New Classes of Permutation Polynomials Having the Forms $(ax^{p^k} - ax + \delta)^s + x$ and $(ax^{p^j} + bx^{p^k} + cx + \delta)^s + x$ Over $\mathbb{F}_{p^n}$

Suphawan Janphaisaeng

Department of Mathematics, Faculty of Science, Naresuan University, Phitsanulok, Thailand

Abstract

A class of permutation polynomials of the form $(x^{2^k} + x + \delta)^s + x$ was derived by Zeng-Zhu-Hu in 2010, and this was generalized to similar forms by Zha-Hu in 2012, by Tu-Zeng-Jiang and Tu-Zeng-Li-Helleseth in 2015, and by Zha-Hu in 2016. Using techniques inspired by the work of Zeng-Zhu-Hu, new classes of permutation polynomials of the forms $(ax^{p^k} - ax + \delta)^s + x$ and $(ax^{p^j} + bx^{p^k} + cx + \delta)^s + x$ are derived.

Keywords: finite fields, permutation polynomials

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of q elements, where $q = p^n$, p is a prime and $n \in \mathbb{N}$ and let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. A polynomial $f(x) \in \mathbb{F}_q[x]$ which induces a bijective map from $\mathbb{F}_q$ to itself is called a permutation polynomial over $\mathbb{F}_q$. Permutation polynomials have been a subject of study for many years, and have applications in coding theory, cryptography, combinatorial designs, and many other areas of mathematics and engineering.

In 2010, Zeng *et al*. [1] provided permutation polynomials over $\mathbb{F}_{2^n}$ in the form $f(x) = (x^{2^k} + x + \delta)^s + x$. Later, Zha and Hu [2] obtained permutation polynomials in very similar form of Zeng-Zhu-Hu but over $\mathbb{F}_{3^n}$ and over $\mathbb{F}_{p^n}$, in 2012. Next, Tu *et al*. [3] provided permutation polynomials in the similar form of Zeng-Zhu-Hu but over $\mathbb{F}_{2^{2m}}$, in 2015 and in the same year, Tu *et al*. [4] obtained permutation polynomials in the form $f(x) = (x^{3^m} - x + \delta)^{3^m+2} + x$ and $f(x) = (x^{3^m} - x + \delta)^{3^{2m} - 3^m - 1} + x$ over $\mathbb{F}_{3^{2m}}$ and permutation polynomials in the form $f(x) = (x^{p^m} - x + \delta)^{i(p^m-1)+1} + x$ over $\mathbb{F}_{p^{2m}}$.

*Corresponding author: E-mail: suphawanj@nu.ac.th

Moreover, in 2016, Zha and Hu [5] derived classes of permutation polynomials in the form $f(x)=(x^{2^m}+x+\delta)^{\frac{2^{2m}+2^m+1}{3}}+x$ and $f(x)=(x^{2^m}+x+\delta)^{2^{2m-2}+2^{m-2}+1}+x$ over $\mathbb{F}_{2^{2m}}$ and also the form $f(x)=(x^{3^m}-x+\delta)^{2\cdot 3^{2m-1}+3^{m-1}}+x$ over $\mathbb{F}_{3^{2m}}$. Using techniques inspired by the work of Zeng *et al*. [1], we obtain new classes of permutation polynomials of the following forms:

1. $(ax^{p^k}-ax+\delta)^s+x$ where $a,k,s\in\mathbb{N}$ with $\gcd(n,k)>1$, $s(p^k-1)\equiv 0(\operatorname{mod} p^n-1)$, $a\in\mathbb{F}_{p^n}^*$ and $\delta\in\mathbb{F}_{p^n}$.
2. $(ax^{p^j}+bx^{p^k}+cx+\delta)^s+x$ where $a,b,c,j,k,s\in\mathbb{N}$ with $j>k,\gcd(n,j,k)=g$, $s(p^g-1)\equiv 0(\operatorname{mod} p^n-1)$, $a,b,c\in\mathbb{F}_{p^n}^*$, $a+b+c=0$ and $\delta\in\mathbb{F}_{p^n}$.

