Ahead of Print
DOI 10.1515/advgeom-2013-0003

Advances in Geometry

Semifields from skew polynomial rings

Michel Lavrauw and John Sheekey*

(Communicated by W. M. Kantor)

Abstract. Skew polynomial rings are used to construct finite semifields, following from a construction of Ore and Jacobson of associative division algebras. Johnson and Jha [10] constructed the so-called *cyclic* semifields, obtained using irreducible semilinear transformations. In this work we show that these two constructions in fact lead to isotopic semifields, show how the skew polynomial construction can be used to calculate the nuclei more easily, and provide an upper bound for the number of isotopism classes, improving the bounds obtained by Kantor and Liebler in [13] and implicitly by Dempwolff in [2].

1 Introduction

A *semifield* is a division algebra, where multiplication is not necessarily associative. Finite nonassociative semifields of order q are known to exist for each prime power $q = p^n > 8$, p prime, with $n > 2$. The study of semifields was initiated by Dickson in [4] and by now many constructions of semifields are known. We refer to the next section for more details.

In 1933, Ore [19] introduced the concept of *skew-polynomial rings* $R = K[t;\sigma]$, where K is a field, t an indeterminate, and σ an automorphism of K. These rings are associative, non-commutative, and are left- and right-Euclidean. Ore ([18], see also Jacobson [6]) noted that multiplication in R, modulo right division by an irreducible f contained in the centre of R, yields associative algebras without zero divisors. These algebras were called *cyclic algebras*. We show that the requirement of obtaining an associative algebra can be dropped, and this construction leads to nonassociative division algebras, i.e. semifields. Subsequent to the writing of this paper, it was brought to the authors' attention that this was noted by Petit [20] in 1966 (see also Wene [21]).

In 1989, Jha and Johnson [10] gave a construction for semifields, using irreducible *semilinear transformations*. These semifields were called *cyclic semifields*.

*The first author acknowledges the support of the Fund for Scientific Research – Flanders (FWO). The second author was supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

In this work we show that the constructions from [10] and [20] lead to isotopic semifields. This is Theorem 15 and Theorem 16 and can be formulated as follows.

Theorem 1. *Each cyclic semifield is isotopic to a semifield constructed as a quotient in a skew polynomial ring, and conversely, each semifield constructed as a quotient in a skew polynomial ring is isotopic to a cyclic semifield.*

We also investigate the number of isotopism classes of semifields of order q^{nd}, obtained from an irreducible f of degree d in the skew polynomial ring $R = \mathbb{F}_{q^n}[t;\sigma]$, where $\mathrm{Fix}(\sigma) = \mathbb{F}_q$. We denote this number by $A(q,n,d)$.

In [13] Kantor and Liebler provided an upper bound for the number of isotopism classes of semifields arising from semilinear transformations. This bound has recently been improved (implicitly) by Dempwolff in [2]. We further improve on this bound by proving an upper bound for $A(q,n,d)$.

We conclude the introduction with the statement of this bound. Let

$$I(q,d) := \{f \in \mathbb{F}_q[y] \mid f \text{ monic, irreducible, degree } d\},$$

and let G be the semidirect product of $\mathbb{F}_q^\times$ and $\mathrm{Aut}(\mathbb{F}_q)$, and define the action of G on $I(q,d)$ in the following way

$$f(y)^{(\lambda,\rho)} := \lambda^{-d} f^\rho(\lambda y)$$

where $\lambda \in \mathbb{F}_q^\times$, $\rho \in \mathrm{Aut}(\mathbb{F}_q)$. If $q = p^h$ for p prime, G has order $h(q-1)$. We will prove the following theorem.

Theorem 2. *The number of isotopism classes of semifields of order q^{nd} obtained from $\mathbb{F}_{q^n}[t;\sigma]$ is less or equal to the number of G-orbits on $I(q,d)$.*

We denote this number of orbits by $M(q,d)$. This number lies in the interval

$$\frac{q^d-\theta}{hd(q-1)} \leq M(q,d) \leq \frac{q^d-\theta}{d},$$

where θ denotes the number of elements of $\mathbb{F}_{q^d}$ contained in a subfield $\mathbb{F}_{q^e}$ for $e|d$, and $q = p^h$, where p is prime.

