archives-ouvertes.fr

On one class of permutation polynomials over finite fields of characteristic two *

Leonid Bassalygo, Victor A. Zinoviev

To cite this version:

Leonid Bassalygo, Victor A. Zinoviev. On one class of permutation polynomials over finite fields of characteristic two *. Pascale Charpin, Nicolas Sendrier, Jean-Pierre Tillich. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Apr 2015, Paris, France. 2016, Proceedings of the 9th International Workshop on Coding and Cryptography 2015 WCC2015. <hal-01275768>

HAL Id: hal-01275768
https://hal.inria.fr/hal-01275768

Submitted on 18 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On one class of permutation polynomials over finite fields of characteristic two *

Leonid A. Bassalygo and Victor A. Zinoviev

Kharkevich Institute for Information Transmission Problems,
Russian Academy of Sciences,
Bol'shoi Karetnyi per. 19, GSP-4,
Moscow, 127994, Russia
bass@iitp.ru, zinov@iitp.ru

Abstract. Polynomials of type $x^{q^3+q^2+q+2}+bx$ over the field $\mathbb{F}_{q^4}$, where $q = 2^m$, $m \geq 2$, are considered. All cases when these polynomials are permutation polynomials are classified.

1 Introduction

Let $q = p^m$ be a prime power and let $\mathbb{F}_q$ denote the finite field of order q. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if $f(x)$ induces a one-to-one mapping of $\mathbb{F}_q$ onto itself. It is well known that permutation polynomials have applications in a variety of areas, including such areas as cryptography for the secure transmission of information, and in combinatorics for the construction of various kinds of combinatorial designs (see [4, 6] and references there). Recently, permutation polynomials have been studied extensively in the literature (see [3, 7, 9, 12], for example).

A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a complete permutation polynomial (CPP), if both $f(x)$ and $f(x) + x$ are PP over $\mathbb{F}_q$. Although there are some results on CPP over $\mathbb{F}_q$ [3, 4, 6, 8, 10, 12], still very few classes of them are known, even for monomial functions. For a positive integer d and $a \in \mathbb{F}_q^*$, a monomial function ax^d is a CPP over $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$ and $ax^d + x$ is a PP over $\mathbb{F}_q$.

In [1, 2] we gave a complete description of PP of type

$$f(x) = x^{1+\frac{q^2-1}{q-1}} + bx$$

over $\mathbb{F}_{q^2}$ (or, monomial CPP of type $f(x) = ax^d$, $d = (q^2-1)/(q-1)+1$) and

$$f(x) = x^{1+\frac{q^3-1}{q-1}} + bx$$

* Supported in part by the Russian Foundation for Basic Research (project no. 15 - 01 - 08051).

over $\mathbb{F}_{q^3}$ (or, monomial CPP of type $f(x) = ax^d$, $d = (q^3-1)/(q-1)+1$) for the fields of any characterictic. Here we extend such description to polynomials of type

$$f(x) = x^{1+\frac{q^4-1}{q-1}} + bx, \tag{1}$$

over $\mathbb{F}_{q^4}$ (or, monomial CPP of type $f(x) = ax^d$, $d = (q^4-1)/(q-1)+1$) but only for the fields of even characteristic ($q = 2^m$).

For odd m, such polynomials were considered [12]. In particular, it was proved (on base of Dickson polynomials) the following result.

Theorem 1 [12] *Let $q = 2^m$ where $m \geq 3$ is odd. A polynomial of the type* (1) *is a PP over $\mathbb{F}_{q^4}$ if the element b looks as follows:*

$$\left.\begin{array}{lll} 1)\ b = u\,(1+\beta+\beta^2) & + v\,\beta^3; & \\ 2)\ b = u\,(1+\beta+\beta^3) & + v\,(\beta+\beta^2) & \\ \textit{or}\ b = u\,(1+\beta^3) & + v\,(1+\beta+\beta^2); & \\ 3)\ b = u\,(\beta+\beta^3) & + v\,(\beta^2+\beta^3), & \end{array}\right\} \tag{2}$$

where u, v run through $\mathbb{F}_q$, $(u,v) \neq (0,0)$, and where β is a root of x^4+x+1.

