Some New Permutation Polynomials Having the Form \((x^{2^m} + x + \delta)^t + x\)

Qingjun Cai and Yuli Zhang

ABSTRACT

Permutation polynomials over finite field with character 2 have many applications on the block cipher. In this paper, we give some new permutation polynomials having the form \((x^{2^m} + x + \delta)^t + x\) over the finite field \(F_{2^m}\), which firstly studied by Ziran Tu in 2015 by solving the equations directly. But the process is too complex. The key break through is the proper commutative diagrams are found for the new permutation polynomial, which make the process of proving the permutation property more simple. Our work also include some results found in the work of Ziran Tu.

INTRODUCTION

For a prime power \(q\), let \(F_q\) be the finite field with \(q\) elements. A polynomial \(F_q[x]\) is called a permutation polynomial (PP) if its associated polynomial mapping \(f : c \mapsto f(c)\) from \(F_q\) to itself is a bijection. Permutation polynomials over finite fields have important applications in cryptography, coding theory and combinatorial design theory, and other areas of mathematics and engineering. Finding new PPs is of great interest in both theoretical and applied aspects. Helleseth and Zinoviev found a class of permutation polynomials with a special form during their research on Kloosterman sums [3]. This motivated Yuan and Ding to investigate the permutation behavior of the polynomials having the form \((x^{2^i} + x + \delta)^t + x\) over the finite field \(F_q\), where \(k, t,\) are integers, and \(\delta\) is an element of \(F_q\) [6][7]. Recently, these permutation polynomials have attracted much attention. Some permutation polynomials of the form \((x^{2^i} + x + \delta)^t + x\) over \(F_{2^m}\) are proposed in[4], which \(t\) satisfies either \(t(2^m + 1) = 2^m + l(\text{mod} 2^m - 1)\) or \(t(2^m - 1) = 2^n - l(\text{mod} 2^m - 1)\).

The method for getting the permutation behavior of the polynomials proposed in[4] is just solving the equations directly, but the process is too complex. The criterion, recently discovered by Akbary, Ghioca and Wang[1] is a simple and effective method that establishes the permutation property of a mapping \(F_q \rightarrow F_q\).
through a commutative diagram. But the difficulty is how to form the proper commutative diagram and the maps on it. In this paper, the proper commutative diagrams and the maps are found for the polynomials \((x^m + x + \delta)' + x \) over \(F_{2^m}\), and the permutation property is reduced to decide whether a simpler function over a small field is a permutation polynomial. We get more permutation polynomials and most work in [4] are included in this paper.

The remainder of this paper is organized as follows. In Section 2, we introduce some basic concepts and related results. In Section 3, some new permutation polynomials are given and some permutation polynomials given in [4] will be proven again using our new method.

PRELIMINARIES

**Lemma 2.1** ([1])(AGW criterion) Let \( R, S \) and \( \sigma \) be finite sets with \(|S| = |\sigma|\), and let \( f : R \rightarrow R, \tilde{f} : S \rightarrow S \), and \( \varphi : R \rightarrow S, \bar{\varphi} : R \rightarrow S \) be maps such that \( \varphi \circ f = \tilde{f} \circ \varphi \), i.e. the following diagram commutes:

\[
\begin{array}{ccc}
R & \xrightarrow{f} & R \\
\downarrow \varphi & & \downarrow \bar{\varphi} \\
S & \xrightarrow{\tilde{f}} & S
\end{array}
\]

**Figure 1. AGW.**

If both \( \varphi \) and \( \bar{\varphi} \) are surjective, then the following statements are equivalent:

1. \( f \) is a permutation of \( R \);
2. \( \tilde{f} \) is bijective from \( S \) to \( S \) and \( f \) is injective on \( \varphi^{-1}(s) = \{x | \varphi(x) = s, x \in R\} \) for each \( s \in S \).

**Lemma 2.2** ([2]) The cubic equation \( x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0 \) has a unique solution \( x \in F_{2^n} \) if and only if

\[
Tr_{F_{2^n}/F_2}(\frac{(\sigma_2 + \sigma_1 \sigma_3)^{\frac{1}{3}}}{\sigma_1 + \sigma_2 \sigma_3} + 1) = 1, \quad \text{where} \quad \sigma_1, \sigma_2, \sigma_3 \in F_{2^n}.
\]

**Lemma 2.3** ([2]) For a positive integer \( m \), the quadratic equation \( x^2 + ax + b = 0 \), has solutions \( x \in F_{2^n} \) if and only if \( Tr_{F_{2^n}/F_1}(\frac{b}{a}) = 0 \), where \( a \neq 0 \).

