Science in China Series A: Mathematics
Apr., 2009, Vol. 53, No. 4, 639–647
www.scichina.com math.scichina.com
www.springerlink.com

Explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$

DING CunSheng[1†], XIANG Qing[2], YUAN Jin[3] & YUAN PingZhi[4]

[1] Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong, China

[2] Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

[3] Department of Computing, Macquarie University, NSW 2109, Australia

[4] School of Mathematics, South China Normal University, Guangzhou 510631, China

(email: cding@ust.hk, xiang@math.udel.edu, jyuan@ics.mq.edu.au, mcsypz@mail.sysu.edu.cn)

Abstract Permutation polynomials have been an interesting subject of study for a long time and have applications in many areas of mathematics and engineering. However, only a small number of specific classes of permutation polynomials are known so far. In this paper, six classes of linearized permutation polynomials and six classes of nonlinearized permutation polynomials over $\mathbb{F}_{3^{3m}}$ are presented. These polynomials have simple shapes, and they are related to planar functions.

Keywords: permutation polynomials, planar functions

MSC(2000): 12E10

1 Introduction

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

Permutation polynomials over finite fields have been an interesting subject of study for many years, and have applications in coding theory, cryptography, combinatorial design theory, and many other areas of mathematics and engineering. Information about properties, constructions, and applications of permutation polynomials can be found in [1–5]. In this paper, we present six classes of linearized permutation polynomials and six classes of nonlinearized permutation polynomials over $\mathbb{F}_{3^{3m}}$. We discover these polynomials in an attempt to find new planar functions. The permutation polynomials in this paper have simple shapes: some of them are trinomials and others are quadrinomials. However, the proof that these polynomials are indeed PP is not trivial. We hope that the proof techniques used in this paper will find further applications in other situations.

2 Auxiliary results

Throughout this paper, let $q = 3^m$. In this section we will prove some auxiliary results that will be needed in the sequel. Also we explore some new connections between planar functions

Received February 27, 2008; accepted June 20, 2008
DOI: 10.1007/s11425-008-0142-8

† Corresponding author

This work was supported by Australian Research Council (Grant No. DP0558773), National Natural Science Foundation of China (Grant No. 10571180) and the Research Grants Council of the Hong Kong Special Administrative Region of China (Grant No. 612405)

Citation: Ding C, Xiang Q, Yuan J, Yuan P Z. Explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$. Sci China Ser A, 2009, 52(4): 639–647, DOI: 10.1007/s11425-008-0142-8

and permutation polynomials.

Lemma 2.1. *If $x^3 - ax + k \in \mathbb{F}_q[x]$ is irreducible, then a must be a square of $\mathbb{F}_q$.*

Proof. Suppose that a is not a square of any element in $\mathbb{F}_q$. We now prove that $x^3 - ax + k$ is a permutation polynomial of $\mathbb{F}_q$. If $x^3 - ax + k = y^3 - ay + k$ for two elements $x, y \in \mathbb{F}_q$, then we have $(x - y)((x - y)^2 - a) = 0$ and thus $x = y$. We have shown that $x^3 - ax + k$ is indeed a permutation polynomial of $\mathbb{F}_q$. Therefore $x^3 - ax + k = 0$ has a solution $x \in \mathbb{F}_q$. Thus $x^3 - ax + k$ is reducible in $\mathbb{F}_q[x]$. We have reached a contradiction.

Lemma 2.2. *Let $a \in \mathbb{F}_q$, $a \neq 0$. The polynomial $y^3 - y^2 + a \in \mathbb{F}_q[y]$ is irreducible if and only if $a = a_1^2$ for some $a_1 \in \mathbb{F}_q$ with $\mathrm{tr}(a_1) \neq 0$, where tr is the absolute trace function on $\mathbb{F}_q$.*

Proof. Clearly, $y^3 - y^2 + a \in \mathbb{F}_q[y]$ is irreducible if and only if $z^3 - \frac{1}{a}z + \frac{1}{a} \in \mathbb{F}_q[z]$ is irreducible. Assume that $z^3 - \frac{1}{a}z + \frac{1}{a}$ is irreducible in $\mathbb{F}_q[z]$. By Lemma 2.1, $\frac{1}{a}$ must be a square of $\mathbb{F}_q$, say $\frac{1}{a} = \frac{1}{a_1^2}$, where $a_1 \in \mathbb{F}_q$. Let $z_1 = a_1 z$. We see that $z_1^3 - z_1 + a_1$ is irreducible in $\mathbb{F}_q[z_1]$. By Corollary 3.79 in [3], we have $\mathrm{tr}(a_1) \neq 0$.

