ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր Том Volume 113 2013 № 1

APPLIED MATHEMATICS

УДК 519.1

M. G. Evoyan

On a Class of Permutations on Finite Field

(Submitted by academician Yu. H. Shoukourian 22/I 2013)

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

1. Introduction. Let q be a power of a prime number p and F_{q^n} be the finite field of order q^n, $n \geq 1$. Any mapping from a finite field into itself is given by a polynomial. A polynomial $F(x)$ is called a permutation polynomial of F_{q^n} if it induces a permutation on F_{q^n}. The study of permutations of finite fields started in 19-th century with the work of Hermite and later Dickson. In recent years, there has been tremendous amount of interest in constructing permutation polynomials of F_q due to their applications in combinatorial, cryptography, and coding theory. In general finding nontrivial classes of permutation polynomials of finite fields is a difficult problem. In [2, Theorem 1] and [2, Theorem 2] Kyureghyan gives very important criteria for constructing permutation polynomials of F_{q^n}. This paper will focus on case $n = 2$, i.e. construction of permutation polynomial over F_{q^2}. The following definition is used further in paper.

Definition. *A non-zero element $\alpha \in F_{q^n}$ is called an α-linear translator for the mapping $f : F_{q^n} \to F_q$ if $f(x+u\alpha) - f(x) = ua$ holds for any $x \in F_{q^n}$, $u \in F_q$ and a fixed $a \in F_q$.*

Theorem 1. *(Theorem 1,* [2]*). Let $L : F_{q^n} \to F_{q^n}$ be an F_q-linear permutation of F_{q^n}. Let $b \in F_q$, $h : F_q \to F_q$ and $\gamma \in F_{q^n}$ be a b-linear translator of $f : F_{q^n} \to F_q$. Then the mapping $G(x) = L(x) + L(\gamma)h(f(x))$ permutes F_{q^n} if and only if $g(u) = u + bh(u)$ permutes F_q.*

Theorem 2. *(Theorem 2,* [2]*). Let* $L: F_{q^n} \to F_{q^n}$ *be an* F_q*-linear mapping of* F_{q^n} *with Kernel* $\alpha F_q, \alpha \neq 0$*. Suppose* α *is a* b*-linear translator of* $f: F_{q^n} \to F_q$ *and* $h: F_q \to F_q$ *is a permutation of* F_q*. Then the mapping*

$$G(x) = L(x) + \gamma h(f(x))$$

permutes F_{q^n} *if and only if* $b \neq 0$ *and* γ *does not belong to the Image set of* L*.*

In this paper a generalization of the following result from [3] is given.

Theorem 3. *(Theorem 5.12,* [3]*). Let* $q = p^m$*. Then the following are permutation polynomials of* F_{q^2}

(a) $f_{a,b,k}(x) := ax^q + bx + (x^q - x)^k$*, for* $a, b \in F_q$ *such that* $a \neq \pm b$*, and for all even positive integer* k*.*

(b) $f_{a,k}(x) := ax^q + ax + (x^q - x)^k$*, if* $a \in F_q^*$*, and* p *and* k *are odd, and in addition* k *is relatively prime with* $q - 1$*.*

2. Results. The following lemma is proved easily with help of Theorem 7.9 from [1].

Lemma 1. *Let* $b \in F_{q^2}$*, where* a *and* b *are not simultaneously equal to* 0*, and* $L_{a,b}: F_{q^2} \to F_{q^2}$ *and* $L_{a,b}(x) = ax^q + bx$*. Then* $L_{a,b}$ *is a* F_q*−linear mapping on* F_{q^2}*. Moreover,*

(a) $|Kernel(L_{a,b})| = \{0\}$*, i.e.* $L_{a,b}(x)$ *permutes* F_{q^2}*, if and only if* $\left(\frac{b}{a}\right)^{q+1} \neq 1$ *or* $b \neq 0$ *and* $a = 0$*;*

(b) $|Kernel(L_{a,b})| = q$*, if and only if* $\left(\frac{b}{a}\right)^{q+1} = 1$*.*

The following theorem generalizes Theorem 3 for case (a).

