# PLANAR POLYNOMIALS FOR COMMUTATIVE SEMIFIELDS WITH SPECIFIED NUCLEI

ROBERT S. COULTER, MARIE HENDERSON, AND PAMELA KOSICK

Abstract. We consider the implications of the equivalence of commutative semifields of odd order and planar Dembowski-Ostrom polynomials. This equivalence was outlined recently by Coulter and Henderson. In particular, following a more general statement concerning semifields we identify a form of planar Dembowski-Ostrom polynomial which must define a commutative semifield with the nuclei specified. Since any strong isotopy class of commutative semifields must contain at least one example of a commutative semifield described by such a planar polynomial, to classify commutative semifields it is enough to classify planar Dembowski-Ostrom polynomials of this form and determine when they describe non-isotopic commutative semifields. We prove several results along these lines. We end by introducing a new commutative semifield of order $3^8$ with left nucleus of order 3 and middle nucleus of order $3^2$.

## 1. Introduction

A *finite semifield* $\mathcal{R}$ is a ring with no zero-divisors, a multiplicative identity and left and right distributivity. If we do not insist on the existence of a multiplicative identity, then we call the ring a *presemifield*. It is not assumed that $\mathcal{R}$ is commutative or associative. Though the definition extends to infinite objects, this article is only concerned with the finite case. The additive group of a semifield must be elementary abelian and thus the order of any semifield is necessarily a prime power; for a simple proof see Knuth [12, Section 2.4].

Finite fields satisfy these requirements and so the existence of semifields is clear. Those semifields which are not fields are called *proper* semifields. The first proper semifields identified were the commutative semifields of Dickson [7] which have order $q^2$ with $q$ an odd prime power. Dickson may have been led to study semifields following the publication of Wedderburn's Theorem [20], which appeared the year before [7] and which Dickson was the first person to provide a correct proof for (see Parshall [18]). As no new structures are obtained by removing commutativity, it is reasonable to investigate those structures which are non-associative instead.

The role of semifields in projective geometry was confirmed following the introduction of coordinates in non-Desarguesian planes by Hall [8]. Subsequent to Hall's work, Lenz [13] developed and Barlotti [1] refined what is now known as the Lenz-Barlotti classification, under which semifields correspond to projective planes of Lenz-Barlotti type V.1. In some sense, modern interest in semifields can be traced back to the important work of Knuth [12]. Presently, semifields are enjoying a true

Date stamped: September 10, 2007
The first author was partially supported by a University of Delaware Research Foundation Grant. He also gratefully acknowledges the support of the Victoria University of Wellington, New Zealand, where part of this research was conducted during a sabbatical in the second half of 2005.

renaissance with well over fifty publications concerning them having appeared since the year 2000.

Let $\mathcal{R}$ be a finite semifield. We define the *left, middle and right nucleus* of $\mathcal{R}$, denoted by $\mathcal{N}_l, \mathcal{N}_m$ and $\mathcal{N}_r$, respectively, as follows:

$$\mathcal{N}_l(\mathcal{R}) = \{\alpha \in \mathcal{R} \mid (\alpha \star x) \star y = \alpha \star (x \star y) \text{ for all } x, y \in \mathcal{R}\}$$
$$\mathcal{N}_m(\mathcal{R}) = \{\alpha \in \mathcal{R} \mid (x \star \alpha) \star y = x \star (\alpha \star y) \text{ for all } x, y \in \mathcal{R}\}$$
$$\mathcal{N}_r(\mathcal{R}) = \{\alpha \in \mathcal{R} \mid (x \star y) \star \alpha = x \star (y \star \alpha) \text{ for all } x, y \in \mathcal{R}\}.$$

It is easily shown that these sets are finite fields. The set $\mathcal{N}(\mathcal{R}) = \mathcal{N}_l \cap \mathcal{N}_m \cap \mathcal{N}_r$ is called the *nucleus* of $\mathcal{R}$. The nuclei are important objects in the study of semifields. They measure how far $\mathcal{R}$ is from being associative. Additionally, as Knuth observed, $\mathcal{R}$ can be represented as a right vector space over $\mathcal{N}_l$, a left vector space over $\mathcal{N}_r$ and both a left or right vector space over $\mathcal{N}_m$.

Let $\mathcal{R}_1 = (\mathbb{Z}_p^n, +, \circ)$ and $\mathcal{R}_2 = (\mathbb{Z}_p^n, +, \star)$ be two semifields of order $p^n$. We say $\mathcal{R}_1$ and $\mathcal{R}_2$ are *isotopic* if there exists a triple of non-singular linear transformations $(M, N, L)$ satisfying

$$L(x \circ y) = M(x) \star N(y)$$

for all $x, y \in \mathbb{Z}_p^n$. This definition of equivalence, which is clearly much weaker than the standard ring isomorphism, arises from projective geometry: two planes coordinatised by semifields are isomorphic if and only if the corresponding semifields are isotopic. A *strong isotopy* is an isotopy where $M = N$.

This article is mainly concerned with commutative semifields of odd order. Recent work by Coulter and Henderson [4] has provided an alternate way to study such objects. In Section 3 we set this new approach in a slightly more general context by considering the semifield case first. We also note an equivalence between the existence of a semifield and the existence of a set of $\mathbb{F}_q$-complete mappings, see Theorem 3.2. The essential ingredient of the approach of [4] is the class of polynomials known as planar Dembowski-Ostrom polynomials, see Section 2. In Section 4 we develop this new approach further, concentrating mainly on determining restrictions on the planar Dembowski-Ostrom polynomials, and further to considering a special form of Dembowski-Ostrom polynomials. This allows us to describe commutative semifields with specified nuclei in terms of the corresponding planar Dembowski-Ostrom polynomials. We then consider isotopism issues, providing a strong restriction on the possible isotopisms between particular isotopes of commutative semifields, as well as a necessary condition on the type of planar DO polynomial which describes commutative semifields isotopic to a finite field. We end with an application of our results by introducing a new commutative semifield of order $3^8$ with left nucleus of order 3 and middle nucleus of order $3^2$.