2 Finite semifields

In this section we collect the terminology of the theory of finite semifields, used in the remainder of the paper. For more details on the subject we refer to [14], [12] and [16]. A *finite semifield* $\mathbb{S}$ is a finite algebra with at least two elements, and two binary operations $+$ and $\circ$, satisfying the following axioms.

(S1) $(\mathbb{S},+)$ is a group with neutral 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) $\exists 1 \in \mathbb{S}$ such that $1 \circ x = x \circ 1 = x$, for all $x \in \mathbb{S}$.

One easily shows that the additive group of a finite semifield is elementary abelian, and the exponent of the additive group of $\mathbb{S}$ is called the *characteristic* of $\mathbb{S}$. Contained in a finite semifield are the following important substructures, all of which are isomorphic to a finite field. 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:

$$\mathbb{N}_l(\mathbb{S}) := \{x : x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall y, z \in \mathbb{S}\}, \tag{1}$$

$$\mathbb{N}_m(\mathbb{S}) := \{y : y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall x, z \in \mathbb{S}\}, \tag{2}$$

$$\mathbb{N}_r(\mathbb{S}) := \{z : z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \forall x, y \in \mathbb{S}\}. \tag{3}$$

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* $Z(\mathbb{S})$. If there is no confusion, we denote these subfields by $\mathbb{N}_l$, $\mathbb{N}_m$, $\mathbb{N}_r$, Z.

Two semifields $\mathbb{S}$ and $\hat{\mathbb{S}}$ are called *isotopic* if there exists a triple (F, G, H) of non-singular linear transformations from $\mathbb{S}$ to $\hat{\mathbb{S}}$ such that $x^F \hat{\circ} y^G = (x \circ y)^H$, for all $x, y, z \in \mathbb{S}$. The triple (F, G, H) is called an *isotopism.*

3 Semifields from skew-polynomial rings

In this section we use an *irreducible* polynomial in a skew polynomial ring to construct a semifield. We start with some definitions and properties of skew polynomial rings. For a more detailed description we refer to Ore [19].

Definition 1. Let K be a field, and σ an automorphism of K. Define the *skew polynomial ring* $R = K[t; \sigma]$ to be the set of polynomials in t with coefficients in K, where addition is defined termwise, and multiplication is defined by $ta = a^\sigma t$ for all $a \in K$.

We 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 $f = ab$.

Theorem 3 (Ore [19]). *Let R 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 $R = K[t; \sigma]$ is $F[t^n; \sigma] \simeq F[y]$, where 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*

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

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

For this paper we will set $K = \mathbb{F}_{q^n}$, and let $F = \mathbb{F}_q$ be the fixed field of σ. The properties of skew polynomial rings allow us to define a semifield in the following way. The result is not new, see Remark 3 below. We include a proof for the sake of completeness.

Theorem 4. *Let V be the vector space consisting of elements of R of degree strictly less than d. Let $f \in R$ be 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 order q^{nd}.

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 the existence of $h \in \mathbb{S}_f$ such that $ab = hf$. Comparing degrees, Part (6) of the previous theorem 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 order q^{nd}. □

Remark 1. Note that for any $0 \neq \alpha \in K$, the polynomials f and αf define the same semifield.

Note that defining the multiplication using remainder on *left* division by f also defines a semifield. However, in Corollary 4 we will show that the semifields obtained are anti-isomorphic.

Remark 2. For the rest of this paper we will write *mod* for *mod$_r$* unless otherwise stated, and write *divides* for *right divides*.

In [18] Ore introduced the following notion of *eigenring* (called the *normalizer* by Jacobson in [6]).

