Construction of Some Composition Permutations via Linear Translators

Sergey Abrahamyan, Knarik Kyuregyan

Abstract: *This paper considers construction of some composition permutation polynomials. For some permutation polynomials the explicit view of their self-compositions and inverse mappings are given. Also for some particular case the cycle structure is considered.*

Keywords: *finite field, polynomial factorization, polynomial composition*

ACM Classification Keywords*: F.2.1 Numerical Algorithms and Problems*

Introduction

Let q be a power of a prime number p and F_q be a finite field. A polynomial $f(x) \in F_q[x]$ is called a permutation polynomial of F_q if it induces a bijective map from F_q to itself. The study of permutation polynomials have intensified in the past few decades, which is connected with their applications in coding theory, cryptography and combinatorial design theory. It is a challenging problem to construct permutation polynomials and their inverse polynomials over finite fields. There are tremendous amount of papers devoted to construction of permutation polynomials. In [Evoyan et. al, 2013] some construction of permutation polynomials of the form $F(x) = x + \lambda_1 f_1(x) + \lambda_2 f_2(x) + \cdots + \lambda_k f_k(x) \in F_{q^m}[x]$ are considered, where $\lambda_1, \lambda_2 \ldots \lambda_k \in F_{q^m}$ are a linearly independent over F_q and $f_j \colon F_{q^m} \to F_q$ $1 \leq j \leq k$ (called coordinate function of F with respect to the basis $\lambda_1, \lambda_2 \ldots \lambda_k$).

Recall that for an integer $k \geq 1$ the fold composition of the mapping F with itself is

$$F_k(x) = \underbrace{F \circ F \ldots \circ F(x)}_{k \text{ times}}.$$

In [Kyureghyan, 2011] it is shown that in case $F(x) = x + \lambda f(x)$ then $F_k(x) = x + B_k \lambda f(x)$ where

$$B_k = \begin{cases} k & \text{if} \quad b = 0 \\ \dfrac{(b+1)^k - 1}{b} & \text{if} \quad b \neq 0 \end{cases}$$

and $\lambda \in F_{q^m}$ is a b linear translator of f (see Definition 1).

It is shown too, that a period of permutation polynomial $F(x) = x + \lambda f(x)$ is p (characteristic of field) when $b = 0$ and $ord(b+1)$ in the contrary case. In this paper the explicit view of permutation polynomials $F_k(x)$, $k \geq 1$ and theirs inverse mappings are given, where $F(x) = x + \lambda_1 f_1(x) + \lambda_2 f_2(x) + \cdots + \lambda_n f_n(x) \in F_{q^m}[x]$ and$n \leq m$. Also, for some particular cases the period of permutation polynomial $F(x)$ is studied. Similar studies were considered in the following works [Charpin et. al, 2009, Evoyan et. al, 2013, Kyureghyan, 2011].

Some preliminary results

In this section some preliminary results and definitions, which will be used, are introduced.

Definition 1. [Kyureghyan, 2011] Let $f: F_{p^n} \to F_p$ and $c \in F_p$. We say that $\alpha \in F_{p^n}^*$ is a $c-$ linear translator(structure) of the function f if $f(x+\alpha) - f(x) = c$ for all $x \in F_{p^n}$. Note that if α is a c-linear structure of f, then necessarily $c = f(\alpha) - f(0)$.

Proposition 1. *[Kyureghyan, 2011] Let $\alpha, \beta \in F_{q^m}^*$,$\alpha + \beta \neq 0$ and $a, b, c \in F_q$, $c \neq 0$. If α is an a-linear translator and β is a b-linear translator of a mapping $f: F_{q^m} \to F_q$, then $\alpha + \beta$ is an $(a+b)$-linear translator of f and $c \cdot \alpha$ is a $(c \cdot a)$-linear translator of f. In particular, if $\Lambda^*(f)$ denotes the set of all linear translators of f, then $\Lambda(f) = \Lambda^*(f) \cup \{0\}$ is an F_q-linear subspace of F_{q^m}.*

Definition 2. We will say that permutation polynomial $F(x)$ has a period k if k is a minimal natural number for which $F_k(x) = F(x)$.

