get $|E(f)| = q^d$, as claimed.

□

Remark 6.10. We see that

$$E(f) = \{z \mod f \ : \ z \in Z(R)\}$$

i.e. $E(f)$ consists of the remainders of all central elements on right division by f.

The parameters of the semifield $\mathbb{S}_f$ now easily follow from Theorem 5.10, Theorem 5.8 and Lemma 6.9.

Theorem 6.11. *If $f \in R$ is irreducible of degree d, then the semifield $\mathbb{S}_f$ has parameters*

$$(\#Z, \#\mathbb{N}_l, \#\mathbb{N}_m, \#\mathbb{N}_r) = (q, q^n, q^n, q^d).$$

The following theorem tells us exactly when two irreducibles are similar.

Theorem 6.12. *Let f and g are irreducible in R. Then $mzlm(g) = mzlm(f)$ if and only if f and g are similar.*

Proof. Suppose first that $mzlm(g) = mzlm(f)$. Let h denote $mzlm(f)$, and write $h = af$. Then $\frac{R}{Rh} \simeq M_n(\mathbb{F}_{q^d})$. As above, let A denote this isomorphism. By Lemma 6.7,

$$\text{rank}(A(f)) = \text{rank}(A(g))(= n-1),$$

and the equality of ranks shows there exist invertible matrices $A(u), A(v)$ such that $A(u)A(f) = A(g)A(v)$. Then $uf \equiv gv \mod h$, so there exists some b such that

$$gv = uf + bh = uf + baf = (u + ba)f.$$

We can write $v = v' + cf$, where $\deg(v') < d$ and $v' \neq 0$ (for otherwise, $v = cf$, and so v has non-trivial common divisor with h, so $A(v)$ is not invertible). Then

$$g(v' + cf) = (u + ba)f$$

$$\Rightarrow gv' = (u + ba - gc)f \Rightarrow gv' = u'f$$

and g and f are similar, as claimed.

Suppose now that f and g are similar. By definition, $gu = vf$ for some u, v of degree less than d. It can be shown that

$$mzlm(ab) = mzlm(a)mzlm(b)$$

if $gcrd(a, b) = 1$. See for example [31]. Hence

$$mzlm(v)mzlm(f) = mzlm(g)mzlm(v),$$

and as $mzlm(f)$ and $mzlm(g)$ are irreducible in $\mathbb{F}_q[y]$, by uniqueness of factorization in $\mathbb{F}_q[y]$ the result follows. □

Hence the number of isotopy classes is upper bounded by the number of irreducible polynomials of degree d in $\mathbb{F}_q[y]$. This was proved in a different way by Dempwolff [19]. The next theorem allows us to further improve this bound.

Definition 6.13. *Consider the group*

$$G = \Gamma\mathrm{L}(1, q) = \{(\lambda, \rho) \mid \lambda \in \mathbb{F}_q^\times, \rho \in \mathrm{Aut}(\mathbb{F}_q)\}.$$

Define an action of G on $I(q, d)$ by

$$f^{(\lambda,\rho)}(y) = \lambda^{-d} f^\rho(\lambda y).$$

Theorem 6.14. *Let $f, g \in R$ be irreducibles of degree d, with $mzlm(f) = \hat{f}(t^n)$, $mzlm(g) = \hat{g}(t^n)$ for $\hat{f}, \hat{g} \in \mathbb{F}_q[y]$. If*

$$\hat{g} = \hat{f}^{(\lambda,\rho)}$$

for some $\lambda \in \mathbb{F}_q^\times$, $\rho \in \mathrm{Aut}(\mathbb{F}_q)$, then $\mathbb{S}_f$ and $\mathbb{S}_g$ are isotopic.

Proof. Choose some $\alpha \in \mathbb{F}_{q^n}$ such that

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \lambda.$$

Then

$$(\alpha t)^n = \alpha\alpha^\sigma \dots \alpha^{\sigma^{n-1}} t^n = \lambda t^n.$$

Define

$$h(t) = f^\rho(\alpha t).$$

By Theorem 6.2, $\mathbb{S}_f$ and $\mathbb{S}_h$ are isomorphic. Let $mzlm(h) = \hat{h}(t^n)$.

