DEMBOWSKI-OSTROM POLYNOMIALS FROM DICKSON POLYNOMIALS

ROBERT S. COULTER AND REX W. MATTHEWS

Abstract. Motivated by several recent results, we determine precisely when $F_k(X^d, a) - F_k(0, a)$ is a Dembowski-Ostrom polynomial, where $F_k(X, a)$ is a Dickson polynomial of the first or second kind. As a consequence, we obtain a classification of all such polynomials which are also planar; all examples found are equivalent to previously known examples.

1. Introduction

Throughout p is an odd prime and $q = p^e$. We denote the finite field of q elements by $\mathbb{F}_q$ and adopt the convention $\mathbb{F}_q^*$ to mean the non-zero elements of the field. We use $\overline{\mathbb{F}}_q$ to denote the algebraic closure of $\mathbb{F}_q$. A polynomial f in indeterminate X over $\mathbb{F}_q$ is called a *permutation* polynomial of $\mathbb{F}_q$ if f induces a bijective map on $\mathbb{F}_q$ under evaluation. We recall that any linear transformation of $\mathbb{F}_q$, when viewed as a vector space over $\mathbb{F}_p$, can be represented by a *linearised polynomial* L – that is, a polynomial of the form $L(X) = \sum_i a_i X^{p^i}$. A linearised polynomial is a permutation polynomial over $\mathbb{F}_q$ precisely when its only root in $\mathbb{F}_q$ is 0.

The *Dickson polynomials of the first kind* (DPFK) and *Dickson polynomials of the second kind* (DPSK) are defined by

$$D_k(X, a) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i} \binom{k-i}{i} (-a)^i X^{k-2i}$$

$$E_k(X, a) = \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k-i}{i} (-a)^i X^{k-2i}$$

respectively, where $\lfloor k/2 \rfloor$ is the largest integer $\leq k/2$, and $a \in \mathbb{F}_q$. Dickson polynomials of the first and second kind have been studied extensively, see the monograph [13]. Their permutation behaviour has been a specific area of study. Nöbauer [15] proved $D_k(X, a)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $(k, q^2 - 1) = 1$. The permutation behaviour of the Dickson polynomials of the second kind remains unresolved and is certainly more complicated; for example, the behaviour is dependent on whether a is a square or non-square in $\mathbb{F}_q$. We refer the interested reader to the articles [3, 6, 10, 9, 11].

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

$$\sum_{i,j} a_{ij} X^{p^i + p^j}.$$

The authors named these polynomials in [5] in honour of Peter Dembowski and Ted Ostrom, whose seminal paper [7] on planar functions first identified these polynomials as significant objects in the study of particular projective planes. For $f \in \mathbb{F}_q[X]$, define the *difference operator of* f, denoted Δ_f, to be the bivariate polynomial

$$\Delta_f(X,Y) = f(X+Y) - f(X) - f(Y).$$

The polynomial $f \in \mathbb{F}_q[X]$ is defined to be *planar* over $\mathbb{F}_q$ if for each $y \in \mathbb{F}_q^*$, the polynomial $\Delta_f(X,y)$ is a permutation polynomial of $\mathbb{F}_q$. It is easy to verify that no polynomial can be planar in characteristic 2, and so we will restrict ourselves to odd characteristic in all that follows. A key characterisation of DO polynomials was given in [5, Theorem 3.2]: a polynomial f is a DO polynomial if and only if $\Delta_f(X,y)$ is a linearised polynomial in X for every $y \in \mathbb{F}_q^*$. Consequently, when considering the planarity of a DO polynomial, one needs only be concerned with the existence of roots (x,y) with $xy \neq 0$ of $\Delta_f(X,Y)$.

Qiu *et al* [16] have shown that the size of the image set on $\mathbb{F}_q^*$ of a planar polynomial over $\mathbb{F}_q$ must be at least $(q-1)/2$. It follows that for planar polynomials of the form $h(X^2)$, h must be injective on the non-zero squares of $\mathbb{F}_q$. In particular, any permutation polynomial h would satisfy this last condition (though $h(X^2)$ may not be planar, of course). Of particular interest are polynomials which are planar for infinitely many extensions of $\mathbb{F}_q$. Two such classes were described by the authors in [5]. One of these classes consists of DO polynomials. In fact it is easily described as $D_5(X^2,a)$, a class which gave rise to previously unknown projective planes, see [5, 4, 8]. These results led us to consider when $D_k(X^d,a) - D_k(0,a)$ is a DO polynomial (the subtraction of $D_k(0,a)$ is important only when k is even, as Dickson polynomials of the first kind have a non-zero constant term when k is even). We provide a complete description. Using similar methods, we also provide a complete description of when $E_k(X^d,a) - E_k(0,a)$ is a DO polynomial. Finally we determine the planarity of all DO polynomials found.

2. Dickson polynomials of the first kind

The following theorem provides a complete description of when $D_k(X^d,a) - D_k(0,a)$ is a Dembowski-Ostrom polynomial.

Theorem 2.1. *Let $q = p^e$ with p an odd prime and fix $a \in \mathbb{F}_q^*$. The polynomial $D_k(X^d,a) - D_k(0,a)$ is a Dembowski-Ostrom polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) $k = p^m$ *and* $d = p^n(p^\alpha + 1)$ *for non-negative integers* α, m, n.
(ii) $k = 2p^m$ *and* $d = p^n(p^\alpha + 1)/2$ *for non-negative integers* α, m, n.
(iii) $p = 3$, $k = 4p^m$ *and* $d = p^n$ *for non-negative integers* m, n.
(iv) $p = 3$, $k = 5p^m$ *and* $d = 2p^n$ *for non-negative integers* m, n.
(v) $p = 5$, $k = 3p^m$ *and* $d = 2p^n$ *for non-negative integers* m, n.

