Finite Fields and Their Applications 50 (2018) 279–292

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Nilpotent linearized polynomials over finite fields and applications

Lucas Reis

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil

ARTICLE INFO

Article history:
Received 30 September 2016
Accepted 7 December 2017
Available online 15 December 2017
Communicated by Gary L. Mullen

MSC:
12E20
11T06

Keywords:
Linearized polynomials
Permutation polynomials
Cycle decomposition
Involutions

ABSTRACT

Let q be a prime power and $\mathbb{F}_{q^n}$ be the finite field with q^n elements, where $n > 1$. We introduce the class of the linearized polynomials $L(X)$ over $\mathbb{F}_{q^n}$ such that

$$L^{(t)}(X) := \underbrace{L \circ L \circ \cdots \circ L}_{t \text{ times}}(X) \equiv 0 \pmod{X^{q^n} - X}$$

for some $t \geq 2$, called *nilpotent linearized polynomials* (NLP's). We discuss the existence and construction of NLP's and, as an application, we show how to obtain permutations of $\mathbb{F}_{q^n}$ from these polynomials. For some of those permutations, we can explicitly give the compositional inverse map and the cycle decomposition. This paper also contains a method for constructing involutions over binary fields with no fixed points, which are useful in block ciphers.

E-mail address: lucasreismat@gmail.com.

https://doi.org/10.1016/j.ffa.2017.12.005
1071-5797/

1. Introduction

Let q be a prime power and $\mathbb{F}_{q^n}$ be the finite field with q^n elements, where $n > 1$. Any map from $\mathbb{F}_{q^n}$ to itself can be represented by a polynomial in $\mathbb{F}_{q^n}[X]$. Conversely, any polynomial in $\mathbb{F}_{q^n}[X]$ induces a map from $\mathbb{F}_{q^n}$ to itself. In this context, the $\mathbb{F}_q$-linear maps of $\mathbb{F}_{q^n}$ correspond to the so called linearized polynomials $L(X) = \sum_{i=0}^{k} a_i X^{q^i}$, $a_i \in \mathbb{F}_{q^n}$. If a polynomial $f(X) \in \mathbb{F}_{q^n}[X]$ induces a permutation in $\mathbb{F}_{q^n}$, $f(X)$ is a *permutation polynomial* over $\mathbb{F}_{q^n}$. For many applications in coding theory [2] and cryptography [6], it is interesting to find permutation polynomials over finite fields. For instance, in block ciphers, permutations of binary fields are used as S-boxes to build a confusion layer in the encryption process and the inverse of this permutation is used in the decryption process. In order to avoid some problems like limited memory, it is interesting to use involutions of binary fields, i.e., permutation polynomials $f(X) \in \mathbb{F}_{2^n}[X]$ such that $f^{-1}(a) = f(a)$ or, equivalently, $f(f(a)) = a$ for any $a \in \mathbb{F}_{2^n}$. If $f(x)$ is a permutation of $\mathbb{F}_{q^n}$, an element $a \in \mathbb{F}_{q^n}$ is a *fixed point* if $f(a) = a$. A random permutation in $\mathbb{F}_{2^n}$ has $O(1)$ fixed points, while a random involution has $2^{n/2} + O(1)$ fixed points. Therefore, an involution with more than $O(1)$ fixed points can be distinguished from random permutations and so can be attacked. In fact, as suggested in [1], good involutions should have no fixed points. For more information on permutation polynomials, see Section 8 of [4].

In this paper, we introduce the class of the *nilpotent linearized polynomials* (NLP's): they are the linearized polynomials $L(X) \in \mathbb{F}_{q^n}[X]$ such that

$$L^{(t)}(X) \equiv 0 \pmod{X^{q^n} - X}$$

for some $t \geq 2$ and $L(X) \not\equiv 0 \pmod{X^{q^n} - X}$, where $L^{(t)}(X)$ denotes the ordinary polynomial composition of $L(X)$ with itself t times. We study the existence and construction of those polynomials, including explicit examples. We describe a method for constructing permutation and complete permutation polynomials from those nilpotent polynomials and, in some particular cases, we determine the compositional inverse map and describe the cycle decomposition. This paper also includes explicit examples of involutions over binary fields with no fixed points.

2. Existence and properties of NLP's

Throughout this paper, $\mathbb{F}_{q^n}$ denotes the finite field with q^n elements, where q is a prime power and $n > 1$. For a nonzero element α in any extension of $\mathbb{F}_q$, $\mathrm{ord}(\alpha)$ denotes the multiplicative order of α. Also, if $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ are finite extensions of $\mathbb{F}_q$, we define the *trace function* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^m}$ as

$$\mathrm{Tr}_{q^n/q^m}(a) := \sum_{i=0}^{n/m-1} a^{q^{mi}}.$$

The trace function is *onto* and, in fact, for each $\alpha \in \mathbb{F}_{q^m}$, there exist q^{n-m} elements $\beta \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^m}(\beta) = \alpha$.

A polynomial $L(X) \in \mathbb{F}_{q^n}[X]$ is *linearized* if $L(X) = \sum_{i=0}^{k} a_i X^{q^i}$. For instance, trace functions are represented by linearized polynomials. If $L(X)$ is linearized, $L(z+y) = L(z) + L(y)$ and $L(az) = aL(z)$ for any $a \in \mathbb{F}_q$ and $y, z \in \mathbb{F}_{q^n}$, hence $L(X)$ induces an $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$. Conversely, if $\{\omega_1, \ldots, \omega_n\}$ is any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, the $n \times n$ matrix $D = (\omega_i^{q^{j-1}})_{ij}$ is invertible and, for an $\mathbb{F}_q$-linear map M of $\mathbb{F}_{q^n}$, $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$ is the linearized polynomial representation of M, where

$$(a_0, \ldots, a_{n-1})^T = D^{-1}(b_1, \ldots, b_n)^T,$$

$b_i = M(\omega_i)$ and ^{T} denotes the transpose. This is a one-to-one correspondence between the $\mathbb{F}_q$-linear maps of $\mathbb{F}_{q^n}$ and the linearized polynomials $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$.