Let ϕ be the automorphism of R defined by $\phi(a) = a^\rho(\alpha t)$. Then as $\phi(f) = h$ and $\hat{f}(t^n) = uf$ for some $u \in R$,

$$\phi(\hat{f}(t^n)) = \phi(u)\phi(f) = \phi(u)h.$$

But

$$\phi(\hat{f}(t^n)) = \hat{f}^\rho((\alpha t)^n) = \hat{f}^\rho(\lambda t^n).$$

As this is in the centre of R, and is divisible by h, we must have that $\hat{h}(y)$ divides $\hat{f}^\rho(\lambda t^n)$, and so, as their degrees are equal and both are monic,

$$\hat{h}(y) = \lambda^{-d}\hat{f}^\rho(\lambda y) = \hat{g}(y).$$

By Theorem 6.4, as h and g have the same minimal central left multiple, $\mathbb{S}_g$ and $\mathbb{S}_h$ are isotopic, and hence $\mathbb{S}_f$ and $\mathbb{S}_g$ are isotopic, as claimed. □

Hence the number of isotopy classes is upper bounded as follows.

Theorem 6.15. *The number of isotopism classes of semifields $\mathbb{S}_f$ of order q^{nd} obtained from $\mathbb{F}_{q^n}[t;\sigma]$ is less than or equal to the number of G-orbits on the set of monic irreducible polynomials of degree d in $\mathbb{F}_q[y]$.*

Proof. Suppose f and g are two monic irreducible polynomials in $\mathbb{F}_{q^n}[t;\sigma]$ of degree d, with $mzlm(f) = \hat{f}(t^n)$, $mzlm(g) = \hat{g}(t^n)$ for $\hat{f}, \hat{g} \in \mathbb{F}_q[y]$. Then by [31], $\hat{f}$ and $\hat{g}$ are monic irreducible of degree d in $\mathbb{F}_q[y]$. Moreover, if $\hat{f}^G = \hat{g}^G$, then by Theorem 6.14, $\mathbb{S}_f$ and $\mathbb{S}_g$ are isotopic. □

6.2.1 Comparison with existing bounds

We saw in Section 5.2.4 that these semifields are isotopic to so-called *cyclic semifields* as defined by Johnson and Jha [40]. Here we note the existing bounds on the number of isotopy classes, and compare our new bound to these.

Let $N(q,d) = \#I(q,d)$, where $I(q,d)$ is the set of monic irreducibles of degree d in $\mathbb{F}_q[y]$. This number is well known ([54], Theorem 3.25) and equal to

$$\sum_{s|d} \mu(s) q^{d/s},$$

where μ denotes the Moebius function.

Recall that $A(q,n,d)$ denotes the number of isotopy classes of semifields of order q^{nd} defined by the skew polynomial ring $\mathbb{F}_{q^n}[t;\sigma]$.

In [41], the authors consider cyclic semifields two-dimensional over their left nucleus, with right and middle nuclei isomorphic to $\mathbb{F}_{q^2}$. The above defines the opposite semifield to those in this paper. Hence they are considering semifields $\mathbb{S}_f$, where $f \in \mathbb{F}_{q^2}[t;\sigma]$ is an irreducible of degree d (denoted by n in their paper). They prove the lower bound

$$A(q,2,d) \geq \frac{N(q,d)}{2hq(q-1)}$$

where $q = p^h$.

In [44], the authors obtain an upper bound

$$A(q,n,d) \leq q^d - 1.$$

They also obtained an upper bound for the total number of isotopy classes of semifields of order q^{nd} obtained from semilinear transformations of order q^{nd}:

$$ndq^{nd/2}\log_2(q).$$

As we will see in the next section, a result of Dempwolff [19] leads to the upper bound:

$$A(q,n,d) \leq N(q,d).$$

Following from (Theorem 6.15) we have the new upper bound:

$$A(q,n,d) \leq M(q,d),$$

where $M(q,d)$ denotes the number of orbits in $I(q,d)$ under the action of G defined in Definition 6.13.

