Several Classes of Permutation Polynomials over Finite Fields

Guanghong Sun
College of Sciences, Hohai University, Nanjing, China
Email: sgh1976@gmail.com
Received October 2013

Abstract
Several classes of permutation polynomials of the form \((x^{p^k} - x + \delta)^r + L(x)\) over finite fields are presented in this paper, which is a further investigation on a recent work of Li et al.

Keywords
Permutation Polynomial; Finite Fields

1. Introduction
Let \(p\) be a prime and \(\mathbb{F}_p\) denote a finite field with \(p^n\) elements. A polynomial \(f(x) \in \mathbb{F}_p[x]\) is called a permutation polynomial over \(\mathbb{F}_p\) if it induces a one-to-one map from \(\mathbb{F}_p\) to itself. Permutation polynomials were first studied by Hermite [1] for the case of finite prime fields and by Dickson [4] for arbitrary finite fields. Permutation polynomials have been studied extensively and have important applications in coding theory, cryptography, combinatorics, and design theory [3-6]. In the recent years, there has been significant progress in finding new permutation polynomials [7-12].

The determination of permutation polynomials is not an easy problem. An important class of permutation polynomials is of the form

\[(x^{p^k} - x + \delta)^r + L(x),\]

where \(k, t\) are integers, \(\delta \in \mathbb{F}_p\), and \(L(x)\) is a linearized polynomial. In [13], Helleseth and Zinoviev derived new identities on Kloosterman sums by making use of this kind of permutation polynomials. Followed by the research of Helleseth and Zinoviev, many researchers began to study such class of permutation polynomials and numerical results were obtained [14-18].

In this paper, inspired by permutation polynomials obtained by Zha and Hu in [18] and Li et al. in [19], we investigate several new classes of permutation polynomials of the form (1) with \(t = \frac{p^{n-1}}{2} + p^r\), where \(p\) is an odd prime and \(r\) is a nonnegative integer.

This paper is organized as follows. In Section 2, we present several classes of permutation polynomials over \(\mathbb{F}_{p^n}\), which are not covered by [18,19], and over \(\mathbb{F}_p\). We conclude the paper in Section 3.

2. Permutation Polynomials over $F_{3^n}$

In this section, we study the permutation polynomials of the form (1) with $t = \frac{p^s - 1}{2} + p^r$ over $F_{3^n}$. These permutation polynomials are not covered by [18,19].

The trace function from $F_{p^n}$ to its subfield $F_{p^k}$, where $k | n$, is defined by

$$Tr_{p^k}^p(x) = x + x^{p^k} + x^{p^{2k}} + \cdots + x^{p^{n-1}}.$$

Let $\alpha$ be a primitive element of $F_{p^n}$, define $D_0 = \langle \alpha^2 \rangle$, and $D_i = \alpha D_0$. Then $F_{p^n} = [0] \cup D_0 \cup D_i$.

Obviously, when $x \in D_i$, we have that $x^{\frac{p^s - 1}{2}} = (\alpha^2)^i = (\alpha^4)^i$ for $i = 0,1$.

When $i = 0,1$, Li et al. in [19] investigates the permutation polynomials with the form of

$$31 333 2() nkkkk xx xx xx = + + + +$$

The following theorem shows that it is also a permutation polynomial when $i = 2$.

**Theorem 1** Let $n = 3k$, where $k$ is a positive integer, and $\delta \in F_{3^n}$ with $Tr_{3^k}^3(\delta) = 0$. Then

$$(x^{3^i} - x + \delta)^{\frac{3^{i+1} - 1}{2}} + x^{3^i} + x$$

is a permutation polynomial over $F_{3^n}$.

**Proof** For any $b \in F_{3^n}$, it is sufficient to prove the Equation

$$(x^{3^i} - x + \delta)^{\frac{3^{i+1} - 1}{2}} + x^{3^i} + x = b$$

has exactly one solution over $F_{3^n}$.

If $x$ is a solution of the Equation (2), then we consider three cases in the following.