## 2. Preliminaries

Throughout $\mathbb{F}_q$ is used to denote the finite field of $q$ elements where $q = p^e$ for some prime $p$ and some $e \in \mathbb{N}$. By $\mathbb{F}_q^*$ we mean the non-zero elements of $\mathbb{F}_q$. The polynomial ring in indeterminate $X$ over $\mathbb{F}_q$ will be denoted by $\mathbb{F}_q[X]$. Any two polynomials $f, h \in \mathbb{F}_q[X]$ representing the same function must satisfy $f(X) \equiv h(X) \pmod{X^q - X}$. Consequently, any function on $\mathbb{F}_q$ can be uniquely represented by a polynomial of degree at most $q-1$ and this polynomial of smallest degree is often referred to as *reduced*. This can be generalised to multivariate polynomials over $\mathbb{F}_q$ with the degree of each variable being at most $q-1$. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* over $\mathbb{F}_q$ if $f$ induces a bijection of the field under evaluation. Planar functions were introduced by Dembowski and Ostrom in [6]. A sufficient definition for our purposes is as follows: a polynomial $f \in \mathbb{F}_q[X]$ is a *planar function* if the difference polynomial $f(X+a)-f(X)-f(a)$ is a permutation polynomial for each $a \in \mathbb{F}_q^*$.

A *linearised polynomial* $L \in \mathbb{F}_q[X]$ is any polynomial of the shape

$$L(X) = \sum_{i=0}^{k} a_i X^{p^i}.$$

More accurately, the linearised polynomial $L(X)$ is called a $p^s$-polynomial for any integer $s$ for which $a_i = 0$ whenever $i \neq \alpha s$, $\alpha \in \mathbb{Z}$. Clearly, every linearised polynomial is a $p$-polynomial but there are occasions where a more specific choice of $s$ is preferable. For examples of these situations, see the papers of Ore [15, 16, 17] or more recently, Henderson and Matthews [9]. The reduction of a linearised polynomial modulo $X^q - X$ is a linearised polynomial and $L(x+y) = L(x) + L(y)$ for all $x, y \in \mathbb{F}_q$. The set of all reduced linearised polynomials represents all linear transformations of $\mathbb{F}_q$ and forms an algebra under composition modulo $X^q - X$, see Vaughan [19]. It is straightforward to show a linearised polynomial is a permutation polynomial over $\mathbb{F}_q$ if and only if its only root in $\mathbb{F}_q$ is zero. The set of all reduced linearised permutation polynomials represents the set of all non-singular linear transformations over $\mathbb{F}_q$. Moreover, if $q = p^e$, then this set forms a group under composition modulo $X^q - X$ isomorphic to the general linear group $GL(p, e)$. There is an extensive literature concerning these polynomials and we refer the interested reader to the book of Lidl and Niederreiter [14] for more information and further references. A result we shall need but have not found a reference for is the following.

**Lemma 2.1.** *Let $e, n \in \mathbb{N}$ with $n > 1$ and $p$ be a prime. Set $q = p^e$ and $t(X) = X^q - X$. If $L \in \mathbb{F}_{q^n}[X]$ is a linearised polynomial and $t$ divides $L$, then there exists a linearised polynomial $M$ such that $L(X) = M(t(X))$.*

*Proof.* Set $L(X) = \sum_{i=0}^{k} a_i X^{p^i}$ for some $k \geq e$ and let $d = p^k$. The case $k = e$ is clear. Assume $k > e$. Since $t$ divides $L$, there exists a polynomial $Q \in \mathbb{F}_{q^n}[X]$ such that $L(X) = t(X)Q(X)$. Thus

$$\begin{aligned} L(X) &= t(X)Q(X) \\ &= (X^q - X)\left(\sum_{i=0}^{d-q} b_i X^i\right) \\ &= -\sum_{i=1}^{q-1} b_{i-1}X^i + \sum_{i=q}^{d-q+1} (b_{i-q} - b_{i-1})X^i + \sum_{i=d-q+2}^{d} b_{i-q}X^i \\ &= -\sum_{i=0}^{e-1} b_{p^i-1}X^{p^i} + \sum_{i=e}^{k-1} (b_{p^i-q} - b_{p^i-1})X^{p^i} + b_{p^k-q}X^{p^k}, \end{aligned}$$

where in the final step we have used the fact $L$ is a $p$-polynomial to remove terms not of the form $b_i X^{p^i}$. We claim $b_{p^i-q} = b_{p^{i-e}-1}$ for all integers $e \leq i \leq k$. If this claim were true, then the lemma would be established as we would have

$$\begin{aligned} L(X) &= -\sum_{i=0}^{e-1} b_{p^i-1}X^{p^i} + \sum_{i=e}^{k-1}(b_{p^{i-e}-1} - b_{p^i-1})X^{p^i} + b_{p^{k-e}-1}X^{p^k} \\ &= \sum_{i=0}^{k-e} b_{p^i-1}(X^{p^e} - X)^{p^i} \\ &= \sum_{i=0}^{k-e} b_{p^i-1}t(X)^{p^i} \\ &= M(t(X)), \end{aligned}$$

as desired.

