Finite Fields and Their Applications 17 (2011) 560–574

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Permutation polynomials over finite fields from a powerful lemma

Pingzhi Yuan [a,1], Cunsheng Ding [b,*]

[a] School of Mathematics, South China Normal University, Guangzhou 510631, PR China
[b] Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Received 15 December 2010
Revised 25 March 2011
Accepted 3 April 2011
Available online 22 April 2011
Communicated by Rudolf Lidl

MSC:
05A05
11T06

Keywords:
Permutation polynomials
Finite fields
Commutative diagrams

ABSTRACT

Using a lemma proved by Akbary, Ghioca, and Wang, we derive several theorems on permutation polynomials over finite fields. These theorems give not only a unified treatment of some earlier constructions of permutation polynomials, but also new specific permutation polynomials over $\mathbb{F}_q$. A number of earlier theorems and constructions of permutation polynomials are generalized. The results presented in this paper demonstrate the power of this lemma when it is employed together with other techniques.

1. Introduction

Let q be a prime power, $\mathbb{F}_q$ be the finite field of order q, and $\mathbb{F}_q[x]$ be the ring of polynomials in a single indeterminate x over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a one-to-one map from $\mathbb{F}_q$ to itself.

Permutation polynomials over finite fields have been an interesting subject of study for many years, and have applications in coding theory [12], cryptography [20,19], combinatorial design theory [10], and other areas of mathematics and engineering. Information about properties, constructions, and applications of permutation polynomials may be found in Lidl and Niederreiter [13,14], and Mullen [17].

[*] Corresponding author. Fax: +852 2358 1477.
E-mail address: cding@ust.hk (C. Ding).

[1] This research was supported by the NSF of China under Grant No. 10971072.

1071-5797/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2011.04.001

The trace function $\mathrm{Tr}(x)$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined by

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

A number of classes of permutation polynomials related to the trace functions were constructed [6,5,4, 11,15,25]. Recently, Akbary, Ghioca and Wang proved a lemma about permutations on finite sets [1,2], which contains two results of Zieve ([23, Lemma 2.1] and [25, Proposition 3]) as special cases [16], and used this lemma to unify some earlier constructions and developed new constructions of permutation polynomials over finite fields. In this paper, we will employ this lemma to derive several theorems about permutation polynomials over finite fields. These theorems give not only a further unified treatment of some of the earlier constructions of permutation polynomials, but also new specific permutation polynomials. The main contributions of this paper are Theorems 3.1, 5.1, 6.1, 6.4, their corollaries and specific permutation polynomials described in the corollaries.

2. Auxiliary results and the powerful lemma

In this section, we present some auxiliary results that will be needed in the sequel. Throughout this paper p is a prime and $q = p^e$ for a positive integer e.

A polynomial of the form

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

is called a *q-polynomial* over $\mathbb{F}_{q^n}$, and is a permutation polynomial on $\mathbb{F}_{q^n}$ if and only if the circulant matrix

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & a_1^q & \cdots & a_{n-2}^q \\ a_{n-2}^{q^2} & a_{n-1}^{q^2} & a_0^{q^2} & \cdots & a_{n-3}^{q^2} \\ \cdots & & & & \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & a_3^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix} \tag{2.1}$$

has nonzero determinant (see [9, p. 362]). In most cases it is not convenient to use this result to find out permutation q-polynomials, as it may be hard to determine if the determinant of this matrix is nonzero [9]. Hence it would be interesting to develop other approaches to the construction of permutation q-polynomials.

We shall use the following trivial fact in the sequel.

Lemma 2.1. *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$ be a q-polynomial and let $\mathrm{Tr}(x)$ be the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Then, for each $\alpha \in \mathbb{F}_{q^n}$, we have*

$$L\big(\mathrm{Tr}(\alpha)\big) = \mathrm{Tr}\big(L(\alpha)\big) = \left(\sum_{i=0}^{n-1} a_i\right)\mathrm{Tr}(\alpha).$$

Definition 2.2. (See [14, p. 115].) The polynomials

$$l(x) = \sum_{i=0}^{m} a_i x^i \quad \text{and} \quad L(x) = \sum_{i=0}^{m} a_i x^{q^i}$$

over $\mathbb{F}_{q^n}$ are called the q-associate of each other. More specifically, $l(x)$ is the *conventional* q-associate of $L(x)$ and $L(x)$ is the linearized q-associate of $l(x)$.

The following lemma is also needed in the sequel.

Lemma 2.3. *(See [14, p. 109].) Let $L_1(x)$ and $L_2(x)$ be two q-polynomials over $\mathbb{F}_q$, and let $l_1(x)$ and $l_2(x)$ be the q-associate polynomials over $\mathbb{F}_q$. Then the common roots of $L_1(x) = 0$ and $L_2(x) = 0$ are all the roots of the linearized q-associate of $\gcd(l_1(x), l_2(x))$. In particular, $x = 0$ is the only common root of $L_1(x) = 0$ and $L_2(x) = 0$ in any finite extension of $\mathbb{F}_q$ if and only if $\gcd(l_1(x), l_2(x)) = 1$.*

The following lemma is taken from Akbary, Ghioca, and Wang [1, Lemma 1.1], and will be employed in the sequel. For completeness and an easy understanding of later applications, we provide its proof here.

Lemma 2.4. *(See [1, Lemma 1.1].) Let A, S and $\bar{S}$ be finite sets with $\sharp S = \sharp\bar{S}$, and let $f : A \to A$, $h : S \to \bar{S}$, $\lambda : A \to S$, and $\bar{\lambda} : A \to \bar{S}$ be maps such that $\bar{\lambda} \circ f = h \circ \lambda$. If both λ and $\bar{\lambda}$ are surjective, then the following statements are equivalent:*

(i) *f is bijective (a permutation of A); and*
(ii) *h is bijective from S to $\bar{S}$ and if f is injective on $\lambda^{-1}(s)$ for each $s \in S$.*

Proof. We have the following commutative diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\lambda"'] & A \arrow[d, "\bar{\lambda}"] \\ S \arrow[r, "h"'] & \bar{S} \end{tikzcd}$$

Assume first that f is bijective. Then f is injective on each $\lambda^{-1}(s)$. Furthermore, because $\bar{\lambda}$ and f are surjective and $\bar{\lambda} \circ f = h \circ \lambda$, then $h : S \to \bar{S}$ is surjective and thus bijective (because S and $\bar{S}$ are finite sets of the same cardinality).

