Finite Fields Appl. 8 (2002), 519-530

On the permutation behaviour of Dickson polynomials of the second kind

Robert S. Coulter[1]

Information Security Research Centre, Queensland University of Technology, GPO Box 2434, Brisbane, Queensland, 4001, Australia
E-mail: shrub@isrc.qut.edu.au

and

Rex W. Matthews

6 Earl St., Sandy Bay, Tasmania, 7005, Australia
E-mail: rex@verdant.com.au

The known permutation behaviour of the Dickson polynomials of the second kind in characteristic 3 is expanded and simplified.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field of $q = p^e$ elements; p a prime, e a positive integer. We use $\mathbb{F}_q^*$ to denote the non-zero elements of $\mathbb{F}_q$ and shall denote the quadratic multiplicative character of $\mathbb{F}_q$ by η when q is odd. Recall, for $a \in \mathbb{F}_q^*$, q odd, $\eta(a) = 1$ or -1 depending on whether a is a square or non-square, respectively. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) if it is one to one (and hence onto) when evaluated on $\mathbb{F}_q$. We say two polynomials $f, g \in \mathbb{F}_q[X]$ are *permutation equivalent* over $\mathbb{F}_q$ if f is a PP over $\mathbb{F}_q$ if and only if g is a PP over $\mathbb{F}_q$.

In this article we will consider the permutation behaviour of the Dickson polynomials of the second kind. The *Dickson polynomials of the first kind* (DPFK) and *Dickson polynomials of the second kind* (DPSK) are defined

[1] This work was supported by Australian Research Council Large Grant #A49801415 while the author was employed at the Centre for Discrete Mathematics and Computing at the University of Queensland

by

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

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

respectively, where $\lfloor k/2 \rfloor$ is the largest integer $\leq k/2$, and $a \in \mathbb{F}_q$. Dickson polynomials are also known as the Chebyshev polynomials of the first and second kind due to their relation with the Chebyshev polynomials from analysis. Much is known about them, see the monograph [7]. Note that both kinds of Dickson polynomials are strictly even or odd functions depending on whether k is even or odd. This implies that, for q odd, k must be odd if either polynomial is a PP.

The PPs among the DPFK have been completely classified: $g_k(X,a)$ is a PP over $\mathbb{F}_q$ if and only if $(k, q^2-1) = 1$, [9]. For the DPSK, the behaviour of $f_k(X,0) = X^k$ is well understood and so we specify $a \in \mathbb{F}_q^*$ for the remainder of this article. Henderson and Matthews, [6, Lemma 2.2], showed $f_k(X,a)$ and $f_k(X,b)$ are permutation equivalent if $\eta(ab) = 1$. Hence, the permutation behaviour of the Dickson polynomials of the second kind splits into two distinct cases, based on whether a is a square or non-square.

Connected to this distinction is the concept of sign classes. For the moment assume q is odd. Suppose $\eta(a) = 1$ and let $(k_0, k_1, k_2) \in \mathbb{Z}^3$ be defined by the congruences

$$\begin{aligned} k_0 &\equiv k+1 \bmod p \\ k_1 &\equiv k+1 \bmod (q-1)/2 \\ k_2 &\equiv k+1 \bmod (q+1)/2. \end{aligned}$$

Set A to be the eight pairs of the form $(\pm k_0, \pm k_1, \pm k_2) \in \mathbb{Z}^3$, where $-k_i$ is calculated using the appropriate modulus. Likewise, for $\eta(a) = -1$, let $(k_1, k_2) \in \mathbb{Z}^2$ be defined by the congruences

$$\begin{aligned} k_1 &\equiv k+1 \bmod (q-1) \\ k_2 &\equiv k+1 \bmod (q+1) \end{aligned}$$

and set A to be the set of four pairs of the form $(\pm k_1, \pm k_2) \in \mathbb{Z}^2$, where $-k_i$ is again calculated using the appropriate modulus. If k corresponds to a triple or pair (depending on $\eta(a)$) in A, then we call A the *sign class* of k. It was shown by Henderson and Matthews, [6, Theorem4.2], that if k and

k' are in the same sign class, then $f_k(X,a)$ and $f_{k'}(X,a)$ are permutation equivalent on $\mathbb{F}_q$.

