Bull. Aust. Math. Soc. **89** (2014), 420–430
doi:10.1017/S0004972713000646

CONSTRUCTING PERMUTATION POLYNOMIALS OVER FINITE FIELDS

XIAOER QIN and SHAOFANG HONG ✉

(Received 3 June 2013; accepted 11 June 2013; first published online 7 August 2013)

Abstract

In this paper, we construct several new permutation polynomials over finite fields. First, using the linearised polynomials, we construct the permutation polynomial of the form $\sum_{i=1}^{k}(L_i(x)+\gamma_i)h_i(B(x))$ over $\mathbf{F}_{q^m}$, where $L_i(x)$ and $B(x)$ are linearised polynomials. This extends a theorem of Coulter, Henderson and Matthews. Consequently, we generalise a result of Marcos by constructing permutation polynomials of the forms $xh(\lambda_j(x))$ and $xh(\mu_j(x))$, where $\lambda_j(x)$ is the jth elementary symmetric polynomial of $x, x^q, \ldots, x^{q^{m-1}}$ and $\mu_j(x) = \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^j)$. This answers an open problem raised by Zieve in 2010. Finally, by using the linear translator, we construct the permutation polynomial of the form $L_1(x) + L_2(\gamma)h(f(x))$ over $\mathbf{F}_{q^m}$, which extends a result of Kyureghyan.

2010 *Mathematics subject classification*: primary 11T06; secondary 12E20.

Keywords and phrases: permutation polynomial, linearised polynomial, linear translator, elementary symmetric polynomial.

1. Introduction

Let $\mathbf{F}_q$ denote the finite field of characteristic p with q elements ($q = p^n$, $n \in \mathbb{N}$), and let $\mathbf{F}_q^* := \mathbf{F}_q \setminus \{0\}$. Let $\mathbf{F}_q[x]$ be the ring of polynomials over $\mathbf{F}_q$ in the indeterminate x. If the polynomial $f(x) \in \mathbf{F}_q[x]$ induces a bijective map from $\mathbf{F}_q$ to itself, then $f(x)$ is called a *permutation polynomial* of $\mathbf{F}_q$. Permutation polynomials have been an interesting subject of study in the area of finite fields for many years. Particularly, permutation polynomials have many important applications in coding theory [5], cryptography [10] and combinatorial design theory. Information about properties, constructions and applications of permutation polynomials may be found in Lidl and Niederreiter [7].

Let $m > 1$ be a given integer. By $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$ we denote the *trace* from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$, that is,

$$\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

Hong was supported partially by the PhD Programs Foundation of Ministry of Education of China Grant #20100181110073.

A polynomial of the form

$$L(x) = \sum_{i=0}^{m-1} a_i x^{q^i} \in \mathbf{F}_{q^m}[x]$$

is called a *linearised polynomial* over $\mathbf{F}_{q^m}$. It is well known that a linearised polynomial $L(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if the set of roots in $\mathbf{F}_{q^m}$ of $L(x)$ equals $\{0\}$ (see, for example, [7, Theorem 7.9]). Throughout, $L(x)$ denotes a linearised polynomial.

To find new classes of permutation polynomials is one of the open problems raised by Lidl and Mullen [6]. There has been significant progress in finding new permutation polynomials. Wan and Lidl [11], Masuda and Zieve [9] and Zieve [13] constructed permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and studied their group structure. Zieve [12] characterised the permutation polynomial of the form $x^r(1 + x^v + x^{2v} + \cdots + x^{kv})^t$. Ayad *et al.* [1] obtained some permutation binomials and proved the bound of p, if $ax^n + x^m$ permutes $\mathbf{F}_p$. A number of classes of permutation polynomials related to the trace functions were constructed. Recently, Coulter *et al.* [3] constructed the permutation polynomials of the form $L(x) + xh(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$. Marcos [8] obtained permutation polynomials of the form $bL(x) + \gamma h(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$. Zieve [14] presented rather more general versions of the first four constructions from [8]. But how to extend the fifth construction from [8] to a more general version is an interesting open problem raised in [14]. For some other permutation polynomials constructed by using the trace function, readers are referred to [2].

The main goal of the present paper is to construct new classes of permutation polynomials over finite fields. In Section 2, we construct some permutation polynomials using linearised polynomials. In fact, we obtain a characterisation so that $\sum_{i=1}^{k}(L_i(x) + \gamma_i)h_i(B(x)) \in \mathbf{F}_{q^m}[x]$, with $L_i(x)$ and $B(x)$ being linearised polynomials, is a permutation polynomial. See Theorem 2.2 below, which extends the results obtained by Coulter *et al.* [3] and by Marcos [8], respectively.