Definition 2. Let f be a monic irreducible element of R of degree d. Define the *eigenring* of f by

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

Remark 3. Ore and Jacobson, when studying *cyclic algebras*, each considered structures obtained from the vector space of residue classes of $R = K[t;\sigma]$ modulo a left ideal Rf. As they were interested only in associative algebras, they restricted their attention to the eigenring $E(f)$. They each proved (in different ways) the following theorem ([18, p. 242] and [6, p. 201–202]):

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

As we have seen above, 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 trivially extends to:

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

The proof relies only on the theorem of Ore (Theorem 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.

This construction was then explicitly formulated by Petit [20] in 1966. As this construction is perhaps not well known, and as some of the tools used are required for later results, we include proofs of some of the results contained therein.

4 Nuclei

We now investigate the nuclei of the above defined semifields. These results can be found in [20].

Theorem 5 ([20]). *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

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

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 $f_i \in K$, 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

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

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

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

implying that for each i we have $f_i = 0$ or $\alpha^{\sigma^i} = \alpha^{\sigma^d}$ for all $a \in K$. 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 $\alpha \in K$, and so $\sigma^i = \mathrm{id}$. Hence if $f_i \neq 0$ then n divides i. Therefore $f \in F[t^n; \sigma] = Z(R)$, 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 $a, b, c \in R$ of degree less than $d = \deg(f)$ we can find unique $u, v, w, z \in R$ of degree less than d such that

$$\begin{aligned} ab &= uf + v, \quad \text{and} \\ bc &= wf + z, \end{aligned}$$

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

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

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 1 (Petit [20]). *$\mathbb{S}_f$ is associative if and only if $f \in Z(R)$.*

We will see in Lemma 3 that if K is a finite field, and σ is not the identity automorphism, 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. Note however that such elements can exist over infinite fields.

Theorem 6 ([20]). *Suppose f is a monic irreducible element of $R = K[t;\sigma]$ such that $f \notin Z(R)$. The left and middle nuclei of $\mathbb{S}_f$ are given by*

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

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

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

Proof. Let $a, b, c \in R$ be of degree less than d, and u, v, w, z be as defined in the proof of Theorem 5. 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 $a \in K$, the centre is therefore equal to the fixed field of σ, which is F. □

Later we will show that $|N_r(\mathbb{S}_f)| = q^d$. The nuclei of $\mathbb{S}_f$ were calculated in a different way by Dempwolff in [3], when he calculated the nuclei of cyclic semifields, which we will show in Section 6 to be equivalent to this construction.

Hence if two semifields defined by polynomials $f \in K[t, \sigma]$ and $f' \in K'[t, \sigma']$ are isotopic, then $K = K'$, $\deg(f) = \deg(f')$, and σ and σ' have the same fixed field (i.e. the same order). In the next section we will investigate when two such semifields are isotopic.

5 Isotopisms between semifields $\mathbb{S}_f$

In this section we will first consider some properties of skew polynomial rings, which we will use later to obtain isotopisms of the above defined semifields.

Lemma 1. *Let φ be an automorphism of $R = K[t; \sigma]$, where σ is not the identity automorphism. Then*

$$\varphi(f) = f^\rho(\alpha t)$$

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

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 K, and assume $\varphi(t) = \alpha t + \beta$, $\alpha, \beta \in K$, $\alpha \neq 0$. Choose $\gamma \in K$ such that $\gamma^\sigma \neq \gamma$. Computing $\varphi(t)\varphi(\gamma) = \varphi(t\gamma) = \varphi(\gamma^\sigma t) = \varphi(\gamma^\sigma)\varphi(t)$, we see that $\beta = 0$, and the assertion follows. □

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

Theorem 7. *Let f be an irreducible of degree d in R. Let φ be an automorphism of R. Define $g = \varphi(f)$. Then $\mathbb{S}_f$ and $\mathbb{S}_g$ are isomorphic, and*

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

The proof is left to the reader. We now consider another type of isotopism between these semifields.