Conversely, if $a = a_1^2$ for some $a_1 \in \mathbb{F}_q$, and $\mathrm{tr}(a_1) \neq 0$, then $z_1^3 - z_1 + a_1$ is irreducible $\mathbb{F}_q[z_1]$. By a change of variable, we find that $z^3 - \frac{1}{a}z + \frac{1}{a} \in \mathbb{F}_q[z]$ is irreducible. Hence $y^3 - y^2 + a \in \mathbb{F}_q[y]$ is irreducible.

Since $[\mathbb{F}_{q^3} : \mathbb{F}_q] = 3$, any $b \in \mathbb{F}_{q^3}$ has a unique monic minimal polynomial $x^d + B_1 x^{d-1} + \cdots + B_{d-1}x + B_d \in \mathbb{F}_q[x]$ over $\mathbb{F}_q$, where $B_d \neq 0$, $d \leqslant 3$. For such an element $b \in \mathbb{F}_{q^3}$, we clearly have $b \in \mathbb{F}_q$ if and only if the minimal polynomial of b over $\mathbb{F}_q$ is $x - b \in \mathbb{F}_q[x]$.

Lemma 2.3. *Let $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. Then the minimal polynomial of b over $\mathbb{F}_q$ cannot be of the form $x^2 + B_1 x + B_2 \in \mathbb{F}_q[x]$.*

Proof. Assume to the contrary that the minimal polynomial of b over $\mathbb{F}_q$ is $x^2 + B_1 x + B_2 \in \mathbb{F}_q[x]$. Then $\mathbb{F}_q(b) = \mathbb{F}_{q^2}$, which implies $\mathbb{F}_{q^2} \subset \mathbb{F}_{q^3}$, a contradiction. The proof is complete.

It follows from the above discussions and Lemma 2.3 that the minimal polynomial of any $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ is of the form

$$C_b(x) := x^3 + B_1 x^2 + B_2 x + B_3 \in \mathbb{F}_q[x], \quad B_3 \neq 0, \tag{2.1}$$

which is irreducible in $\mathbb{F}_q[x]$. The three roots of $C_b(x)$ in $\mathbb{F}_{q^3}$ are $x_1 = b$, $x_2 = b^q$ and $x_3 = b^{q^2}$. It then follows that

$$\begin{cases} b^3 + b^{3q} + b^{3q^2} = x_1^3 + x_2^3 + x_3^3 = (x_1 + x_2 + x_3)^3 = -B_1^3, \\ b^{1+q+q^2} = x_1 x_2 x_3 = -B_3, \\ b^{1+2q} + b^{q+2q^2} + b^{2+q^2} = x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2. \end{cases} \tag{2.2}$$

Define

$$\begin{cases} u_1(b) := b^{2+q} + b^{2q+q^2} + b^{2q^2+1} = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1, \\ u_2(b) := b^{1+2q} + b^{q+2q^2} + b^{2+q^2} = x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2. \end{cases} \tag{2.3}$$

Then we have

$$\begin{aligned} u_2(b) + u_1(b) &= x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2 + x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 \\ &= (x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) - (x_1^3 + x_2^3 + x_3^3) \\ &= (x_1 + x_2 + x_3)((x_1 + x_2 + x_3)^2 - 2(x_1 x_2 + x_2 x_3 + x_3 x_1)) - (x_1 + x_2 + x_3)^3 \end{aligned}$$

$$\begin{aligned}&= (x_1+x_2+x_3)(x_1x_2+x_2x_3+x_3x_1)\\ &= -B_1B_2,\end{aligned}$$

and

$$\begin{aligned}u_2(b)u_1(b) &= (x_1x_2^2+x_2x_3^2+x_3x_1^2)(x_1^2x_2+x_2^2x_3+x_3^2x_1)\\ &= (x_1x_2)^3+(x_2x_3)^3+(x_3x_1)^3+x_1^4x_2x_3+x_2^4x_1x_3+x_3^4x_1x_2+3x_1^2x_2^2x_3^2\\ &= (x_1x_2+x_2x_3+x_3x_1)^3+(x_1+x_2+x_3)^3x_1x_2x_3\\ &= B_2^3+B_1^3B_3.\end{aligned}$$

It follows that $u_1(b)$ and $u_2(b)$ are the two roots of the following quadratic polynomial:

$$u^2+B_1B_2u+B_2^3+B_1^3B_3\in\mathbb{F}_q[u]. \tag{2.4}$$

Hence we have

$$u_i(b)=B_1B_2\pm\sqrt{B_1^2B_2^2-(B_2^3+B_1^3B_3)},$$

and

$$\Delta_b:=(x_1-x_2)(x_2-x_3)(x_3-x_1)=u_2(b)-u_1(b)=\pm\sqrt{B_1^2B_2^2-(B_2^3+B_1^3B_3)}. \tag{2.5}$$

More precisely, we have $u_1(b)=B_1B_2+\Delta_b, u_2(b)=B_1B_2-\Delta_b$.