1) Case A: $x^{3^i} - x + \delta = 0$. By (2), we have $x^{3^i} + x = b$. Then the two Equations lead to $x = -b - \delta$. Hence

$$x^{3^i} - x + \delta = -b^{3^i} - b - \delta^{3^i} - \delta.$$

2) Case B: $x^{3^i} - x + \delta \in D_0$. By (2), we have

$$-x^{3^{2i}} + x^{3^i} - x = -b - \delta^{3^{2i}}.$$  \hspace{1cm} (3)

Raising the $3^i$th power on the both sides of Equation (3), we have

$$-x + x^{3^{2i}} - x^{3^i} = b^{3^i} - \delta.$$  \hspace{1cm} (4)

By Equations (3) and (4), we have $x = b + b^{3^i} - \delta - \delta^{3^{2i}}$. Hence

$$x^{3^i} - x + \delta = b^{3^i} - b + \delta^{3^{2i}} - \delta^{3^i} + \delta.$$

By $Tr_{3^k}^3(\delta) = 0$, $x^{3^i} - x + \delta = b^{3^i} - b + \delta^{3^{2i}}$.  \hspace{1cm} (5)

3) Case C: $x^{3^i} - x + \delta \in D_i$. By (2), we have $x^{3^{2i}} + x^{3^i} = b + \delta^{3^{2i}}$. Raising the $3^i$th and $3^{2i}$th power on the both sides of the above Equation, respectively, we have $x + x^{3^{2i}} = b^{3^i} + \delta$ and $x^{3^i} + x = b^{3^{2i}} + \delta^{3^i}$. By the three Equations, we have $x = b - b^{3^i} - b^{3^{2i}} + \delta - \delta^{3^i} + \delta^{3^{2i}}$. So

$$x^{3^i} - x + \delta = \delta^{3^{2i}} + b - b^{3^i}.$$

Let $\omega = \delta^{3^{2i}} + b - b^{3^i}$, then $x^{3^i} - x + \delta = \omega$ in Case B.

If Case A happens, namely, $-b^{3^i} + b - \delta^{3^i} = 0$, then $\omega = \delta^{3^{2i}} + b = b^{3^{2i}} + \delta^{3^i} = 0$. Hence only one case will happen in the above three cases. So $(x^{3^i} - x + \delta)^{\frac{3^{i+1} - 1}{2}} + x^{3^i} + x = b$ has exactly one solution over $F_{3^n}$, that is to say, $(x^{3^i} - x + \delta)^{\frac{3^{i+1} - 1}{2}} + x^{3^i} + x$ is a permutation polynomial over $F_{3^n}$. The theorem holds.
The following theorems give several new classes of permutation polynomials which are not covered by [18,19].

**Theorem 2** Let \( n = 3k \) , where \( k \) is a positive integer, and \( \delta \in F_{3^k} \) with \( Tr_k^i (\delta) = 0 \). Then \((x^{3^i} - x + \delta)^{\frac{3^{k_i} - 1}{3^i}} + x^{3^i} + x \) is a permutation polynomial over \( F_{3^k} \) for any \( i = 0,1 \) or 2.

**Proof** For all \( b \in F_{3^k} \), it is sufficient to prove the Equation \((x^{3^i} - x + \delta)^{\frac{3^{k_i} - 1}{3^i}} + x^{3^i} + x = b \) has exactly one solution over \( F_{3^k} \) for any \( i = 0,1 \) or 2. For \( i = 0,1 \) or 2, the proof is similar, so we only prove the permutation polynomial for \( i = 1 \), namely,

\[
(x^{3^i} - x + \delta)^{\frac{3^{k_i} - 1}{3^i}} + x^{3^i} + x = b \tag{5}
\]

If \( x \) is a solution of the Equation (5), then we consider three cases in the following.

1) Case A: \( x^{3^i} - x + \delta = 0 \). By (5), we have \( x^{3^i} + x = b \). Raising the \( 3^i \) th power on both sides, we have \( x + x^{3^i} = b^{3^i} \). By \( x^{3^i} - x + \delta = 0 \) and \( x + x^{3^i} = b^{3^i} \), we have \( x = -b^{3^i} - \delta \). Hence \( x^{3^i} - x + \delta = -b^{3^i} + b^{3^i} - \delta^{3^i} - \delta \).