Definition 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 8. *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

$$(a \circ_g b)^H = (ab-vg)^H = (ab-vg)u \mod f = (abu-vgu) \mod f \equiv abu \mod f$$

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 [7] Jacobson investigated when two skew polynomials are similar. We include a proof here for completeness, and because some of the concepts introduced will be of use later in this paper.

Definition 4. 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 [5] Giesbrecht showed that $mzlm(f)$ exists, is unique, has degree d and is irreducible when viewed as an element of $\mathbb{F}_q[y]$ (which we state 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 [8].

Lemma 2 ([5]). *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.*

Lemma 3. *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) $\dfrac{R}{Rh} \simeq M_n(\mathbb{F}_{q^d})$*;*
(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 [9, 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 ([15, Chapter 17]). It is easily shown (see for example [5], 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 $\mathrm{Ann}_M(U)$ 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 $\mathrm{Ann}_M(\mathrm{Ker}(A(f)))$, and so $A(f)$ has rank $n - 1$ as claimed. □

Remark 4. Hence 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 [17], and is an upper bound for $A(q, n, d)$. However, we will see that this is far from optimal.

Lemma 4. *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 $\deg(u') < \deg(f)$. Then $fu \equiv 0 \mod f$ if and only if $u' \in E(f)$. 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 3, $\frac{R}{Rh} \simeq M_n(\mathbb{F}_{q^d}) = M$. If A denotes this isomorphism, then by Part (3) of Lemma 3, $A(f) := A(f + Rh)$ has rank $n - 1$. Let $\mathrm{Ker}(A(f)) = \langle v \rangle$ for $0 \neq v \in (\mathbb{F}_{q^d})^n$. Then

$$u + Rh \in E' \quad \Longleftrightarrow \quad A(f)A(u) \in M.A(f) \quad \Longleftrightarrow \quad A(u)v = \lambda v$$

for some $\lambda \in \mathbb{F}_{q^d}$. Then $A(u) - \lambda I \in \mathrm{Ann}_M(v)$, and so

$$|E'| = q^d |\mathrm{Ann}_M(v)| = q^{d(n^2-n+1)}.$$

Hence from the two expressions for $|E'|$ we get $|E(f)| = q^d$, as claimed. □

Remark 5. We see that $E(f) = \{z \mod f : z \in Z(R)\}$, i.e. the remainders of all central elements of R on right division by f.

The sizes of the nuclei and the centre of the semifield $\mathbb{S}_f$ now easily follow from Theorems 5, 6 and Lemma 4.

Theorem 9. *If $f \in R$ is irreducible of degree d, then for the nuclei and the centre of semifield $\mathbb{S}_f$ we have*

$$(\#Z, \#\mathbb{N}_l, \#\mathbb{N}_m, \#\mathbb{N}_r) = (q, q^n, q^n, q^d).$$

The following theorem tells us exactly when two irreducibles are similar.

Theorem 10. *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 3,

$$\mathrm{rank}(A(f)) = \mathrm{rank}(A(g)) = n - 1,$$

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 a non-trivial common divisor with h, so $A(v)$ is not invertible). Then

$$g(v' + cf) = (u + ba)f \quad \Longrightarrow \quad gv' = (u + ba - gc)f \quad \Longrightarrow \quad gv' = u'f$$

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 [5]. 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 [2]. The next theorem allows us to further improve this bound.

Definition 5. 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 11. *Let $f, g \in R$ be irreducibles of degree d, with $mzlm(f) = \hat{f}(t^n)$ and $mzlm(g) = \hat{g}(t^n)$ 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

$$(\alpha t)^n = \alpha\alpha^\sigma \ldots \alpha^{\sigma^{n-1}} t^n = \lambda t^n.$$

Define

$$h(t) = f^\rho(\alpha t).$$

By Theorem 7, $\mathbb{S}_f$ and $\mathbb{S}_h$ are isomorphic. Let $mzlm(h) = \hat{h}(t^n)$.