The following lemma is proved in [3, p. 362].

Lemma 2.4. *Let $b\in\mathbb{F}_{q^3}$ and $\alpha_i:=\alpha_i(b)$ be polynomials in b with coefficients in $\mathbb{F}_{q^3}$, $i=0,1,2$. The polynomial $L_b(x)=\alpha_2x^{q^2}+\alpha_1x^q+\alpha_0x\in\mathbb{F}_{q^3}[x]$ is a permutation polynomial of $\mathbb{F}_{q^3}$ if and only if the determinant of the matrix*

$$M_b:=\begin{bmatrix}\alpha_0 & \alpha_2^q & \alpha_1^{q^2}\\ \alpha_1 & \alpha_0^q & \alpha_2^{q^2}\\ \alpha_2 & \alpha_1^q & \alpha_0^{q^2}\end{bmatrix} \tag{2.6}$$

is nonzero.

Straightforward computations show that

$$\det(M_b)=\alpha_0^{1+q+q^2}+\alpha_1^{1+q+q^2}+\alpha_2^{1+q+q^2}-\mathrm{tr}_{q^3/q}(\alpha_0\alpha_1^q\alpha_2^{q^2}), \tag{2.7}$$

where $\mathrm{tr}_{q^3/q}$ is the trace function from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$.

The following two lemmas will be useful in Section 3.

Lemma 2.5. *Let m be a positive integer such that $m\not\equiv 0\pmod 3$. If the minimal polynomial of $b\in\mathbb{F}_{q^3}$ over $\mathbb{F}_q$ is x^3-x-1, then $u_1(b)=-\epsilon$, $u_2(b)=\epsilon$, where $\epsilon\equiv m\pmod 3$.*

Proof. Since $b^3=b+1$, it follows that $b^q=b+\epsilon$ and $b^{q^2}=b-\epsilon$. Hence

$$\begin{aligned}u_1(b) &= b^{2+q}+b^{2q+q^2}+b^{2q^2+1}\\ &= b^2(b+\epsilon)+(b+\epsilon)^2(b-\epsilon)+(b-\epsilon)^2b\\ &= -\epsilon.\end{aligned}$$

Similarly, one can prove that $u_2(b)=\epsilon$.

Lemma 2.6. *Let $b\in\mathbb{F}_{q^3}$. If the minimal polynomial of b over $\mathbb{F}_q$ is $x^3-x^2+a^2$, then $u_1(b)=-a\,\mathrm{tr}(a)$, $u_2(b)=a\,\mathrm{tr}(a)$.*

Proof. Define $c = a/b$. Then $c^3 = c - a$. It follows that $c^q = c - \mathrm{tr}(a)$, $c^{q^2} = c + \mathrm{tr}(a)$, $c^{1+q+q^2} = -a$. We have

$$\begin{aligned} u_1(b) &= b^{2+q} + b^{2q+q^2} + b^{2q^2+1} \\ &= a^3 \frac{c^{2+3q+q^2} + c^{3+q+2q^2} + c^{1+2q+3q^2}}{c^{3+3q+3q^2}} = a(c^{1+2q} + c^{2+q^2} + c^{q+2q^2}) \\ &= a(c(c-\mathrm{tr}(a))^2 + c^2(c+\mathrm{tr}(a)) + (c-\mathrm{tr}(a))(c+\mathrm{tr}(a))^2) = -a\,\mathrm{tr}(a). \end{aligned}$$

Similarly, one can prove that $u_2(b) = a\,\mathrm{tr}(a)$.

Let r be an odd prime power. A function $\Pi : \mathbb{F}_r \to \mathbb{F}_r$ is said to be 2-to-1 if $\Pi(0) = 0$ and $|\Pi^{-1}(y)| = 0$ or 2 for every nonzero y in $\mathbb{F}_r$. A function $\Pi : \mathbb{F}_r \to \mathbb{F}_r$ is said to be planar if the polynomial $\Pi(x+a) - \Pi(x)$ is a PP of $\mathbb{F}_r$ for every $a \in \mathbb{F}_r^*$. A typical planar polynomial over $\mathbb{F}_r$ is x^2. Recent advances on planar functions may be found in [6, 7].

The following result shows that under certain conditions, a planar function from $\mathbb{F}_r$ to itself is the composition of a PP with x^2.

Theorem 2.7. *Let $r \equiv 3 \pmod 4$ be a prime power, and $f : \mathbb{F}_r \to \mathbb{F}_r$ be a function such that $f(-x) = -f(x)$ for all $x \in \mathbb{F}_r$. If $\Pi(x) := f(x^2)$ is a planar function from $\mathbb{F}_r$ to $\mathbb{F}_r$, then f is a permutation of $\mathbb{F}_r$.*

Proof. Since $f(-x) = -f(x)$ for all $x \in \mathbb{F}_r$, we have $f(0) = 0$. Hence $\Pi(0) = 0$. We now prove that Π is 2-to-1.

