Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 482–493

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$

Jin Yuan [a,*], Cunsheng Ding [b], Huaxiong Wang [c,d], Josef Pieprzyk [a]

[a] *Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*

[b] *Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China*

[c] *Division of Mathematical Sciences, Nanyang Technological University, Singapore*

[d] *Centre for Advanced Computing—Algorithms and Cryptography, Department of Computing, Macquarie University, Australia*

Received 26 July 2006; revised 15 May 2007

Available online 2 June 2007

Communicated by Stephen D. Cohen

Abstract

Recently, several classes of permutation polynomials of the form $(x^2 + x + \delta)^s + x$ over $\mathbb{F}_{2^m}$ have been discovered. They are related to Kloosterman sums. In this paper, the permutation behavior of polynomials of the form $(x^p - x + \delta)^s + L(x)$ over $\mathbb{F}_{p^m}$ is investigated, where $L(x)$ is a linearized polynomial with coefficients in $\mathbb{F}_p$. Six classes of permutation polynomials on $\mathbb{F}_{2^m}$ are derived. Three classes of permutation polynomials over $\mathbb{F}_{3^m}$ are also presented.

Keywords: Permutation polynomials; Kloosterman polynomials

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, where q is a prime power. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if the associated polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Permutation polynomials have been a subject of study for many

* Corresponding author. Fax +61 2 9850 9551.

E-mail addresses: jyuan@ics.mq.edu.au (J. Yuan), cding@cs.ust.hk (C. Ding), hwang@ics.mq.edu.au (H. Wang), josef@ics.mq.edu.au (J. Pieprzyk).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.05.003

years, and have important applications in various areas, such as coding theory, cryptography, and combinatorial designs. For an introduction to permutation polynomials, we refer the reader to [6, Chapter 7].

We use $\mathrm{Tr}(\cdot)$ to denote the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, i.e.,

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{m-1}}.$$

For any $e \in \mathbb{F}_2$, define

$$\mathbf{T}_e = \left\{ x \in \mathbb{F}_{2^m} \;\middle|\; \mathrm{Tr}(x) = e \right\}.$$

Let c be an integer in $\{1, 2, \ldots, 2^m - 1\}$, and let the binary representation of c be $c = \sum_{i=0}^{m-1} c_i \cdot 2^i$ with $c_i \in \{0, 1\}$. Define the *weight* of c to be $w(c) = \sum_{i=0}^{m-1} c_i$. We define a polynomial function on $\mathbb{F}_{2^m}$ as

$$L_c(x) = \sum_{i=0}^{m-1} c_i x^{2^i}.$$

Given integers $c, d \in \{0, 1, \ldots, 2^m - 1\}$, we define a polynomial function on $\mathbb{F}_{2^m}$ as

$$L_{c,d}(x) = L_c(x) + L_d(1/x)$$

with the understanding that $L_{c,d}(0) = 0$.

In the study of Kloosterman sum identities, Hollmann and Xiang [3] introduced Kloosterman polynomials which are defined as follows.

Let $e = w(c) \pmod 2$. The polynomial $L_{c,d} : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is called a *Kloosterman polynomial* on $\mathbb{F}_{2^m}$ if $w(d)$ is even and $L_{c,d}$ maps $\mathbf{T}_1$ bijectively onto $\mathbf{T}_e$.

Kloosterman polynomials are interesting because every Kloosterman polynomial gives rise to a Kloosterman sum identity (see [3, Theorem 3.2]). It is proved in [3] that $L_{1,3}(x) = x + 1/x + 1/x^2$, $L_{1,6}(x) = x + 1/x^2 + 1/x^4$, and $L_{1,10}(x) = x + 1/x^2 + 1/x^8$ are Kloosterman polynomials on $\mathbb{F}_{2^m}$ for all m, and it is conjectured that for all $m \geqslant 1$, $L_{1,d}$ is a Kloosterman polynomials on $\mathbb{F}_{2^m}$ if and only if $d \in \{0, 3, 6, 10\}$.

In this paper, we first prove the equivalence of Kloosterman polynomials of the form $L_{1,d}$ and permutation polynomials of a special form. Then we present six classes of permutation polynomials over $\mathbb{F}_{2^m}$ with the form $(x^2 + x + \delta)^s + L_c(x)$. Finally, we describe three classes of permutation polynomials of similar formats over $\mathbb{F}_{3^m}$.

2. A link between Kloosterman polynomials and permutation polynomials

The objective of this section is to describe the relationship between Kloosterman polynomials $L_{1,d}$ and permutation polynomials of a special form, and then present several classes of permutation polynomials related to the Kloosterman polynomial $L_{1,10}$.