Note that if $q = p^h$ for p prime, then $|G| = h(q-1)$, and so

$$\frac{N(q,d)}{h(q-1)} \leq M(q,d) \leq N(q,d) < q^d - 1.$$

Example: For $q = \{2,3,4,5\}$, $n = d = 2$, the upper bounds $M(q,d) = \{1,2,1,3\}$ are tight by computer calculation. This was checked using the computer package

MAGMA. For each irreducible polynomial F_i of degree 2 in $\mathbb{F}_q[y]$, the element $F_i(t^2)$ of $\mathbb{F}_{q^2}[t;\sigma]$ was formed, and a divisor f_i of degree 2 in $\mathbb{F}_{q^2}[t;\sigma]$ was calculated. From this, the subspace of endomorphisms of left multiplication $L_{\mathbb{S}_{f_i}}$ was calculated and represented as a subspace of $M_4(\mathbb{F}_q)$. These were then tested pairwise for equivalence (in the sense of Section 1.1.3), and the above results were returned.

Example: If q is prime, and $(q-1,d)=1$, then $M(q,d)=\frac{N(q,d)}{q-1}$.

Remark 6.16. It is likely that a closed formula for $M(q,d)$, similar to that for $N(q,d)$, exists. However, we have not been able to obtain such a formula at the time of this writing.

Remark 6.17. To produce a specific example of every isotopy class of cyclic semifields, it suffices to find representatives $\hat{f}_i$ of each G-orbit of $I(q,d)$. We form the skew-polynomials $\hat{f}_i(t^n)$, and calculate a particular irreducible divisor f_i of each, using for example the algorithm of Giesbrecht [31]. Then the semifields $\mathbb{S}_{f_i}$ are representatives of each isotopy class.

Remark 6.18. As noted in Remark 5.14, the semifields obtained from irreducibles in $\mathbb{F}_{q^n}[t;\sigma]$ and $\mathbb{F}_{q^n}[t;\sigma^{-1}]$ are isotopic. Hence the total number of isotopy classes defined by degree d irreducibles in $\mathbb{F}_{q^n}[t;\sigma]$ for all σ fixing precisely $\mathbb{F}_q$ is upper bounded by $\frac{\phi(n)}{2}M(q,d)$, when $n \neq 2$, where ϕ is Euler's totient function.

6.2.2 Application to conjugacy classes of irreducible semilinear transformations

In this section we will apply the above work to obtain a new proof of a theorem of Dempwolff.

Theorem 6.19. *Let f and g be two monic irreducibles of degree d in $R=\mathbb{K}[t;\sigma]$. Then*

1. *$L_{t,f}$ and $L_{t,g}$ are $\mathrm{GL}(d,\mathbb{K})$-conjugate if and only if f and g are similar;*

2. *$L_{t,f}$ and $L_{t,g}$ are $\Gamma\mathrm{L}(d,\mathbb{K})$-conjugate if and only if f and g^ρ are similar for some $\rho \in \mathrm{Aut}(\mathbb{K})$.*

Proof. Suppose $L_{t,f}\phi = \phi L_{t,g}$ for some $\phi \in \Gamma\mathrm{L}(d,\mathbb{K})$, where ϕ has automorphism ρ. Let $\phi(1) = u$. Then

$$\phi(t^i) = \phi(L_{t,g}^i(1)) = L_{t,f}^i\phi(1) = L_{t,f}^i(u) = t^i u \mod f$$

for all $i = 0, 1, \dots, d-1$. Now, with $g = t^d - \sum_{i=0}^{d-1} g_i t^i$, we have

$$\begin{aligned}\phi L_{t,g}(t^{d-1}) &= \phi(t^d \mod g)\\ &= \phi\left(\sum_{i=0}^{d-1} g_i t^i\right) = \sum_{i=0}^{d-1} g_i^\rho \phi(t^i)\\ &= \sum_{i=0}^{d-1} g_i^\rho (t^i u \mod f) = \left(\sum_{i=0}^{d-1} g_i^\rho t^i\right) u \mod f\\ &= (t^d - g^\rho)u \mod f.\end{aligned}$$