Proof. It is straightforward to check that each of the cases listed yield DO polynomials in all cases, and so we need only show the necessity of these cases to complete the proof.

Suppose $D_k(X^d,a) - D_k(0,a)$ is a DO polynomial over $\mathbb{F}_q$. We first simplify the problem. It is clear that DO polynomials are closed under left or right composition with X^p. Since $D_{kp}(X^d,a) = D_k^p(X^d,a)$, it follows that all cases reduce to the case where p does not divide k or d, and we shall assume this in all that follows.

If $k = 1$, then $D_k(X^d, a) - D_k(0, a) = X^d$, which is a DO polynomial provided $d = p^\alpha + 1$ with $\alpha \geq 0$; this corresponds to case (i). If $k = 2$, then $D_k(X^d, a) - D_k(0, a) = X^{2d}$, which is a DO polynomial provided $d = (p^\alpha+1)/2$; this corresponds to case (ii).

For the remainder, suppose $k \geq 3$. The two terms of largest degree in $D_k(X, a)$ are $X^k + (-a)kX^{k-2}$. Since $k \not\equiv 0 \bmod p$, $D_k(X, a)$ necessarily has at least two terms.

We shall deal with k even or odd separately, though the methods are similar.

Case 1 k **is even**

Then $D_k(X, a)$ has non-zero terms X^k and X^2. Hence $kd = p^\alpha + 1$ and $2d = p^\beta + 1$ for non-negative integers α, β. From $k \geq 4$ it follows that $\beta < \alpha$. The coefficient of X^{k-2} in $D_k(X, a)$ being non-zero, we have

$$p^\alpha + 1 - 2d = p^i + p^j$$

for some non-negative integers i, j. So $p^\alpha = p^\beta + p^i + p^j$. This is only possible if $p = 3$ and $\beta = i = j$, and so $\alpha = \beta + 1$. Thus $k(3^\beta + 1) = 2(3^{\beta+1} + 1)$. Since k is even, either $\beta = 0$ or $\beta|(\beta + 1)$, in which case $\beta = 1$. However, $\beta = 1$ implies $k = 5$, contrary to k even, and so $\beta = 0$. Thus $p = 3$, $d = 1$ and $k = 4$, which is (iii).

Case 2 k **is odd**

Then $D_k(X, a)$ has non-zero terms X^k and X. Hence $kd = p^\alpha + 1$ and $d = p^\beta + 1$ for non-negative integers α, β. From $k \geq 3$ it follows that $\beta < \alpha$. Note that since $(p^\beta + 1)|(p^\alpha + 1)$, we must $\beta = 0$ or $\beta|\alpha$ with α odd.

The coefficient of X^{k-2} in $D_k(X, a)$ being non-zero, we have

$$p^\alpha + 1 - 2d = p^i + p^j$$

for some non-negative integers i, j. So $p^\alpha = 2p^\beta + p^i + p^j + 1$. This implies $p = 3$ or $p = 5$.

When $p = 3$, we have $3^\beta|(1 + 3^i + 3^j)$. If $\beta > 0$, then $i = j = 0$ and $\beta = 1$ is forced. But then $\alpha = 2$, contrary to α odd. If $\beta = 0$, then $3^{\alpha-1} = 1 + 3^{i-1} + 3^{j-1}$, and so $i = j = 1$. This yields $\beta = 0$, $\alpha = 2$, which corresponds to (iv).

If $p = 5$ then $\beta = i = j = 0$ and so $\alpha = 1$. In this case, we deduce $d = 2$ and $k = 3$, which corresponds to (v).

□

3. Dickson polynomials of the second kind

Theorem 3.1. *Let $q = p^e$ with p an odd prime and fix $a \in \mathbb{F}_q^*$. The polynomial $E_k(X^d, a) - E_k(0, a)$ is a Dembowski-Ostrom polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) $k = 1$ *and* $d = p^n(p^\alpha + 1)$ *for non-negative integers* α, n.
(ii) $k = 2$ *and* $d = p^n(p^\alpha + 1)/2$ *for non-negative integers* α, n.
(iii) $k = 3$ *and either*
  (a) $p = 3$ *and* $d = p^n(p^\alpha + 1)$ *for non-negative integers* α, n*; or*
  (b) $p = 5$ *and* $d = 2p^n$ *for some non-negative integer* n.
(iv) $k = 4$, $p = 3$ *and* $d = p^n(p^\alpha + 1)/4$ *for non-negative integers* α, n *and* α *odd.*
(v) $k = 5$ *and either*

(a) $p = 3$ *and* $d = 2p^n$ *for non-negative integer* n*; or*
(b) $p = 5$ *and* $d = 2p^n$ *for non-negative integer* n*.*

(vi) $k = 6$ *and either*
(a) $p = 3$ *and* $d = p^n$ *for non-negative integer* n*; or*
(b) $p = 5$ *and* $d = p^n$ *for non-negative integer* n*.*

(vii) $k = 7$*,* $p = 3$ *and* $d = 4p^n$ *for non-negative integer* n*.*

(viii) $k = 9$*,* $p = 3$ *and* $d = 4p^n$ *for non-negative integer* n*.*

(ix) $k = 10$*,* $p = 3$ *and* $d = p^n$ *for non-negative integer* n*.*

(x) $k = 12$*,* $p = 3$ *and* $d = p^n$ *for non-negative integer* n*.*

Proof. Suppose $E_k(X^d, a) - E_k(0, a)$ is a DO polynomial over $\mathbb{F}_q$. We may assume p does not divide d, but $E_{kp}(X, a) \neq E_k^p(X, a)$ in general, so we can no longer assume p does not divide k. We know

$$kd = p^{\alpha+m} + p^m, \tag{1}$$

for some non-negative integers α, m where $k = p^m k'$ with $(p, k') = 1$. We deal with small cases of k separately.