Proposition 2.1. *For any integer $d \in \{0, 1, \ldots, 2^m - 1\}$ with $w(d)$ being even, $L_{1,d}(x) = x + L_d(1/x)$ is a Kloosterman polynomial of $\mathbb{F}_{2^m}$ if and only if for any $\delta \in \mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta) = 1$, the polynomial*

$$\big(L_d(x)+\delta\big)^{2^m-2}+x=\frac{1}{L_d(x)+\delta}+x$$

is a permutation polynomial of $\mathbb{F}_{2^m}$.

Proof. Assume that $L_{1,d}(x)$ is a Kloosterman polynomial. For any $\delta\in\mathbf{T}_1$, $a\in\mathbb{F}_{2^m}$, consider the equation

$$\frac{1}{L_d(x)+\delta}+x=a. \tag{1}$$

Since $\delta\in\mathbf{T}_1$, $\mathrm{Tr}(\delta)=1$. On the other hand, since $w(d)$ is even, $\mathrm{Tr}(L_d(x))=0$ for all x. It then follows that $L_d(x)+\delta\neq 0$ for any $x\in\mathbb{F}_{2^m}$. So $x=a$ cannot be a solution of (1). Thus, Eq. (1) is equivalent to

$$(x+a)\big(L_d(x)+\delta\big)+1=0. \tag{2}$$

Let $y=x+a$, then $y\neq 0$. Equation (2) then becomes $y(L_d(y)+L_d(a)+\delta)+1=0$. Hence

$$L_{1,d}(1/y)=1/y+L_d\big(1/(1/y)\big)=L_d(a)+\delta. \tag{3}$$

Since $w(d)$ is even, $L_d(z)\in\mathbf{T}_0$ for any $z\in\mathbb{F}_{2^m}$. Because $\mathrm{Tr}(\delta)=1$, we have $L_d(a)+\delta\in\mathbf{T}_1$ and $1/y\in\mathbf{T}_1$. Since the function $L_{1,d}$ maps $\mathbf{T}_1$ injectively to $\mathbf{T}_1$, there is a unique $y\in\mathbb{F}_{2^m}$ satisfying Eq. (3). Hence there is a unique $x\in\mathbb{F}_{2^m}$ satisfying Eq. (1). This proves that $\frac{1}{L_d(x)+\delta}+x$ is a permutation polynomial of $\mathbb{F}_{2^m}$.

Assume that for any $\delta\in\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta)=1$, the function $\frac{1}{L_d(x)+\delta}+x$ is a permutation polynomial of $\mathbb{F}_{2^m}$. Now given any element $b\in\mathbf{T}_1$, consider the equation $L_{1,d}(y)=y+L_d(1/y)=b$. Since $L_{1,d}(0)=0$, let $z=1/y$. Then the equation becomes $1/z+L_d(z)=b$. Since $z\neq 0$ and $L_d(z)+b\neq 0$, this can be reformulated as $\frac{1}{L_d(z)+b}+z=0$. From the hypothesis, this equation has a unique root $z\in\mathbb{F}_{2^m}$. Hence there exists a $y\in\mathbb{F}_{2^m}$ such that $L_{1,d}(y)=y+L_d(1/y)=b$. Moreover, $\mathrm{Tr}(y)=\mathrm{Tr}(y+L_d(1/y))=\mathrm{Tr}(b)=1$ as $w(d)$ is even. Hence we have $y\in\mathbf{T}_1$. It then follows that $L_{1,d}(y)=y+L_d(1/y)$ maps $\mathbf{T}_1$ injectively to $\mathbf{T}_1$, and hence $L_{1,d}$ is a Kloosterman polynomial. □

In the remainder of this section, we present several classes of permutation polynomials related to the Kloosterman polynomial $L_{1,10}$. We first present the following two lemmas that will be needed in the sequel.

Lemma 2.2. *Let m be a positive integer. Let $u,v\in\mathbb{F}_{2^m}$ with $u\neq 0$. The equation $x^2+ux+v=0$ has roots in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(v/u^2)=0$.*

Lemma 2.3. *(See [4].) Let m be a positive integer. Let k be an integer in $\{1,\dots,m-1\}$ with $\gcd(k,m)=1$, and let $r\in\{1,\dots,m-1\}$ be such that $kr\equiv 1 \pmod m$. Define the integer m' by $kr=1+mm'$ and write $\sigma=2^k$. For $\alpha,\beta\in\{0,1\}$, we define the polynomials*

$$f_\alpha(X)=\alpha\,\mathrm{Tr}(X)+\sum_{i=0}^{r-1}X^{\sigma^i}$$

and

$$g_\beta(X) = \beta \operatorname{Tr}(X) + \sum_{j=0}^{k-1} X^{2^j}.$$

The functions f_α and g_β have the following properties:

1. *g_β is a permutation on $\mathbb{F}_{2^m}$ if and only if $k + \beta m \equiv 1 \pmod 2$.*
2. *For every $x \in \mathbb{F}_{2^m}$, we have $f_\alpha(g_\beta(x)) = g_\beta(f_\alpha(x)) = x + \omega \operatorname{Tr}(x)$ with*

$$\omega = m' + \alpha k + \beta r + \alpha\beta m.$$

The following proposition describes a class of permutation polynomials of $\mathbb{F}_{2^m}$ related to $L_{1,10}$.