Let φ be the automorphism of R defined by $\varphi(a) = a^\rho(\alpha t)$. Then as $\varphi(f) = h$ and $\hat{f}(t^n) = uf$ for some $u \in R$,

$$\varphi(\hat{f}(t^n)) = \varphi(u)\varphi(f) = \varphi(u)h.$$

But

$$\varphi(\hat{f}(t^n)) = \hat{f}^\rho((\alpha t)^n) = \hat{f}^\rho(\lambda t^n).$$

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 8, 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 12. *The number of isotopism classes of semifields $\mathbb{S}_f$ of order q^{nd} obtained from $\mathbb{F}_{q^n}[t;\sigma]$ is less 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 [5], $\hat{f}$ 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 11, $\mathbb{S}_f$ and $\mathbb{S}_g$ are isotopic. □

In the next section we will relate this construction to the construction of Johnson–Jha, and in the last section we will compare this new bound to existing bounds.

6 Cyclic semifields and endomorphisms of left multiplication

Definition 6. A *semilinear transformation* on a vector space $V = K^d$ is an additive map $T : V \to V$ such that

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

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

Note that choosing a basis for V gives us

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

where A is some invertible K-linear transformation from V to itself, σ is an automorphism of 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 7. An element T of $\Gamma\mathrm{L}(d,K)$ is said to be *irreducible* if the only T-invariant subspaces of V are V and $\{0\}$.

Theorem 13. *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 $\Gamma\mathrm{L}(d,K)$ 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 $(v_0,v_1,\dots,v_{d-1})^t$, then*

$$L_t(v)=A_f(v^\sigma)$$

where

$$A_f=\begin{pmatrix}0 & 0 & \dots & 0 & f_0\\ 1 & 0 & \dots & 0 & f_1\\ 0 & 1 & \dots & 0 & f_2\\ \vdots & \vdots & \dots & \vdots & \vdots\\ 0 & 0 & \dots & 1 & f_{d-1}\end{pmatrix}.$$

(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 $\mathbb{F}_{q^n}$. 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:

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

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 an 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 $\mathbb{F}_{q^n}$, 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 2. *The spread set of endomorphisms of left multiplication of elements in* $\mathbb{S}_f$ *is* $\{a(L_t) \mid a \in \mathbb{S}_f\}$.

In [10] Jha and Johnson defined a semifield as follows.

Theorem 14. *Let T be an irreducible element of* $\Gamma\mathrm{L}(d, K)$. *Fix a K-basis* $\{e_0, e_1, \ldots, e_{d-1}\}$ *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.*

The following theorem is an immediate consequence of the definition of $\mathbb{S}_T$ and Theorem 13.

Theorem 15. *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 noted that conjugate semilinear transformations define isotopic semifields:

Lemma 5. *Suppose* $T = \varphi^{-1}U\varphi$ *for some* $\varphi \in \Gamma\mathrm{L}(d, K)$, *and let* $\rho \in \mathrm{Aut}(K)$ *be the accompanying automorphism of* φ. *Let* $\mathbb{S}_T = (V, \circ)$, $\mathbb{S}_U = (V, \star)$. *Then*

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

We will show that each semifield defined by a semilinear transformation is isotopic to some semifield $\mathbb{S}_f$ with f irreducible in some skew polynomial ring.

Theorem 16. *Let T be any irreducible element of $\Gamma\mathrm{L}(d,K)$ with automorphism σ. Then T is $\mathrm{GL}(d,K)$-conjugate to $L_{t,f}$ for some irreducible $f \in R = K[t;\sigma]$, 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 $\varphi \in \mathrm{GL}(d,K)$ by

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

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

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

It is left to the reader to verify that $T\varphi = \varphi L_{t,f}$, where

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

As shown in Theorem 13, Part (4), $L_{t,f}$ is irreducible if and only if f is irreducible in R. □

Theorem 17. *Let f and g be two monic irreducibles of degree d in R. Then*

(1) *$L_{t,f}$ and $L_{t,g}$ are $\mathrm{GL}(d,K)$-conjugate if and only if f and g are similar;*
(2) *$L_{t,f}$ and $L_{t,g}$ are $\Gamma\mathrm{L}(d,K)$-conjugate if and only if f and g^ρ are similar for some $\rho \in \mathrm{Aut}(K)$.*