Cases (i) and (ii) correspond to $k = 1$ and $k = 2$, and follow immediately from (1).

If $k = 3$, then $E_k(X, a) = X^3 - 2aX$. Hence $d = p^\beta + 1$, and so $3p^\beta + 3 = p^{\alpha+m} + p^m$ where $m = 1$ if $p = 3$ and if $p \neq 3$, $m = 0$ and $\alpha > \beta$. For $p = 3$, we find $\beta = \alpha$, and we obtain the first part of (iii). For $p \neq 3$, $3p^\beta + 2 = p^\alpha$ forces $p = 5$ and $\beta = 0$. Hence $d = 2$ and we have the second part of (iii).

If $k = 4$, then $E_k(X, a) - E_k(0, a) = X^4 - 3aX^2$. For $p = 3$, we have $d = (3^\alpha + 1)/4$ with α odd, which is (iv). For $p > 3$, we have $2d = p^\beta + 1$, where $\beta < \alpha$. Equation 1 now implies $2p^\beta + 1 = p^\alpha$, which can only hold if $p = 3$, contrary to $p > 3$. So no further cases arise for $k = 4$.

If $k = 5$, then $E_k(X, a) = X^5 - 4aX^3 + 3a^2X$. It follows that $m = 1$ if $p = 5$ and $m = 0$ otherwise. So $3d = p^{\beta+n} + p^n$ where $n = 1$ if $p = 3$ and if $p > 3$, $n = 0$ and $\alpha > \beta$. Now for $p = 3$ we find $d = 3^\beta + 1$, and combining with (1) now yields $5 \cdot 3^\beta + 4 = 3^\alpha$. This forces $\beta = 0$ and $\alpha = 2$, which is the first part of (v). When $p = 5$, (1) yields $d = 5^\alpha + 1$, and so $3 \cdot 5^\alpha + 2 = 5^\beta$. Then $\alpha = 0$ and $\beta = 1$ is forced, and we obtain the 2nd part of (v). For $p > 5$, $d = p^\gamma + 1$ follows from the linear term of $E_k(X, a)$, and now combining with (1) we obtain $5p^\gamma + 4 = p^\alpha$, which implies $p = 3$ or 5, contrary to $p > 5$.

If $k = 6$, then $E_k(X, a) - E_k(0, a) = X^6 - 5aX^4 + 6a^2X^2$. When $p = 3$, $m = 1$ and $4d = 3^\beta + 1$. In combination with (1) we find $\alpha = 0$, $\eta = 1$ is forced and so $d = 1$, establishing the first part of (vi). For $p \geq 5$ we have $m = 0$ and $2d = p^\beta + 1$ with $\beta < \alpha$. We now find $3p^\beta + 2 = p^\alpha$, which forces $p = 5$, $\beta = 0$ and $\alpha = 1$. This establishes the second part of (vi).

For the remainder let $k \geq 7$. The polynomial $E_k(X, a)$ has a term of degree

- $k - 2$ unless $k \equiv 1 \bmod p$;
- $k - 4$ unless $k \equiv 2, 3 \bmod p$.

Suppose $k \not\equiv 1, 2, 3 \bmod p$. Then

$$\begin{aligned} kd &= p^\alpha + 1, \\ (k-2)d &= p^\beta + 1, \\ (k-4)d &= p^{\gamma+n} + p^n, \end{aligned}$$

with $\alpha > \beta > \gamma + n$. In particular, $\alpha, \beta > 0$. This forces $2d = p^\alpha - p^\beta$ to be divisible by p, and so $p|d$, which is a contradiction. So $E_k(X^d, a) - E_k(0, a)$ cannot be a DO polynomial in this case.

Suppose $k \equiv 1 \bmod p$. We have

$$kd = p^\alpha + 1,$$
$$(k-4)d = p^{\beta+n} + p^n,$$

with $n = 0$ unless $p = 3$. We note $\alpha > \beta + n$. If $n = 0$, then $4d = p^\alpha - p^\beta$. This implies $\beta = 0$, as otherwise $p|d$. But then $(k-4)d = 2$, contradicting $k \geq 7$. So $n > 0$ and $p = 3$. It follows from the second equation that $k = t3^n + 4$ for some integer t, so that $td = 3^\beta + 1$. If $t > 2$, then

$$\begin{aligned} 2(3^\beta + 1) &> \frac{4}{t}(3^\beta + 1) \\ &= 3^\alpha + 1 - 3^{\beta+n} - 3^n. \end{aligned}$$

