Mathematical Problems of Computer Science 39, 5–12, 2013.

# On $k$-Switching of Mappings on Finite Fields

Mikayel G. Evoyan[1], Gohar M. Kyuregyan[2] and Melsik K. Kyuregyan[1]

Institute for Informatics and Automation Problems of NAS RA[1]
Institute of Algebra and Geometry, Otto-von-Guericke University Magdeburg[2]
e-mail: michael.evoyan@gmail.com, gohar.kyureghyan@ovgu.de, melsik@ipia.sci.am

**Abstract**

The switching construction was used in several recent papers to construct special mappings on finite fields. In this paper we generalize the concept of switching to a $k$-switching with $1 \leq k \leq n$. We present some general properties of $k$-switching and describe permutations produced using $k$-switching.

**Keywords:** Mappings of finite fields, switching, permutation.

## 1. Introduction

Let $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ and $(\gamma_1, \ldots, \gamma_n)$ be an $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$. The uniquely determined functions $f_i : \mathbf{F}_{q^n} \to \mathbf{F}_q$, $1 \leq i \leq n$, such that

$$F(x) = f_1(x) \cdot \gamma_1 + \ldots + f_n(x) \cdot \gamma_n,$$

are called the *coordinate functions* of $F$ with respect to the basis $(\gamma_1, \ldots, \gamma_n)$. The *component functions* of $F$ over the subfield $\mathbf{F}_q$ are the functions $Tr_{q^n/q}(\alpha F(x))$ with $\alpha \in \mathbf{F}_{q^n}^*$, where $Tr_{q^n/q}$ is a trace mapping of $\mathbf{F}_{q^n}$ into $\mathbf{F}_q$ given by

$$Tr_{q^n/q} = x + x^q + \ldots + x^{q^{n-1}}.$$

The set of component functions of a mapping coincides with one of its coordinate functions:

**Proposition 1:** *Any component function over $\mathbf{F}_q$ of a mapping $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ is a coordinate function with respect to some $\mathbf{F}_q$-basis, and vice versa.*

**Proof.** Recall that any basis $(\gamma_1, \ldots, \gamma_n)$ has a unique dual basis $(\bar{\gamma}_1, \ldots, \bar{\gamma}_n)$ defined by

$$Tr_{q^n/q}(\gamma_i \bar{\gamma}_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

for all $1 \leq i, j \leq n$. In particular for any $a \in \mathbf{F}_{q^n}$ the coefficients $a_i$ in the linear combination $a = \sum_{i=1}^n a_i \gamma_i$ are given by

$$a_i = Tr_{q^n/q}(\bar{\gamma}_i a).$$

Consequently, the coordinate function $f_i(x)$ of $F(x)$ with respect to $(\gamma_1, \ldots, \gamma_n)$ is the component function $Tr_{q^n/q}(\bar{\gamma}_i F(x))$. On the other hand, a component function $Tr_{q^n/q}(\alpha F(x))$ is a coordinate function of $F(x)$ with respect to the dual basis of any basis containing $\alpha$. ■

A mapping $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ is called a switching of $G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ if there is an $\mathbf{F}_q$-basis $(\gamma_1, \ldots, \gamma_n)$ such that all but the first coordinate functions of $F$ and $G$ are equal, i.e.

$$F(x) = f_1(x) \cdot \gamma_1 + \ldots + f_n(x) \cdot \gamma_n,$$

and

$$G(x) = g_1(x) \cdot \gamma_1 + \ldots + g_n(x) \cdot \gamma_n,$$

with $f_1(x) \neq g_1(x)$ and $f_i(x) = g_i(x)$ for all $2 \leq i \leq n$. Switching was used to produce interesting classes of special mappings of finite fields in [2]–[8]. Construction of bijective mappings by changing two coordinate functions of the identity mapping were studied in [5, 7]. In this paper we generalize the concept of switching to a $k$-switching with $1 \leq k \leq n$ and describe permutations produced using $k$-switching.