For any $a \in \mathbb{F}_r^*$, define $\Delta_{\Pi,a}(x) = \Pi(x+a) - \Pi(x)$. Assume that $\Pi(b_1) = \Pi(b_2) = \beta \in \mathbb{F}_r$ for two distinct b_1 and b_2 in $\mathbb{F}_r$. We have

$$\Delta_{\Pi,b_1-b_2}(b_2) = \Pi(b_1) - \Pi(b_2) = 0 = \Pi(-b_2) - \Pi(-b_1) = \Delta_{\Pi,b_1-b_2}(-b_1).$$

It follows from the planar property of Π that $b_2 = -b_1$. Hence, Π is 2-to-1.

For each $u \in \mathbb{F}_r$, define $W_\Pi(u) = |\Pi^{-1}(u)|$. It is known from [8] that

$$\sum_{u \in \mathbb{F}_r} W_\Pi(u+y) W_\Pi(u) = \begin{cases} r-1, & \text{if } y \neq 0, \\ 2r-1, & \text{if } y = 0. \end{cases} \tag{2.8}$$

Since $\Pi(x)$ is 2-to-1, we have

$$W_\Pi(u) = \begin{cases} 1, & \text{if } u = 0, \\ 2, & \text{if } u \in \mathrm{Image}(\Pi) \setminus \{0\}, \\ 0, & \text{if } u \in \mathbb{F}_r \setminus \mathrm{Image}(\Pi). \end{cases} \tag{2.9}$$

Hence, for $y \in \mathbb{F}_r^*$, we have

$$r - 1 = 4|\{u : \{u, u+y\} \subset \mathrm{Image}(\Pi) \setminus \{0\}\}| + 2|\{y, -y\} \cap (\mathrm{Image}(\Pi) \setminus \{0\})|. \tag{2.10}$$

Note that $r - 1 \equiv 2 \pmod 4$ and $0 \leqslant |\{y, -y\} \cap (\mathrm{Image}(\Pi) \setminus \{0\})| \leqslant 2$. We have $|\{y, -y\} \cap (\mathrm{Image}(\Pi) \setminus \{0\})| = 1$ for every nonzero $y \in \mathbb{F}_r$. Consequently, for any $a, b \in \mathbb{F}_r$,

$$\Pi(a) + \Pi(b) = 0 \text{ implies } a = b = 0. \tag{2.11}$$

We now prove the permutation property of f. Denote the set of all nonzero squares and nonsquares in $\mathbb{F}_r$ by Q and N, respectively. Then $\{\{0\}, Q, N\}$ forms a partition of $\mathbb{F}_r$.

We prove that f is injective on Q. Take any two elements of Q, then they can be written as a^2 and b^2, where $a, b \in \mathbb{F}_r^*$. Suppose $f(a^2) = f(b^2)$. Then $\Pi(a) = \Pi(b) = \Pi(-b)$. Since Π is 2-to-1, we have $a = \pm b$, and consequently $a^2 = b^2$.

Note that -1 is a nonsquare in $\mathbb{F}_r$. Take any two elements of N, then they can be written as $-a^2$ and $-b^2$, where $a, b \in \mathbb{F}_r^*$. Suppose $f(-a^2) = f(-b^2)$. Since $f(-x) = -f(x)$ for all $x \in \mathbb{F}_r$, we have $f(a^2) = f(b^2)$. Hence $a^2 = b^2$ by the same arguments as above. Thus f is injective in N too.

We now prove that $f(Q)$ and $f(N)$ are disjoint. Otherwise, there exist $a, b \in \mathbb{F}_r^*$ such that $f(a^2) = f(-b^2)$. Thus $f(a^2) + f(b^2) = \Pi(a) + \Pi(b) = 0$. It follows from (2.11) that $a = b = 0$. This is a contradiction. In summary, we see that f is a permutation of $\mathbb{F}_r$.

Remark. Some of the techniques used in the proof of Theorem 2.7 are borrowed from [8].

3 Six classes of permutation polynomials

Now we are ready to present some explicit classes of permutation polynomials.

Theorem 3.1. *Let m be a positive integer such that $m \equiv 0$ or $1 \pmod 3$. Then*

$$F_b(x) = bx^{q^2} - b^q x^q + (b + b^{q^2})x \in \mathbb{F}_{q^3}[x]$$

is a permutation polynomial of $\mathbb{F}_{q^3}$ for all nonzero $b \in \mathbb{F}_{q^3}$.

Proof. Since $F_b(x)$ is a linearized polynomial, by Theorem 7.9 in [3], we have that $F_b(x)$ is a permutation polynomial of $\mathbb{F}_{q^3}$ if and only if $x = 0$ is the only solution of $F_b(x) = 0$.