For $a \neq 0$, the classification of PPs among the DPSK is not complete, although there have been some significant results. For q odd, Matthews, [8, Theorem 2.5], showed that $f_k(X,1)$ is a PP over $\mathbb{F}_q$ if k belongs to the sign class $(2,2,2)$. Cohen showed that these conditions were necessary for $q = p$, [1], and $q = p^2$, [2]. The result of Henderson and Matthews on the permutation equivalence of all square $a \in \mathbb{F}_q^*$ obviously extends this result to all square $a \in \mathbb{F}_q^*$, $q = p, p^2$ odd. For $q = p^n$, $n \geq 3$ or $p = 2$, some PPs have been identified in the work of Henderson and Matthews, see [5] for $\eta(a) = 1$ and [6] for $\eta(a) = -1$. In both cases the new established classes occur over fields of small characteristic.

It is obvious that the sign class containing the triple $(2,2,2)$ for $\eta(a) = 1$ or pair $(2,2)$ for $\eta(a) = -1$ is a permutation class ($f_1(X,a) = X$). In this article we concentrate specifically on the case $\eta(a) = -1$ and $p = 3$. The case $\eta(a) = -1$ was considered by Henderson and Matthews in [6]. They established that for $p = 5$ the sign class containing the pair $(2,(q-1)/2)$ corresponds to a permutation class ([6, Theorem 5.3]), and for $p = 7$ the sign class containing the pair $(2,(q-1)/4)$ corresponds to a permutation class if e is odd ([6, Theorme 5.4]). Their description of permutation classes in characteristic 3 gave 6 classes. For this case we give a new description of the known permutations.

Theorem 1.1. *Let $q = 3^e$ and $\eta(a) = -1$. The DPSK $f_k(X,a)$ is a PP over $\mathbb{F}_q$ if the sign class of k contains the pair $(4,4)$ with e even, or the pair (k_1,k_2), with*

$$k_1 = \left(\frac{3^s-1}{2}\right)^{-1} + 1$$

where $(s,2e) = 1$; and

$$k_2 = \begin{cases} \left(\frac{3^t-1}{2}\right)^{-1} + 1 \text{ where } t \text{ is odd, or} \\ \left(\frac{3^t+1}{2}\right)^{-1} - 1 \text{ where } t \text{ and } e/(t,e) \text{ are even.} \end{cases}$$

The inverses for k_1 and k_2 are calculated modulo $(q-1)$ and $(q+1)$, respectively.

This result expands the known PPs among DPSK in characteristic 3 and dramatically simplifies the description of classes given in [6, Theorem 5.2]. In the next section we provide further relevant background information, including the definition of S-sets, sign classes and H-functions which have so far proved to be the most effective tools for dealing with the permutation behaviour of the DPSK. After some further preliminary work, we describe the new classes and give a proof of their permutation behaviour. We end by discussing how the results of [6, Theorem 5.2] are contained in the above result.

2. FURTHER BACKGROUND AND DEFINITIONS

Throughout the remainder of this article, unless specified, q is assumed to be odd. The majority of this section is either developed or described in [6], and we follow the notation established there and elsewhere.

Central to discussing properties of the Dickson polynomials is the notion of S-sets, which are dependent on the choice of a. For q odd they can be defined as follows. If $\eta(a) = 1$, then the S-sets are

$$\begin{aligned}
S_0 &= \{\pm 2\sqrt{a}\}\\
S_1 &= \{x = u + au^{-1} \ : \ u \in \mathbb{F}_{q^2} \mid u^{q-1} = 1 \text{ and } u \neq \pm\sqrt{a}\}\\
S_2 &= \{x = u + au^{-1} \ : \ u \in \mathbb{F}_{q^2} \mid u^{q+1} = a \text{ and } u \neq \pm\sqrt{a}\}.
\end{aligned}$$

If $\eta(a) = -1$, then the S-sets are

$$\begin{aligned}
S_1 &= \{x = u + au^{-1} \ : \ u \in \mathbb{F}_{q^2} \mid u^{q-1} = 1 \text{ and } u \neq \pm\sqrt{a}\}\\
S_2 &= \{x = u + au^{-1} \ : \ u \in \mathbb{F}_{q^2} \mid u^{q+1} = a \text{ and } u \neq \pm\sqrt{a}\};
\end{aligned}$$