However, it was not proved that there do not exist other elements b for which polynomials $x^{1+\frac{q^4-1}{q-1}} + bx$ are also permutation polynomials. Here we fill this gap and prove, firstly, these sufficient conditions from [12] are also necessary; secondly, these sufficient and necessary conditions are fulfilled only for b from [12]; and, thirdly, permutation polynomials of the type (1) do not exist for the even $m \geq 4$ (for $m = 2$ such polynomials exist).

Our approach as well as in [1,2] is based on the following lemma from [8], which in our special case of $f(x) \in \mathbb{F}_{q^4}[x]$ can be reformulated as follows:

Lemma 1. *The polynomial*

$$f(x) = x^{1+\frac{q^4-1}{q-1}} + bx$$

over $\mathbb{F}_{q^4}$ is a permutation polynomial if and only if $b \in \mathbb{F}_q^4 \setminus \mathbb{F}_q$ and the following inequality:

$$x(b+x)^{q^3+q^2+q+1} \neq y(b+y)^{q^3+q^2+q+1} \tag{3}$$

holds for all $x, y \in \mathbb{F}_q$, such that $x \neq 0, y \neq 0, x \neq y$.

2 Polynomials $x^{1+\frac{q^4-1}{q-1}} + bx,\ q = 2^m,\ m \geq 2$

Following our approach in [1,2], first, we reduce the inequality (3) to the equation over x and y. Using that

$$\left.\begin{array}{r} x(b+x)^{q^3+q^2+q+1} + y(b+y)^{q^3+q^2+q+1} = \\ = z\left(x^4 + B_2x^2 + (z^3+B_2z)x + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4\right), \end{array}\right\} \tag{4}$$

where

$$\left.\begin{array}{l} B_1 = b + b^q + b^{q^2} + b^{q^3}, \\ B_2 = b^{1+q} + b^{1+q^2} + b^{1+q^3} + b^{q+q^2} + b^{q+q^3} + b^{q^2+q^3}, \\ B_3 = b^{1+q+q^2} + b^{1+q+q^3} + b^{1+q^2+q^3} + b^{q+q^2+q^3}, \\ B_4 = b^{1+q+q^2+q^3}. \end{array}\right\} \qquad (5)$$

and $z = x + y$, we can rewrite the lemma 1 as follows:

Lemma 2. *Let $q = 2^m$. The polynomial*

$$f(x) = x^{1+\frac{q^4-1}{q-1}} + bx,$$

over $\mathbb{F}_{q^4}$ is a permutation polynomial if and only if $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ and the equation

$$x^4 + B_2x^2 + (z^3 + B_2z)x + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4 = 0 \qquad (6)$$

has no solutions $x, z \in \mathbb{F}_q$ such that $z \neq 0$ (for $x = 0$ and $x = z$, i.e. $y = 0$, this equation has no solutions).

Using a new variable $w = x + B_1$, we obtain the equation

$$w^4 + B_2w^2 + (z^3 + zB_2)w + z^4 + B_2z^2 + Dz + E = 0, \qquad (7)$$

where we denote

$$D = B_1B_2 + B_3 \text{ and } E = B_1^4 + B_1^2B_2 + B_4. \qquad (8)$$

Introducing again a new variable $\gamma = w/z$ we arrive to the equivalent equation (recall that $z \neq 0$):

$$\gamma^4 + \gamma + \frac{B_2}{z^2} \cdot (\gamma^2 + \gamma + 1) + 1 + \frac{D}{z^3} + \frac{E}{z^4} = 0. \qquad (9)$$

Thus, we reduced the problem of solution of equation (6) to the problem of solution of equation (9) with $z \neq 0$. For convenience we denote, for an integer $s \geq 1$ and $q = 2^m$, the trace function

$$\mathrm{Tr}_{q^s}(a) = a + a^2 + a^4 + \cdots + a^{2^{sm-1}}, \;\; a \in \mathbb{F}_{q^s}$$

and the relative trace function for integers $s, r \geq 1$

$$\mathrm{Tr}_{q^{sr} \to q^s}(a) = a + a^{q^s} + a^{q^{2s}} + \cdots + a^{q^{s(r-1)}}, \;\; a \in \mathbb{F}_{q^{sr}}$$

The cases $B_2 \neq 0$ and $B_2 = 0$ we consider separately.