Hence

$$3^{\beta+1} \geq 2 \cdot 3^\beta + 1 > 3^\alpha - 3^{\beta+n} - 3^n.$$

But this is impossible with $\alpha > \beta + n$. So $t \in \{1, 2\}$. If $t = 1$, then $k = 3^n + 4$ and $d = 3^\beta + 1$ with $\beta \geq 1$ as $d \equiv 1 \bmod 3$. Substituting into our first equation we find

$$3^{\beta+n} + 3^n + 4 \cdot 3^\beta + 3 = 3^\alpha.$$

If $\beta < n$, then this means $4 \cdot 3^\beta + 3 \equiv 0 \bmod 3^n$, which is impossible. Similarly, if $\beta > n$, then $3^n + 3 \equiv 0 \bmod 3^\beta$, also impossible. Thus $\beta = n$, and now we obtain $3 \equiv 0 \bmod 3^\beta$, so that $\beta = 1$. This yields $\alpha = 3$, so that $k = 7$ and $d = 4$, corresponding to case (vii). If $t = 2$, then $2d = 3^\beta + 1$. Since $d \equiv 1 \bmod 3$, $\beta = 0$ is forced and $d = 1$. We then have $3^\alpha = 2 \cdot 3^n + 3$, and so $n = 1$ and $\alpha = 2$ follow. This yields $n = 10$ and $d = 1$, which is case (ix).

Suppose $k \equiv 2 \bmod p$. We have

$$kd = p^\alpha + 1,$$
$$(k-2)d = p^{\beta+n} + p^n,$$

with $n \geq 1$ and $\alpha > \beta + n$. So $k = p^n t + 2$ with $(t, p) = 1$ and $td = p^\beta + 1$. Since $t \geq 1$, we have

$$2(p^\beta + 1) \geq \frac{2}{t}(p^\beta + 1) = p^\alpha + 1 - p^{\beta+n} - p^n.$$

We rearrange this to obtain

$$2p^\beta + 1 + p^n + p^{\beta+n} \geq p^\alpha \geq p \cdot p^{\beta+n}.$$

Dividing through by $p^{\beta+n}$ we arrive at the inequality

$$\frac{2}{p^n} + \frac{1}{p^{\beta+n}} + \frac{1}{p^\beta} + 1 \geq p.$$

Since $n \geq 1$, this can only hold if $p = 3$, $\beta = 0$ and $n = 1$. Further, equality holds in that case, so that $t = 1$ must also hold. But then $k = 5$, contrary to $k \geq 7$. So $E_k(X^d, a) - E_k(0, a)$ cannot be a DO polynomial in this case.

Suppose $k \equiv 3 \bmod p$. If $p > 3$, then we have

$$kd = p^\alpha + 1,$$
$$(k-2)d = p^\beta + 1.$$

Since $k \geq 7$, $\beta \geq 1$ is forced. It follows that $p|d$, a contradiction. So $p = 3$. We now have

$$kd = 3^{\alpha+m} + 3^m,$$
$$(k-2)d = 3^\beta + 1,$$

with $m \geq 1$ and $\beta \geq 2$ as $k \geq 9$. We write $k = 3^m t$ and $d = (3^\alpha + 1)/t$ with $(t, 3) = 1$. It now follows from the second equation that $d \equiv 1 \bmod p$. If $\alpha = 0$, then $td = 2$ and so $d = 1$. The second equation then yields $2 \cdot 3^m = 3^\beta + 3$, implying $m = 1$ and $k = 6$, contradicting $k \geq 9$. Hence $\alpha \geq 1$ and $t \equiv 1 \bmod p$. Now $E_k(X, a)$ also has a term of degree $k - 8$ unless $k - 6 \equiv 0 \bmod 9$. However, since $k = 3^m t$ and $t \equiv 1 \bmod 3$, it is clear $k \not\equiv 6 \bmod 9$. We therefore have the additional equation

$$(k-8)d = 3^\gamma + 1. \tag{2}$$

It follows that $6d = 3^\beta - 3^\gamma$, which forces $\gamma = 1$. As $d \equiv 1 \bmod 3$, (2) now forces $d = 1$ and $k = 12$, or $d = 4$ and $k = 9$. Either possibility yields a DO polynomial. □

4. Planarity considerations

We now address the question of when the DO polynomials obtained in the previous sections give rise to planar functions. While the planarity of some of the DO polynomials arising in Theorems 2.1 and 3.1 are known, the majority of the examples, particularly those involving the Dickson polynomials of the second kind, have not previously been considered. The following facts will prove useful.

Proposition 4.1. *Let $f \in \mathbb{F}_q[X]$ be a DO polynomial. If $z \in \mathbb{F}_q^*$ satisfies $f(z) = 0$, then f is not planar over $\mathbb{F}_q$.*

The proof is immediate from the observation $\Delta_f(z, z) = 2f(z) = 0$, so that both 0 and z are roots of $\Delta_f(X, z)$. We shall also use the following result of Weil [17].

Proposition 4.2. *Let $q = p^e$ and suppose $f(X, Y)$ is absolutely irreducible over $\mathbb{F}_q$. Then the number N of $(x, y) \in \mathbb{F}_q^2$ with $f(x, y) = 0$ satisfies*

$$N \geq q - (d-1)(d-2)\sqrt{q} - d - 1,$$

where d is the total degree of f.