As every quadratic over $\mathbb{F}_q$ splits completely in $\mathbb{F}_{q^2}$, every $x \in \mathbb{F}_q$ satisfies $x = u + au^{-1}$ for some $u \in \mathbb{F}_{q^2}$. As $x^q = x$ for all $x \in \mathbb{F}_q$, we have $u^q + au^{-q} = u + au^{-1}$, from which we have

$$(u^{q-1} - 1)(u^{q+1} - a) = 0.$$

Using this notation, it can be established, see [7, Chapter 2], that for $x \in \mathbb{F}_q$, we have $g_k(x, a) = u^k + a^k u^{-k}$ and for $u^2 \neq a$

$$f_k(x, a) = \frac{u^{k+1} - a^{k+1}u^{-(k+1)}}{u - au^{-1}}.$$

When $\eta(a) = 1$, the case $u^2 = a$ is dealt with separately with $f_k(\epsilon\sqrt{a}, a) = (k+1)(\epsilon\sqrt{a})^k$, where $\epsilon = \pm 1$, from the original definition. The definition of S-sets above can be seen to differentiate between the two cases underlying the quadratic and clearly $\bigcup_i S_i = \mathbb{F}_q$ in either case. It can be shown that S_i, $i = 1, 2$, consists of those $x \in \mathbb{F}_q$ for which $\eta(x^2 - 4a) = (-1)^{i-1}$, ignoring the zero when $\eta(a) = -1$.

In a sense, the congruences of the sign class can be seen to correspond with the S-sets. This "correspondence" between the sign class and the

S-sets is used to prove the permutation behaviour of classes by considering the mappings on each of the S-sets separately. Effectively, the proof of a permutation class involves proving that a sign class is *S-preserving*, in that it maps S_i onto itself.

The following transformation of $f_k(X, a)$ will be used.

Lemma 2.1 ([6, Lemma 3.1]). *Let $g_\alpha(X, a)$ be a PP over $\mathbb{F}_q$. Then the function $H_{[k,\alpha]}(X, a)$, given by*

$$H_{[k,\alpha]}(x, a) = f_k(g_\alpha(x, a), a^\alpha) \\ = \frac{u^{\alpha(k+1)} - a^{\alpha(k+1)}u^{-\alpha(k+1)}}{u^\alpha - a^\alpha u^{-\alpha}}$$

for each $x \in \mathbb{F}_q$, is permutation equivalent to $f_k(X, a)$. If q is odd then $H_{[k,\alpha]}$ is an odd function.

This transformation of the DPSK is particularly significant as it differentiates between the behaviour of the DPSK on each S-set.

Lemma 2.2 ([6, Lemma 3.2]). *Let k and α satisfy the congruences*

$$k+1 \equiv \begin{cases} k_1 \bmod (q-1) \\ k_2 \bmod (q+1) \end{cases} \qquad \text{and} \quad \alpha \equiv \begin{cases} \alpha_1 \bmod (q-1) \\ \alpha_2 \bmod (q+1) \end{cases}$$

where k_1, k_2 are even and α_1, α_2 are odd. Then

$$H_{[k,\alpha]}(x, a) = H_{[k_1-1,\alpha_1]}(x, a)$$

for all $x \in S_1$, and

$$H_{[k,\alpha]}(x, a) = \pm a^n H_{[k_2-1,\alpha_2]}(x, a)$$

for all $x \in S_2$, where $n = (\alpha_1(k_1-1) - \alpha_2(k_2-1))/2$.

We end this section with two lemmas on greatest common divisors. A proof of the first lemma is given in [3, 4]. The authors are unable to find a reference for the second lemma, and so we provide a proof.

Lemma 2.3. *Let $d = (n, m)$ and p be a prime. If n/d is odd then*

$$(p^n - 1, p^m + 1) = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{otherwise.} \end{cases}$$

If n/d is even then $(p^n - 1, p^m + 1) = p^d + 1$.