But as $L_{t,f}\phi = \phi L_{t,g}$, this is equal to

$$L_{t,f}\phi(t^{d-1}) = L_{t,f}(t^{d-1}u \mod f).$$

Let $t^{d-1}u = af + b$ where $\deg(b) < d$. Then

$$L_{t,f}(t^{d-1}u \mod f) = L_{t,f}(t^{d-1}u - af)$$

$$= (t^d u - taf) \mod f = t^d u \mod f.$$

Hence

$$(t^d - g^\rho)u \equiv t^d u \mod f$$

and so

$$g^\rho u = 0 \mod f$$

i.e. f and g^ρ are similar. If $\phi \in \mathrm{GL}(n,\mathbb{K})$, then ρ is the identity automorphism, and so f and g are similar. □

This provides an alternate proof of the following result proved by Dempwolff ([19], Theorem 2.10).

Corollary 6.20. Let T and U be two irreducible elements of $\Gamma\mathrm{L}(d,\mathbb{F}_{q^n})$, where the accompanying automorphism σ of both T and U is a generator of $Gal(\mathbb{F}_{q^n},\mathbb{F}_q)$. Then

(1) T and U are $\mathrm{GL}(d,\mathbb{F}_{q^n})$-conjugate if and only if T^n and U^n have the same minimal polynomial over $\mathbb{F}_q$;

(2) T and U are $\Gamma\mathrm{L}(d,\mathbb{F}_{q^n})$-conjugate if and only if the minimal polynomials of T^n and U^n over $\mathbb{F}_q$ are $\mathrm{Aut}(\mathbb{F}_q)$ conjugate.

Proof. (1) By Theorem 5.25, we may assume T is $\mathrm{GL}(d,\mathbb{F}_{q^n})$-conjugate to $L_{t,f}$, U is $\mathrm{GL}(d,\mathbb{F}_{q^n})$-conjugate to $L_{t,g}$, for some $f,g\in R$ irreducibles of degree d. Let $mzlm(f)=\hat{f}(t^n)$ for $\hat{f}\in\mathbb{F}_q[y]$, and suppose $\hat{f}(t^n)=af$. As σ has order n, T^n and U^n are $\mathbb{F}_{q^n}$-linear. We claim that $\hat{f}$ is the minimal polynomial of $L_{t,f}^n$ over $\mathbb{F}_q$, and hence the minimal polynomial of T^n over $\mathbb{F}_q$. For any v,

$$\hat{f}(L_{t,f}^n)v=\hat{f}(t^n)v \mod f$$

$$=v\hat{f}(t^n) \mod f = vaf \mod f = 0.$$

Hence $\hat{f}(L_{t,f}^n)=0$. Suppose now $\hat{h}(L_{t,f}^n)=0$ for some $\hat{h}\in\mathbb{F}_q[y]$. Then

$$\hat{h}(L_{t,f}^n)(1)=\hat{h}(t^n) \mod f = 0.$$

But then f divides $\hat{h}(t^n)$, and $\hat{h}(t^n)$ is in the centre of R, so $\hat{f}$ divides $\hat{h}$. Therefore $\hat{f}$ is the minimal polynomial of $L_{t,f}^n$ (and hence T^n) over $\mathbb{F}_q$ as claimed.

Similarly, if $mzlm(g)=\hat{g}(t^n)$, then $\hat{g}$ is the minimal polynomial of $L_{t,g}^n$, and U^n, over $\mathbb{F}_q$.