Proposition 2.4. *Let m be a positive integer, and let δ be an element of $\mathbb{F}_{2^m}$ with $\operatorname{Tr}(\delta) = 1$. Then $h(x) = (\frac{1}{x^4+x+\delta})^2 + x$ is a permutation function of $\mathbb{F}_{2^m}$.*

Proof. Assume there exist elements x, y in $\mathbb{F}_{2^m}$ such that $x \neq y$ and $h(x) = h(y)$. Then we have

$$x + y = \left(\frac{1}{x^4 + x + \delta}\right)^2 + \left(\frac{1}{y^4 + y + \delta}\right)^2 \tag{4}$$

$$= \left(\frac{x^4 + y^4 + x + y}{(x^4 + x + \delta)(y^4 + y + \delta)}\right)^2. \tag{5}$$

Let $s = x + y$ and $t = xy$, then $s \neq 0$. We write $s^{2^{m-1}}$ as $\sqrt{s}$. Raising both sides of (5) to the power of 2^{m-1}, we have

$$\sqrt{s} = \frac{x^4 + y^4 + x + y}{(x^4 + x + \delta)(y^4 + y + \delta)}. \tag{6}$$

We have $(x^4 + x + \delta)(y^4 + y + \delta) = t^4 + st(s^2 + t) + \delta s^4 + t + \delta s + \delta^2$. Thus (6) becomes

$$\sqrt{s} = \frac{s^4 + s}{t^4 + st(s^2 + t) + \delta s^4 + t + \delta s + \delta^2}. \tag{7}$$

Since $s \neq 0$, writing (7) as an equation in t, we have

$$t^4 + st^2 + \left(s^3 + 1\right)t + \delta s^4 + \delta s + \delta^2 + \left(s^4 + s\right)/\sqrt{s} = 0. \tag{8}$$

Writing $T = t^2 + (s + 1)t$, we can rewrite (8) as

$$T^2 + \left(s^2 + s + 1\right)T + \delta s^4 + \delta s + \delta^2 + \left(s^4 + s\right)/\sqrt{s} = 0. \tag{9}$$

We claim that $s^2+s+1\neq 0$. Otherwise, suppose $s^2+s+1=0$. Then $s^3=1$. Since $y=x+s$, we have $y^4+y+\delta=x^4+s^4+x+s+\delta=x^4+x+\delta+s(s^3-1)=x^4+x+\delta$. Thus (4) becomes $s=0$, which contradicts our assumption.

By Lemma 2.2, Eq. (9) has a solution T in $\mathbb{F}_{2^m}$ if and only if $A=0$, where

$$A=\mathrm{Tr}\left(\frac{\delta s^4+\delta s+\delta^2+(s^4+s)/\sqrt{s}}{(s^2+s+1)^2}\right).$$

On the other hand, we have

$$\begin{aligned}
A&=\mathrm{Tr}\left(\frac{\delta(s^4+s^2+1)+\delta(s^2+s+1)+\delta^2+(s^4+s)/\sqrt{s}}{s^4+s^2+1}\right)\\
&=\mathrm{Tr}\left(\delta+\frac{\delta}{s^2+s+1}+\left(\frac{\delta}{s^2+s+1}\right)^2+\frac{(s^4+s)/\sqrt{s}}{s^4+s^2+1}\right)\\
&=1+\mathrm{Tr}\left(\frac{(s^4+s)/\sqrt{s}}{s^4+s^2+1}\right)\\
&=1+\mathrm{Tr}\left(\frac{(s^8+s^2)}{s(s^8+s^4+1)}\right)\\
&=1+\mathrm{Tr}\left(\frac{s^7+s}{s^8+s^4+1}\right).
\end{aligned}$$

Note that

$$\begin{aligned}
\frac{s^7+s}{s^8+s^4+1}&=\frac{s(s^2+1)(s^4+s^2+1)}{(s^4+s^2+1)^2}\\
&=\frac{s^3+s}{s^4+s^2+1}\\
&=\frac{s(s^2+s+1)+s^2}{s^4+s^2+1}\\
&=\frac{s}{s^2+s+1}+\left(\frac{s}{s^2+s+1}\right)^2.
\end{aligned}$$

So we have $A=1$. Hence (9) has no solution T in $\mathbb{F}_{2^m}$, and there do not exist distinct elements $x, y\in\mathbb{F}_{2^m}$ with $h(x)=h(y)$. □

Remark. Proposition 2.4 can also be proved with the help of [3, Theorem 4.1] and Proposition 2.1. But we prefer the direct proof above.