For any positive integer j, let $\mu_j(x) = \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^j)$ $(j \le q^m - 1)$ and $\lambda_j(x) = \sigma_j(x, x^q, \ldots, x^{q^{m-1}})$ $(j \le m - 1)$, where $\sigma_j(x, x^q, \ldots, x^{q^{m-1}})$ is the jth elementary symmetric polynomial of $x, x^q, \ldots, x^{q^{m-1}}$. Marcos [8] used the function $\lambda(x)$ (equal to $\lambda_2(x)$ or $\mu_2(x)$) to construct permutation polynomials and only obtained some sufficient conditions for $xh(\lambda(x))$ to be a permutation polynomial. In Section 3, using $\lambda_j(x)$ and $\mu_j(x)$, we extend this result of Marcos [8] by giving sufficient and necessary conditions for $xh(\lambda_j(x))$ and $xh(\mu_j(x))$ to be permutation polynomials. This answers an open problem raised by Zieve [14].

In Section 4, by using the technique of linear translator (see Section 4 for its definition), we construct the permutation polynomial of the form $L_1(x) + L_2(\gamma)h(f(x))$. This result generalises one of the main results in [4].

2. Permutation polynomials constructed by the linearised polynomials

In this section, we construct a new class of permutation polynomials involving linearised polynomials. We need the following results in the sequel.

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

LEMMA 2.1. *Let $B(x) \in \mathbf{F}_q[x]$ and $L(x) \in \mathbf{F}_q[x]$ be linearised polynomials. Then, for any $a \in \mathbf{F}_q$ and x and $y \in \mathbf{F}_{q^m}$, $aB(x) = B(ax)$, $B(x+y) = B(x) + B(y)$ and $B(L(x)) = L(B(x))$.*

We can now give the first main result of this paper.

THEOREM 2.2. *For $1 \le i \le k$, let $\gamma_i \in \mathbf{F}_{q^m}$ and let $L_i(x), B(x) \in \mathbf{F}_q[x]$ be linearised polynomials. Let $h_i(x) \in \mathbf{F}_{q^m}[x]$ be such that $h_i(B(\mathbf{F}_{q^m})) \subseteq \mathbf{F}_q$. Then $F(x) := \sum_{i=1}^{k}(L_i(x) + \gamma_i)h_i(B(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if each of the following is true.*

(1) *$\sum_{i=1}^{k}(L_i(x) + B(\gamma_i))h_i(x)$ permutes $B(\mathbf{F}_{q^m})$.*
(2) *For any $y \in B(\mathbf{F}_{q^m})$, $\sum_{i=1}^{k} L_i(x)h_i(y) = 0$ and $B(x) = 0$ with $x \in \mathbf{F}_{q^m}$ are both true if and only if $x = 0$.*

PROOF. First we show the sufficiency part. Assume that (1) and (2) hold. Suppose that there exist two elements $\alpha, \beta \in \mathbf{F}_{q^m}$ such that $F(\alpha) = F(\beta)$. Thus $B(F(\alpha)) = B(F(\beta))$. That is,

$$B\Big(\sum_{i=1}^{k}(L_i(\alpha) + \gamma_i)h_i(B(\alpha))\Big) = B\Big(\sum_{i=1}^{k}(L_i(\beta) + \gamma_i)h_i(B(\beta))\Big). \tag{2.1}$$

Then Lemma 2.1 applied to both sides of (2.1) gives us that

$$\sum_{i=1}^{k}(L_i(B(\alpha)) + B(\gamma_i))h_i(B(\alpha)) = \sum_{i=1}^{k}(L_i(B(\beta)) + B(\gamma_i))h_i(B(\beta)). \tag{2.2}$$

Since $\sum_{i=1}^{k}(L_i(x) + B(\gamma_i))h_i(x)$ permutes $B(\mathbf{F}_{q^m})$, it follows from (2.2) that $B(\alpha) = B(\beta)$. Write $t := B(\alpha) = B(\beta)$. Then $t \in B(\mathbf{F}_{q^m})$ and $B(\alpha - \beta) = 0$. Since $F(\alpha) = F(\beta)$,

$$\sum_{i=1}^{k} L_i(\alpha - \beta)h_i(t) = 0.$$

Now applying condition (2) to $\alpha - \beta$, we obtain that $\alpha - \beta = 0$ which implies that $\alpha = \beta$. Hence $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$. The sufficiency part is proved.

