Finite Fields and Their Applications 49 (2018) 126–131

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On permutation trinomials of type $x^{2p^s+r} + x^{p^s+r} + \lambda x^r$

Daniele Bartoli [a], Giovanni Zini [b,*,1]

[a] *Department of Mathematics and Computer Science, University of Perugia, Italy*
[b] *Department of Mathematics and Computer Science "Ulisse Dini", University of Florence, Italy*

A R T I C L E I N F O

Article history:
Received 18 May 2017
Accepted 23 September 2017
Available online 2 October 2017
Communicated by Gary L. Mullen

MSC:
11T06
05A05

Keywords:
Permutation trinomials
Exceptional polynomials

A B S T R A C T

We determine all permutation trinomials of type $x^{2p^s+r} + x^{p^s+r} + \lambda x^r$ over the finite field $\mathbb{F}_{p^t}$ when $(2p^s + r)^4 < p^t$. This partially extends a previous result by Bhattacharya and Sarkar in the case $p = 2$, $r = 1$.

1. Introduction

Let p be a prime number, t be a positive integer, $\mathbb{F}_{p^t}$ be the finite field with p^t elements, and $f(x)$ be a polynomial over $\mathbb{F}_{p^t}$. If $f : x \mapsto f(x)$ is a permutation of $\mathbb{F}_{p^t}$, then $f(x)$ is a *permutation polynomial* (PP) of $\mathbb{F}_{p^t}$. If $f(x)$ is a PP of $\mathbb{F}_{(p^t)^m}$ for infinitely many m,

* Corresponding author.
E-mail addresses: daniele.bartoli@unipg.it (D. Bartoli), gzini@math.unifi.it (G. Zini).

[1] The research of D. Bartoli and G. Zini was supported in part by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza" – Prot. N. 2012XZE22K_005) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA-INdAM).

https://doi.org/10.1016/j.ffa.2017.09.010
1071-5797/

then $f(x)$ is an *exceptional polynomial* over $\mathbb{F}_{p^t}$. If both $f(x)$ and $f(x)+x$ are PPs of $\mathbb{F}_{p^t}$, then $f(x)$ is a *complete permutation polynomial* (CPP) of $\mathbb{F}_{p^t}$.

The study of permutation polynomials over finite fields is motivated not only by their theoretical importance, but also by their remarkable applications to cryptography, combinatorial designs, and coding theory; see for instance [7,9,12]. For a detailed introduction to old and new developments on permutation polynomials, see the survey [6] and the references therein. Permutation polynomials of monomial and binomial type have been intensively investigated, while much less is known on permutation trinomials; see [3,5].

In this note we characterize a certain class of permutation trinomials. Let s and r be non-negative integers. For $\lambda \in \mathbb{F}_{p^t}$, denote by $f_\lambda(x)$ the polynomial

$$f_\lambda(x) = x^{2p^s+r} + x^{p^s+r} + \lambda x^r \in \mathbb{F}_{p^t}[x].$$

If $r=0$, define $d=0$. If $r \neq 0$, write $r = p^u v$ with $u \geq 0$ and $p \nmid v$, and define $d = 2p^{s-u} + v$ if $u \leq s$, $d = 2 + p^{u-s}v$ if $u > s$; that is,

$$d = (2p^s + r)/p^m, \quad m := \max\{n \geq 0 \ : \ p^n \mid (2p^s + r),\ p^n \mid (p^s + r),\ p^n \mid r\}.$$

We prove the following result.

Theorem 1.1. *Assume that $d^4 < p^t$. Then $f_\lambda(x)$ is a PP of $\mathbb{F}_{p^t}$ if and only if one of the following cases holds:*

- $p = 2$, *t is odd, and* $f_\lambda(x) = x^3 + x^2 + x$ *or* $f_\lambda(x) = x^5 + x^3 + x$;
- $p \equiv 2 \pmod 3$, *t is odd, and* $f_\lambda(x) = x^3 + x^2 + \frac{1}{3}x$.

The case $p = 2$ and $r = 1$ was already considered by Bhattacharya and Sarkar [2], where the result proved for $f_\lambda(x)$ was then used to characterize permutation binomials of $\mathbb{F}_{p^{2tp^s}}$ of type $g_b(x) = x^{\frac{p^{2tp^s}-1}{p^t-1}+1} + bx$. Here for $p > 2$ and $r = 1$ we go the opposite direction, using the characterization in [1] for permutation binomials of type $g_b(x)$ to deduce the result for $f_\lambda(x)$.