2.1 The case $B_2 \neq 0$.

Because

$$\gamma^4 + \gamma + \frac{B_2}{z^2} \cdot (\gamma^2 + \gamma + 1) + 1 + \frac{D}{z^3} + \frac{E}{z^4}$$
$$= (\gamma^2 + \gamma + 1)^2 + (\gamma^2 + \gamma + 1)(1 + \frac{B_2}{z^2}) + 1 + \frac{D}{z^3} + \frac{E}{z^4}, \tag{10}$$

in this case the problem of existence of a solution of the equation (9) is reduced to the existence of solutions of the two following equations:

$$\xi^2 + \xi\ (1 + \frac{B_2}{z^2}) + 1 + \frac{D}{z^3} + \frac{E}{z^4} = 0. \tag{11}$$

and

$$\gamma^2 + \gamma + 1 = \xi. \tag{12}$$

When $z \neq \sqrt{B_2}$ the equation (11) has a solution if and only if

$$\mathrm{Tr}_q \left(\frac{1 + \frac{D}{z^3} + \frac{E}{z^4}}{(1 + \frac{B_2}{z^2})^2} \right) = \mathrm{Tr}_q(1 + Cv + Dv^3) = 0.$$

where

$$C^4 = D\sqrt{B_2} + E + B_2^2 \ \text{ and } \ v = \frac{1}{z + \sqrt{B_2}}.$$

The subcase $(C, D) = (0, 0)$**.**
In this subcase the equation (11) looks as follows:

$$\xi^2 + \xi\ \left(1 + \frac{B_2}{z^2}\right) + \left(1 + \frac{B_2}{z^2}\right)^2 = 0. \tag{13}$$

Here we have

Proposition 2 *Let $q = 2^m$ and $m \geq 3$ be odd. Let $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$, $B_2 \neq 0$, and the following two conditions be satisfied:*

$$B_3 = B_1 B_2, \tag{14}$$

$$B_4 = B_1^4 + B_1^2 B_2 + B_2^2. \tag{15}$$

Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial over $\mathbb{F}_{q^4}$.

If $D = 0$ and $E = B_2^2$, then for even m the equation (11) has solutions for all z, $z \neq 0$, including $z = \sqrt{B_2}$ and, obviously, in this case there exist many solutions of the equation (12). Therefore, we have the following

Proposition 3 *Let $q = 2^m$ and $m \geq 2$ be even. Let $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$, $B_2 \neq 0$, and the conditions* (14) *and* (15) *be satisfied. Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is not a permutation polynomial over $\mathbb{F}_{q^4}$.*

The subcase $(C, D) \neq (0, 0)$**.**

For this subcase we are going to prove that for all $m \geq 6$ solutions for the both equations (11) and (12) always exist. For this purpose it is enough to prove the existence of $v \neq 0$ and $v \neq \frac{1}{\sqrt{B_2}}$, such that

$$\mathrm{Tr}_q(1 + Cv + Dv^3) = 0 \tag{16}$$

and

$$\mathrm{Tr}_q\left(1 + \frac{B_2}{z^2}\right) = 1. \tag{17}$$

Hence we obtain

Proposition 4 *Let $q = 2^m$, $B_2 \neq 0$ and $(C, D) \neq (0, 0)$. Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is not a permutation polynomial over $\mathbb{F}_{q^4}$ for all $m \geq 6$.*

2.2 The case $B_2 = 0$

The subcase $D \neq 0$**.**

Set $u = \frac{1}{z}$. The number N of $\mathbb{F}_q$-rational points of the plane absolutely irreducible non-singular curve P over $\mathbb{F}_q$,

$$P = \{(\gamma, u) : \ \gamma^4 + \gamma + 1 + Du^3 + Eu^4 = 0\},$$

satisfies the following known (see [11]) inequality: $N \geq q - 6\sqrt{q}$. Because the number of points with $u = 0$ does not exceed 4, when $q - 6\sqrt{q} > 4$ there exists a solution $\gamma, z \in \mathbb{F}_q$, $z \neq 0$, of the equation (9). For this case, the following proposition holds.

Proposition 5 *Let $q = 2^m$, $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ and*

$$B_2 = 0, \ \ B_3 \neq 0.$$

Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is not a permutation polynomial over $\mathbb{F}_{q^4}$ for $m \geq 6$.

