Journal of Computational and Applied Mathematics 259 (2014) 536–545

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Permutations of finite fields with prescribed properties

Ayça Çeşmelioğlu [a,b], Wilfried Meidl [b,*], Alev Topuzoğlu [b]

[a] Otto-von-Guericke-University, Faculty of Mathematics, 39106 Magdeburg, Germany
[b] Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey

ARTICLE INFO

Article history:
Received 15 February 2013
Received in revised form 31 May 2013

Keywords:
Permutation polynomial
Cycle decomposition
APN permutation
Differential uniformity
Dispersion
Costas permutation

ABSTRACT

Classes of permutations of finite fields with various specific properties are often needed for applications. We use a recent classification of permutation polynomials using their Carlitz rank with advantage, to produce examples of classes of permutations of $\mathbb{F}_p$, for odd p, which for instance are "random", have low differential uniformity, prescribed cycle structure, high polynomial degree, large weight and large dispersion. They are also easy to implement. We indicate applications in coding and cryptography.

1. Introduction

Permutation polynomials over finite fields have attracted significant attention in the last decades, due to their vast applications, especially in combinatorics, cryptography, coding and pseudorandom number generation. Naturally, methods of construction of various types of permutations and/or new ways of classifying them are needed in order to meet the specific requirements of individual applications. Here we present classes of permutations of finite fields $\mathbb{F}_q$, $q = p^r$, $r \geq 1$, for odd primes p, which possess a variety of properties that can be advantageous for diverse applications.

Permutations with low differential uniformity, for instance, are sought for to be used in symmetric cryptography since they provide good resistance to differential attacks, see [1–3]. We recall that the differential uniformity δ_f of a function f from a finite field $\mathbb{F}_q$ to itself is determined by properties of the difference map $D_{f,a}(x) = f(x + a) - f(x), a \in \mathbb{F}_q^*$; i.e., $\delta_f = \max_{a\in\mathbb{F}_q^*, b\in\mathbb{F}_q} \delta_f(a, b)$, where $\delta_f(a, b) = \#\{x \in \mathbb{F}_q, D_{f,a}(x) = b\}$. One would also need such permutations to be implemented easily, hence usually sparse polynomials are studied, for example in [4–6]. Our approach provides examples with added polynomial complexity, i.e., high degree and large weight, yet they can still be implemented easily. We note that while most cryptosystems use Boolean functions or permutations of finite fields of characteristic two, there is an increasing interest in permutations of finite fields of odd characteristic or bijections between finite groups of the same cardinality also, for details we refer the reader to [1,2,7] and references therein. The concepts of ambiguity and deficiency of permutations between two finite abelian groups of the same cardinality, which concern the difference map are introduced and permutations with optimal behavior with respect to these measures are studied in [8,9], see Remark 3.2 below for further comments. Costas permutations, which are interesting combinatorial objects were first introduced for applications and the corresponding difference map shows an extreme behavior, as we explain in Section 2. The relationship between almost perfect nonlinear (APN) and Costas permutations of the rings $\mathbb{Z}_n$ has been first investigated in [10]. We also explore this relationship and provide evidence supporting the description of [10], that it is "quite erratic". For small primes we give

* Corresponding author. Tel.: +90 2164839583.
E-mail address: wmeidl@sabanciuniv.edu (W. Meidl).

0377-0427/$ – see front matter
http://dx.doi.org/10.1016/j.cam.2013.07.036

examples of almost Costas permutations, in a sense that we describe below. Permutations with a particular cycle structure are of importance in turbo-like coding or low-density-parity-check codes (LDPC), see [11–13]. Those which decompose into cycles of length two for instance are their own inverses, and hence the same procedure for encoding can be used for decoding. "Random" permutations with prescribed cycle structure are of particular interest for use as interleavers in turbo codes.

We use two basic tools to relate various favorable properties of permutations of $\mathbb{F}_q$ and obtain classes with such attributes. Our first tool is the classification of permutation polynomials with respect to their Carlitz rank. We recall that S_q, the symmetric group on q letters, is isomorphic to the group of permutation polynomials of $\mathbb{F}_q$ of degree less than q, under the operation of composition and subsequent reduction modulo $x^q - x$. A well known result of Carlitz [14] states that S_q is generated by the linear polynomials $ax + b$, for $a, b \in \mathbb{F}_q$, $a \neq 0$, and x^{q-2}. Consequently, as pointed out in [15], with $\mathcal{P}_0(x) = a_0x + a_1$, any permutation $\mathcal{P}$ of $\mathbb{F}_q$ can be represented by a polynomial of the form

$$\mathcal{P}_n(x) = (\cdots((a_0x + a_1)^{q-2} + a_2)^{q-2} \cdots + a_n)^{q-2} + a_{n+1}, \quad n \geq 0, \tag{1}$$

where $a_1, a_{n+1} \in \mathbb{F}_q$, $a_i \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ for $i = 0, 2, \ldots, n$.