It remains to show $b_{p^i-q} = b_{p^{i-e}-1}$ for all integers $e \le i \le k$. Note first for any $e \le i \le k$ and $1 \le m \le p^{i-e} - 1$ the coefficient of $X^{p^{i-e}+m(q-1)}$ in the expansion of $t(X)Q(X)$ above is zero as this can never be a prime power for the range of $m$ specified. Hence $b_{p^{i-e}+(m-1)(q-1)-1} = b_{p^{i-e}+m(q-1)-1}$ for all $1 \le m \le p^{i-e} - 1$. In particular, using the extremes of the range for $m$ yields $b_{p^{i-e}-1} = b_{p^i-q}$ for all $e \le i \le k$, as desired. □

A *Dembowski-Ostrom (DO) polynomial* $D \in \mathbb{F}_q[X]$ is any polynomial of the shape

$$D(X) = \sum_{i,j=0}^{k} a_{ij}X^{p^i+p^j}.$$

DO polynomials were characterised via their difference polynomials by Coulter and Matthews [5]: A polynomial $f \in \mathbb{F}_q[X]$ is a DO polynomial if and only if every difference polynomial $f(X+a) - f(X) - f(a)$, $a \in \mathbb{F}_q^*$, is a linearised polynomial. Results from Blokhuis *et al* [2] show that DO polynomials are closed under (left or right) composition with linearised polynomials and, provided $q$ is odd, under reduction modulo $X^q - X$.

Most relevant for this article is the recent work of Coulter and Henderson [4] who showed that there is a one-to-one correspondence between commutative presemifields of odd order and planar DO polynomials. Formally, given a planar DO polynomial $f \in \mathbb{F}_q[X]$, $q$ odd, then $\mathcal{R} = (\mathbb{F}_q, +, \star)$ is a commutative presemifield with the multiplication $\star$ defined by

$$a \star b = f(a+b) - f(a) - f(b)$$

for all $a, b \in \mathbb{F}_q$. We denote this presemifield by $\mathcal{R}_f$. Conversely, given a commutative presemifield $\mathcal{R} = (\mathbb{F}_q, +, \star)$ of odd order, the polynomial given by $f(X) = \frac{1}{2}(X \star X)$ is a planar DO polynomial and $\mathcal{R} = \mathcal{R}_f$.

## 3. Semifields

Let $\mathcal{R}$ be a semifield of order $q = p^e$ with middle nucleus $\mathcal{N}_m$. As noted in the introduction, the additive group of $\mathcal{R}$ is necessarily elementary abelian. Consequently, we can view the multiplication of any $\mathcal{R}$ as a bivariate polynomial over $\mathbb{F}_q$ of degree less than $q$ in both variables. In fact, the relationship between the bivariate polynomial and the semifield imposes additional restrictions upon the polynomial.

**Theorem 3.1.** *Let $n$ and $e$ be natural numbers. Set $q = p^e$ for some prime $p$ and $t(X) = X^q - X$. For any semifield of order $q^n$ with middle nucleus containing $\mathbb{F}_q$ there exists an isotopic semifield $\mathcal{R} = (\mathbb{F}_{q^n}, +, \star)$ and a polynomial $K \in \mathbb{F}_{q^n}[X, Y]$ of the shape*

$$K(X,Y) = \sum_{i,j=0}^{(n-1)e-1} a_{ij} X^{p^i} Y^{p^j}$$

*such that $x \star y = K(t(x), t(y)) + xy$ for all $x, y \in \mathbb{F}_{q^n}$.*

*Proof.* The case $n = 1$ is clear as then $\mathcal{R}$ is isotopic to a finite field. Assume $n \geq 2$. Since a semifield can be viewed as a vector space over $\mathcal{N}_m$, there must exist isotopes of the semifield for which $a \star x = ax$ for all $x \in \mathbb{F}_{q^n}$ and $a \in \mathcal{N}_m$. Let $\mathcal{R} = (\mathbb{F}_{q^n}, +, \star)$ be one of these isotopes and $M(X, Y)$ be the bivariate polynomial of degree less than $q^n$ satisfying $x \star y = M(x, y)$ for all $x, y \in \mathbb{F}_{q^n}$. We can write $M(X, Y) = L(X, Y) + XY$ so that $L(x, a) = L(a, x) = 0$ for all $x \in \mathbb{F}_{q^n}$ and $a \in \mathcal{N}_m$. As the left and right distributive laws hold in $\mathcal{R}$, $M$ and so $L$ only have terms of the shape $X^{p^i} Y^{p^j}$. Fix $a \notin \mathcal{N}_m$. Then $L_a(X) = L(X, a)$ and $R_a(X) = L(a, X)$ are linearised polynomials for which $x \in \mathcal{N}_m$ is a root. Let $\mathbb{F}_q$ be some subfield of $\mathcal{N}_m$ and $t(X) = X^q - X$. Then $t(X)$ must divide both $L_y(X)$ and $R_y(X)$. It follows from Lemma 2.1 that $t$ is necessarily a compositional factor of $L_y$ and $R_y$ for all $y \in \mathbb{F}_q$. It is clear this can be done sequentially so that $L(X, Y) = K(t(X), t(Y))$ for a suitable polynomial $K(X, Y) = \sum_{i,j=0}^{(n-1)e-1} a_{ij} X^{p^i} Y^{p^j}$. □

There are a large number of bijective maps defined by any semifield. Theorem 3.1 allows us to make a more restrictive statement concerning these bijections. Let $S$ be some subset of $\mathbb{F}_q$. We call a polynomial $f \in \mathbb{F}_q[X]$ a *$S$-complete mapping over $\mathbb{F}_q$* if $f(X) + sX$ is a permutation polynomial over $\mathbb{F}_q$ for every $s \in S$. Clearly every polynomial is an $S$-complete mapping for some set $S$, although it is clear that in some cases $S = \varnothing$; for example when $f(X) = X^{q-1}$. Complete mappings, which are essentially the case $S = \{0, 1\}$, have been studied in various areas. Semifields define very specific types of $S$-complete mappings, as the following theorem shows.

