Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 57–62*

On complete permutation polynomials [1]

L. A. Bassalygo bass@iitp.ru
V. A. Zinoviev zinov@iitp.ru
A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

Abstract. All cases when the polynomials of type $x^{q+2}+bx$ over the field $\mathbb{F}_{q^2}$ and $x^{q^2+q+2}+bx$ over $\mathbb{F}_{q^3}$ ($q=p^m>2$ is a power of a prime p) are permutation polynomials are classified. Therefore all cases when the polynomials x^{q+2} over $\mathbb{F}_{q^2}$ and x^{q^2+q+2} over $\mathbb{F}_{q^3}$ are complete permutation polynomials are enumerated.

1 Introduction

In the recent times the interest to the special case of the permutation polynomials – complete permutation polynomials – has appeared again. A polynomial $f(x)$ over a finite field $\mathbb{F}_q$ of order q is called a *complete permutation*, if it is a permutation polynomial and there exists an element $b\in\mathbb{F}_q^*$, such that $f(x)+bx$ has also this property. In [1] the following necessary and sufficient conditions for the polynomial

$$f(x)=x^{1+\frac{q-1}{n}}+bx,\quad n|(q-1),\quad n>1,$$

to be a permutation polynomial are given:
the element b is such that $(-b)^n\neq 1$ and the following inequality holds

$$((b+\omega^i)(b+\omega^j)^{-1})^{\frac{q-1}{n}}\neq\omega^{j-i}\tag{1}$$

for all i,j, such that $0\le i<j<n$, where ω is the fixed primitive root of the nth degree of 1 in the field $\mathbb{F}_q$. Here we use the result of [1] for certain special cases of $\mathbb{F}_q$ and the integer n. We assume that $q=p^m$, where p is the field characteristic and $p^m>2$.

2 The case of polynomial $x^{q+2}+bx$

Consider the field $\mathbb{F}_{q^2}$ and set $n=q-1$. Then the condition $(-b)^n\neq 1$ implies that $b\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. Set $x=\omega^i$ and $y=\omega^j$, then the inequality (1), changes into the following one:

$$x(b+x)^{q+1}\neq y(b+y)^{q+1},$$

[1] This work has been partially supported by the Russian fund of fundamental researches (under the project No. 12 - 01 - 00905).

for all $x, y \in \mathbb{F}_q$, such that $x \neq 0, y \neq 0, x \neq y$. Thus the polynomial $x^{q+2} + bx$ is a permutation if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and the equation over $\mathbb{F}_q$

$$x(b^q + x)(b + x) - y(b^q + y)(b + y) = 0$$

has no solutions $x, y \in \mathbb{F}_q,\ x \neq 0,\ y \neq 0,\ x \neq y$. Since

$$x(b^q+x)(b+x)-y(b^q+y)(b+y) = (x-y)((x+y)^2+(x+y)(b+b^q)+b^{q+1}-xy),$$

this condition turns into the following

Proposition 1. *The polynomial $x^{q+2} + bx$ is a permutation over the field $\mathbb{F}_{q^2}$ if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and the equation*

$$(x + y)^2 + (x + y)(b + b^q) + b^{q+1} - xy = 0, \tag{2}$$

has no solutions $x, y \in \mathbb{F}_q, x \neq 0, y \neq 0, x \neq y$.

2.1 Fields of even characteristic

Let $q = 2^m, m > 1$. In (2) set $x + y = z, xy = u$. This system is equivalent to the quadratic equation $x^2+xz+u = 0$, where $u = z^2+z(b+b^q)+b^{q+1}$ is defined by the relation (2). Note that the conditions $x, y \in \mathbb{F}_q,\ x \neq 0,\ y \neq 0,\ x \neq y$, are equivalent to the condition $z \neq 0$. Therefore from Proposition 1 we obtain

Proposition 2. *Let $q = 2^m, m > 1$. The polynomial $x^{q+2} + bx$ is a permutation over the field F_{q^2} if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and the equation*

$$x^2 + xz + z^2 + z(b + b^q) + b^{q+1} = 0 \tag{3}$$

has no solutions in the field $\mathbb{F}_q$ for all $z \in \mathbb{F}_q^*$.

Proposition 2 allows to solve the permutability problem for the polynomial $x^{q+2} + bx$ over $\mathbb{F}_{q^2}$. Although it was already solved in [2], our approach essentially differs from the one used in [2], and so we describe our approach here.