Conversely, assume $f(a_1) = f(a_2)$ for some $a_1, a_2 \in A$. Then $h(\lambda(a_1)) = \bar{\lambda}(f(a_1)) = \bar{\lambda}(f(a_2)) = h(\lambda(a_2))$. As h is a bijection, we obtain $\lambda(a_1) = \lambda(a_2)$. Hence a_1, a_2 are in $\lambda^{-1}(s)$ for some $s \in S$. Since f is injective on each $\lambda^{-1}(s)$, we conclude that $a_1 = a_2$. So f is injective and in fact bijective (because A is a finite set). □

3. The first theorem about permutation polynomials

Our objective in this section is to present a general result on permutation polynomials which contains some earlier results as special cases. This gives a uniform treatment of some earlier constructions of permutation polynomials and also new permutation polynomials. The following theorem is derived from Lemma 2.4, and is a generalization of Theorems 1.5 and 6.1 in [1].

Theorem 3.1. *Let q be a prime power, and let $r \geqslant 1$ and $n \geqslant 1$ be positive integers. Let $B(x), L_1(x), \dots, L_r(x) \in \mathbb{F}_q[x]$ be q-polynomials, $g(x) \in \mathbb{F}_{q^n}[x]$, $h_1(x), \dots, h_r(x) \in \mathbb{F}_q[x]$ and $\delta_1, \dots, \delta_r \in \mathbb{F}_{q^n}$ such that $B(\delta_i) \in \mathbb{F}_q$ and $h_i(B(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$. Then*

$$f(x) = g\bigl(B(x)\bigr) + \sum_{i=1}^{r} \bigl(L_i(x) + \delta_i\bigr) h_i\bigl(B(x)\bigr)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if

(1) *$B(g(x)) + \sum_{i=1}^{r}(L_i(x) + B(\delta_i))h_i(x)$ permutes $B(\mathbb{F}_{q^n})$; and*
(2) *for any $y \in B(\mathbb{F}_{q^n})$, $\sum_{i=1}^{r} L_i(x)h_i(y)$ permutes $\ker(B)$.*

Moreover, (2) is equivalent to $\gcd(\sum_{i=1}^{r} l_i(x)h_i(y), b(x)) = 1$ for any $y \in \mathbb{F}_q$, where $l_i(x)$ and $b(x)$ are the conventional q-associate of $L_i(x)$ and $B(x)$.

Proof. Note that $B(x)$ is a q-polynomial over $\mathbb{F}_q$. We have $aB(x) = B(ax)$ for all $a \in \mathbb{F}_q$ and all $x \in \mathbb{F}_{q^n}$, and $B(x+y) = B(x) + B(y)$ for all x and y in $\mathbb{F}_{q^n}$. Hence $B(\mathbb{F}_{q^n})$ is a linear subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Since $B(x)$ and $L_i(x)$ are q-polynomials over $\mathbb{F}_q$, we have $L_i(B(x)) = B(L_i(x))$. By assumption, $B(\delta_i) \in \mathbb{F}_q$ for all i. It follows that the following polynomial

$$h(x) := (B \circ g)(x) + \sum_{i=1}^{r}\bigl(L_i(x) + B(\delta_i)\bigr)h_i(x)$$

induces a mapping from $B(\mathbb{F}_{q^n})$ to itself.

Since $h_i(B(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$ and $B, L_1, L_2, \ldots, L_r$ are $\mathbb{F}_q$-linear over $\mathbb{F}_q$, we have $B \circ f = h \circ B$. Hence we have the following diagram

$$\begin{tikzcd}
\mathbb{F}_{q^n} \arrow[r, "f"] \arrow[d, "B"'] & \mathbb{F}_{q^n} \arrow[d, "B"] \\
B(\mathbb{F}_{q^n}) \arrow[r, "h"'] & B(\mathbb{F}_{q^n})
\end{tikzcd}$$

We would now apply Lemma 2.4 with $A = \mathbb{F}_{q^n}$, $f = g \circ B + \sum_{i=1}^{r}(L_i + \delta_i)h_i \circ B$, $S = \bar{S} = B(\mathbb{F}_{q^n})$, $\lambda = \bar{\lambda} = B$ and h as defined above. By Lemma 2.4, $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $h(x)$ induces a permutation of $B(\mathbb{F}_{q^n})$ and $f(x)$ is injective on each $B^{-1}(y) \in \mathbb{F}_{q^n}$ for all $y \in B(\mathbb{F}_{q^n})$.

For any given $y \in B(\mathbb{F}_{q^n})$ and $\alpha, \beta \in B^{-1}(y)$, we have $\beta = \alpha + x$ for some $x \in \ker B$. Since

$$f(\beta) = f(\alpha + x) = g\bigl(B(\alpha)\bigr) + \sum_{i=1}^{r}\bigl(L_i(\alpha + x) + \delta_i\bigr)h_i\bigl(B(\alpha)\bigr) = f(\alpha) + \sum_{i=1}^{r} L_i(x)h_i(y),$$

$f(x)$ is injective on each $B^{-1}(y) \in \mathbb{F}_{q^n}$ for all $y \in B(\mathbb{F}_{q^n})$ if and only if

$$\ker B \cap \ker\left(\sum_{i=1}^{r} L_i h_i(y)\right) = \{0\}$$

for all $y \in B(\mathbb{F}_{q^n})$.

The last conclusion of this theorem then follows from Lemma 2.3. □

In what follows in this section, we show that some earlier results on permutation polynomials are special cases of Theorem 3.1 and present new results on permutation polynomials.

Corollary 3.2. *(See [1, Theorem 6.1].) Let q be a prime power, and let $L_1, L_2, L_3 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be q-polynomials over $\mathbb{F}_q$. Let $w(x) \in \mathbb{F}_{q^n}[x]$ such that $w(L_3(\mathbb{F}_{q^n})) \in \mathbb{F}_q$. Then*

$$f(x) = L_1(x) + L_2(x)w\bigl(L_3(x)\bigr)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the following two conditions hold:

(i) $\ker(F_y) \cap \ker(L_3) = \{0\}$, *for any* $y \in L_3(\mathbb{F}_{q^n})$, *where*

$$F_y(x) := L_1(x) + L_2(x)w(y).$$

(ii) $h(x) := L_1(x) + L_2(x)w(x)$ *permutes* $L_3(\mathbb{F}_{q^n})$.