Every permutation polynomial of $\mathbb{F}_{p^t}$ with degree less than $(p^t)^{1/4}$ is exceptional over $\mathbb{F}_{p^t}$; thus, the condition $d^4 < p^t$ allows us to consider only exceptional polynomials. For $r > 1$, this leads to the non-existence of permutation trinomials of type $f_\lambda(x)$.

2. Proof of Theorem 1.1

Since the maps $x \mapsto x^{p^u}$ and $x \mapsto x^{p^s}$ are permutations of $\mathbb{F}_{p^t}$, we can assume that $u = 0$ if $u \leq s$, and $s = 0$ if $u > s$.

- Case $r = 0$. Since $f_\lambda(x) = f_\lambda(-x-1)$, $f_\lambda(x)$ is not a PP of $\mathbb{F}_{p^t}$.
- Case $r = 1$ and $p = 2$. The claim is proved in [2, Theorem 1.3].

- Case $r = 1$ and $p > 2$.
Assume first that $s = 0$, so that $f_\lambda(x) = x^3 + x^2 + \lambda x$. By direct computation,

$$\frac{f_\lambda(x) - f_\lambda(y)}{x - y} = x^2 + xy + y^2 + x + y + \lambda$$

splits into two linear components if and only if $p \neq 3$ and $\lambda = \frac{1}{3}$. In this case

$$\frac{f_\lambda(x) - f_\lambda(y)}{x - y} = \left(x + \frac{1+\sqrt{-3}}{2}y + \frac{1}{2} + \frac{\sqrt{-3}}{6}\right) \cdot \left(x + \frac{1-\sqrt{-3}}{2}y + \frac{1}{2} - \frac{\sqrt{-3}}{6}\right)$$

and the two components are not defined over $\mathbb{F}_{p^t}$ if and only if -3 is a non-square in $\mathbb{F}_{p^t}$. From [4, Lemma 4.5], this is equivalent to require t odd and $p \equiv 2 \pmod 3$. Now assume that $s > 0$. Let $\mu \in \mathbb{F}_{p^t}$ with $\mu^{p^s} = \lambda$, so that $f(x) = x\left(x^2 + x + \mu\right)^{p^s}$. Let $b, b^{p^t} \in \mathbb{F}_{p^{2t}}$ be the zeros of $x^2 + x + \mu$; then, for any $x \in \mathbb{F}_{p^t}$,

$$f_\lambda(x) = x\,(x+b)^{p^s}\,(x+b^{p^t})^{p^s} = x\,(x+b)^{(p^t)^{2p^s-1}+(p^t)^{2p^s-2}+\cdots+p^t+1}.$$

Suppose that $f_\lambda(x)$ is a PP of $\mathbb{F}_{p^t}$; in particular, $b \notin \mathbb{F}_{p^t}$. Since $(\deg f_\lambda(x))^4 = d^4 < p^t$, $f_\lambda(x)$ is an exceptional polynomial over $\mathbb{F}_{p^t}$ from [10, Theorem 8.4.19]. Also, from [1, Proposition 2.4], $f_\lambda(x)$ is indecomposable as exceptional polynomial over $\mathbb{F}_{p^t}$. Hence, from [10, Theorem 8.4.11], $\deg f_\lambda(x) = 2p^s + 1$ is a prime not dividing $p^t - 1$. From the Niederreiter–Robinson criterion [11, Lemma 1], the polynomial $x^{\frac{(p^t)^{2p^s}-1}{p^t-1}+1} + bx$ is a PP of $\mathbb{F}_{(p^t)^{2p^s}}$; equivalently, the monomial $b^{-1}x^{\frac{p^{2tp^s}-1}{p^t-1}+1}$ is a CPP of $\mathbb{F}_{p^{2tp^s}}$. Thus, from [1, Theorem 3.1], one of the following cases hold, where ζ is a primitive $(2p^s+1)$-th root of unity and $\alpha := \zeta + \zeta^{-1}$, $\beta := \zeta - \zeta^{-1}$:
  - p^t has order $2p^s$ modulo $2p^s + 1$ and $b = \zeta - 1$ up to multiplication by a non-zero element in $\mathbb{F}_{p^t}$. Since $b \in \mathbb{F}_{p^{2t}} \setminus \mathbb{F}_{p^t}$ and $2p^s + 1$ is prime, we have $(2p^s+1) \mid (p^t+1)$. Hence $p^t \equiv -1 \pmod{2p^s+1}$ has order $2 \neq 2p^s$ modulo $2p^s + 1$, a contradiction.
  - p^t has order $2p^s$ modulo $2p^s+1$ and $b = e(\alpha-1)\sqrt{\beta^2(e^2-4a)}$ up to multiplication by a non-zero element in $\mathbb{F}_{p^t}$, for some $e, a \in \mathbb{F}_{p^t}$, $a \neq 0$, such that $e^2 - 4a$ is a square in $\mathbb{F}_{p^t}$. Since $b \in \mathbb{F}_{p^{2t}} \setminus \mathbb{F}_{p^t}$ we have $\alpha \in \mathbb{F}_{p^t}$, which implies $\zeta^{p^t-1} = 1$ or $\zeta^{p^t+1} = 1$. As $2p^s + 1$ is prime and $b \notin \mathbb{F}_{p^t}$, this yields $(2p^s+1) \mid (p^t+1)$; hence, p^t has order 2 modulo $2p^s + 1$, a contradiction to $s > 0$.
  - p^t has order p^s modulo $2p^s+1$ and $b = e(\alpha-1)\sqrt{\beta^2(e^2-4a)}$ up to multiplication by a non-zero element in $\mathbb{F}_{p^t}$, for some $e, a \in \mathbb{F}_{p^t}$, $a \neq 0$, such that $e^2 - 4a$ is 0 or a non-square in $\mathbb{F}_{p^t}$. From $b \in \mathbb{F}_{p^{2t}} \setminus \mathbb{F}_{p^t}$ we have $\alpha \in \mathbb{F}_{p^t}$ which implies $\zeta^{p^t-1} = 1$ or $\zeta^{p^t+1} = 1$; hence, p^t has order 1 or 2 modulo $2p^s + 1$, a contradiction to $s > 0$.