If $b \in \mathbb{F}_q^*$, then $F_b(x) = b(x^{q^2} - x^q - x)$. Assume that $x^{q^2} - x^q - x = 0$. Raising both sides of this equation to the q-th power, we have $x - x^{q^2} - x^q = 0$. Adding these two equations together gives $x = 0$. Hence the conclusion of the theorem is true when $b \in \mathbb{F}_q^*$.

We now assume that $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and the minimal polynomial of b over $\mathbb{F}_q$ is $C_b(x) = x^3 + B_1 x^2 + B_2 x + B_3$ as in (2.1). Let $\alpha_0 = b + b^{q^2}$, $\alpha_1 = -b^q$ and $\alpha_2 = b$. It follows from (2.7) that

$$\det(M_b) = B_3 - B_1^3 + \Delta_b, \tag{3.1}$$

where M_b is the matrix in (2.6) and Δ_b is defined in (2.5).

By Lemma 2.4, it suffices to prove that $\det(M_b) \neq 0$. We do so by considering the following two cases.

Case I. $B_1 = 0$. By Lemma 2.1, $B_2 = -A_2^2$ for some $A_2 \in \mathbb{F}_q$. Furthermore, since $b \notin \mathbb{F}_q$, we have $A_2 \neq 0$. Note that the minimal polynomial of b/A_2 over $\mathbb{F}_q$ is $y^3 - y + B_3/A_2^3$. Since $\det(M_{ab}) = a^3 \det(M_b)$ for any $a \in \mathbb{F}_q$, we may assume that $B_2 = -1$ and $B_3 = k$. With these assumptions, we have $\Delta_b = \pm 1$. Suppose that $\det(M_b) = 0$. Then we have $k = \pm 1$. Thus the minimal polynomial of b over $\mathbb{F}_q$ is $x^3 - x \pm 1$. Note that b has minimal polynomial $x^3 - x \pm 1$ if and only if $-b$ has minimal polynomial $x^3 - x \mp 1$. Hence, we may assume that $k = -1$.

If 3 divides m, then $\mathrm{tr}(1) = 0$. Hence, $x^3 - x - 1$ is reducible in $\mathbb{F}_q[x]$, contradicting the fact that the minimal polynomial is irreducible in $\mathbb{F}_q[x]$. If $m \equiv 1 \pmod 3$, it follows from Lemma 2.5 that $\Delta_b = u_2(b) - u_1(b) = -1$. Then $\det(M_b) = 1 \neq 0$, contradicting the assumption that $\det(M_b) = 0$. This completes the proof for Case I.

Case II. $B_1 \neq 0$. Again due to the fact that $\det(M_{ab}) = a^3 \det(M_b)$ for any $a \in \mathbb{F}_q$, we may assume that $B_1 = -1$. Then we have

$$x^3 - x^2 + B_2 x + B_3 = (x + B_2)^3 - (x + B_2)^2 + B_3',$$

where $B_3' = -B_2^3 + B_2^2 + B_3 \neq 0$. So the minimal polynomial of $b + B_2$ over $\mathbb{F}_q$ is $y^3 - y^2 + B_3'$, which should be irreducible over $\mathbb{F}_q$. By Lemma 2.2, $B_3' = a^2$ for some $a \in \mathbb{F}_q^*$ with $\mathrm{tr}(a) \neq 0$. So we may assume that $y^3 - y^2 + a^2$ is the minimal polynomial of $b + B_2$. Hence

$$x^3 - x^2 + B_2 x + B_2^3 - B_2^2 + a^2 \in \mathbb{F}_q[x]$$

is the minimal polynomial of b over $\mathbb{F}_q$. In this case, we have $B_1 = -1, B_3 = B_2^3 - B_2^2 + a^2$.

By (2.5) and Lemma 2.6, $\Delta_b = \Delta_{b+B_2} = -a\,\mathrm{tr}(a)$. If $\det(M_b) = 0$, then we have

$$B_2^3 - B_2^2 + (a + \mathrm{tr}(a))^2 = 0, \tag{3.2}$$

which implies that $z^3 - z^2 + (a + \mathrm{tr}(a))^2$ is reducible in $\mathbb{F}_q[x]$.

However, if $m \equiv 0 \pmod 3$, then $\mathrm{tr}(a + \mathrm{tr}(a)) = \mathrm{tr}(a \pm 1) = \mathrm{tr}(a) \neq 0$. It follows from Lemma 2.2 that $z^3 - z^2 + (a + \mathrm{tr}(a))^2$ is irreducible in $\mathbb{F}_q[x]$. So we have reached a contradiction. If $m \equiv 1 \pmod 3$, then $\mathrm{tr}(a + \mathrm{tr}(a)) = (m + 1)\,\mathrm{tr}(a) = \pm 1 \neq 0$. It follows from Lemma 2.2 that $z^3 - z^2 + (a + \mathrm{tr}(a))^2$ is irreducible over $\mathbb{F}_q$. So we have again reached a contradiction. This completes the proof in Case II.