Let $F_k(X, a)$ be a Dickson polynomial of either kind. Then it follows from the definitions that, for any $b \in \mathbb{F}_q^*$, $b^{kd} F_k(X^d, a) = F_k((bX)^d, ab^{2d})$. It follows (see for example [5, Theorem 2.3]) that the planarity of $F_k(X^d, a)$ and $F_k(X^d, ab^{2d})$ is equivalent. We summarise with

Proposition 4.3. *Fix $k, d \in \mathbb{N}$. Set $a \in \mathbb{F}_q^*$ and let $F_k(X, a)$ be a Dickson polynomial of the first or second kind. Then $F_k(X^d, a)$ is planar equivalent over $\mathbb{F}_q$ to $F_k(X^d, ab^{2d})$ for any $b \in \mathbb{F}_q^*$.*

There is a further critical consequence of this relation on Dickson polynomials: in the algebraic closure , we may always choose $b \in \overline{\mathbb{F}}_q$ satisfying $ab^{2d} = 1$, so that the factorisations of $\Delta_{F_k(X^d,a)}$ and $\Delta_{F_k(X^d,1)}$ over $\overline{\mathbb{F}}_q$ are linearly related. Consequently, the absolutely irreducible factors of $\Delta_{F_k(X^d,a)}$ are of the same form for all non-zero a. We now proceed to consider the planarity of the various DO polynomials arising from Theorems 2.1 and 3.1.

Cases (i) and (ii) of both theorems correspond to DO monomials. The planar behaviour of $X^{p^{\alpha+n}+p^n}$ is well understood – it is planar over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd (see [5, Theorem 3.3]). Theorem 3.1 (iv) also produces DO monomials, but limited only to characteristic 3. Theorem 3.1 (iii)(a) is also connected to DO monomials – this case produces the DO polynomials $(X^3 + aX) \circ X^{3^\alpha+1} \circ X^{3^n}$. These are planar over $\mathbb{F}_{3^e}$ provided $X^{3^\alpha+1}$ is planar over $\mathbb{F}_{3^e}$ and $X^3 + aX$ is a permutation polynomial over $\mathbb{F}_{3^e}$. So this case yields planar DO polynomials if and only if $e/(\alpha, e)$ is odd and a is a square in $\mathbb{F}_{3^e}$.

Theorem 2.1 (iv) corresponds to the motivating examples mentioned at the beginning of this paper: $f(X) = D_5(X^2, a)$ is planar over $\mathbb{F}_{3^e}$ if and only if $e = 2$ or e is odd; the proof of [5, Theorem 3.4], though only given for $a = 1$, suffices as it argues based on the factorisation of Δ_f in $\overline{\mathbb{F}}_q$ (see the comments following Proposition 4.3).

For Theorem 2.1 (iii), let $q = 3^e$, fix $a \in \mathbb{F}_q^*$ and set $f(X) = D_4(X, a) - D_4(0, a) = X^4 - aX^2$. Now

$$\Delta_f(X, Y) = f(X + Y) - f(X) - f(Y) = XYh(X, Y)$$

where $h(X, Y) = X^2 + Y^2 + a$. Let $z \in \overline{\mathbb{F}}_q$ satisfy $z^2 = -a$. Then $(Y - z)|(Y^2 + a)$, and $Y^2 + a$ has no repeated factors. Eisenstein's criteria now states $h(X, Y)$ is absolutely irreducible. It follows from Proposition 4.2 that there are at least $q - 3$ solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ to this equation. At most four solutions (x, y) can be accounted for with $xy = 0$, and so when $q - 3 > 4$, there must be a root (x, y) of $h(X, Y)$ with $xy \neq 0$. But then $\Delta_f(X, y)$ is not a permutation polynomial and so $f(X)$ is not planar if $e > 1$. If $e = 1$, then $f(X) \equiv (1 - a)X^2 \bmod (X^3 - X)$, which is planar provided $a = 2$. So this case yields a planar polynomial if and only if $e = 1$ and $a = 2$.

Theorem 2.1 (v) and Theorem 3.1 (iii), (vi)(b) yield practically the same DO polynomial: $D_3(X^2, a) = X^6 + 2aX^2$, while $E_3(X^2, a) = X^6 - 2aX^2$ and $E_6(X, a) - E_6(0, a) = X^6 + a^2X^2$. Consequently, we deal with the planarity of $f(X) = X^6 + 2aX^2$, the analysis for the others may then be determined. Set $q = 5^e$. We have $\Delta_f(X, Y) = XYh(X, Y)$ where

$$h(X, Y) = X^4 + Y^4 - a.$$

Let $z \in \overline{\mathbb{F}}_q$ satisfy $z^4 = a$. Using the prime $Y - z$, Eisenstein's criteria shows that $h(X, Y)$ is absolutely irreducible. Appealing to Proposition 4.2, the number N of roots in $\mathbb{F}_q^2$ of $h(X, Y)$ satisfies

$$N \geq q - 6\sqrt{q} - 5.$$

Since at most eight roots of $h(X, Y)$ in $\mathbb{F}_q^2$ can be accounted for with $xy = 0$, there must be a root (x, y) of $h(X, Y)$ with $xy \neq 0$ provided

$$q - 6\sqrt{q} - 13 > 0,$$

which holds for all $e \geq 3$. If $e = 1$, then $f(X) \equiv (1 + 2a)X \bmod (X^5 - X)$, which is planar provided $1 + 2a \neq 0$ – i.e. $a \neq 2$. For $e = 2$, one computes the number N of solutions of $x^4 + y^4 = a$:

$$N = \begin{cases} 40 & \text{if } j = 0, \\ 0 & \text{if } j = 1, \\ 16 & \text{if } j = 2, \\ 32 & \text{if } j = 3, \end{cases}$$

where $a = g^{4i+j}$. It follows at once that $f(X)$ is planar over $\mathbb{F}_{25}$ if and only if $a = g^{4i+1}$ for some integer i.

We have completed the analysis of the planarity of all DO polynomials described by Theorem 2.1. Cases (v) through (x) of Theorem 3.1 remain to be considered. We consider them sequentially.

(v) For $k = 5$ we have two sub-cases. In either case, $d = 2$.