## 2. $k$-Switching

**Definition 1:** *Let $1 \leq k \leq n$ be an integer. A mapping $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ is called a $k$-switching of $G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ over $\mathbf{F}_q$ if $k$ is the minimal integer such that there is an $\mathbf{F}_q$-basis $(\gamma_1, \ldots, \gamma_n)$ with respect to which all but the first $k$ coordinate functions of $F$ and $G$ are equal, i.e.*

$$F(x) = f_1(x) \cdot \gamma_1 + \ldots + f_n(x) \cdot \gamma_n,$$

*and*

$$G(x) = g_1(x) \cdot \gamma_1 + \ldots + g_n(x) \cdot \gamma_n,$$

*with $f_j(x) \neq g_j(x)$ for all $1 \leq j \leq k$ and $f_i(x) = g_i(x)$ for all $k+1 \leq i \leq n$.*

Note that 1-switching reduces to a switching defined above. Clearly, for any two different mappings $F$ and $G$ there is an integer $1 \leq k \leq n$ such that $F$ is a $k$-switching of $G$. Moreover, if $F$ is a $k$-switching of $G$, then also $G$ is a $k$-switching of $F$.

**Remark 1:** *Let $1 \leq k < k' \leq n$. If the mapping $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ is a $k$-switching of $G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$, then there is an $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$ with respect to which exactly $k'$ coordinate functions of $F$ and $G$ differ. Indeed, let*

$$F(x) = \sum_{i=1}^{k} f_i(x)\gamma_i + \sum_{i=k+1}^{n} a_i(x)\gamma_i,$$

*and*

$$G(x) = \sum_{i=1}^{k} g_i(x)\gamma_i + \sum_{i=k+1}^{n} a_i(x)\gamma_i,$$

*with respect to an $\mathbf{F}_q$-basis $(\gamma_1, \ldots, \gamma_n)$ and $f_i(x) \neq g_i(x)$ for all $1 \leq i \leq k$. Then with respect to the $\mathbf{F}_q$-basis*

$$(\gamma_1, \ldots, \gamma_{k-1}, \sum_{j=k}^{k'} \gamma_j, , \gamma_{k+1}, \ldots, \gamma_n),$$

*the coordinate functions of $F$ and $G$ are as follows:*

$$F(x)=\sum_{i=1}^{k-1} f_i(x)\gamma_i + f_k(x)\left(\sum_{j=k}^{k'}\gamma_j\right) + \sum_{i=k+1}^{k'}(a_i(x)-f_k(x))\gamma_i + \sum_{i=k'+1}^{n} a_i(x)\gamma_i,$$

*and*

$$G(x)=\sum_{i=1}^{k-1} g_i(x)\gamma_i + g_k(x)\left(\sum_{j=k}^{k'}\gamma_j\right) + \sum_{i=k+1}^{k'}(a_i(x)-g_k(x))\gamma_i + \sum_{i=k'+1}^{n} a_i(x)\gamma_i.$$

In the following for a subset $S \subseteq \mathbf{F}_{q^n}$ we use $\langle S\rangle$ to denote the $\mathbf{F}_q$-subspace spanned by $S$.

**Theorem 1:** *Let $1 \le k \le n$ and $F, G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$. Then the following statements are equivalent:*

**(i)** *$F$ is a $k$-switching of $G$.*

**(ii)** *The image set of the mapping $F-G : x \mapsto F(x)-G(x)$ spans a $k$-dimensional vector space over $\mathbf{F}_q$.*

**Proof.** Let $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ be a $k$-switching of $G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$. Then there is an $\mathbf{F}_q$-basis $(\gamma_1, \dots, \gamma_n)$ of $\mathbf{F}_{q^n}$ such that

$$F(x)=\sum_{i=1}^{k} f_i(x)\gamma_i + \sum_{i=k+1}^{n} a_i(x)\gamma_i,$$

and

$$G(x)=\sum_{i=1}^{k} g_i(x)\gamma_i + \sum_{i=k+1}^{n} a_i(x)\gamma_i,$$

where $f_i(x) \neq g_i(x)$ for all $1 \le i \le k$. Hence

$$F(x)-G(x)=\sum_{i=1}^{k}(f_i(x)-g_i(x))\gamma_i,$$

showing that the dimension $l$ of $\langle Image(F-G)\rangle$ is less or equal to $k$. Now let $(\delta_1, \dots, \delta_\ell)$ be a basis for $\langle Image(F-G)\rangle$, and $(\delta_1, \dots, \delta_\ell, \dots \delta_n)$ a basis for $\mathbf{F}_{q^n}$. Let $h_i, u_j : \mathbf{F}_{q^n} \to \mathbf{F}_q$ be such that

$$F(x)-G(x)=\sum_{i=1}^{\ell} h_i(x)\delta_i,$$

and

$$G(x)=\sum_{i=1}^{n} u_i(x)\delta_i.$$

Then

$$F(x)=\sum_{i=1}^{\ell}(u_i(x)+h_i(x))\delta_i + \sum_{i=\ell+1}^{n} u_i(x)\delta_i,$$

and thus $k \le \ell$ by the definition of $k$-switching, completing the proof. ■