Let us now show the necessity part. Let $F(x)$ be a permutation polynomial of $\mathbf{F}_{q^m}$. First we prove that (1) is true. To do so, we let $B(x)$ act on $F(x)$ for $x \in \mathbf{F}_{q^m}$, and then by Lemma 2.1 we get that

$$B(F(x)) = \sum_{i=1}^{k}(L_i(B(x)) + B(\gamma_i))h_i(B(x)). \tag{2.3}$$

Since $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$,

$$|\{B(F(x)) : x \in \mathbf{F}_{q^m}\}| = |\{B(x) : x \in \mathbf{F}_{q^m}\}| = |B(\mathbf{F}_{q^m})|. \tag{2.4}$$

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

Hence by (2.3) and (2.4),

$$\left|\left\{\sum_{i=1}^{k}(L_i(B(x))+B(\gamma_i))h_i(B(x)) : x\in \mathbf{F}_{q^m}\right\}\right| = |B(\mathbf{F}_{q^m})|.$$

This implies that $\sum_{i=1}^{k}(L_i(x)+B(\gamma_i))h_i(x)$ permutes $B(\mathbf{F}_{q^m})$. Thus (1) is proved.

It remains to show that (2) is true. For this purpose, we assume that for certain $y\in B(\mathbf{F}_{q^m})$ and $x\in\mathbf{F}_{q^m}$, we have $\sum_{i=1}^{k}L_i(x)h_i(y)=0$ and $B(x)=0$. We can take two elements $\alpha,\beta\in\mathbf{F}_{q^m}$ satisfying that $B(\alpha)=B(\beta)=y$. Then $B(\alpha-\beta)=0$. But $B(x)=0$. Therefore, $\alpha-\beta$ and x are both in the kernel $\ker(B)$ of $B(x)$. So we can write $x=\alpha-\beta+z$ for some $z\in\ker(B)$. Since $\sum_{i=1}^{k}L_i(x)h_i(y)=0$,

$$\sum_{i=1}^{k}L_i(\alpha-\beta+z)h_i(y)=0. \tag{2.5}$$

On the other hand, since $z\in\ker(B)$, we have $B(z)=0$, which implies that $B(\beta-z)=B(\alpha)=y$. It then follows immediately that

$$\begin{aligned} F(\alpha)-F(\beta-z) &= \sum_{i=1}^{k}(L_i(\alpha)+\gamma_i)h_i(B(\alpha))-\sum_{i=1}^{k}(L_i(\beta-z)+\gamma_i)h_i(B(\beta-z)) \\ &= \sum_{i=1}^{k}L_i(\alpha-\beta+z)h_i(y). \end{aligned} \tag{2.6}$$

Hence, by (2.5) and (2.6), we derive that $F(\alpha)=F(\beta-z)$. Since $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, we obtain that $\alpha-\beta+z=0$. Namely, $x=0$. Thus (2) is true. The necessity part is proved.

This completes the proof of Theorem 2.2. □

As a special case of Theorem 2.2, we have the following result.

Corollary 2.3. *Let $L_1(x), L_2(x)\in\mathbf{F}_q[x]$ be linearised polynomials. Let $h(x)\in\mathbf{F}_q[x]$ and $\gamma\in\mathbf{F}_{q^m}$. Then $F(x):=L_1(x)+(L_2(x)+\gamma)h(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if each of the following is true.*

(1) *$L_1(x)+(L_2(x)+\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma))h(x)\in\mathbf{F}_q[x]$ is a permutation polynomial over $\mathbf{F}_q$.*
(2) *For any $y\in\mathbf{F}_q$, $L_1(x)+L_2(x)h(y)=0$ and $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)=0$ with $x\in\mathbf{F}_{q^m}$ are both true if and only if $x=0$.*

From Corollary 2.3, we derive the following consequences.

Corollary 2.4 [3]. *Let $F(x):=L(x)+xh(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$ with $L(x)\in\mathbf{F}_q[x]$ being a linearised polynomial and $h(x)\in\mathbf{F}_q[x]$. Then $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if each of the following is true.*

(1) *$L(x)+xh(x)$ is a permutation polynomial over $\mathbf{F}_q$.*
(2) *For any $y\in\mathbf{F}_q$, we have that $x\in\mathbf{F}_{q^m}$ satisfies $L(x)+xh(y)=0$ and $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)=0$ if and only if $x=0$.*

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

PROOF. This follows from Corollary 2.3 by setting $L_1(x) = L(x)$, $L_2(x) = x$ and $\gamma = 0$. □

COROLLARY 2.5 [8]. *Let $L(x) = a_0x + a_1x^q + \cdots + a_{m-1}x^{q^{m-1}} \in \mathbf{F}_q[x]$ be a linearised polynomial which permutes $\mathbf{F}_{q^m}$. Let $h(x) \in \mathbf{F}_q[x]$ and $\gamma \in \mathbf{F}_{q^m}$. Then the polynomial $F(x) := L(x) + \gamma h(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$ permutes $\mathbf{F}_{q^m}$ if and only if the polynomial $(a_0 + a_1 + \cdots + a_{m-1})x + \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma)h(x)$ permutes $\mathbf{F}_q$.*

PROOF. Since $L(x)$ is a permutation of $\mathbf{F}_{q^m}$, we have that for any $x \in \mathbf{F}_{q^m}$, $L(x) = 0$ if and only if $x = 0$. So by Corollary 2.3 we know that $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if $L(x) + \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma)h(x)$ is a permutation polynomial over $\mathbf{F}_q$.