(a) $p = 3$: Set $f(X) = E_5(X^2, a) = X^{10} - aX^6$ and set $q = 3^e$. This polynomial is planar over $\mathbb{F}_q$ if and only if

$$\Delta_f(X, y) = yX^9 + ay^3X^3 + y^9X$$

is a permutation polynomial over $\mathbb{F}_q$ for all $y \in \mathbb{F}_q^*$. Now

$$\Delta_f(X, Y) = XYh(X, Y),$$

where $h(X, Y) = X^8 + Y^8 + aX^2Y^2$. The polynomial f is planar over $\mathbb{F}_q$ if and only if $h(X, Y)$ has no roots $(x, y) \in \mathbb{F}_q^*$. Now

$$h(X, XY) = X^8 \left(aY^2X^{-4} + (Y^8 + 1)\right).$$

Set $A(X, Y) = aY^2X^4 + (Y^8 + 1)$ and let $z \in \overline{\mathbb{F}}_q$ satisfy $z^8 = -1$. Then $(Y - z)|(Y^8 + 1)$, and $Y^8 + 1$ has no repeated factors. It follows from Eisenstein's criteria that $A(X, Y)$ is absolutely irreducible. By Proposition 4.2, the number N of solutions of $A(x, y) = 0$ satisfies

$$N \geq q - 42\sqrt{q} - 9.$$

At most eight of these solutions (x, y) satisfy $xy = 0$. Consequently, there exists a root $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ of $A(X, Y)$ provided

$$q - 42\sqrt{q} - 17 > 0.$$

This holds provided $e \geq 7$. But then, given such a solution $A(x, y) = 0$ with $xy \neq 0$, we have

$$h(x^{-1}, x^{-1}y) = x^{-8}A(x, y) = 0,$$

and so f is not planar over $\mathbb{F}_{3^e}$. Computation quickly shows f is never planar over $\mathbb{F}_q$ for any $a \in \mathbb{F}_q^*$ with $3 \leq e \leq 6$. For $e = 2$, the difference operator reduces to $ay^3X^3 - yX$, which is a permutation polynomial if and only if $N(ay^2) = N(a) \neq 1$.

(b) $p = 5$: Set $f(X) = E_5(X^2, a) = X^{10} + aX^6 - 2a^2X^2 = X^2(X^4 - a)(X^4 + 2a)$ and $q = 5^e$ with $e \geq 2$. If either a or $-2a$ is a fourth power in $\mathbb{F}_q$, then f has four non-zero roots. Consequently, f is not planar by Proposition 4.1 in those cases. These conditions coincide only when $4 \mid e$, so that whenever $4 \nmid e$, f is not planar for half the

possible choices for $a \in \mathbb{F}_q^*$. When $e = 3$, computation reveals f is in fact planar over $\mathbb{F}_{27}$ for all remaining choices of a.
Now let $e \geq 4$. We have $\Delta_f(X, Y) = XYh(X, Y)$, where

$$h(X, Y) = (2Y^4 + a)X^4 + aY^4 + a^2.$$

Let $z \in \overline{\mathbb{F}}_q$ satisfy $z^4 = -a$. Then $(Y - z)|(aY^4 + a^2)$ and $aY^4 + a^2$ has no repeated factors. By Eisenstein's criteria, $h(X, Y)$ is absolutely irreducible. Applying Proposition 4.2, the number N of solutions $(x, y) \in \mathbb{F}_q^2$ satisfying $h(x, y) = 0$ satisfies

$$N \geq q - 42\sqrt{q} - 9.$$

At most eight solutions can also satisfy $xy = 0$ and so provided $e \geq 5$, the polynomial $h(X, Y)$ has a root (x, y) with $xy \neq 0$. Hence f cannot be planar over $\mathbb{F}_q$ in such cases. Computation then shows there are no examples of planar polynomials arising from this case with $e = 4$ either.

(vi) For $k = 6$ we again have two sub-cases, but the $p = 5$ case has already been considered above. Set $p = 3$, $f(X) = E_6(X, a) - E_6(0, a) = X^6 + aX^4$ and $q = 3^e$ with $e \geq 2$. The difference operator for f is $\Delta_f(X, Y) = XYh(X, Y)$ with $h(X, Y) = aX^2 + aY^2 - X^2Y^2$. Set $A(X, Y) = X^2 + Y^2 - a^{-1}$. By our previous arguments for Theorem 2.1 (iii), we know $A(X, Y)$ has roots $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ for all $e \geq 2$. But then

$$h(x^{-1}, y^{-1}) = ax^{-2}y^{-2}A(x, y) = 0,$$

and so f is not planar for any $e \geq 2$.

(vii) $k = 7$, $d = 4$ and $p = 3$: Set $f(X) = E_7(X^4, a) = X^{28} + a^2X^{12} - a^3X^4$ and $q = 3^e$. This polynomial is never planar when e is even as then $4|(q-1)$, so that the order of the image set of f on $\mathbb{F}_q^*$ is at most $(q-1)/4$. Now suppose e is odd, so that -1 is a non-square in $\mathbb{F}_q$. If a is a non-square in $\mathbb{F}_q^*$, then since $(8, q - 1) = 2$, we may write $a = -b^8$ for some $b \in \mathbb{F}_q^*$. It is easily checked that $f(b) = 0$, so that f is not planar over $\mathbb{F}_{3^e}$ by Proposition 4.1.

