NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 48 (2018), 25-29

A NOTE ON PERMUTATION BINOMIALS AND TRINOMIALS OVER FINITE FIELDS

Neranga Fernando

(Received August 5, 2017)

Abstract. Let p be an odd prime and e be a positive integer. We completely explain the permutation binomials and trinomials arising from the reversed Dickson polynomials of the $(k+1)$-th kind $D_{n,k}(1,x)$ over $\mathbb{F}_{p^e}$ when $n=p^l+2$, where $l \in \mathbb{N}$.

1. Introduction

Let p be a prime and e be a positive integer. Let $\mathbb{F}_{p^e}$ be the finite field with p^e elements. A polynomial $f \in \mathbb{F}_{p^e}[\mathbf{x}]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_{p^e}$ if the associated mapping $x \mapsto f(x)$ from $\mathbb{F}_{p^e}$ to $\mathbb{F}_{p^e}$ is a permutation of $\mathbb{F}_{p^e}$.

Let k be an integer such that $0 \leq k \leq p-1$ and $a \in \mathbb{F}_{p^e}$. The n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ is defined by

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i}, \tag{1.1}$$

and $D_{0,k}(a,x) = 2-k$; see [**6**].

The permutation behaviour of the n-th reversed Dickson polynomial of the $(k+1)$-kind $D_{n,k}(a,x)$ over finite fields and its properties were explored by the author of the present paper in [**2**]. It was shown in [**2**] that to discuss the permutation property of $D_{n,k}(a,x)$, one only has to consider $a=1$. The cases $n=p^l$, $n=p^l+1$, and $n=p^l+2$, where p is an odd prime and $l \geq 0$ is an integer, were discussed in [**2**]. The first two cases were completely explained and we list the results of the last case obtained in [**2**] below.

Result 1. ([**2**, Remark 2.14]) Let p be an odd prime, $k=0$, and $l=e$. Then we have

$$D_{p^e+2,0}(1,x) = \frac{1}{2}(1-4x)^{\frac{p^e+1}{2}} - x + \frac{1}{2}$$

which is a PP of $\mathbb{F}_{p^e}$ if and only if $p^e \equiv 1 \pmod 3$.

Result 2. ([**2**, Theorem 2.15]) Let p be an odd prime and $k=2$. Then $D_{p^l+2,k}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $l=0$.

Result 3. ([**2**, Theorem 2.16]) Let $p>3$ and $k=4$. Then $D_{p^l+2,k}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if the binomial $x^{\frac{p^l-1}{2}} - \frac{1}{2}x$ is a PP of $\mathbb{F}_{p^e}$.

2010 *Mathematics Subject Classification* 11T06, 11T55.
Key words and phrases: Finite field, Permutation polynomial, Binomial, Trinomial, Reversed Dickson polynomial.

Result 4. ([**2**, Theorem 2.17]) Let p be an odd prime, $n = p^l + 2$, and $k \neq 0, 2, 4$. Then $D_{n,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if the trinomial $(4-k)\, x^{\frac{p^l+1}{2}} + k\, x^{\frac{p^l-1}{2}} + (2-k)x$ is a PP of $\mathbb{F}_{p^e}$.

This paper is a result of a question asked by Xiang-dong Hou. He asked the author (private communication) "when is the trinomial in Result 4 a PP of $\mathbb{F}_{p^e}$?". This paper answers that question completely.

The paper is organized as follows.

In Section 2, we present some preliminaries that will be used throughout the paper. In Section 3, we explain a family of permutation trinomials over $\mathbb{F}_{p^e}$ arising from the reversed Dickson polynomials when $p > 3$ is odd and k is an integer such that $k \neq 0, 2, 4$. In Section 4, we explain a family of permutation binomials over $\mathbb{F}_{p^e}$ arising from the reversed Dickson polynomials when $p = 3$.

2. Preliminaries

In this section, we list some preliminaries that will be useful in latter sections. Let $q = p^e$ in the following two theorems.

Theorem 2.1 (Hermite's Criterion, [**4**])**.** *$f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

(i) *$f^{q-1} \pmod{x^q - x}$ has degree $q-1$;*

(ii) *for each integer s with $1 \leq s \leq q-2$, $f^s \equiv f_s \pmod{x^q - x}$ for some $f_s \in \mathbb{F}_q[x]$ with deg $f_s \leq q-2$.*

Theorem 2.2 ([**8**])**.** *Pick $d, r > 0$ with $d \mid (q-1)$, and let $h \in \mathbb{F}_q[x]$. Then $f(x) = x^r h(x^{\frac{q-1}{d}})$ permutes $\mathbb{F}_q$ if and only if*

(1) *$\gcd(r, \frac{q-1}{d}) = 1$, and*

(2) *$x^r h(x)^{\frac{q-1}{d}}$ permutes μ_d,*

where μ_d is the set of d^{th} roots of unity in the algebraic closure of $\mathbb{F}_q$.

3. A Family of Permutation Trinomials

In this section, we completely explain the permutation behaviour of the trinomial in result 4 when $p > 3$.

