On complete permutation polynomials

Leonid Bassalygo, Victor Zinoviev

Harkevich Institute for Problems of Information Transmission, Moscow, Russia

International Workshop:
Algebraic and Combinatorial Coding Theory (ACCT-2014).
Svetlogorsk, Russia, September 7-13, 2014

Outline

Introduction

In the recent times the interest to the special case of the permutation polynomials – complete permutation polynomials – has appeared again.

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 polynomial*, 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.

Introduction

Lemma [Niederreiter, Robinson, 1982]
The polynomial

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

is a permutation polynomial over $\mathbb{F}_q$ *if and only if:*

Introduction

Lemma [Niederreiter, Robinson, 1982]
The polynomial

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

is a permutation polynomial over $\mathbb{F}_q$ *if and only if:*
the element b *is such that* $(-b)^n \neq 1$

Introduction

Lemma [Niederreiter, Robinson, 1982]
The polynomial

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

is a permutation polynomial over $\mathbb{F}_q$ *if and only if: 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* $0 \leq i < j < n$*, where* ω *is the fixed primitive root of the* n*th degree of* 1 *in the field* $\mathbb{F}_q$*.*

Introduction

Here we use the result of Niederreiter, Robinson for the two first natural cases of polynomials:

$$\mathbb{F}_{q^2},\ n = q-1,\ f(x) = x^{\frac{q^2-1}{q-1}+1} + bx = x^{q+2} + bx;$$

$$\mathbb{F}_{q^3},\ n = q-1,\ f(x) = x^{\frac{q^3-1}{q-1}+1} + bx = x^{q^2+q+2} + bx.$$

Introduction

Here we use the result of Niederreiter, Robinson for the two first natural cases of polynomials:

$$\mathbb{F}_{q^2},\ n = q-1,\ f(x) = x^{\frac{q^2-1}{q-1}+1} + bx = x^{q+2} + bx;$$

$$\mathbb{F}_{q^3},\ n = q-1,\ f(x) = x^{\frac{q^3-1}{q-1}+1} + bx = x^{q^2+q+2} + bx.$$

We assume that $q = p^m$, where p is the field characteristic and $p^m > 2$.

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

Consider the field $\mathbb{F}_{q^2}$ and set $n = q - 1$.

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

Consider the field $\mathbb{F}_{q^2}$ and set $n = q - 1$.
Set $x = \omega^i$ and $y = \omega^j$. Then Lemma above changes to the following

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

Consider the field $\mathbb{F}_{q^2}$ and set $n = q - 1$.
Set $x = \omega^i$ and $y = \omega^j$. Then Lemma above changes to 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 $x, y \in \mathbb{F}_q$, $x \neq 0$, $y \neq 0$, $x \neq y$.

Fields of even characteristic

Let $q = 2^m, m > 1$.
Using the identity $xy = x^2 + x(x+y)$ and setting $x + y = z$, from the equation (2) we arrive to the equivalent equation

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

Fields of even characteristic

Let $q = 2^m, m > 1$.
Using the identity $xy = x^2 + x(x + y)$ and setting $x + y = z$, from the equation (2) we arrive to the equivalent equation

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

Hence from Proposition 1 we obtain

Fields of even characteristic

Let $q = 2^m, m > 1$.
Using the identity $xy = x^2 + x(x+y)$ and setting $x + y = z$, from the equation (2) we arrive to the equivalent equation

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

Hence 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*

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

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

Fields of even characteristic

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 [Charpin, Kyureghyan, 2008] and in [Sarkar, Bhattacharya, Cesmelioglu, 2012], our approach essentially differs from the ones used in the papers above.

Fields of even characteristic

Fields of even characteristic

Theorem 1 (see also [Charpin, Kyureghyan, 2008], and [Sarkar, Bhattacharya, Cesmelioglu, 2012]) *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:*

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

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

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

Fields of odd characteristic

Let $q = p^m$, where $p \geq 3$. After changing the variables $x + y = z$ and $x - y = u$, Proposition 1 turns into

Fields of odd characteristic

Let $q = p^m$, where $p \geq 3$. 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*

$$3z^2 + 4z(b + b^q) + 4b^{q+1} + u^2 = 0 \tag{5}$$

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

Fields of odd characteristic

First consider the case $p = 3$.

Fields of odd characteristic

First consider the case $p = 3$.

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:*

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

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

Fields of odd characteristic

First consider the case $p=3$.

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:*

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

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

Corollary 2. *Let $q=3^m$. The polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\mathbb{F}_{q^2}$ if and only if b satisfies the condition of Theorem 2.*

Fields of odd characteristic

For the case $p > 3$, solving the quadratic equation, Proposition 3 can be equivalently replaced by

Fields of odd characteristic

For the case $p > 3$, solving the quadratic equation, 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*

$$4b^2 - 4b^{q+1} + 4b^{2q} - 3u^2 = v^2 \tag{6}$$

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

Fields of odd characteristic

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 $q - 1$, and the number of solutions which have $u = 0$ is not greater than two, then the equation (6) 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 $\mathbb{F}_q$.

Fields of odd characteristic

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 $q-1$, and the number of solutions which have $u = 0$ is not greater than two, then the equation (6) 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 $\mathbb{F}_q$.*

Fields of odd characteristic

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

$$b = \alpha^{\frac{q+1}{6}(6t+1)} \text{ or } b = \alpha^{\frac{q+1}{6}(6t+5)}, \quad t = 0, 1, \ldots, q-2, \tag{7}$$

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

Fields of odd characteristic

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

$$b = \alpha^{\frac{q+1}{6}(6t+1)} \text{ or } b = \alpha^{\frac{q+1}{6}(6t+5)}, \quad t = 0, 1, \ldots, q-2, \tag{7}$$

where α is a primitive element of $\mathbb{F}_{q^2}$.
The number of different solutions $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ equals $2(q-1)$.