The first class of nonlinearized permutation trinomials is described in the following theorem.

Theorem 3.2. *Let m be an odd positive integer such that $m \equiv 0$ or $1 \pmod 3$. Then $f(x) = x^{(q^2+1)/2} + x^q - x$ is a permutation polynomial of $\mathbb{F}_{q^3}$.*

Proof. Define $\Pi(x) = f(x^2)$. Then for any $b \in \mathbb{F}_{q^3}$, $\Pi(x + b) - \Pi(x) = F_b(x) + \Pi(b)$, where $F_b(x)$ is the same as in Theorem 3.1. It follows from Theorem 3.1 that $\Pi(x)$ is a planar function on $\mathbb{F}_{q^3}$. Noting that $(q^2 + 1)/2$ is odd, we have $f(-x) = -f(x)$ for all $x \in \mathbb{F}_{q^3}$. Also since m is odd, we see that $q^3 \equiv 3 \pmod 4$. It now follows from Theorem 2.7 that f is a permutation polynomial of $\mathbb{F}_{q^3}$.

The proof of the following theorem is similar to that of Theorem 3.1, and is thus omitted.

Theorem 3.3. *Let m be a positive integer such that $m \equiv 0$ or $1 \pmod 3$. Then*

$$F_b(x) = bx^{q^2} + b^q x^q + (b + b^{q^2})x \in \mathbb{F}_{q^3}[x]$$

is a permutation polynomial on $\mathbb{F}_{q^3}$ for any nonzero $b \in \mathbb{F}_{q^3}$.

The second class of nonlinearized permutation trinomials is described in the following theorem.

Theorem 3.4. *Let m be an odd positive integer such that $m \equiv 0$ or $1 \pmod 3$. Then $g(x) = x^{(q^2+1)/2} - x^q - x$ is a permutation polynomial on $\mathbb{F}_{q^3}$.*

Proof. The conclusion of the theorem follows from Theorems 2.7 and 3.3.

Now we present another class of linearized permutation polynomials.

Theorem 3.5. *Let m be a positive integer such that $m \equiv 0$ or $2 \pmod 3$. Then*

$$H_b(x) = bx^{q^2} + b^q x^q + (b^{q^2} - b)x \in \mathbb{F}_{q^3}[x]$$

is a permutation polynomial on $\mathbb{F}_{q^3}$ *for any nonzero* $b \in \mathbb{F}_{q^3}$.

Proof. Since $H_b(x)$ is a linearized polynomial, by Theorem 7.9 in [3], we see that $H_b(x)$ is a permutation polynomial on $\mathbb{F}_{q^3}$ if and only if $x = 0$ is the only solution of $H_b(x) = 0$.

If $b \in \mathbb{F}_q^*$, then $H_b(x) = b(x^{q^2} + x^q)$. If $x^{q^2} + x^q = 0$. Then $x^q + x = 0$. Suppose that $x^{q-1} = -1$. Then we have $1 = x^{(q-1)(q^2+q+1)} = (-1)^{q^2+q+1} = -1$. This is impossible. Hence $x = 0$. This proves the conclusion of the theorem for all $b \in \mathbb{F}_q^*$.

We now assume that $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and that the minimal polynomial of b is $C_b(x) = x^3 + B_1x^2 + B_2x + B_3$ as in (1). Put $\alpha_0 = b^{q^2} - b$, $\alpha_1 = b^q$ and $\alpha_2 = b$. It follows from (2.7) that

$$\det(M_b) = B_3 + B_1^3 + u_2(b) = B_3 + B_1^3 + B_1B_2 - \Delta_b, \tag{3.3}$$

where M_b is the matrix in (2.6), and $u_2(b)$ and Δ_b are defined as before.

By Lemma 2.4, it suffices to prove that $\det(M_b) \neq 0$. We do so by considering the following two cases.

Case I. $B_1 = 0$. By Lemma 2.1, $B_2 = -A_2^2$ for some $A_2 \in \mathbb{F}_q$. Note that the minimal polynomial of b/A_2 over $\mathbb{F}_q$ is $y^3 - y + B_3/A_2^3$. Since $\det(M_{ab}) = a^3 \det(M_b)$ for any $a \in \mathbb{F}_q$, we may assume without loss of generality that $B_2 = -1$ and $B_3 = k$. With these assumptions, we have $\Delta_b = \pm 1$. Suppose $\det(M_b) = 0$. Then we have $k = \pm 1$. Thus the minimal polynomial of b over $\mathbb{F}_q$ is $x^3 - x \pm 1$. Since b has minimal polynomial $x^3 - x \pm 1$ if and only if $-b$ has minimal polynomial $x^3 - x \mp 1$, we may assume that $k = -1$.