Lemma 2.4. *Let $d = (n, m)$ and p be an odd prime. Then*

$$(p^n+1, p^m+1) = \begin{cases} 2 & \text{if } \frac{n}{d} \not\equiv \frac{m}{d} \bmod 2, \\ p^d+1 & \text{if } p \equiv 3 \bmod 4 \text{ and } nm \equiv 1 \bmod 2, \\ \frac{p^d+1}{2} & \text{in all other cases.} \end{cases}$$

Proof. There are effectively two cases: (i) n/d odd, m/d even; and (ii) n/d and m/d odd. We have

$$(p^{2n}-1, p^m+1) = (p^n-1, p^m+1)\left(p^n+1, \frac{p^m+1}{(p^n-1, p^m+1)}\right) \qquad (1)$$

In case (i), using Lemma 2.3, Equation 1 simplifies to $(p^n+1, \frac{p^m+1}{2}) = 1$, which resolves the first case. For case (ii), we again simplify (1) using the previous lemma to obtain

$$\left(p^n+1, \frac{p^m+1}{2}\right) = \frac{p^d+1}{2}.$$

Observing that $(p^n+1, \frac{p^m+1}{2}) = (p^n+1, p^m+1)$ unless $p^m+1 \equiv 0 \bmod 4$ completes the proof. ▮

3. A GENERAL OBSERVATION

We begin by considering the problem of when $H_{[k,\alpha]}(x,a) = H_{[k,\alpha]}(y,a)$, for $x \neq y$.

Lemma 3.5. *Let $a \in \mathbb{F}_q^*$ and k and α be as in Lemma 2.2. Then $H_{[k,\alpha]}(x,a) = H_{[k,\alpha]}(y,a)$ if and only if*

$$\left((uw)^{\alpha(k+2)} - a^{\alpha(k+2)}\right)\left(u^{\alpha k} - w^{\alpha k}\right) \\ = a^{\alpha}\left(u^{\alpha(k+2)} - w^{\alpha(k+2)}\right)\left((uw)^{\alpha k} - a^{\alpha k}\right)$$

where $x, y \in \mathbb{F}_q$ with $x = u + au^{-1}$ and $y = w + aw^{-1}$.
If $x, y \in S_1$ then $H_{[k,\alpha]}(x,a) = H_{[k,\alpha]}(y,a)$ if and only if

$$\left((uw)^{\alpha_1(k_1+1)} - a^{\alpha_1(k_1+1)}\right)\left(u^{\alpha_1(k_1-1)} - w^{\alpha_1(k_1-1)}\right) \\ = a^{\alpha_1}\left(u^{\alpha_1(k_1+1)} - w^{\alpha_1(k_1+1)}\right)\left((uw)^{\alpha_1(k_1-1)} - a^{\alpha_1(k_1-1)}\right). \qquad (2)$$

If $x, y \in S_2$ then $H_{[k,\alpha]}(x,a) = H_{[k,\alpha]}(y,a)$ if and only if

$$\begin{aligned}\left((uw)^{\alpha_2(k_2+1)} - \epsilon a^{\alpha_2(k_2+1)}\right)&\left(u^{\alpha_2(k_2-1)} - \epsilon w^{\alpha_2(k_2-1)}\right)\\ &= a^{\alpha_2}\left(u^{\alpha_2(k_2+1)} - \epsilon w^{\alpha_2(k_2+1)}\right)\left((uw)^{\alpha_2(k_2-1)} - \epsilon a^{\alpha_2(k_2-1)}\right)\end{aligned} \tag{3}$$

where $\epsilon = \pm 1$.

Proof. We prove the first statement only. The rest follows from Lemma 2.1. Suppose $H_{[k,\alpha]}(x,a) - H_{[k,\alpha]}(y,a) = 0$. This is equivalent to

$$\begin{aligned}(u^{\alpha(k+1)} - a^{\alpha(k+1)}u^{-\alpha(k+1)})&(w^{\alpha} - a^{\alpha}w^{-\alpha})\\ &= (w^{\alpha(k+1)} - a^{\alpha(k+1)}w^{-\alpha(k+1)})(u^{\alpha} - a^{\alpha}u^{-\alpha}).\end{aligned}$$

