Planar polynomials and commutative semifields two dimensional over their middle nucleus and four dimensional over their nucleus

Robert Coulter[*1], **Marie Henderson**[2], **Lei Hu**[3], **Pamela Kosick**[4], **Qing Xiang**[1], and **Xiangyong Zeng**[5]

[1] Department of Mathematical Sciences, Ewing Hall, University of Delaware, Newark, Delaware, 19716, U.S.A.
[2] 9/84a Boulcott St., Te Aro (Wellington) 6001, New Zealand.
[3] The State Key Laboratory of Information Security, Graduate School of Chinese Academy of Science, Beijing, 100049, China.
[4] Natural Sciences and Mathematics, The Richard Stockton College of New Jersey, PO Box 195, Pomona, NJ, 08240, USA
[5] Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China.

1 Introduction and overview

A *semifield* $\mathcal{R}$ is a not necessarily associative ring with no zero-divisors, a multiplicative identity and left and right distributive laws. A semifield which is not a field is called *proper*. If a multiplicative identity is not insisted upon, then we talk of *presemifields*. It is an easy exercise to show any finite semifield must have prime power order, and as with finite fields we shall refer to the prime involved as the *characteristic* of the semifield. The study of semifields is largely motivated by their equivalence to projective planes of Lenz-Barlotti class V.1, see Dembowski [5]. Since associativity is not assumed, it is reasonable to ask how near $\mathcal{R}$ is to being associative. To this end one defines the *left, middle and right nucleus* of $\mathcal{R}$, denoted by $\mathcal{N}_l, \mathcal{N}_m$ and $\mathcal{N}_r$, respectively, as follows:

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

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 $\mathcal{R}$. It is clear the nuclei provide some measure of how far $\mathcal{R}$ is from being associative. Additionally, as Knuth observed [8], $\mathcal{R}$ can be represented as a right vector space over $\mathcal{N}_l$, a left vector space over $\mathcal{N}_r$ and both a left and right vector space over $\mathcal{N}_m$. In the commutative case it can be shown $\mathcal{N}_l = \mathcal{N}_r \subseteq \mathcal{N}_m$, so that we need only talk of the middle nucleus and the nucleus.

The recently described equivalence of commutative presemifields of odd order and planar Dembowski-Ostrom (DO) polynomials, see Coulter and Henderson [2], has exposed a gap in our knowledge of planar DO polynomials. There remain several classical classes of commutative semifields for which a corresponding class of planar DO polynomial representatives is not known. Even in the case of the semifields of Dickson [6], the first proper semifields known and arguably the most fundamental, there is no known corresponding planar DO polynomial.

This article is a first step in rectifying this imbalance: we introduce a class of planar DO polynomials describing a commutative semifield of dimension two over its middle nucleus and dimension four over its nucleus. The bound given by Ball and Lavrauw [1, Corollary 2] shows any such commutative semifield must be isotopic to a finite field or a Dickson semifield. Since Dickson's construction yields only one such commutative semifield, we therefore fill this gap in our knowledge of planar DO polynomials in this case. We give a further class of planar DO polynomials which yield this Dickson semifield when the nucleus has order congruent to 1 modulo 4. This second class consists of binomials, therefore providing a simpler form of planar DO polynomial representative when $|\mathcal{N}(\mathcal{R})| \equiv 1 \pmod 4$ than that provided by our main theorem. This may be of some use for isotopy questions using the method developed in [2].

[*] Rejected in 2007, and later superseded by other articles by various authors

2 Background results and notation

Let $\mathbb{F}_q$ denote the finite field of q elements, where q is the power of an odd prime, and $\mathbb{F}_q[X]$ denote the ring of polynomials over $\mathbb{F}_q$. We use $\mathbb{F}_q^*$ to denote the set of non-zero elements of $\mathbb{F}_q$. If $q = r^2$ for some prime power r, then it is well known $\mathbb{F}_r = S_1 \cup S_2$, where

$$\begin{aligned} S_1 &= \{z + z^{-1} \,:\, z \in \mathbb{F}_q \text{ and } z^{r-1} = 1\}, \\ \text{and } S_2 &= \{z + z^{-1} \,:\, z \in \mathbb{F}_q \text{ and } z^{r+1} = 1\}. \end{aligned}$$

Moreover, $S_1 \cap S_2 = \{2, -2\}$. If $q = r^n$, then the trace mapping $\mathrm{Tr}_{q/r} : \mathbb{F}_q \to \mathbb{F}_r$ is defined by

$$\mathrm{Tr}_{q/r}(x) = x + x^r + \cdots + x^{r^{n-1}}$$

for all $x \in \mathbb{F}_q$.