Theorem 3.1. *Let $p > 3$ be an odd prime and $q = p^e$, where e is a non-negative integer. Let k be an integer such that $k \neq 0, 2, 4$ and $0 \leq k \leq p-1$. Let*

$$f(x) = (4-k)x^{\frac{p^l+1}{2}} + kx^{\frac{p^l-1}{2}} + (2-k)x.$$

Then f is a PP of $\mathbb{F}_q$ if and only if $l = 0$ and $k \neq 3$.

Proof. Assume $l = 0$ and $k \neq 3$.

Since $l = 0$, $f(x) = 2(3-k)x + k$. Since $k \neq 3$, clearly f is a PP of $\mathbb{F}_q$.

Consider the following three cases.

Case 1. $l = 0$ and $k = 3$.

Case 2. $l \neq 0$ and $k = 3$.

Case 3. $l \neq 0$ and $k \neq 3$.

Now we claim that f is not a PP of $\mathbb{F}_{p^e}$ in each case above.

Case 1. Since $l = 0$ and $k = 3$, $f(x) = 3$, which is clearly not a PP of $\mathbb{F}_{p^e}$.

Case 2. Let $l \neq 0$ and $k = 3$. Then

$$f(x) = x^{\frac{p^l+1}{2}} + 3x^{\frac{p^l-1}{2}} - x.$$

Note that $f(1) = 3$ and

$$f(-1) = (-1)^{\frac{p^l+1}{2}} + 3(-1)^{\frac{p^l-1}{2}} + 1,$$

which implies

$$f(-1) = \begin{cases} -1, & \frac{p^l+1}{2} \text{ is even,} \\ 3, & \frac{p^l+1}{2} \text{ is odd.} \end{cases}$$

Clearly, $f(x)$ is not a PP when $\frac{p^l+1}{2}$ is odd.

When $\frac{p^l+1}{2}$ is even, we have $p^l + 1 \equiv 0 \pmod 4$ and hence $p > 5$. It is clear that $f(4) \equiv 3 \pmod p$ when $\frac{p^l+1}{2}$ is even.

Hence f is not a PP of $\mathbb{F}_{p^e}$ in Case 2.

Case 3. Let $l \neq 0$ and $k \neq 3$. Consider

$$f(x) = (4-k)x^{\frac{p^l+1}{2}} + kx^{\frac{p^l-1}{2}} + (2-k)x.$$

Note that $f(0) = 0$. Also note that $f(\mathbb{F}_p) \subseteq \mathbb{F}_p$.

Sub Case 3.1. $l = (2n)e$, where $n \in \mathbb{Z}^+$. Then we have

$$\frac{p^l+1}{2} = \frac{p^{(2n)e}+1}{2} = \frac{(p^{ne}-1)(p^{ne}+1)}{2} + 1 \equiv 1 \pmod{p^e - 1},$$

which implies

$$f(x) = (4-k)x^{\frac{p^l+1}{2}} + kx^{\frac{p^l-1}{2}} + (2-k)x \equiv 2(3-k)x + kx^{p^e-1} \pmod{x^{p^e} - x}.$$

Since

$$2(k-3)x \equiv k \pmod p$$

has a non-zero solution, there exists a non-zero $x \in \mathbb{F}_p$ such that $f(x) = 0$. Hence f is not a PP of $\mathbb{F}_{p^e}$.

(or by Hermite's criterion, f is not a PP of $\mathbb{F}_{p^e}$ since the degree of $f(x) > p^e - 2$).

Sub Case 3.2. $l \neq (2n)e$, where $n \in \mathbb{Z}^+$. Note that here we only need to consider $1 \leq l \leq 2e-1$ since

$$\frac{p^{2e+i}+1}{2} \equiv \frac{p^i+1}{2} \pmod{p^e - 1} \text{ and } \frac{p^{2e+i}-1}{2} \equiv \frac{p^i-1}{2} \pmod{p^e - 1},$$

which imply

$$(4-k)x^{\frac{p^{2e+i}+1}{2}} + kx^{\frac{p^{2e+i}-1}{2}} + (2-k)x \equiv (4-k)x^{\frac{p^i+1}{2}} + kx^{\frac{p^i-1}{2}} + (2-k)x \pmod{x^{p^e} - x}.$$

So, let $1 \leq l \leq 2e-1$ and consider

$$f(x) = (4-k)x^{\frac{p^l+1}{2}} + kx^{\frac{p^l-1}{2}} + (2-k)x.$$

Let $x \in \mathbb{F}_p^*$ and l be even. Then

$$\begin{aligned} f(x) &= (4-k)x^{\frac{p^l-1}{2}+1} + kx^{\frac{p^l-1}{2}} + (2-k)x \\ &= 2(3-k)x + k. \end{aligned}$$

Since

$$2(k-3)x \equiv k \pmod{p}$$

has a non-zero solution, there exists a non-zero $x \in \mathbb{F}_p$ such that $f(x) = 0$. Hence f is not a PP of $\mathbb{F}_{p^e}^*$.

Assume that l is odd. Then clearly for $x \in \mathbb{F}_{p^e} \setminus \mathbb{F}_p$, $f(x) \notin \mathbb{F}_p$.