Proof. Suppose $L_{t,f}\varphi = \varphi L_{t,g}$ for some $\varphi \in \Gamma\mathrm{L}(d,K)$, where φ has automorphism ρ. Let $\varphi(1) = u$. Then

$$\varphi(t^i) = \varphi(L^i_{t,g}(1)) = L^i_{t,f}\varphi(1) = L^i_{t,f}(u) = t^i u \mod f$$

for all $i = 0, 1, \dots, d-1$. Now, with $g = t^d - \sum_{i=0}^{d-1} g_i t^i$, we have

$$\begin{aligned}\varphi L_{t,g}(t^{d-1}) &= \varphi(t^d \mod g) = \varphi\left(\sum_{i=0}^{d-1} g_i t^i\right) = \sum_{i=0}^{d-1} g_i^\rho \varphi(t^i) \\ &= \sum_{i=0}^{d-1} g_i^\rho (t^i u \mod f) = \left(\sum_{i=0}^{d-1} g_i^\rho t^i\right) u \mod f = (t^d - g^\rho)u \mod f.\end{aligned}$$

But as $L_{t,f}\varphi = \varphi L_{t,g}$, this is equal to

$$L_{t,f}\varphi(t^{d-1}) = L_{t,f}(t^{d-1}u \mod f).$$

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 $\varphi \in \mathrm{GL}(n,K)$, 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 ([2, Theorem 2.10], compare to Asano–Nakayama [1, Satz 13]).

Corollary 3. *Let T and U be two irreducible elements of $\Gamma\mathrm{L}(d,K)$, $K = \mathbb{F}_{q^n}$, where the accompanying automorphism σ of both T and U is a generator of $Gal(K,\mathbb{F}_q)$. Then*

(1) *T and U are $\mathrm{GL}(d,K)$-conjugate if and only if T^n and U^n have the same minimal polynomial over $\mathbb{F}_q$;*
(2) *T and U are $\Gamma\mathrm{L}(d,K)$-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 16, we may assume T is $\mathrm{GL}(d,K)$-conjugate to $L_{t,f}$, U is $\mathrm{GL}(d,K)$-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 10 and Theorem 17, $L_{t,f}$ and $L_{t,g}$ are $\mathrm{GL}(d,K)$-conjugate if and only if $mzlm(f) = mzlm(g)$. Hence T and U are $\mathrm{GL}(d,K)$-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 $\Gamma\mathrm{L}(d,K)$ 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 an upper bound on the number of conjugacy classes, and hence the number of isotopy classes:

$$A(q,n,d) \leq N(q,d) = \#I(q,d).$$

7 Isotopisms between different skew-polynomial rings

In this section, we consider the isotopism problem for semifields constructed from different skew polynomial rings. The most general skew polynomial ring has the form $K[t;\sigma,\delta]$, with multiplication defined by

$$ta = a^\sigma t + a^\delta,$$

where σ is an automorphism of K and δ is a σ-derivation, i.e. an additive map on K such that

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

for all $a, b \in K$. For example, 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. Petit [20] showed that these rings can also be used to define semifields. However, as the following theorem of Jacobson shows, $K[t;\sigma,\delta_x]$ is isomorphic to $K[t;\sigma]$ for all x, and hence the semifields obtained are isotopic.

Theorem 18 (Jacobson [9, Proposition 1.2.20]). *Let $R = K[t;\sigma]$ and $R' = K[t;\sigma,\delta_x]$ be skew-polynomial rings. Denote the multiplication in R and R' by $\circ$ and $\circ'$ respectively. Define a map $\varphi : R \to R'$ by*

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

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

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

for all $a, b \in R$.

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

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

for all $\alpha \in K$. Now

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

while

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

and the result holds. □

Note that defining the multiplication using remainder on *left* division by f also defines a semifield. However, the following theorems show that the semifields obtained are anti-isomorphic.