A polynomial $f \in \mathbb{F}_q[X]$ is a *permutation polynomial* over $\mathbb{F}_q$ if it induces a bijective map from $\mathbb{F}_q$ to itself under evaluation. The polynomial f is called *planar* over $\mathbb{F}_q$ if the polynomial $f(X + a) - f(X) - f(a)$ is a permutation polynomial for all $a \in \mathbb{F}_q^*$. A *Dembowski-Ostrom* (DO) polynomial is a polynomial $D \in \mathbb{F}_q[X]$ of the shape

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

For commutative semifields of odd order there is an equivalent representation in terms of planar Dembowski-Ostrom polynomials over finite fields. Any commutative presemifield $\mathcal{R} = (\mathbb{F}_q, +, \star)$ of odd order q is equivalent to a planar DO polynomial $f \in \mathbb{F}_q[X]$ with the field addition and the multiplication in $\mathcal{R}$ given by $x \star y = f(x + y) - f(x) - f(y)$, see [2]. We underline the correspondence by talking of the commutative semifield $\mathcal{R}_f$. This correspondence was exploited by Coulter, Henderson and Kosick [3] to determine restrictions on the planar DO polynomials in terms of the nuclei of the corresponding commutative semifield. Most relevant to our considerations is the following.

Lemma 2.1 *Let $\mathcal{R}$ be a commutative semifield of order $q = r^2$ with middle nucleus of order at least $r = s^m$ and nucleus of order at least $s = p^k$, p an odd prime. Then there exists an isotope $\mathcal{R}_f$ of $\mathcal{R}$ with $f \in \mathbb{F}_q[X]$ a planar DO polynomial of the shape*

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

where $L = \sum_i a_i X^{s^i}$ and $t(X) = X^r - X$. Conversely, any planar DO polynomial of the shape (1) describes a commutative semifield with the given parameters. The commutative semifield $\mathcal{R}_f$ is isotopic to a finite field if and only if $Deg(L) = 1$.

The shape of f is a consequence of [3, Theorem 4.3], while the statement on equivalence to a finite field is [3, Corollary 5.3].

3 A planar polynomial representing a Dickson semifield

Although it is easy to generate specific examples, as mentioned earlier, there is no known planar polynomial class which represent any subclass of the Dickson semifields. We now introduce a new class of planar polynomials equivalent to the class of Dickson semifields of dimension two over their middle nucleus and four over their nucleus.

Theorem 3.1 *Let p be an odd prime, k an arbitrary positive integer, and set $s = p^k$, $r = s^2$ and $q = r^2$. Let $\alpha \in \mathbb{F}_p$ satisfy $\alpha = (-8)^{-1}$, $L(X) = X^s + X$ and $t(X) = X^r - X$. The polynomial*

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

is planar over $\mathbb{F}_q$.

Proof. We need to show

$$\begin{aligned} L_a(X) &= f(X+a) - f(X) - f(a) \\ &= 2\alpha L(t(a)t(X)) + aX \end{aligned}$$

is a permutation polynomial for all $a \neq 0$. Noting $t(a)^r = -t(a)$, for any $a \neq 0$ and $x \in \mathbb{F}_q$ we have

$$\begin{aligned} L(t(a)t(x)) &= t(a)t(x) + t(a)^s t(x)^s \\ &= t(a)(x^{s^2} - x) + t(a)^s(x^{s^3} - x^s) \\ &= -t(a)x - t(a)^{s^2} x^{s^2} - t(a)^s x^s - t(a)^{s^3} x^{s^3} \\ &= -\mathrm{Tr}_{q/s}(t(a)x). \end{aligned}$$