Proposition 2 (Theorem 3 [Evoyan et. al, 2013]). *. Let $1 \leq k \leq n$, $\lambda_1, \lambda_2, \ldots, \lambda_k \in F_{q^m}$ be linearly independent over F_q and $f_j: F_{q^m} \to F_q$, $j = 1, 2, \ldots, k$. Further, suppose λ_i is a $b_{j,i}$ linear translator for f_j, where $i, j \in \{1, 2, \ldots, k\}$. Set*

$$B: = \begin{pmatrix} 1+b_{1,1} & b_{1,2} & \ldots & b_{1,k} \\ b_{2,1} & 1+b_{2,2} & \ldots & b_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k,1} & b_{k,2} & \ldots & 1+b_{k,k} \end{pmatrix},$$

and let $F: F_{q^m} \to F_{q^m}$ be defined as

$$F(x) = x + \lambda_1 f_1(x) + \lambda_2 f_2(x) + \cdots + \lambda_k f_k(x).$$

Then $F(x) = F(y)$ for some $x, y \in F_{q^m}$ if and only if

$$x = y + \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_k a_k,$$

and $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} \in F_{q^m}$ belongs to the kernel of B. In particular, the mapping F is a q^{n-r}-to-1 on F_{q^m}, where r is the rank of the matrix B.

Proposition 3 (Corollary1, [Evoyan et. al, 2013]). *With the notation of Proposition2, the mapping F is bijective on F_{q^m} if and only if the matrix B has a full rank. Let B^{-1} be the inverses matrix of B. Define the functions $h_j: F_{q^m} \to F_q$, $j = 1, 2, \ldots, k$ by*

$$\begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_k(x) \end{pmatrix} : = B^{-1} \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_k(x) \end{pmatrix}.$$

Then the inverse mapping of $F(x)$ is given by

$$F^{-1}(x) = x - \sum_{j=1}^{k} \lambda_j h_j(x).$$

Construction of Some Composition Permutations

In this chapter the explicit view of permutation polynomial of the form $F_k(x) = F \circ \ldots \circ F(x)$, where $F(x) = x + \lambda_1 f_1(x) + \cdots + \lambda_n f_n(x)$ and their inverse mapping is given. Also for some particular case we compute the period of $F_k(x)$. It is clear that if $F(x)$ is a permutation polynomial then $F_k(x)$ is also permutation. Finding the explicit view and period of permutation polynomial $F_k(x)$ is a equivalent to finding the inverse of permutation polynomial $F_k(x)$.

Theorem 1. *Let $F(x) = x + \lambda_1 f_1(x) + \cdots + \lambda_n f_n(x) \in F_{q^n}[x]$ be a permutation polynomial, where $\lambda_1, \lambda_2, \ldots, \lambda_n \in F_{q^m}$ are linearly independent, $f_j \colon F_{q^m} \to F_q$ and λ_i is a b_{ji}-liner translator of f_j for $i, j = 1, 2 \ldots n$. Define*

$$\overline{B_i} = \begin{pmatrix} 1+b_{1,1} & b_{1,2} & \ldots & b_{1,n} & 0 \\ b_{2,1} & 1+b_{2,2} & \ldots & b_{2,n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n,1} & b_{n,2} & \ldots & 1+b_{n,n} & 0 \\ a_1 & a_2 & \ldots & a_n & 1 \end{pmatrix} \qquad a_j = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases} \; j = 1, \ldots, n$$

then

$$F_k(x) = x + \sum_{i=1}^{n} \lambda_i (a_1, a_2 \ldots a_n \; 1) \overline{B}_i^{(k-1)} \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix}$$

Proof. We will proof by mathematical induction method. As assumed earlier, λ_i is a b_{ji}-liner translator of f_j. Hence by Proposition 1 we have

$$f_i \left(x + \sum_{j=1}^{n} \lambda_j f_j(x) \right) = (1 + b_{i,i}) f_i + \sum_{\substack{j=1 \\ j \neq i}}^{n} b_{i,j} f_j, \qquad i = 1, 2, \ldots, n. \tag{1}$$