As byproducts, in the case that m is odd, we have the following permutation polynomials of the form $(x^2+x+\delta)^{-2}+L_c(x)$ over $\mathbb{F}_{2^m}$.

Corollary 2.5. *If $m \equiv 1 \pmod 4$ and δ is an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta) = 1$, then*

$$l_1(x) = \frac{1}{(x^2+x+\delta)^2} + \sum_{i=0}^{(m-1)/2} x^{2^{2i}}$$

is a permutation of $\mathbb{F}_{2^m}$.

Proof. We apply Lemma 2.3, with $k = 2$, $r = (m+1)/2$, $m' = 1$, $\alpha = 0$, $\beta = 1$. Note that $g_1(x) = x^2 + x + \mathrm{Tr}(x)$ is a permutation polynomial of $\mathbb{F}_{2^m}$. We have $\omega = m' + \alpha k + \beta r + \alpha\beta m = m' + \beta r = 1 + (m+1)/2 = 0$, and so $f_0(g_1(x)) = x + \omega\,\mathrm{Tr}(x) = x$. Note that $l_1(x) = \frac{1}{(x^2+x+\delta)^2} + f_0(x)$. Hence

$$l_1\big(g_1(x)\big) = \frac{1}{(g_1(x)^2 + g_1(x) + \delta)^2} + f_0\big(g_1(x)\big) = \frac{1}{(x^4+x+\delta)^2} + x = h(x).$$

Thus $l_1(z) = h(g_1^{-1}(z))$ is a permutation of $\mathbb{F}_{2^m}$ since both g_1 and h are permutations of $\mathbb{F}_{2^m}$. □

Corollary 2.6. *If $m \equiv 3 \pmod 4$ and δ is an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta) = 1$, then*

$$l_2(x) = \frac{1}{(x^2+x+\delta)^2} + \sum_{i=0}^{(m-1)/2} x^{2^{2i}} + \mathrm{Tr}(x)$$

is a permutation of $\mathbb{F}_{2^m}$.

Proof. We apply Lemma 2.3, with $k = 2$, $r = (m+1)/2$, $m' = 1$, $\alpha = 0$, $\beta = 1$. Note that $g_1(x) = x^2 + x + \mathrm{Tr}(x)$ is a permutation polynomial of $\mathbb{F}_{2^m}$. We have $\omega = m' + \alpha k + \beta r + \alpha\beta m = m' + \beta r = 1 + (m+1)/2 = 1$, and so $f_0(g_1(x)) = x + \omega\,\mathrm{Tr}(x) = x + \mathrm{Tr}(x)$. Note that $l_2(x) = \frac{1}{(x^2+x+\delta)^2} + f_0(x) + \mathrm{Tr}(x)$. It follows that

$$\begin{aligned} l_2\big(g_1(x)\big) &= \frac{1}{(g_1(x)^2 + g_1(x) + \delta)^2} + f_0\big(g_1(x)\big) + \mathrm{Tr}\big(g_1(x)\big) \\ &= \frac{1}{(x^4+x+\delta)^2} + x = h(x). \end{aligned}$$

Thus $l_2(z) = h(g_1^{-1}(z))$ is a permutation of $\mathbb{F}_{2^m}$ since both g_1 and h are permutations of $\mathbb{F}_{2^m}$. □

3. Two classes of permutation polynomials on $\mathbb{F}_{2^m}$ for odd m

In this section, we consider permutation polynomials over $\mathbb{F}_{2^m}$ of the form $f(x) = (x^2 + x + \delta)^s + \mathrm{Tr}(x)$ where $\mathrm{Tr}(\delta) = 1$. If m is even, then $f(x)$ cannot be a permutation since $f(0) = f(1)$. For small values of odd m we ran a computer search and recorded the numerical results in Table 1. Here $S = \{1 \leqslant s \leqslant q-1\colon\ (x^2+x+\delta)^s + \mathrm{Tr}(x)$ is a permutation polynomial of $\mathbb{F}_{2^m}\}$, and α is

Table 1
Values of s such that $(x^2+x+\delta)^s+\mathrm{Tr}(x)$ permutes $\mathbb{F}_{2^m}$

m	α's minimal polynomial	δ	Values of s
3	$\alpha^3+\alpha+1$	α^3	1, 3, 5
5	$\alpha^5+\alpha^2+1$	α^3	1, 7, 11, 19, 25
7	$\alpha^7+\alpha+1$	α^7	1, 15, 27, 43, 45, 51, 71, 77, 85, 89, 99, 113
9	$\alpha^9+\alpha^4+1$	α^5	1, 31, 57, 71, 103, 115, 171, 173, 213, 271, 291, 307, 313, 341, 391, 401, 409, 451, 481

a primitive element of $\mathbb{F}_{2^m}$. From every cyclotomic coset modulo 2^m-1, we only record one value of s.