On the other hand, if $x \in \mathbf{F}_q$, we have $L(x) = (a_0 + a_1 + \cdots + a_{m-1})x$. It then follows that $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if $(a_0 + a_1 + \cdots + a_{m-1})x + \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma)h(x)$ is a permutation polynomial over $\mathbf{F}_q$, as desired. □

We now give an example to illustrate Corollary 2.3.

EXAMPLE 2.6. Let $\mathbf{F}_{q^m} = \mathbf{F}_{8^m}$ with $m > 1$ an odd integer. Let $h(x) = x^3 - ax$, $L_1(x) = a^2x$ and $L_2(x) = x^2$, where $a \in \mathbf{F}_8^*$. Then $L_1(x) + L_2(x)h(x) = D_5(x, a)$, the Dickson polynomial of degree five over $\mathbf{F}_8$. Since $\gcd(5, q^2 - 1) = 1$, by [7, Theorem 7.16] we know that $D_5(x, a)$ is a permutation polynomial over $\mathbf{F}_8$. That is, $L_1(x) + L_2(x)h(x) = x^5 - ax^3 + a^2x$ is a permutation polynomial over $\mathbf{F}_8$. Let $y \in \mathbf{F}_8$ be any element and $x \in \mathbf{F}_{q^m}$ satisfy that $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x) = 0$ and $L_1(x) + L_2(x)h(y) = 0$. If $h(y) = 0$, then $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x) = 0$ and $L_1(x) = 0$. From $L_1(x) = a^2x = 0$, we derive that $x = 0$. If $h(y) \neq 0$, it then follows from $L_1(x) + L_2(x)h(y) = 0$ that $x = 0$ or $x = a^2/(y^3 - ay) \neq 0$. Assume that $x = a^2/(y^3 - ay)$. Since m is odd and $a^2/(y^3 - ay) \neq 0$,

$$\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x) = \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}\left(\frac{a^2}{y^3 - ay}\right) = \frac{ma^2}{y^3 - ay} \neq 0.$$

Thus we conclude that for any $y \in \mathbf{F}_8$, $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x) = 0$ and $L_1(x) + L_2(x)h(y) = 0$ if and only if $x = 0$. Now, by Corollary 2.3,

$$L_1(x) + L_2(x)h(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x)) = a^2x + x^2(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x)^3 - a\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x))$$

is a permutation polynomial over $\mathbf{F}_{q^m}$.

3. Permutation polynomials constructed by the elementary symmetric polynomials

Let m and j be positive integers such that $j \leq m$. Let $\sigma_j(x_1, \ldots, x_m)$ denote the jth elementary symmetric polynomial in m variables $x_1, \ldots, x_m$. That is,

$$\sigma_j(x_1, \ldots, x_m) = \sum_{1 \leq i_1 < \cdots < i_j \leq m} x_{i_1} \cdots x_{i_j}.$$

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

Then we can define the polynomial $\lambda_j(x)$ by

$$\lambda_j(x) := \sigma_j(x, x^q, \ldots, x^{q^{m-1}}) = \sum_{0 \le i_1 < i_2 < \cdots < i_j \le m-1} x^{q^{i_1} + \cdots + q^{i_j}}.$$

Marcos [8] used the polynomials $\lambda_2(x)$ and $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^2)$ to give two sufficient conditions for $xh(\lambda_2(x))$ and $xh(\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^2))$ to be permutation polynomials.

In this section, we construct two new classes of permutation polynomials by using the functions $\lambda_j(x)$ and $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^j)$. We begin with the following two lemmas.