  Therefore, $f_\lambda(x)$ is not a PP of $\mathbb{F}_{p^t}$.

- Case $r > 1$.
  Assume first $u \le s$, so that we can take $u = 0$ and $d = 2p^s + r$. Suppose by contradiction that $f_\lambda(x)$ is a PP of $\mathbb{F}_{p^t}$. As $(\deg f_\lambda(x))^4 < p^t$, $f_\lambda(x)$ is exceptional over $\mathbb{F}_{p^t}$, see [10, Theorem 8.4.19]. Note that $f_\lambda(x)$ has exactly three distinct zeros, one in $\mathbb{F}_{p^t}$ with multiplicity r and two in $\mathbb{F}_{p^{2t}} \setminus \mathbb{F}_{p^t}$ with multiplicity p^s.
  - Suppose that $f(x)$ is indecomposable as exceptional polynomial over $\mathbb{F}_{p^t}$. From [10, Theorem 8.4.10], one of the following cases holds.
    * $2p^s + r = p^w$ for some $w \ge 1$. In this case
      $$f(x) = \left(x^{p^{w-s}} + x^{p^{w-s}-1} + \lambda x^{p^{w-s}-2}\right)^{p^s};$$
      since $x \mapsto x^{p^s}$ is a permutation of $\mathbb{F}_{p^t}$, we can assume $s = 0$. Then
      $$\begin{aligned}\frac{f(x)-f(y)}{x-y} \\ &= (x-y)^{p^w-1} + x^{p^w-2} + x^{p^w-3}y + \cdots + y^{p^w-2} \\ &\quad + \lambda(x^{p^w-3} + x^{p^w-4}y + \cdots + y^{p^w-3}). \qquad (1)\end{aligned}$$
      Let $\mathcal{C}$ be the plane curve of degree $p^w - 1$ defined over $\mathbb{F}_{p^t}$ by affine equation $\frac{f(x)-f(y)}{x-y} = 0$. From Equation (1), $\mathcal{C}$ has a unique point at infinity P_∞. Moreover, $\mathcal{C}$ intersects the line $x = y$ at the affine points $(0, 0)$ and $(-2\lambda, -2\lambda)$ with multiplicity $p^w - 3$ and 1, respectively; hence, P_∞ is a simple point for $\mathcal{C}$. This implies that $\mathcal{C}$ is absolutely irreducible, a contradiction to the exceptionality of $f(x)$ (see [10, Theorem 8.4.4]).
    * $2p^s + r = \frac{p^a(p^a-1)}{2}$, with $p \in \{2, 3\}$ and $a > 1$ odd; this is not possible, since $p \nmid r$.
    * $2p^s + r$ is coprime with p. From [10, Theorem 8.4.11], one of the following holds:
      · $f_\lambda(x)$ is linear. This is not possible by the assumptions.
      · $f_\lambda(x) = x^{2p^s+r}$ where $2p^s + r$ is a prime not dividing $p^t - 1$, up to composition with linear functions. Then $f_\lambda(x)$ has either one or n distinct roots in $\overline{\mathbb{F}}_{p^t}$, a contradiction.
      · $f_\lambda(x) = \ell_1 \circ D_{2p^s+r}(\ell_2(x), a)$, where $2p^s + r$ is a prime not dividing $p^{2t} - 1$, $D_{2p^s+r}(x, a)$ is a Dickson polynomial with $a \ne 0$ of degree $2p^s + r$, and $\ell_1, \ell_2 \in \mathbb{F}_{p^t}[x]$ are linear permutations. If $(2p^s + r) \nmid (p^{2t} + 1)$, then $D_{2p^s+r}(x, a)$ is a PP of $\mathbb{F}_{p^{2t}}$; see [10, Theorem 8.4.11]. This is not possible, as $f_\lambda(x)$ has three distinct zeros in $\mathbb{F}_{p^{2t}}$. Thus, $(2p^s + r) \mid (p^{2t} + 1)$. Denote $\ell_1(x) = bx + c$. As ℓ_2 permutes $\mathbb{F}_{p^{2t}}$, the number of zeros of $f_\lambda(x)$ in $\mathbb{F}_{p^{2t}}$ is equal to the number Z of preimages of $-c/b$ under $D_{2p^s+r}(x, a)$; hence, $Z = 3$. On the other hand, from [8, Theorems 3.26 and 3.26′] we have $Z \in \{1, 2p^s + r, \frac{2p^s+r}{2}, \frac{2p^s+r+1}{2}\}$. Then $s = 0$ and $r = 3$, so that $f_\lambda(x) = x^5 + x^4 + \lambda x^3$ with $p \ne 5$. We have $D_5(x, a) = x^5 - 5ax^3 + 5a^2x$; by direct inspection, the polynomial $\ell_1 \circ D_5(\ell_2(x), a)$ cannot have the form $x^5 + x^4 + \lambda x^3$ for any ℓ_1, ℓ_2.