Proof. The conclusion of this corollary follows from Theorem 3.1 by setting $r = 2$, $g = 0$, $h_1 = 1$, $h_2 = w$, $\delta_1 = \delta_2 = 0$, $B = L_3$. □

The following is a consequence of Theorem 3.1.

Corollary 3.3. *Let* $r \geqslant 1$ *and* $n \geqslant 1$ *be positive integers. Let* $L_1(x), \ldots, L_r(x) \in \mathbb{F}_q[x]$ *be* q*-polynomials,* $g(x) \in \mathbb{F}_{q^n}[x]$*,* $h_1(x), \ldots, h_r(x) \in \mathbb{F}_q[x]$ *and* $\delta_1, \ldots, \delta_r \in \mathbb{F}_{q^n}$*. Then*

$$F(x) = g\bigl(\mathrm{Tr}(x)\bigr) + \sum_{i=1}^{r}\bigl(L_i(x) + \delta_i\bigr)h_i\bigl(\mathrm{Tr}(x)\bigr)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ *if and only if*

(1) $\mathrm{Tr}(g(x)) + \sum_{i=1}^{r}(L_i(x) + \mathrm{Tr}(\delta_i))h_i(x)$ *permutes* $\mathbb{F}_q$; *and*
(2) *for any* $y \in \mathbb{F}_q$, $\sum_{i=1}^{r} L_i(x)h_i(y)$ *permutes* $\ker(\mathrm{Tr})$.

Moreover, (2) *is equivalent to* $\gcd(\sum_{i=1}^{r} l_i(x)h_i(y), \sum_{i=0}^{n-1} x^i) = 1$ *for any* $y \in \mathbb{F}_q$*, where* $l_i(x)$ *is the conventional* q*-associate of* $L_i(x)$.

Proof. Put $B(x) = \mathrm{Tr}(x)$ in Theorem 3.1. We have then $B(\mathbb{F}_{q^n}) = \mathrm{Tr}(\mathbb{F}_{q^n}) = \mathbb{F}_q$. Hence $B(\delta_i) \in \mathbb{F}_q$. The conclusion of this corollary follows from Theorem 3.1. □

The following is a consequence of Corollary 3.3 and Lemma 2.3.

Corollary 3.4. *Let* $r \geqslant 1$ *and* $n \geqslant 1$ *be positive integers. Let* $L_i(x) = \sum_{j=1}^{n-1} a_j^{(i)} x^{q^j}$, $i = 1, \ldots, r$, *be* q*-polynomials over* $\mathbb{F}_q$*,* $g(x) \in \mathbb{F}_{q^n}[x]$*,* $h_1(x), \ldots, h_r(x) \in \mathbb{F}_q[x]$ *and* $\delta_1, \ldots, \delta_r \in \mathbb{F}_{q^n}$*. Then*

$$F(x) = g\bigl(\mathrm{Tr}(x)\bigr) + \sum_{i=1}^{r}\bigl(L_i(x) + \delta_i\bigr)h_i\bigl(\mathrm{Tr}(x)\bigr)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ *if and only if the following two conditions hold*:

(1) $\mathrm{Tr}(g(x)) + \sum_{i=1}^{r}(\sum_{j=1}^{n-1} a_j^{(i)} x + \mathrm{Tr}(\delta_i))h_i(x)$ *is a permutation polynomial of* $\mathbb{F}_q$.
(2) *For any* $y \in \mathbb{F}_q$*, the only common solution of the two equations* $\sum_{i=1}^{r} L_i(x)h_i(y) = 0$ *and* $\mathrm{Tr}(x) = 0$ *in* $\mathbb{F}_{q^n}$ *is* $x = 0$.

Moreover, (2) *is equivalent to* $\gcd(\sum_{i=1}^{r} l_i(x)h_i(y), \sum_{i=0}^{n-1} x^i) = 1$ *for any* $y \in \mathbb{F}_q$*, where* $l_i(x)$ *is the conventional* q*-associate of* $L_i(x)$.

Proof. By Lemma 2.3, $\gcd(\sum_{i=1}^{r} l_i(x)h_i(y), \sum_{i=0}^{n-1} x^i) = 1$ for any $y \in \mathbb{F}_q$ if and only if condition (2) is satisfied. The desired conclusion then follows from Corollary 3.3. □

Corollary 3.5. *Let $L(x)=\sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$ be a q-polynomial, and let $\alpha \in \mathbb{F}_{q^n}$. Then*

$$L_\alpha(x)=\alpha\,\mathrm{Tr}(x)+L(x)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $\sum_{i=0}^{n-1} a_i+\mathrm{Tr}(\alpha)\neq 0$ and $\gcd(l(x),\sum_{i=0}^{n-1} x^i)=1$, where $l_i(x)$ is the conventional q-associate of $L_i(x)$.

Proof. In Corollary 3.4, put $g(x)=\alpha x$, $r=1$, $L_1(x)=L(x)$, $\delta_1=0$, and $h_1(x)=1$. We have then

$$g\big(\mathrm{Tr}(x)\big)+\sum_{i=1}^{r}\big(L_i(x)+\delta_i\big)h_i\big(\mathrm{Tr}(x)\big)=\alpha\,\mathrm{Tr}(x)+L(x)=L_\alpha(x).$$

On the other hand, we have

$$J(x):=\mathrm{Tr}\big(g(x)\big)+\sum_{i=1}^{r}\big(L_i(x)+\mathrm{Tr}(\delta_i)\big)h_i(x)=\mathrm{Tr}(\alpha x)+L(x).$$

Clearly, $J(x)$ maps $\mathbb{F}_q$ to $\mathbb{F}_q$. Restricting $J(x)$ on $\mathbb{F}_q$, we have

$$J(x):=\mathrm{Tr}(\alpha x)+L(x)=\mathrm{Tr}(\alpha)x+\left(\sum_{i=0}^{n-1}a_i\right)x.$$

The desired conclusion then follows from Corollary 3.4. □

The following follows from Corollary 3.5 directly.