LEMMA 3.1. *Let $\alpha \in \mathbf{F}_{q^m}$ and $a \in \mathbf{F}_q$. Then for any positive integer j with $j \le m$, we have $\lambda_j(x) \in \mathbf{F}_q[x]$, $\lambda_j(\alpha) \in \mathbf{F}_q$, $\lambda_j(\alpha^q) = \lambda_j(\alpha)$ and $\lambda_j(a\alpha) = a^j \lambda_j(\alpha)$.*

PROOF. By the definition of λ_j, one can easily check that Lemma 3.1 is true. □

LEMMA 3.2. *For any integer j satisfying that $1 \le j \le m$ and $\gcd(j, q-1) = 1$, the mapping $\lambda_j : \mathbf{F}_{q^m} \to \mathbf{F}_q$ is onto.*

PROOF. First we show that there is an $\alpha \in \mathbf{F}_{q^m}$ such that $\lambda_j(\alpha) \ne 0$. Since $\lambda_j(x)$ has at most

$$\deg(\lambda_j(x)) = q^{m-j} + \cdots + q^{m-1} \le 1 + q + \cdots + q^{m-1} = \frac{q^m - 1}{q - 1} < q^m = |\mathbf{F}_{q^m}|$$

roots in $\mathbf{F}_{q^m}$, there exists an element $\alpha \in \mathbf{F}_{q^m}$ such that $\lambda_j(\alpha) \ne 0$. Now pick an $\alpha \in \mathbf{F}_{q^m}$ such that $a := \lambda_j(\alpha) \ne 0$. In what follows, we show that for any $b \in \mathbf{F}_q$, we can find an element $\beta \in \mathbf{F}_{q^m}$ such that $\lambda_j(\beta) = b$.

Since $\gcd(j, q-1) = 1$, by [7, Theorem 7.8] we know that ax^j is a permutation polynomial over $\mathbf{F}_q$. It follows that for any given $b \in \mathbf{F}_q$, there exists an element $c \in \mathbf{F}_q$ such that $b = ac^j$. Since $\lambda_j(\alpha) = a$, letting $\beta := c\alpha$ gives us that

$$\lambda_j(\beta) = \lambda_j(c\alpha) = c^j \lambda_j(\alpha) = ac^j = b,$$

as desired. Thus Lemma 3.2 is proved. □

Using the polynomials $\lambda_j(x)$, we can give the following characterisation of permutation polynomials of the form $xh(\lambda_j(x))$, which is the second main result of this paper.

THEOREM 3.3. *Let m and j be positive integers such that $j \le m-1$ and $\gcd(j, q-1) = 1$. Let $h(x) \in \mathbf{F}_q[x]$. Then $xh(\lambda_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if $h(0) \ne 0$ and $xh(x)^j$ permutes $\mathbf{F}_q$.*

PROOF. Write $F(x) := xh(\lambda_j(x))$. First we show the sufficiency part. Since $xh(x)^j$ permutes $\mathbf{F}_q$, we obtain that $\delta h(\delta)^j \ne 0$ for $\delta \in \mathbf{F}_q^*$. We get that $h(\delta) \ne 0$ for $\delta \in \mathbf{F}_q^*$. Hence $h(\delta) \ne 0$ for all $\delta \in \mathbf{F}_q$.

Now we choose two elements $\alpha, \beta \in \mathbf{F}_{q^m}$ such that $F(\alpha) = F(\beta)$, namely,

$$\alpha h(\lambda_j(\alpha)) = \beta h(\lambda_j(\beta)). \tag{3.1}$$

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

Then $\lambda_j(F(\alpha)) = \lambda_j(F(\beta))$. Using Lemma 3.1,

$$\lambda_j(\alpha)h(\lambda_j(\alpha))^j = \lambda_j(\beta)h(\lambda_j(\beta))^j. \tag{3.2}$$

Since $xh(x)^j$ permutes $\mathbf{F}_q$, (3.2) tells us that $\lambda_j(\alpha) = \lambda_j(\beta)$. It then follows from (3.1) and the fact that $h(\delta) \neq 0$ for all $\delta \in \mathbf{F}_q$ that $\alpha = \beta$. Hence $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$. The sufficiency part is proved.

Let us now show the necessity part. Assume that $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$. First we prove that $h(0) \neq 0$. By Lemma 3.2, we know that the mapping λ_j is onto if $\gcd(j, q-1) = 1$. For $1 \leq j \leq m-1$,

$$\deg \lambda_j(x) = q^{m-j} + \cdots + q^{m-1} \leq q + \cdots + q^{m-1}.$$

Thus, for any $a \in \mathbf{F}_q^*$, the equation $\lambda_j(x) = a$ has at most $q + \cdots + q^{m-1}$ roots in $\mathbf{F}_{q^m}$. Then the equation $\lambda_j(x) = 0$ has at least $q^m - (q-1)(q + \cdots + q^{m-1}) = q$ roots in $\mathbf{F}_{q^m}$. Hence $\lambda_j(x) = 0$ has a nonzero root in $\mathbf{F}_{q^m}$. We pick $\alpha \in \mathbf{F}_{q^m}^*$ such that $\lambda_j(\alpha) = 0$. Then $\alpha h(0) = \alpha h(\lambda_j(\alpha)) = F(\alpha)$. Since $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ and α is nonzero, we have $F(\alpha) \neq 0$. That is, $\alpha h(0) \neq 0$. Thus $h(0) \neq 0$.

