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:

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

for $k = 1, \ldots, p-1$. We denote the number of distinct integers appearing in $T_k(P)$ by $|T_k(P)|$ and distinct elements appearing in $T_{p,k}(P)$ by $\left|T_{p,k}(P)\right|$. Note that a permutation P has the Costas property if and only if each row of its difference triangle $DT(P)$ consists of distinct integers. Since no R-periodic Costas permutations of $\{0, 1, \ldots, p-1\}$ exist, there is no permutation of $\mathbb{F}_p$, with distinct values in each row of its p-difference triangle.

Note that for such permutations P, the equation $P(x \oplus a) \ominus P(x) = b$ has at most two solutions for all $a, b \in \mathbb{F}_p$, $a \neq 0$, in other words they are APN. Therefore for an APN permutation P, any element in each row of $DT_p(P)$ (and hence of $DT(P)$) appears at most twice. If in addition one can control the number of repeating elements in each row of $DT(P)$, one can obtain interesting combinatorial objects, which almost have Costas property since P is Costas if no element repeats in a row of $DT(P)$. We use dispersion to quantify this argument.

We put $\left|D(P, \mathbb{F}_p)\right| = \sum_{k=1}^{p-1} \left|T_{p,k}(P)\right|$ and $|D(P)| = \sum_{k=1}^{p-1} |T_k(P)|$. The reader can see easily that the latter quantity coincides with the dispersion of P, that we defined in Section 1. With our notation introduced above, we write $D(P) = \{(k, P(i \oplus k) - P(i)) | 1 \leq k \leq p-1, 0 \leq i \leq p-1-k\}$. Since we study permutations of $\mathbb{F}_p$, we focus on evaluating $\left|D(P, \mathbb{F}_p)\right|$ also, which we call the *p-dispersion*.

Clearly a Costas permutation of $\{0, 1, \ldots, p-1\}$ has (maximum possible) dispersion $p(p-1)/2$. Accordingly the normalized dispersion is defined as

$$\gamma(P) = \frac{2\,|D(P)|}{p(p-1)},$$

and hence $\gamma(P) \leq 1$ for any permutation P of $\mathbb{F}_p$. We note that the expected value of the normalized dispersion of a random permutation is approximately 0.8, see [18,19,17]. Accordingly $\gamma(P)$ is used as a randomness measure, see Section 3.6.4 in [17]. More precisely a permutation P is considered as being random (and hence as a favorable interleaver) if $\gamma(P)$ is close to 0.8. Earlier results on dispersion are only about monomials. It is easy to see that $|D(P)| = \left|D(P, \mathbb{F}_p)\right|$ in case of a monomial. However these values may differ considerably when P is an arbitrary permutation.

In the next section, among other results we show that when $p \equiv 5 \bmod 6$, and $\mathcal{P}$ is a permutation of Carlitz rank 1, $\gamma(\mathcal{P})$ attains the value $3/4 + 5/4p$ for $a_2 = 0$, $-a_1/a_0 = \lfloor \frac{p-1}{4} \rfloor$ or $\lfloor \frac{3p-1}{4} \rfloor \bmod p$. Hence an appropriate choice of $\mathcal{P}$ ensures $\gamma(\mathcal{P})$ to be close to 0.8, yielding "random" permutations, or good candidates for use in turbo codes as interleavers. A lower bound for $\gamma(\mathcal{P})$, when $\mathrm{Crk}(\mathcal{P}) = 1$ is also given below, which is ≈ 0.5. This value is close to that of monomials.

3. Dispersion of permutations of Carlitz rank 1

Throughout this and the next sections $\mathcal{P}$ denotes a permutation of $\mathbb{F}_p$ of Carlitz rank 1, i.e., $\mathcal{P} = (a_0 x \oplus a_1)^{p-2} \oplus a_2$. We first give an exact formula for the p-dispersion $\left|D(\mathcal{P}, \mathbb{F}_p)\right|$, when $p \equiv 5 \bmod 6$. We then evaluate $|D(\mathcal{P})|$ when $a_2 = 0$.

In what follows, the element $\ominus \frac{a_1}{a_0}$ of the prime field $\mathbb{F}_p$, which is the *pole* of the polynomial $\mathcal{P} \in \mathbb{F}_p[x]$, is denoted by x_p. As it turns out, the integer in $\{0, 1, \ldots, p-1\}$, which x_p is identified with, plays an important role in the real valued formulae for the dispersion. Naturally this integer then has to be dealt with as a real number. To indicate which arithmetic has to be applied, we denote this integer by x_I.

Lemma 3.1. *Let $p \equiv 5 \bmod 6$. For a fixed k, $1 \leq k \leq p-1$, and $i \neq j$*

$$\mathcal{P}(i \oplus k) \ominus \mathcal{P}(i) = \mathcal{P}(j \oplus k) \ominus \mathcal{P}(j) \tag{4}$$

if and only if $i \oplus j \oplus k = 2x_p$.

Proof. First we consider the case $i = x_p$ or $i \oplus k = x_p$.

We observe that in both cases we have

$$\mathcal{P}(i \oplus k) \ominus \mathcal{P}(i) = \frac{1}{a_0 k}.$$

Consequently if $i = x_p$ (thus $i \oplus k, j$ are both different from x_p) and $j \oplus k = x_p$, we have

$$\mathcal{P}(i \oplus k) \ominus \mathcal{P}(i) = \mathcal{P}(j \oplus k) \ominus \mathcal{P}(j) = \frac{1}{a_0 k}.$$

If on the other hand $i = x_p$ and $j \oplus k \neq x_p$ or $i \oplus k = x_p$ and $j \neq x_p$, then

$$\mathcal{P}(i \oplus k) \ominus \mathcal{P}(i) = \mathcal{P}(j \oplus k) \ominus \mathcal{P}(j)$$

if and only if j is a root of the quadratic equation

$$a_0^2 j^2 \oplus (a_0^2 k \oplus 2a_0 a_1) j \oplus a_0^2 k^2 \oplus a_0 a_1 k \oplus a_1^2 = 0. \tag{5}$$

Applying the quadratic formula to Eq. (5), one obtains $-3a_0^4k^2$ as discriminant. Consequently Eq. (5) has a solution in $\mathbb{F}_p$ if and only if -3 is a square which applies if and only if $p \equiv 1 \bmod 6$.