Theorem 19. *Let $R = K[t;\sigma]$ and $R' = K[t;\sigma^{-1}]$ 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 4. *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.*

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

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

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. □

Remark 6. It is not clear when different skew polynomial rings $R = K[t;\sigma]$ and $R' = K[t;\sigma']$ define isotopic semifields. It is a necessary condition that σ and σ' have the same order. The following observation of Kantor and Liebler (in [13]) gives a result in this direction. *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 [13, Remark 4.1] where the statement is made in terms of projective planes.)

This implies that every semifield $\mathbb{S}_f$ for $f \in K[t;\sigma]$ is isotopic to $\mathbb{S}_{\bar{f}}$ for some $\bar{f} \in K[t;\sigma^{-1}]$. In fact it can be shown that $\bar{f}$ is the reciprocal of f. 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 $\frac{\varphi(n)}{2}M(q,d)$, when $n \neq 2$, where φ is Euler's totient function.

8 New and existing bounds for $A(q, n, d)$

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 and equal to $\frac{1}{d}\sum_{s|d}\mu(s)q^{d/s}$, where μ denotes the Moebius function. Following the notation of [11], we can write this as $N(q,d) = \frac{q^d-\theta}{d}$, where θ denotes the number of elements of $\mathbb{F}_{q^d}$ contained in a proper subfield $\mathbb{F}_{q^e}$.

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

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

In [11], the authors consider cyclic semifields two-dimensional over their left nucleus, with right and middle nuclei isomorphic to $\mathbb{F}_{q^2}$t. 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

$$A(q,2,d) \geq \frac{q^d - \theta}{2dhq(q-1)}$$

where $q = p^h$.

In [13], 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}:

$$ndq^{nd/2}\log_2(q).$$

The bounds for $A(q,n,d)$ that are proved in this paper arise from the following isotopism criteria. In Theorem 8, we proved that if f and g are irreducibles of degree d in $\mathbb{F}_{q^n}[t;\sigma]$, with $gu \equiv 0 \mod f$ for some $u \in \mathbb{F}_{q^n}[t;\sigma]$, then $\mathbb{S}_f$ and $\mathbb{S}_g$ are isotopic, and

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

where $b^H = b \circ_f u$. Next we have shown that this condition is equivalent to $mzlm(f) = mzlm(g)$ (Theorem 10). This leads to the following upper bound (this also follows from the result of Dempwolff [2], by Theorem 16 above):

$$A(q,n,d) \leq N(q,d) = \frac{q^d-\theta}{d}.$$

We improve this bound by showing that $\mathbb{S}_f$ and $\mathbb{S}_g$ are also isotopic when

$$\lambda^{-d}\hat{f}^\rho(\lambda y) = \hat{g},$$

for some $\lambda \in \mathbb{F}_q^\times$, $\rho \in \mathrm{Aut}(\mathbb{F}_q)$, where $\hat{f} = mzlm(f)$ and $\hat{g} = mzlm(g)$ (Theorem 12). This leads to the 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 the introduction.

Note that if $q = p^h$ for p prime, then

$$\frac{q^d-\theta}{dh(q-1)} \leq M(q,d) \leq \frac{q^d-\theta}{d}.$$

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.

Example. If q is prime, and $(q-1,d) = 1$, then $M(q,d) = \frac{N(q,d)}{q-1}$.

Remark 7. 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 [5]. Then the semifields $\mathbb{S}_{f_i}$ are representatives of each isotopy class.

Acknowledgement. The authors thank W. M. Kantor and the anonymous referee for their many helpful suggestions in improving this paper, and for bringing the papers of Petit and Wene to their attention after this paper was submitted.