Since l is odd, for $x \in \mathbb{F}_p$ we have

$$f(x) = (4-k)x^{\frac{p+1}{2}} + kx^{\frac{p-1}{2}} + (2-k)x$$

which implies

$$f^2(x) = k^2x^{p-1} + \text{ terms with lower degree.}$$

By Hermite's criterion, $f(x)$ does not permute $\mathbb{F}_p$. Hence f is not a PP of $\mathbb{F}_{p^e}$. This completes the proof.

□

4. A Family of Permutation Binomials

In this section, we completely explain the permutation behaviour of the trinomial in result 4 when $p = 3$.

Let $p = 3$. Since $k \neq 0, 2$, we have $k = 1$. Then

$$f(x) = (4-k)x^{\frac{p^l+1}{2}} + kx^{\frac{p^l-1}{2}} + (2-k)x = x^{\frac{p^l-1}{2}} + x.$$

Theorem 4.1. *Let $p = 3$ and $q = 3^e$, where e is a non-negative integer. Let*

$$f(x) = x^{\frac{p^l-1}{2}} + x.$$

Then f is a PP of $\mathbb{F}_q$ if and only if

(i) *$l = 0$, or*

(ii) *$l = me + 1$, where m is a non-negative even integer.*

Proof. When $l = 0$, $f(x) = x + 1$ which is a PP of $\mathbb{F}_q$.

Let $l = me + 1$, where m is a non-negative even integer. Note that since m is a non-negative even integer, we have

$$\frac{3^{me+1}-1}{2} = \frac{3^{me}-1}{2} + 3^{me} = \frac{(3^{\frac{me}{2}}-1)(3^{\frac{me}{2}}+1)}{2} + 3^{me} \equiv 1 \pmod{3^e-1}.$$

So, when $l = me + 1$, where m is a non-negative even integer, $f(x) \equiv 2x \pmod{x^{3^e}-x}$ which is clearly a PP of $\mathbb{F}_{3^e}$.

Now assume that $l \neq 0$ and $l = me + 1$, where m is a non-negative odd integer.

$$\frac{3^{me+1}-1}{2} \pmod{3^e-1} \text{ is } \begin{cases} \text{even}, & \text{e is odd}, \\ \text{odd}, & \text{e is even}. \end{cases}$$

If $\frac{3^{me+1}-1}{2} \pmod{3^e-1}$ is even, then $f(0) = 0 = f(-1)$ which implies $f(x)$ is not a PP of $\mathbb{F}_q$.

Now consider the case where $\frac{3^{me+1}-1}{2} \pmod{3^e-1}$ is odd. Note that in this case e is even. Also,

$\frac{3^{me+1}-1}{2} \equiv \frac{3^e-1}{2} + 1 \pmod{3^e-1}$. Then

$$f(x) = x^{\frac{3^{me+1}-1}{2}} + x \equiv x^{\frac{3^e-1}{2}+1} + x \pmod{x^{3^e} - x}.$$

Now we claim that $x^{\frac{3^e-1}{2}+1} + x$ is not a PP of $\mathbb{F}_{3^e}$.

$$x^{\frac{3^e-1}{2}+1} + x = x(x^{\frac{3^e-1}{2}} + 1) = x\,h(x^{\frac{3^e-1}{2}}),$$

where $h(x) = x+1$. $\gcd(1, \frac{3^e-1}{2}) = 1$, but $-1 \in \mu_2$ and $h(-1) = 0$. So $x\,h(x)^{\frac{3^e-1}{2}}$ does not permute μ_2. Then by Theorem 2.2, f is not a PP of $\mathbb{F}_{3^e}$.

This completes the proof.

□

Acknowledgements

The author is grateful to the referee for useful comments. He wants to thank the referee for pointing out that Theorem 2.2 appeared in [**1**], [**3**] and [**7**] in different formats. He also wants to thank the referee for drawing his attention to Lemma 1 in [**5**] that also explains the last part of Theorem 4.1 where Theorem 2.2 is used.

References

[1] A. Akbary and Q. Wang, *On polynomials of the form $x^r f(x^{\frac{(q-1)}{l}})$*, Int. J. Math. Math. Sci. 2007, Art. ID 23408, 7 pp.

[2] N. Fernando, *Reversed Dickson polynomials of the $(k+1)$-th kind over finite fields*, J. Number Theory **172** (2017), 234–255.

[3] J.B. Lee and Y.H. Park, *Some permuting trinomials over finite fields*, Acta Math. Sci. (English Ed.), **17** (3) (1997), 250–254.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[5] H. Niederreiter and K.H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. Ser. A, **33** (2) (1982), 197–212.

[6] Q. Wang and J.L. Yucas, *Dickson polynomials over finite fields*, Finite Fields Appl., **18** (2012), 814–831.

[7] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, from *Sequences, Subsequences, and Consequences*, Lecture Notes in Comput. Sci., 4893, Springer, Berlin, 2007.

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

Neranga Fernando
Department of Mathematics,
Northeastern University,
Boston, MA 02115
w.fernando@northeastern.edu