Multiplying through by $(uw)^{\alpha(k+1)}$ and gathering terms we arrive at

$$\begin{aligned}(u^{2k+2}w^{k+2})^{\alpha} - (w^{2k+2}u^{k+2})^{\alpha} &+ (a^{k+2}w^{k})^{\alpha} - (a^{k+2}u^{k})^{\alpha}\\ &= (u^{2k+2}w^{k})^{\alpha} - (w^{2k+2}u^{k})^{\alpha} + (a^{k}w^{k+2})^{\alpha} - (a^{k}u^{k+2})^{\alpha}\end{aligned}$$

from which the factorisation described is obtained. ▮

4. DESCRIBING THE DPSK PERMUTATIONS IN CHARACTERISTIC 3

We are now ready to prove our main result. Our proof follows the general method developed in [5, 6], and although there is some overlap with the proof of [6, Theorem 5.2], we give a self-contained proof here for completeness.

Proof (of Theorem 1.1). The class $(4,4)$ with e even can be shown directly. In fact, $f_3(X,a) = X^3 + aX$ is a linearised polynomial. It is well known that a linearised polynomial is a PP over $\mathbb{F}_q$ if and only if it has no non-zero roots in $\mathbb{F}_q$. Thus $f_3(X,a)$ is a permutation polynomial over $\mathbb{F}_{3^e}$ if and only if $-a$ is a non-square, which holds whenever e is even.

Suppose (k_1, k_2) is an element of the sign class of k. Throughout the proof we set

$$k_1 = \left(\frac{3^s - 1}{2}\right)^{-1} + 1$$

with $(s, 2e) = 1$. Let α satisfy the congruence

$$\alpha \equiv \begin{cases} \alpha_1 \bmod (q-1) \\ \alpha_2 \bmod (q+1) \end{cases}$$

with $\alpha_1 = \frac{3^s-1}{2}$. We will set $\alpha_2 = \frac{3^t-1}{2}$ or $\alpha_2 = \frac{3^t+1}{2}$, depending on which of the two cases for k_2 we are dealing with. In either case, using Lemma 2.3 or Lemma 2.4 and the conditions on s and t shows $(\alpha, q^2-1) = 1$. It follows that $g_\alpha(X, a)$ is a PP and from Lemma 2.1 we have $H_{[k,\alpha]}(X, a)$ and $f_k(X, a)$ are permutation equivalent.

We first show the function $H_{[k,\alpha]}(x, a)$ is bijective on S_1. Let $x, y \in S_1$ be given by $x = u + au^{-1}$ and $y = w + aw^{-1}$ and suppose $H_{[k,\alpha]}(x, a) = H_{[k,\alpha]}(y, a)$. From (2) we have

$$(u-w)(uw-a)^{3^s} = a^{(3^s-1)/2}(u-w)^{3^s}(uw-a).$$

Thus either $u = w$, $uw = a$ or $(uw-a)^{3^s-1} = a^{(3^s-1)/2}(u-w)^{3^s-1}$. If the final condition holds, then as $(s, e) = 1$, we have $(uw-a)^2 = a(u-w)^2$. Solving for a gives $a = u^2$ or $a = w^2$, contradicting $\eta(a) = -1$. The remaining two possibilities both imply $x = y$. Hence $H_{[k,\alpha]}(x, a)$ is injective on S_1. To show that $H_{[k,\alpha]}(x, a)$ is surjective on S_1 we calculate the quadratic character of $H_{[k,\alpha]}(x, a)^2 - 4a$. We have

$$\begin{aligned} H_{[k,\alpha]}(x,a)^2 - 4a &= \left(\frac{u^{(3^s+1)/2} - a^{(3^s+1)/2}u^{-(3^s+1)/2}}{u^{(3^s-1)/2} - a^{(3^s-1)/2}u^{-(3^s-1)/2}} \right)^2 - a \\ &= \left(\frac{u^{3^s+1} - a^{(3^s+1)/2}}{u^{3^s} - a^{(3^s-1)/2}u} \right)^2 - a \\ &= \frac{u^{2(3^s+1)} - au^{2.3^s} - a^{3^s}u + a^{3^s+1}}{(u^{3^s} - a^{(3^s-1)/2}u)^2} \\ &= \frac{(u^2-a)^{3^s+1}}{(u^{3^s} - a^{(3^s-1)/2}u)^2} \\ &= \left(\frac{(u^2-a)^{(3^s+1)/2}}{u^{3^s} - a^{(3^s-1)/2}u} \right)^2, \end{aligned}$$

which is the square of an element of $\mathbb{F}_q$. Thus $H_{[k,\alpha]}(x, a)$ is bijective on S_1.