**Proposition 2:** *Let $1 \le k \le n$ and $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ be a $k$-switching of $G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$. Then $F$ and $G$ have exactly $q^{n-k}-1$ equal component functions over $\mathbf{F}_q$.*

**Proof.** Let $\alpha \in \mathbf{F}_{q^n}, \alpha \neq 0$. Then $Tr_{q^n/q}(\alpha F(x)) = Tr_{q^n/q}(\alpha G(x))$ holds if and only if $Tr_{q^n/q}(\alpha(F(x) - G(x)))$ is the constant zero function, or, the equivalent, image set of the mapping $F - G$ is contained in the hyperplane $\mathcal{H}_\alpha = \{y \in \mathbf{F}_{q^n} : Tr_{q^n/q}(\alpha y) = 0\}$. Note that $Image(F - G) \subseteq \mathcal{H}_\alpha$ if and only if the linear span $\langle Image(F - G)\rangle$ is a subspace of $\mathcal{H}_\alpha$. By Theorem 1 the dimension of $\langle Image(F - G)\rangle$ is $k$. Hence, there are $\frac{q^{n-k}-1}{q-1}$ different hyperplanes containing $\langle Image(F - G)\rangle$. To complete the proof it remains to recall that $\mathcal{H}_\alpha = \mathcal{H}_{\alpha'}$ if and only if $\alpha' = \alpha \cdot u$ with a non-zero $u \in \mathbf{F}_q$. ■

## 3. $k$-Switching of the Identity Mapping

In this section we consider bijective $k$-switching of the identity mapping. As the next observation shows the study of $k$-switching of an arbitrary permutation on $\mathbf{F}_{q^n}$ can be reduced to one of the identity mappings. Let $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ be a $k$-switching of $G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$, and either $F$ or $G$ be a permutation on $\mathbf{F}_{q^n}$. Without loss of generality, say $F$ is a permutation and denote its inverse mapping by $F^{-1}$. Then

$$G(x) = F(x) + \sum_{i=0}^{k} f_i(x) \cdot \gamma_i, \tag{1}$$

with respect to some basis $(\gamma_1, \ldots, \gamma_n)$. Note that (1) holds if and only if

$$G \circ F^{-1}(x) = x + \sum_{i=0}^{k} f_i \circ F^{-1}(x) \cdot \gamma_i,$$

that is when $G \circ F^{-1}$ is a $k$-switching of the identity mapping. Hence, understanding of the behaviour of $k$-switching of the identity mapping is an important step for the general problem.

The remaining part of this section is devoted to a class of permutations obtained by $k$-switching using the so-called functions with a linear translator. Our results generalize several constructions of permutations given in [1, 3, 5, 7].

A non-zero element $\alpha \in \mathbf{F}_{q^n}$ is called an $a$-linear translator (or $a$-linear structure, cf. [3]) for the mapping $f : \mathbf{F}_{q^n} \to \mathbf{F}_q$ if

$$f(x + u\alpha) - f(x) = ua, \tag{2}$$

for all $x \in \mathbf{F}_{q^n}, u \in \mathbf{F}_q$ and some fixed $a \in \mathbf{F}_q$.

The following theorem from [3] allows to construct functions with linear translators explicitly.

**Theorem 2:** *Let $G : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ and $f(x) = Tr_{q^n/q}(G(x))$. Then $f$ has a linear translator if and only if there is a non-bijective $\mathbf{F}_q$-linear mapping $L : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ such that*

$$f(x) = Tr_{q^n/q}(G(x)) = Tr_{q^n/q}(H \circ L(x) + \beta x),$$

*for some $H : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ and $\beta \in \mathbf{F}_{q^n}$. In this case, any element from the kernel of $L$ is a linear translator for $f$.*

