ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS
Հատոր Том Volume 112 2012 № 1

NATHENATICS

УДК 519.4

M. K. Kyureghyan, S. Y. Abrahamyan

A Method of Constructing Permutation Polynomials over Finite Fields

(Submitted by academician G. H. Khachatrian 20/I 2012)

Keywords: finite field, permutation polynomial, linear translator

1. **Introduction**. Let q be a power of a prime number and F_{q^n} be the finite field of order $q^n \geq 1$. Recall that any mapping of a finite field into itself is given by polynomial. A polynomial $F(x)$ is called a permutation polynomial of F_{q^n} if it induces a permutation on F_{q^n}. The construction of permutation polynomials over any finite fields is a challenging mathematical problem. Interest in permutation polynomials stems from both mathematical theory as well as practical applications such as cryptography. In recent papers [1-4] method to construct permutation are introduced. In this paper are considered permutations of the form $x + \gamma f(x) + \delta g(x) + \tau l(x)$ over F_q .

This paper is organized by the following way. In section2 background and preliminary results on functions with linear structures are given.

In section 3 method for constructing permutation polynomial is presented.

2. Preliminaries. We begin with recalling some definitions and basic results that will be helpful to derive our main result.

Definition 1. *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 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 $c = f(\alpha) - f(0)$.

Definition 2. *Define* $F(x) = G(x) \circ H(x)$ *composition of the mapping* G *with* H.

5.Proposition1([2] Proposition1). *Let* $\alpha, \beta \in \mathbb{F}_q^n, \alpha + \beta \neq 0$ *and* $a, b, c \in \mathbb{F}_q, c \neq 0$. *If* α *is an* a*-linear translator and* β *is a* b*-linear translator of a mapping* $f: \mathbb{F}_q^n \to \mathbb{F}_q$, *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* $\mathbb{F}_q$*-linear subspace of* $\mathbb{F}_q^n$.

6.Proposition 2([2] theorem3). *Let* $\gamma \in \mathbb{F}_q^n$ *be a b-linear translator of* $f: \mathbb{F}_q^n \to \mathbb{F}_q$ *and* $b \neq -1$ *then the inverce maping of the permutation* $F(x) = x + \gamma f(x)$ *is*

$$F^{-1}(x) = x - \frac{\gamma}{b+1} f(x).$$

7. Proposition 3 ([2] theorem8). *Let* $\gamma \subset \mathbb{F}_q^n$ *be a* b*-linear translator of* $f: \mathbb{F}_q^n \to \mathbb{F}_q$.

(a) Then $F(x) = x + \gamma f(x)$ *is a permutation of* $\mathbb{F}_q^n$ *if* $b \neq -1$.

(b) Then $F(x) = x + \gamma f(x)$ *is a q-to1 mapping of* $\mathbb{F}_q^n$ *if* $b = -1$.

Proposition 4 ([3] theorem10). *Let* $\gamma, \delta \in \mathbb{F}_q^n$. *Suppose* γ *is a* b_1*-linear translator of* $f: \mathbb{F}_q^n \to \mathbb{F}_q$ *and a* b_2*-linear translator of* $g: \mathbb{F}_q^n \to \mathbb{F}_q$, *and moreover* δ *is a* d_1*-linear translator of* f *and a* d_2*-linear translator of* g. *Then*

$$F(x) = x + \gamma f(x) + \delta g(x)$$

is a permutation of $\mathbb{F}_q^n$, *if* $b_1 \neq -1$ *and* $d_2 - \frac{d_1 b_2}{b_1+1} \neq -1$, *or by symmetry, if* $b_2 \neq -1$ *and* $d_1 - \frac{d_2 b_1}{b_2+1} \neq -1$.

3. Constructing permutations. In this section we characterize permutation polynomials of the form $P(x) = x + \gamma f(x) + \delta g(x) + \tau l(x)$.

Theorem. *Let* $\gamma, \delta, \tau, \in \mathbb{F}_q^n$.*Suppose* $\gamma, \delta, \tau,$ *is a respectively* b_1, d_1, c_1*-linear translators of* $f: \mathbb{F}_q^n \to \mathbb{F}_q$ *and* b_2, d_2, c_2 *-linear translators of* $g: \mathbb{F}_q^n \to \mathbb{F}_q$ *and* b_3, d_3, c_3 *-linear translators of* $l: \mathbb{F}_q^n \to \mathbb{F}_q$. *Then*

$$P(x) = x + \gamma f(x) + \delta g(x) + \tau l(x)$$

is a permutation polynomial of $\mathbb{F}_q^n$ *if*

1. $b \neq -1,$ (1)
2. $d_2 - \frac{d_1 b_2}{b_1+1} \neq -1$ (2)
3. $c_3 - \frac{b_3 c_1}{b_1+1} - \left(c_2 - \frac{b_2 c_1}{b_1+1}\right)\left(\frac{d_1 b_3 - d_3 b_1 - d_3}{(1+d_2)(b_1+1) - d_1 b_2}\right) \neq -1$ (3)