Theorem 1 (see also [2].) *Let $q = 2^m, m > 1$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over $\mathbb{F}_{q^2}$, if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, the number m is odd and $b^{3(q-1)} = 1$. The number of such different elements b is equal to $2(q-1)$, all these elements can be written in the following form:*

$$b = \alpha^{(q+1)(3t+1)/3} \ \text{ or } \ b = \alpha^{(q+1)(3t+2)/3},\ \ t = 0, 1, \ldots, 2^m - 2,$$

where α is a primitive element of the field $\mathbb{F}_{q^2}$.

Corollary 1. *Let $q = 2^m$, where $m > 1$. The polynomial x^{q+2} is a complete permutation polynomial over the field $\mathbb{F}_{q^2}$, if and only if the number m is odd.*

2.2 Fields of odd characteristic

Let $q = p^m$, where $p \geq 3$. Since for this case $4xy = (x+y)^2 - (x-y)^2$, the equation (2) is equivalent to

$$3(x+y)^2 + 4(x+y)(b+b^q) + 4b^{q+1} + (x-y)^2 = 0.$$

After changing the variables $x+y = z$ and $x-y = u$, Proposition 1 turns into

Proposition 3. *Let $q = p^m$ and $p \geq 3$. The polynomial $x^{q+2} + bx$ is a permutation over the field $\mathbb{F}_{q^2}$ if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and the equation*

$$3z^2 + 4z(b+b^q) + 4b^{q+1} + u^2 = 0 \tag{4}$$

has no solutions $u, z \in \mathbb{F}_q, u \neq 0$.

In the case, when the field characteristic of $\mathbb{F}_q$ equals 3, we obtain

Theorem 2. *Let $q = 3^m$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over the field $\mathbb{F}_{q^2}$, if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $b^{q-1} = -1$. The number of such different elements b equals $q-1$, and all these elements can be presented in the following form:*

$$b = \alpha^{\frac{q+1}{2}(2t+1)}, \quad t = 0, 1, \ldots, q-2,$$

where α is a primitive element of the field $\mathbb{F}_{q^2}$.

Corollary 2. *Let $q = 3^m$. The polynomial x^{q+2} is a complete permutation polynomial over the field $\mathbb{F}_{q^2}$.*

For the case $p > 3$, solving the quadratic equation (4) over z, Proposition 3 can be equivalently replaced by

Proposition 4. *Let $q = p^m$ and $p > 3$. The polynomial $x^{q+2} + bx$ is a permutation over $\mathbb{F}_{q^2}$, if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and the equation*

$$4b^2 - 4b^{q+1} + 4b^{2q} - 3u^2 = v^2 \tag{5}$$

has no solutions $u, v \in \mathbb{F}_q,\ u \neq 0$.

If $4b^2 - 4b^{q+1} + 4b^{2q} \neq 0$, then (5) has always a solution $u, v \in \mathbb{F}_q,\ u \neq 0$, since the number of solutions of the equation $3u^2 + v^2 = a \neq 0$ in the field $\mathbb{F}_q$ is not less than $q-1$ (see [5, Lemma 6.24]), and the number of solutions which have $u = 0$ is not greater than two. If $4b^2 - 4b^{q+1} + 4b^{2q} = 0$, then the equation (5) has a solution $u, v \in \mathbb{F}_q,\ u \neq 0$, if and only if the quadratic equation $w^2 + 3 = 0$ has a solution in the field $\mathbb{F}_q$.

Theorem 3. *Let $q = p^m$ and $p > 3$. The polynomial $x^{q+2} + bx$ is a permutation over $\mathbb{F}_{q^2}$, if and only if $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $1 - b^{q-1} + b^{2(q-1)} = 0$ and the equation $w^2 + 3 = 0$ has no solution in $\mathbb{F}_q$.*

Clearly the equation $1 - b^{q-1} + b^{2(q-1)} = 0$ has a solution, if and only if 3 divides $q+1$. The number of solutions $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ equals $2(q-1)$ and all these elements are of the form

$$b = \alpha^{\frac{q+1}{6}(6t+1)} \text{ and } b = \alpha^{\frac{q+1}{6}(6t+5)}, \ \ t = 0, 1, \dots, q-2, \tag{6}$$

where α is a primitive element of $\mathbb{F}_{q^2}$.

Further, a prime number $p > 3$ is of the form $p = 6k \pm 1$. It is known (see [6, Ch. 5]), that the equation $w^2 + 3 = 0$ has a solution in $\mathbb{F}_p$, if and only if $p = 6k + 1$. Hence when m is odd and $p = 6k + 1$ the equation $w^2 + 3 = 0$ has a solution in $\mathbb{F}_q$, but when m is odd and $p = 6k - 1$ has no solution in $\mathbb{F}_q$. For the even m and $p > 3$ the equation $w^2 + 3 = 0$ has a solution in $\mathbb{F}_q$, since when $m = 2k$ the equation $w^2 + c = 0$, for $c \in F_{p^k}$, has always a solution in the quadratic extension $\mathbb{F}_{p^{2k}}$.