– Now suppose that $f_\lambda(x)$ is a decomposable exceptional polynomial over $\mathbb{F}_{p^t}$, say $f_\lambda(x) = h(k(x))$ for some exceptional polynomials $h, k \in \mathbb{F}_{p^t}[x]$ with $\deg(h), \deg(k) > 1$. The roots of $f_\lambda(x)/x^r$ are conjugated under the Frobenius map $x \mapsto x^{p^t}$; hence, the polynomial

$$\frac{f_\lambda(-x) - f_\lambda(0)}{(-x)^r} = \frac{h(k(-x)) - h(k(0))}{(-x)^r} = \frac{(k(-x) - k(0)) \prod_{i=1}^{\deg(h)-1}(k(-x) - \beta_i)}{(-x)^r}$$

is a power of a unique irreducible factor over $\mathbb{F}_{p^t}$.
Suppose that $k(-x) - k(0)$ has a monic absolutely irreducible factor different from x and defined over $\mathbb{F}_{p^t}$. Since the roots of $f_\lambda(x)/x^r$ are conjugated under $x \mapsto x^{p^t}$, we have $\beta_i = k(0)$ for all i. Hence, $\frac{f_\lambda(-x)-f_\lambda(0)}{(-x)^r} = \frac{(k(-x)-k(0))^{\deg(h)}}{(-x)^r}$. Also, $m \cdot \deg(h) = r$, where x^m is the maximum power of x which divides $k(-x) - k(0)$; in particular, $p \nmid \deg(h)$. On the other hand, $f_\lambda(x)$ has just two distinct non-zero roots (the ones of $x^2+x+\mu$ where $\mu^{p^s} = \lambda$) with multiplicity p^s; hence, $\deg(h) \mid p^s$. This is a contradiction, either to $p \nmid \deg(h)$ or to $\deg(h) > 1$.
Suppose that $k(-x) - k(0) = ax^m$, for some $a \in \mathbb{F}_{p^t}$ and $m > 1$ with $\gcd(m, p^t - 1) = 1$. If $p \mid m$, then $f_\lambda(x)$ is invariant under $x \mapsto \gamma x$ when $\gamma \in \mathbb{F}_p$; this is a contradiction to $\gcd(2p^s + r, p^s + r) = 1$. Then $p \nmid m$. Let $\bar{x}$ be a non-zero root of $f_\lambda(x)$; for any δ with $\delta^m = 1$, $k(\delta\bar{x}) = k(\bar{x})$ and $f_\lambda(\delta\bar{x}) = 0$. Thus, the number of distinct non-zero roots of $f_\lambda(x)$ is a multiple of m; hence, $m = 2$. This implies $p = 2$. Therefore $f_\lambda(x) = h(k(0) + ax^2) = h((\ell_0 + \ell_1 x)^2)$ with $\ell_0, \ell_1 \in \mathbb{F}_{p^t}$, so that the polynomial $h(x^2)$ is also exceptional of degree $\deg(f_\lambda)$. Since $\deg(h)$ is odd, this is not possible.