**Theorem 3:** *Let $1 \leq k \leq n$, $\lambda_1, \lambda_2, \cdots, \lambda_k \in \mathbf{F}_{q^n}$ be linearly independent over $\mathbf{F}_q$ and $f_j : \mathbf{F}_{q^n} \to \mathbf{F}_q$, $j = 1, \ldots, k$. Further, suppose $\lambda_i$ is a $b_{j,i}$-linear translator for $f_j$, where $i, j \in \{1, 2, \cdots, k\}$. Set*

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

*and let $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ 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 $x, y \in \mathbf{F}_{q^n}$ if and only if*

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

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

**Proof.** Let $x, y \in \mathbf{F}_{q^n}$ be such that $F(x) = F(y)$. Then, by the definition of $F$

$$x + \lambda_1 f_1(x) + \lambda_2 f_2(x) + \cdots + \lambda_k f_k(x) = y + \lambda_1 f_1(y) + \lambda_2 f_2(y) + \cdots + \lambda_k f_k(y),$$

and thus

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

for some elements $a_i \in \mathbf{F}_q$. Observe, that when $a_i \in \mathbf{F}_q$, then

$$\begin{aligned} F\left(y + \sum_{i=1}^{k} \lambda_i a_i\right) &= y + \sum_{i=1}^{k} \lambda_i a_i + \sum_{j=1}^{k} \lambda_j f_j\left(y + \sum_{i=1}^{k} \lambda_i a_i\right) \\ &= y + \sum_{i=1}^{k} \lambda_i a_i + \sum_{j=1}^{k} \lambda_j \left(f_j(y) + \sum_{i=1}^{k} b_{j,i} a_i\right) \\ &= y + \sum_{j=1}^{k} \lambda_j f_j(y) + \sum_{i=1}^{k} \lambda_i a_i + \sum_{j=1}^{k} \lambda_j \left(\sum_{i=1}^{k} b_{j,i} a_i\right) \\ &= F(y) + \sum_{j=1}^{k} \lambda_j \left((b_{j,j}+1) a_j + \sum_{i=1, i\neq j}^{k} b_{j,i} a_i\right). \end{aligned}$$

To complete the proof it remains to note that the linear independence of $\lambda_j$ implies

$$F(y) + \sum_{j=1}^{k} \lambda_j \left((b_{j,j}+1) a_j + \sum_{i\neq j, i=1}^{k} b_{j,i} a_i\right) = F(y),$$

if and only if all coefficients

$$(b_{j,j}+1) a_j + \sum_{i\neq j, i=1}^{k} b_{j,i} a_i = 0,$$

or equivalently if $\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ is in the kernel of the matrix $B$. ■

Theorem 1 reduces to Theorem 8 from [5] when $k = 1$. For $k = 2, 3$, it extends Theorem 10 from [5] and Theorem 1, 2 from [7] considerably.

**Remark 2:** *Let $(\gamma_1, \ldots, \gamma_k)$ be linear independent over $\mathbf{F}_q$ and $f_1(x)$, $\ldots$, $f_k(x)$ non-zero functions from $\mathbf{F}_{q^n}$ into $\mathbf{F}_q$. Suppose the $k$-switching of the identity mapping*

$$x + \sum_{j=1}^{k} f_j(x)\gamma_j,$$

*is a permutation on $\mathbf{F}_{q^n}$. Note that in this case the $(k-1)$-switching*

$$x + \sum_{j=1}^{k-1} f_j(x)\gamma_j,$$

*must not be a permutation on $\mathbf{F}_{q^n}$. This follows easily from Theorem 3. Indeed, there are non-singular matrices over $\mathbf{F}_q$ whose leading principal $(n-1) \times (n-1)$ minor is 0.*

**Corollary 1:** *With the notations of Theorem 3, the mapping $F$ is bijective on $\mathbf{F}_{q^n}$ if and only if the matrix $B$ has a full rank. Let $B^{-1}$ be the inverses matrix of $B$. Define the functions $h_j : \mathbf{F}_{q^n} \to \mathbf{F}_q$, $j = 1, \ldots, k$ by*

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

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

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

**Proof.** Let $B_j$ be the $j$th row in the matrix $B$. The calculations in the proof of Theorem 3 show that

$$\begin{aligned} F\left(x - \sum_{j=1}^{k} \lambda_j h_j(x)\right) &= x + \sum_{j=1}^{k} \lambda_j f_j(x) - \sum_{j=1}^{k} \lambda_j B_j \cdot \begin{pmatrix} h_1(x) \\ \vdots \\ h_k(x) \end{pmatrix} \\ &= x + \sum_{j=1}^{k} \lambda_j f_j(x) - \sum_{j=1}^{k} \lambda_j B_j \cdot B^{-1} \cdot \begin{pmatrix} f_1(x) \\ \vdots \\ f_k(x) \end{pmatrix} \\ &= x + \sum_{j=1}^{k} \lambda_j f_j(x) - \sum_{j=1}^{k} \lambda_j f_j(x) \\ &= x. \end{aligned}$$

■

The inverse mapping of the permutation $F$ obtained in Corollary 1 is a $k$-switching of the identity mapping as well. The next proposition shows that this property holds for all permutations obtained via switching from the identity mapping.