Remark 2.1. If $L(X) = \sum_{i=0}^{k} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ and $k > n-1$, the $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$ induced by $L(X)$ can be represented by another linearized polynomial of the form $L_0(X) = \sum_{i=0}^{n-1} b_i X^{q^i} \in \mathbb{F}_{q^n}[X]$. In fact, $L_0(X)$ is the reduction of $L(X)$ modulo $X^{q^n} - X$. For this reason, we are mostly interested in the linearized polynomials of the form $\sum_{i=0}^{n-1} a_i X^{q^i}$.

Definition 2.2. If $t \geq 2$ is an integer, $L(X) \in \mathbb{F}_{q^n}[X]$ is a *t-nilpotent linearized polynomial* (t-NLP) over $\mathbb{F}_{q^n}$ if $L(X)$ is a linearized polynomial such that $L(X) \not\equiv 0 \pmod{X^{q^n} - X}$ and $L^{(t)}(X) \equiv 0 \pmod{X^{q^n} - X}$. In other words, $L^{(t)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$ and $L(a) \neq 0$ for some $a \in \mathbb{F}_{q^n}$.

It follows from definition that $L(X)$ is a t-NLP over $\mathbb{F}_{q^n}$ if, and only if, its polynomial reduction modulo $X^{q^n} - X$ is a t-NLP over $\mathbb{F}_{q^n}$. Moreover, any t-NLP is also a d-NLP for any $d > t$.

If $f \in \mathbb{F}_{q^n}[X]$, $Z_f = \{z \in \mathbb{F}_{q^n} \mid f(z) = 0\}$ denotes the set of the roots of f in $\mathbb{F}_{q^n}$ and $V_f = \{f(z) \mid z \in \mathbb{F}_{q^n}\}$ denotes the value set of f over $\mathbb{F}_{q^n}$. If $L(X)$ is a linearized polynomial over $\mathbb{F}_{q^n}$, the sets V_L and Z_L are $\mathbb{F}_q$-vector spaces. In fact V_L and Z_L are, respectively, the image and the kernel of the $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$ induced by L.

The following theorem gives a necessary and sufficient condition for the existence of t-NLP's over $\mathbb{F}_{q^n}$ with prescribed value set V.

Theorem 2.3. *Let $V \subseteq \mathbb{F}_{q^n}$ be any $\mathbb{F}_q$-vector space. Then there exist an integer $t \geq 2$ and a t-NLP over $\mathbb{F}_{q^n}$ such that $V = V_L$ if, and only if, $V \neq \{0\}, \mathbb{F}_{q^n}$.*

Proof. Suppose that $t \geq 2$ and $L(X)$ is a t-NLP over $\mathbb{F}_{q^n}$ such that $V = V_L$. We observe that $L(a) \neq 0$ for some $a \in \mathbb{F}_{q^n}$, hence $V_L \neq \{0\}$. Since $L^{(t)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$, the $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$ induced by $L(X)$ is not an isomorphism, hence $V_L \neq \mathbb{F}_{q^n}$. Conversely, suppose that $V \neq \{0\}, \mathbb{F}_{q^n}$ and let $\{\omega_1, \ldots, \omega_k\}$ be any basis of V over $\mathbb{F}_q$,

where $0 < k < n$. Let $\omega_{k+1}, \ldots, \omega_n$ be elements of $\mathbb{F}_{q^n}$ such that $\{\omega_1, \ldots, \omega_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let M be the $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$ defined as follows:

$$M(\omega_i) = \begin{cases} \omega_1 & \text{if} \quad i = n \\ \omega_{i+1} & \text{if} \quad 1 \leq i \leq k-1 \\ 0 & \text{if} \quad k \leq i \leq n-1. \end{cases}$$

Since $0 < k < n$ and $n > 1$, M is well defined and a direct calculation shows that $V_M = V$ and $M^{(k+1)}(\omega_i) = 0$ for any $1 \leq i \leq n$. Hence $M^{(k+1)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$ and $M(\omega_n) \neq 0$. Then $L(X)$, the linearized polynomial representation of M, is a $(k+1)$-NLP over $\mathbb{F}_{q^n}$ and satisfies $V_L = V$. $\square$

As it was noticed at the beginning of this section, for a given basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, the construction of the linearized polynomial associated to a linear map requires only the computation of the inverse of a matrix. In this context, the proof of Theorem 2.3 suggests a computational method for constructing t-NLP's with a given value set. However, we can find explicit examples of such polynomials.

Example 2.4. Let $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ be finite extensions of $\mathbb{F}_q$. If θ is an element of $\mathbb{F}_{q^n}^*$ such that $\mathrm{Tr}_{q^n/q^m}(\theta) = 0$, then $L_\theta(X) := \theta \cdot \mathrm{Tr}_{q^n/q^m}(X)$ is a 2-NLP over $\mathbb{F}_{q^n}$ and its value set over $\mathbb{F}_{q^n}$ is given by $\theta \cdot \mathbb{F}_{q^m}$. In particular, if n/m is divisible by $p = \mathrm{char}(\mathbb{F}_q)$, $L(X) = \mathrm{Tr}_{q^n/q^m}(X)$ is a 2-NLP over $\mathbb{F}_{q^n}$.

Example 2.5. Let m be any positive integer and $n = 2m$. If α and β are two elements in $\mathbb{F}_{q^n}^*$ such that $\alpha^{q^m} + \alpha = 0$ and $\beta^{q^m+1} = 1$, a direct calculation shows that $L_{\alpha,\beta}(X) := \alpha\beta X^{q^m} + \alpha X$ is a 2-NLP over $\mathbb{F}_{q^n}$. The equations $Y^{q^m} + Y = 0$ and $Y^{q^m+1} = 1$ have $q^m - 1$ and $q^m + 1$ solutions in $\mathbb{F}_{q^n}^*$, respectively. Hence there are $q^n - 1$ polynomials of the form $L_{\alpha,\beta}(X)$.

2.1. NLP's in $\mathbb{F}_q[X]$

Here we give a complete characterization of the t-NPL's over $\mathbb{F}_{q^n}$ such that their coefficients lie in the base field, i.e., $L(X) \in \mathbb{F}_q[X]$. First, we recall some concepts of the theory of linearized polynomials. For more details, see Section 3.4 of [3].