2. Preliminaries

In order to prove the results in this paper, some following basic properties of finite fields are need.

Theorem 2.1 [6] *Let R be a commutative ring of prime characteristic p. Then*

$$(a+b)^{p^n}=a^{p^n}+b^{p^n} \text{ and } (a-b)^{p^n}=a^{p^n}-b^{p^n}$$

for all $a,b\in\mathbb{R}$ and $n\in\mathbb{N}$.

Theorem 2.2 [6] *If F is a finite field with q elements, then every $a\in F$ satisfies $a^q=a$.*

Corollary 2.3 [7] *Let F be a finite field with q elements and E be a field which contains F as a subfield. Then $a^q=a$ for all $a\in F$ and, moreover, for any $\alpha\in E$, $\alpha^q=\alpha$ implies $\alpha\in F$.*

A permutation polynomial over a finite field $\mathbb{F}_{p^n}$ is a polynomial that can be induced to be a permutation of $\mathbb{F}_{p^n}$. Precisely, $f(x)$ is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if f is a bijective map from $\mathbb{F}_{p^n}$ to itself. However, there are several equivalent ways to determine such polynomials, which we collect from [6] as:

Lemma 2.4 [6] *A polynomial $f(x)\in\mathbb{F}_q[x]$ is said to be a permutation polynomial over $\mathbb{F}_q$ if and only if one of the following conditions holds*:

(1) $f:c\mapsto f(c)$ *is onto;*

(2) $f:c\mapsto f(c)$ *is one-to-one;*

(3) $f(x)=a$ *has a solution in* $\mathbb{F}_q$ *for each* $a\in\mathbb{F}_q$;

(4) $f(x)=a$ *has a unique solution in* $\mathbb{F}_q$ *for each* $a\in\mathbb{F}_q$.

Moreover, the main results in [1] and [8] are also required which we record them as:

Proposition 2.5 [1] *For any n and k with $\gcd(n,k)>1$, let s be a positive integer with $s(2^k-1)\equiv 0(\operatorname{mod} 2^n-1)$ and $\delta\in\mathbb{F}_{2^n}$. Then $f(x)=(x^{2^k}+x+\delta)^s+x$ is a permutation polynomial over $\mathbb{F}_{2^n}$.*

Proposition 2.6 [8] *For any $a\in\mathbb{F}_q^*$ and $i,j\in\mathbb{N}$, we have $a^i=a^j$ if and only if $i\equiv j(\operatorname{mod} q-1)$.*

3. Main Results

Theorem 3.1 *Let* $n, a, k, s \in \mathbb{N}$ *with* $\gcd(n,k) > 1$, $s(p^k - 1) \equiv 0 (\bmod\ p^n - 1)$, $a \in \mathbb{F}_{p^n}^*$ *and* $\delta \in \mathbb{F}_{p^n}$. *Then*

$$f(x) = (ax^{p^k} - ax + \delta)^s + x$$

is a permutation polynomial over $\mathbb{F}_{p^n}$.

Proof. By Lemma 2.4, the polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if $f(x) = d$ has a solution in $\mathbb{F}_{p^n}$ for each $d \in \mathbb{F}_{p^n}$, it is enough to show that the equation

$$(ax^{p^k} - ax + \delta)^s + x \quad = d \tag{3.1}$$

has a solution in $\mathbb{F}_{p^n}$. From (3.1), we have

$$\begin{aligned} (ax^{p^k} - ax + \delta)^s \quad &= d - x, \\ (ax^{p^k} - ax + \delta)^{s(p^k-1)} &= (d-x)^{p^k-1}. \end{aligned} \tag{3.2}$$

Case I. $ad^{p^k} - ad + \delta = 0$. Then (3.1) has a solution $x = d$.