**Proposition 3:** *If a permutation $F : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ is a $k$-switching of the identity mapping of $\mathbf{F}_{q^n}$, then its inverse is a $k$-switching of the identity mapping as well.*

**Proof.** Let $(\gamma_1, \dots, \gamma_k)$ be linear independent over $\mathbf{F}_q$ and $f_1(x), \dots, f_k(x) : \mathbf{F}_{q^n} \to \mathbf{F}_q$ be non-zero functions. Further suppose that the mapping

$$F(x) = x + \sum_{j=1}^{k} f_j(x)\gamma_j,$$

is a permutation of $\mathbf{F}_{q^n}$. If $F^{-1}$ is the inverse mapping of $F$, then

$$x = F \circ F^{-1}(x) = F^{-1}(x) + \sum_{j=1}^{k} (f_j \circ F^{-1})(x)\gamma_j.$$

Thus

$$F^{-1}(x) = x - \sum_{j=1}^{k} (f_j \circ F^{-1}(x))\gamma_j,$$

implying the result. ■

## References


[1] A. Akbary, D. Ghioca and Q. Wang, "On constructing permutations of finite fields", *Finite Fields Appl.*, vol. 17, pp. 51-67, 2011.

[2] L. Budaghyan, C. Carlet and G. Leander, "Constructing new APN functions from known ones", *Finite Fields Appl.*, vol. 15, pp. 150-159, 2009.

[3] P. Charpin and G. Kyureghyan, "When does $G(x) + \gamma \mathrm{Tr}(H(x))$ permute $\mathbf{F}_{p^n}$?", *Finite Fields Appl.*, vol. 15, pp. 615-632, 2009.

[4] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic", *Adv. Math. Commun.*, vol. 3, pp. 59-81, 2009.

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

[6] G. Kyureghyan and Yin Tan, "On a family of planar mappings", *Enhancing cryptographic primitives with techniques from error correcting codes, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. 23*, IOS, Amsterdam, pp. 175-178, 2009.

[7] M. Kyureghyan and S. Abrahamyan, "A method of constructing permutation polynomials over finite fields", *Int. J. Information Theories and Applications*, vol. 17, pp. 328-334, 2010.

[8] A. Pott and Y. Zhou, "Switching construction of planar functions on finite fields", *Arithmetic of finite fields, Lecture Notes in Comput. Sci. 6087*, Springer, Berlin, pp. 135-150, 2010.


**Submitted 14.12.2012, accepted 11.02.2013.**

## Վերջավոր դաշտերի վրա արտապատկերումների $k$-փոխարկումների մասին

Մ. Էվոյան, Գ. Կյուրեղյան և Մ. Կյուրեղյան

**Ամփոփում**

Փոխարկումները կիրառվում են վերջերս լույս տեսած վերջավոր դաշտերի վրա յուրահատուկ արտապատկերումների կառուցմանը նվիրված աշխատանքներում: Այս աշխատանքում ընդհանրացվում է փոխարկման հասկացությունը մինչև $k$ -փոխարկում, որտեղ $\leq k \leq n$ , ինչպես նաև ներկայացվում են $k$-փոխարկումների ընդհանուր հատկություններ և նկարագրվում է $k$-փոխարկումների միջոցով տեղափոխությունների կառուցման մեթոդ:

## О $k$-обменах отображений на конечных полей

М. Эвоян, Г. Кюрегян и М. Кюрегян

**Аннотация**

Конструкция обмена используется в нескольких недавних работах по построению специфических отображений на конечных полей. В этой статье понятие об обмене обобщено до $k$-обмена с $\leq k \leq n$ . Также представлены некоторые общие свойства $k$-обмена и описан метод получения перестановок с использованием $k$-обмена.