If $m \equiv 0 \pmod 3$, then $\mathrm{tr}(1) = 0$. Hence, $x^3 - x - 1$ is reducible over $\mathbb{F}_q$, contradicting the fact that the minimal polynomial is irreducible in $\mathbb{F}_q[x]$. If $m \equiv 2 \pmod 3$, it follows from Lemma 2.5 that $\Delta_b = u_2(b) - u_1(b) = 1$. Then $\det(M_b) = 1 \neq 0$. This is contrary to the assumption that $\det(M_b) = 0$. This completes the proof for Case I.

Case II. $B_1 \neq 0$. Again due to that $\det(M_{ab}) = a^3 \det(M_b)$ for any $a \in \mathbb{F}_q$, we may assume that $B_1 = -1$. Then we have

$$x^3 - x^2 + B_2x + B_3 = (x + B_2)^3 - (x + B_2)^2 + B_3',$$

where $B_3' = -B_2^3 + B_2^2 + B_3 \neq 0$. So the minimal polynomial of $b + B_2$ over $\mathbb{F}_q$ is $y^3 - y^2 + B_3'$, which should be irreducible over $\mathbb{F}_q$. Then by Lemma 2.2, $B_3' = a^2$ for some $a \in \mathbb{F}_q^*$ with $\mathrm{tr}(a) \neq 0$. So we may assume that $y^3 - y^2 + a^2$ is the minimal polynomial of $b + B_2$ over $\mathbb{F}_q$. Hence

$$x^3 - x^2 + B_2x + B_2^3 - B_2^2 + a^2 \in \mathbb{F}_q[x]$$

is the minimal polynomial of b. In this case, we have $B_1 = -1, B_3 = B_2^3 - B_2^2 + a^2$. By Lemma 2.6, $\Delta_b = \Delta_{b+B_2} = -a\,\mathrm{tr}(a)$. If $\det(M_b) = 0$, then we have

$$(B_2 - 1)^3 - (B_2 - 1)^2 + (a - \mathrm{tr}(a))^2 = 0, \tag{3.4}$$

which implies that $z^3 - z^2 + (a - \mathrm{tr}(a))^2$ is reducible in $\mathbb{F}_q[x]$. However, note that $\mathrm{tr}(a - \mathrm{tr}(a)) = \pm 1 \neq 0$ in both cases $m \equiv 0 \pmod 3$ and $m \equiv 2 \pmod 3$. It then follows from Lemma 2.2 that $z^3 - z^2 + (a - \mathrm{tr}(a))^2$ is irreducible in $\mathbb{F}_q[x]$. So we have reached a contradiction. This completes the proof in Case II.

The third class of nonlinearized permutation polynomials is described in the following theorem.

Theorem 3.6. *Let* m *be an odd positive integer such that* $m \equiv 0$ *or* $2 \pmod 3$. *Then* $h(x) = x^{(q^2+1)/2} - x^q + x$ *is a permutation polynomial of* $\mathbb{F}_{q^3}$.

Proof. The theorem follows from Theorem 3.5 and Theorem 2.7.

4 More explicit classes of permutation polynomials

In this section we present more classes of permutation polynomials. Some of the PP are trinomial, while others are quadrinomials. For the next three theorems, since the proofs of these theorems are analogous to those in Section 3, we omit the proofs.

Theorem 4.1. *Let m be a positive integer. Then*

$$I_b(x) = b^{q^2}x^{q^2} - (b^q - b)x^q + (b^q - b)x \in \mathbb{F}_{q^3}[x]$$

is a permutation polynomial on $\mathbb{F}_{q^3}$ for all nonzero $b \in \mathbb{F}_{q^3}$.

Theorem 4.2. *Let m be a positive integer such that $m \equiv 0$ or $2 \pmod 3$. Then*

$$J_b(x) = b^{q^2}x^{q^2} - (b^q + b)x^q - (b^q - b)x \in \mathbb{F}_{q^3}[x]$$

is a permutation polynomial of $\mathbb{F}_{q^3}$ for all nonzero $b \in \mathbb{F}_{q^3}$.

Theorem 4.3. *Let m be a positive integer such that $m \equiv 0$ or $1 \pmod 3$. Then*

$$K_b(x) = b^{q^2}x^{q^2} + (b^q - b)x^q - (b^q + b)x \in \mathbb{F}_{q^3}[x]$$

is a permutation polynomial of $\mathbb{F}_{q^3}$ for all nonzero $b \in \mathbb{F}_{q^3}$.

The fourth class of nonlinearized permutation polynomials is described in the following theorem.