Definition 2.6. If $L_1, L_2 \in \mathbb{F}_{q^n}[X]$ are linearized polynomials we define their *symbolic product* by $L_1 \otimes L_2 = L_1(L_2(X))$, which is a linearized polynomial.

A simple calculation shows that the symbolic product $\otimes$ is associative, distributive with respect to the ordinary addition, but is not commutative. However, if $L_1, L_2 \in \mathbb{F}_q[X]$ it can be verified that $L_1 \otimes L_2 = L_2 \otimes L_1$.

Definition 2.7. Let $L(X) = \sum_{i=0}^{t} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ be a linearized polynomial and $l(X) = \sum_{i=0}^{t} a_i X^i$. The polynomials $l(X)$ and $L(X)$ are called q-associates of each other. More specifically, $l(X)$ is the *conventional* q-associate of $L(X)$ and $L(X)$ is the *linearized* q-associate of $l(X)$.

The following lemma shows an interesting property of the linearized polynomials with coefficients in $\mathbb{F}_q$.

Lemma 2.8 *([3], Lemma 3.59). Let L_1 and L_2 be linearized polynomials with conventional q-associates l_1 and l_2, respectively. If the coefficients of L_1 and L_2 lie in the base field $\mathbb{F}_q$, the polynomials $l = l_1 \cdot l_2$ and $L = L_1 \otimes L_2$ are q-associates.*

We start with the following proposition.

Proposition 2.9. *Suppose that $g \in \mathbb{F}_q[X]$ satisfies $g(X + a) = g(X)$ for any a in $\mathbb{F}_{q^n}$. Then there exists a polynomial $R \in \mathbb{F}_q[X]$ such that $g(X) = R(X^{q^n} - X)$. In particular, if g is linearized, then so is R.*

Proof. For the first statement, we proceed by induction on $n = \deg g$. If g is a constant then there is nothing to prove. Suppose that the statement is true for any polynomial of degree at most k and let $g \in \mathbb{F}_q[X]$ a polynomial of degree $k+1$ satisfying $g(X+a) = g(X)$ for any $a \in \mathbb{F}_{q^n}$. We have $g(0) = g(a)$ for any $a \in \mathbb{F}_{q^n}$ and so the polynomial $g(X) - g(0)$ has degree $k + 1 > 0$ and vanishes at any element of $\mathbb{F}_{q^n}$. In particular we have that

$$g(X) - g(0) = (X^{q^n} - X)G(X) \tag{1}$$

for some non-zero polynomial $G(X) \in \mathbb{F}_q[X]$. Since $g(X + a) - g(0) = g(X) - g(0)$ and $(X + a)^{q^n} - (X + a) = X^{q^n} - X$ for any $a \in \mathbb{F}_{q^n}$, it follows from Eq. (1) that $G(X) = G(X + a)$ for any $a \in \mathbb{F}_{q^n}$ and $\deg G < \deg g$. By the induction hypothesis, $G(X) = F(X^{q^n} - X)$ for some $F \in \mathbb{F}_q[X]$. Therefore, $g(X) = (X^{q^n} - X)F(X^{q^n} - X) + g(0)$ and so $g(X) = R(X^{q^n} - X)$, where $R(X) = X \cdot F(X) + g(0) \in \mathbb{F}_q[X]$.

For the second statement we observe that, if g is linearized, the equality $g(X) = R(X^{q^n} - X)$ yields:

$$bR(z^{q^n} - z) = bg(z) = g(bz) = R((bz)^{q^n} - bz) = R(b(z^{q^n} - z)) \tag{2}$$

and

$$R(z^{q^n} - z) + R(y^{q^n} - y) = g(z) + g(y) = g(z + y) = R(z^{q^n} - z + (y^{q^n} - y)) \tag{3}$$

for any $b \in \mathbb{F}_q$ and $y, z \in \overline{\mathbb{F}}_{q^n}$, where $\overline{\mathbb{F}}_{q^n}$ is the algebraic closure of $\mathbb{F}_{q^n}$. In particular, for any $A, B \in \overline{\mathbb{F}}_{q^n}$ there exist elements A_0 and B_0 in $\overline{\mathbb{F}}_{q^n}$ such that $A_0^{q^n} - A_0 = A$ and $B_0^{q^n} - B_0 = B$ and then, from Eq. (2) and (3), we conclude that

$$R(A+B) = R(A) + R(B) \quad \text{and} \quad R(bA) = bR(A)$$

for any $b \in \mathbb{F}_q$ and $A, B \in \overline{\mathbb{F}}_{q^n}$. Hence $R(X)$ induces an $\mathbb{F}_q$-linear map T from $\overline{\mathbb{F}}_{q^n}$ to itself. Set $r = \deg R$ and let s be a positive integer such that $q^s > r$. If $S(X)$ is the linearized polynomial representation of T when restricted to $\mathbb{F}_{q^s}$, then $R(z) = S(z)$ for any $z \in \mathbb{F}_{q^s}$ and $\deg R, \deg S < q^s$. Therefore, $R(X) = S(X)$ and so $R(X)$ is linearized. □

The main result of this section is the following theorem.

Theorem 2.10. *Let $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_q[X]$ be a nonzero linearized polynomial and $l(X) = \sum_{i=0}^{n-1} a_i X^i$ its conventional q-associate. Then $L(X)$ is a t-NLP over $\mathbb{F}_{q^n}$ if, and only if, $X^n - 1$ divides $l(X)^t$. In particular, if n is not divisible by p, then for any $t \geq 2$ there do not exist t-NLP's over $\mathbb{F}_{q^n}$ with coefficients in $\mathbb{F}_q$.*

Proof. Suppose that $l(X)^t = (X^n - 1) \cdot g(X)$ for some $g(X) \in \mathbb{F}_q[X]$ and $t \geq 2$. From Lemma 2.8, we have that

$$L^{(t)}(X) = \underbrace{L(X) \otimes \cdots \otimes L(X)}_{t \text{ times}} = (X^{q^n} - 1) \otimes G(X),$$

where $G(X)$ is the linearized q-associate to $g(X)$. In particular $G(X)$ is linearized and then $(X^{q^n} - X) \otimes G(X)$ is divisible by $X^{q^n} - X$. Therefore $L^{(t)}(X) \equiv 0 \pmod{X^{q^n} - X}$ and, since $\deg L(X) < q^n$ and $L(X)$ is nonzero, we conclude that $L(X) \not\equiv 0 \pmod{X^{q^n} - X}$. Hence $L(X)$ is a t-NLP over $\mathbb{F}_{q^n}$.