NEW PERMUTATION POLYNOMIALS

In this subsection, we give the main results of this paper.

**Theorem 3.1** For a positive integer \( m \), any element \( \delta \in F_{2^m} \), the polynomial \((x^m + x + \delta)' + x \) permutes \( F_{2^m} \) for \( t \in \{2^i | u = 1, \cdots, 2m - 1\} \).

242
Proof Let $R = F_{2^m}, S = F_{2^n}, \phi(x) = \varphi(x) = x^{2^{m}} + x + \delta^{2^{m}} + \delta$, then

\[
\varphi(x)^{2^{m}} = (x^{2^{m}} + x + \delta^{2^{m}} + \delta)^{2^{m}}
\]
\[
= x^{2^{m}} + x^{2^{2m}} + \delta^{2^{2m}} + \delta^{2^{m}}
\]
\[
= x^{2^{m}} + x + \delta^{2^{m}} + \delta = \varphi(x)
\]

So $\varphi(x) = \varphi(x) \in F_{2^{n}},$ i.e. $\varphi(x), \varphi(x)$ are maps from $F_{2^{m}}$ to $F_{2^n}$.

Let $f(x) = x + (x + \delta)^{t} + (x + \delta^{2^{m}})^{t}$, then

\[
\varphi(f(x)) = [(x^{2^{m}} + x^{2^{2m}} + \delta^{2^{2m}} + \delta)^{2^{m}}]^{2^{m}}
\]
\[
= [(x^{2^{m}} + x^{2^{2m}} + \delta^{2^{2m}} + \delta)^{2^{m}}]^{2^{m}}
\]
\[
= (x^{2^{m}} + x^{2^{2m}} + \delta^{2^{2m}} + \delta)^{2^{m}}
\]
\[
= (x^{2^{m}} + x + \delta^{2^{m}})^{t} + (x^{2^{m}} + x + \delta^{2^{m}})^{t} + x + \delta^{2^{m}} + \delta
\]
\[
= (\varphi(x) + \delta^{t} + (\varphi(x) + \delta^{2^{m}})^{t} + \varphi(x)) = f(\varphi(x))
\]

From the lemma 2.1 AGW criterion, in order to prove $f$ is a permutation on $F_{2^n}$, we only need to show that $\varphi(x) = \varphi(x) = x^{2^{m}} + x + \delta^{2^{m}} + \delta$ are surjective, $\tilde{f}$ is injective from $S = F_{2^n}$ to $\tilde{S} = F_{2^n}$ and $f$ is injective on $\phi^{-1}(s)$ for each $s \in S$. From the theorem 7.16 in [5], $\varphi(x) = \varphi(x) = x^{2^{m}} + x + \delta^{2^{m}} + \delta$

are surjective. For each $s \in S$, let $x_1, x_2 \in \phi^{-1}(s)$, then

\[
x_1^{2^{m}} + x_1 + \delta^{2^{m}} + \delta = x_2^{2^{m}} + x_2 + \delta^{2^{m}} + \delta = s, \quad \text{and} \quad f(x_1) = (x_1^{2^{m}} + x_1 + \delta^{2^{m}})^{t} + x_1
\]
\[
\neq (s + \delta^{2^{m}})^{t}
\]
\[
+ x_2 = f(x_2), \quad \text{so} \quad f \quad \text{is injective on} \quad \phi^{-1}(s) \quad \text{for each} \quad s \in S. \quad \text{Finally, we will show that}
\]
\[
\tilde{f}(x) = x +
\]
\[
(x + \delta)^{t} + (x + \delta^{2^{m}})^{t} \quad \text{is a bijective map on the} \quad F_{2^n}. \quad \text{When} \quad x_1, x_2 \in F_{2^n} \quad \text{satisfies}
\]
\[
\tilde{f}(x_1) = \tilde{f}(x_2),
\]
then $x_1 + (x_1 + \delta^{t}) + (x_1 + \delta^{2^{m}})^{t} = x_2 + (x_2 + \delta^{t}) + (x_2 + \delta^{2^{m}})^{t}$, As $t = 2^n$, then