2) Case B: \( x^{3^i} - x + \delta = x^{3^k} - x + b^{3^i} \). By (5), we have \( -x^{3^k} - x + b^{3^i} = b^{3^i} - \delta^{3^i} \). Raising the \( 3^i \) th power and \( 3^k \) th power on the both sides of the above Equation, respectively, then we have \( -x^{3^k} - x + x^{3^i} = b^{3^i} - \delta^{3^i} \) and \( -x^{3^k} - x + x^{3^i} = b^{3^i} - \delta^{3^i} \). By the two Equations, we have \( x = b^{3^i} - \delta^{3^i} + b^{3^i} - \delta^{3^k} \). Hence \( x^{3^i} - x + \delta = -b^{3^i} + b^{3^i} + \delta^{3^i} \).

3) Case C: \( x^{3^i} - x + \delta = D_3 \). By (5), we have \( x^{3^i} + x = b^{3^i} \). Raising the \( 3^i \) th power and \( 3^k \) th power on the both sides of the above Equation, respectively, then we have \( x^{3^i} + x^{3^i} = b^{3^i} - \delta^{3^i} \) and \( x^{3^i} + x^{3^i} = b^{3^i} + \delta^{3^k} \). By the three equations, we have \( x = -b^{3^i} + b^{3^i} - \delta^{3^i} - \delta \). Hence only one case will happen in the above three cases. Therefore, \((x^{3^i} - x + \delta)^{\frac{3^{k_i} - 1}{3^i}} + x^{3^i} + x = b \) has exactly one solution over \( F_{3^k} \), that is to say, \((x^{3^i} - x + \delta)^{\frac{3^{k_i} - 1}{3^i}} + x^{3^i} + x \) is a permutation polynomial over \( F_{3^k} \). The theorem holds.

**Theorem 3** Let \( n = 3k \), where \( k \) is a positive integer, and \( \delta \in F_{3^k} \) with \( Tr_k^i (\delta) = 0 \). Then \((x^{3^i} - x + \delta)^{\frac{3^{k_i} - 1}{3^i}} + x^{3^i} + x^3 - x \) is a permutation polynomial over \( F_{3^k} \) for any \( i = 0,1 \) or 2.

**Proof** Since the proof is similar for any \( i = 0,1 \) or 2, we only prove the permutation polynomial when \( i = 1 \). For all \( b \in F_{3^k} \), it is sufficient to prove

\[
(x^{3^i} - x + \delta)^{\frac{3^{k_i} - 1}{3^i}} + x^{3^i} + x^3 - x = b \tag{6}
\]

has exactly one solution over \( F_{3^k} \). If \( x \) is a solution of the Equation (6), then we consider three cases in the following.

1) Case A: \( x^{3^i} - x + \delta = 0 \). By (6), we have \( x^{3^k} + x^3 - x = b \).

By the two Equations, we have \( x^{3^k} = b + \delta \).

So \( x = b^{3^i} + \delta^{3^i} \) and \( x^{3^i} - x + \delta = b^{3^i} + \delta^{3^i} - b^{3^i} - \delta^{3^i} + \delta \).

2) Case B: \( x^{3^i} - x + \delta = D_3 \). By (6), we have \( x^{3^i} + x = \delta^{3^i} - b \). Let \( u = \delta^{3^i} - b \), then \( x + x^{3^i} = u^{3^i} \) and \( x^{3^i} + x^{3^k} = u^{3^i} \). By the three Equations, we have \( x = u^{3^i} - u^{3^i} - u \). So \( x^{3^i} - x + \delta = -b^{3^i} + b - \delta^{3^i} \).

3) Case C: \( x^{3^i} - x + \delta = D_3 \). By (6), we have \( x^{3^i} + x = -b - \delta^{3^i} \). Let \( v = -b - \delta^{3^i} \), then \( x^{3^i} + x^3 = v^{3^i} \) and \( x + x^{3^i} = v^{3^i} \). By the three equations, we have \( x = -v^{3^i} + v^{3^i} - v \). Hence
\[ x^3 - x + \delta = b^{3k_1} - b^{3k_2} - \delta^{3k_2} - \delta. \]

Let \( \Delta = b^{3k_1} - b - \delta^{3k_2} - \delta \), then \( b^{3k_1} - b^{3k_2} - \delta^{3k_2} - \delta = \Delta^{3k_2} \) in Case C.