For $k = 2$ we will have

$$F_2(x) = F \circ F(x) =$$

$$= x + \sum_{i=1}^{n} \lambda_i f_i(x) + \lambda_1 f_1 \left(x + \sum_{i=1}^{n} \lambda_i f_i(x) \right) + \cdots + \lambda_n f_n \left(x + \sum_{i=1}^{n} \lambda_i f_i(x) \right)$$

Substituting (1) in the provided expression we derive

$$F_2(x) = x + \sum_{i=1}^{n} \lambda_i f_i(x) + \lambda_1 \left((1 + b_{1,1}) f_1 + \sum_{\substack{j=1 \\ j \neq 1}}^{n} b_{1,j} f_j \right) +$$

$$+ \lambda_2 \left((1 + b_{2,2}) f_2 + \sum_{\substack{j=1 \\ j \neq 2}}^{n} b_{2,j} f_j \right) + \cdots + \lambda_n \left((1 + b_{n,n}) f_n + \sum_{\substack{j=1 \\ j \neq n}}^{n} b_{n,j} f_j \right)$$

Grouping similar terms we obtain

$$F_2(x) = F \circ F(x) = x + \sum_{i=1}^{n} \lambda_i(a_1, a_2, \dots a_n,\ 1)\overline{B}_i \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix},\ a_j = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases} \quad j = 1, 2, \dots, n$$

.

Now suppose that theorem's condition is true for $k = s$, i.e

$$F_s(x) = x + \sum_{i=1}^{n} \lambda_i(a_1, a_2, \dots a_n,\ 1)\overline{B}_i^{s-1} \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix},\ a_j = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases} \quad j = 1, 2, \dots, n$$

Next we will proof that it is true for $k = s + 1$.

$$F_{s+1}(x) = F_s \circ F(x) =$$

$$= x + \sum_{j=1}^{n} \lambda_j f_j(x) + \sum_{i=1}^{n} \lambda_i(a_1, a_2 \dots a_n\, 1)\overline{B}_i^{s-1} \begin{pmatrix} f_1\left(x + \sum_{j=1}^{n} \lambda_j f_j(x)\right) \\ f_2\left(x + \sum_{j=1}^{n} \lambda_j f_j(x)\right) \\ \vdots \\ f_n\left(x + \sum_{j=1}^{n} \lambda_j f_j(x)\right) \\ 0 \end{pmatrix} =$$

$$= x + \sum_{j=1}^{n} \lambda_j f_j(x) +$$

$$+ \sum_{i=1}^{n} \lambda_i(a_1, a_2, \dots a_n\ 1)\overline{B}_i^{(s-1)} \begin{pmatrix} (1 + b_{1,1})f_1 + \sum_{\substack{j=1 \\ j \neq 1}}^{n} b_{1,j} f_j \\ (1 + b_{2,2})f_2 + \sum_{\substack{j=1 \\ j \neq 2}}^{n} b_{2,j} f_j \\ \vdots \\ (1 + b_{n,n})f_n + \sum_{\substack{j=1 \\ j \neq n}}^{n} b_{n,j} f_j \\ 0 \end{pmatrix} \qquad (2)$$

It is obvious

$$\begin{pmatrix} (1 + b_{1,1})f_1 + \sum_{\substack{j=1 \\ j \neq 1}}^{n} b_{1,j} f_j \\ (1 + b_{2,2})f_2 + \sum_{\substack{j=1 \\ j \neq 2}}^{n} b_{2,j} f_j \\ \vdots \\ (1 + b_{n,n})f_n + \sum_{\substack{j=1 \\ j \neq n}}^{n} b_{n,j} f_j \\ 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 1+b_{1,1} & b_{1,2} & \dots & b_{1,n} & 0 \\ b_{2,1} & 1+b_{2,2} & \dots & b_{2,n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n,1} & b_{n,2} & \dots & 1+b_{n,n} & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix} \tag{3}$$