The Carlitz rank of $\mathcal{P}$, denoted as $\mathrm{Crk}(\mathcal{P})$, is defined in [16] to be the smallest integer $n \geq 0$ satisfying $\mathcal{P} = \mathcal{P}_n$ for a permutation $\mathcal{P}_n$ of the form (1). Our second tool is the so called dispersion. Dispersion is also concerned with the difference map and for a permutation P of the set $\{0, 1, \ldots, n-1\}$, it is defined as the cardinality of the set $\{(j - i, P(j) - P(i)) | 0 \leq i < j \leq n-1\}$. This concept has been in use as a randomness measure of permutations for their possible use as interleavers in turbo codes, see [17].

This paper is organized as follows. After giving preliminaries in Section 2, we focus on evaluation in Section 3 of dispersion of permutations of Carlitz rank 1, and show that with an appropriate choice of parameters, these polynomials provide the first examples having provably high dispersion, and hence can be considered as "random". Indeed only a few non-empirical results on the dispersion of permutations of finite fields have appeared so far, in connection with coding theoretical applications, and only about monomials, see [18,19]. In Section 4 we characterize and enumerate permutations of Carlitz rank 1 with prescribed dispersion and cycle decomposition. Section 5 focuses on permutations of Carlitz rank > 1. We complete this work by presenting results on the differential uniformity of permutations of small Carlitz rank in Section 6.

2. Preliminaries

We start by recalling that a permutation π_c of $\{0, 1, \ldots, n-1\}$ is called a Costas permutation (or a Costas array) if for every $0 \leq i, j, k, i + k, j + k \leq n - 1$,

$$\pi_c(i + k) - \pi_c(i) = \pi_c(j + k) - \pi_c(j)$$

implies $k = 0$ or $i = j$. For an extensive review of literature on Costas permutations, together with its applications we refer to [20,21].

Drakakis et al. consider permutations with the following stronger properties in [10]. A permutation π of $\{0, 1, \ldots, n-1\}$ is called a *range (R-) periodic Costas permutation* if for every $0 \leq i, j, k, i + k, j + k \leq n - 1$,

$$(\pi(i + k) - \pi(i)) \bmod n = (\pi(j + k) - \pi(j)) \bmod n \tag{2}$$

implies $k = 0$ or $i = j$. Similarly π is called a *domain-and-range (DR-) periodic Costas permutation* if (2) is replaced by

$$(\pi((i + k) \bmod n) - \pi(i)) \bmod n = (\pi((j + k) \bmod n) - \pi(j)) \bmod n. \tag{3}$$

Hence a DR-periodic Costas permutation permutes the ring $\mathbb{Z}_n$. As it is proved in [10], R-periodic Costas permutations of $\{0, 1, \ldots, n-1\}$ do not exist if n is odd. Therefore there are no DR-periodic Costas permutations of a finite field $\mathbb{F}_p$, $p > 2$.

As usual we identify the finite field $\mathbb{F}_p$ with $\{0, 1, \ldots, p-1\}$. We need to calculate both in $\mathbb{Z}$ and in $\mathbb{F}_p$, and in order to avoid confusion, we denote addition and subtraction in $\mathbb{F}_p$ by "$\oplus$", and "$\ominus$". With this notation $P \in \mathbb{F}_p[x]$ is a (DR-) Costas permutation if

$$P(i \oplus k) \ominus P(i) = P(j \oplus k) \ominus P(j)$$

implies $k = 0$ or $i = j$, for all $i, j, k, i \oplus k, j \oplus k \in \mathbb{F}_p$.

Difference triangles are often used to help visualizing the Costas property and similar combinatorial concepts. We also utilize them to describe the results of this paper in a simple way.

Recall that a difference triangle of a permutation $P \in \mathbb{F}_p[x]$ is a triangular array $DT(P)$ of integers, which has $p - 1$ *rows* $T_1(P), \ldots, T_{p-1}(P)$, where $T_k(P)$ is the vector

$$T_k(P) = (P(k) - P(0), P(1 + k) - P(1), \ldots, P(p - 1) - P(p - k - 1)),$$

for $k = 1, \ldots, p - 1$. Calculating in $\mathbb{F}_p$, we obtain a p-difference triangle $DT_p(P)$ of P, whose rows are:

$$T_{p,k}(P) = (P(k) \ominus P(0), P(1 \oplus k) \ominus P(1), \ldots, P(p \ominus 1) \ominus P(p \ominus k \ominus 1)),$$