If Case A occurs, then we have \( \Delta = - (\delta + \delta^{3k_2} + \delta^{3k_2}) = 0 \). Hence only one case will happen in the above three cases. Therefore, \( (x^3 - x + \delta)^{\text{ord}^k} + x^{3k_1} + x^3 - x = b \) has exactly one solution over \( F_{3^n} \). The theorem holds.

In the above section, we consider permutation polynomials over \( F_{3^n} \). In the following, we investigate permutation polynomials over \( F_{p^n} \) for an odd prime \( p \).

**Theorem 4** Let \( n = 4k \), where \( k \) is a positive integer and \( p \) be an odd prime. Then
\[
(x^{p^{2k}} - x + \delta) + x^{p^{2k}} + x \text{ is a permutation polynomial over } F_{p^n} \text{ for any } i = 0, 1, 2 \text{ or } 3.
\]

**Proof** For all \( b \in F_{p^n} \), it is sufficient to prove \( (x^{p^{2k}} - x + \delta)^{\text{ord}^{p^i}} + x^{p^{2k}} + x = b \) only have a solution over \( F_{p^n} \) for any \( i = 0, 1, 2 \) or 3.

Since the proof is similar for \( i = 0 \) or 2, we only consider \( i = 0 \).

Similarly, the proof is also similar for \( i = 1 \) or 3, so we only consider \( i = 1 \).

For \( i = 0 \), if \( x \) is a solution of the equation \( (x^{p^{2k}} - x + \delta)^{\text{ord}^{p^i}} + x^{p^{2k}} + x = b \), then we consider three cases in the following.

1) **Case A** \( 0 \): \( x^{p^{2k}} - x + \delta = 0 \). Then we have \( x^{p^{2k}} + x = b \). Hence \( x = \frac{1}{2}(b + \delta) \). Therefore,
\[
x^{p^{2k}} - x + \delta = \frac{1}{2}(b^{p^{2k}} - b + \delta^{p^{2k}} + \delta).
\]

2) **Case B** \( 0 \): \( x^{p^{2k}} - x + \delta \in D_0 \). Then we have \( x^{p^{2k}} = \frac{1}{2}(b - \delta) \) and \( x = \frac{1}{2}(b^{p^{2k}} - \delta^{p^{2k}}) \). Hence
\[
x^{p^{2k}} - x + \delta = \frac{1}{2}(b^{p^{2k}} - b + \delta^{p^{2k}} + \delta).
\]

3) **Case C** \( 0 \): \( x^{p^{2k}} - x + \delta \in D_1 \). Then we have \( x = \frac{1}{2}(b + \delta) \). Hence \( x^{p^{2k}} - x + \delta = \frac{1}{2}(b^{p^{2k}} - b + \delta^{p^{2k}} + \delta) \).

Hence only one case will occur in the above three cases. Therefore, \( (x^{p^{2k}} - x + \delta)^{\text{ord}^{p^i}} + x^{p^{2k}} + x = b \) only have a solution over \( F_{p^n} \).

For \( i = 1 \), if \( x \) is a solution of the equation
\[
(x^{p^{2k}} - x + \delta)^{\text{ord}^{p^i}} + x^{p^{2k}} + x = b,
\]
then we also consider three cases in the following.

1) **Case A** \( 1 \): \( x^{p^{2k}} - x + \delta = 0 \). Then we have \( x^{p^{2k}} + x = b \). Hence \( x = \frac{1}{2}(b + \delta) \). Therefore,
\[
x^{p^{2k}} - x + \delta = \frac{1}{2}(b^{p^{2k}} - b + \delta^{p^{2k}} + \delta).
\]

2) **Case B** \( 1 \): \( x^{p^{2k}} - x + \delta \in D_0 \). Then we have
\[
x^{p^{2k}} + x^{p^{2k}} - x^{p^{2k}} + x = b - \delta^{p^{2k}}. \tag{7}
\]

