Finite Fields and Their Applications 49 (2018) 156–165

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Carlitz rank and index of permutation polynomials

Leyla Işık [a,*], Arne Winterhof [b]

[a] *Salzburg University, Hellbrunnerstr. 34, 5020 Salzburg, Austria*
[b] *Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria*

ARTICLE INFO

Article history:
Received 19 November 2016
Received in revised form 14 March 2017
Accepted 7 September 2017
Available online xxxx
Communicated by Xiang-dong Hou

MSC:
11T06
11T24
11T41
11T71

Keywords:
Carlitz rank
Character sums
Cryptography
Finite fields
Index
Invertibility
Linearity
Permutation polynomials
Cyclotomic mappings
Discrete logarithm

ABSTRACT

Carlitz rank and index are two important measures for the complexity of a permutation polynomial $f(x)$ over the finite field $\mathbb{F}_q$. In particular, for cryptographic applications we need both, a high Carlitz rank and a high index. In this article we study the relationship between Carlitz rank $Crk(f)$ and index $Ind(f)$. More precisely, if the permutation polynomial is neither close to a polynomial of the form ax nor a rational function of the form ax^{-1}, then we show that $Crk(f) > q - \max\{3Ind(f), (3q)^{1/2}\}$. Moreover we show that the permutation polynomial which represents the discrete logarithm guarantees both a large index and a large Carlitz rank.

* Corresponding author.
E-mail addresses: leyla.isik@sbg.ac.at (L. Işık), arne.winterhof@oeaw.ac.at (A. Winterhof).

http://dx.doi.org/10.1016/j.ffa.2017.09.002
1071-5797/

1. Introduction

In 1953, L. Carlitz [2] proved that all permutation polynomials over the finite field $\mathbb{F}_q$ of order $q \geq 3$ are compositions of linear polynomials $ax + b$, $a, b \in \mathbb{F}_q$, $a \neq 0$, and inversions $x^{q-2} = \begin{cases} 0, & x = 0, \\ x^{-1}, & x \neq 0, \end{cases}$ see [2] or [5, Theorem 7.18]. Consequently, any permutation of $\mathbb{F}_q$ can be represented by a polynomial of the form

$$P_n(x) = (\dots((c_0x + c_1)^{q-2} + c_2)^{q-2} \dots + c_n)^{q-2} + c_{n+1}, \tag{1}$$

where $c_i \neq 0$, for $i = 0, 2, \dots, n$. (Note that c_1c_{n+1} can be zero.) This representation is not unique and n is not necessarily minimal. We recall that the *Carlitz rank* $Crk(f)$ of a permutation polynomial $f(x)$ over $\mathbb{F}_q$ is the smallest integer $n \geq 0$ satisfying $f(x) = P_n(x)$ for a permutation polynomial $P_n(x)$ of the form (1). The Carlitz rank was first introduced in [1] and further studied in [3,4]. For a survey see [10].

In 2009, Aksoy et al. [1] showed

$$Crk(f) \geq q - \deg(f) - 1 \quad \text{if } \deg(f) \geq 2. \tag{2}$$

In [3] Gomez-Perez et al. gave a similar bound for $Crk(f)$ in terms of the weight $w(f)$ of $f(x)$, that is the number of its nonzero coefficients. If $f(x) \neq a + bx^{q-2}$, for all $a, b \in \mathbb{F}_q$, $b \neq 0$, then

$$Crk(f) > \frac{q}{w(f) + 2} - 1 \quad \text{if } \deg(f) \geq 2. \tag{3}$$

In this paper, we study the relationship between the Carlitz rank and the least index of a polynomial introduced in [8,12] as follows.

Let ℓ be a positive divisor of $q - 1$ and ξ a primitive element of $\mathbb{F}_q$. Then the set of nonzero ℓth powers

$$C_0 = \left\{ \xi^{j\ell} : j = 0, 1, ..., \frac{q-1}{\ell} - 1 \right\}$$

is a subgroup of $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ of index ℓ. The elements of the factor group $\mathbb{F}_q^*/C_0$ are the *cyclotomic cosets*

$$C_i = \xi^i C_0, \quad i = 0, 1, ..., \ell - 1.$$

For any positive integer r and any $a_0, a_1, ..., a_{\ell-1} \in \mathbb{F}_q^*$, we define the *$r$-th order cyclotomic mapping $f^r_{a_0,a_1,...,a_{\ell-1}}$ of index ℓ* by

$$f^r_{a_0,a_1,...,a_{\ell-1}}(x) = \begin{cases} 0 & \text{if } x = 0, \\ a_i x^r & \text{if } x \in C_i,\ 0 \leq i \leq \ell - 1. \end{cases} \tag{4}$$