Now assuming that none of the elements i, $i \oplus k$, j, $j \oplus k$ is x_p, Eq. (4) can be written as

$$\frac{\ominus a_0 k}{(a_0(i \oplus k) \oplus a_1)(a_0 i \oplus a_1)} = \frac{\ominus a_0 k}{(a_0(j \oplus k) \oplus a_1)(a_0 j \oplus a_1)}.$$

Hence we obtain the equation

$$a_0^2(i^2 \oplus ik \ominus j^2 \ominus jk) \oplus 2a_0a_1(i \ominus j) = 0,$$

which can also be written as $a_0(i \ominus j)(a_0(i \oplus j) \oplus a_0k \oplus 2a_1) = 0$. Since $a_0 \neq 0$, this implies $i \oplus j \oplus k = \ominus 2\frac{a_1}{a_0} = 2x_p$, for $i \neq j$. □

Remark 3.1. As noted in the proof of Lemma 3.1, in case $p \equiv 1 \bmod 6$ and $i = x_p, j \oplus k \neq x_p$ Eq. (5) has solutions, namely

$$j = x_p \ominus \frac{1 \pm \sqrt{\ominus 3}}{2}k.$$

Therefore the dispersion is smaller since $D(\mathcal{P}, \mathbb{F}_p)$ has fewer elements.

The following proposition shows that it is sufficient to consider the case $0 \leq x_I \leq (p-1)/2$.

Proposition 3.2. *Let* $\mathcal{P}(x) = (a_0x \oplus a_1)^{p-2} \oplus a_2 \in \mathbb{F}_p[x]$ *and* $\tilde{\mathcal{P}}(x) = (a_0x \oplus a_0 \ominus a_1)^{p-2} \oplus b_2 \in \mathbb{F}_p[x]$. *Then* $\left|D(\mathcal{P}, \mathbb{F}_p)\right| = \left|D(\tilde{\mathcal{P}}, \mathbb{F}_p)\right|$.

Proof. We first observe that with $x_p = \ominus\frac{a_1}{a_0}$ and $\tilde{x}_p = \ominus\frac{a_0 - a_1}{a_0} = \ominus 1 \ominus x_p$, we have $\tilde{x}_I = p - 1 - x_I$. Applying Lemma 3.1 we obtain

$$\begin{aligned}\mathcal{P}(i \oplus k) \ominus \mathcal{P}(i) &= \mathcal{P}(2x_p \ominus i) \ominus \mathcal{P}(2x_p \ominus k \ominus i)\\ &= (a_0(\ominus i \ominus 1) \oplus a_0 \ominus a_1)^{p-2} \ominus (a_0(\ominus i \ominus 1 \ominus k) \oplus a_0 \ominus a_1)^{p-2}\\ &= \tilde{\mathcal{P}}(\ominus i \ominus 1) \ominus \tilde{\mathcal{P}}(\ominus i \ominus 1 \ominus k) = \tilde{\mathcal{P}}(\tilde{i} \oplus k) \ominus \tilde{\mathcal{P}}(\tilde{i})\end{aligned}$$

with $\tilde{i} = p \ominus 1 \ominus k \ominus i$. Since $\tilde{i}$ runs through the set $\{0, \ldots, p \ominus 1 \ominus k\}$ when i does, we have $D(\mathcal{P}, \mathbb{F}_p) = D(\tilde{\mathcal{P}}, \mathbb{F}_p)$, by the definition of $D(\mathcal{P}, \mathbb{F}_p)$. □

Theorem 3.3. *Let* $p \equiv 5 \bmod 6$ *and* $\mathcal{P}(x) = (a_0x \oplus a_1)^{p-2} \oplus a_2 \in \mathbb{F}_p[x]$, $a_0 \neq 0$. *Then*

$$\left|D(\mathcal{P}, \mathbb{F}_p)\right| = \begin{cases} \dfrac{(p+3)(p-1) + 4x_I(p - 2x_I - 2)}{4} : & 0 \leq x_I \leq \dfrac{p-1}{2},\\ \dfrac{(p+3)(p-1) + 4(p-1-x_I)(2x_I - p)}{4} : & \dfrac{p-1}{2} < x_I \leq p-1. \end{cases}$$

Proof. First we assume that $0 \leq x_I \leq \frac{p-1}{2}$. For $j \neq i$, and for each pair (k, i) satisfying the above conditions, there exists at most one j, such that $i \oplus j \oplus k = 2x_I$ and $0 \leq j \leq p - k - 1$. Lemma 3.1 implies then that Eq. (4) holds. Let W be the set of pairs (k, i), which admit such j. Then

$$\left|D(\mathcal{P}, \mathbb{F}_p)\right| = p(p-1)/2 - \frac{1}{2}|W|. \tag{6}$$

To determine the cardinality of W we observe the following:

(i) For a given k, $1 \leq k \leq p-1$, and $0 \leq i \leq 2x_I - k$, the integer j, satisfying $i \oplus j \oplus k = 2x_I$, is $j = 2x_I - k - i \in \{0, \ldots, 2x_I - k\}$. Note that $2x_I - k \leq p - k - 1$.