Theorem 4.4. *Let m be an odd positive integer. Then $h(x) = x^{q^2} - x^q - x^{(q^3+q)/2} - x$ is a permutation polynomial on $\mathbb{F}_{q^3}$.*

Proof. Define $\Pi(x) = h(x^2)$. Then for any $b \in \mathbb{F}_{q^3}$, $\Pi(x + b) - \Pi(x) \equiv -I_b(x) + \Pi(b) \pmod{x^{q^3} - x}$, where $I_b(x)$ is the same as in Theorem 4.1. It follows from Theorem 4.1 that $\Pi(x)$ is a planar function on $\mathbb{F}_{q^3}$. Noting that $(q^3 + q)/2$ is odd, we have $h(-x) = -h(x)$ for all $x \in \mathbb{F}_{q^3}$. Also since m is odd, we see that $q^3 \equiv 3 \pmod 4$. It now follows from Theorem 2.7 that h is a permutation polynomial of $\mathbb{F}_{q^3}$.

The proofs of the following two theorems are similar to that of Theorem 4.4. We omit the details.

Theorem 4.5. *Let m be an odd positive integer such that $m \equiv 0$ or $2 \pmod 3$. Then $h(x) = x^{q^2} - x^q + x^{(q^3+q)/2} + x$ is a permutation polynomial of $\mathbb{F}_{q^3}$.*

Theorem 4.6. *Let m be an odd positive integer such that $m \equiv 0$ or $1 \pmod 3$. Then $h(x) = x^{q^2} + x^q + x^{(q^3+q)/2} - x$ is a permutation polynomial of $\mathbb{F}_{q^3}$.*

Remarks. Two planar functions f and g on $\mathbb{F}_r$ with $f(0) = g(0) = 0$ are said to be equivalent if there are two linearized permutation polynomials L and M of $\mathbb{F}_r$ such that $L(f(x)) = g(M(x))$ for all $x \in \mathbb{F}_r$. As byproducts, we find the following six planar functions on $\mathbb{F}_{q^3}$:

- $P_1(x) = x^{q^2+1} + x^{2q} - x^2$, where $m \equiv 0 \pmod 3$ or $m \equiv 1 \pmod 3$.
- $P_2(x) = x^{q^2+1} - x^{2q} - x^2$, where $m \equiv 0 \pmod 3$ or $m \equiv 1 \pmod 3$.
- $P_3(x) = x^{q^2+1} - x^{2q} + x^2$, where $m \equiv 0 \pmod 3$ or $m \equiv 2 \pmod 3$.
- $P_4(x) = x^{2q^2} - x^{2q} - x^{q+1} - x^2$.
- $P_5(x) = x^{2q^2} - x^{2q} + x^{q+1} + x^2$, where $m \equiv 0 \pmod 3$ or $m \equiv 2 \pmod 3$.
- $P_6(x) = x^{2q^2} + x^{2q} + x^{q+1} - x^2$, where $m \equiv 0 \pmod 3$ or $m \equiv 1 \pmod 3$.

Unfortunately, the six planar functions are equivalent to the known ones from the Albert twisted fields by a theorem of [9]. Nevertheless we believe that the permutation polynomials, especially the nonlinearized ones, are interesting.

Acknowledgments. We thank Weng Guobiao for his helpful comments on Theorems 4.4, 4.5 and 4.6.

References

1 Cohen S D. Permutation group theory and permutation polynomials. In: Algebras and Combinatorics (Hong Kong, 1997). Singapore: Springer, 1999, 133–146
2 Laigle-Chapuy Y. Permutation polynomials and applications to coding theory. *Finite Fields Appl*, **13**: 58–70 (2007)
3 Lidl R, Niederreiter H. Finite Fields, 2nd ed. Encyclopedia of Mathematics and its Applications, 20. Cambridge: Cambridge University Press, 1997
4 Mullen G L. Permutation polynomials over finite fields. In: Proc Conf Finite Fields and Their Applications, Lecture Notes in Pure and Applied Mathematics, Vol 141. New York: Marcel Dekker, 1993, 131–151
5 Sun Q, Wan D. Permutation Polynomials and Their Applications (in Chinese). Shenyang: Liaoning Education Press, 1987
6 Coulter R, Henderson M. Commutative presemifields and semifields. *Adv Math*, **217**: 282–304 (2008)
7 Ding C, Yuan J. A family of skew Hadamard difference sets. *J Combin Theory Ser A*, **113**: 1526–1535 (2006)
8 Weng G B, Qiu W S, Wang Z Y, et al. Pseudo-Paley graphs and skew Hadamard difference sets from commutative semifields. *Des Codes Cryptogr*, **44**: 49–62 (2007)
9 Menichetti G. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J Algebra*, **47**: 400–410 (1977)