Substituting (3) in (2) we will derive

$$F_{s+1}(x) = x + \lambda_1 f_1(x) + \dots + \lambda_n f_n(x) +$$

$$+ \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\, 1) \overline{B}_i^{(s-1)} \begin{pmatrix} 1+b_{1,1} & b_{1,2} & \dots & b_{1,n} & 0 \\ b_{2,1} & 1+b_{2,2} & \dots & b_{2,n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n,1} & b_{n,2} & \dots & 1+b_{n,n} & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix} =$$

$$= x + \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\, 1) \overline{B}_i^{(s-1)} \begin{pmatrix} 1+b_{1,1} & b_{12} & \dots & b_{1,n} & 0 \\ b_{2,1} & 1+b_{2,2} & \dots & b_{2,n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n,1} & b_{n,2} & \dots & 1+b_{n,n} & 0 \\ a_1 & a_2 & \dots & a_n & 1 \end{pmatrix} \cdot \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix} =$$

$$= x + \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\, 1) \overline{B}_i^{(s)} \cdot \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix}.$$

□

Let B^{-1} be an inverse matrix of B. Denote the (i,j)-th element of matrix B^{-1} by $d_{i,j}$.

Let $h_j(x)\colon F_{q^m} \to F_q, j = 1, 2, \dots, n$ be a functions with the notation of Proposition 3 and namely

$$\begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \end{pmatrix} = B^{-1} \cdot \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix}. \tag{4}$$

In (4) instead of x substituting $x - \sum_{j=1}^{n} \lambda_j h_j(x)$ we will get

$$\begin{pmatrix} h_1(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \\ h_2(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \\ \vdots \\ h_n(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \end{pmatrix} = B^{-1} \cdot \begin{pmatrix} f_1(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \\ f_2(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \\ \vdots \\ f_n(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \end{pmatrix} =$$

In accordance to (1) we will have

$$= B^{-1} \cdot \begin{pmatrix} f_1(x) - \sum_{j=1}^{n} b_{1,j} h_j(x) \\ f_2(x) - \sum_{j=1}^{n} b_{2,j} h_j(x) \\ \vdots \\ f_n(x) - \sum_{j=1}^{n} b_{n,j} h_j(x) \end{pmatrix} =$$

$$= B^{-1} \cdot \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} + B^{-1} \cdot \begin{pmatrix} h_1(x) - \sum_{j=1}^{n} b_{1,j} h_j(x) - h_1(x) \\ h_2(x) - \sum_{j=1}^{n} b_{2,j} h_j(x) - h_2(x) \\ \vdots \\ h_n(x) - \sum_{j=1}^{n} b_{n,j} h_j(x) - h_n(x) \end{pmatrix} =$$

$$= B^{-1} \cdot \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} - B^{-1} \cdot B \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \end{pmatrix} + B^{-1} \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \end{pmatrix} = B^{-1} \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \end{pmatrix}$$

Finally we derive

$$h_i \left(x - \sum_{j=1}^{n} \lambda_j h_j(x) \right) = \sum_{j=1}^{n} d_{i,j} h_j(x). \tag{5}$$

Let $F(x) = x + \lambda_1 f_1(x) + \cdots + \lambda_n f_n(x)$ is a permutation polynomial with the notation of Proposition 1 . As mentioned in Proposition 3 the inverse mapping of $F(x)$ is $F^{-1}(x) = x - \sum_{j=1}^{n} \lambda_j h_j(x)$. Below the explicit view of the inverse of permutation polynomial $F_k(x)$ is given.

Theorem 2. *Let $f_1, f_2, \ldots, f_n \colon F_{q^m} \to F_q$, $\lambda_1, \lambda_2, \ldots, \lambda_n \in F_{q^m}$ are linearly independent, λ_i is a $b_{j,i}$-linear translator of f_j and $F(x) = x + \sum_{j=1}^{n} \lambda_j f_j(x) \in F_{q^m}$ is a permutation polynomial for which $H(x) = x - \sum_{j=1}^{n} \lambda_j h_j(x)$ is an inverse mapping of $F(x)$. Then the inverse polynomial of $F_k(x)$ will be*

$$H_k(x) = \underbrace{H \circ H \circ \ldots \circ H}_{k \text{ times}}(x) = x - \sum_{i=1}^{n} \lambda_i (a_1, a_2, \ldots a_n, 1) {D_i}^{k-1} \cdot \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \\ 0 \end{pmatrix},$$

where

$$D_i \stackrel{def}{=} \begin{pmatrix} d_{1,1} & d_{1,2} & \ldots & d_{1,n} & 0 \\ d_{2,1} & d_{2,2} & \ldots & d_{2,n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{n,1} & d_{n,2} & \ldots & d_{n,n} & 0 \\ a_1 & a_2 & \ldots & a_n & 1 \end{pmatrix}, \qquad a_j = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases} \qquad j = 1, ..., n$$