(ii) For a given k, $1 \leq k \leq p-1$, and $\max\{0, 2x_I - k + 1\} \leq i \leq 2x_I$, the integer $j \in \{0, 1, \ldots, p-1\}$, satisfying $i \oplus j \oplus k = 2x_I$, is $j = p + 2x_I - k - i$. Note that $p + 2x_I - k - i > p - k - 1$.

(iii) For a given k, $1 \leq k \leq p-1$, and $2x_I + 1 \leq i \leq p - 1 - k$, the integer j, satisfying $i \oplus j \oplus k = 2x_I$, is $j = 2x_I - k - i \in \{2x_I + 1, \ldots, p - 1 - k\}$. Thus we can write W as the union of the disjoint sets

$$W_1 = \{(k, i) \mid 1 \leq k \leq p-1, 0 \leq i \leq 2x_I - k, i \neq 2x_I - k - i\}$$
$$W_2 = \{(k, i) \mid 1 \leq k \leq p-1, 2x_I + 1 \leq i \leq p - k - 1, i \not\equiv 2x_I - k - i \bmod p\}.$$

We remark that k in fact, varies over $1 \leq k \leq 2x_I$ in W_1 and over $1 \leq k \leq p - 2 - 2x_I$ in W_2.

Note that the number of pairs (k, i) satisfying $1 \leq k \leq 2x_I$ and $0 \leq i \leq 2x_I - k$ is

$$\sum_{k=1}^{2x_I}(2x_I - k + 1) = \sum_{k=1}^{2x_I} k = 2x_I(2x_I + 1)/2,$$

and since among these, there are x_l pairs with $i = 2x_l - k - i$, we have $|W_1| = 2x_l(2x_l + 1)/2 - x_l = 2x_l^2$. The number of pairs (k, i) satisfying $1 \le k \le p - 2 - 2x_l$ and $2x_l + 1 \le i \le p - 1 - k$ is given by

$$\sum_{k=1}^{p-2-2x_l} k = (p - 2 - 2x_l)(p - 1 - 2x_l)/2.$$

On the other hand, $(p - 1 - 2x_l)/2$ pairs satisfy $1 \le k \le p - 2 - 2x_l$, $2x_l + 1 \le i \le p - 1 - k$, and additionally $i \equiv 2x_l - k - i \bmod p$. Hence

$$|W_2| = (p - 2 - 2x_l)(p - 1 - 2x_l)/2 - (p - 1 - 2x_l)/2 = (p - 3 - 2x_l)(p - 1 - 2x_l)/2.$$

Finally by (6)

$$\left|D(\mathcal{P}, \mathbb{F}_p)\right| = p(p-1)/2 - x_l^2 - (p - 3 - 2x_l)(p - 1 - 2x_l)/4$$

gives the result for $0 \le x_l \le \frac{p-1}{2}$. The rest follows from Proposition 3.2. □

Corollary 3.4. *If $p \equiv 1 \bmod 6$, then for $0 \le x_l \le (p-1)/2$*

$$\left|D(\mathcal{P}, \mathbb{F}_p)\right| \ge \frac{p^2 - 6p + 13 + 4x_l(p - 2x_l - 2)}{4}.$$

Proof. Let $p \equiv 1 \bmod 6$. For each $1 \le k \le p - 2$ at most two more elements of $D(\mathcal{P}, \mathbb{F}_p)$ can be the same and hence

$$\left|D(\mathcal{P}, \mathbb{F}_p)\right| \ge \frac{(p+3)(p-1) + 4x_l(p - 2x_l - 2)}{4} - 2(p-2). \quad \square$$

Given the p-dispersion, the exact value of the dispersion for the polynomial $\mathcal{P}$ can be determined when $a_2 = 0$.

Theorem 3.5. *Let $p \equiv 5 \bmod 6$ and let $\underline{\mathcal{P}}(x) = (a_0 x \oplus a_1)^{p-2} \in \mathbb{F}_p[x]$, $a_0 \ne 0$. Then*

$$\left|D(\underline{\mathcal{P}})\right| = \begin{cases} \dfrac{(p+3)(p-1) + 4x_l(p - 2x_l - 1)}{4} : & 0 \le x_l \le \dfrac{p-1}{2}, \\ \dfrac{(p+3)(p-1) + 4(p - 1 - x_l)(2x_l - p + 1)}{4} : & \dfrac{p-1}{2} < x_l \le p - 1. \end{cases}$$

Proof. We need to evaluate the cardinality of the set T of triples (i, j, k), $1 \le k \le p - 1$, $0 \le i < j \le p - 1 - k$, for which $\mathcal{P}(i \oplus k) \ominus \mathcal{P}(i) = \mathcal{P}(j \oplus k) \ominus \mathcal{P}(j)$ (i.e. $i \oplus j \oplus k = 2x_p$) but $\underline{\mathcal{P}}(i \oplus k) - \underline{\mathcal{P}}(i) \ne \underline{\mathcal{P}}(j \oplus k) - \underline{\mathcal{P}}(j)$. Then $|D(\mathcal{P})| = \left|D(\mathcal{P}, \mathbb{F}_p)\right| + |T|$. First suppose that $i, j, i \oplus k, j \oplus k \ne x_p$. Then

$$\begin{aligned} \mathcal{P}(i \oplus k) - \mathcal{P}(i) &= \left(\frac{1}{a_0(i \oplus k) \oplus a_1} \oplus a_2\right) - \left(\frac{1}{a_0 i \oplus a_1} \oplus a_2\right) \\ &= \left(\frac{1}{a_0(2x_p \ominus j) \oplus a_1} \oplus a_2\right) - \left(\frac{1}{a_0(2x_p \ominus j \ominus k) \oplus a_1} \oplus a_2\right) \\ &= \left(\frac{\ominus 1}{a_0 j \oplus a_1} \oplus a_2\right) - \left(\frac{\ominus 1}{a_0(j \oplus k) \oplus a_1} \oplus a_2\right). \end{aligned}$$