Let \( u = b - \delta^{p^{2k}} \). Then raising the \( p^k \) th power, \( p^{2k} \) th power, and \( p^{3k} \) th power on the both sides for Equation (7), respectively, we have
\[
x + x^{p^{2k}} - x^{p^{2k}} + x^{p^{2k}} = u^{p^k} \tag{8}
\]
\[
x^{p^{2k}} + x - x^{p^{2k}} + x^{p^{2k}} = u^{p^{2k}} \tag{9}
\]
Adding (7) to (8), we have
\[ 2x^{p^2} + 2x = u + u^{p^2}. \]  
(11)

Subtracting (10) from (9), we have
\[ 2x - 2x^{p^2} = u^{p^2} - u^{p^2} . \]  
(12)

Adding (11) to (12), we have
\[ 4x = u + u^{p^2} + u^{p^2} - u^{p^2} . \]
Hence
\[ x = \frac{1}{4}(u + u^{p^2} + u^{p^2} - u^{p^2}) \]
and
\[ x^{p^2} - x + \delta = \frac{1}{2}(b^{p^2} - b^{p^2} + \delta^{p^2} + \delta) . \]

3) Case C\(_1\) : \( x^{p^2} - x + \delta \in D_1 \). Then we have
\[ x^{p^2} - x^{p^2} - x^{p^2} - x = -b - \delta^{p^2} . \]  
(13)

Let \( \nu = -b - \delta^{p^2} \). Raising the \( p \) th power, \( p^2 \) th power, and \( p^3 \) th power on both sides of Equation (13), respectively, then we obtain
\[ x - x^{p^2} - x^{p^2} - x^{p^2} = \nu^{p^2} \]  
(14)
\[ x^{p^2} - x - x^{p^2} - x^{p^2} = \nu^{p^2} \]  
(15)
\[ x^{p^2} - x^{p^2} - x - x^{p^2} = \nu^{p^2} \]  
(16)

Subtracting (13) from (14), then we obtain
\[ 2x - 2x^{p^2} = \nu^{p^2} - \nu. \]  
(17)
Adding (15) to (16), then we have
\[ -2x - 2x^{p^2} = \nu^{p^2} + \nu^{p^2} . \]  
(18)
Subtracting (18) from (17), then we obtain
\[ 4x = -\nu + \nu^{p^2} - \nu^{p^2} - \nu^{p^2} . \]
Hence
\[ x = \frac{1}{4}(-\nu + \nu^{p^2} - \nu^{p^2} - \nu^{p^2}) \]
and
\[ x^{p^2} - x + \delta = \frac{1}{2}(-b^{p^2} + b^{p^2} + \delta^{p^2} + \delta) . \]

Let \( \Delta = b^{p^2} - b^{p^2} + \delta^{p^2} + \delta \). Then \( -b^{p^2} + b^{p^2} + \delta^{p^2} + \delta = \Delta^{p^2} \) in the Case C\(_1\).

If Case A\(_1\) occurs, then \( b^{p^2} - b + \delta^{p^2} + \delta = 0 \).
Hence
\[ \Delta = b^{p^2} - b^{p^2} + \delta^{p^2} + \delta = b^{p^2} - b^{p^2} + \delta^{p^2} + \delta \]
\[ = -\delta^{p^2} - \delta^{p^2} + \delta^{p^2} + \delta = -(x - x^{p^2})^{p^2} - (x - x^{p^2})^{p^2} + (x - x^{p^2})^{p^2} + x - x^{p^2} = 0 \]
Hence only one case will occur in the above three cases. Therefore, \((x^{p^2} - x + \delta)^{\frac{p^2-1}{2}} + x^{p^2} + x = b\) only has a solution over \(F_{p^r}\). The theorem holds.

3. Conclusion

In the paper, we obtain some permutation polynomials of the form \((x^{p^2} - x + \delta)^t + L(x)\) with \(t = \frac{p^2-1}{2} + p'\), which are not covered by [18,19]. It is possible that they have some applications in coding theory, cryptography, combinatorics, design theory and so on.

Acknowledgements

This work was supported by the Natural Science Foundation of China under Grant No. 61103184, No. 61173134, and No. 61272542.

References