In Table 1, the value $s=1$ is explained by the following simple result, as x^2+x has only two zeros 0 and 1 in $\mathbb{F}_{2^m}$.

Proposition 3.1. *Let m be an odd integer, and let c be an integer in $\{1,2,\ldots,2^m-1\}$ with even weight. Then $L_c(0)=L_c(1)=0$ in $\mathbb{F}_{2^m}$. Assume that 0 and 1 are the only zeros of $L_c(x)$ in $\mathbb{F}_{2^m}$. Then $L_c(x)+\mathrm{Tr}(x)$ is a permutation polynomial of $\mathbb{F}_{2^m}$.*

Proof. Note that $\mathrm{Tr}(1)=1$ since m is odd. Assume that there exist $a,b\in\mathbb{F}_{2^m}$, $a\neq b$, with $L_c(a)+\mathrm{Tr}(a)=L_c(b)+\mathrm{Tr}(b)$. We consider the following two cases.

If $\mathrm{Tr}(a)=\mathrm{Tr}(b)$, then we have $L_c(a-b)=L_c(a)-L_c(b)=0$. Thus $a-b=0$ or 1. Since $a\neq b$, we have $a-b=1$. Thus $\mathrm{Tr}(a)-\mathrm{Tr}(b)=\mathrm{Tr}(1)=1$. This is a contradiction.

If $\mathrm{Tr}(a)\neq\mathrm{Tr}(b)$, then we have $L_c(a)=L_c(b)+1$. Thus $\mathrm{Tr}(L_c(a))=\mathrm{Tr}(L_c(b))+\mathrm{Tr}(1)=\mathrm{Tr}(L_c(b))+1$. However, since the weight of c is even, we have that $\mathrm{Tr}(L_c(a))=\mathrm{Tr}(L_c(b))=0$. This is also a contradiction.

Thus $L_c(x)+\mathrm{Tr}(x)$ is a permutation polynomial of $\mathbb{F}_{2^m}$. □

All the remaining values of s in Table 1 are explained by the following result.

Proposition 3.2. *Let m be odd and let δ be an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta)=1$. Let i, j be integers with $0\leqslant i<j\leqslant m-1$. Let e be any positive integer with $(2^i+2^j)\cdot e\equiv 1 \pmod{2^m-1}$. Then*

$$f(x)=\left(x^2+x+\delta\right)^e+\mathrm{Tr}(x)$$

is a permutation polynomial of $\mathbb{F}_{2^m}$.

Proof. Since m is odd, it is easy to prove that $\gcd(2^i+2^j,2^m-1)=1$ (see e.g. [1, Lemma 2.1]). Thus such an e exists for any i, j with $0\leqslant i<j\leqslant m-1$.

Assume there exist distinct elements $x,y\in\mathbb{F}_{2^m}$ such that $f(x)=f(y)=a$ for some $a\in\mathbb{F}_{2^m}$. We now claim that $\mathrm{Tr}(x)\neq\mathrm{Tr}(y)$. Otherwise, suppose $\mathrm{Tr}(x)=\mathrm{Tr}(y)$. Then we have $(x^2+x+\delta)^e=(y^2+y+\delta)^e$. Thus $x^2+x+\delta=y^2+y+\delta$. It follows that $(x+y)(x+y+1)=0$. Since $x\neq y$, we have $x=y+1$. Then $\mathrm{Tr}(x)=\mathrm{Tr}(y)+\mathrm{Tr}(1)=\mathrm{Tr}(y)+1$ since m is odd. This is contrary to the assumption that $\mathrm{Tr}(x)=\mathrm{Tr}(y)$.

Now without loss of generality, assume that $\mathrm{Tr}(x)=0$ and $\mathrm{Tr}(y)=1$. We rewrite $f(x)=a$ as

$$\left(x^2+x+\delta\right)^e=\mathrm{Tr}(x)+a. \tag{10}$$

Raising both sides of (10) to the power of $2^i + 2^j$, we obtain that

$$x^2 + x + \delta = \big(\mathrm{Tr}(x) + a\big)^{2^i+2^j},$$

which can be reformulated as

$$x^2 + x + \delta = \mathrm{Tr}(x)\big(1 + a^{2^i} + a^{2^j}\big) + a^{2^i+2^j}. \tag{11}$$

Since $\mathrm{Tr}(x) = 0$, taking the trace function of both sides of (11), we have $\mathrm{Tr}(a^{2^i+2^j}) = 1$.