Hence

$$\mathcal{P}(i \oplus k) - \mathcal{P}(i) = (\ominus \mathcal{P}(j) \oplus 2a_2) - (\ominus \mathcal{P}(j \oplus k) \oplus 2a_2). \tag{7}$$

Since $a_2 = 0$, we have $\underline{\mathcal{P}}(i \oplus k) - \underline{\mathcal{P}}(i) = \underline{\mathcal{P}}(j \oplus k) - \underline{\mathcal{P}}(j)$ and thus the set T has no elements satisfying $i, j, i \oplus k, j \oplus k \ne x_p$. For $i = x_p$, hence $j \oplus k = x_p$, we have

$$\begin{aligned} \underline{\mathcal{P}}(i \oplus k) - \underline{\mathcal{P}}(i) &= \underline{\mathcal{P}}(x_p \oplus k) - \underline{\mathcal{P}}(x_p) \\ &= (a_0(x_p \oplus k) \oplus a_1)^{p-2} - (a_0 x_p \oplus a_1)^{p-2} = \frac{1}{a_0 k} \end{aligned}$$

and

$$\begin{aligned} \underline{\mathcal{P}}(j \oplus k) - \underline{\mathcal{P}}(j) &= \underline{\mathcal{P}}(x_p) - \underline{\mathcal{P}}(x_p \ominus k) \\ &= (a_0 x_p \oplus a_1)^{p-2} - (a_0(x_p \ominus k) \oplus a_1)^{p-2} = \frac{1}{a_0 k} - p. \end{aligned}$$

Now, the conditions $0 \le x_l - k, x_l \le p-1-k$ imply that $k \le p-1-x_l$ and $k \le x_l$, i.e, $1 \le k \le \min\{p-1-x_l, x_l\}$. For each k in this range we have exactly one element $(k, i = x_l, j = x_l - k)$ in T. Therefore $|T| = \min\{p-1-x_l, x_l\}$ and

$$\left|D(\underline{\mathcal{P}})\right| = \left|D(\underline{\mathcal{P}}, \mathbb{F}_p)\right| + |T| = \left|D(\underline{\mathcal{P}}, \mathbb{F}_p)\right| + \min\{p-1-x_l, x_l\},$$

giving the result. □

Corollary 3.6. *Let $p \equiv 5 \bmod 6$ and let $\underline{\mathcal{P}}(x) = (a_0 x \oplus a_1)^{p-2} \in \mathbb{F}_p[x]$, $a_0 \neq 0$. Then $\left|D(\underline{\mathcal{P}}, \mathbb{F}_p)\right| = \left|D(\underline{\mathcal{P}})\right|$ if and only if $\underline{\mathcal{P}}(x) = a_0 x^{p-2}$ or $\underline{\mathcal{P}}(x) = (a_0 x \oplus a_0)^{p-2}$ where $a_0 \in \mathbb{F}_p^*$ is arbitrary.*

We remark that Eq. (7) above suggests $|D(\mathcal{P})|$ to be larger when $a_2 \neq 0$. Indeed, a careful analysis of the proof of Theorem 3.5 yields that $D(\mathcal{P})$ has additional points exactly when one of $\mathcal{P}(j)$, $\mathcal{P}(j \oplus k)$ is smaller than $2a_2$, and the other one is larger. Naturally one expects that this happens most frequently if $2a_2 \approx (p-1)/2$. Hence the maximum value of the dispersion is expected to occur when $x_l = a_2 = \lfloor \frac{p-1}{4} \rfloor$. Numerical results for $p \equiv 5 \bmod 6$, $5 \le p \le 71$ confirm this guess. One can also check easily that all Costas permutations of $\mathbb{F}_5$ are of Carlitz rank 1. The maximum values of $\gamma(\mathcal{P})$ for small primes can be calculated, which show that for $x_l = a_2 = \lfloor \frac{p-1}{4} \rfloor$, and various values of a_0, the normalized dispersion of $\mathcal{P}$ is close to 1, i.e. such $\mathcal{P}$ are almost Costas. As one expects, considering the symmetries in $DT(\mathcal{P})$, the minimum values are attained for $x_l = a_2 = \frac{p-1}{2}$. To exemplify, $\gamma(\mathcal{P}_0) \approx 0.94$ and $\gamma(\bar{\mathcal{P}}_0) \approx 0.78$ for $\mathcal{P}_0(x) = (8x+2)^9 + 2 \in \mathbb{F}_{11}$ and $\bar{\mathcal{P}}_0 = (x-126)^{507} + 15 \in \mathbb{F}_{509}$, respectively.

Remark 3.2. The concepts of ambiguity and deficiency are introduced in [8,9], in order to understand the injectivity and surjectivity of the difference map $D_{f,a}(x)$ when $f : G_1 \to G_2$ is a permutation and G_1, G_2 are Abelian groups of the same size. Although deficiency and p-dispersion for a permutation of $\mathbb{F}_p$ seem to be similar concepts, deficiency is invariant under extended affine (EA) equivalence, but p-dispersion is not. We recall that two functions $f, g : \mathbb{F}_p \to \mathbb{F}_p$ are called EA-equivalent if there exist affine permutations A_1, A_2 and an affine map A such that $g = A_1 \circ f \circ A_2 + A$. Lemma 2 and Theorem 17 in [9] show that the deficiency of all permutations of $\mathbb{F}_p$ of Carlitz rank 1 is $(p-1)(p-3)/2$, since they are EA-equivalent to the inversion. On the contrary, it follows from Theorem 3.3 and Corollary 3.4 above that the p-dispersion of permutations in the same class, namely of those of Carlitz rank 1, vary considerably.