Now $L_a(X)$ is a p-polynomial and so is a permutation polynomial over $\mathbb{F}_q$ if and only if $x = 0$ is the only root of $L_a(X)$ in $\mathbb{F}_q$, see [9]. Fix $a \in \mathbb{F}_q^*$ and let $x \in \mathbb{F}_q$ be a root of $L_a(X)$. Since $\alpha \in \mathbb{F}_p$ and $\mathrm{Tr}_{q/s}(y) \in \mathbb{F}_s$ for all $y \in \mathbb{F}_q$, we must have $x = a^{-1}\beta$ with $\beta \in \mathbb{F}_s$. Hence

$$\begin{aligned} 0 &= -2\alpha \mathrm{Tr}_{q/s}(t(a)a^{-1}\beta) + \beta \\ &= \beta\left(-2\alpha \mathrm{Tr}_{q/s}(a^{r-1} - 1) + 1\right), \end{aligned}$$

so that $\beta = 0$ or $-2\alpha\mathrm{Tr}_{q/s}(a^{r-1} - 1) + 1 = 0$. Since $\beta = 0$ implies $x = 0$, to establish the theorem it remains to prove $-2\alpha\mathrm{Tr}_{q/s}(a^{r-1} - 1) + 1 \neq 0$ if $a \neq 0$.

Suppose $a \in \mathbb{F}_q^*$ satisfies $-2\alpha\mathrm{Tr}_{q/s}(a^{r-1} - 1) + 1 = 0$. Now

$$\begin{aligned} -2\alpha\mathrm{Tr}_{q/s}(a^{r-1} - 1) + 1 &= -2\alpha\mathrm{Tr}_{q/s}(a^{r-1}) - 2\alpha\mathrm{Tr}_{q/s}(-1) + 1 \\ &= -2\alpha\mathrm{Tr}_{q/s}(a^{r-1}) + 8\alpha + 1 \\ &= -2\alpha\mathrm{Tr}_{q/s}(a^{r-1}). \end{aligned}$$

Thus $\mathrm{Tr}_{q/s}(a^{r-1}) = 0$. Set $z = a^{r-1}$ and note $z^r = z^{-1}$. We therefore have

$$\begin{aligned} 0 &= z + z^s + z^{s^2} + z^{s^3} \\ &= (z + z^{-1}) + (z + z^{-1})^s \\ &= \mathrm{Tr}_{r/s}(z + z^{-1}). \end{aligned}$$

Now for $z = a^{r-1}$, we have $z^{r+1} = a^{q-1} = 1$, so that $z + z^{-1} \in S_2$. In addition we know $\mathrm{Tr}_{r/s}(z + z^{-1}) = 0$, so that

$$z^s + z^{-s} + z + z^{-1} = 0.$$

Multiplying through by z^s we find

$$0 = z^{2s} + z^{s+1} + z^{s-1} + 1 = (z^{s+1} + 1)(z^{s-1} + 1).$$

Thus $z^{s+1} = -1$ or $z^{s-1} = -1$. In either case we find $z^{r-1} = 1$, so that $z + z^{-1} \in S_1$. It follows that $z + z^{-1} \in \{2, -2\}$, in which case $\mathrm{Tr}_{r/s}(z + z^{-1}) \neq 0$, a contradiction. Hence there is no $a \in \mathbb{F}_q^*$ for which $-2\alpha\mathrm{Tr}_{q/s}(a^{r-1} - 1) + 1 = 0$, completing the proof. □

Corollary 3.2 *The commutative semifield $\mathcal{R}_f$, where f is as defined in Theorem 3.1, is isotopic to the Dickson semifield two dimensional over the middle nucleus and four dimensional over the nucleus.*

Proof. By [1], Corollary 2, the semifield $\mathcal{R}_f$ can only be isotopic to a finite field or a Dickson semifield. Now $f(X) = L(t^2(X)) + \frac{1}{2}X^2$ with $\mathrm{D}eg(L) > 1$, so Lemma 2.1 applies, showing $\mathcal{R}_f$ is not isotopic to the finite field. Since there is only one Dickson commutative semifield with the given parameters, the result now follows. □

4 A second class of planar polynomials

We now wish to introduce an additional class of planar polynomials. The following lemma will be needed. Though the result was given previously by Heden [7], we provide a proof for convenience.