By Theorem 6.19, $L_{t,f}$ and $L_{t,g}$ are $\mathrm{GL}(d,\mathbb{F}_{q^n})$-conjugate if and only if $mzlm(f)=mzlm(g)$. Hence T and U are $\mathrm{GL}(d,\mathbb{F}_{q^n})$-conjugate if and only if T^n and U^n have the same minimal polynomial over $\mathbb{F}_q$.

(2) Similarly, T and U are $\Gamma\mathrm{L}(d,\mathbb{F}_{q^n})$ conjugate if and only if $\hat{f}=\hat{g}^\rho$ for some $\rho\in\mathrm{Aut}(\mathbb{F}_q)$, i.e. if and only if the minimal polynomials T^n and U^n over $\mathbb{F}_q$ are $\mathrm{Aut}(\mathbb{F}_q)$ conjugate. □

As we know that these minimal polynomials are irreducible and have degree d in $\mathbb{F}_q[y]$, this result of Dempwolff implies:

The number of conjugacy classes of irreducible elements of $\Gamma\mathrm{L}(d,\mathbb{F}_{q^n})$ *with automorphism σ is precisely $\#I(q,d)$.*

Hence we have

$$A(q,n,d) \leq N(q,d) = \#I(q,d).$$

As we have seen in the previous section, we have improved this bound to

$$A(q,n,d) \leq M(q,d) = \#I(q,d)^G.$$

Bibliography

[1] Albert, A. A.; *On nonassociative division algebras*, Trans. Amer. Math. Soc. **72** (1952) 296-309.

[2] Albert, A.A.; *Generalized twisted fields*, Pacific J. Math. **11** (1961) 1-8.

[3] Albert, A. A.; *Finite division algebras and finite planes*, Proc. Sympos. Appl. Math. **10** (1960) 53-70.

[4] Ball, S.; Lavrauw, M.; *On the Hughes-Kleinfeld and Knuth's semifields two-dimensional over a weak nucleus*, Des. Codes Cryptogr. **44** (2007) 63-67.

[5] Beasley, L.B.; Laffey, T.J.; *Linear operators on matrices: the invariance of rank-k matrices*, Linear Algebra Appl. **133** (1990) 175-184. Erratum, Linear Algebra Appl. **180** (1993) 2.

[6] Beasley, L.B.; *Spaces of rank-2 matrices over GF(2)*, Electron. J. Algebra **20** (1999) 11-18.

[7] Boston, N.; *Spaces of constant rank matrices over GF(2)*, Electron. J. Algebra **20** (2010) 1-5.

[8] Bott, R,; Milnor, J.; *On the parallelizability of the spheres*, Bull. Amer. Math. Soc. **64** (1958) 87-89.

[9] Cafure, A.; Matera, G.; *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), 155-185.

[10] Calderbank, R.; Kantor, W.M.; *The geometry of two-weight codes*, Bull. London Math. Soc. **18** (1986), 97-122.

[11] Carlitz, L.; *A theorem of Dickson on nonvanishing cubic forms in a finite field*, Proc. Amer. Math. Soc. **8** (1957), 975-977.

[12] Causin, A.; Pirola, G.P.; *A note on spaces of symmetric matrices*, Linear Algebra Appl. **426** (2007) 533-539.

[13] Cordero, M.; Jha, V.; *On the Multiplicative Structure of Quasifields and Semifields: Cyclic and Acyclic Loops*, Note Mat. **29** (2009) 45-59.

[14] de Boer, M. A.; *Codes spanned by quadratic and Hermitian forms*, IEEE Trans. Inform. Theory **42** (1996) 1600-1604.

[15] Delsarte, P.; *Weights of linear codes and strongly regular normed spaces*, Discrete Math. **3** (1972) 47-64.

[16] Delsarte, P.; *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A **25** (1978) 226-241.

[17] Dembowski, P.; *Finite Geometries*, Springer, 1968.

[18] Dembowski, P.; Ostrom, T.G.; *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968) 239-258.

[19] Dempwolff, U.; *On irreducible semilinear transformations*, Forum Math. **22** (2010), 1193-1206.