It remains to show that, for either choice of k_2, $H_{[k,\alpha]}(x, a)$ is bijective on S_2. For either case, we set $d = (t, e)$.

Let t be odd and set

$$k_2 = \left(\frac{3^t-1}{2} \right)^{-1} + 1.$$

Let $\alpha_2 = \frac{3^t-1}{2}$. By Lemma 2.2, $f_k(X, a)$ is permutation equivalent on S_2 to $H_{[k_2-1,\alpha_2]}(X, a)$. Let $x, y \in S_2$ be given by $x = u + au^{-1}$ and $y = w + aw^{-1}$ and suppose $H_{[k,\alpha]}(x, a) = H_{[k,\alpha]}(y, a)$. From (3) we obtain

$$(uw - \epsilon a)^{3^t}(u - \epsilon w) = a^{(3^t-1)/2}(uw - \epsilon a)(u - \epsilon w)^{3^t}.$$

Thus either $uw = \epsilon a$, $u = \epsilon w$, or $(uw - \epsilon a)^{3^t-1} = a^{(3^t-1)/2}(u - \epsilon w)^{3^t-1}$. The first two conditions imply $x = \pm y$. Suppose $(uw - \epsilon a)^{3^t-1} = a^{(3^t-1)/2}(u - \epsilon w)^{3^t-1}$. Raising both sides by $(q-1)/(p^d-1)$ and recalling $a^{(q-1)/2} = \eta(a) = -1$, we obtain

$$(uw - \epsilon a)^{(q-1)(3^t-1)/(3^d-1)} = -(u - \epsilon w)^{(q-1)(3^t-1)/(3^d-1)}.$$

Since $(3^t-1)/(3^d-1)$ is odd (as t/d is) and relatively prime to $q-1$, we have $(uw - \epsilon a)^{q-1} = -(u - \epsilon w)^{q-1}$. Multiplying through by $(uw - \epsilon a)(u - \epsilon w)$ and then expanding and simplifying we obtain $w^q + w = \epsilon(u^q + u)$. Since $a = u^{q+1} = w^{q+1}$ we thus have $w + aw^{-1} = \epsilon(u + au^{-1})$, or equivalently $x = \pm y$ again. Now $H_{[k,\alpha]}(X, a)$ is an odd polynomial so if $x = -y$, then

$$H_{[k,\alpha]}(x, a) = H_{[k,\alpha]}(y, a) = -H_{[k,\alpha]}(y, a).$$

It follows that $H_{[k,\alpha]}(x, a) = 0$, or equivalently, $u^{3^t+1} = a^{(3^t+1)/2}$. Since t is odd, $u^2 = \pm a$. If $u^2 = a$, then $u^{q+1} = (u^2)^{(q+1)/2} = a^{(q+1)/2} = -a$, which contradicts $u^{q+1} = a$. Hence $u^2 = -a$, so that $x = 0$. We conclude that $x = y$ and thus $H_{[k,\alpha]}(x, a)$ is injective on S_2. To show it is surjective, we again determine $\eta(H_{[k,\alpha]}(x, a)^2 - 4a)$. A similar calculation as for $x \in S_1$ yields

$$H_{[k,\alpha]}(x, a)^2 - 4a = \frac{(u^2 - a)^{3^t+1}}{(u^{3^t} - a^{(3^t-1)/2}u)^2}.$$

Raising this to the power $(q-1)/2$ and using $u^q = au^{-1}$ we have

$$\begin{aligned}
\left(H_{[k,\alpha]}(x, a)^2 - 4a\right)^{(q-1)/2} &= \frac{\left((u^2 - a)^{q-1}\right)^{(3^t+1)/2}}{(u^{3^t} - a^{(3^t-1)/2}u)^{q-1}} \\
&= \frac{(u^{2q} - a^q)^{(3^t+1)/2}(u^{3^t} - a^{(3^t-1)/2}u)}{(u^{3^t q} - a^{q(3^t-1)/2}u^q)(u^2 - a)^{(3^t+1)/2}} \\
&= \frac{(a^2u^{-2} - a)^{(3^t+1)/2}(u^{3^t} - a^{(3^t-1)/2}u)}{(a^{3^t}u^{-3^t} - a^{(3^t+1)/2}u^{-1})(u^2 - a)^{(3^t+1)/2}} \\
&= -(-1)^{(3^t+1)/2} = -1
\end{aligned}$$