Case II. $ad^{p^k} - ad + \delta \neq 0$. We claim that d is not a solution of (3.1). Suppose that d is a solution of (3.1). Then

$$\begin{aligned} (ad^{p^k} - ad + \delta)^s + d &= d, \\ (ad^{p^k} - ad + \delta)^s &= 0, \\ ad^{p^k} - ad + \delta &= 0, \end{aligned}$$

which is a contradiction. Thus d is not a solution of (3.1).

If x_0 is a solution of (3.1), then $x_0 \neq d$ and $ax_0^{p^k} - ax_0 + \delta \neq 0$. From (3.2), we have

$$(ax_0^{p^k} - ax_0 + \delta)^{s(p^k-1)} = (d - x_0)^{p^k-1}.$$

Since $s(p^k - 1) \equiv 0 (\bmod\ p^n - 1)$, by Proposition 2.6,

$$(d - x_0)^{p^k-1} = (ax_0^{p^k} - ax_0 + \delta)^{s(p^k-1)} = 1,$$

so $(d - x_0)^{p^k} = d - x_0$. By Corollary 2.3, $d - x_0 \in \mathbb{F}_{p^k}^*$. Let $d - x_0 = \beta$ for some $\beta \in \mathbb{F}_{p^k}^*$. Hence $x_0 = d - \beta$.

Substituting x_0 into (3.1), we have

$$\begin{aligned} (a(d-\beta)^{p^k} - a(d-\beta) + \delta)^s + (d-\beta) &= d, \\ (a(d^{p^k} - \beta^{p^k}) - ad + a\beta + \delta)^s &= d - d + \beta \qquad \text{[by Theorem 2.1]}, \\ (ad^{p^k} - a\beta^{p^k} - ad + a\beta + \delta)^s &= \beta, \\ (ad^{p^k} - a\beta - ad + a\beta + \delta)^s &= \beta \qquad [\because \beta \in \mathbb{F}_{p^k}^*], \\ (ad^{p^k} - ad + \delta)^s &= \beta. \end{aligned}$$

Hence $x_0 = d - \beta = d - (ad^{p^k} - ad + \delta)^s$.

Next, we shall show that $x = d - (ad^{p^k} - ad + \delta)^s$ is a solution of (3.1).

Let $B = ad^{p^k} - ad + \delta$. Then $x = d - B^s$.

Since $(B^s)^{p^k} = (B^s)^{p^k - 1} \cdot (B^s) = 1 \cdot B^s = B^s$, $B^s \in \mathbb{F}_{p^k}^*$, consider

$$\begin{aligned}
[a(d-B^s)^{p^k} - a(d-B^s) + \delta]^s + (d - B^s) &= [a(d^{p^k} - (B^s)^{p^k}) - ad + aB^s + \delta]^s + d - B^s \\
&= [a(d^{p^k} - B^s) - ad + aB^s + \delta]^s + d - B^s \\
&= [ad^{p^k} - aB^s - ad + aB^s + \delta]^s + d - B^s \\
&= [ad^{p^k} - ad + \delta]^s + d - B^s \\
&= B^s + d - B^s = d.
\end{aligned}$$

Thus (3.1) has a solution $x = d - (ad^{p^k} - ad + \delta)^s$. Hence $f(x)$ is a permutation polynomial over $\mathbb{F}_{p^n}$.

Choosing $p = 2$ in Theorem 3.1, we get:

Corollary 3.2 *Let* n, a, k *and* s *be positive integers with* $s(2^k - 1) \equiv 0 (\bmod 2^n - 1)$ *and* $\delta \in \mathbb{F}_{2^n}$. *Then*

$$f(x) = (ax^{2^k} + ax + \delta)^s + x$$

is a permutation polynomial over $\mathbb{F}_{2^n}$.