4. Dispersion and cycle structure

In this section we first recall the results of [15, Section 2] on the cycle decomposition of permutations $\mathcal{P}$ of Carlitz rank 1, (see also [22]). The polynomial

$$f(x) = x^2 \ominus (a_0 a_2 \oplus a_1)x \ominus a_0 \tag{8}$$

associated to $\mathcal{P}(x)$, plays the central role in studying the cycle structure of $\mathcal{P}(x)$. Let $\alpha, \beta \in \mathbb{F}_{p^2}$ be the roots of $f(x)$, then the multiplicative order m of α/β, a divisor of $p-1$ or $p+1$, determines the cycle structure of $\mathcal{P}(x)$. When a permutation P is decomposed into a product of disjoint cycles, we write $\mathcal{C}_P = [n_1 \times l_1, n_2 \times l_2, \ldots, n_s \times l_s]$ to indicate that the permutation is composed of n_1 cycles of length l_1, n_2 cycles of length l_2,…,n_s cycles of length l_s, $l_1 > l_2 > \cdots > l_s \ge 1$.

Proposition 4.1 (*[15, Theorem 2]*). *For a permutation $\mathcal{P}(x) = (a_0 x \oplus a_1)^{p-2} \oplus a_2$, let f be the associated polynomial in (8), and α, β be the roots of f. Suppose that m is the order of α/β in $\mathbb{F}_{p^2}$. Then $\mathcal{C}_{\mathcal{P}} = \mathcal{C}_{\mathcal{P}}(m)$ depends on m as follows:*

$$\mathcal{C}_{\mathcal{P}}(m) = \begin{cases} [(t-1)\times m, 1\times(m-1)] : & m = (p+1)/t,\ 1 \le t < (p+1)/2, \\ [(t-1)\times m, 1\times(m-1), 2\times 1] : & m = (p-1)/t,\ 1 \le t < (p-1)/2, \\ [1\times(p-1), 1\times 1] : & m = 1, \\ [((p-1)/2 - \delta(f))\times 2, (1+2\delta(f))\times 1] : & m = 2, \end{cases}$$

with $\delta(f) = 0$ if f is irreducible and $\delta(f) = 1$ if f is reducible.

It follows that for $m = p \pm 1$ we have only one nontrivial cycle having length $m-1$. If $2 < m < p-1$, all nontrivial cycles have the same length m, except for one of length $m-1$. If $m = 2$, all nontrivial cycles have length 2. As seen in Section 3, the p-dispersion of $\mathcal{P}$ depends only on $\ominus a_1/a_0$. In this section we show how to choose the remaining parameters in order to obtain a prescribed cycle structure. Furthermore we determine the number of permutations $\mathcal{P}(x) = (a_0 x \oplus a_1)^{p-2} \oplus a_2 \in \mathbb{F}_p[x]$ with prescribed p-dispersion and cycle structure. Note that we partially answer a question raised in [13] also, where cycle structure of various permutations are studied and finding their dispersion is proposed.

Theorem 4.2. *Let p be an arbitrary odd prime. For any $x_p \in \mathbb{F}_p$ and any integer m dividing $p-1$ or $p+1$, there is a permutation $\mathcal{P}(x) = (a_0 x \oplus a_1)^{p-2} \oplus a_2 \in \mathbb{F}_p[x]$ with cycle decomposition $\mathcal{C}_{\mathcal{P}}(m)$ and $x_p = \ominus a_1/a_0$.*

Proof. Throughout the proof, x_p will be a fixed element of $\mathbb{F}_p$. We address the cases $m = 1$, $m = 2$ and $m > 2$ separately. For $m = 1$ we can choose $\alpha = \beta \in \mathbb{F}_p^*$ for the root of (8), and consequently we obtain $a_0 = \ominus\alpha^2$ and $a_1 = \ominus a_0 x_p = \alpha^2 x_p$. From $a_0 a_2 \oplus a_1 = 2\alpha$ we get $a_2 = x_p \ominus 2/\alpha$, which is an element of $\mathbb{F}_p$. Summarizing, the permutations $\mathcal{P}(x)$ with fixed x_p and cycle decomposition $\mathcal{C}_{\mathcal{P}}(1)$ are given by

$$\mathcal{P}(x) = (\ominus\alpha^2 x \oplus \alpha^2 x_p)^{p-2} \oplus x_p \ominus 2/\alpha, \quad \alpha \in \mathbb{F}_p^*. \tag{9}$$

For $m = 2$ we have $\alpha = \ominus\beta$, thus $a_0 a_2 \oplus a_1 = 0$. For an arbitrary $a_0 \in \mathbb{F}_p^*$ we get $a_2 = \ominus a_1/a_0 = x_p$. Hence the permutations $\mathcal{P}(x)$ with fixed x_p and cycle decomposition $\mathcal{C}_{\mathcal{P}}(2)$ are given by

$$\mathcal{P}(x) = (a_0 x \ominus a_0 x_p)^{p-2} \oplus x_p, \quad a_0 \in \mathbb{F}_p^*. \tag{10}$$