Proof. Like theorem 1 this one also, is proved by introduction method. For $k = 2$, we will have

$$H_2(x) = H \circ H(x) =$$

$$= x - \sum_{j=1}^{n} \lambda_j h_j(x) - \lambda_1 h_1 \left(x - \sum_{j=1}^{n} \lambda_j h_j(x) \right) - \cdots - \lambda_n h_n \left(x - \sum_{j=1}^{n} \lambda_j h_j(x) \right)$$

Substituting (5) in above expression we obtain

$$H_2(x) =$$

$$= x - \sum_{j=1}^{n} \lambda_j h_j(x) - \lambda_1 \sum_{j=1}^{n} d_{1,j} h_j - \lambda_2 \sum_{j=1}^{n} d_{2,j} h_j - \cdots - \lambda_n \sum_{j=1}^{n} d_{n,j} h_j =$$

$$= x - \sum_{j=1}^{n} \lambda_j (a_1, a_2 \dots a_n\, 1) D_i \cdot \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \\ 0 \end{pmatrix} where \qquad a_j = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

Assume that theorem's conditions is right for $k = s$, I.e

$$H_s(x) = x - \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\, 1) D_i^{s-1} \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \\ 0 \end{pmatrix}.$$

$$H_{s+1}(x) = H_s \circ H(x) =$$

$$= x - \sum_{j=1}^{n} \lambda_j h_j(x) - \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\, 1) D_i{}^{s-1} \begin{pmatrix} h_1(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \\ h_2(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \\ \vdots \\ h_n(x - \lambda_1 h_1(x) - \dots - \lambda_n h_n(x)) \\ 0 \end{pmatrix} =$$

$$= x - \sum_{j=1}^{n} \lambda_j h_j(x) - \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\, 1) D_i{}^{s-1} \begin{pmatrix} \sum_{j=1}^{n} d_{1,j} h_j(x) \\ \sum_{j=1}^{n} d_{2,j} h_j(x) \\ \vdots \\ \sum_{j=1}^{n} d_{n,j} h_j(x) \\ 0 \end{pmatrix} =$$

$$x - \sum_{j=1}^{n} \lambda_j h_j(x) -$$

$$- \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\ 1) D_i{}^{s-1} \begin{pmatrix} d_{1,1} & d_{1,2} & \dots & d_{1,n} & 0 \\ d_{2,1} & d_{2,2} & \dots & d_{2,n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{n,1} & d_{n,2} & \dots & d_{n,n} & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \\ 0 \end{pmatrix} =$$

$$= x - \sum_{i=1}^{n} \lambda_i (a_1, a_2 \dots a_n\, 1) D_i{}^{s} \begin{pmatrix} d_{1,1} & d_{1,2} & \dots & d_{1,n} & 0 \\ d_{2,1} & d_{2,2} & \dots & d_{2,n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{n,1} & d_{n,2} & \dots & d_{n,n} & 0 \\ a_1 & a_2 & \dots & a_n & 1 \end{pmatrix} \begin{pmatrix} h_1(x) \\ h_2(x) \\ \vdots \\ h_n(x) \\ 0 \end{pmatrix}$$

where $a_j = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$ □

Our next theorem is about a period of permutation polynomial $F(x) = x + \lambda_1 f_1(x) + \dots + \lambda_n f_n(x) \in F_{q^m}[x]$.