Corollary 3.6. *Let $L(x)=\sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$ be a q-polynomial over $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}(\alpha)=0$. Then*

$$L_\alpha(x)=\alpha\,\mathrm{Tr}(x)+L(x)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $\gcd(l(x),x^n-1)=1$. In particular, $L(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $\gcd(l(x),x^n-1)=1$, where $l(x)$ is the conventional q-associate of $L(x)$.

In Theorem 3.1, putting $L_1(x)=L_2(x)=\cdots=L_r(x)=L(x)$, we obtain the following.

Corollary 3.7. *Let q be a prime power, and let $r\geqslant 1$ and $n\geqslant 1$ be positive integers. Let $B(x),L(x)\in\mathbb{F}_q[x]$ be q-polynomials, $g(x)\in\mathbb{F}_{q^n}[x]$, $h_1(x),\dots,h_r(x)\in\mathbb{F}_q[x]$ and $\delta_1,\dots,\delta_r\in\mathbb{F}_{q^n}$ such that $B(\delta_i)\in\mathbb{F}_q$ and $h_i(B(\mathbb{F}_{q^n}))\in\mathbb{F}_q$. Then*

$$f(x)=g\big(B(x)\big)+\sum_{i=1}^{r}\big(L(x)+\delta_i\big)h_i\big(B(x)\big)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if

(1) *$B(g(x))+\sum_{i=1}^{r}(L(x)+B(\delta_i))h_i(x)$ permutes $B(\mathbb{F}_{q^n})$; and*
(2) *$\gcd((\sum_{i=1}^{r}h_i(y))l(x),b(x))=1$ for any $y\in B(\mathbb{F}_{q^n})$, where $l_i(x)$ and $b(x)$ are the conventional q-associate of $L_i(x)$ and $B(x)$.*

The following result in [1] is a special case of Corollary 3.7.

Corollary 3.8. *(See [1, Theorem 5.5].) Let q be a prime power, $a \in \mathbb{F}_q$, and let $b \in \mathbb{F}_{q^n}$. Let $P(x)$ be a q-polynomial over $\mathbb{F}_q$ which permutes $\mathbb{F}_{q^n}$, and $L(x)$ be a q-linear polynomial over $\mathbb{F}_q$. Let $g(x) \in \mathbb{F}_{q^n}[x]$ such that $g(L(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$. Then*

$$f(x) = aP(x) + \big(P(x) + b\big)g\big(L(x)\big)$$

is a permutation polynomial over $\mathbb{F}_{q^n}$ if and only if

(i) $-a \notin g(L(\mathbb{F}_{q^n}))$; *and*
(ii) $h(x) = aP(x) + (P(x) + L(b))g(x)$ *permutes* $L(\mathbb{F}_{q^n})$.

4. Specific permutation polynomials from the first theorem

In this section, we present a few classes of specific permutation polynomials that are consequences of Theorem 3.1. The following corollary is a generalization of Theorem 5 in [6].

Corollary 4.1. *Assume that* $\gcd(n, k) = 1$, $\gcd(n, q) = 1$ *and $\delta \in \mathbb{F}_{q^n}$ is an element with* $\mathrm{Tr}(\delta) = 0$. *Then the polynomial*

$$F(X) = ax^{q^k} + (x + \delta)\big(\mathrm{Tr}(x)\big)^{q^k-1}$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ for all $a \in \mathbb{F}_q \setminus \{0, -1\}$.

Proof. We apply Corollary 3.4 with $g(x) = 0$, $r = 2$, $L_1(x) = ax^{q^k}$, $L_2(x) = x$, $\delta_1 = 0$, $\delta_2 = \delta$, $h_1(x) = 1$, and $h_2(x) = x^{q^k-1}$. Then

$$F(x) := g\big(\mathrm{Tr}(x)\big) + \sum_{i=1}^{r} \big(L_i(x) + \delta_i\big)h_i\big(\mathrm{Tr}(x)\big) = ax^{q^k} + (x + \delta)\big(\mathrm{Tr}(x)\big)^{q^k-1}.$$

Note that

$$J(x) := \mathrm{Tr}\big(g(x)\big) + \sum_{i=1}^{r} \big(L_i(x) + \mathrm{Tr}(\delta_i)\big)h_i(x) = ax^{q^k} + x\big(\mathrm{Tr}(x)\big)^{q^k-1}.$$

Restricting $J(x)$ on $\mathbb{F}_q$, we have

$$J(x) := (a + 1)x$$

because $\gcd(n, q) = 1$. Hence $J(x)$ permutes $\mathbb{F}_q$.

On the other hand, we have

$$\sum_{i=1}^{r} L_i(x)h_i(y) = ax^{q^k} + xy^{q^k-1}.$$

If there is an element $y \in \mathbb{F}_q$ and an element $x \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}(x) = 0$ and

$$ax^{q^k} + xy^{q^k-1} = 0$$

which implies $x = 0$ or $x = by$ for some $0 \neq b \in \mathbb{F}_q$ due to $\gcd(k, n) = 1$. If the latter equality holds, we have $\mathrm{Tr}(x) = nby = 0$, and thus $y = 0$ and $x = 0$.

Therefore the conditions of Corollary 3.4 are satisfied and the desired conclusion follows from Corollary 3.4. □

Corollary 4.2. *Let n be a prime and let $q = 2$. Define for each i with $0 \leqslant i < n$*

$$a_i = \begin{cases} 1 & \textit{if } i \textit{ is a quadratic residue modulo } n, \\ 0 & \textit{otherwise.} \end{cases}$$

Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$ and

$$L_\alpha(x) = \alpha\,\mathrm{Tr}(x) + L(x),$$

where $\alpha \in \mathbb{F}_{q^n}$. Then $L_\alpha(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if $n \equiv 3 \pmod 8$ and $\mathrm{Tr}(\alpha) = 0$ or $n \equiv 5 \pmod 8$ and $\mathrm{Tr}(\alpha) = 1$.