as t is odd. Thus $H_{[k,\alpha]}(x,a)$ is bijective on S_2 and $H_{[k,\alpha]}(X,a)$ is a permutation polynomial over $\mathbb{F}_q$. Hence $f_k(X,a)$ is a permutation polynomial if (k_1,k_2) is an element of the sign class of k.

Now assume both t and $te/2d$ are even, and define

$$\begin{aligned} k_2 &= -\left(\left(\frac{3^t+1}{2}\right)^{-1} - 1\right) \\ &= -\left(\frac{3^t+1}{2}\right)^{-1} + 1. \end{aligned}$$

Set $\alpha_2 = \frac{3^t+1}{2}$. Let $x,y \in S_2$ be given by $x = u + au^{-1}$ and $y = w + aw^{-1}$ and suppose $H_{[k,\alpha]}(x,a) = H_{[k,\alpha]}(y,a)$. From (3) we again obtain

$$(uw - \epsilon a)^{3^t}(u - \epsilon w) = a^{(3^t-1)/2}(uw - \epsilon a)(u - \epsilon w)^{3^t}.$$

Thus either $uw = \epsilon a$, $u = \epsilon w$, or $(uw - \epsilon a)^{3^t-1} = a^{(3^t-1)/2}(u - \epsilon w)^{3^t-1}$. Again we need only deal with the third possibility. If e/d is even, then $(3^t-1)/(3^d-1)$ is odd, and it follows that $x = \pm y$ as in the previous case. Therefore $H_{[k_2-1,\alpha_2]}(X,a)$ is injective on S_2. It remains to prove $H_{[k_2-1,\alpha_2]}(X,a)$ is surjective on S_2. To do this, it is sufficient to show $\eta\left(H_{[k,\alpha]}(x,a)^2 - 4a\right) = -1$ for $x \in S_2$. If $x = u + au^{-1}$ is an element of S_2, then

$$\begin{aligned} H_{[k,\alpha]}(x,a)^2 - 4a &= a^{\alpha_1(k_1-1)-\alpha_2(k_2-1)} H_{[k_2-1,\alpha_2]}(x,a)^2 - a \\ &= a^2 \frac{(u^{3^t} - a^{(3^t-1)/2}u)^2}{(u^{3^t+1} - a^{(3^t+1)/2})^2} - a \\ &= a\left(\frac{a(u^{3^t} - a^{(3^t-1)/2}u)^2 - (u^{3^t+1} - a^{(3^t+1)/2})^2}{(u^{3^t+1} - a^{(3^t+1)/2})^2}\right) \\ &= \frac{a(au^{2.3^t} - u^{2(3^t+1)} + a^{3^t}u^2 - a^{3^t+1}}{(u^{3^t+1} - a^{(3^t+1)/2})^2} \\ &= \frac{-a(u^2-a)^{3^t+1}}{(u^{3^t+1} - a^{(3^t+1)/2})^2}. \end{aligned}$$

Raising this to the power $(q-1)/2$ and using $u^q = au^{-1}$, we have

$$\begin{aligned}
(H_{[k,\alpha]}(x,a)^2 - 4a)^{(q-1)/2} &= \frac{(-1)^{(q-1)/2}a^{(q-1)/2}(u^2-a)^{(q-1)(3^t+1)/2}}{(u^{3^t+1} - a^{(3^t+1)/2})^{q-1}} \\
&= \frac{-(u^{2q}-a)^{(3^t+1)/2}(u^{3^t+1} - a^{(3^t+1)/2})}{(u^{q(3^t+1)} - a^{(3^t+1)/2})(u^2-a)^{(3^t+1)/2}} \\
&= \frac{-(a^2u^{-2}-a)^{(3^t+1)/2}(u^{3^t+1} - a^{(3^t+1)/2})}{(a^{3^t+1}u^{-(3^t+1)} - a^{(3^t+1)/2})(u^2-a)^{(3^t+1)/2}} \\
&= \frac{-(au^{-2}-1)^{(3^t+1)/2}(u^{3^t+1} - a^{(3^t+1)/2})}{(a^{(3^t+1)/2} - u^{3^t+1})(1-au^{-2})^{(3^t+1)/2}} \\
&= -1.
\end{aligned}$$