We have shown that $f_\lambda(x)$ is not a PP of $\mathbb{F}_{p^t}$ under the assumption $u \le s$. If $u > s$, then we can take $s = 0$ so that $d = r + 2$ and $f_\lambda(x) = x^r(x^2 + x + \lambda)$. The same arguments as in the case $u \le s$ still apply and show that $f_\lambda(x)$ is not a PP of $\mathbb{F}_{p^t}$.

Remark 2.1. Theorem 1.1 yields the characterization also of permutation trinomials of $\mathbb{F}_{p^t}$ of type $g_{\alpha,\beta}(x) = x^{2p^s+r} + \alpha x^{p^s+r} + \beta x^r$, under the assumptions $\alpha \neq 0$ and $d^4 < p^t$ (with d defined as in Theorem 1.1).

In fact, let $\gamma \in \mathbb{F}_{p^t}$ satisfy $\gamma^{p^s} = \alpha$. Then $g_{\alpha,\beta}(x)$ is a PP of $\mathbb{F}_{p^t}$ if and only if $\frac{1}{\gamma^{2p^s+r}} g(\gamma x) = f_{\beta/\alpha^2}(x)$ is a PP of $\mathbb{F}_{p^t}$. Thus, $g_{\alpha,\beta}(x)$ is a PP of $\mathbb{F}_{p^t}$ exactly in the following cases:

- $p = 2$, t is odd, and $g_{\alpha,\beta}(x) = x^3 + \alpha x^2 + \alpha^2 x$ or $g_{\alpha,\beta}(x) = x^5 + \alpha x^3 + \alpha^2 x$ for some $\alpha \in \mathbb{F}_{p^t}$;
- $p \equiv 2 \pmod 3$, t is odd, and $g_{\alpha,\beta}(x) = x^3 + \alpha x^2 + \frac{\alpha^2}{3} x$ for some $\alpha \in \mathbb{F}_{p^t}$.

References

[1] D. Bartoli, M. Giulietti, L. Quoos, G. Zini, Complete permutation polynomials from exceptional polynomials, J. Number Theory 176 (2017) 46–66.

[2] S. Bhattacharya, S. Sarkar, On some permutation binomials and trinomials over $\mathbb{F}_{2^n}$, Des. Codes Cryptogr. 82 (2017) 149–160.

[3] C. Ding, Q. Longjiang, Q. Wang, J. Yuan, P. Yuan, Permutation trinomials over finite fields with even characteristic, SIAM J. Discrete Math. 29 (1) (2015) 79–92.

[4] M. Giulietti, On plane arcs contained in cubic curves, Finite Fields Appl. 8 (2002) 69–90.

[5] X.-D. Hou, Determination of a type of permutation trinomials over finite fields. II, Finite Fields Appl. 35 (2015) 16–35.

[6] X.-D. Hou, Permutation polynomials over finite fields: a survey of recent advances, Finite Fields Appl. 32 (2015) 82–119.

[7] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (1) (2007) 58–70.

[8] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Pitman Monogr. Surv. Pure Appl. Math., vol. 65, 1993.

[9] G.L. Mullen, H. Niederreiter, Dickson polynomials over finite fields and complete mappings, Can. Math. Bull. 30 (1) (1987) 19–27.

[10] G.L. Mullen, D. Panario, Handbook of Finite Fields, Chapman and Hall, 2013.

[11] H. Niederreiter, K.H. Robinson, Complete mappings of finite fields, J. Aust. Math. Soc. Ser. A 33 (1982) 197–212.

[12] P. Stanica, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, Investigations on bent and negabent functions via the nega-Hadamard transform, IEEE Trans. Inf. Theory 58 (6) (2012) 4064–4072.