Similarly, we have the equation

$$y^2 + y + \delta = \mathrm{Tr}(y)\big(1 + a^{2^i} + a^{2^j}\big) + a^{2^i+2^j}. \tag{12}$$

Since $\mathrm{Tr}(y) = 1$, we obtain that $1 = \mathrm{Tr}(1) + \mathrm{Tr}(a^{2^i+2^j})$. Thus we have $\mathrm{Tr}(a^{2^i+2^j}) = 0$, which is a contradiction. □

4. Three classes of permutation polynomials on $\mathbb{F}_{2^m}$ for even m

In this section, we first prove that permutation polynomials of a particular form always appear in pairs when m is even. We then describe three classes of permutations polynomials over $\mathbb{F}_{2^m}$ for even m.

Two functions f and g from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ are said *permutation equivalent* if f induces a permutation of $\mathbb{F}_{2^m}$ if and only if g induces a permutation of $\mathbb{F}_{2^m}$.

Proposition 4.1. *Let m be even, δ be an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta) = 1$, and let $h(x)$ be any function from $\mathbf{T}_1$ to $\mathbb{F}_{2^m}$. Assume that s and t are integers in $\{1, 2, \ldots, 2^m - 1\}$ such that $w(s)$ is even and $w(t)$ is odd. Let $f_1(x) = h(L_s(x) + \delta) + L_t(x)$ and $f_2(x) = f_1(x) + \mathrm{Tr}(x)$. Then f_1 and f_2 are permutation equivalent.*

Proof. Assume that f_1 induces a permutation of $\mathbb{F}_{2^m}$. We now prove that f_2 also induces a permutation of $\mathbb{F}_{2^m}$. Assume there exist $a, b \in \mathbb{F}_{2^m}$ with $f_2(a) = f_2(b)$. We consider the following two cases.

If $\mathrm{Tr}(a) = \mathrm{Tr}(b)$, then from $f_1(a) + \mathrm{Tr}(a) = f_2(a) = f_2(b) = f_1(b) + \mathrm{Tr}(b)$ we have $f_1(a) = f_1(b)$. Since f_1 is a permutation of $\mathbb{F}_{2^m}$, we have $a = b$.

If $\mathrm{Tr}(a) \neq \mathrm{Tr}(b)$, without loss of generality, assume that $a \in \mathbf{T}_1$ and $b \in \mathbf{T}_0$. From $f_2(a) = f_2(b)$ and $f_2(x) = f_1(x) + \mathrm{Tr}(x)$ we have that $f_1(a) + 1 = f_1(b)$. Let $\bar{a} = a + 1$. Then we have $L_s(\bar{a}) = L_s(a)$ since $w(s)$ is even. Note that $L_t(\bar{a}) = L_t(a) + 1$ because $w(t)$ is odd. We also have $\mathrm{Tr}(\bar{a}) = \mathrm{Tr}(a + 1) = \mathrm{Tr}(a) = 1$ since m is even. Thus we have $f_1(\bar{a}) = h(L_s(\bar{a}) + \delta) + L_t(\bar{a}) = h(L_s(a) + \delta) + L_t(a) + 1 = f_1(a) + 1 = f_1(b)$. However, we have $\bar{a} \neq b$ since $\bar{a} \in \mathbf{T}_1$, $b \in \mathbf{T}_0$. This contradicts the fact that f_1 is a permutation of $\mathbb{F}_{2^m}$. Hence f_2 is a permutation of $\mathbb{F}_{2^m}$ given that f_1 is a permutation of $\mathbb{F}_{2^m}$.

By definition, we have

$$f_1(x) = f_2(x) + \mathrm{Tr}(x) = h\big(L_s(x) + \delta\big) + L_t(x) + \mathrm{Tr}(x) = h\big(L_s(x) + \delta\big) + L_{t'}(x),$$

where $t' = 2^m - 1 - t$. Since $w(t)$ is odd and m is even, $w(t')$ is odd. Hence by symmetry and the proof above, f_1 is a permutation of $\mathbb{F}_{2^m}$ if f_2 is a permutation of $\mathbb{F}_{2^m}$. □

Applying Proposition 4.1 to [2, Lemma 1], Proposition 2.4 of this paper, and [7, Theorems 3.1 and 3.3], we have the following results.

Corollary 4.2. *Let m be even, and let δ be an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(\delta) = 1$. We have the following classes of permutation polynomials of $\mathbb{F}_{2^m}$:*

- $f_1(x) = \frac{1}{L_d(x)+\delta} + x + \mathrm{Tr}(x)$, *where* $d = 3, 6, 10$.
- $f_2(x) = (\frac{1}{x^2+x+\delta})^{2^{m-1}+2^{m/2-1}-1} + x + \mathrm{Tr}(x)$.
- $f_3(x) = (x^2 + x + \delta)^{(2^{m+1}-2^{m/2}-1)/3} + x + \mathrm{Tr}(x)$.

5. Three classes of permutation polynomials on $\mathbb{F}_{3^m}$

In the concluding remarks of [3], Hollmann and Xiang mentioned the fact that over $\mathbb{F}_{3^m}$, $x \mapsto x - 1/x + 1/x^3$ is injective outside $\mathbf{T}_0$. This motivated us to consider whether $\frac{1}{x^3-x+\delta} + x$ is a permutation of $\mathbb{F}_{3^m}$ where $\mathrm{Tr}(\delta) \neq 0$.