The subcase $D = 0$**.**

Here we are obliged to consider separately odd and even m. For odd m the analysis is simple: if $E \neq 0$, the equation (9) has a solution for any γ because z^4 is an automorphism of the field F_{2^m} and $\gamma^4 + \gamma + 1 \neq 0$ for odd m and $\gamma \in \mathbb{F}_{2^m}$. If $E = 0$, then a solution of (9) does not exist. But the conditions $B_2 = 0, D = 0, E = 0$ represent a special case of the conditions (14) and (15) and so the following proposition holds.

Proposition 6 *Let $q = 2^m$ and $m \geq 3$ be odd. Let $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ and*

$$B_2 = 0, \ \ B_3 = 0.$$

Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial over $\mathbb{F}_{q^4}$ if and only if $B_4 = B_1^4$.

For even m the situation is more complicated since the equation (9), for the case $E = 0$, has no solutions in $\mathbb{F}_{2^m}$ when $m \equiv 2 \pmod 4$. Hence for $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$, such that $B_2 = 0$, $B_3 = 0$, and $B_4 = B_1^4$, the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial over $\mathbb{F}_{q^4}$ for $m \equiv 2 \pmod 4$. But it turned out to be that such b does not exist for even m (for odd m such b exists).

Lemma 3. *Let $b \in \mathbb{F}_{q^4}$ where $q = 2^m$ and let B_2 and B_3 be the expressions* (5) *obtained from b. Then, for even m,*

$$B_2 = B_3 = 0$$

if and only if b is an element of $\mathbb{F}_q$.

3 The main results

Now we give the results for the cases $m = 2, 3, 4, 5$.

The direct calculations show that for $m = 4$ there are no permutation polynomials of the type $x^{1+\frac{q^4-1}{q-1}} + bx$ over $\mathbb{F}_{q^4}$, $q = 2^4$. But for $m = 2$ there are 48 such polynomials (for $b = \alpha^i, i = 3, 11, 37, 61, 63, 91$, and their cyclotomic classes $L_i = \{i, 2i, 2^2 i, \ldots, 2^8 i\}$ modulo 255 where α is a primitive element of $\mathbb{F}_{4^4}$).

From here, Proposions 3, 4, 5, and Lemma 3 the following theorem is valid.

Theorem 7 *Let $q = 2^m$ and $m \geq 4$ be even. The polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ over $\mathbb{F}_{q^4}$ is not a permutation polynomial for any $b \in \mathbb{F}_{q^4}^*$.*

For $m = 3$ and $m = 5$ the direct calculations show that the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial over $\mathbb{F}_{q^4}$ if and only if the conditions of Proposition 3 are satisfied. From here and Proposions 2, 4, 5, and 6 the following theorem is valid.

Theorem 8 *Let $q = 2^m$ and $m \geq 3$ be odd. The polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ over $\mathbb{F}_{q^4}$ is a permutation polynomial if and only if the following conditions are satisfied:*

$$b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q, \;\; B_3 + B_1 B_2 = 0, \quad \textit{and} \;\; B_4 + B_1^4 + B_1^2 B_2 + B_2^2 = 0.$$

As we mentioned already, in [12] it was proved in a different way that conditions from Theorem 8 are sufficient conditions.

Now, for odd m, we show that we find all solutions for b when the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial. Present any element x of $\mathbb{F}_{q^4}$ as a polynomial of degree 3 over $\mathbb{F}_q$:

$$x = x_0 + x_1\beta + x_2\beta^2 + x_3\beta^3, \;\; x_i \in \mathbb{F}_q,$$

where β is a primitive element of $\mathbb{F}_{2^4}$, i.e. it is a root of the equation $1+\beta+\beta^4=0$. Now express B_1, B_2, B_3, B_4 in terms of x_i (since they are elements of $\mathbb{F}_q$):

$$\begin{aligned}
B_1 &= x_3,\\
B_2 &= x_0x_3 + x_1x_2 + x_3^2,\\
B_3 &= x_0^2x_3 + x_1^3 + x_1x_2x_3 + x_1x_3^2 + x_2^3 + x_2^2x_3 + x_3^3,\\
B_4 &= x_0^4 + x_0^3x_3 + x_0^2x_1x_2 + x_0^2x_3^2 + x_0x_1^3 + x_0x_1x_2x_3 + x_0x_1x_3^2 + x_0x_2^3 +\\
&+ x_0x_2^2x_3 + x_0x_3^3 + x_1^4 + x_1^2x_2x_3 + x_1x_2^3 + x_1x_3^3 + x_2^4 + x_2x_3^3 + x_3^4.
\end{aligned}$$