\[
x_1 + x_2 + (x_1 + \delta^{2^{m}})^{t}
\]
\[
+ (x_2 + \delta^{t}) + (x_2 + \delta^{2^{m}})^{t} = 0, \quad \text{then} \quad x_1 + x_2 +
\]
\[
(x_1 + \delta^{t}) + (x_1 + \delta^{2^{m}})^{t} + (x_2 + \delta^{t}) + (x_2 + \delta^{2^{m}})^{t} = 0,
\]
\[
\therefore x_1 + x_2 = 0, \quad \text{so} \quad x_1 = x_2, \quad \text{that is} \quad \tilde{f} \quad \text{a injective map, as} \quad F_{2^n} \quad \text{is a finite set, then} \quad \tilde{f} \quad \text{is a bijective map.} \quad \blacksquare
\]

Remark 3.1 In theorem 3.1, if $\delta \in F_{2^n}$, then

\[
\delta^{2^{m}} = \delta, \quad \text{so} \quad \tilde{f}(x) = x + (x + \delta)^{t} + (x + \delta^{2^{m}})^{t} = x .
\]

Obviously, $\tilde{f}(x) = x$ is a permutation on $F_{2^n}$ for any $t \in \{0,1, \cdots 2^{m} - 1\}$, then

\[
(x^{2^{m}} + x + \delta)^{t} + x \quad \text{is a permutation on} \quad F_{2^n} \quad \text{for any} \quad t \in \{0,1, \cdots 2^{m} - 1\}.
\]

From remark 3.1, we only need to prove the permutation property of

\[
(x^{2^{m}} + x + \delta)^{t} + x \quad \text{when} \quad \delta \in F_{2^n} \setminus F_{2^n} \quad \text{for some} \quad t .
\]

Theorem 3.2 For a positive integer $m$, any element $\delta \in F_{2^n}$ or $\delta \in F_{2^m} \setminus F_{2^n}$ with

\[
Tr_{2^{m} \rightarrow 2^n}(\delta) = \delta^{2^{m}} + \delta = 1,
\]
the polynomial $(x^{2^{m}} + x + \delta)^{t} + x$ permutes $F_{2^n}$ for $t \in 2^{m} + 1, 2^{m} + 2^{u} | u = 0,1, \cdots, 2m - 1$.

Proof Let $R = F_{2^n}, S = \bar{S} = F_{2^n}, \varphi(x) = \varphi(x)$

\[
= x^{2^{m}} + x + \delta^{2^{m}} + \delta, \quad \tilde{f}(x) = x + (x + \delta)^{t} + (x + \delta^{2^{m}})^{t}.
\]
From the proof of theorem 3.1 and remark 3.1, we get the results. ■

**Theorem 3.3** For a positive integer \( m \), any element \( \delta \in F_{2^m} \), and
\[
t \cdot 2^n \equiv t \mod(2^{2m} - 1)
\]
(i.e. \( t = (2^m + 1) \cdot k \), \( k = 0, 1, \ldots, 2^m - 2 \)) the polynomial \( (x^{2^n} + x + \delta)^t + x \) permutes \( F_{2^m} \).

**Proof** Let \( R = F_{2^m}, S = S = F_{2^m} \), \( \varphi(x) = \bar{\varphi}(x) = x^{2^n} + x + \delta^{2^m} + \delta \), \( \tilde{f}(x) = x. \) From the proof of theorem 3.1 and remark 3.1, we get the results. ■

**Theorem 3.4** For a positive integer \( m \), any element \( \delta \in F_{2^m} \) with \( Tr_{2^{2m}/2^m}(\delta) = \delta^{2^n} + \delta = 1 \), or \( \delta \in F_{2^m} \) the polynomial
\[
(x^{2^n} + x + \delta)^{2^{m-1}2^{m-1}+1} + x \text{ permutes } F_{2^m} \).

**Proof** Let \( R = F_{2^m}, S = S = F_{2^m} \), \( \varphi(x) = \bar{\varphi}(x) = x^{2^n} + x + \delta^{2^n} + \delta \), \( \tilde{f}(x) = x \)
\[
(x + \delta)^{2^{m-1}2^{m-1}+1} + (x + \delta^{2^n})^{2^{m-1}2^{m-1}+1}, \text{ From the AGW criterion, we get the desired result. ■}

In the following, we assume \( 0^{-1} = 0 \).