Theorem 4. *Let $q = p^m$, and $p > 3$. The polynomial $x^{q+2} + bx$ is a permutation over the field $\mathbb{F}_{q^2}$, if and only if $p = 6k - 1$, m is odd and b satisfies (6).*

Corollary 3. *Let $q = p^m$, and $p > 3$. The polynomial x^{q+2} is a complete permutation polynomial over $\mathbb{F}_{q^2}$, if and only if $p = 6k - 1$ and m is odd.*

3 The case of polynomial $x^{q^2+q+2} + bx$

Proposition 5. *The polynomial $x^{q^2+q+2} + bx$ is a permutation over the field $\mathbb{F}_{q^3}$, if and only if $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and the equation*

$$(x+y)^3 - 2(x+y)xy + ((x+y)^2 - xy)B_1 + (x+y)B_2 + B_3 = 0, \tag{7}$$

has no solution $x, y \in \mathbb{F}_q, x \neq 0, y \neq 0, x \neq y$, where

$$B_1 = b^{q^2} + b^q + b, \ \ B_2 = b^{q+1} + b^{q^2+1} + b^{q^2+q}, \ \ B_3 = b^{q^2+q+1}.$$

3.1 Fields of even characteristic

Let $q = 2^m$, and $m > 1$. Set $x + y = z$, $xy = u$. This system is equivalent to the quadratic equation $x^2 + xz + u = 0$, where u is defined from the expression

$$uB_1 = z^3 + z^2 B_1 + zB_2 + B_3, \tag{8}$$

which follows from (7). Note that the conditions $x, y \in \mathbb{F}_q, \ x \neq 0, \ y \neq 0, \ x \neq y$, are equivalent to the condition $z \neq 0$. By the same argument, when $B_1 = 0$ the equation $x^2 + xz + u = 0$ has no solution in $\mathbb{F}_q$ for any $u \in \mathbb{F}_q, \ u \neq 0$, since in this case $z \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. Therefore, the polynomial $x^{q^2+q+2} + bx$ is a permutation over F_{q^3}, if $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $B_1 = b + b^q + b^{q^2} = 0$.

However, if $B_1 \neq 0$, then the polynomial $x^{q^2+q+2} + bx$ is a permutation over $\mathbb{F}_{q^3}$, if and only if $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and the equation over x

$$x^2 + xz + u = x^2 + xz + \frac{z^3 + z^2 B_1 + zB_2 + B_3}{B_1} = 0, \tag{9}$$

has no solution in $\mathbb{F}_q$ for any $z \in \mathbb{F}_q^*$. It can be shown, that there exists $z \in \mathbb{F}_q^*$, such that (9) has a solution in $\mathbb{F}_q$.

Using that B_1 is the relative trace function form $\mathbb{F}_{q^3}$ into $\mathbb{F}_q$, i.e.

$B_1 = Tr_{q^3 \to q}(b) = b + b^q + b^{q^2}$, we conclude, that the number of different elements $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ for which $B_1 = 0$ equals $q^2 - 1$.

Theorem 5. *Let $q = 2^m$ and $m > 1$. The polynomial $x^{q^2+q+2} + bx$ is a permutation over the field $\mathbb{F}_{q^3}$ if and only if $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $b + b^q + b^{q^2} = 0$. The number of such different elements b equals $q^2 - 1$.*

Remark. Theorem 5 gives the exhaustive answer to the question on permutability of the polynomial $x^{q^2+q+2} + bx$ over $\mathbb{F}_{q^3}$, $q = 2^m, m > 1$. In [3,4] a partial answer was obtained: for the case $m \not\equiv 0 \pmod 9$ the elements $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ were given for which the polynomial $x^{q^2+q+2} + bx$ is a permutation. However, it was not stated that other such elements did not exist.

Corollary 5. *Let $q = 2^m$ and $m > 1$. Then the polynomial x^{q^2+q+2} is a complete permutation polynomial over the field $\mathbb{F}_{q^3}$.*

3.2 Fields of odd characteristic

Proposition 6. *Let $q = p^m$, and $p \geq 3$. The polynomial $x^{q^2+q+2} + bx$ is a permutation over the field $\mathbb{F}_{q^3}$, if and only if $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and the equation*

$$(x-y)^2(2(x+y) + B_1) + 2(x+y)^3 + 3(x+y)^2 B_1 + 4(x+y)B_2 + 4B_3 = 0$$

has no solution $x, y \in \mathbb{F}_q$, $x \neq 0$, $y \neq 0$, $x \neq y$.