It remains to show that $xh(x)^j$ permutes $\mathbf{F}_q$. On the one hand, by Lemma 3.1,

$$\lambda_j(F(x)) = \lambda_j(x)h(\lambda_j(x))^j. \tag{3.3}$$

In addition, applying Lemma 3.2, we know that for all integers j with $1 \leq j \leq m-1$ and $\gcd(j, q-1) = 1$, $\lambda_j(x)$ is a mapping from $\mathbf{F}_{q^m}$ onto $\mathbf{F}_q$. This implies that

$$\{xh(x)^j : x \in \mathbf{F}_q\} = \{\lambda_j(x)h(\lambda_j(x))^j : x \in \mathbf{F}_{q^m}\}. \tag{3.4}$$

Since $F(x)$ permutes $\mathbf{F}_{q^m}$, it then follows from (3.3) and (3.4) that

$$\begin{aligned} |\{xh(x)^j : x \in \mathbf{F}_q\}| &= |\{\lambda_j(x)h(\lambda_j(x))^j : x \in \mathbf{F}_{q^m}\}| \\ &= |\{\lambda_j(F(x)) : x \in \mathbf{F}_{q^m}\}| \\ &= |\{\lambda_j(x) : x \in \mathbf{F}_{q^m}\}| = q. \end{aligned}$$

Hence $xh(x)^j$ permutes $\mathbf{F}_q$. The necessity part is proved.

The proof of Theorem 3.3 is complete. □

Now define

$$\mu_j(x) := \sum_{i=0}^{m-1} x^{jq^i} = \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^j) \quad \text{for } 1 \leq j \leq q^m - 1.$$

Then $\mu_j(x) \in \mathbf{F}_q[x]$, $\mu_j(\alpha) \in \mathbf{F}_q$ and $\mu_j(a\alpha) = a^j\mu_j(\alpha)$ for all $a \in \mathbf{F}_q$ and $\alpha \in \mathbf{F}_{q^m}$. Also $\mu_j(x)$ is a mapping from $\mathbf{F}_{q^m}$ onto $\mathbf{F}_q$ if $\gcd(j, q^m - 1) = 1$. Replacing $\lambda_j(x)$ by $\mu_j(x)$, we can characterise the permutation polynomials of the form $xh(\mu_j(x))$ as follows. Theorem 3.4 is the third main result of this paper and its proof is similar to that of Theorem 3.3, and so we just give a sketch of the proof.

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

THEOREM 3.4. *Let m and j be positive integers such that $j \le q^m - 1$ and $\gcd(j, q^m - 1) = 1$. Let $h(x) \in \mathbf{F}_q[x]$. Then $xh(\mu_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if $h(0) \neq 0$ and $xh(x)^j$ permutes $\mathbf{F}_q$.*

PROOF. We here merely prove that if $xh(\mu_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$, then $h(0) \neq 0$. The other part of the proof is similar to that of Theorem 3.3.

Assume that $xh(\mu_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$. Clearly, there exists a nonzero element θ such that $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\theta) = 0$. Since $\gcd(j, q^m - 1) = 1$, x^j permutes $\mathbf{F}_{q^m}$. So there is a nonzero element $\omega \in \mathbf{F}_{q^m}$ such that $\omega^j = \theta$. Therefore, $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\omega^j) = 0$, that is, $\mu_j(\omega) = 0$. Then $\omega h(0) = \omega h(\mu_j(\omega))$. Since $xh(\mu_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ and ω is nonzero, we have $\omega h(0) \neq 0$. Thus $h(0) \neq 0$. Theorem 3.4 is proved. □

Picking $j = 2$, then the sufficiency part of Theorems 3.3 and 3.4 becomes [8, Proposition 12]. Evidently, Theorems 3.3 and 3.4 give an answer to the open problem raised by Zieve in [14].

4. Permutation polynomials constructed by linear translators

The main idea of this section is to construct permutation polynomials over finite fields with linear translators. We first recall the definition of linear translators as follows.

DEFINITION 4.1 [4]. Let $f : \mathbf{F}_{q^m} \to \mathbf{F}_q$, $a \in \mathbf{F}_q$ and α be a nonzero element in $\mathbf{F}_{q^m}$. If $f(x + u\alpha) - f(x) = ua$ for all $x \in \mathbf{F}_{q^m}$ and $u \in \mathbf{F}_q$, then we say that α is an *a-linear translator* of the function f. In particular, $a = f(\alpha) - f(0)$.

Using linear translators to construct permutation polynomials, we are now in a position to give the fourth main result of this paper.