**Theorem 3.2.** *Let $n > 1$ be an integer and $q = p^e$ with $p$ a prime. Set $t(X) = X^q - X$ and let $K(X, Y) \in \mathbb{F}_{q^n}[X, Y]$ satisfy*

$$K(X,Y) = \sum_{i,j=0}^{(n-1)e-1} a_{ij} X^{p^i} Y^{p^j}.$$

*Define a multiplication on $\mathbb{F}_{q^n}$ by $x \star y = K(t(x), t(y)) + xy$ for all $x, y \in \mathbb{F}_{q^n}$. For each $a \in \mathbb{F}_{q^n}$ set $L_a(X) = X \star a$ and $R_a(X) = a \star X$. Set $m = (q^{n-1} - 1)/(q - 1)$ and let*

$$B = \{1\} \bigcup_{i=1}^{m} \{c\beta_i \ : \ c \in \mathbb{F}_q^*\}$$

*form a complete set of coset representatives for $(\mathbb{F}_q, +)$ in $(\mathbb{F}_{q^n}, +)$. Then $\mathcal{R} = (\mathbb{F}_{q^n}, +, \star)$ is a semifield if and only if $L_{\beta_i}(X)$ and $R_{\beta_i}(X)$ are $\mathbb{F}_q$-complete mappings for every $1 \leq i \leq m$.*

*Proof.* Suppose $\mathcal{R} = (\mathbb{F}_{q^n}, +, \star)$ is a semifield and note that $\mathbb{F}_q \subseteq \mathcal{N}_m$ by Theorem 3.1. It follows that $L_a(X)$ and $R_a(X)$ are permutation polynomials for all $a \in \mathbb{F}_{q^n}^*$.

If $a \in \mathbb{F}_q^*$, then $L_a(X) = R_a(X) = aX$. If $a \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, then there exists a $\beta_i$ and elements $c, \alpha \in \mathbb{F}_q$ with $c \neq 0$ such that $a = c(\beta_i + \alpha)$.

$$\begin{aligned} L_a(X) &= X \star a \\ &= X \star (c \star (\beta_i + \alpha)) \\ &= cX \star (\beta_i + \alpha) \\ &= cX \star \beta_i + cX \star \alpha \\ &= L_{\beta_i}(cX) + \alpha(cX). \end{aligned}$$

Similarly, $R_a(X) = R_{\beta_i}(cX) + \alpha(cX)$. As $L_a(X)$ and $R_a(X)$ are permutation polynomials for all $a \in \mathbb{F}_{q^n}^*$, it follows that $L_{\beta_i}(X) + \alpha X$ is a permutation polynomial for all $\alpha \in \mathbb{F}_q$. Hence $L_{\beta_i}(X)$ is an $\mathbb{F}_q$-complete mapping. A similar argument shows $R_{\beta_i}(X)$ is an $\mathbb{F}_q$-complete mapping also. The argument can be reversed to prove the converse. □

Essentially, the theorem says the isotopy class of any semifield of order $q^n$ with middle nucleus of order $q$ is equivalent to the existence of $2(q^{n-1} - 1)/(q - 1)$ $\mathbb{F}_q$-complete maps – one simply considers the isotope of the form outlined in the theorem. As noted by a referee, there is a much simpler argument which shows any semifield of order $q^n$ with *nucleus* of order $q$ is equivalent to the existence of $2(q^n - 1)/(q - 1)$ $\mathbb{F}_q$-complete maps. Our statement is therefore much stronger whenever the nucleus and middle nucleus differ in cardinality.

We believe $\mathbb{F}_q$-complete mappings could be interesting to study in their own right. However, there is added motivation for studying them based on the above observation. At present, there is no non-trivial upperbound known for the number of semifields of any given order (non-trivial lower bounds for even order follow from the work of Kantor [11]). It may be possible to provide non-trivial, possibly asymptotic, estimates on the number of $\mathbb{F}_q$-complete mappings over $\mathbb{F}_{q^n}$. In particular, if a non-trivial upperbound could be found for their number, then this may lead to the first non-trivial upperbound for the number of semifields of a given order. Some results along these lines have already been given in a more general context by Hsiang, Hsu and Shieh [10].

## 4. Commutative semifields

We now turn to commutative semifields of odd order. In all of the following we assume we are dealing with a commutative isotope $\mathcal{R}$ of a semifield in which $a \star x = ax$ for all $x \in \mathcal{R}$ and $a \in \mathcal{N}_m$; that is to say precisely the type of isotope considered in Theorem 3.1. Our motivation for doing so stems from the results of [4], where it is shown that dealing with a commutative semifield of odd order is equivalent to dealing with a planar DO polynomial over the finite field of the same order. To summarise, for the remainder of this article

> $\mathcal{R}_f$ denotes a commutative semifield of order $q^n$ (where $q = p^e$, $p$ an odd prime), with middle nucleus $\mathbb{F}_q$, in which $a \star x = ax$ for all $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$. By Theorem 3.1, $x \star y = K(t(x), t(y)) + xy$ for all $x, y \in \mathbb{F}_{q^n}$, where $K \in \mathbb{F}_{q^n}[X, Y]$ is as outlined in Theorem 3.1. The corresponding reduced planar DO polynomial is $f(X) = \frac{1}{2}(X \star X)$ and we write $\mathcal{R}_f$ to underline the correspondence between the commutative semifield and the planar DO polynomial

Des. Codes Crytogr. 44 (2007), 275-286

$f$ which defines it. In all statements involving $\mathcal{R}_f$ the parameters just described are assumed.