Conversely, suppose that $L(X)$ is a t-NLP over $\mathbb{F}_{q^n}$ and set $M(X) = L^{(t)}(X)$. Since $M(X) \in \mathbb{F}_q[X]$ is linearized and vanishes at any point of $\mathbb{F}_{q^n}$, it follows that $M(X+a) = M(X) + M(a) = M(X)$ for any $a \in \mathbb{F}_{q^n}$. From Proposition 2.9 there is a linearized polynomial $R \in \mathbb{F}_q[X]$ such that $M(X) = R(X^{q^n} - X)$, i.e., $M(X) = R(X) \otimes (X^{q^n} - X)$. Therefore,

$$L^{(t)}(X) = \underbrace{L(X) \otimes \cdots \otimes L(X)}_{t} = R(X) \otimes (X^{q^n} - X). \tag{4}$$

Since $R(X) \in \mathbb{F}_q[X]$, from Lemma 2.8 and Eq. (4) we conclude that

$$l(X)^t = (X^n - 1) r(X),$$

where $r(X)$ is the conventional q-associate of $R(X)$ and so $l(X)^t$ is divisible by $X^n - 1$.

Suppose that n is not divisible by p and there exist $t \geq 2$ and $L(X)$ such that $L(X) \in \mathbb{F}_q[X]$ is a t-NLP over $\mathbb{F}_{q^n}$. In particular, if $L_0(X) = \sum_{i=0}^{n-1} b_i X^i$ is the reduction of $L(X)$ modulo $X^{q^n} - X$, then $L_0(X) \in \mathbb{F}_q[X]$ is also a t-NLP over $\mathbb{F}_{q^n}$ and so $l_0(X) = \sum_{i=0}^{n-1} b_i X^i$, the conventional q-associate of $L_0(X)$, is such that $l_0(X)^t$ is divisible by $X^n - 1$. However, since n is not divisible by p, the polynomial $X^n - 1$ has only simple

roots and so we conclude that $l_0(X)$ is also divisible by X^n-1. Since $l_0(X)$ has degree at most $n-1$, it follows that $l_0(X)=0$, hence $L_0(X)=0$ and so $L(X)\equiv 0 \pmod{X^{q^n}-X}$, a contradiction. □

Theorem 2.10 suggests a method for the construction of t-NLP's over $\mathbb{F}_{q^n}$ in the case when n is divisible by p.

Corollary 2.11. *Let $t\geq 2$ be an integer, $p=\mathrm{char}(\mathbb{F}_{q^n})$ and $n=p^s u$, where $\gcd(u,p)=1$ and $s\geq 1$. Let $r(X)\in\mathbb{F}_q[X]$ be any nonzero polynomial of degree at most $v=n-1-u\cdot\left\lceil\frac{p^s}{t}\right\rceil$ and*

$$l_{r,t}(X)=r(X)(X^u-1)^{\left\lceil\frac{p^s}{t}\right\rceil}.$$

Then $L_{r,t}(X)\in\mathbb{F}_q[X]$, the linearized q-associate of $l_{r,t}(X)$, is a t-NLP over $\mathbb{F}_{q^n}$.

Proof. A direct calculation shows that $l_r(X)^t$ is divisible by X^n-1 and the degree of $l_r(X)$ is at most $n-1$. The result follows from Theorem 2.10. □

A simple investigation shows that $v=n-1-u\cdot\left\lceil\frac{p^s}{t}\right\rceil\geq 0$ if $n=p^s u$ and $t\geq 2$. The following example is a particular case of Corollary 2.11 when $r(X)=1$.

Example 2.12. Let $p=\mathrm{char}(\mathbb{F}_{q^n})$, $\alpha\in\mathbb{F}_q^*$ and $n=p^s u$, where $\gcd(u,p)=1$ and $s\geq 1$. The polynomial

$$L_{1,t}(X)=\sum_{i=0}^{d_{p,t}}(-1)^{d_{p,t}-i}\binom{d_{p,t}}{i}X^{q^{ui}}$$

is a t-NLP over $\mathbb{F}_{q^n}$, where $d_{p,t}=\left\lceil\frac{p^s}{t}\right\rceil$.

3. Constructing permutations via t-NLP's

In this section, we present a method for constructing permutation polynomials over $\mathbb{F}_{q^n}$ which are the sum of two polynomials, one of them being a t-NLP. Recall that a polynomial $f(X)\in\mathbb{F}_{q^n}[X]$ is a *permutation polynomial* over $\mathbb{F}_{q^n}$ if the map $c\mapsto f(c)$ induced by $f(X)$ on $\mathbb{F}_{q^n}$ is a permutation of $\mathbb{F}_{q^n}$. A permutation polynomial $f(X)$ is a *complete permutation* polynomial if $f(X)+X$ is also a permutation polynomial. The set $G(q^n)$ of the permutation polynomials over $\mathbb{F}_{q^n}$ is a group under the polynomial composition modulo $X^{q^n}-X$, and this group is isomorphic to the symmetric group S_{q^n} of permutations of q^n symbols. The identity element of $(G(q^n),\circ)$ is the identity map $g(X)=X$. For each $f\in G(q^n)$, $\mathcal{O}(f)$ denotes the order of f in the group $(G(q^n),\circ)$, i.e., $\mathcal{O}(f)=\min\{d>0\,|\,f^{(d)}(z)=z,\forall z\in\mathbb{F}_{q^n}\}$.

The following theorem gives an interesting relation between the t-NLP's and some permutation and complete permutation polynomials.