Proof. In accordance Proposition 3 and (1) $G(x) = x + \gamma f(x)$- is a permutation polynomial in F_{q^n} . Similarly according to proposition4 $F(x) = x + \gamma f(x) + \delta g(x)$ is also permutation polynomial while

$$b \neq -1, \quad \frac{d_1 d_2}{b_1+1} \neq -1$$

We will show that $H(x) = x + \delta h(x)$ is also permutation polynomial, where

$h(x) = g(x) - \frac{b_2}{b_1+1} f(x)$.

$$h(x+\delta u) = g(x+\delta u) - \frac{b_2}{b_1+1} f(x+\delta u) = g(x) + d_2 u - \frac{b_2}{b_1+1}(f(x) + d_1 u) =$$

$$= h(x) + \left(d_2 - \frac{d_1 b_2}{b_1+1}\right) u$$

So δ is a $\left(d_2 - \frac{d_1 b_2}{b_1+1}\right)$ -linear translator of $h: F_{q^n} \to F_q$. As $d_2 \quad \frac{d_1 d_2}{b_1+1} \neq 0$ then according to proposition 3 $H(x)$ – is also permutation polynomial in F_{q^n}.

In accordance proposition 2

$$H^{-1}(x) = x - \frac{\delta\, h(x)}{1 + d_2 - \frac{d_1 b_2}{b_1+1}} = x - \frac{\delta\, h(x)}{\frac{(1+d_2)(b_1+1) - d_1 b_2}{b_1+1}}$$

Denote $A = \frac{(1+d_2)(b_1+1) - d_1 b_2}{b_1+1}$.

It is easy to see that

$$G^{-1}(x) \circ H^{-1}(x) = x - \left(\frac{f(x)}{b_1+1} - d_1 \frac{h(x)}{A(b_1+1)}\right)\gamma - \frac{h(x)\delta}{A}.$$

Consider

$$F(x) \circ G^{-1}(x) \circ H^{-1}(x) = x - \left(\frac{f(x)}{b_1+1} - \frac{d_1}{b_1+1} \cdot \frac{h(x)}{A}\right)\gamma - \frac{h(x)}{A}\delta +$$

$$\gamma\left(f(x) - \left(\frac{f(x)}{b_1+1} - \frac{d_1}{b_1+1} \cdot \frac{h(x)}{A}\right) b_1 - \frac{h(x)}{A} d_1\right)$$

$$+ \delta\left(g(x) - \left(\frac{f(x)}{b_1+1} - \frac{d_1}{b_1+1} \cdot \frac{h(x)}{A}\right) b_2 - \frac{h(x)}{A} d_2\right)$$

To take into account that, γ and δ respectively is a b_1 and d_1 linear translators of $f: F_{q^n} \to F_q$ and b_2 , d_2 linear translators of $g: F_{q^n} \to F_q$ we get

$$F(x)\circ G^{-1}(x)\circ H^{-1}(x) = x - \frac{f(x)}{b_1+1}\gamma - \frac{d_1}{b_1+1}\cdot\frac{h(x)}{A}\gamma - \frac{h(x)}{A}\delta + \gamma f(x)$$

$$-\frac{b_1 f(x)}{b_1+1}\gamma + \frac{d_1 b_1}{(b_1+1)}\frac{h(x)}{A}\gamma - \frac{h(x)}{A}d_1\gamma + \delta g(x) - \frac{\delta f(x) b_2}{b_1+1} + \delta\frac{d_2 b_2}{(b_1+1)}\frac{h(x)}{A} - \frac{h(x)}{A}d_2$$

Substituting $\delta g(x) - \delta\frac{b_2}{b_1+1}f(x)$ for $\delta h(x)$-we get

$$F(x)\circ G^{-1}(x)\circ H^{-1}(x) = x + \gamma f(x)\left(1 - \frac{1}{b_1+1} - \frac{b_1}{b_1+1}\right) -$$
$$\frac{h(x)d_1}{A}\gamma\left(1 - \frac{1}{b_1+1} - \frac{b_1}{b_1+1}\right) + \frac{h(x)}{A}\left(A + \frac{d_1 b_2}{b_1+1} - d_2 - 1\right) = x$$

Next we observe

$$P(x)\circ(G^{-1}(x)\circ H^{-1}(x) = (x + \gamma f(x) + \delta g(x) + \tau l(x))\circ(G^{-1}(x)\circ H^{-1}(x)$$

$$= \left(F(x) + \tau l(x)\right)\circ\left(G^{-1}(x)\circ H^{-1}(x)\right)$$

Take into account that

$$G^{-1}(x)\circ H^{-1}(x) = x - \left(\frac{f(x)}{b_1+1} - \frac{d_1 h(x)}{A}\right)\gamma - \frac{\delta h(x)}{A} \quad \text{and}$$

$$F(x)\circ G^{-1}(x)\circ H^{-1}(x) = x$$

We have $P(x)\circ G^{-1}(x)\circ H^{-1}(x) = x + \tau l\left(x - \left(\frac{f(x)}{b_1+1} - \frac{h(x)}{A}\right)\gamma - \frac{h(x)}{A}\delta\right)$

$$= x + \tau l(x - b_2\left(\frac{f(x)}{b_1+1} - \frac{d_1 h(x)}{(b_1+1)A}\right) - d_2\frac{h(x)}{A})$$

Denote $l(x) - b_2\left(\frac{f(x)}{b_1+1} - \frac{d_1 h(x)}{(b_1+1)A}\right) - d_2\frac{h(x)}{A} = k(x)$.