Now suppose a is a square in $\mathbb{F}_{3^e}$ with e odd. Since $(4, q - 1) = 2$, Proposition 4.3 shows $E_7(X^4, a)$ is planar equivalent over $\mathbb{F}_{3^e}$ to $E_7(X^4, 1)$. Consequently, we need only consider the planarity of $f(X) = E_7(X^4, 1)$. We have $\Delta_f(X, Y) = XY(X^2 + Y^2)h(X, Y)$, where

$$h(X, Y) = \left(\sum_{i=0}^{12}(-1)^i X^{24-2i}Y^{2i}\right) - \left(\sum_{i=1}^{3}(-1)^i X^{8-2i}Y^{2i}\right) - 1.$$

Direct computation using the Magma algebra package [2] shows $h(X, Y)$ is absolutely irreducible. By Proposition 4.2, the number N of solutions $(x, y) \in \mathbb{F}_q^2$ with $h(x, y) = 0$ satisfies

$$N > q - 506\sqrt{q} - 25.$$

Any solution of $h(x, y) = 0$ with $xy = 0$ satisfies $x^{24} = -1$ or $y^{24} = -1$. However, there are no solutions to either equation in odd degree extensions of $\mathbb{F}_3$, and so there are no solutions to $h(x, y) = 0$ with $xy = 0$ in cases relevant to our analysis. It follows that f is not planar over $\mathbb{F}_q$ provided

$$q - 506\sqrt{q} - 25 > 0,$$

which holds provided $e \geq 12$. It is easily checked that f is not planar over $\mathbb{F}_{3^e}$ for all odd $e < 12$.

(viii) $k = 9$, $d = 4$ and $p = 3$: Set $f(X) = E_9(X^4, a) = X^{36} + aX^{28} + a^3X^{12} - a^4X^4$ and $q = 3^e$. Again, this polynomial is never planar when e is even as then $4|(q-1)$, so that the order of the image set of f on $\mathbb{F}_q^*$ is at most $(q-1)/4$.

Now suppose e is odd. Since $(4, q-1) = 2$, we may again appeal to Proposition 4.3, this time showing $E_9(X^4, a)$ is planar equivalent over $\mathbb{F}_{3^e}$ to $E_9(X^4, 1)$ if a is a square and $E_9(X^4, -1)$ if a is a non-square. Consequently, we need only consider the planarity of $f(X) = E_9(X^4, a)$ with $a \in \{1, -1\}$. We have $\Delta_f(X, Y) = XY(X^2 + Y^2)h(X, Y)$, where

$$h(X,Y) = \left(\sum_{i=4}^{12}(-1)^i X^{32-2i}Y^{2i}\right) + a\left(\sum_{i=0}^{12}(-1)^i X^{24-2i}Y^{2i}\right) - a^3\left(\sum_{i=1}^{3}(-1)^i X^{8-2i}Y^{2i}\right) - a^4$$

Computation shows $h(X, Y)$ is absolutely irreducible for either choice of a. By Proposition 4.2, the number N of $(x, y) \in \mathbb{F}_q^2$ with $h(x, y) = 0$ satisfies

$$N > q - 930\sqrt{q} - 25.$$

If $a = 1$, then four solutions of $h(x, y) = 0$ have $xy = 0$, and there are none otherwise. It follows that, in either case, f is not planar over $\mathbb{F}_q$ provided

$$q - 930\sqrt{q} - 29 > 0,$$

which holds provided $e \geq 13$. Computation now shows that f is not planar for either choice of a over $\mathbb{F}_{3^e}$ for all odd e satisfying $5 \leq e < 13$, while for $e = 3$, $E_9(X^4, a)$ is planar over $\mathbb{F}_{27}$ precisely when a is a square.

(ix) $k = 10$, $d = 1$ and $p = 3$: Set $f(X) = E_{10}(X, a) - E_{10}(0, a) = X^{10} + a^2X^6 + a^3X^4$ and $q = 3^e$. We first note that $f(X) = X^4(X^2 - a)(X^4 + aX^2 - a^2)$, so that if a is a square, then f has a non-zero root and cannot be planar. Computation shows f is planar over $\mathbb{F}_{27}$ when a is a non-square.

When a is a non-square and e is even, we have $X^4 + aX^2 - a^2 = (X^2 - a - za)(X^2 - a + za)$, where $z^2 = -1$. Consequently, f has a root if either $(1 - z)$ or $(1 + z)$ is a non-square, which holds precisely when $e = 2m$ with m odd.

We have $\Delta_f(X, Y) = XYh(X, Y)$, where

$$h(X, Y) = X^8 + Y^8 - a^2X^2Y^2 + a^3(X^2 + Y^2).$$

The discussion following Proposition 4.3 shows that $h(X, Y)$ is absolutely irreducible for any choice of $a \in \mathbb{F}_q^*$ if it is absolutely irreducible for $a = 1$. Appealing to Magma reveals $h(X, Y)$ is, indeed, absolutely irreducible. By Proposition 4.2, the number N of solutions $(x, y) \in \mathbb{F}_q^2$ of $h(x, y) = 0$ satisfies

$$N > q - 42\sqrt{q} - 9.$$

With a a non-square, only one solution (x, y) satisfies $xy = 0$: $x = y = 0$. Consequently, there exists a root $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ of $h(X, Y)$ provided

$$q - 42\sqrt{q} - 10 > 0,$$

which holds provided $e \geq 7$. Hence f is not planar over $\mathbb{F}_q$ if $e \geq 7$. Computation reveals f is not planar for $4 \leq e \leq 6$ also.

