Finite Fields and Their Applications 47 (2017) 330–350

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Ambiguity, deficiency and differential spectrum of normalized permutation polynomials over finite fields

Daniel Panario [a,1], Daniel Santana [b,2], Qiang Wang [a,*,1]

[a] *School of Mathematics and Statistics, Carleton University, Canada*
[b] *Department of Informatics and Statistics, Federal University of Santa Catarina, Brazil*

ARTICLE INFO

Article history:
Received 23 August 2016
Received in revised form 6 March 2017
Accepted 14 June 2017
Available online xxxx
Communicated by Gary McGuire

MSC:
12Y05
11T99

Keywords:
Finite fields
Permutation polynomials
Normalized polynomials
Differential map
Spectrum
Ambiguity
Deficiency

ABSTRACT

We obtain exact formulas for the differential spectrum, deficiency and ambiguity of all normalized permutation polynomials of degree up to six over finite fields.

[*] Corresponding author.
E-mail addresses: daniel@math.carleton.ca (D. Panario), santana.d@ufsc.br (D. Santana), wang@math.carleton.ca (Q. Wang).

[1] These authors are supported in part by NSERC of Canada.

[2] This work was developed while the second author was visiting the School of Mathematics and Statistics at Carleton University. The second author was supported by a scholarship from the Brazilian Research Council (CNPq – Brazil), Grant number 201601/2015-3.

http://dx.doi.org/10.1016/j.ffa.2017.06.003
1071-5797/© 2017 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, where q is a prime power, and let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function. If f induces a bijection, f is a *permutation polynomial*. Permutation polynomials have been largely studied since the 19th century. There has been a revival on the interest on permutation polynomials in the last 30 years due in part to their applications in several areas, including cryptography and combinatorics. For more information on permutation polynomials see [5, Chapter 7], [6, Chapter 8], and the recent survey [2].

The set of permutation polynomials of $\mathbb{F}_q$ is closed under composition; in particular, if f is a permutation polynomial of $\mathbb{F}_q$, the polynomial $g(x) = cf(x+b)+d$ is a permutation polynomial of $\mathbb{F}_q$ for all choices of $b, c, d \in \mathbb{F}_q$, $c \neq 0$. A permutation polynomial $f \in \mathbb{F}_q[x]$ is in *normalized* form if f is monic, $f(0) = 0$, and when the degree n of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is zero. Normalized permutation polynomials are known up to degree six. A list of all normalized permutation polynomials of degree less than six, taken from [5, Section 7.1], can be found in Table 12. The characterization of all normalized permutation polynomials of degree six is more recent [12] and can be found in Table 13. For related material on low degree permutation polynomials, see [4] for all permutation polynomials of degree six and seven over finite fields with even characteristic. In this paper, we focus on all normalized permutation polynomials of degree up to six.

For $f : \mathbb{F}_q \to \mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, the difference map of f is defined as

$$\Delta_{f,a}(x) = f(x+a) - f(x).$$

This can indeed be defined for any map between any two Abelian groups of the same size but here we focus on the case where f is a permutation polynomial over a finite field. The difference map plays a central role in several applications, including, most noticeably, differential cryptanalysis [1,7]. This map measures the degree of linearity of f. The function f is perfect non-linear (PN) if $\Delta_{f,a}$ is injective, and almost perfect non-linear (APN) if $\Delta_{f,a}$ is at worst 2-to-1. In cryptographic applications, to resist linear and differential cryptanalysis, we want functions $f : \mathbb{F}_q \to \mathbb{F}_q$ that are permutations and such that $\lambda_{a,b} = |\Delta_{f,a}^{-1}(b)|$ is low for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. We define

$$n_k(f) = \left|\left\{(a,b) : |\Delta_{f,a}^{-1}(b)| = k\right\}\right|, \quad 0 \le k \le q.$$

That is, $n_k(f)$ is the number of pairs (a, b) such that $f(x + a) - f(x) = b$ has exactly k solutions. The vector $[n_0(f), \dots, n_q(f)]$ is the *spectrum* vector of the difference map of f. The spectrum gives precise information on the difference map of f and its potential uses in cryptography. Other related measures have been defined [9,10]. The *deficiency* of f, denoted by $D(f)$, is defined as $D(f) = n_0(f)$ and it measures how close the $\Delta_{f,a}$'s are to be surjective. The *(weighted) ambiguity* of f, denoted by $A(f)$, is defined as