Theorem 3.1. *Let $p = \mathrm{char}(\mathbb{F}_{q^n})$. Let $L(X)$ be a t-NLP over $\mathbb{F}_{q^n}$ and $k(X)$ be any linearized permutation polynomial over $\mathbb{F}_{q^n}$ such that, under the ordinary polynomial composition, $k(X)$ commutes with $L(X)$, i.e.,*

$$k \circ L(X) = L \circ k(X).$$

Suppose that $s = \mathcal{O}(k)$. The following hold:

a) *$L(X)+k(X)$ is also a permutation polynomial over $\mathbb{F}_{q^n}$ and its compositional inverse map is given by*

$$\sum_{i=0}^{t-1}(-1)^i L^{(i)}(k^{(s-1-i)}(X)),$$

where $k^{(0)}(X) = L^{(0)}(X) = X$ and $s-1-i$ is taken modulo s;
b) *if $k(X)$ is a complete permutation polynomial, then so is $L(X)+k(X)$;*
c) *$\mathcal{O}(L+k)$ divides $\mathrm{lcm}(s, p^e)$, where $e = \lceil \log_p t \rceil$;*
d) *if $t = 2$ and $\gcd(s,p) = 1$, then $\mathcal{O}(L+k) = ps$.*

Proof. In the proof of this result and many others in this section we use the following identity:

$$(L+k)^{(p^l)}(z) = L^{(p^l)}(z) + k^{(p^l)}(z)$$

for any $z \in \mathbb{F}_{q^n}$ and $l \in \mathbb{N}$, which is the Frobenius identity in the case when $L(X)$ and $k(X)$ are commuting linearized polynomials over $\mathbb{F}_{q^n}$.

a) We observe that:

$$(L+k) \circ \left(\sum_{i=0}^{t-1}(-1)^i L^{(i)}(k^{(s-1-i)}(z)) \right) = \sum_{i=0}^{t-1}(-1)^i L^{(i+1)}(k^{(s-1-i)}(z)) +$$
$$\sum_{i=0}^{t-1}(-1)^i L^{(i)}(k^{(s-i)}(z)) = (-1)^{t-1} L^{(t)}(k^{(s-t)}(z)) + k^{(s)}(z) = 0 + z = z,$$

for any $z \in \mathbb{F}_{q^n}$. In particular, $L(X) + k(X)$ is a permutation over $\mathbb{F}_{q^n}$ and its compositional inverse is given by $\sum_{i=0}^{t-1}(-1)^i L^{(i)}(k^{(s-1-i)}(X))$.

b) If $k(X)$ is a complete permutation polynomial, then $K(X) = k(X) + X$ is a permutation polynomial. Additionally, item (a) shows that $L(X) + k(X)$ is a permutation polynomial. One can verify that $K \circ L(X) = L \circ K(X)$ and then, from item (a),

it follows that $K(X) + L(X)$ is a permutation polynomial, i.e., $L(X) + k(X)$ is a complete permutation polynomial.

c) Let $v = \mathcal{O}(L+k)$ and $u = \mathrm{lcm}(s, p^e)$, where $e = \lceil \log_p t \rceil$. We observe that $p^e \geq t$ and, in particular, $L^{(p^e)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$. Since $p = \mathrm{char}(\mathbb{F}_{q^n})$ and u is divisible by p^e and s, the following equality holds for any $z \in \mathbb{F}_{q^n}$:

$$(L+k)^{(u)}(z) = ((L+k)^{(p^e)})^{(u/p^e)}(z) = (L^{(p^e)} + k^{(p^e)})^{(u/p^e)}(z) = k^{(u)}(z) = z.$$

In particular, $\mathcal{O}(L+k) = v$ divides u.

d) Suppose that $t = 2$ and $\gcd(s, p) = 1$. In particular, $e = \lceil \log_p t \rceil = 1$ and item (c) shows that $v = \mathcal{O}(L+k)$ divides $u = \mathrm{lcm}(s, p) = ps$. Since $L^{(2)}(z) = 0$, for any $z \in \mathbb{F}_{q^n}$ and $d \in \mathbb{N}$, we have the following equality:

$$(L+k)^{(d)}(z) = dL(k^{(d-1)}(z)) + k^{(d)}(z).$$

This is a version of the Binomial Theorem in the in the case when $L(X)$ and $k(X)$ are commuting linearized polynomials over $\mathbb{F}_{q^n}$ and $L^{(2)}(z) = 0$ for any $z \in \mathbb{F}_{q^n}$. Since $\gcd(s, p) = 1$, if $v = \mathcal{O}(L+k)$ is not divisible by p, v is a divisor of s. Therefore,

$$z = (L+k)^{(s)}(z) = sL(k^{(s-1)}(z)) + k^{(s)}(z) = sL(k^{(s-1)}(z)) + z$$

or, equivalently, $sL(k^{(s-1)}(z)) = 0$ for any $z \in \mathbb{F}_{q^n}$. Since $k^{(s-1)}(z)$ is a permutation polynomial over $\mathbb{F}_{q^n}$ and s is not divisible by p, it follows that $L(z) = 0$ for any $z \in \mathbb{F}_{q^n}$, a contradiction with $L(X) \not\equiv 0 \pmod{X^{q^n} - X}$. Hence, p divides v and so $v = ps_0$ for some s_0. Therefore,

$$z = (L+k)^{(ps_0)}(z) = (L^{(p)} + k^{(p)})^{(s_0)}(z) = k^{(ps_0)}(z),\ z \in \mathbb{F}_{q^n}.$$

Since the equality above holds for any $z \in \mathbb{F}_{q^n}$, it follows that $s = \mathcal{O}(k)$ divides $ps_0 = v$. This shows that v is divisible by $u = \mathrm{lcm}(s, p) = ps$ and, since v divides $u = ps$ we conclude that $v = u = ps$. □

In a particular case when $k = \gamma X$ with $\gamma \in \mathbb{F}_q^*$, we have the following corollary.

Corollary 3.2. *Let $L(X)$ be a t-NLP over $\mathbb{F}_{q^n}$, $p = \mathrm{char}(\mathbb{F}_{q^n})$ and γ be any element of order s in the multiplicative group $\mathbb{F}_q^*$. The following hold:*

(i) *$L(X)+\gamma X$ is a permutation polynomial over $\mathbb{F}_{q^n}$ and its compositional inverse map is given by*

$$\sum_{i=0}^{t-1} \gamma^{s-1-i}(-1)^i L^{(i)}(X);$$

(ii) *if* $\gamma \neq -1$, $L + \gamma X$ *is a complete permutation polynomial;*
(iii) $\mathcal{O}(L + \gamma X)$ *divides* $p^e s$, *where* $e = \lceil \log_p t \rceil$ *and, for* $t = 2$, $\mathcal{O}(L + \gamma X) = ps$.