**Theorem 3.5** For a positive integer \( m \), any element \( \delta \in F_{2^m} \) with \( Tr_{2^{2m}/2^m}(\delta) = \delta^{2^n} + \delta = 1 \), or \( \delta \in F_{2^m} \) the polynomial
\[
(x^{2^n} + x + \delta)^{2^{m-1}+1} + x \text{ permutes } F_{2^m} \).

**Proof** Let \( R = F_{2^m}, S = S = F_{2^m} \), \( \varphi(x) = \bar{\varphi}(x) = x^{2^n} + x + \delta^{2^n} + \delta \), \( \tilde{f}(x) = x + (x + \delta)^{2^{m-1}} \)
\[
+ (x + \delta^{2^n})^{2^{m-1}}, \text{ We only need to show that } \tilde{f}(x) \text{ is a bijective map on the } F_{2^m} \text{ for } \delta \notin F_{2^m}.
\]
\[
\tilde{f}(x) = x + (x + \delta)^{2^{m-1}} + (x + \delta^{2^n})^{2^{m-1}}
\]
\[
= x + (x + \delta) + (\delta + \delta^{2^n})^2(x + \delta)^{-1}
\]
\[
+ (x + \delta^{2^n}) + (\delta + \delta^{2^n})^2(x + \delta^{2^n})^{-1}
\]
\[
= x + \delta + \delta^{2^n} + (\delta + \delta^{2^n})^2[(x + \delta)^{-1}
\]
\[
+ (x + \delta^{2^n})^{-1}]
\]

For a \( \alpha \in F_{2^m} \), if \( \tilde{f}(x) = \alpha \), then we get
\[
x^3 + (\delta + \delta^{2^n} + \alpha)x^2 + (\alpha \delta + \alpha \delta^{2^n} + \delta^{2^{2m}+1})x + (\delta + \delta^{2^n})^3 + \alpha \delta^{2^{2m}+1} = 0.
\]

Using the notions in lemma 2.2, \( \sigma_1 = \delta + \delta^{2^n} + \alpha \),
\[
\sigma_2 = \alpha \delta + \alpha \delta^{2^n} + \delta^{2^{2m}+1}, \sigma_3 = (\delta + \delta^{2^n})^3 + \alpha \delta^{2^{2m}+1},
\]
then
\[
Tr_{F_{2^m}/F_2} \left( \frac{(\sigma_2 + \sigma_1^{-1})^3}{\sigma_3 + \sigma_1 \sigma_2} + 1 \right) = Tr_{F_{2^m}/F_2} \left( \frac{(\alpha + \delta)(\alpha + \delta^{2^n})}{\delta^2 + (\delta^{2^n})^2} \right)
\]

As the quadratic equation
\[
x^2 + (\delta + \delta^{2^n})x + (\alpha + \delta)(\alpha + \delta^{2^n}) = 0
\]
has solutions $\alpha + \delta, \alpha + \delta^{2^m} \in F_{2^m} \setminus F_{2^n}$, as $\alpha \in F_{2^n}$ while $\delta \notin F_{2^n}$, then from lemma 2.2, $\text{Tr}_{F_{2^n}/F_{2^m}}\left(\frac{\alpha + \delta(\alpha + \delta^{2^m})}{\delta^2 + (\delta^{2^m})^2}\right) = 1$. At last, from lemma 2.3, $\tilde{f}(x)$ is a bijective map. ■

**Theorem 3.6** For a positive integer $m$, any element $\delta \in F_{2^m}$ with

$$\text{Tr}_{F_{2^m}/F_{2^n}}(\delta) = \delta^{2^m} + \delta = 1,$$

or $\delta \in F_{2^n}$, the polynomial $(x^{2^n} + x + \delta)^{2^{m-1}} + x$ permutes $F_{2^n}$.