In this section, we first prove the following result about quartic equations.

Lemma 5.1. *Let m be a positive integer, and let b be an element of $\mathbb{F}_{3^m}$ with $\mathrm{Tr}(b) \neq 0$. Then the quartic equation*

$$x^4 - x^2 + bx + 1 = 0 \tag{13}$$

has at most one solution in $\mathbb{F}_{3^m}$.

Proof. Suppose on the contrary that (13) has two solutions x and $x + a$, where $a \neq 0$. Clearly $x \neq 0$ and $x \neq -a$. We have then

$$\begin{cases} x^4 - x^2 + bx + 1 = 0, \\ (x+a)^4 - (x+a)^2 + b(x+a) + 1 = 0. \end{cases} \tag{14}$$

Hence

$$\begin{cases} x^4 - x^2 + bx + 1 = 0, \\ x^3 + \left(a^2+1\right)x + a^3 - a + b = 0. \end{cases} \tag{15}$$

It follows that $a^2 \neq 1$ because $\mathrm{Tr}(b) \neq 0$. By (15) we have

$$\begin{cases} x^4 - x^2 + bx + 1 = 0, \\ \left(a^2-1\right)x^2 + a\left(a^2-1\right)x - 1 = 0. \end{cases} \tag{16}$$

Note that $x \neq 0$. The second equation in (16) yields

$$\left(\frac{1}{x}\right)^2 + 2a\left(a^2-1\right)\frac{1}{x} - \left(a^2-1\right) = 0.$$

It then follows that

$$\left(\frac{1}{x} + \left(a^3 - a\right)\right)^2 = \left(a^2 - 1\right)\left(a^2 + 1\right)^2. \tag{17}$$

Therefore, $a^2 - 1$ must be a square. Assume that $a^2 - 1 = A^2$, where $A \in \mathbb{F}_{3^m}$. Then by (17)

$$\frac{1}{x} = -\left(a^3 - a\right) \pm \left(A^3 - A\right).$$

Hence $\mathrm{Tr}(1/x) = 0$. But $\mathrm{Tr}(b) = \mathrm{Tr}(-x^3 + x - 1/x) = \mathrm{Tr}(-1/x) = 0$. This is contrary to the assumption that $\mathrm{Tr}(b) \neq 0$. The proof is completed. □

The first class of permutation polynomials on $\mathbb{F}_{3^m}$ is described by the following proposition.

Proposition 5.2. *Let m be a positive integer, and let δ be an element of $\mathbb{F}_{3^m}$ with $\mathrm{Tr}(\delta) \neq 0$. Then $\frac{1}{x^3 - x + \delta} + x$ is a permutation of $\mathbb{F}_{3^m}$.*

Proof. It suffices to prove that the following equation

$$\frac{1}{x^3 - x + \delta} + x = a \tag{18}$$

has at most one solution for each $a \in \mathbb{F}_{3^m}$.

We rewrite (18) as

$$\left(x^3 - x + \delta\right)(x - a) + 1 = 0.$$

Set $y = x - a$. Then the above equation has the same number of solutions x as that of the following equation:

$$y^4 - y^2 + \left(\delta - \left(a^3 - a\right)\right)y + 1 = 0$$

in y. The conclusion then follows from Lemma 5.1. □

We are now interested in values of s with $2 \leqslant s \leqslant 3^m - 2$ such that $(x^3 - x + \delta)^s + x$ is a permutation of $\mathbb{F}_{3^m}$. For small values of m, we recorded the experimental results in Table 2, where α is a primitive element of $\mathbb{F}_{3^m}$, and $\mathrm{Tr}(\delta) \neq 0$.

In Table 2, the values of s marked with ^{a} are covered by Proposition 5.2, and those marked with ^{b} correspond to linearized permutation polynomials. We now explain those marked with ^{c} and ^{d}.

Table 2
Values of s such that $(x^3 - x + \delta)^s + x$ permutes $\mathbb{F}_{3^m}$

m	α's minimal polynomial	δ	Values of s
3	$\alpha^3 - \alpha + 1$	α^2	$3^b, 9^b, 11, 13^c, 16, 21^d, 24, 25^a$
4	$\alpha^4 - \alpha^3 - 1$	α	$9^b, 30, 40^c, 79^a$
5	$\alpha^5 - \alpha + 1$	α^4	$3^b, 9^b, 27^b, 81^b, 97^d, 121^c, 241^a$
6	$\alpha^6 - \alpha^4 + \alpha^2 - \alpha - 1$	α^2	$9^b, 81^b, 364^c, 727^a$