Proof. Since $\gamma \in \mathbb{F}_q^*$, it follows that γX is a permutation polynomial over $\mathbb{F}_{q^n}$, commutes with $L(X)$ and satisfies $\mathcal{O}(\gamma X) = \text{ord}(\gamma) = s$. Additionally, if γ is not -1, γX is a complete permutation polynomial. Finally, since $\text{ord}(\gamma) = s$ divides $q - 1$, $\gcd(s, p) = 1$ and $\text{lcm}(s, p^d) = p^d \cdot s$ for any $d \in \mathbb{N}$. Now, the results follow directly from Theorem 3.1. □

Example 3.3. Let $n = 2m$, let α and β be elements of $\mathbb{F}_{q^n}^*$ such that $\alpha^{q^m} + \alpha = 0$ and $\beta^{q^m+1} = 1$ and let γ be any element of $\mathbb{F}_q^*$. From Example 2.5 and Corollary 3.2, the polynomials

$$L_{\alpha,\beta,\gamma}(X) = (\alpha\beta X^{q^m} + \alpha X) + \gamma X$$

are permutation polynomials over $\mathbb{F}_{q^n}$, $\mathcal{O}(L_{\alpha,\beta,\gamma}) = p \cdot \text{ord}(\gamma)$ and the compositional inverse map of $L_{\alpha,\beta,\gamma}(X)$ is given by:

$$\gamma^{-1}X - \gamma^{-2}(\alpha\beta X^{q^m} + \alpha X).$$

From Corollary 2.11, we can construct a large class of permutation polynomials.

Corollary 3.4. *Let* $t \geq 2$ *be an integer,* $p = \text{char}(\mathbb{F}_{q^n})$ *and* $n = p^s u$, *where* $\gcd(u, p) = 1$ *and* $s \geq 1$. *Let* $r(X) \in \mathbb{F}_q[X]$ *be any nonzero polynomial of degree at most* $v = n - 1 - u \cdot \left\lceil \frac{p^s}{t} \right\rceil$ *and*

$$l_r(X) = r(X)(X^u - 1)^{\left\lceil \frac{p^s}{t} \right\rceil}.$$

Also, let $L_r(X) \in \mathbb{F}_q[X]$ *be the linearized* q*-associate of* $l_r(X)$ *and* α, β *be elements of* $\mathbb{F}_q^*$. *The polynomials*

$$L_{r,\alpha,\beta}(X) := L_r(X) + \alpha \text{Tr}_{q^n/q}(X) + \beta X,$$

are permutation polynomials over $\mathbb{F}_{q^n}$. *Moreover, for* $\beta \neq -1$, $L_{r,\alpha,\beta}(X)$ *is a complete permutation polynomial over* $\mathbb{F}_{q^n}$.

Proof. Since n is divisible by $p = \text{char}(\mathbb{F}_{q^n})$ and $\alpha \in \mathbb{F}_q^*$, a direct calculation shows that the polynomial $\alpha \text{Tr}_{q^n/q}(X)$ is a 2-NLP over $\mathbb{F}_{q^n}$. From Corollary 3.2, $\alpha \text{Tr}_{q^n/q}(X) + \beta X$ is a permutation over $\mathbb{F}_{q^n}$ and $\alpha \text{Tr}_{q^n/q}(X) + \beta X$ is also a complete permutation polynomial in the case when $\beta \neq -1$. From Corollary 2.11, $L_r(X)$ is a t-NLP over $\mathbb{F}_{q^n}$. But $L_r(X)$ and $\alpha \text{Tr}_{q^n/q}(X) + \beta X$ belong to $\mathbb{F}_q[X]$ and so these polynomials commute with each other. Now we apply Theorem 3.1 to $L = L_r(X)$ and $k = \alpha \text{Tr}_{q^n/q}(X) + \beta X$. □

In the notation of Corollary 3.4, we give explicit examples of permutation polynomials of the type $L_{r,\alpha,\beta}(X)$ over $\mathbb{F}_{2^6}$ and $\mathbb{F}_{3^3}$; see Table 1.

Table 1
Permutation polynomials $L_{r,1,1}$ over $\mathbb{F}_{2^6}$ $(t = 2)$ and $L_{r,1,-1}$ over $\mathbb{F}_{3^3}$ $(t = 3)$.

$r(X)$	$L_{r,1,1}(X)$
1	$X^{32} + X^{16} + X^4 + X^2 + X$
X	$X^{32} + X^8 + X^4$
$X + 1$	$X^{32} + X^4 + X$
X^2	$X^{16} + X^8 + X^2$
$X^2 + 1$	$X^{16} + X^2 + X$
$X^2 + X$	X^8
$X^2 + X + 1$	X

$r(X)$	$L_{r,1,-1}(X)$
1	$X^9 - X^3 - X$
-1	$X^9 + X$
X	$-X^9$
$-X$	$-X^3$
$X + 1$	$-X^9 + X^3 - X$
$X - 1$	$-X^9 - X^3 + X$
$-X + 1$	$X^3 + X$
$-X - 1$	$-X$

3.1. Cycle decomposition

If F is any function from a finite set S to itself, we can associate to it a directed graph $G(F, S)$ with vertex set S and edge set $\{(a, F(a))\}_{a\in S}$. The graph $G(F, S)$ is defined as the *functional graph* associated to F. If $f(X)$ is a permutation polynomial over $\mathbb{F}_{q^n}$, the graph $G_f := G(f, \mathbb{F}_{q^n})$ is decomposed into disjoint cycles; each cycle is isomorphic to a cyclic graph. The vertex of G_f associated to $a \in \mathbb{F}_{q^n}$ belongs to a cycle of length d if, and only if, d is the least positive integer such that $f^{(d)}(a) = a$. Moreover, the number $\mathcal{O}(f)$ previously defined is just the least common multiple of the cycle lengths in G_f. The cycle decomposition of G_f plays an important role in the theory of permutation polynomials. In [5], the cycle decomposition of certain linearized permutation polynomials is given.