Theorem 4. *Let* $q = p^m$ *and* $f_{a,b,\alpha,k}(x) := ax^q + bx + \alpha(x^q + x)^k$*, where* $a, b, \alpha \in F_{q^2}$ *such that* $\left(\frac{b}{a}\right)^{q+1} = 1$ *or* $b \neq 0$ *and* $a = 0$*. Then* $f_{a,b,\alpha,k}(x)$ *permutes* F_{q^2} *if and only if* $g(x) = x + (\gamma^q + \gamma)x^k$ *permutes* F_q*, where* γ *is the preimage of* α *in* $ax^q + bx$*.*

Proof. Let $L(x) := ax^q + bx$, $f(x) := x^q + x$ and $h(x) := x^k$. Since $\left(\frac{b}{a}\right)^{q+1} \neq 1$ *or* $b \neq 0$ *and* $a = 0$, from Lemma 1 we get that $L(x)$ permutes on F_{q^2}.

So preimage of a exists. Let γ be the preimage of α, so $L(\gamma) = a\gamma^q + b\gamma = \alpha$. Next we show that $\gamma \in F_{q^2}$ is a $(\gamma^q + \gamma)$-linear translator of $x^q + x$:

$$(x + \gamma u)^q + x + \gamma u = x^q + x + (\gamma u)^q + \gamma u = x^q + x + (\gamma^q + \gamma)u.$$

Note that $\left(\gamma^q+\gamma\right)\in F_q$ if $\gamma\in F_{q^2}$. So γ is a $\left(\gamma^q+\gamma\right)$-linear translator of $f(x)$. Hence from Theorem 1, we will have that

$$f_{a,b,\alpha,k}(x):=ax^q+bx+\alpha\left(x^q+x\right)^k$$

permutes F_{q^2} if and only if $g(x)=x+\left(\gamma^q+\gamma\right)x^k$ permutes F_q.

Theorem 5 generalizes Theorem 3 for case (b).

Theorem 5. *Let $q=p^m$. Let $f_{a,b,\alpha,k}(x):=ax^q+bx+\alpha\left(x^q+x\right)^k$, where $a,b,\gamma\in F_{q^2}$, $\left(\frac{b}{a}\right)^{q+1}=1$ and $gcd(k,q-1)=1$. Then $f_{a,b,\alpha,k}(x)$ permutes F_{q^2} if and only if $a\neq b$ and $\gamma\notin Image(L)$.*

Proof. We will prove this theorem with help of Theorem 2.

Let $L(x)=ax^q+bx$, $h(x)=x^k$ and $f(x)=x^q+x$.

Lemma 1 shows that $\left|Kernel(L)\right|=q$. Let γ be a generator of $Kernel(L)$. It is obvious that γ is an $\left(\gamma^q+\gamma\right)$-linear translator of $f(x)$. Theorem 7.8 from [1] shows that $h(x)=x^k$ permutes F_q if and only if $\gcd(k,q-1)=1$. So by Theorem 2 $f_{a,b,\alpha,k}(x)$ permutes F_{q^2} if and only if $\gamma\notin Image(L)$ and $\gamma^q+\gamma\neq 0$. Note that $\gamma^q+\gamma$ equals to 0 if and only if $a=b$ because $a\gamma^q+b\gamma=0$.

3. Examples. The following examples show that Theorem 4 and Theorem 5 generalize Theorem 3. First we consider case (a) from Theorem 3.

Let $f_{a,b,k}(x)=ax^q+bx+\left(x^q-x\right)^k$, where $a,b\in F_q$ such that $a\neq\pm b$ and $k>0$ is an even integer. Let $\omega\in F_{q^2}$ such, that $\omega^q=-\omega$. Note that such an element exists, since by Lemma 1 kernel of x^q+x is not equal to $\{0\}$. Then

$$f_{a,b,k}(\omega x)=a\omega^q x^q+b\omega x+a\left(\omega^q x^q-\omega x\right)^k=-\omega a x^q-\omega^q bx+\left(-\omega x^q-\omega x\right)^k.$$

Thus

$$f_{a,b,k}(\omega x)=a^* x^q+b^* x+(-\omega)^k\left(x^q-x\right)^k,$$

where $a^*=-\omega a$, $b^*=\omega b$. Note that $\left(-\omega^k\right)=\omega^k$ because k is even. Let $L(x):=a^* x^q+b^* x$. If $a=0$ then $a^*=0$ and $b^*\neq 0$ because $\omega\neq 0$ and $b\neq 0$. For case when a $a\neq 0$ it is obvious that $\left(\frac{b^*}{a^*}\right)^{q+1}$ can be equal to 1 if and only if $\left(\frac{b}{a}\right)^{q+1}=1$. Further $\left(\frac{b}{a}\right)^{q+1}=\left(\frac{b}{a}\right)^2$, since $a,b\in F_q$, and therefore $\left(\frac{b}{a}\right)^{q+1}$ can be equal to 1 if and only if $a\neq\pm b$. Thus $\left(\frac{b^*}{a^*}\right)^{q+1}\neq 1$ or $a^*=0$ and $b^*\neq 0$.