Choosing $a = 1$ in Corollary 3.2, we obtain the following corollary which is Proposition 2.5

Corollary 3.3 *For any* n *and* k *with* $\gcd(n,k) > 1$, *let* s *be a positive integer with* $s(2^k - 1) \equiv 0 (\bmod 2^n - 1)$ *and* $\delta \in \mathbb{F}_{2^n}$. *Then*

$$f(x) = (x^{2^k} + x + \delta)^s + x$$

is a permutation polynomial over $\mathbb{F}_{2^n}$.

Theorem 3.4 *Let* $n, a, b, c, j, k, s \in \mathbb{N}$ *with* $g = \gcd(n, j, k)$, $j \ge k$, $s(p^g - 1) \equiv 0 (\bmod p^n - 1)$, $a, b, c \in \mathbb{F}_{p^n}^*$ *and* $a + b + c = 0$. *Let* $\delta \in \mathbb{F}_{p^n}$. *Then*

$$f(x) = (ax^{p^j} + bx^{p^k} + cx + \delta)^s + x$$

is a permutation polynomial over $\mathbb{F}_{p^n}$.

Proof. By Lemma 2.4, the polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if $f(x) = d$ has a solution in $\mathbb{F}_{p^n}$ for each $d \in \mathbb{F}_{p^n}$,it is enough to show that the equation

$$(ax^{p^j} + bx^{p^k} + cx + \delta)^s + x \quad = d \tag{3.3}$$

has a solution in $\mathbb{F}_{p^n}$. From (3.3), we have

$$\begin{aligned}
(ax^{p^j} + bx^{p^k} + cx + \delta)^s &= d - x, \\
(ax^{p^j} + bx^{p^k} + cx + \delta)^{s(p^g - 1)} &= (d - x)^{p^g - 1}.
\end{aligned} \tag{3.4}$$

Case I. $ad^{p^j} + bd^{p^k} + cd + \delta = 0$. Then (3.3) has a solution $x = d$.

Case II. $ad^{p^j} + bd^{p^k} + cd + \delta \neq 0$ .We claim that d is not a solution of (3.3). Suppose that d is a solution of (3.3). Then

$$(ad^{p^j} + bd^{p^k} + cd + \delta)^s + d = d,$$
$$(ad^{p^j} + bd^{p^k} + cd + \delta)^s = 0,$$
$$ad^{p^j} + bd^{p^k} + cd + \delta = 0,$$

which is a contradiction. Thus d is not a solution of (3.3).

If x_0 is a solution of (3.3), then $x_0 \neq d$ and $ax_0^{p^j} + bx_0^{p^k} + cx_0 + \delta \neq 0$. From (3.4), we have

$$(ax_0^{p^j} + bx_0^{p^k} + cx_0 + \delta)^{s(p^g-1)} = (d - x_0)^{p^g-1}.$$

Since $s(p^g - 1) \equiv 0(\bmod p^n - 1)$, by Proposition 2.6,

$$(d - x_0)^{p^g-1} = (ax_0^{p^j} + bx_0^{p^k} + cx_0 + \delta)^{s(p^g-1)} = 1,$$

so $(d - x_0)^{p^g} = d - x_0$. By Corollary 2.3, $d - x_0 \in \mathbb{F}_{p^g}^*$. Let $d - x_0 = \beta$ for some $\beta \in \mathbb{F}_{p^g}^*$. Hence $x_0 = d - \beta$.

Substituting x_0 into (3.3), we have

$$(a(d-\beta)^{p^j} + b(d-\beta)^{p^k} + c(d-\beta) + \delta)^s + (d-\beta) = d,$$
$$(a(d^{p^j} - \beta^{p^j}) + b(d^{p^k} - \beta^{p^k}) + cd - c\beta + \delta)^s = d - d + \beta \qquad [\text{ by Theorem 2.1}],$$
$$(ad^{p^j} - a\beta^{p^j} + bd^{p^k} - b\beta^{p^k} + cd - c\beta + \delta)^s = \beta,$$
$$(ad^{p^j} - a\beta + bd^{p^k} - b\beta + cd - c\beta + \delta)^s = \beta \qquad [\because \beta \in \mathbb{F}_{p^k}^* \subseteq \mathbb{F}_{p^j}^*],$$
$$(ad^{p^j} + bd^{p^k} + cd + \delta - (a+b+c)\beta)^s = \beta,$$
$$(ad^{p^j} + bd^{p^k} + cd + \delta)^s = \beta \qquad [\because a + b + c = 0].$$