References

[1] K. Asano, T. Nakayama, Über halblineare Transformationen. *Math. Ann.* **115** (1938), 87–114. Zbl 0018.00402

[2] U. Dempwolff, On irreducible semilinear transformations. *Forum Math.* **22** (2010), 1193–1206. MR2735892 (2011k:15003) Zbl 1205.15006

[3] U. Dempwolff, Autotopism groups of cyclic semifield planes. *J. Algebraic Combin.* **34** (2011), 641–669. MR2842914 (2012k:51009) Zbl pre05968648

[4] L. E. Dickson, Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.* **7** (1906), 370–390. MR1500755 Zbl 37.0111.06

[5] M. Giesbrecht, Factoring in skew-polynomial rings over finite fields. *J. Symbolic Comput.* **26** (1998), 463–486. MR1646671 (99i:16053) Zbl 0941.68160

[6] N. Jacobson, Non-commutative polynomials and cyclic algebras. *Ann. of Math.* (2) **35** (1934), 197–208. MR1503154 Zbl 60.0104.01

[7] N. Jacobson, Pseudo-linear transformations. *Ann. of Math.* (2) **38** (1937), 484–507. MR1503347 Zbl 0017.15001 JFM 63.0087.01

[8] N. Jacobson, *The Theory of Rings*. Amer. Math. Soc. 1943. MR0008601 (5,31f) Zbl 0060.07302

[9] N. Jacobson, *Finite-dimensional division algebras over fields*. Springer 1996. MR1439248 (98a:16024) Zbl 0874.16002

[10] V. Jha, N. L. Johnson, 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. MR1023461 (90i:51009) Zbl 0684.51003

[11] N. L. Johnson, G. Marino, O. Polverino, R. Trombetti, On a generalization of cyclic semifields. *J. Algebraic Combin.* **29** (2009), 1–34. MR2470113 (2010e:12010) Zbl 1230.51002

[12] W. M. Kantor, Finite semifields. In: *Finite geometries, groups, and computation*, 103–114, de Gruyter 2006. MR2258004 (2007i:51003) Zbl 1102.51001

[13] W. M. Kantor, R. A. Liebler, Semifields arising from irreducible semilinear transformations. *J. Aust. Math. Soc.* **85** (2008), 333–339. MR2476443 (2010d:51013) Zbl 1172.51006

[14] D. E. Knuth, Finite semifields and projective planes. *J. Algebra* **2** (1965), 182–217. MR0175942 (31 #218) Zbl 0128.25604

[15] S. Lang, *Algebra*. Addison-Wesley Publ. Co., Reading, MA 1984. MR783636 (86j:00003) Zbl 0712.00001

[16] M. Lavrauw, O. Polverino, Finite Semifields. In: *Current research topics in Galois geometries*, 127–155, Nova Academic Publishers (ed. J. De Beule and L. Storme) 2011.

[17] R. W. K. Odoni, On additive polynomials over a finite field. *Proc. Edinburgh Math. Soc.* (2) **42** (1999), 1–16. MR1669401 (2000j:11188) Zbl 1055.11524

[18] Ø. Ore, Formale Theorie der linearen Differentialgleichungen. II. Teil. *J. Reine Angew. Math.* **168** (1932), 233–252. Zbl 0005.39601

[19] Ø. Ore, Theory of non-commutative polynomials. *Ann. of Math.* (2) **34** (1933), 480–508. MR1503119 Zbl 0007.15101 JFM 59.0925.01

[20] J.-C. Petit, Sur certains quasi-corps généralisant un type d'anneau-quotient. In: *Algèbre Théorie Nombres* (ed. Sém. P. Dubreil, M.-L. Dubreil-Jacotin, L. Lesieur and C. Pisot), vol. 20, 1–13, 1968. Zbl 0203.33703

[21] G. P. Wene, Finite semifields three-dimensional over the left nuclei. In: *Nonassociative algebra and its applications* (*São Paulo,* 1998), 447–456, Dekker 2000.
MR1758093 (2001g:17004) Zbl 0976.17003

Received 6 April, 2011; revised 18 March, 2012

M. Lavrauw, J. Sheekey, Department of Management and Engineering, Università di Padova, Italy
Email: michel.lavrauw@unipd.it, johnsheekey@gmail.com