(x) $k = 12$, $d = 1$ and $p = 3$: Set $f(X) = E_{12}(X, a) - E_{12}(0, a) = X^{12} + aX^{10} + a^4X^4$ and $q = 3^e$ with $e \geq 2$. Again we can find a partial factorisation of $f(X)$: $f(X) = X^4(X^2 - a)(X^6 - aX^4 - a^2X^2 - a^3)$. It now follows from Proposition 4.1 that if a is a square in $\mathbb{F}_q$, then f is not planar over $\mathbb{F}_q$.

Now suppose a is a non-square. If $e = 2$, then set $h(X) = f(X) \bmod (X^q - X) = (a^4 + 1 + a)X^2$. The polynomial h is planar equivalent to f. As a is a non-square, $a^4 = -1$, and so $h(X) = aX^2$, which is planar. Again, computation shows f is planar over $\mathbb{F}_{27}$ for all non-square a.

Now $\Delta_f(X, Y) = XYh(X, Y)$ where

$$h(X, Y) = X^8Y^2 + X^2Y^8 + a(X^8 + Y^8) + a^4(X^2 + Y^2).$$

Again, the discussion following Proposition 4.3 shows that $h(X, Y)$ is absolutely irreducible for any $a \in \mathbb{F}_q^*$ if it is absolutely irreducible when $a = 1$. Magma duly computes that this is indeed the case. Invoking Proposition 4.2 one last time, we find $h(X, Y)$ has a root $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ provided

$$q - 72\sqrt{q} - 12 > 0,$$

which holds for all $e \geq 8$. Hence f is not planar over $\mathbb{F}_q$ for all $e \geq 8$. A quick calculation now shows f is not planar when $4 \leq e \leq 7$ either.

We summarise the above discussion as a lemma.

Lemma 4.4. *The only infinite classes of planar DO polynomials arising from $D_k(X^d, a)$ or $E_k(X^d, a)$ are planar equivalent to $X^{p^\alpha+1}$ with p any odd prime, or $D_5(X^2, a)$ with $p = 3$.*

We conclude with some remarks on the corresponding planes. The planar DO monomials $X^{p^{\alpha+n}+p^n}$ correspond to Albert's twisted field planes [1] when $\alpha \not\equiv 0 \bmod e$ and the Desarguesian plane otherwise. Composition of a linearised permutation polynomial with a planar polynomial results in a plane isomorphic to the plane defined by the planar polynomial (see [5, Theorem 5.2]). Consequently, Theorem 3.1 (iii)(a) yields twisted field planes also.

When $e \geq 5$ is odd, the class of planar polynomials over $\mathbb{F}_{3^e}$ given by $D_5(X^2, a)$ yields two Lenz-Barlotti type V planes, not equivalent to each other, nor to any twisted field, nor to the Desarguesian plane. When $e = 3$, this class yields both the Desarguesian plane and the solitary twisted field plane of order 27. When $e = 2$, the Desarguesian plane is obtained. For these and related results see [4].

All remaining examples of planar DO polynomials identified in this article occur over fields of order p^e with $e \in \{1, 2, 3\}$. Knuth [12] noted that any semifield plane of order p or p^2 is necessarily Desarguesian, while it follows from the results of Menichetti [14] that any proper semifield of order p^3 is necessarily a twisted field. Since any planar DO polynomial necessarily generates a commutative semifield plane, it follows that all of the remaining planes identified in this paper are either Desarguesian or twisted field planes.

References

[1] A.A. Albert. On nonassociative division algebras. *Trans. Amer. Math. Soc.*, 72:296–309, 1952.
[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[3] M. Cipu and S.D. Cohen. Dickson polynomial permutations. In G.L. Mullen, D. Panario, and I.E. Shparlinski, editors, *Finite fields and applications*, volume 461 of *Contemp. Math.*, pages 79–90. Amer. Math. Soc., 2008.
[4] R.S. Coulter and M. Henderson. Commutative presemifields and semifields. *Adv. Math.*, 217:282–304, 2008.
[5] R.S. Coulter and R.W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10:167–184, 1997.
[6] R.S. Coulter and R.W. Matthews. On the permutation behaviour of Dickson polynomials of the second kind. *Finite Fields Appl.*, 8:519–530, 2002.
[7] P. Dembowski and T.G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103:239–258, 1968.
[8] C. Ding and J. Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113:1526–1535, 2006.
[9] M. Henderson. A note on the permutation behaviour of the Dickson polynomials of the second kind. *Bull. Austral. Math. Soc.*, 56:499–505, 1997.
[10] M. Henderson and R. Matthews. Permutation properties of Chebyshev polynomials of the second kind over a finite field. *Finite Fields Appl.*, 1:115–125, 1995.
[11] M. Henderson and R. Matthews. Dickson polynomials of the second kind which are permutation polynomials over a finite field. *New Zealand J. Math.*, 27:227–244, 1998.
[12] D.E. Knuth. Finite semifields and projective planes. *J. Algebra*, 2:182–217, 1965.
[13] R. Lidl, G.L. Mullen, and G. Turnwald. *Dickson Polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Appl. Math.* Longman Scientific and Technical, Essex, England, 1993.
[14] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J. Algebra*, 47:400–410, 1977.
[15] W. Nöbauer. Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen. *J. Reine Angew. Math.*, 231:215–219, 1968.
[16] W. Qiu, Z. Wang, G. Weng, and Q. Xiang. Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. *Des. Codes Cryptogr.*, 44:49–62, 2007.
[17] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Number 1064. Hermann, Paris, 1948.

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

6 Earl St., Sandy Bay, Tasmania 7005, Australia