If $L(X)$ and $k(X)$ are linearized polynomials over $\mathbb{F}_{q^n}$ as in Theorem 3.1, we know that $L(X) + k(X)$ is a permutation polynomial over $\mathbb{F}_{q^n}$. We ask if there is any relation between the functional graphs G_k and G_{L+k}. In the case when $L(X)$ is a 2-NLP over $\mathbb{F}_{q^n}$, the following theorem shows that the cycle lengths of G_{L+k} cannot be much larger than the ones of G_k and, with an additional condition on $\mathcal{O}(k)$, we can completely describe the cycle decomposition of G_{L+k} from G_k.

Theorem 3.5. *Let L be a 2-NLP over $\mathbb{F}_{q^n}$ and let k be any linearized permutation polynomial over $\mathbb{F}_{q^n}$ such that $k \circ L(X) = L \circ k(X)$. Set $s = \mathcal{O}(k)$ and $p = \mathrm{char}(\mathbb{F}_{q^n})$. Suppose that the vertex associated to $a \in \mathbb{F}_{q^n}$ belongs to cycles of lengths m_a and m'_a in G_k and G_{L+k}, respectively. The following hold:*

a) *m'_a divides $\mathrm{lcm}(m_a, p)$ and, if $L(a) = 0$, then $m_a = m'_a$;*
b) *if $\gcd(s, p) = 1$, then* $m'_a = \begin{cases} m_a & \text{if } \ L(a) = 0, \\ pm_a & \text{otherwise.} \end{cases}$

Proof.

a) Let $v = \mathrm{lcm}(m_a, p)$. We observe that

$$(L + k)^{(v)}(z) = (L^{(p)} + k^{(p)})^{(v/p)}(z) = k^{(v)}(z), z \in \mathbb{F}_{q^n}.$$

Since m_a divides v, it follows that $k^{(v)}(a) = a$, hence $(L+k)^{(v)}(a) = a$ and so m'_a divides v. If $L^{(2)}(z) = 0$, recall that $(L+k)^{(d)}(z) = dk^{(d-1)}(L(z)) + k^{(d)}(z)$ for any $d \in \mathbb{N}$ and $z \in \mathbb{F}_{q^n}$. Therefore, if $L(a) = 0$, $(L+k)^{(d)}(a) = k^{(d)}(a)$. In particular, $m'_a = m_a$ if $L(a) = 0$.

b) If $L(a) = 0$, item (a) shows that $m_a = m'_a$. Suppose that $L(a) \neq 0$ and that m'_a is not divisible by p. It follows from item (a) that m'_a divides m_a and then

$$a = (L+k)^{(m_a)}(a) = m_a L(k^{(m_a-1)}(a)) + k^{m_a}(a) = m_a k^{(m_a-1)}(L(a)) + a,$$

hence $m_a k^{(m_a-1)}(L(a)) = 0$. Now, since $\gcd(s,p) = 1$ and m_a divides s, it follows that m_a is not divisible by p, hence $k^{(m_a-1)}(L(a)) = 0$. Observe that $k^{(m_a-1)}(X)$ is a linearized permutation polynomial and so the only preimage of $0 \in \mathbb{F}_{q^n}$ is the element 0. Since $L(a) \neq 0$, it follows that the composition $k^{(m_a-1)}(L(a))$ is never zero and so we get a contradiction. Hence, p divides m'_a and so there exists an integer u such that $m'_a = pu$. Therefore

$$a = (L+k)^{(pu)}(a) = (L^{(p)} + k^{(p)})^{(u)}(a) = k^{(pu)}(a),$$

and so m_a divides pu. Since m_a is not divisible by p it follows that m_a divides u, hence pm_a divides $pu = m'_a$. Item (a) shows that m'_a divides $\operatorname{lcm}(m_a, p) = pm_a$ and so $m'_a = pm_a$. □

In the case when $k(X) = \gamma X$ for some $\gamma \in \mathbb{F}_q^*$, we can determine precisely the graphs G_{L+k}.

Corollary 3.6. *Let $L(X)$ be a 2-NLP over $\mathbb{F}_{q^n}$ and γ be an element of order s in the multiplicative group $\mathbb{F}_q^*$. Then the functional graph $G_{L+\gamma X}$ has one cycle of length 1, $\frac{z_L - 1}{s}$ cycles of length s and $\frac{q^n - z_L}{ps}$ cycles of length ps, where $z_L = \#Z_L$ is the number of roots of L in $\mathbb{F}_{q^n}$. In particular, if L_1 and L_2 are 2-NLP's over $\mathbb{F}_{q^n}$ and $\gamma_1, \gamma_2 \in \mathbb{F}_q^*$, the graphs $G_{L_1+\gamma_1 X}$ and $G_{L_2+\gamma_2 X}$ have the same cycle decomposition (hence isomorphic) if, and only if, $z_{L_1} = z_{L_2}$ and $\operatorname{ord}(\gamma_1) = \operatorname{ord}(\gamma_2)$.*

Proof. For the first statement, notice that any nonzero element belongs to a cycle of length s in $G_{\gamma X}$ and the zero element is a fixed point. Since $\mathcal{O}(\gamma X) = s$ and s divides $q-1$, we have that $\gcd(d,p) = 1$ and now the result follows from item (b) of Theorem 3.5. The second statement follows directly from the first. □

3.2. Involutions in binary fields

Here we are interested in the construction of involutions over binary fields with no fixed points. Let q be a power of 2 and $L(X)$ be any 2-NLP over $\mathbb{F}_{q^n}$. From Theorem 3.1, we know that $L(X) + X$ is a permutation polynomial over $\mathbb{F}_{q^n}$ and it can be verified

that $L(X)+X$ is, in fact, an involution over $\mathbb{F}_{q^n}$. However, $L(X)+X$ has many fixed points: the fixed points are the roots of $L(X)$ over $\mathbb{F}_{q^n}$. The following proposition shows how to eliminate those fixed points.