For an integer $m > 2$ dividing $p - 1$ or $p + 1$ let $\gamma \in \mathbb{F}_{p^2}$ be an element of order m. If $\alpha, \beta \in \mathbb{F}_{p^2}$ are the roots of (8) with $\alpha/\beta = \gamma$, then $a_1 = \ominus a_0 x_p$ implies

$$\gamma = \frac{\alpha}{\beta} = \frac{a_0 a_2 \ominus a_0 x_p \oplus \sqrt{(a_0 a_2 \ominus a_0 x_p)^2 \oplus 4a_0}}{a_0 a_2 \ominus a_0 x_p \ominus \sqrt{(a_0 a_2 \ominus a_0 x_p)^2 \oplus 4a_0}}.$$

With straightforward algebraic transformations this yields

$$(a_2 \ominus x_p)^2 = \frac{(\gamma \oplus 1)^2}{\ominus\gamma a_0}. \tag{11}$$

Let $c = \ominus(\gamma \oplus \gamma^{-1})$ and thus $(x \ominus \gamma)(x \ominus \gamma^{-1}) = x^2 \oplus cx \oplus 1$, then

$$\frac{(\gamma \oplus 1)^2}{\ominus\gamma a_0} = \frac{\ominus c\gamma \ominus 1 \oplus 2\gamma \oplus 1}{\ominus\gamma a_0} = \frac{c \ominus 2}{a_0},$$

and Eq. (11) gives

$$(a_2 \ominus x_p)^2 = \frac{c \ominus 2}{a_0}. \tag{12}$$

We emphasize that c is always an element of $\mathbb{F}_p$ regardless of γ being in $\mathbb{F}_p$ or not. Moreover $c \ominus 2 \neq 0$ since $\gamma \neq \ominus 1$. Thus (11) is solvable for a_2 in $\mathbb{F}_p$ if we choose $a_0 \in \mathbb{F}_p$ such that $\left(\frac{a_0}{p}\right) = \left(\frac{c-2}{p}\right)$, where $\left(\frac{*}{*}\right)$ denotes the Legendre symbol. □

Theorem 4.3. *Let p be an arbitrary odd prime, m be a divisor of $p - 1$ or $p + 1$ and let $\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p)$ be the number of permutations $\mathcal{P}(x) = (a_0 x \oplus a_1)^{p-2} \oplus a_2 \in \mathbb{F}_p[x]$ with given $x_p = \ominus a_1/a_0 \in \mathbb{F}_p$ and cycle decomposition $\mathcal{C}_{\mathcal{P}}(m)$. Then*

$$\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p) = p - 1 \quad \text{if } m = 1, 2, \text{ and}$$
$$\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p) = \frac{p-1}{2}\varphi(m) \quad \text{if } m > 2,$$

where φ denotes Euler's phi-function.

Proof. For $m = 1, 2$ the result follows immediately from Eqs. (9) and (10), respectively. For the construction of $\mathcal{P}$ with fixed x_p and cycle decomposition $\mathcal{C}_{\mathcal{P}}(m)$, $m > 2$, we choose γ among the $\varphi(m)$ elements of order m in $\mathbb{F}_{p^2}$. We put $c = \ominus(\gamma \oplus \gamma^{-1})$ and note that each $c \in \mathbb{F}_p$ is obtained by two distinct choices for γ, since $\gamma \neq 1, \ominus 1$. Thus there are $\varphi(k)/2$ possible values for c. We choose $a_0 \in \mathbb{F}_p$ such that $\left(\frac{a_0}{p}\right) = \left(\frac{c-2}{p}\right)$. This gives $(p-1)/2$ choices for a_0. Finally we determine a_2 so as to satisfy Eq. (12). For each pair (c, a_0) we have two choices for a_2 since $c \ominus 2 \neq 0$, and the formula for $\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p)$ follows. □

Theorem 4.4. *Suppose $p \equiv 5 \mod 6$. Let $N(\mathcal{C}_{\mathcal{P}}(m), x_p)$ be the number of permutations $\mathcal{P}$ with p-dispersion associated to x_p and cycle decomposition $\mathcal{C}_{\mathcal{P}}(m)$. We have:*

$$N(\mathcal{C}_{\mathcal{P}}(m), x_p) = 4\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p) \quad \text{if } x_l \notin \left\{0, \frac{p-1}{4}, \frac{p-1}{2}, \frac{3(p-1)}{4}, p-1\right\},$$
$$N(\mathcal{C}_{\mathcal{P}}(m), x_p) = 3\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p) \quad \text{if } x_l \in \left\{0, \frac{p-1}{2}, p-1\right\}, \text{ and}$$
$$N(\mathcal{C}_{\mathcal{P}}(m), x_p) = 2\mathcal{N}(\mathcal{C}_{\mathcal{P}}(m), x_p) \quad \text{if } x_l = \frac{p-1}{4}, \frac{3(p-1)}{4}.$$

Proof. The proof easily follows from the observation that $x = x_l$ and $x = (p-1)/2 - x_l$ yield the same values of the expression $4x(p-2x-1)$. Moreover we have $\left|D(\mathcal{P}, \mathbb{F}_p)\right| = \left|D(\tilde{\mathcal{P}}_1, \mathbb{F}_p)\right|$ if $0 \le x_l \le (p-1)/2$ and $\tilde{x_l} = p-1-x_l$, by Proposition 3.2. □

We remark that the last case in Theorem 4.4 can occur only if $p \equiv 1 \bmod 4$ since x_l is an integer.

5. Permutations of Carlitz rank $n > 1$

Let $\mathcal{P}$ be a permutation of $\mathbb{F}_q$, with $\mathrm{Crk}(\mathcal{P}) = n$, and suppose that $\mathcal{P}$ has a representation $\mathcal{P}_n$ as in (1), i.e.,

$$\mathcal{P}_n(x) = (\cdots((a_0x \oplus a_1)^{q-2} \oplus a_2)^{q-2} \oplus \cdots \oplus a_k)^{q-2} \oplus a_{k+1}.$$

One can associate a rational linear transformation $\mathcal{R}_n$ to $\mathcal{P}_n$ as

$$\mathcal{R}_n(x) = \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n}, \tag{13}$$

where $\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2}$ and $\beta_k = a_k\beta_{n-k-1} + \beta_{k-2}$, for $k \ge 2$ and $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$, see [15].