[20] Dempwolff, U.; *Autotopism groups of cyclic semifield planes*, to appear in J. Algebraic Combin.

[21] Dempwolff, U.: *Semifield planes of order 81*, J. Geom. **89** (2008), 1-16.

[22] Dickson, L. E.; *On finite algebras*, Nachrichten der Gesellschaften der Wissenschaften zu Göttingen (1905) 358-393.

[23] Dickson, L.E.; *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc. **7** (1906) 514-522.

[24] Dickson, L.E.; *On triple algebras and ternary cubic forms*, Bull. Amer. Math. Soc. **14** (1907-1908), 160-169.

[25] Dickson, L. E.; *Linear algebras with associativity not assumed*, Duke Math. J. **1** (1935) 113-125.

[26] Dumas, J.-G.; Gow, R.; McGuire, G.; Sheekey, J.; *Subspaces of matrices with special rank properties*, Linear Algebra Appl. **433** (2010), 191-202.

[27] Fitzgerald, R. W.; Yucas, J. L.; *Pencils of quadratic forms over finite fields*, Discrete Math. **283** (2004), 71-79.

[28] Gabidulin, E. M.; *Theory of codes with maximum rank distance*, Probl. Inf. Transm. **21** (1985) 1-12.

[29] Gabidulin, E. M.; Pilipchuk, N. I.; *Symmetric rank codes*, translation in Probl. Inf. Transm. **40** (2004) 103-117.

[30] Ghorpade, S.R.; Lachaud, G.; *Étale cohomology, Lefschetz theorems and the number of points of singular varieties over finite fields*, Mosc. Math. J. **2** (2002), 589-631.

[31] Giesbrecht, Mark: *Factoring in skew-polynomial rings over finite fields*, J. Symbolic Comput. **26** (1998) 463-486.

[32] Goethals, J-M.; *Nonlinear codes defined by quadratic forms over GF(2)*, Information and Control **31** (1976) 43-74.

[33] Hentzel, I.R.; Rúa, I.F.; *Primitivity of finite semifields with 64 and 81 elements*, Internat. J. Algebra Comput. **17** (2007), 1411-1429.

[34] Ilic, B.; Landsberg, J.M.; *On symmetric degeneracy loci, spaces of matrices of constant rank and dual varieties*, Math. Ann. **314** (1999), 159-174.

[35] Jacobson, N.; *Non-commutative polynomials and cyclic algebras.* Ann. of Math. (2) **35** (1934) 197-208.

[36] Jacobson, N.; *Pseudo-linear transformations*, Ann. of Math. (2) **38** (1937), no. 2, 484–507.

[37] Jacobson, N.; *The Theory of Rings*, American Math. Soc. (1943).

[38] Jacobson, N.; *Finite-dimensional division algebras over fields*, Springer (1996).

[39] Jha, V.; Johnson, N. L.; *The centre of a finite semifield plane is a geometric invariant*, Arch. Math. **50** (1988) 93-96.

[40] Jha, V.; Johnson, N. L.; *An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem*, Algebras Groups Geom. **6** (1989) 1-35.

[41] Johnson, N. L.; Marino, G.; Polverino, O.; Trombetti, R.; *On a generalization of cyclic semifields*, J. Algebraic Combin. **29** (2009) 1-34.

[42] Kantor, W.M.; *Commutative semifields and symplectic spreads*, J. Algebra **270** (2003) 96-114.

[43] Kantor, W.M.; *Finite semifields*, Finite geometries, groups, and computation, de Gruyter, Berlin (2006), 103-114,

[44] Kantor, W. M.; Liebler, R.A.; *Semifields arising from irreducible semilinear transformations*, J. Aust. Math. Soc. **85** (2008) 333-339.

[45] Kervaire, M.A.; *Non-parallelizability of the n-sphere for $n > 7$*, Proc. Nat. Acad. Sci. USA **44** (1958) 280-283.

[46] Knuth, D.E.; *Finite semifields and projective planes*, J. Algebra **2** (1965), 182-217.