**Proof** Let $R = F_{2^{2m}}, S = \bar{S} = F_{2^n}, \phi(x) = \overline{\phi}(x)$

$$= x^{2^n} + x + \delta^{2^n} + \delta, \quad \tilde{f}(x) = x + (x + \delta)^{2^{m-1}}$$

$$+ (x + \delta^{2^n})^{2^{m-1}} = x + (x + \delta)^{-1} + (x + \delta^{2^n})^{-1},$$

We will prove $\tilde{f}(x)$ is a bijective map. As $F_{2^n}$ is a finite set, then we only need to prove $\tilde{f}(x)$ is a surjective map. For $\alpha \in F_{2^n}$, if

$$x + (x + \delta)^{-1} + (x + \delta^{2^n})^{-1} = \alpha, \quad \delta^{2^n} + \delta = 1,$$

then we get $x^3 + (1 + \alpha)x^2 + (\alpha + \delta^{2^n+1})x + 1 + \alpha \delta^{2^n+1} = 0$.

Using the notions of lemma 2.2, $\sigma_1 = 1 + \alpha$, $\sigma_2 = \alpha + \delta^{2^n+1}$, $\sigma_3 = 1 + \alpha \delta^{2^n+1}$, then

$$\text{Tr}_{F_{2^n}/F_{2^m}}\left(\frac{(\sigma_2 + \sigma_1^2)^3}{\sigma_3 + \sigma_1 \sigma_2}\right) + 1)$$

$$= \text{Tr}_{F_{2^n}/F_{2^m}}\left((\sigma_2 + \sigma_1^2 + 1)^\frac{1}{2} + 1\right)$$

$$= \text{Tr}_{F_{2^n}/F_{2^m}}\left((\sigma_2 + \sigma_1^2 + 1)^\frac{1}{2} + 1\right)$$

$$= \text{Tr}_{F_{2^n}/F_{2^m}}\left((\sigma_2 + \sigma_1^2 + 1)^\frac{1}{2} + 1\right)$$

$$= \text{Tr}_{F_{2^n}/F_{2^m}}\left((\delta^{2^n+1})^{12^{m-1}}\right)$$

$$= \delta^{(2^n+1)(2^{m-1})} + \delta^{(2^n+1)(2^{m-1})} + \delta^{(2^n+1)(2^{m-1})} + \cdots + \delta^{(2^n+1)(2^{m-1})}$$

$$= \delta^{(2^n+1)(2^{m-1})} + \delta^{(2^n+1)(2^{m-1})} + \delta^{(2^n+1)(2^{m-1})} + \cdots + \delta^{(2^n+1)(2^{m-1})}$$

$$= \delta^{(2^n+1)(2^{m-1})} + \delta^{(2^n+1)(2^{m-1})} + \delta^{(2^n+1)(2^{m-1})} + \cdots + \delta^{(2^n+1)(2^{m-1})}$$

$$= \delta + \delta^{2^n} = 1$$

from lemma 2.3, $\tilde{f}(x)$ is a bijective map. ■

In the following table, we list known results on $(x^{2^m} + x + \delta)^{t} + x$ over $F_{2^n}$.
CONCLUDING REMARKS

Three classes of new permutation polynomials over finite fields of characteristic 2 are proposed, and these polynomials have the form \( x^{2^m} + x + \alpha^t + \delta \). This paper continues the study in [4]. Table 1 summarizes known permutation polynomials over \( F_{2^m} \) of the form \( x^{2^m} + x + \alpha^t + \delta \).

ACKNOWLEDGMENT

The authors would like to acknowledge the anonymous reviews and the financial support of the Natural Sciences Foundation Council of China (NSFC) 11371106.

REFERENCES


[4] ZiRan Tu, Xiangyong Zeng, Yupeng Jiang, Two classes of permutation polynomials having the form \( x^{2^m} + x + \alpha^t + \delta \), Finite Fields Appl. 31(2015)12-24.


<table>
<thead>
<tr>
<th>( k ) and ( s )</th>
<th>conditions on ( \delta )</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>( k = 1 ) and ( s = 2^t )</td>
<td>( s \in {0, 1} )</td>
<td>[3]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
<tr>
<td>( m + 1 ) even, ( s = 2^m + 1 )</td>
<td>( s \in {0, 1} )</td>
<td>[4]</td>
</tr>
</tbody>
</table>

Table 1: known results in \( f(x) = x^{2^m} + x + \alpha^t + \delta \) over \( F_{2^m} \).
[10] X. Zeng, X. Zhu, L. Hu, Two new permutation polynomials with the form \((x^{2^k} + x + \delta)' + x\) over 
\(F_{2^n}\), Applicable Algebra in Engineering, Communication and Computing March 2010,
Volume 21, Issue 2, 145-150.