Lemma 4.1 *Let $r \equiv 1 \pmod 4$ be an odd prime power, $q = r^2$, and g be a primitive element of $\mathbb{F}_q$. If $z = g^{e(r-1)}$, with $0 \le e < r+1$, then*

$$z + z^{-1} - 2 = \begin{cases} 0 & \text{if } e = 0, \\ \text{a square of } \mathbb{F}_r^* & \text{if } e \text{ is odd}, \\ \text{a non-square of } \mathbb{F}_r^* & \text{if } e \text{ is even}. \end{cases}$$

Proof. The case $e = 0$ is clear. By hypothesis, $z^{r+1} = 1$ so that $z + z^{-1} \in S_2$ and so $z + z^{-1} - 2 \in \mathbb{F}_r$. Set $y = g^{e(r-1)/2} \in \mathbb{F}_q$, so that $(y - y^{-1})^2 = z + z^{-1} - 2$. Clearly $z + z^{-1} - 2$ is a square in $\mathbb{F}_r^*$ if and only if $y - y^{-1} \in \mathbb{F}_r^*$. Now $(y - y^{-1})^r = y - y^{-1}$ if and only if $(y^{r+1} + 1)(y^{r-1} - 1) = 0$, so that $y^{r+1} = -1$ or $y^{r-1} = 1$. The former case forces e odd, while the latter case forces $e = (r+1)/2$, which is odd by hypothesis. □

Theorem 4.2 *Let p be an odd prime and $k \in \mathbb{N}$ satisfy $p^k \equiv 1 \pmod 4$. Set $s = p^k$, $r = s^2$, $q = r^2$ and let g be a primitive element of $\mathbb{F}_q$. If $u = g^{e(s-1)}$ with e odd, then the polynomial $\Omega_u(X) = X^{r+1} + uX^{2s}$ is planar over $\mathbb{F}_q$.*

Proof. We need to show

$$\begin{aligned} L_a(X) &= \Omega_u(X + a) - \Omega_u(X) - \Omega_u(a) \\ &= aX^r + 2ua^sX^s + a^rX \end{aligned}$$

is a permutation polynomial for all $a \in \mathbb{F}_q^*$. Fix $a \in \mathbb{F}_q^*$. Now $L_a(X) = a^{r+1}(Y^r + \omega Y^s + Y)$ where $Y = X/a$ and $\omega = 2ua^{-(s-1)^2}$. Setting $M_a(Y) = Y^r + \omega Y^s + Y$, we note $L_a(X)$ is a permutation polynomial if and only if $M_a(Y)$ is. By the discussion on pages 361–362 of [9], $M_a(Y)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $Det(A) \neq 0$, where

$$A = \begin{pmatrix} 1 & 0 & 1 & \omega^{s^3} \\ \omega & 1 & 0 & 1 \\ 1 & \omega^s & 1 & 0 \\ 0 & 1 & \omega^{s^2} & 1 \end{pmatrix}.$$

A short calculation shows

$$\begin{aligned} Det(A) &= \mathrm{Tr}_{q/s}(\omega^{s+1}) - \omega^{s^3+s^2+s+1} \\ &= 4\mathrm{Tr}_{r/s}(z + z^{-1} - 2), \end{aligned}$$

where $z = u^{s+1}a^{-(s-1)(r-1)} = g^{d(r-1)}$ with d odd. By Lemma 4.1, $z + z^{-1} - 2 = \beta^{2m}$ for some integer m and where β is a primitive element of $\mathbb{F}_r$. If $\mathrm{Tr}_{r/s}(\beta^{2m}) = 0$, then $\beta^{2m(s-1)} = -1 = \beta^{(r-1)/2}$, or equivalently,

$$2m(s-1) \equiv \frac{1}{2}(s-1)(s+1) \pmod{r-1}. \qquad (2)$$

Now $iu \equiv v \pmod n$ has a solution i if and only if $\gcd(u, n)$ divides v. However, $\gcd(2(s-1), r-1) = 2(s-1)$ does not divide $\frac{1}{2}(s-1)(s+1)$ as $(s+1)/2$ is odd by hypothesis. So m cannot satisfy (2) and $M_a(Y)$ is a permutation polynomial. Hence $\Omega_u(X)$ is planar over $\mathbb{F}_q$. □