The elements of the string $\mathbf{O}_n = \{x_i : x_i = \frac{-\beta_i}{\alpha_i}, i = 1, \ldots, n\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ are (naturally) called the poles. Corresponding to the rational transformation $\mathcal{R}_n$, one can define a permutation $\mathcal{F}_n$ as $\mathcal{F}_n(x) = \mathcal{R}_n(x)$ for $x \notin \mathbf{O}_n$, and $\mathcal{F}_n(x_n) = \alpha_{n+1}/\alpha_n$. The maps $\mathcal{F}_n(x)$ and $\mathcal{R}_n(x)$ are linear if $\alpha_n = 0$. Since $\mathcal{P}_n(x) = \mathcal{F}_n(x)$ for $x \notin \mathbf{O}_n$, the permutations $\mathcal{P}_n$ and $\mathcal{F}_n$ coincide except for at most n elements of $\mathbb{F}_q$, see [15,22] for details. Note that the permutations $\mathcal{F}_n$ when $\alpha_n \ne 0$ and the permutations of Carlitz rank 1 are in one-to-one correspondence. Therefore any permutation of Carlitz rank n with corresponding rational transformation $\mathcal{R}_n$, satisfying $\alpha_n \ne 0$, differs from a permutation of Carlitz rank 1 only on a subset of $\mathbb{F}_q$ of cardinality at most n.

Now we are ready to prove the following theorem for $q = p$, which is non-trivial when n is small in comparison to p.

Theorem 5.1. *Let $p \equiv 5 \bmod 6$ and $\mathcal{P}$ be a permutation of $\mathbb{F}_p$ of Carlitz rank n.*

(i) *If $n = 1$ and $\mathcal{P}(x) = (a_0x \oplus a_1)^{p-2}$, $a_0 \ne 0$, then the maximum value $\gamma_M(\mathcal{P})$ for the normalized dispersion is $\gamma_M(\mathcal{P}) = 0.75 + \frac{5}{4p}$. This value is attained for $\ominus a_0/a_1 = \lfloor \frac{p-1}{4} \rfloor$ and $\ominus a_0/a_1 = \lfloor \frac{3p-1}{4} \rfloor$.*

(ii) *If $n = 2$ and $\mathcal{P}$ has a representation of the form $\mathcal{P}_2(x) = ((a_0x \oplus a_1)^{p-2} \oplus a_2)^{p-2} - 1/a_2$, $a_0a_2 \ne 0$, then the maximum value for the normalized dispersion satisfies $\gamma_M(\mathcal{P}) \ge 0.75 + \frac{5}{4p} - \frac{4}{p}$. When $\mathcal{P}_2$ is a permutation with $\ominus(a_1a_2+1)/a_0a_2 = \lfloor \frac{p-1}{4} \rfloor$ or $\ominus(a_1a_2+1)/a_0a_2 = \lfloor \frac{3p-1}{4} \rfloor$, then $\gamma(\mathcal{P}) \ge 0.75 + \frac{5}{4p} - \frac{4}{p}$.*

(iii) *If $n > 2$ and $\mathcal{P}$ has a representation $\mathcal{P}_n$ as in (1), where α_n in (13) is not zero, then the maximum value of the normalized dispersion of $\mathcal{P}$ satisfies $\gamma_M(\mathcal{P}) \ge 0.75 + \frac{5}{4p} - \frac{2n}{p}$.*

Proof. The proof of Part (i) is a direct consequence of Theorem 3.5. When $\mathcal{P}$ is a permutation of Carlitz rank 2, and has a representation $\mathcal{P}_2$ as in Part (ii), then the corresponding permutation $\mathcal{F}_2$ is of the form $\mathcal{F}_2 = (-a_0x - a_1 - 1/a_2)^{p-2}$, and $\mathcal{P}$ and $\mathcal{F}_2$ differ only for at two elements of $\mathbb{F}_p$. This means that at most 4 integers in each row of the difference triangle $DT(\mathcal{F}_2)$ change, which may cause at most 4 more integers in each row to repeat, implying $T_k(\mathcal{P}) \ge T_k(\mathcal{F}_2) - 4$ for $k \ge 4$. Adding over k and normalizing we obtain the bound. The rest of (ii) follows from Part (i).

Part (iii) can be proved by following the argument used in the proof of (ii). The condition that $\alpha_n \ne 0$ guarantees the associated rational transformation $\mathcal{R}_n$ to be nonlinear, so that $\mathcal{F}_n$ is a permutation of Carlitz rank 1. □

We remark that although a permutation P of small Carlitz rank differs from a permutation with Carlitz rank 1 at only a small number of elements in $\mathbb{F}_q$, increased Carlitz rank provides wider-ranging properties for P. For instance the cycle structure of permutations of Carlitz rank 1 is rather simple, however even when the Carlitz rank is 2 or 3, we get many different possibilities of decomposition into cycles, see [15]. Therefore the above theorem shows that when p is large enough, by considering permutations with Carlitz rank > 1, one can still obtain "random" permutations, but can also have more ways of decomposing them into cycles. The proof of part (ii) yields a method of specifying permutations P with larger Carlitz rank and ensured lower bound for $\gamma(P)$.