Proposition 3.7. *Let $\mathbb{F}_{q^n}$ be a finite field such that $\mathrm{char}(\mathbb{F}_{q^n})=2$ and $L(X)$ be any 2-NLP over $\mathbb{F}_{q^n}$ such that $V_L \subsetneq Z_L$. Then, for any $a \in Z_L \setminus V_L$, $f(X)=L(X)+X+a$ is an involution over $\mathbb{F}_{q^n}$ with no fixed points. Additionally, if $\dim_{\mathbb{F}_q} V_L < n/2$, there exists an element $b \in Z_L \setminus V_L$.*

Proof. Since $L(a)=0$ and $\mathrm{char}(\mathbb{F}_{q^n})=2$, a direct calculation shows that $f(X)=L(X)+X+a$ is an involution over $\mathbb{F}_{q^n}$. If $f(X)$ has a fixed point $\alpha \in \mathbb{F}_{q^n}$, then $f(\alpha)=\alpha$ and so $L(\alpha)=a$, which is impossible since $a \notin V_L$. Therefore, $f(X)$ has no fixed points.

Since $L^{(2)}(z)=0$ for any $z \in \mathbb{F}_{q^n}$, we have that $V_L \subseteq Z_L$. If $\dim_{\mathbb{F}_q} V_L < n/2$ then $\dim_{\mathbb{F}_q} Z_L = n - \dim_{\mathbb{F}_q} V_L > n/2$ and so $V_L \subsetneq Z_L$. In particular, there is some element $b \in Z_L \setminus V_L$. □

We have the following corollary.

Corollary 3.8. *Let q be a power of 2 and let $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ be finite extensions of $\mathbb{F}_q$ such that $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ and $m < n/2$. If θ is an element of $\mathbb{F}_{q^n}^*$ such that $\mathrm{Tr}_{q^n/q^m}(\theta)=0$, then there exists an element $\alpha \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^m}(\alpha)=0$ and $\alpha \notin \theta \cdot \mathbb{F}_{q^m}$. In particular,*

$$f(X)=\theta \cdot \mathrm{Tr}_{q^n/q^m}(X)+X+\alpha=\theta \cdot \sum_{i=1}^{\frac{n}{m}-1} X^{q^i}+(\theta+1)X+\alpha$$

is an involution over $\mathbb{F}_{q^n}$ with no fixed points.

Proof. In the notation of Proposition 3.7, take $L(X)=\theta \cdot \mathrm{Tr}_{q^n/q^m}(X)$. We observe that $L(X)$ is a 2-NLP over $\mathbb{F}_{q^n}$ and $V_L=\theta \cdot \mathbb{F}_{q^m}$ is an $\mathbb{F}_q$-vector space of dimension $m < n/2$. Now the result follows directly from Proposition 3.7. □

The corollary above suggests explicit constructions of involutions with no fixed points which can be represented by *sparse polynomials*, i.e., polynomials with few nonzero coefficients. For instance, let m be any positive integer and $n=4m$. If $f(X)$ is any irreducible polynomial over $\mathbb{F}_2$ of degree n, then $\mathbb{F}_{2^n}=\mathbb{F}_2[X]/(f(X))=\mathbb{F}_2[\beta]$, where β is the coset of X in the quotient $\mathbb{F}_2[X]/(f(X))$. Consider the following trace function:

$$\mathrm{Tr}_{2^n/2^m}(X)=X^{2^{3m}}+X^{2^{2m}}+X^{2^m}+X.$$

A direct calculation shows that $\mathrm{Tr}_{2^n/2^m}(1)=\mathrm{Tr}_{2^n/2^m}(\beta^{2^m}+\beta)=0$. But if $\beta^{2^m}+\beta \in \mathbb{F}_{2^m}$, it follows that $\beta^{2^{2m}}=\beta$, i.e., $\beta \in \mathbb{F}_{2^{2m}}$. Therefore, $\mathbb{F}_{2^n}=\mathbb{F}_2[\beta] \subset \mathbb{F}_{2^{2m}}$, a contradiction

since $n = 4m$. In conclusion, $\beta^{2^m} + \beta \notin \mathbb{F}_{2^{2m}}$ and so, if we take $\alpha = \beta^{2^m} + \beta$ and $\theta = 1$ in Corollary 3.8, we have that

$$f(X) = X^{2^{3m}} + X^{2^{2m}} + X^{2^m} + \beta^{2^m} + \beta$$

is an involution over $\mathbb{F}_{2^n} = \mathbb{F}_2[\beta]$ with no fixed points.

Example 3.9. Let $\mathbb{F}_{2^{32}} = \mathbb{F}_2[\beta]$, where β is the coset of X in the quotient $\mathbb{F}_2[X]/(f)$ and $f(X) = X^{32} + X^7 + X^3 + X + 1$. The polynomial $f(X) = X^{2^{24}} + X^{2^{16}} + X^{2^8} + \beta^{2^8} + \beta$, is an involution over $\mathbb{F}_{2^{32}}$ and has no fixed points.

4. Conclusions and future work

In this paper, we introduce the class of *nilpotent linearized polynomials* over finite fields and give a partial characterization of such polynomials. We describe a method for constructing permutations of finite fields from the *nilpotent linearized polynomials* and, for some special permutations, we determine the cycle decomposition and the compositional inverse map.

We present two further problems motivated by theoretical considerations.

Problem 4.1. Obtain a complete characterization of nilpotent linearized polynomials over finite fields.

Problem 4.2. Obtain a generalization of Theorem 3.5 for t-NLP's.

Acknowledgments

I would like to thank Michel Spira for some helpful suggestions in the preparation of this work.

References

[1] C. Boura, A. Canteaut, L.R. Knudsen, et al., Reflection ciphers, Des. Codes Cryptogr. 82 (2017) 3–25.
[2] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (2007) 58–70.
[3] R. Lidl, L. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, New York, NY, USA, 1986.
[4] G.L. Mullen, D. Panario, Handbook of Finite Fields, Taylor and Francis, Boca Raton, 2013.
[5] G.L. Mullen, T.P. Vaughan, Cycles of linear permutations over a finite field, Linear Algebra Appl. 108 (1988) 63–82.
[6] J. Schwenk, K. Huber, Public key encryption and digital signatures based on permutation polynomials, Electron. Lett. 34 (1998) 759–760.