THEOREM 4.2. *Let $L_1(x) \in \mathbf{F}_{q^m}[x]$ be a linearised permutation polynomial of $\mathbf{F}_{q^m}$ and $L_2(x) \in \mathbf{F}_{q^m}[x]$ be a linearised polynomial of $\mathbf{F}_{q^m}$. Let $b \in \mathbf{F}_q$, $\gamma \in \mathbf{F}_{q^m}$, $h : \mathbf{F}_q \to \mathbf{F}_q$, $f : \mathbf{F}_{q^m} \to \mathbf{F}_q$ be surjective and $L_1^{-1}L_2(\gamma)$ be a b-linear translator of f. Then $L_1(x) + L_2(\gamma)h(f(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if either $L_2(\gamma) = 0$ or $x + bh(x)$ is a permutation polynomial of $\mathbf{F}_q$.*

PROOF. Write $g(x) := x + bh(x)$ and $G(x) := L_1(x) + L_2(\gamma)h(f(x))$.

First we show the sufficiency part. Since $L_1(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$, so is $G(x)$ if $L_2(\gamma) = 0$. Assume that $L_2(\gamma) \neq 0$ and $g(x)$ is a permutation polynomial of $\mathbf{F}_q$. In the following, we show that $G(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$. Take any two elements $x_1, y_1 \in \mathbf{F}_{q^m}$ such that $G(x_1) = G(y_1)$. That is,

$$L_1(x_1) + L_2(\gamma)h(f(x_1)) = L_1(y_1) + L_2(\gamma)h(f(y_1)), \tag{4.1}$$

which implies that $L_1(x_1 - y_1) = aL_2(\gamma)$, where $a := h(f(y_1)) - h(f(x_1)) \in \mathbf{F}_q$. But the assumption that $L_1(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ implies that there

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

exists a unique element $\alpha \in \mathbf{F}_{q^m}$ such that $L_1(\alpha) = aL_2(\gamma)$. Thus $\alpha = aL_1^{-1}L_2(\gamma)$ and $L_1(\alpha) = L_1(x_1 - y_1)$. It follows immediately that $\alpha = x_1 - y_1$, that is,

$$x_1 = y_1 + aL_1^{-1}L_2(\gamma). \tag{4.2}$$

So (4.1) gives us that

$$L_1(aL_1^{-1}L_2(\gamma)) + L_2(\gamma)h(f(y_1 + aL_1^{-1}L_2(\gamma))) = L_2(\gamma)h(f(y_1)), \tag{4.3}$$

which is equivalent to

$$aL_2(\gamma) + L_2(\gamma)h(f(y_1 + aL_1^{-1}L_2(\gamma))) = L_2(\gamma)h(f(y_1)). \tag{4.4}$$

By the assumption, we have $L_2(\gamma) \neq 0$. So (4.4) is equivalent to

$$a + h(f(y_1 + aL_1^{-1}L_2(\gamma))) = h(f(y_1)). \tag{4.5}$$

Since $L_1^{-1}L_2(\gamma)$ is the b-linear translator of f, we have $f(y_1 + aL_1^{-1}L_2(\gamma)) - f(y_1) = ab$. Hence (4.5) is equivalent to

$$a + h(f(y_1) + ab) = h(f(y_1)). \tag{4.6}$$

Clearly, (4.6) is equivalent to

$$(f(y_1) + ab) + bh(f(y_1) + ab) = f(y_1) + bh(f(y_1)).$$

In other words, (4.6) is equivalent to

$$g(f(y_1) + ab) = g(f(y_1)). \tag{4.7}$$

We claim that $a = 0$. In fact, if $b = 0$ then, by (4.6), $a = 0$, as claimed. If $b \neq 0$, then it follows from the assumption that $g(x)$ is a permutation polynomial of $\mathbf{F}_q$, and from (4.7) that $a = 0$. The claim is proved. Then by the claim and (4.2), we derive immediately that $x_1 = y_1$. This implies that $G(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$. The sufficiency part is proved.

Now let us prove the necessity part. Let $G(x)$ be a permutation polynomial of $\mathbf{F}_{q^m}$. Suppose that $L_2(\gamma) \neq 0$. In what follows we show that $g(x)$ is a permutation polynomial of $\mathbf{F}_q$. If $b = 0$, then $g(x) = x$, which is, of course, a permutation polynomial of $\mathbf{F}_q$. If $b \neq 0$, then we choose any two elements $u_1 \in \mathbf{F}_q$ and $u \in \mathbf{F}_q$ such that

$$g(u_1) = g(u_1 + bu). \tag{4.8}$$

Since f is surjective, there exists an element $v_1 \in \mathbf{F}_{q^m}$ such that $u_1 = f(v_1)$. Then (4.8) is equivalent to

$$g(f(v_1)) = g(f(v_1) + bu). \tag{4.9}$$

Replacing y_1 and a by v_1 and u, respectively, then (4.7) becomes (4.9). Thus the equivalence of (4.3) and (4.7) applied to (4.9) gives us that

$$L_1(v_1) + L_2(\gamma)h(f(v_1)) = L_1(v_1 + uL_1^{-1}L_2(\gamma)) + L_2(\gamma)h(f(v_1 + uL_1^{-1}L_2(\gamma))).$$