Proof. By definition, $\mathrm{Tr}(\alpha) + \sum_{i=0}^{n-1} a_i = 1$ in both cases. Let $l(x)$ be the conventional q-associate of $L(x)$. It was proved in [8] that $\gcd(x^n - 1, l(x)) = 1$ if $n \equiv 3 \pmod 8$ and $\gcd(x^n - 1, l(x)) = x - 1$ if $n \equiv 5 \pmod 8$. The desired conclusions then follow from Corollary 3.5. □

Corollary 4.3. *Let $n = n_1 n_2$, where n_1 and n_2 are two distinct primes such that $\gcd(n_1 - 1, n_2 - 1) = 2$, and let $q = 2$. Define for each i with $0 \leqslant i < n$*

$$a_i = \begin{cases} 0, & i \in \{0, n_2, 2n_2, \ldots, (n_1 - 1)n_2\}, \\ 1, & i \in \{n_1, 2n_1, \ldots, (n_2 - 1)n_1\}, \\ (1 - (\frac{i}{n_1})(\frac{i}{n_2}))/2, & \textit{otherwise}, \end{cases} \tag{4.1}$$

where $(\frac{a}{n_1})$ denotes the Legendre symbol. Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$ and

$$L_\alpha(x) = \alpha\,\mathrm{Tr}(x) + L(x),$$

where $\alpha \in \mathbb{F}_{q^n}$ with $\mathrm{Tr}(\alpha) = 1$. Then $L_\alpha(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if $n_1 \equiv 1 \pmod 8$ and $n_2 \equiv 3 \pmod 8$ or $n_1 \equiv 5 \pmod 8$ and $n_2 \equiv 7 \pmod 8$.

Proof. By definition, $\mathrm{Tr}(\alpha) + \sum_{i=0}^{n-1} a_i = 1$ in both cases. Let $l(x)$ be the conventional q-associate of $L(x)$. It was proved in [7] that $\gcd(x^n - 1, l(x)) = x - 1$ in both cases. The desired conclusions then follow from Corollary 3.5. □

5. The second theorem and its applications

The following theorem is another application of Lemma 2.4, and is a multiplication version of Theorem 1.4 in [1].

Theorem 5.1. *Assume that A is a finite field and S is a subset of A such that the map $\lambda : A \to S$ is surjective. Let $g : A \to A$, $h : S \to S$, and $f : A \to A$ be maps such that the following diagram commutes:*

$$\begin{tikzcd}
A \arrow[r, "f(x)g(\lambda(x))"] \arrow[d, "\lambda"'] & A \arrow[d, "\lambda"] \\
S \arrow[r, "h"'] & S
\end{tikzcd}$$

Then the map $p(x) = f(x)g(\lambda(x))$ permutes A if and only if the following conditions hold.

(i) *h is a bijection from $\lambda(A)$ to $\lambda(A)$.*
(ii) *$g(y) \neq 0$ for every $y \in \lambda(A)$ with $\sharp\lambda^{-1}(y) > 1$.*
(iii) *$f(x)$ is injective on each $\lambda^{-1}(y)$ for all $y \in \lambda(A)$.*

Proof. By Lemma 2.4 and the assumptions of this theorem, $f(x)g(\lambda(x))$ permutes A if and only if h is a bijection from $\lambda(A)$ to $\lambda(A)$ and $f(x)g(\lambda(x))$ is injective on each $\lambda^{-1}(y)$ for all $y \in \lambda(A)$.

For given $y \in \lambda(A)$ and $\alpha, \beta \in \lambda^{-1}(y)$, we have $\lambda(\alpha) = \lambda(\beta) = y$. Define $p(x) = f(x)g(\lambda(x))$. If $p(\alpha) = p(\beta)$, then

$$p(\alpha) = f(\alpha)g(y) = f(\beta)g(y) = p(\beta).$$

Therefore $p(x)$ is injective on each $\lambda^{-1}(y)$ for all $y \in \lambda(A)$ if and only if $g(y) \neq 0$ for every $y \in \lambda(A)$ with $\sharp\lambda^{-1}(y) > 1$ and $f(x)$ is injective on each $\lambda^{-1}(y)$ for all $y \in \lambda(A)$. □

The following is a consequence of Theorem 5.1 and Corollary 11 in [15]. It can be also derived from Theorem 6.3 in [1]. This demonstrates that Theorem 5.1 is a generalization of Corollary 11 in [15].

Corollary 5.2. *If $h(x) \in \mathbb{F}_q[x]$, $h(0) \neq 0$, then the polynomial $p(x) = xh(\mathrm{Tr}(x))$ permutes $\mathbb{F}_{q^n}$ if and only if $u(x) = xh(x)$ permutes $\mathbb{F}_q$.*

Proof. Define $A = \mathbb{F}_{q^n}$ and

$$\lambda(x) = \mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}}.$$

Since the following diagram

$$\begin{tikzcd}
\mathbb{F}_{q^n} \arrow[r, "xh(\mathrm{Tr}(x))"] \arrow[d, "\mathrm{Tr}"'] & \mathbb{F}_{q^n} \arrow[d, "\mathrm{Tr}"] \\
\mathbb{F}_q \arrow[r, "xh(x)"'] & \mathbb{F}_q
\end{tikzcd}$$

commutes, the desired conclusion follows from Theorem 5.1. □

Corollary 5.2 is related to [3,18,21,24]. Note that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{F}_q \arrow[r, "x^r g(x^s)"] \arrow[d, "x^s"'] & \mathbb{F}_q \arrow[d, "x^s"] \\
x^s(\mathbb{F}_q) \arrow[r, "x^r g(x)^s"'] & x^s(\mathbb{F}_q)
\end{tikzcd}$$

Note also that $\alpha^r = \beta^r, \alpha^s = \beta^s$ implies $\alpha = \beta$ if and only if $\gcd(r, s, q-1) = 1$. The following follows from Corollary 5.2.

Corollary 5.3. *(See [1, Proposition 3.1].) Let r and s be positive integers. Then $x^r g(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(r, s, q-1) = 1$ and $x^r g(x)^s$ permutes $(\mathbb{F}_q^*)^s$.*

Combining Corollaries 5.2 and 5.3, we have the following corollary, which is an improvement of Proposition 2.12 in [22].

Corollary 5.4. *Assume $q \equiv 1 \pmod d$. If $h(x) \in \mathbb{F}_q[x]$, $h(0) \neq 0$, then the polynomial $p(x) = xh(\mathrm{Tr}(x)^{(q-1)/d})$ permutes $\mathbb{F}_{q^n}$ if and only if $xh(x)^{(q-1)/d}$ permutes μ_d, which is the set of all dth roots of unity in $\mathbb{F}_q$.*

The permutation polynomials in Corollary 5.4 are related to permutation polynomials from cyclotomy [23,25].