We will use the following lemma frequently. The proof is straightforward.

**Lemma 4.1.** *For any commutative semifield $\mathcal{R}$, the left (and therefore right) nucleus of $\mathcal{R}$ is contained in the middle nucleus. Moreover, $k$ divides $e$ where $|\mathcal{N}_l| = |\mathcal{N}_r| = p^k$ and $|\mathcal{N}_m| = p^e$.*

We now turn to the implications of Theorem 3.1 to commutative semifields. We begin with

**Theorem 4.2.** *If the commutative semifield $\mathcal{R}_f$ has left nucleus $\mathbb{F}_{p^k}$ with $k|e$, then the bivariate polynomial $K(X,Y)$ by which $f(X)$ is defined is symmetric in $X$ and $Y$ and every term of $K$ is of the shape $a_{ij}X^{p^{ki}}Y^{p^{ki}}$.*

*Proof.* Following the notation of Theorem 3.1 set

$$K(X,Y) = \sum_{i,j=0}^{(n-1)e-1} a_{ij}X^{p^i}Y^{p^j}.$$

As $\mathcal{R}_f$ is commutative, we have

$$K(t(x),t(y)) = K(t(y),t(x)) \tag{1}$$

for all $x, y \in \mathbb{F}_{q^n}$. In fact, for each $y \notin \mathbb{F}_q$ we have $K(t(X),t(y)) = K(t(y),t(X))$ as polynomials and we can thus equate coefficients. Now

$$\begin{aligned} K(t(X),t(y)) &= \sum_{i,j=0}^{n-1-e} a_{ij}t(X)^{p^i}t(y)^{p^j} \\ &= \sum_{i,j=0}^{n-1-e} a_{ij}t(y)^{p^j}(X^{p^{i+e}} - X^{p^i}) \\ &= \sum_{i=0}^{e-1} X^{p^i}\left(-\sum_{j=0}^{n-1-e} a_{ij}t(y)^{p^j}\right) \\ &\quad + \sum_{i=e}^{n-1-2e} X^{p^i}\left(\sum_{j=0}^{n-1-e}(a_{(i-e)j} - a_{ij})t(y)^{p^j}\right) \\ &\quad + \sum_{i=n-2e}^{n-1-e} X^{p^i}\left(\sum_{j=0}^{n-1-e} a_{ij}t(y)^{p^j}\right). \end{aligned}$$

Setting $B_i(X) = \sum_{j=0}^{n-1-e} a_{ij}X^{p^j}$ we obtain

$$\begin{aligned} K(t(X),t(y)) = \sum_{i=0}^{e-1} -B_i(t(y))X^{p^i} + \sum_{i=n-2e}^{n-1-e} B_i(t(y))X^{p^i} \\ + \sum_{i=e}^{n-1-2e}\big(B_{i-e}(t(y)) - B_i(t(y))\big)X^{p^i}. \end{aligned}$$

Likewise, we have

$$K(t(y), t(X)) = \sum_{i=0}^{e-1} -C_i(t(y))X^{p^i} + \sum_{i=n-2e}^{n-1-e} C_i(t(y))X^{p^i} + \sum_{i=e}^{n-1-2e} \big(C_{i-e}(t(y)) - C_i(t(y))\big)X^{p^i},$$

where $C_i(X) = \sum_{j=0}^{n-1-e} a_{ji}X^{p^j}$. Equating coefficients in (1) for all $y \in \mathbb{F}_{q^n}$ reveals $B_i(t(X)) = C_i(t(X))$ for all $i \in \{0, 1, \ldots, n-e-1\}$. Expanding much as above and equating coefficients we immediately have $a_{ij} = a_{ji}$ for any $i$ with $0 \le j \le e-1$ and $n-2e \le j \le n-1-e$. On the other hand for any $i$ and $e \le j \le n-1-2e$ we have $a_{i\,(j-e)} - a_{ij} = a_{(j-e)\,i} - a_{ji}$. Strong induction on $j$ for $e \le j \le n-1-2e$ now yields the remaining cases, so that $a_{ij} = a_{ji}$ for all $i, j$ and $K$ is indeed symmetric.

It remains to prove $K(X, Y)$ is a $p^k$-polynomial in both $X$ and $Y$. Since $K$ is symmetric, we need only prove this for $X$. For any $\alpha \in \mathbb{F}_{p^k} \subseteq \mathcal{N}_l$ we have $\alpha \star (X \star y) = (\alpha \star X) \star y$ for all $y \in \mathbb{F}_{q^n}$. Now

$$\alpha \star (X \star y) = \alpha yX + \alpha K(t(X), t(y)) + K(t(\alpha), t(yX)) + K(t(\alpha), t(K(t(X), t(y)))),$$

while

$$(\alpha \star X) \star y = \alpha yX + yK(t(X), t(\alpha)) + K(t(y), t(\alpha X)) + K(t(y), t(K(t(X), t(\alpha)))).$$

By Lemma 4.1 we know $\alpha \in \mathcal{N}_m$ and so $t(\alpha) = 0$. Fixing $y \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ and equating we find $\alpha K(t(X), t(y)) = K(t(\alpha X), t(y))$ holds for all $\alpha \in \mathbb{F}_{p^k}$. Setting $L_y(X) = K(t(X), t(y)) = \sum_j b_j X^{p^j}$ yields $\alpha^{p^j} = \alpha$ whenever $b_j \neq 0$. Since this holds for all $\alpha \in \mathbb{F}_{p^k}$, it follows that $L_y$ is a $p^k$-polynomial. Hence $K(X, Y)$ is a $p^k$-polynomial in $X$. □

Since any nuclei of any commutative semifield must contain an isotopic copy of $\mathbb{F}_p$ our result always holds for $t(X) = X^p - X$, that is when $e = k = 1$.