[47] Knuth, D. E.; *A class of projective planes*, Trans. Amer. Math. Soc. **115** (1965) 541-549.

[48] Lam, K.Y.; Yiu, P.; *Linear spaces of real matrices of constant rank*, Linear Algebra Appl. **195** (1993) 6979.

[49] Lang, S.; *Algebra*, third ed., Addison-Wesley, Reading, Mass (1993).

[50] Lang, S.; Weil, A.; *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819-827.

[51] Lavrauw, M.; *Scattered spaces with respect to spreads, and eggs in finite projective spaces.* Ph.D Thesis.

[52] Lavrauw, M.; *Finite semifields and nonsingular tensors*, Des. Codes Cryptogr., to appear.

[53] Lavrauw, M.; Polverino, O.; *Finite Semifields.* Chapter to appear in *Current research topics in Galois geometries.* Nova Academic Publishers (J. De Beule and L. Storme, Eds.).

[54] Lidl, R.; Niederreiter, H.; *Finite Fields*, Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, Mass. (1983).

[55] Maduram, D. M.; *Transposed translation planes*, Proc. Amer. Math. Soc. **53** (1975) 265-270.

[56] Menichetti, G.; *n-dimensional division algebras over a field with a cyclic extension of degree n*, Geom. Dedicata **63** (1996), 69-94

[57] Meshulam, R.; *On k-spaces of real matrices*, Linear and Multilinear Algebra **26** (1990) 3941.

[58] Odoni, R. W. K.; *On additive polynomials over a finite field.* Proc. Edinburgh Math. Soc. (2) **42** (1999) 1-16.

[59] Oggier, F.; *Cyclic algebras for noncoherent differential space-time coding*, IEEE Trans. Inform. Theory **53** (2007) 3053-3065.

[60] Ore, O.; *Formale Theorie der linearen Differentialgleichungen II*, Jour. für Math. **168** (1932) 233-252

[61] Ore, O.; *Theory of non-commutative polynomials.* Ann. of Math. (2) **34** (1933), 480-508.

[62] Ore, O.; *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559-584.

[63] Petit, J-C.; *Sur certains quasi-corps généralisant un type d'anneau-quotient*, Séminaire Dubriel. Algèbre et théorie des nombres **20** (1966-1967), 1-18.

[64] Rúa, I.F.; *Primitive and non primitive finite semifields*, Comm. Algebra **32** (2004), 793-803

[65] Rúa, I.F.; Combarro, E.F.; Ranilla, J.; *Classification of semifields of order 64*, J. Algebra **322** (2009) 4011-4029.

[66] Rúa, I.F.; Combarro, E.F.; Ranilla, J.; *New advances in the computational exploration of semifields*, Int. J. Comput. Math. **88** (2011) 1990-2000.

[67] Rúa, I.F.; Combarro, E.F.; Ranilla, J.; *Determination of division algebras with 243 elements*, arXiv:1010.0228v1.

[68] Sandler, R.; *Autotopism groups of some finite non-associative algebras*, Amer. J. Math. **84** (1962) 239-264.

[69] Roth, R. M.; *Maximum-rank array codes and their application to crisscross error correction*, IEEE Trans. Info. Theory **37** (1991) 328-336.

[70] Taylor, D. E.; *The geometry of the classical groups*, Heldermann Verlag, Berlin, 1992.

[71] Waterhouse, W. C.; *Pairs of quadratic forms*, Invent. Math. **37** (1976) 157-164.

[72] Wedderburn, J. H. M.; *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905) 349-352.

[73] Wene, G.P.; *On the multiplicative structure of finite division rings*, Aequationes Math. **41** (1991) 222-233.

[74] Westwick, R.; *Spaces of matrices of fixed rank.* Linear and Multilinear Algebra **20** (1987) 171-174.

[75] Westwick, R.; *Spaces of matrices of fixed rank. II*, Linear Algebra Appl. **235** (1996) 163-169