For any integer $d \geqslant 2$, define

$$h_d(x) = x^{d-1} + x^{d-2} + \cdots + x + 1 \in \mathbb{F}_q[x].$$

Corollary 5.5. *Let $2 \leqslant d < q-1$ such that $d \mid (q-1)$, $u \geqslant 1$, $r \geqslant 1$ and $0 \leqslant k_i \leqslant d-1$, $s_i \in \mathbb{Z}$, $i = 1, \ldots, r$. Let $b_i \in \mathbb{F}_q$, $i = 1, \ldots, r$, and polynomials $g_i(x) \in \mathbb{F}_q[x]$, $i = 1, \ldots, r$, be divisible by $h_d(x)$. The polynomial*

$$g(x) = x^u \prod_{i=1}^{r} \bigl(g_i\bigl(x^{(q-1)/d}\bigr) + b_i x^{k_i(q-1)/d}\bigr)^{s_i} \in \mathbb{F}_q[x]$$

is a permutation polynomial if and only if the following four conditions hold:

(1) $b_1 \cdots b_r \neq 0$ *in* $\mathbb{F}_q$.
(2) $\gcd(u, (q-1)/d) = 1$.
(3) $\gcd(u + (\sum_{i=1}^{r} k_i s_i)(q-1)/d, d) = 1$.
(4) $\prod_{i=1}^{r} (g_i(1)/b_i + 1)^{s_i}$ *is a dth power in* $\mathbb{F}_q^\star$.

Proof. By convention, we use μ_d to denote the set of all dth roots of unity in $\mathbb{F}_q$. It is easy to check that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{F}_q \arrow[r, "g(x)"] \arrow[d, "x^s"'] & A \arrow[d, "x^s"] \\
(\mathbb{F}_q)^s \arrow[r, "h"'] & (\mathbb{F}_q)^s
\end{tikzcd}$$

where $s = (q-1)/d$ and

$$h(x) = x^u \prod_{i=1}^{r} \bigl(g_i(x) + b_i x^{k_i}\bigr)^{s_i(q-1)/d}.$$

Since $h(1) = \prod_{i=1}^{r} (g_i(1) + b_i)^{s_i(q-1)/d}$ and

$$h(x) = x^u \prod_{i=1}^{r} \bigl(b_i x^{k_i}\bigr)^{s_i(q-1)/d} = \prod_{i=1}^{r} (b_i)^{s_i(q-1)/d} x^{u+(\sum_{i=1}^{r} k_i s_i)(q-1)/d} \tag{5.1}$$

for any $x \in \mu_d \setminus \{1\}$, we have condition (1).

It follows from Corollary 5.3 that $\gcd(u, (q-1)/d, q-1) = 1$, i.e., $\gcd(u, (q-1)/d) = 1$. So we get condition (2). By (5.1), $h(x)$ permutes $x^s(\mathbb{F}_q)$ if and only if

$$\gcd\left(u + \left(\sum_{i=1}^{r} k_i s_i\right)(q-1)/d, d\right) = 1$$

and $\prod_{i=1}^{r} (g_i(1)/b_i + 1)^{s_i}$ is a dth power in $\mathbb{F}_q$. These are conditions (3) and (4). We are done. □

Corollary 5.5 above is a generalization of Theorem 1 in [25] and Theorem 2 in [15].

6. Two more theorems on permutation polynomials

The following theorem is another application of Lemma 2.4, and is a variant of Theorem 1.4(c) and Theorem 5.1(c) in [1].

Theorem 6.1. *Assume that A is a finite field and $S, \bar{S}$ are finite subsets of A with $\sharp(S) = \sharp(\bar{S})$ such that the maps $\psi : A \to S$ and $\bar{\psi} : A \to \bar{S}$ are surjective and $\bar{\psi}$ is additive, i.e.,*

$$\bar{\psi}(x + y) = \bar{\psi}(x) + \bar{\psi}(y), \quad x, y \in A.$$

Let $g : S \to A$, and $f : A \to A$ be maps such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "f+g\circ\psi"] \arrow[d, "\psi"'] & A \arrow[d, "\bar{\psi}"] \\ S \arrow[r, "f"'] & \bar{S} \end{tikzcd}$$

and $\bar{\psi}(g(\psi(x))) = 0$ for every $x \in A$. Then the map $p(x) = f(x) + g(\psi(x))$ permutes A if and only if f permutes A.

Proof. It follows from Lemma 2.4 and the assumptions of this theorem that $f(x) + g(\psi(x))$ permutes A if and only if f is a bijection from S to $\bar{S}$ and $f(x) + g(\psi(x))$ is injective on each $\psi^{-1}(s)$ for all $s \in S$.

On the other hand, by assumption we have $\bar{\psi}(g(\psi(x))) = 0$ for every $x \in A$. Hence,

$$\bar{\psi}\bigl(f(x) + g\bigl(\psi(x)\bigr)\bigr) = \bar{\psi}\bigl(f(x)\bigr) + \bar{\psi}\bigl(g\bigl(\psi(x)\bigr)\bigr) = \bar{\psi}\bigl(f(x)\bigr)$$

for all $x \in A$. Therefore, the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\psi"'] & A \arrow[d, "\bar{\psi}"] \\ S \arrow[r, "f"'] & \bar{S} \end{tikzcd}$$

Applying Lemma 2.4 to this commutative diagram, we know that $f(x)$ permutes A if and only if f is a bijection from S to $\bar{S}$ and $f(x)$ is injective on each $\psi^{-1}(s)$ for all $s \in S$.

Let $a_1 \in \psi^{-1}(s)$ and $a_2 \in \psi^{-1}(s)$, where $s \in S$. Note that $\psi(a_1) = \psi(a_2) = s$. We have then

$$f(a_1) + g\bigl(\psi(a_1)\bigr) = f(a_1) + g(s)$$

and

$$f(a_2) + g\bigl(\psi(a_2)\bigr) = f(a_2) + g(s).$$

It follows that $f(x) + g(\psi(x))$ is injective on each $\psi^{-1}(s)$ for all $s \in S$ if and only if $f(x)$ is injective on each $\psi^{-1}(s)$ for all $s \in S$.