Hence $H_{[k,\alpha]}(X,a)$ is surjective on S_2 and $f_k(X,a)$ is a permutation polynomial over $\mathbb{F}_q$. ∎

We note that when $k_2 = \left(\frac{3^t-1}{2}\right)^{-1} + 1$, the condition t odd is necessary and sufficient for the inverse to exist. This is not the case when $k_2 = \left(\frac{3^t+1}{2}\right)^{-1} - 1$, where the conditions t and $e/(t,e)$ even are, together, sufficient but not necessary. We underline that the PP behaviour in this second case does not extend to all cases where the inverse exists and believe that the statement as given is best possible.

It remains to discuss how the previous work, [6, Theorem 5.2], is covered by our new result. (It should be pointed out that the statement given in [6] is slightly inaccurate in that the condition $(s,e) = 1$ is omitted from the final two possibilities, although it is required for the inverses to exist.) We note without proofs the following: parts (v) and (vi) of [6, Theorem 5.2] is absorbed by the new case and the case $k_2 = (q+1)/2$, e odd, is equivalent to $\left(\frac{3^e-1}{2}\right)^{-1} + 1$. Finally, part (iv) of [6, Theorem 5.2] is absorbed in the following manner:

$$\frac{3^{2m}+1}{2} - 3^m \equiv \begin{cases} \left(\frac{3^m-1}{2}\right)^{-1} + 1 \ m \text{ odd} \\ \left(\frac{3^m+1}{2}\right)^{-1} - 1 \ m \text{ even;} \end{cases}$$

$$\frac{3^{2m}+1}{2} + 3^m \equiv \begin{cases} \left(\frac{3^{3m}-1}{2}\right)^{-1} + 1 \ m \text{ odd} \\ \left(\frac{3^{3m}+1}{2}\right)^{-1} - 1 \ m \text{ even;} \end{cases}$$

where $e = 2m$. Finally, the new description yields new PPs among the DPSK. The first field in which we obtain new examples is $\mathbb{F}_{3^9}$, where the sign classes $(2, 9086)$, $(7382, 9086)$ and $(10086, 9086)$ give classes of PPs not previously described.

We end by restating a conjecture from [6] which suggests that the description of PPs among the DPSK is not complete.

Conjecture 4.1 (Henderson & Matthews, [6, Conjecture 6.1]). *Let p be an odd prime and set $q = p^{3e}$. Let $a \in \mathbb{F}_q^*$ satisfy $\eta(a) = -1$. If the pair $(p^e(p^e+1), p^e(p^e-1))$ belongs to the sign class of k, then the polynomial $f_k(X, a)$ is a PP over $\mathbb{F}_q$.*

REFERENCES

1. S.D. Cohen, *Dickson polynomials of the second kind that are permutations*, Canad. J. Math. **46** (1994), 225–238.
2. ———, *Dickson permutations*, Number-Theoretic and Algebraic Methods in Computer Science (Moscow, 1993), World Sci. Publishing, River Edge, NJ, 1995, pp. 29–51.
3. R.S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arith. **83** (1998), 241–251.
4. ———, *On the evaluation of a class of Weil sums in characteristic 2*, New Zealand J. Math. **28** (1999), 171–184.
5. M. Henderson and R. Matthews, *Permutation properties of Chebyshev polynomials of the second kind over a finite field*, Finite Fields Appl. **1** (1995), 115–125.
6. ———, *Dickson polynomials of the second kind which are permutation polynomials over a finite field*, New Zealand J. Math. **27** (1998), 227–244.
7. R. Lidl, G.L. Mullen, and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Appl. Math., vol. 65, Longman Scientific and Technical, Essex, England, 1993.
8. R. Matthews, *Permutation polynomials in one and several variables*, Ph.D. thesis, University of Tasmania, 1982.
9. W. Nöbauer, *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen*, J. Reine Angew. Math. **231** (1968), 215–219.