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

Namely, $G(v_1) = G(v_1 + uL_1^{-1}L_2(\gamma))$. But $G(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$. So $v_1 = v_1 + uL_1^{-1}L_2(\gamma)$. Since $L_1(x)$ is a permutation polynomial and $L_2(\gamma) \neq 0$, we have $L_1^{-1}L_2(\gamma) \neq 0$. Hence $u = 0$. Thus $g(x)$ is a permutation polynomial of $\mathbf{F}_q$. The necessity part is proved.

This completes the proof of Theorem 4.2. □

Letting $L_2(x) = L_1(x)$, Theorem 4.2 gives the main result of Kyureghyan in [4].

Corollary 4.3 [4]. *Let $L(x) \in \mathbf{F}_{q^m}[x]$ be a linearised permutation polynomial of $\mathbf{F}_{q^m}$. Let $b \in \mathbf{F}_q$, $\gamma \in \mathbf{F}_{q^m}$, $h : \mathbf{F}_q \to \mathbf{F}_q$, $f : \mathbf{F}_{q^m} \to \mathbf{F}_q$ be surjective and γ be a b-linear translator of f. Then $L(x) + L(\gamma)h(f(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $x + bh(x)$ is a permutation polynomial of $\mathbf{F}_q$.*

Acknowledgements

The authors would like to thank the anonymous referee and the editor for their careful reading of the manuscript and helpful comments and corrections.

References

[1] M. Ayad, K. Belghaba and O. Kihel, 'On permutation binomials over finite fields', *Bull. Aust. Math. Soc.* **89** (2014), 112–124.
[2] P. Charpin and G. Kyureghyan, 'When does $F(x) + \gamma Tr(H(x))$ permute F_{p^n}?', *Finite Fields Appl.* **15** (2009), 615–632.
[3] R. Coulter, M. Henderson and R. Matthews, 'A note on constructing permutation polynomials', *Finite Fields Appl.* **15** (2009), 553–557.
[4] G. Kyureghyan, 'Constructuring permutations of finite fields via linear translators', *J. Combin. Theory Ser. A* **118** (2011), 1052–1061.
[5] Y. Laigle-Chapuy, 'Permutation polynomials and applications to coding theory', *Finite Fields Appl.* **13** (2007), 58–70.
[6] R. Lidl and G. L. Mullen, 'When does a polynomial over a finite field permute the elements of the field?', *Amer. Math. Monthly* **95** (1988), 243–246.
[7] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edn, Encyclopedia of Mathematics and its Applications, 20 (Cambridge University Press, Cambridge, 1997).
[8] J. E. Marcos, 'Specific permutation polynomials over finite fields', *Finite Fields Appl.* **17** (2011), 105–112.
[9] A. Masuda and M. E. Zieve, 'Permutation binomials over finite fields', *Trans. Amer. Math. Soc.* **361** (2009), 4169–4180.
[10] J. Schwenk and K. Huber, 'Public key encryption and digital signatures based on permutation polynomials', *Electron. Lett.* **34** (1998), 759–760.
[11] D. Wan and R. Lidl, 'Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure', *Monatsh. Math.* **112** (1991), 149–163.
[12] M. E. Zieve, 'Some families of permutation polynomials over finite fields', *Int. J. Number Theory* **4** (2008), 851–857.
[13] M. E. Zieve, 'On some permutation polynomials over F_q of the form $x^r h(x^{(q-1)/d})$', *Proc. Amer. Math. Soc.* **137** (2009), 2209–2216.
[14] M. E. Zieve, 'Classes of permutation polynomials based on cylotomy and an additive analogue', in: *Additive Number Theory* (Springer, 2010), 355–361.

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press

XIAOER QIN, Mathematical College, Sichuan University,
Chengdu 610064, PR China
and
College of Mathematics and Computer Science, Yangtze Normal University,
Chongqing 408100, PR China
e-mail: qincn328@sina.com

SHAOFANG HONG, Yangtze Center of Mathematics, Sichuan University,
Chengdu 610064, PR China
and
Mathematical College, Sichuan University, Chengdu 610064, PR China
e-mail: sfhong@scu.edu.cn, s-f.hong@tom.com, hongsf02@yahoo.com

https://doi.org/10.1017/S0004972713000646 Published online by Cambridge University Press