Hence $L(x)$ permutes F_{q^2}, so a preimage of ω^k exists. Let α be the preimage of ω^k. It is easy to check that $\alpha = \frac{\omega^{k-1}}{a+b}$.

Hence by Theorem 4, $f_{a,b,k}(\omega x)$ permutes F_{q^2} if and only if $g(x) = x + (\alpha^q + \alpha)x^k$ permutes F_q. Note that

$$\alpha^2 + \alpha = \left(\frac{\omega^{k-1}}{a+b}\right)^q + \frac{\omega^{k-1}}{a+b} = -\frac{\omega^{k-1}}{a+b} + \frac{\omega^{k-1}}{a+b} = 0$$

and thus $g(x) = x$ and it permutes F_q. Hence by Theorem 4 $f_{a,b,k}(\omega x)$ permutes F_{q^2}, and so does $f_{a,b,k}(x) = ax^q + bx + (x^q - x)^k$.

Next we show that Theorem 5 generalizes of part (b) of Theorem 3. Let $q = p^m$ and $f_{a,k}(x) ax^q + ax + (x^q - x)^k$, where $a \in F_q$, p and k are odd, and in addition k is relatively prime with $q-1$. Let $\omega \in F_{q^2}$ such, that $\omega^q = -\omega$. Then

$$f_{a,k}(\omega x) = -\left(a\omega x^q - a\omega x + \omega^k (x^q + x)^k\right).$$

Note that $\left(\frac{-a\omega}{a\omega}\right)^{q+1} = 1$ and $-a\omega \neq a\omega$ if p is odd. Further we show that $\omega^k \notin \mathrm{Im}age(L)$, where $L(x) := a\omega x^q - a\omega x$.

Let, in contrary, $\omega^k \in Image(L)$. Then for some $\delta \in F_{q^2}$ $a\omega\delta^q - a\omega\delta = \omega^k$. Since $\omega \neq 0$, we get

$$a\delta^q - a\delta = \omega^{k-1}.$$

By raising both sides of the previous equation to power q, we get

$$a\delta - a\delta^q = \omega^{k-1},$$

since $k-1$ is even and $a \in F_{q^2}$. From the last two equations and the fact that p is odd we get that $\omega^k \in Image(L)$ if and only if $\omega = 0$.

So by Theorem 5 $f_{a,k}(\omega x)$ permutes F_{q^2}, and so does $f_{a,k}(x)$.

Institute of Informatics and Automation
Problems of NAS RA

M. G. Evoyan

On A Class Of Permutations On Finite Field

Problem of determining permutation polynomials of the shape $F(x) := ax^q + bx + \alpha(x^q + x)^k$ over the F_{q^2} field is considered. Two new criteria of determining permutation polynomials of the shape $F(x) = ax^q + bx + a(q^x + x)^k$ over the F_{q^2} are given.

Մ. Գ. Էվոյան

Վերջավոր դաշտերի վրա տեղափոխությունների մի դասի մասին

Ուսումնասիրված է F_{q^2} դաշտի վրա $F(x) := ax^q + bx + \alpha\left(q^x + x\right)^k$ տեսքի տեղադրության բազմանդամների կառուցման խնդիրը: Առաջարկված է $F(x) = ax^q + bx + \alpha\left(x^q + x\right)^k$ տեսքի բազմանդամների տեղափոխության բազմանդամ լինելու երկու նոր չափանիշ:

М. Г. Эвоян

О типе перестановок на конечных полях

Рассматривается проблема определения перестановочных полиномов формы $F(x) := ax^q + bx + \alpha\left(x^q + x\right)^k$ над полем F_{q^2}. Даны два новых критерия перестановочности полиномов формы $F(x) = ax^q + bx + \alpha\left(x^q + x\right)^k$ над полем F_{q^2}.

References

1. *Lidl R., Niederreiter H.* Finite Fields. Encyclopedia Math. Appl. Cambridge University Press. 1997.
2. *Kyureghyan G.* - Journal of Combinatorial Theory. 2011. Series A(118). P. 1052-1061.
3. *Akbary A., Ghioca D., Wang Q.* - Finite Fields and Their Applications. 2011. V. 17. P. 5167.