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 xxxx
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/© 2017 Elsevier Inc. All rights reserved.

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

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