A METHOD OF CONSTRUCTING PERMUTATION POLYNOMIALS OVER FINITE FIELDS

Melsik Kyureghyan, Sergey Abrahamyan

Abstract: *In this paper we consider the problem of characterizing permutation polynomials of the shape $P(x) = x + \gamma f(x) + \delta\, g(x) + \tau l(x)$ over the field F_q; that is, we seek conditions on the coefficients of a polynomial which are necessary for it to represent a permutation.*

Keywords: *finite field, permutation polynomial, linear translator.*

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}. These polynomials were first explored in the research of Betti [Betti,1851], Mathieu and Hermite [Hermite 1863] as a way of representing permutations. A general theory was developed by Hermite [Hermite 1863] and Dickson [Dickson 1896], with many subsequent developments by Carlitz et.al. 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. Recent papers [Betti,1851]- [Markos 2011] highlight a method of construction of permutation polynomials. The given article considers permutations of the form $x + \gamma f(x) + \delta\, g(x) + \tau l(x)$ over F_q .

Preliminaries

Let's start 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.

Proposition1 ([Kyureghyan G. 2011**] 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 $\mathbb{F}_{q^n}$.

Proposition 2 ([Kyureghyan G. 2011**] 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 $Fx = x + \gamma f x$ is

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

Proposition 3 ([Kyureghyan G. 2011**] theorem8)** Let $\gamma \in \mathbb{F}_{q^n}$ 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 ([Kyureghyan G. 2011**] 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 $d_1 - \frac{d_2 b_1}{b_2+1} \neq -1$.

Constructing Permutation

In this section we characterize permutation polynomials of the form

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

Theorem1

Let $F(x) = x + \gamma f(x) + \delta g(x)$ be a permutation polynomial in $\mathbb{F}_{q^n}$. Suppose γ is a b_1 −linear translator of $f\colon F_{q^n} \to F_q$ and a b_2 −linear translator of $g\colon F_{q^n} \to F_q$ moreover δ is a d_1 −linear translator of f and a d_2 −linear translator of g.

Then the inverse mapping of the permutation $F(x) = x + \gamma f(x) + \delta g(x)$

is $F^{-1}(x) = x - \left(f(x) - d_1 \frac{g(x)(b_1+1) - b_2 f(x)}{A}\right)\frac{\gamma}{b_1+1} - \frac{g(x)(b_1+1) - b_2 f(x)}{A}\delta$

where $A = (1 + d_2)(b_1 + 1) - d_1 b_2$.

Proof

Consider

$$F(x)^{\circ}\left(x - \left(f(x) - d_1 \frac{g(x)(b_1+1) - b_2 f(x)}{A}\right)\frac{\gamma}{b_1+1} - \frac{g(x)(b_1+1) - b_2 f(x)}{A}\delta\right)$$

$$= x - \left(f(x) - d_1 \frac{g(x)(b_1+1) - b_2 f(x)}{A}\right)\frac{\gamma}{b_1+1}$$

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

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

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

Taking 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

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

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

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

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

Composing similar members we have

$$= x + \gamma f(x)\left(1 - \frac{1}{b_1+1} - \frac{b_1}{b_1+1}\right) - d_1\frac{g(x)(b_1+1) - b_2 f(x)}{A}\left(1 - \frac{1}{b_1+1} - \frac{b_1}{b_1+1}\right)\gamma$$

$$\frac{g(x)(b\_1+1) - b\_2\, f(x)}{A}\left(\frac{A}{b_1+1} - 1 - d_2 + \frac{d_1 b_2}{b_1+1}\right) = x$$

Theorem2

Let $\gamma, \delta, \tau, \in F_{q^n}$ .Suppose γ, δ, τ, is a respectively b_1, d_1, c_1-linear translators of $f: F_{q^n} \to F_q$ and b_2, d_2, c_2 -linear translators of $g: F_{q^n} \to F_q$ and b_3, d_3, c_3 -linear translators of $l: F_{q^n} \to F_q$. Then

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

is a permutation polynomial of F_{q^n} if

1. $b_1 \neq -1,$ (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

$G(x) = x + \gamma f(x)$- is a permutation polynomial in F_{q^n} by Proposition3 and condition(1).

We show that $H(x) = x + \delta\left(\frac{g(x)(b_1+1)-b_2 f(x)}{b_1+1}\right)$ is also permutation polynomial.

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

$$h(x+\delta u) = g(x+\delta u) - \frac{b_2}{b_1+1} f(x+\delta u) = g(x) + \mathrm{d}_2 u - \frac{b_2}{b_1+1}(f(x)+\mathrm{d}_1 u) =$$

$$= h(x) + \left(\mathrm{d}_2 - \frac{d_1 b_2}{b_1+1}\right) u$$

So, δ is a $\left(\mathrm{d}_2 - \frac{d_1 b_2}{b_1+1}\right)$ -linear translator of $h\colon F_{q^n} \to F_q$. As $\mathrm{d}_2 - \frac{\mathrm{d}_1 \mathrm{d}_2}{\mathrm{b}_1+1} \neq 0$ then according to proposition3 $H(x)$ – is also permutation polynomial in F_{q^n}.