It is tempting to conclude from Theorem 4.2 that every planar DO polynomial $f$ describing a commutative semifield $\mathcal{R}_f$ must be of the special form $f(X) = L(t^2(X)) + \frac{1}{2}X^2$. In fact this is not the case. We illustrate with a counterexample. Take $f(X) = X^{10} + X^6 - X^2$. This polynomial is planar over $\mathbb{F}_{p^e}$ if and only if $p = 3$ and either $e = 2$ or is odd, see Coulter and Matthews [5]. For the case $p = 3, e = 5$, it is easy to compute an isotope satisfying $a \star x = ax$ for all $x \in \mathbb{F}_{3^5}$ and $a \in \mathbb{F}_3$. However, the planar DO polynomial corresponding to this isotope is $f(X) = M(t(X))N(t(X)) + \frac{1}{2}X^2$, where $t(X) = X^3 - X, M(X) = -X^9 + X^3 - X$ and $N(X) = X^{27} + X^9 - X^3$. This yields $K(X, Y) = M(X)N(Y) + M(Y)N(X)$ with $K(X, X) \neq L(X^2)$ for any linearised polynomial $L \in \mathbb{F}_{3^5}[X]$. We can, however, determine the shape of the planar DO polynomials describing the commutative semifields $\mathcal{R}_f$.

**Theorem 4.3.** *If the commutative semifield $\mathcal{R}_f$ has left nucleus $\mathbb{F}_{p^k}$ with $k|e$ and either $e = 1$ and $n = 2$, or $e > 1$ and $n$ arbitrary, then*

$$f(X) = L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2, \quad (2)$$

*where* $L \in \mathbb{F}_{q^n}[X]$ *is a linearised polynomial and* $D \in \mathbb{F}_{q^n}[X]$ *is a Dembowski-Ostrom polynomial of the shape*

$$D(X) = \sum_{j=0}^{[e/k]-1} \sum_{i=1}^{n-2} c_{ji} \left(X^{q^i+1}\right)^{p^{jk}}.$$

*Conversely, any planar polynomial* $f$ *of the shape (2) defines a commutative semifield* $\mathcal{R}$ *with* $x \star y = f(x+y) - f(x) - f(y)$ *and where the middle nucleus contains* $\mathbb{F}_q$ *and the left nucleus contains* $\mathbb{F}_{p^k}$.

*Proof.* If $f(X) = L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2$ is planar over $\mathbb{F}_{q^n}$ and $L$ and $D$ are of the claimed form, then clearly $\mathbb{F}_q \subseteq \mathcal{N}_m(\mathcal{R})$ and $\mathbb{F}_{p^k} \subseteq \mathcal{N}_l(\mathcal{R})$.

Now suppose $\mathcal{R}_f$ has left nucleus $\mathbb{F}_{p^k}$. By Theorem 4.2 we may write $K(X,Y)$ as

$$K(X,Y) = \sum_{i=0}^{[(n-1)e/k]-1} a_i (XY)^{p^{ik}} + \sum_{0 \le i < j < (n-1)e/k} b_{ij} (X^{p^{ik}} Y^{p^{jk}} + X^{p^{jk}} Y^{p^{ik}}).$$

If $e = 1$ and $n = 2$, then the second sum is zero and we are done. For the remainder let $e > 1$. For any $\alpha \in \mathbb{F}_q$ we have $\alpha X \star Y = X \star \alpha Y$. In particular $K(t(\alpha X), t(Y)) = K(t(X), t(\alpha Y))$. Equating coefficients and gathering terms we find

$$\sum_{0 \le i < j < (n-1)e/k} b_{ij} (\alpha^{p^{ik}} - \alpha^{p^{jk}})(t(X)^{p^{ik}} t(Y)^{p^{jk}} - t(X)^{p^{jk}} t(Y)^{p^{ik}}) = 0.$$

The left hand side of this equation is a bivariate polynomial over $\mathbb{F}_{q^n}$ of degree less than $q^n$ in each variable (in fact, the total degree is less than $q^n$), and for this to be the zero polynomial we can only conclude $b_{ij} = 0$ whenever $e$ does not divide $k(j-i)$. Hence

$$K(X,Y) = \sum_{i=0}^{[(n-1)e/k]-1} a_i (XY)^{p^{ik}} + \sum_{j=0}^{[e/k]-1} \sum_{i=1}^{n-2} c_{ji} \left(X^{q^i} Y + X Y^{q^i}\right)^{p^{jk}},$$

from which the claimed shape for $f(X)$ now follows. □

Note that for $n = 2$ we find the corresponding DO polynomial is exactly of the special form $L(t^2(X)) + \frac{1}{2}X^2$.

## 5. On Isotopy for Commutative Semifields

One of the main problems with commutative semifields is distinguishing between non-isotopic examples. We now consider the problem for the specific commutative semifields $\mathcal{R}_f$. Our first result establishes restrictions on the possible strong isotopisms between any two such commutative semifield isotopes.

**Theorem 5.1.** *Suppose* $\mathcal{R}_f$ *and* $\mathcal{R}_h$ *are strongly isotopic with a strong isotopism given by* $(N, N, M)$ *where* $M, N$ *are linearised permutation polynomials over* $\mathbb{F}_{q^n}$. *Then*

$$N(X) = \left(\sum_{i=0}^{n-1} n_i X^{q^i}\right)^{p^k}$$

*for some integer* $0 \le k < e$ *and* $M(X) \equiv N(1) \star N(X) \pmod{X^{q^n} - X}$.