Theorem 3. *Let* $F(x) = x + \lambda_1 f_1(x) + \cdots + \lambda_n f_n(x) \in F_{q^m}[x]$ *be a permutation polynomial with the notation of Proposition 2, where* $b_{i,j} = 0$ *when* $i \neq j$.
Denote $r_i = \begin{cases} ord(1+b_{i,i}) & b_{i,i} \neq 0 \\ p & b_{i,i} = 0 \end{cases}$, *for* $i = 1, 2, \ldots, n$. *Then the period of* $F(x)$ *is equal to* $l = lcm(r_1, r_2, \ldots, r_n) + 1$.

Proof. In order to find the period of $F(x)$ one should find some $k \geq 1$ integer, for which

$$F_k(x) = x + \sum_{i=1}^{n} \lambda_i (a_1, a_2 \ldots a_n \ 1) \overline{B}_i^{(k-1)} \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \\ 0 \end{pmatrix} = x.$$

Denote $C_j^k = 1 + (1 + b_{j,j}) + \cdots + (1 + b_{j,j})^k$. Considering that $b_{i,j} = 0$, when $i \neq j$, it is easy to see that

$$\overline{B}_i^k = \begin{pmatrix} (1+b_{1,1})^k & 0 & \ldots & 0 & 0 \\ 0 & (1+b_{2,2})^k & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & (1+b_{n,n})^k & 0 \\ a_1 & a_2 & \ldots & a_n & 1 \end{pmatrix}$$

where $a_j = \begin{cases} 0 & i \neq j \\ C_i^{k-1} & i = j \end{cases}$

Hence, $(a_1, a_2, \ldots a_i \ldots, a_n) \cdot \overline{B}_i^k = (0, \ldots 0, (1+b_{i,i})^k + C_i^{k-1}, 0 \ldots 0, 1) = (0, 0, \ldots, C_i^k, 0 \ldots 0, 1)$

and $F_k(x) = x + \sum_{i=1}^{n} \lambda_i C_i^k f_i(x)$

Now let's consider the following two cases.

Let $b_{i,i} = 0$, then $C_i^k = k$ and C_i^k be equal to 0 provided k is a multiple of p.

Let $b_{i,i} \neq 0$, then $C_i^k = \frac{(1+b_{1,1})^k - 1}{b_{i,i}}$ and C_i^k be equal to 0 provided k is a order of $1 + b_{i,i}$.

In case $r_i = \begin{cases} ord(1+b_{i,i}) \\ p \end{cases}$ we have $C_i^{r_i} = 0$ and $F_l(x) = x$.
So we obtain that $F_{i+1}(x) = F(x)$

□

Acknowledgements

This work was supported by State Committee Science MES RA, in the frame of research project SCS-13-1B352.

Bibliography

[Charpin et. al, 2009] P. Charpin, G. Kyureghyan. When does $G(x) + \gamma \cdot Tr(H(x))$ permute $F_(p^n)$?, Finite Fields Appl., vol 15, 2009, pp 615 - 632.

[Evoyan et. al, 2013] M. Evoyan, G.M Kyuregyan, M. K.Kyuregyan. On k-Switching of Mappings on Finite Fields. Mathematical Problems of Computer Science 39, 2013, pp. 5 - 12.

[Kyureghyan, 2011] G. Kyureghyan. Constructing permutations of finite fields via linear translators. J. Combin. Theory Ser. A, vol. 118, 2011, pp. 1052-1061.

[M. Kyureghyan, Abrahamyan, 2012] M. Kyureghyan, S. Abrahamyan. A Method of Constructing Permutation Polynomials over Finite Fields. vol. 19, Number 4, 202, 2012, pp. 350 - 354.

Authors' Information

Sergey Abrahamyan *Researcher at , Institute for Informatics and automation problems of NAS RA, P.O. Box: 0014, P. Sevak street 1, Yerevan 0014, Armenia;*
e-mail:serj.abrahamyan@gmail.com
Major Fields of Scientific Research: Cryptography, Coding Theory

Knarik Kyuregyan *Researcher at , Institute for Informatics and automation problems of NAS RA P.O. Box: 0014, P. Sevak street 1, Yerevan 0014, Armenia;*
e-mail: knarikyuregyan@gmail.com
Major Fields of Scientific Research: Cryptography, Coding Theory