In accordance with proposition 2

$$\mathrm{H}^{-1}(\mathrm{x}) = \mathrm{x} - \frac{\delta\ \mathrm{h}(\mathrm{x})}{1 + \mathrm{d}_2 - \frac{\mathrm{d}_1 \mathrm{b}_2}{\mathrm{b}_1+1}} = \mathrm{x} - \frac{\delta\,\mathrm{h}(\mathrm{x})}{\frac{(1+\mathrm{d}_2)(\mathrm{b}_1+1)-\mathrm{d}_1\mathrm{b}_2}{\mathrm{b}_1+1}} = \frac{\delta\,\mathrm{h}(\mathrm{x})(\mathrm{b}_1+1)}{\mathrm{A}}$$

It is easy to see that

$$G^{-1}(x) o H^{-1}(x) = x - \left(f(x) - d_1 \frac{g(x)(b_1+1)-b_2 f(x)}{A}\right)\frac{\gamma}{b_1+1} - \frac{g(x)(b_1+1)-b_2 f(x)}{A}\delta:$$

Now we consider $\mathrm{P(x)} o G^{-1}(x) o H^{-1}(x)$

$$= (x + \gamma f(x) + \delta\, g(x)) o \left(x - \left(f(x) - d_1 \frac{g(x)(b_1+1)-b_2 f(x)}{A}\right)\frac{\gamma}{b_1+1} - \frac{g(x)(b_1+1)-b_2 f(x)}{A}\delta\right)(1)$$

$$+\tau l\left(x - \left(f(x) - d_1 \frac{g(x)(b_1+1)-b_2 f(x)}{A}\right)\frac{\gamma}{b_1+1} - \frac{g(x)(b_1+1)-b_2 f(x)}{A}\delta\right)$$

Since $b_1 \neq -1$ and $d_2 - \frac{d_1 b_2}{b_1+1} \neq -1$, so according to proposition 4

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

is permutation polynomial in $\mathrm{F}_{\mathrm{q}^{\mathrm{n}}}$. So by theorem1 we can imply that $(1) = x$,and we have

$\mathrm{P(x)} o G^{-1}(x) o H^{-1}(x) =$

$$= x + \tau\left(l(x) - \left(f(x) - d_1 \frac{g(x)(b_1+1) - b_2 f(x)}{A} \right) \frac{b_3}{b_1+1} - \frac{g(x)(b_1+1) - b_2 f(x)}{A} d_3 \right)$$

Denote

$$l(x) - \left(f(x) - d_1 \frac{g(x)(b_1+1) - b_2 f(x)}{A} \right) \frac{b_3}{b_1+1} - \frac{g(x)(b_1+1) - b_2 f(x)}{A} d_3 = k(x)\ .$$

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

We show that τ is a $c_3 - \frac{b_3 c_1}{b_1+1} - \frac{1}{A}\left(c_2 - \frac{b_2 c_1}{b_1+1}\right)\left(\frac{d_1 b_3 - d_3 b_1 - d_3}{(1+\mathrm{d}_2)(\mathrm{b}_1+1) - \mathrm{d}_1 \mathrm{b}_2}\right)$ linear translator of $k(x) \in F_{q^n} \rightarrow F_q$.

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

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

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

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

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

$$= k(x) + \left[c_3 - \frac{b_3 c_1}{b_1+1} - \left(c_2 - \frac{b_2 c_1}{b_1+1}\right)\left(\frac{d_1 b_3 - d_3 b_1 - d_3}{(1+\mathrm{d}_2)(\mathrm{b}_1+1) - \mathrm{d}_1 \mathrm{b}_2}\right)\right] u$$

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

Conclusion

In recent years in cryptography and coding theory permutations are applied very often. So it is important to propose new methods for generating permutation polynomials. Method for constructing permutation polynomials of the shape $P(x) = x + \gamma f(x) + \delta\, g(x) + \tau l(x)$ is given.

Bibliography

[Betti,1851] E. Betti, Sopra la risolubilit`a per radicali delle equazioni algebriche irriduttibili di grado primo, Annali di Scienze Matematiche e Fisiche 2 (1851), 5–19. (=Opere Matematiche, v.1, 17–27)

[Charpin 2009]. P.Charpin, G. Kyureghyan, When does $F(x) + \gamma Tr(H(x))$ permute F_{p^n} ?, Finite Fields .Appl15 (5) 2009 615-632

[Dickson 1896] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Annals Math. 11 (1896-7), 65–120 and 161–183.

[Hermite 1863] Ch. Hermite, Sur les fonctions de sept lettres, C. R. Acad. Sci. Paris 57 (1863), 750–757.

[Kyureghyan G. 2011]. G. Kyureghyan, Constructing permutations of finite fields via linear translator, Journal of Combinatorial Theory 2011. P. 1052-1061

[Lidl,1987]. R. Lidl, H. Niederreiter, Finite Fields. Cambridge University Press 1987.

[Markos 2011]. J.Markos Specific permutation polynomials over finite fields Appl. 2011 V.17 p.105-112

Authors' Information

Melsik Kyureghyan *– Head of Data Coding Laboratory of Institute of Informatics and Automation problems of NAS of RA 1, P.Sevak St., Yerevan, 0014, Republic of Armenia*
e-mail: melsik@ipia.sci.am

Sergey Abrahamyan *– Researcher; Data Coding Laboratory of Institute of Informatics and Automation problems of NAS of RA 1, P.Sevak St., Yerevan, 0014, Republic of Armenia*
e-mail: serj.abrahamyan@gmail.com