Des. Codes Crytogr. 44 (2007), 275-286

*Proof.* By assumption $a \circ x = ax$ and $a \star x = ax$ for all $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$. Also, $M(a \circ b) = N(a) \star N(b)$ for all $a, b \in \mathbb{F}_{q^n}$. In particular, $M(x \circ 1) = M(x) = N(x) \star N(1)$ for all $x \in \mathbb{F}_{q^n}$ and so $M(X) \equiv N(1) \star N(X) \pmod{X^{q^n} - X}$.

Let $\beta \in \mathbb{F}_{q^n}$ satisfy $N(\beta) = 1$, so that $M(x \circ \beta) = N(x) \star N(\beta) = N(x)$ for all $x \in \mathbb{F}_{q^n}$. For $a \in \mathbb{F}_q$ and any $x, y \in \mathbb{F}_{q^n}$ we have

$$\begin{aligned} N(x) \star N(ay) &= M(x \circ ay) \\ &= M(xa \circ y) \\ &= N(ax) \star N(y). \end{aligned}$$

In particular, $N(ax) = N(x) \star N(a\beta)$. It follows that

$$\begin{aligned} N(x) \star N(ay) &= N(x) \star (N(a\beta) \star N(y)) \\ &= (N(x) \star N(a\beta)) \star N(y) = N(ax) \star N(y) \end{aligned}$$

for all $a \in \mathbb{F}_q$ and $x, y \in \mathbb{F}_{q^n}$. Hence $N(a\beta) \in \mathcal{N}_m(\mathcal{R}_h) = \mathbb{F}_q$ for all $a \in \mathbb{F}_q$. It now follows that $N(ax) = N(a\beta)N(x)$ for all $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$, and since $N$ is a reduced linearised permutation polynomial, we have $N(aX) = N(a\beta)N(X)$ for all $a \in \mathbb{F}_q$. Set $N(X) = \sum_{i=0}^{ne-1} n_i X^{p^i}$ with $n_i \in \mathbb{F}_{q^n}$. Equating coefficients yields the system of equations

$$n_j a^{p^j} = n_j N(a\beta)$$

for all $a \in \mathbb{F}_q$ and $0 \leq j < ne$. Either $N(X) = n_k X^{p^k}$ for some integer $k$, in which case $N$ is certainly in the form claimed, or $N$ has at least two non-zero coefficients. Take any two such coefficients $n_k$ and $n_l$ with $k < l$ and $n_k n_l \neq 0$. Then we may cancel the $n_k$ and $n_l$ in the equations corresponding to $n_k a^{p^k}$ and $n_l a^{p^l}$ and find

$$a^{p^k} = N(a\beta) = a^{p^l},$$

for all $a \in \mathbb{F}_q$. It follows that $e$ divides $l - k$ and since this holds for any two non-zero coefficients of $N$, we can only have $N$ in the form claimed. □

We return to our examination of planar DO polynomials of the shape $f(X) = L(t^2(X)) + \frac{1}{2}X^2$ by considering the situation where such polynomials yield an isotope of a finite field.

**Theorem 5.2.** *Consider the commutative semifield $\mathcal{R}_f$ with $f(X) = L(t^2(X)) + \frac{1}{2}X^2$, $L \in \mathbb{F}_{q^n}[X]$ a linearised polynomial. If $L(X) = aX$ with $a \neq 0$, then $\mathcal{R}_f$ is isotopic to $\mathbb{F}_{q^n}$. Conversely, if $\mathcal{R}_f$ is isotopic to $\mathbb{F}_{q^n}$, then $L$ is a $q$-polynomial.*

*Proof.* Suppose $L(X) = aX$ with $a \in \mathbb{F}_{q^n}$. Consider the two equations associated with the middle nucleus of $\mathcal{R}_f$:

$$x \star (\alpha \star y) = x\alpha y + 2xL(t(\alpha)t(y)) + 2L(t(x)t(\alpha y)) + 4L(t(x)L(t(\alpha)t(y))), \quad (3)$$

$$(x \star \alpha) \star y = x\alpha y + 2yL(t(\alpha)t(x)) + 2L(t(y)t(\alpha x)) + 4L(t(y)L(t(\alpha)t(x))). \quad (4)$$

For any $\alpha \in \mathbb{F}_q$, $t(\alpha) = 0$. So $(x \star \alpha) \star y = x \star (\alpha \star y)$ for all $x, y \in \mathbb{F}_{q^n}$ and we have $\mathbb{F}_q \subseteq \mathcal{N}_m$. Next consider $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. Let $t(\alpha) = \beta \neq 0$. Now $t(\alpha x) = \alpha t(x) + \beta x^q$. Returning to (3) and (4), we have

$$x \star (\alpha \star y) = \alpha xy + 2a\beta x t(y) + 2a\alpha t(x)t(y) + 2a\beta y^q t(x) + 4a^2\beta t(x)t(y),$$

$$(x \star \alpha) \star y = \alpha xy + 2a\beta y t(x) + 2a\alpha t(x)t(y) + 2a\beta x^q t(y) + 4a^2\beta t(x)t(y).$$

Now

$$xt(y) + y^q t(x) = yt(x) + x^q t(y) \quad (5)$$

holds for all $x, y \in \mathbb{F}_{q^n}$ and it is easily observed that this is equivalent to $(x \star \alpha) \star y = x \star (\alpha \star y)$ holding for all $x, y \in \mathbb{F}_{q^n}$. Since (5) is not dependent on $\alpha$, it follows that $\mathbb{F}_{q^n} \subseteq \mathcal{N}_m$ and so $\mathcal{R}_f$ is isotopic to $\mathbb{F}_{q^n}$.