So $P(x)\circ G^{-1}(x)\circ H^{-1}(x) = x + \tau k(x)$

We show that τ is a $c_3 - \frac{b_3 c_1}{b_1+1} - \frac{1}{A}\left(c_2 - \frac{b_2 c_1}{b_1+1}\right)\left(\frac{d_1 b_3 - d_3 b_1 - d_3}{(1+d_2)(b_1+1)-d_1 b_2}\right)$ linear translator of $k(x) \in F_{q^n} \to F_q$.

$$k(x+\tau u) = l(x+\tau u) - \frac{b_3}{b_1+1} f(x+\tau u) - \frac{d_1 b_3}{(b_1+1)A} h(x+\tau u) - \frac{d_3}{A} h(x+\tau u) =$$

$$l(x) + c_3 u - \frac{b_3}{b_1+1}(f(x) + u c_1) + \frac{d_1 b_3}{(b_1+1)A}\left(h(x) + \left(c_2 - \frac{b_2 c_1}{b_1+1}\right)u\right) - \frac{d_3}{A}\left(h(x) + \left(c_2 - \frac{b_2 c_1}{b_1+1}\right)u\right) =$$

$$l(x) + c_3 u - \frac{b_3}{b_1+1} f(x) - \frac{b_3}{b_1+1} c_1 u + \frac{d_1 b_3}{(b_1+1)A} h(x) + \frac{d_1 b_3}{(b_1+1)A}\left(c_2 - \frac{b_2 c_1}{b_1+1}\right)u - \frac{d_3}{A} h(x) - \frac{d_3}{A}\left(c_2 - \frac{b_2 c_1}{b_1+1}\right)u$$

$$= k(x) + \left[c_3 - \frac{b_3 c_1}{b_1+1} - \frac{d_1 b_3}{(b_1+1)A}\left(c_2 - \frac{b_2 c_1}{b_1+1}\right) - \frac{d_3}{A}\left(c_2 - \frac{b_2 c_1}{b_1+1}\right)\right] u =$$

$$= k(x) + \left[c_3 - \frac{b_3 c_1}{b_1+1} - \left(c_2 - \frac{b_2 c_1}{b_1+1}\right)\left(\frac{d_1 b_3 - d_3 b_1 - d_3}{(1+d_2)(b_1+1) - d_1 b_2}\right)\right] u$$

In accordance to proposition3 and condition (3) $P(x) o G^{-1}(x) o H^{-1}(x)$ is a permutation polynomial in F_{q^n}. Since $H(x)$ and $G(x)$ is also permutation polynomials in F_{q^n}, then $P(x)$ also will be a permutation polynomial in F_{q^n} .

Institute of Informatics and Automation Problems of NAS RA

M. K. Kyureghyan, S. Y. Abrahamyan

A Method of Constructing Permutation Polynomials over Finite Fields

Problem of constructing permutation polynomials of the shape $P(x) = x + \gamma f(x) + \delta g(x) + \tau l(x)$ over the field F_q is considered. Method for constructing some family of permutation polynomial is given.

Մ. Կ. Կյուրեղյան, Ս.Ե. Աբրահամյան

Վերջավոր դաշտերի վրա տեղադրության բազմանդամների կառուցման եղանակ

Ուսումնասիրված է F_q դաշտի վրա $P(x) = x + \gamma f(x) + \delta g(x) + \tau l(x)$ տեսքի տեղադրության բազմանդամների կառուցման խնդիրը: Առաջարկվել է մեթոդ տեղադրության բազմանդամների որոշակի դաս կառուցելու համար:

М. К. Кюрегян, С. Е. Абраамян

Метод построения перестановочных полиномов над конечными полями

Рассматривается проблема построения перестановочных полиномов формы $P(x) = x + \gamma f(x) + \delta g(x) + \tau l(x)$ над полем F_q. Дан метод построения некоторого семейства перестановочных полиномов.

References

1. *Charpin P., Kyureghyan G.* - Finite Fields . Appl. 2009. V.15 (5) P. 615-632.
2. *Kyureghyan G.* - Journal of Combinatorial Theory. 2011. A. V. 118. P. 1052-1061.
3. *Lidl R. Niederreiter H.*, Finite Fields. Cambridge University Press 1987.
4. *Markos J.* Finite Fields Appl. 2011. V.17. P.105-112.