Using these expressions we obtain:
the condition $B_1B_2 = B_3$ is equivalent to the condition:

$$x_0x_3(x_0+x_3) + x_1(x_1+x_3)^2 + x_2^2(x_2+x_3) = 0 \tag{18}$$

and the condition $B_4 = B_1^4 + B_1^2B_2 + B_2^2$ is equivalent to the condition

$$\left.\begin{aligned}
x_0^4 + x_0^3x_3 + x_0^2x_1x_2 + x_0x_1^3 + x_0x_2^3 + x_0x_2^2x_3 + x_0x_1x_3^2 +\\
+ x_0x_1x_2x_3 + x_1^4 + x_1^2x_2^2 + x_1^2x_2x_3 + x_1x_2x_3^2 + x_1x_3^3 + x_2^4 + x_2x_3^3 = 0
\end{aligned}\right\} \tag{19}$$

Theorem 9 *All solutions of the system of two equations* (18) *and* (19) *for odd m are:*

$$\begin{array}{llll}
(x_0 = x_2, & x_1 = x_2, & x_2, & x_3),\\
(x_0 = x_2 + x_3, & x_1 = x_2, & x_2, & x_3),\\
(x_0 = 0, & x_1 = x_2 + x_3, & x_2, & x_3),\\
(x_0 = x_3, & x_1 = x_2 + x_3, & x_2, & x_3),
\end{array}$$

where x_2, x_3 run over $\mathbb{F}_q$ and $(x_2, x_3) \neq (0, 0)$.

Just these solutions were given in [12], but it was not proved there that the other solutions do not exist. Thus, here we filled this gap. In the same paper [12] the authors counted also the number of their different solution: $2(2q+1)(q-1)$, that naturally coincides with the sum of the number of solutions for $x_3 \neq 0$ equal $4q(q-1)$, and for $x_3 = 0$ equal $2(q-1)$.

References

1. L.A. Bassalygo, V.A. Zinoviev, On complete permutation polynomials, In: "Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory", September 7 -13, 2014, Svetlogorsk (Kaliningad region), Russia, Proceedings, 57 - 62.
2. L.A. Bassalygo, V.A. Zinoviev, Permutation and complete permutation polynomials, Finite Fields Appl. 33 (2015) 198-211.
3. P. Charpin, G.M. Kyureghyan, Cubic monomial bent functions: a subclass of $\mathcal{M}^*$, SIAM J. Discrete Math. 22 (2) (2008), 650-665.
4. X. Hou, Permutation polynomials over finite fields – A survey of recent advances, Finite Fields Appl. 32 (2015) 82-119.
5. R. Lidl, H. Niederreiter, Finite Fields. Encyclopedia of Mathematics and Its Applications. V. 20. Addison-Wesley Publishing Company. London. 1983.

6. G. L. Mullen, Q. Wang, Permutation polynomials: one variable, in "Handbook of Finite Fields", Eds. G. L. Mullen, D. Panario, Chapman and Hall/CRC, 2013.
7. A. Muratovic-Ribic, E. Pasalic, A note on complete polynomials over finite fields and their applications in cryptography, Finite Fields Appl. 25 (2014) 306-315.
8. H. Niederreiter, K.H. Robinson, Complete mappings of finite fields, J. Austral. Math. Soc. (Series A) 33 (1982), 197-212.
9. S. Sarkar, S. Bhattacharya, A. Cesmelioglu, On Some Permutation Binomials of the Form $x^{(2^n-1)/k+1}+ax$ over $\mathbb{F}_{2^n}$: Existence and Count. International Workshop on the Arithmetic of Finite Fields, WAIFI 2012, Springer LNCS 7369, (2012) 236-246. 2012.
10. Z. Tu, X. Zeng, L. Hu, Several classes of complete permutation polynomials. Finite Fields Appl. 25 (2014), 182-193.
11. S.G. Vladüt, D.Yu. Nogin, M.A. Tsfasman, Algebraic-geometric codes, Moscow, Independent Moscow University, 2003.
12. G. Wu, N. Li, T. Helleseth, Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, Finite Fields Appl. 28 (2014) 148-165.