Now suppose $\mathcal{R}_f$ is isotopic to $\mathbb{F}_{q^n}$. Then returning to (3) and (4) let us fix $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ with $t(\alpha) = \beta \neq 0$. Equating, we find in particular that for $y \in \mathbb{F}_q$ we have

$$L(y\beta t(X)) = yL(\beta t(X)).$$

Setting $L(X) = \sum_i a_i X^{p^i}$ and recalling $L$ is reduced, we can equate coefficients and find $y^{p^i} = y$ whenever $a_i \neq 0$. Since this holds for all $y \in \mathbb{F}_q$, we conclude $L$ is a $q$-polynomial. □

We note in particular the implications of this result for the case $n = 2$, where the shape of $f(X)$ assumed in Theorem 5.2 is forced by Theorem 4.3.

**Corollary 5.3.** *Let $\mathcal{R}_f$ be a commutative semifield of order $q^2$, so that $f(X) = L(t^2(X)) + \frac{1}{2}X^2$ where $L \in \mathbb{F}_{q^2}[X]$ is a linearised polynomial. Then $\mathcal{R}_f$ is isotopic to $\mathbb{F}_{q^2}$ if and only if $L(X) = aX$ with $a \neq 0$.*

*Proof.* Given Theorem 5.2, we need only show $L$ is linear if $\mathcal{R}_f$ is isotopic to $\mathbb{F}_{q^2}$. However, since $f(X) = L(t^2(X)) + \frac{1}{2}X^2$ has degree less than $q^2$, we see

$$\mathrm{Deg}(L(t^2)) = 2q\,\mathrm{Deg}(L) < q^2.$$

Hence $\mathrm{Deg}(L) < q$ and since $L$ is a $q$-polynomial, the result now follows. □

We end this paper with an illustration of the effectiveness of Theorem 4.2. To our knowledge, there is no example known of a commutative semifield of order $3^8$ with left nucleus of order 3 and middle nucleus of size $3^2$. Set $L(X) = X^{243} + X^9$ and $D(X) = X^{246} + X^{82} - X^{10}$, and consider the polynomial $f(X) = L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2$, where $t(X) = X^9 - X$. Using the Magma algebra package [3], it is easy to check $f(X)$ is planar over $\mathbb{F}_{3^8}$ and so yields a commutative semifield $\mathcal{R}_f$ of order $3^8$ with left nucleus of order at least 3 and middle nucleus of order at least $3^2$. Again, a little computing in Magma shows the left and middle nuclei are $\mathbb{F}_3$ and $\mathbb{F}_9$, respectively. We note that present geometric techniques work well when considering commutative semifields of dimension two over one of the nuclei; however they have so far proved to be less effective when the dimension is larger.

## References


1. A. Barlotti, *Le possibili configurazioni del sistema delle coppie punto-retta $(A, a)$ per cui un piano grafico risulta $(A, a)$-transitivo*, Boll. Un. Mat. Ital. **12** (1957), 212–226.
2. A. Blokhuis, R.S. Coulter, M. Henderson, and C.M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite Fields and Applications: proceedings of the Fifth International Conference on Finite Fields and Applications (D. Jungnickel and H. Niederreiter, eds.), 2001, pp. 37–42.
3. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.
4. R.S. Coulter and M. Henderson, *Commutative presemifields and semifields*, Adv. Math., to appear.
5. R.S. Coulter and R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167–184.
6. P. Dembowski and T.G. Ostrom, *Planes of order $n$ with collineation groups of order $n^2$*, Math. Z. **103** (1968), 239–258.
7. L.E. Dickson, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc **7** (1906), 514–522.

8. M. Hall, *Projective planes*, Trans. Amer. Math. Soc. **54** (1943), 229–277.
9. M. Henderson and R. Matthews, *Composition behaviour of sub-linearised polynomials over a finite field*, Finite Fields: Theory, Applications and Algorithms (R.C. Mullin and G.L. Mullen, eds.), Contemporary Mathematics, vol. 225, American Mathematical Society, 1999, pp. 67–75.
10. J. Hsiang, D.F. Hsu, and Y-P. Shieh, *On the hardness of counting problems of complete mappings*, Discrete Math. **277** (2004), 87–100.
11. W.M. Kantor, *Commutative semifields and symplectic spreads*, J. Algebra **270** (2003), 96–114.
12. D.E. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217.
13. H. Lenz, *Zur Begründung der analytischen Geometrie*, S.-B. Math.-Nat. Kl. Bayer. Akad. Wiss. (1954), 17–72.
14. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).
15. O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559–584, Errata, *ibid.* **36**, 275 (1934).
16. ———, *Theory of non-commutative polynomials*, Annals of Math. **34** (1933), 480–508.
17. ———, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. **36** (1934), 243–274.
18. K.H. Parshall, *In pursuit of the finite division algebra theorem and beyond: Joseph H. M. Wedderburn, Leonard E. Dickson, and Oswald Veblen*, Arch. Internat. Hist. Sci. **33** (1983), 274–299.
19. T.P. Vaughan, *Polynomials and linear transformations over finite fields*, J. reine Angew. Math **267** (1974), 179–206.
20. J.H.M. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), 349–352.

[R.S. Coulter & P. Kosick] Department of Mathematical Sciences, Ewing Hall, University of Delaware, Newark, DE, 19716, U.S.A.

[M. Henderson] 310/60 Willis St., Te Aro (Wellington) 6011, New Zealand