Hence $x_0 = d - \beta = d - (ad^{p^j} + bd^{p^k} + cd + \delta)^s$.

Next, we shall show that

$$x = d - (ad^{p^j} + bd^{p^k} + cd + \delta)^s$$

is a solution of (3.3).

Let $B = ad^{p^j} + bd^{p^k} + cd + \delta$. Then $x = d - B^s$.

Since $(B^s)^{p^g} = (B^s)^{p^g-1} \cdot (B^s) = 1 \cdot B^s = B^s$, $B^s \in \mathbb{F}_{p^g}^*$, consider

$$
\begin{aligned}
&[a(d-B^s)^{p^j}+b(d-B^s)^{p^k}+c(d-B^s)+\delta]^s+(d-B^s)\\
&=[a(d^{p^j}-(B^s)^{p^j})+b(d^{p^k}-(B^s)^{p^k})+cd-cB^s+\delta]^s+d-B^s\\
&=[a(d^{p^j}-B^s)+b(d^{p^k}-B^s)+cd-cB^s+\delta]^s+d-B^s\\
&=[ad^{p^j}-aB^s+bd^{p^k}-bB^s+cd-cB^s+\delta]^s+d-B^s\\
&=[ad^{p^j}+bd^{p^k}+cd+\delta-(a+b+c)B^s]^s+d-B^s\\
&=[ad^{p^j}+bd^{p^k}+cd+\delta]^s+d-B^s\\
&=B^s+d-B^s=d.
\end{aligned}
$$

Thus (3.3) has a solutin $x=d-(ad^{p^j}+bd^{p^k}+cd+\delta)^s$. Hence $f(x)$ is a permutation polynomial over $\mathbb{F}_{p^n}$.

4. Acknowledgements

This research was financially supported by Naresuan University, Thailand under Grant no. P2558C360.

References

[1] Zeng, X., Zhu, X. and Hu, L., **2010**. Two new permutation polynomials with the form $(x^{2^k}+x+\delta)^s+L(x)$ over $\mathbb{F}_{2_n}$. *Appl. Algebra Eng. Commun. Comput*., 21, 145-150.

[2] Zha, Z. and Hu, L., **2012**. Two classes of permutation polynomials over finite fields. *Finite Fields and Their Applications*, 18, 781-790.

[3] Tu, Z., Zeng, X. and Jiang, Y., **2015**. Two classes of permutation polynomials having the form $(x^{2^m}+x+\delta)^s+x$. *Finite Fields and Their Applications*, 31, 12-24.

[4] Tu, Z., Zeng, X., Li, C. and Helleseth, T., **2015**. Permutation polynomials of the for $(x^{p^m}-x+\delta)^s+L(x)$ over the finite field $\mathbb{F}_{p^{2m}}$. *Finite Fields and Their Applications*, 34, 20-35.

[5] Zha, Z. and Hu, L., **2016**. Some classes of permutation polynomials of the form $(x^{p^m}-x+\delta)^s+x$ over $\mathbb{F}_{p^{2m}}$. *Finite Fields and Their Applications*, 40, 150-162.

[6] Lidl, R. and Niederreiter, H., **1988**. *Finite Field. Reading*. Addison-Wesley.

[7] Wan, Z.-X., **2003**. *Lectures on Finite Fields and Galois Rings*. Singapore: World Scientific.

[8] Grillet, P.A., **1999**. *Algebra*. New York. John Wiley & Sons, Inc.