Proposition 5.3. *Let $q = p^m$ be a prime power. Let $h(x)$ be a function defined over $\mathbb{F}_q$. Let $L(x)$ be a linearized polynomial over $\mathbb{F}_q$ such that for any $a, b \in \mathbb{F}_q$, $h(a) - h(b) \in \ker(L) := \{x \in \mathbb{F}_q \mid L(x) = 0\}$. Then $f(x) = h(L(x) + c) + x$ is a permutation polynomial of $\mathbb{F}_q$ for any $c \in \mathbb{F}_q$.*

Proof. Assume there exist $x, y \in \mathbb{F}_q$ such that $f(x) = f(y)$. Then we have $x - y = h(L(y) + c) - h(L(x) + c) \in \ker(L)$. So $L(x) = L(y)$, which in turn implies $x - y = h(L(y) + c) - h(L(x) + c) = 0$. Hence f is a permutation over $\mathbb{F}_q$. □

An example is the permutation functions $\eta(x^3 - x + c) + x$ of $\mathbb{F}_{3^m}$, where η is the quadratic character of $\mathbb{F}_{3^m}$ and $c \in \mathbb{F}_{3^m}$. This explains the values marked with ^{c} above.

The following proposition explains the values of s marked with ^{d} in Table 2.

Proposition 5.4. *Let m be odd, and let b be any element of $\mathbb{F}_{3^m}$. If $m \equiv 3 \pmod 4$, then the function*

$$f(x) = \left(x^3 - x + b\right)^{\frac{4 \cdot 3^m - 3}{5}} + x$$

is a permutation polynomial of $\mathbb{F}_{3^m}$.

If $m \equiv 1 \pmod 4$, then the function

$$f(x) = \left(x^3 - x + b\right)^{\frac{2 \cdot 3^m - 1}{5}} + x$$

is a permutation polynomial of $\mathbb{F}_{3^m}$.

Proof. We have $\frac{4 \cdot 3^m - 3}{5} \equiv 5^{-1} \pmod{3^m - 1}$ when $m \equiv 3 \pmod 4$ and $\frac{2 \cdot 3^m - 1}{5} \equiv 5^{-1} \pmod{3^m - 1}$ when $m \equiv 1 \pmod 4$. Let $a \in \mathbb{F}_{3^m}$. We need to prove $f(x) = a$ has exactly one solution in $\mathbb{F}_{3^m}$.

Since m is odd, $\gcd(5, 3^m - 1) = 1$. $f(x) = a$ is equivalent to

$$x^3 - x + b = (a - x)^5.$$

Let $x - a = y$. Then $y^5 + (y + a)^3 - (y + a) + b = 0$, i.e., $y^5 + y^3 - y = -a^3 + a - b$. Since $\gcd(5, 3^{2m} - 1) = 1$, $y^5 + y^3 - y$ is a Dickson permutation polynomial [5]. So $f(x)$ is a permutation on $\mathbb{F}_{3^m}$. □

It is open whether the remaining unexplained values of s in Table 2 lead to new classes of permutation polynomials.

6. Concluding remarks

The Kloosterman sum $K(a)$ over $\mathbb{F}_{2^m}$ is defined for any $a \in \mathbb{F}_{2^m}$ by

$$K(a) = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(ax + \frac{1}{x})}.$$

Helleseth and Zinoviev [2] proved two identities involving Kloosterman sums, and proved that $1/(x^2 + x + \delta)^s + x$ is a permutation polynomial of $\mathbb{F}_{2^m}$ where $s = 1$ or 2, and δ is an element

with $\mathrm{Tr}(\delta) = 1$. in [7], more permutation polynomials of this form are derived. This paper is a continuation of earlier works in [2–4,7].

Acknowledgments

The authors thank the referee for his/her constructive comments that improved the presentation of this paper.

The research of Jin Yuan and Huaxiong Wang is supported by the ARC Grant DP0558773. The research of Cunsheng Ding is supported by the Research Grants Council of the Hong Kong Special Administrative Region, China, Proj. No. 612405.

References

[1] R.S. Coulter, On the evaluation of a class of Weil sums in characteristic 2, New Zealand J. Math. 28 (1999) 171–184.
[2] T. Helleseth, V. Zinoviev, New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m, Finite Fields Appl. 9 (2003) 187–193.
[3] H.D.L. Hollmann, Q. Xiang, Kloosterman sum identities over $\mathbb{F}_{2^m}$, Discrete Math. 279 (2004) 277–286.
[4] H.D. Hollmann, Q. Xiang, A class of permutation polynomials of $\mathbb{F}_{2^m}$ related to Dickson polynomials, Finite Fields Appl. 11 (1) (2005) 111–122.
[5] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Longman, 1993.
[6] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[7] J. Yuan, C. Ding, Four classes of permutation polynomials of $\mathbb{F}_{2^m}$, Finite Fields Appl. 13 (4) (2007) 869–876.