Summarizing the discussions above proves the desired conclusion. □

We will employ Theorem 6.1 to prove the following corollary.

Corollary 6.2. *Let n and k be positive integers such that $\gcd(n,k) = d > 1$, let s be any positive integer with $s(q^k - 1) \equiv 0 \pmod{q^n - 1}$. Let*

$$L_1(x) = a_0 x + a_1 x^{q^d} + a_1 x^{q^{2d}} + \cdots + a_{n/d-1} x^{q^{n-d}}, \quad a_i \in \mathbb{F}_q,$$

be a q^d-polynomial with $L_1(1) = 0$ and let $L_2(x) \in \mathbb{F}_q[x]$ be a linearized polynomial and $g(x) \in \mathbb{F}_{q^n}[x]$. Then

$$f(x) = \bigl(g\bigl(L_1(x)\bigr)\bigr)^s + L_2(x)$$

permutes $\mathbb{F}_{q^n}$ if and only if $L_2(x)$ permutes $\mathbb{F}_{q^n}$.

Proof. Since $\gcd(k,n) = d$, so $\gcd(q^k - 1, q^n - 1) = q^d - 1$, and thus $s(q^k - 1) \equiv 0 \pmod{q^n - 1}$ if and only if $s(q^d - 1) \equiv 0 \pmod{q^n - 1}$. Therefore

$$sq^{dr} \equiv sq^{d(r-1)} \equiv \cdots \equiv s \pmod{q^n - 1}.$$

It follows that for any $x \in \mathbb{F}_{q^n}$, $(g(L_1(x)))^{sq^{rd}} = (g(L_1(x)))^s$ for any positive integer r. Hence $L_1((g(L_1(x)))^s) = L_1(1)(g(L_1(x)))^s = 0$ for every $x \in \mathbb{F}_{q^n}$. Now applying Theorem 6.1 with $\psi = \bar{\psi} = L_1(x)$ and $f = L_2(x)$, we obtain the desired conclusion. □

Note that Corollary 6.2 can also be derived from Theorem 2 and Theorem 1 in [11].

In Corollary 6.2 putting $L_1(x) = x^{q^k} - x$, $g(x) = x + \delta$, $\delta \in \mathbb{F}_{q^n}$ and $L_2(x) = x$, we obtain the following corollary, which is a slight generalization of Proposition 2 and Remark 1 in [22] as in the following corollary q could be any prime power.

Corollary 6.3. *Let n and k be positive integers such that $\gcd(n,k) = d > 1$, and let s be any positive integer with $s(q^k - 1) \equiv 0 \pmod{q^n - 1}$. Then*

$$h(x) = \bigl(x^{q^k} - x + \delta\bigr)^s + x$$

permutes $\mathbb{F}_{q^n}$ for any $\delta \in \mathbb{F}_{q^n}$.

Theorem 6.4. *Let $q = p^e$ for some positive integer e.*

(a) *If $k \geqslant 2$ is an even integer or k is odd and q is even, then $f_{a,b,k}(x) := ax^q + bx + (x^q - x)^k$, $a, b \in \mathbb{F}_{q^2}$ with $a + b \in \mathbb{F}_q^*$, permutes $\mathbb{F}_{q^2}$ if and only if $b \neq a^q$.*

(b) *If k and q are odd positive integers, then $f_{a,k}(x) := ax^q + a^q x + (x^q - x)^k$, $a \in \mathbb{F}_{q^2}^*$ and $a + a^q \neq 0$, permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(k, q-1) = 1$.*

Proof. Note that

$$\left(f_{a,b,k}(x)\right)^q - f_{a,b,k}(x) = \left(\left(b - a^q\right)x\right)^q - \left(b - a^q\right)x + \left(x - x^q\right)^k - \left(x^q - x\right)^k.$$

(a) Since k is even or k is odd and q is even, we have

$$\left(f_{a,b,k}(x)\right)^q - f_{a,b,k}(x) = \left(\left(b - a^q\right)x\right)^q - \left(b - a^q\right)x.$$

On the other hand, since $a + b, a + a^q \in \mathbb{F}_q$, then $b - a^q \in \mathbb{F}_q$, and so

$$\left(b - a^q\right)\left(x^q - x\right) = \left(\left(b - a^q\right)x\right)^q - \left(b - a^q\right)x.$$

Hence in case (a) we have the following commutative diagram

$$\begin{tikzcd}
\mathbb{F}_{q^2} \arrow[r, "f_{a,b,k}(x)"] \arrow[d, "x^q-x"'] & \mathbb{F}_{q^2} \arrow[d, "x^q-x"] \\
S \arrow[r, "(b-a^q)x"'] & \bar{S}
\end{tikzcd}$$

where $S = \{\alpha^q - \alpha,\ \alpha \in \mathbb{F}_{q^2}\}$ and $\bar{S} = \{(b - a^q)s\colon\ s \in S\}$. Note that $s \in S$ if and only if $\operatorname{Tr}(s) = 0$. It is obvious that $(b - a^q)x$ is a bijection from S to $\bar{S}$ if and only if $b^q - a \neq 0$.

For any $x, y \in \mathbb{F}_{q^2}$ with

$$x^q - x = y^q - y \quad \text{and} \quad ax^q + bx = ay^q + by,$$

we have

$$(x - y)^q = x - y, \qquad a(x - y)^q = -b(x - y).$$

Therefore by Lemma 2.4, $f_{a,b,k}(x) := ax^q + bx + (x^q - x)^k$, $a, b \in \mathbb{F}_{q^2}$ with $a + b \in \mathbb{F}_q^*$, permutes $\mathbb{F}_{q^2}$ if and only if $b \neq a^q$.

(b) Since k is odd, we have the following commutative diagram

$$\begin{tikzcd}
\mathbb{F}_{q^2} \arrow[r, "f_{a,b,k}(x)"] \arrow[d, "x^q-x"'] & \mathbb{F}_{q^2} \arrow[d, "x^q-x"] \\
S \arrow[r, "-2x^k"'] & \bar{S}
\end{tikzcd}$$

where $S = \{\alpha^q - \alpha,\ \alpha \in \mathbb{F}_{q^2}\}$ and $\bar{S} = \{-2s^k\colon\ s \in S\}$.