Set $x + y = z$ and $x - y = u$. Then the equation

$$(x-y)^2(2(x+y) + B_1) + 2(x+y)^3 + 3(x+y)^2 B_1 + 4(x+y)B_2 + 4B_3 = 0$$

is equivalent to

$$u^2(2z + B_1) + 2z^3 + 3z^2 B_1 + 4zB_2 + 4B_3 = 0.$$

Proposition 7. *Let $q = p^m$, and $p \geq 3$. The polynomial $x^{q^2+q+2} + bx$ is a permutation over the field $\mathbb{F}_{q^3}$, if and only if $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and the equation*

$$u^2(2z + B_1) + 2z^3 + 3z^2 B_1 + 4zB_2 + 4B_3 = 0 \tag{10}$$

has no solution $u \in \mathbb{F}_q^*,\ z \in \mathbb{F}_q$.

Since for the case $z = -B_1/2$, the equation above reduces to the condition

$$B_1^3 - 4B_1B_2 + 8B_3 = 0, \tag{11}$$

for the element b, the polynomial $x^{q^2+q+2} + bx$ is not permutation over $\mathbb{F}_{q^3}$, if the element b satisfies (11), because for any $u \in \mathbb{F}_q^*$ the equation (11) has the solution $z = -B_1/2$.

Now let $B_1^3 - 4B_1B_2 + 8B_3 \neq 0$ and, therefore, $z \neq -B_1/2$. Then after several changing of variables we arrive to the result.

Proposition 8. *Let* $q = p^m,\ \ p \geq 3$. *The polynomial* $x^{q^2+q+2} + bx$ *is a permutation over* $\mathbb{F}_{q^3}$*, if and only if* $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q,\ \ D \neq 0$ *and the equation*

$$Y^2 = X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4} \tag{12}$$

has no solutions $Y, X \in \mathbb{F}_q^*$.

Since by the Hasse Theorem (see, for example, [7, Ch. 3.3.3]) the number of solutions of this equation in the field $\mathbb{F}_q$ is not less than $q + 1 - 2\sqrt{q}$, and the number of solutions, when $X = 0$, or $Y = 0$, does not exceed 5, then the equation (12) has a solution $Y \neq 0, X \neq 0$ under the condition that $q + 1 - 2\sqrt{q} - 5 \geq 1$. Therefore, for the case $q \geq 11$ the permutation polynomials over $\mathbb{F}_{q^3}$ of type $x^{q^2+q+2} + bx$ do not exist.

It remains to consider only the cases $q = 3, 5, 7, 9$. It is easy to check, that for $q = 5$ and $q = 9$ there exists a solution $Y \neq 0, X \neq 0$ and, consequently, the permutation polynomials over $\mathbb{F}_{q^3}$ of type $x^{q^2+q+2} + bx$ also do not exist. For $q = 3, 7$, such permutation polynomials exist and they can be easily enumerated.

Theorem 6. *Let* $q = p^m$*, and* $p \geq 3$. *The polynomial* x^{q^2+q+2} *is a complete permutation polynomial over the field* $\mathbb{F}_{q^3}$*, if and only if* $q = 3$ *or* $q = 7$.

References.

1. *Niederreiter H., Robinson K.H.* Complete mappings of finite fields// J. Austral. Math. Soc. (Series A). 1982. V. 33. P. 197-212.
2. *Charpin P., Kyureghyan G. M.* Cubic monomial bent functions: a subclass of $\mathcal{M}^*$// SIAM J. Discrete Math. 2003. V. 22. N° 2. P. 650-665.
3. *Wu G., Li N., Helleseth T., Zhang Y.* Some classes of monomial complete permutation polynomials over finite fields of characteristic two// Finite Fields Appl. 2014, to appear.
4. *Tu Z., Zeng X., Hu L.* Several calsses of complete permutation polynomials. Finite Fields Appl. 2014. V. 25. N° 2. P. 182-193.
5. *Lidl R., Niederreiter H.* Finite Fields. Encyclopedia of Mathematics and Its Applications. V. 20. Addison-Wesley Publishng Company. London. 1983.
6. *Vinogradov I.M.* Basics of number theory. VIII Publishing. Moscow: Nauka. 1972.
7. *Vladüt S.G., Nogin D. Yu., Tsfasman M.A.* Algebraic-geometric Codes. Moscow, Independent Moscow University. 2003.