It remains to show $\mathcal{R}_{\Omega_u}$ is isotopic to $\mathcal{R}_f$.

Theorem 4.3 *The commutative semifield $\mathcal{R}_{\Omega_u}$ is isotopic to $\mathcal{R}_f$, where f is as defined in Theorem 3.1.*

Proof. Set $L(X) = \Omega_u(X+1) - \Omega_u(X) - \Omega_u(1) = X^r + 2uX^s + X$. As Ω_u is planar, L is a permutation polynomial and so there exists a linearised polynomial $M(X) = aX^{rs} + bX^r + cX^s + dX$ such that $M(L(X)) \equiv X \pmod{X^q - X}$. An easy calculation shows

$$\begin{aligned} M(L(X)) \pmod{X^q - X} =& (a + c + 2u^r b)X^{rs} + (b + d + 2u^s c)x^r \\ &+ (a + c + 2ud)X^s + (b + d + 2u^{rs}a)X. \end{aligned}$$

Equating coefficients yields the system of equations

$$\begin{aligned} a + c &= -2u^r b \\ &= -2ud \\ b + d &= -2u^s c \\ &= 1 - 2u^{rs}a. \end{aligned}$$

Since M is a linearised permutation polynomial, $M(\Omega_u)$ is a planar polynomial (see [4, Theorem 2.3]). Set $h(X) = M(\Omega_u(X)) \pmod{X^q - X}$. Using the above system of equations, a short calculation shows

$$\begin{aligned} h(X) &= (a + c)X^{rs+s} + (b + d)X^{r+1} + u^{rs}aX^2 + u^s cX^{2r} + udX^{2s} + u^r bX^{2rs} \\ &= N(t(X)^2) + \frac{1}{2}X^2, \end{aligned}$$

where $N(X) = udX^s - \frac{b+d}{2}X$ and $t(X) = X^r - X$. Now $\mathcal{R}_h$ and $\mathcal{R}_{\Omega_u}$ are isotopic by [4, Theorem 5.2]. Lemma 2.1 tells us $\mathcal{R}_h$ is isotopic to a finite field if D$eg(N) = 1$ or $\mathcal{R}_f$ if D$eg(N) > 1$. But D$eg(N) = 1$ implies $d = 0$, which in turn yields a contradiction via the system of equations; on one hand we find $a = b = c = d = 0$, while $b + d = 1 - 2u^{rs}a$. So D$eg(N) = s$ and $\mathcal{R}_h$ is isotopic to $\mathcal{R}_f$. □

References

[1] S. Ball and M. Lavrauw, *Commutative semifields of rank 2 over their middle nucleus*, Finite Fields with Applications to Coding Theory, Cryptography and Related Areas (G.L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, eds.), Springer-Verlag, 2002, Proceedings of the Sixth International Conference on Finite Fields and Applications, Oaxaca, 2001, pp. 1–21.

[2] R.S. Coulter and M. Henderson, *Commutative presemifields and semifields*, Adv. Math. **217** (2008), 282–304.

[3] R.S. Coulter, M. Henderson, and P. Kosick, *Planar polynomials for commutative semifields with specified nuclei*, Des. Codes Cryptogr. **44** (2007), 275–286.

[4] R.S. Coulter and R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167–184.

[5] P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, Heidelberg, Berlin, 1968, reprinted 1997.

[6] L.E. Dickson, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc **7** (1906), 514–522.

[7] O. Heden, *On Bruen chains*, Discrete Math. **146** (1995), 69–96.

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

[9] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).