Fields of odd characteristic

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

$$b = \alpha^{\frac{q+1}{6}(6t+1)} \text{ or } b = \alpha^{\frac{q+1}{6}(6t+5)}, \quad t = 0, 1, \ldots, q-2, \qquad (7)$$

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

The number of different solutions $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ equals $2(q-1)$.

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

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*

$$(x+y)^3-2(x+y)xy+((x+y)^2-xy)B_1+(x+y)B_2+B_3=0, \quad (8)$$

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

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

Fields of even characteristic

Let $q = 2^m$, and $m > 1$.

Fields of even characteristic

Let $q = 2^m$, and $m > 1$. Set $x + y = z$, $xy = u$. Using the identity $xy = x^2 + x(x + y)$ from (8) we arrive to the equivalent equation

$$uB_1 = z^3 + z^2 B_1 + zB_2 + B_3. \tag{9}$$

Fields of even characteristic

Let $q=2^m$, and $m>1$. Set $x+y=z$, $xy=u$. Using the identity $xy=x^2+x(x+y)$ from (8) we arrive to the equivalent equation

$$uB_1 = z^3 + z^2B_1 + zB_2 + B_3. \tag{9}$$

By the same argument, when $B_1=0$ the equation (9) has no solution in $\mathbb{F}_q$ for any $u \in \mathbb{F}_q,\ u \neq 0$, since in this case $z \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$.

Fields of even characteristic

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* $q^2 - 1$.

Fields of even characteristic

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 $\mathbb{F}_{q^3}$, $q=2^m, m>1$.

Fields of even characteristic

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 [Tu, Zeng, Hu, 2014] and in [Wu-Li-Helleseth-Zhang, 2014-2015] partial answers were obtained:

Fields of even characteristic

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 [Tu, Zeng, Hu, 2014] and in [Wu-Li-Helleseth-Zhang, 2014-2015] partial answers were obtained: in [Tu, Zeng, Hu, 2014] for the case $m \equiv 1 \pmod 3$

Fields of even characteristic

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 [Tu, Zeng, Hu, 2014] and in [Wu-Li-Helleseth-Zhang, 2014-2015] partial answers were obtained: in [Tu, Zeng, Hu, 2014] for the case $m \equiv 1 \pmod 3$ and in [Wu, Li, Helleseth, Zhang, 2014-2015] for the case $m \equiv 3 \pmod 9$, 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.

Fields of even characteristic

Corollary 4. *Let* $q = 2^m$ *and* $m > 1$. *Then the polynomial* $b^{-1}x^{q^2+q+2}$ *is a complete permutation polynomial over the field* $\mathbb{F}_{q^3}$ *if and only if* b *satisfies the condition of the Theorem 5.*

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*

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

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

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*

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

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 Proposition 6 turns to

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*

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

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 Proposition 6 turns to

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*

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

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

Fields of odd characteristic

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 (10) has the solution $z=-B_1/2$.

Fields of odd characteristic

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

Fields of odd characteristic

Now let $B_1^3 - 4B_1B_2 + 8B_3 \neq 0$ and, therefore, $z \neq -B_1/2$. Then 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 $Y, X \in \mathbb{F}_q^*$.

Fields of odd characteristic

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 (by the Hasse Theorem for the number of solutions of the equation above).

Fields of odd characteristic

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 (by the Hasse Theorem for the number of solutions of the equation above). It remains to consider only the cases $q = 3, 5, 7, 9$.

Fields of odd characteristic

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 (by the Hasse Theorem for the number of solutions of the equation above). It remains to consider only the cases $q = 3, 5, 7, 9$.

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

Fields of odd characteristic

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 (by the Hasse Theorem for the number of solutions of the equation above). It remains to consider only the cases $q = 3, 5, 7, 9$.

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

Because x^{14} (respectively x^{58}) is not a permutation polynomial over the field $\mathbb{F}_{3^3}$ (respectively over the field $\mathbb{F}_{7^3}$) then the following result holds.

Fields of odd characteristic

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 (by the Hasse Theorem for the number of solutions of the equation above). It remains to consider only the cases $q = 3, 5, 7, 9$.

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

Because x^{14} (respectively x^{58}) is not a permutation polynomial over the field $\mathbb{F}_{3^3}$ (respectively over the field $\mathbb{F}_{7^3}$) then the following result holds.

Corollary 6. *Let $q = p^m$ and $p \geq 3$. Then the polynomial $b^{-1}x^{q^2+q+2}$ is not a complete permutation polynomial over the field $\mathbb{F}_{q^3}$ for any $b \in \mathbb{F}^*_{q^3}$.*

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.

Fields of odd characteristic

It is known, that the equation $w^2 + 3 = 0$ has a solution in $\mathbb{F}_p$, if and only if $p = 6k + 1$.

Fields of odd characteristic

It is known, 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 $\mathbb{F}_{p^{2k}}$.

Fields of even characteristic

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

$$x^2 + xz + u = x^2 + xz + \frac{z^3 + z^2 B_1 + z B_2 + B_3}{B_1} = 0, \qquad (13)$$

has no solution in $\mathbb{F}_q$ for any $z \in \mathbb{F}_q^*$.

Fields of even characteristic

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

$$x^2 + xz + u = x^2 + xz + \frac{z^3 + z^2 B_1 + zB_2 + B_3}{B_1} = 0, \qquad (13)$$

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 (13) has a solution in $\mathbb{F}_q$.

Fields of even characteristic

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

$$x^2 + xz + u = x^2 + xz + \frac{z^3 + z^2 B_1 + zB_2 + B_3}{B_1} = 0, \qquad (13)$$

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 (13) 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 $q^2 - 1$.