For any $x, y \in \mathbb{F}_{q^2}$, $a \in \mathbb{F}_{q^2}$ with $a + a^q \neq 0$,

$$x^q - x = y^q - y \quad \text{and} \quad ax^q + a^q x = ay^q + a^q y$$

hold only when $x = y$. Therefore by Lemma 2.4, $f_{a,k}(x) := ax^q + a^q x + (x^q - x)^k$, $a \in \mathbb{F}_{q^2}$ with $a + a^q \neq 0$, permutes $\mathbb{F}_{q^2}$ if and only if $-2x^k$ is a bijection from S to $\bar{S}$.

Let $\epsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\epsilon^{q-1} = -1$ (since q is odd). Then each $\alpha \in \mathbb{F}_{q^2}$ is uniquely written as $u + v\epsilon$ for some $u, v \in \mathbb{F}_q$. We compute then easily that $\alpha^q - \alpha = -2v\epsilon$. Since k is odd, so $(-2v\epsilon)^k = (-2d\epsilon)^k$ implies $v = d$ if and only if $\gcd(k, q-1) = 1$. Therefore $f_{a,k}(x) := ax^q + a^q x + (x^q - x)^k$, $a \in \mathbb{F}^*_{q^2}$ with $a + a^q \neq 0$, permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(k, q-1) = 1$. This completes the proof. □

Theorem 6.4 above is a generalization of Theorem 5.12 in [1] in the following aspects:

1. In case (a), the constants a and b in Theorem 6.4 belong to $\mathbb{F}_{q^2}$, while in Theorem 5.12 of [1] the two elements a and b are in the subfield $\mathbb{F}_q$.
2. In case (b), the constant a in Theorem 6.4 belongs to $\mathbb{F}_{q^2}$, while in Theorem 5.12 of [1] the constant a is in the subfield $\mathbb{F}_q$.
3. In Theorem 6.4 above, the case that k is odd and q is even dealt with, while this case is not considered in Theorem 5.12 of [1].

7. Concluding remarks

Lemma 2.4 does not require the sets A, S and $\bar{S}$ to have any algebraic structures. As demonstrated in [1] and this paper, Lemma 2.4 can be employed to construct many types of permutation polynomials over finite fields when the sets A, S and $\bar{S}$ are finite fields and subsets of finite fields. This clearly shows the power and potential of Lemma 2.4. Of course, one has to figure out specific techniques of using Lemma 2.4 in order to construct specific permutation polynomials. All the results presented in this paper were obtained by using Lemma 2.4 and specific techniques in finite fields.

Acknowledgments

The authors would like to thank the reviewers for their detailed comments that improved the quality and presentation of this paper.

References

[1] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, Finite Fields Appl. 17 (2011) 51–67.

[2] A. Akbary, Q. Wang, A generalized Lucas sequence and permutation binomials, Proc. Amer. Math. Soc. 134 (2005) 15–22.

[3] A. Akbary, Q. Wang, On polynomials of the form $x^r f(x^{q-1}/\ell)$, Int. J. Math. Math. Sci. (2007), Article ID 23408.

[4] P. Charpin, G. Kyureghyan, When does $F(X) + \gamma \operatorname{Tr}(H(X))$ permute $\mathbb{F}_{p^n}$?, Finite Fields Appl. 15 (5) (2009) 615–632.

[5] P. Charpin, G. Kyureghyan, On a class of permutation polynomials over $\mathbb{F}_{2^n}$, in: SETA 2008, in: Lecture Notes in Comput. Sci., vol. 5203, Springer-Verlag, 2008, pp. 368–376.

[6] A. Blokhuis, R.S. Coulter, M. Henderson, C.M. O'Keefe, Permutations amongst the Dembowski–Ostrom polynomials, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications: Proceedings of the Fifth International Conference on Finite Fields and Applications, Springer-Verlag, 2001, pp. 37–42.

[7] C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, Finite Fields Appl. 3 (1997) 159–174.

[8] C. Ding, T. Helleseth, W. Shan, On the linear complexity of Legendre sequences, IEEE Trans. Inform. Theory 44 (1998) 1276–1278.

[9] C. Ding, Q. Xiang, J. Yuan, P. Yuan, Explicit classes of permutation polynomials over GF(3^{3m}), Sci. China Ser. A 53 (2009) 639–647.

[10] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Combin. Theory Ser. A 113 (2006) 1526–1535.

[11] G. Kyureghyan, Constructing permutations of finite fields via linear translators, J. Combin. Theory Ser. A 118 (2011) 1052–1061.

[12] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (2007) 58–70.

[13] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1997.

[14] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge, 1986.

[15] J.E. Marcos, Specific permutation polynomials over finite fields, Finite Fields Appl. 17 (2011) 105–112.

[16] A.M. Masuda, M.E. Zieve, Permutation binomials over finite fields, Trans. Amer. Math. Soc. 361 (2009) 4169–4180.

[17] G.L. Mullen, Permutation polynomials over finite fields, in: Proc. Conf. Finite Fields and Their Applications, in: Lect. Notes Pure Appl. Math., vol. 141, Marcel Dekker, 1993, pp. 131–151.

[18] Y.H. Park, J.B. Lee, Permutation polynomials and group permutation polynomials, Bull. Aust. Math. Soc. 63 (2001) 67–74.

[19] R.L. Rivest, A. Shamir, L.M. Adelman, A method for obtaining digital signatures and public-key cryptosystems, ACM Commun. Comput. Algebra 21 (1978) 120–126.

[20] J. Schwenk, K. Huber, Public key encryption and digital signatures based on permutation polynomials, Electron. Lett. 34 (1998) 759–760.

[21] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, in: Sequences, Subsequences, and Consequences, International Workshop, SSC 2007, Los Angeles, CA, USA, May 31–June 2, 2007, in: Lecture Notes in Comput. Sci., vol. 4893, 2007, pp. 119–128.

[22] X. Zeng, X. Zhu, L. Hu, Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over $\mathbb{F}_{2^n}$, Appl. Algebra Engrg. Comm. Comput. 21 (2010) 145–150.

[23] M.E. Zieve, Some families of permutation polynomials over finite fields, Int. J. Number Theory 4 (2008) 851–857.

[24] M.E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Soc. 137 (2009) 2209–2216.

[25] M.E. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, in: Additive Number Theory, Springer-Verlag, 2010, pp. 355–361.