6. Differential uniformity

In this section we add some remarks on differential uniformity, and differently from other sections we consider fields $\mathbb{F}_q$ where q can be a power of an odd prime. We first recall that a polynomial $f \in \mathbb{F}_q[x]$ is called perfect nonlinear if the difference maps $D_{f,a}(x) = f(x+a) - f(x)$, $a \in \mathbb{F}_q^*$, are permutations, in which case f, itself cannot be a permutation. When the equation $D_{f,a}(x) = b$ has at most 2 solutions for all b and all nonzero a in $\mathbb{F}_q$, then f is called almost perfect nonlinear, abbreviated as APN. Permutations P of $\mathbb{F}_q$ can be APN, and this is the best they can achieve, in other words among permutations, those which are APN provide the highest resistance to differential cryptanalysis.

For $b \in \mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, consider $\delta_f(a, b) = \sharp\{x \in \mathbb{F}_q : D_{f,a}(x) = b\}$. Recall that the differential uniformity δ_f of f is defined as

$$\delta_f = \max_{b \in \mathbb{F}_q, a \in \mathbb{F}_q^*} \delta_f(a, b).$$

One of the essential properties of a permutation to be used in cryptography is to have low differential uniformity, see [4–6]. It is well known that the differential uniformity of a function is invariant under EA-equivalence. It is expected therefore, and is easy to see that when $q = p^r$, $p \equiv 5 \mod 6$, and r is odd, permutations of Carlitz rank 1, being EA equivalent to the inversion x^{q-2}, are APN. It is surprising though to obtain a new class of permutations with differential uniformity 4, when $p \equiv 5 \mod 6$, and r is odd. This new class can be obtained in a straightforward manner by our approach; they are permutations of Carlitz rank 2.

Theorem 6.1. *Let $q = p^r$, $r \geq 1$, $p \equiv 5 \mod 6$, and r be odd.*

(i) *Let $\mathcal{P} \in \mathbb{F}_q[x]$ be a permutation of Carlitz rank 1. Then $\mathcal{P}$ is APN.*
(ii) *Let $\mathcal{P} \in \mathbb{F}_q[x]$ be a permutation of Carlitz rank 2. Then $\mathcal{P}$ is differentially 4 uniform.*

Proof. For the proof of (i) we first note that it is sufficient to show that x^{q-2} is APN, see [10, Theorem 8]. Proving that the inversion, x^{q-2} is APN follows the proof of the case of characteristic 2. The equation $(x \oplus a)^{q-2} \ominus x^{q-2} = b$ has a solution $x \neq 0, \ominus a$ if and only if $bx^2 \oplus abx \oplus a = 0$ has a solution. Hence we have at most 2 solutions different from 0 and $\ominus a$. Observe that $x = 0, \ominus a$ are solutions when $b = 1/a$. Hence for x^{q-2} being APN, we have to exclude that $bx^2 \oplus abx \oplus a = 0$ has solutions in $\mathbb{F}_q$ for $b = 1/a$. This applies if and only if -3 is not a square in $\mathbb{F}_q$, which holds if and only if $p \equiv 5 \mod 6$ and r is odd.

To prove (ii) we consider a representation of $\mathcal{P}$ in the form $\mathcal{P}_2(x) = ((a_0x \oplus a_1)^{q-2} \oplus a_2)^{q-2} + a_3$, $a_0a_2 \neq 0$. Again we associate a permutation $\mathcal{F}_2$ to it, which is a permutation of Carlitz rank 1. We note here that $\mathcal{R}_2$ in (13) is always nonlinear. Now the permutations $\mathcal{P}$ and $\mathcal{F}_2$ differ only at the poles x_1, x_2, which are distinct elements of $\mathbb{F}_q$, and we have $\mathcal{P}(x_1) = \mathcal{F}_2(x_2)$, $\mathcal{P}(x_2) = \mathcal{F}_2(x_1)$, or in terms of cycles of $\mathcal{P}$ we have

$$\mathcal{P}(x) = (\mathcal{F}_2(x_1)\ \mathcal{F}_2(x_2))\mathcal{F}_2(x), \tag{14}$$

see [15] for details. As a consequence $D_{\mathcal{P},a}(x) = \mathcal{P}(x + a) - \mathcal{P}(x)$ and $D_{\mathcal{F}_2,a}(x) = \mathcal{F}_2(x + a) - \mathcal{F}_2(x)$ differ at most at 4 positions. On the other hand (14) implies that only two of the values for $D_{\mathcal{P},a}(x)$ which are different from those of $D_{\mathcal{F}_2,a}(x)$ can be the same. As $\mathcal{F}_2$ is of Carlitz rank 1, hence is APN, $\delta_{\mathcal{P}}(a, b) \leq 4$ for all $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$. □

Remark 6.1. Suppose that $\mathcal{P}$ is of Carlitz rank n, $n > 2$. Then $\mathcal{P}$ has a representation $\mathcal{P}_n$ as in (1). If the element α_n in (13) is non-zero then $\mathcal{R}_n$ is nonlinear. In this case the permutations $\mathcal{P}$ and $\mathcal{F}_n$ differ at most at n positions and the values of $D_{\mathcal{P},a}(x)$ and $D_{\mathcal{F}_n,a}(x)$ differ at most at $2n$ positions. The permutation $\mathcal{F}_n$ being APN, we get $\delta_{\mathcal{P}}(a, b) \leq 2n + 2$. In particular $\delta_{\mathcal{P}}(a, b) \leq 8$ if $n = 3$ and $a_2a_3 + 1 \neq 0$ for a_2, a_3 as in (1).

Our Theorem 6.1 adds to known results on differential uniformity in characteristic 2, where the inversion is the classical example of an APN permutation (when the extension degree is odd). For further analysis of the differential uniformity of power functions in characteristic 2 we may refer to [4–6]. We remark that in order that a polynomial can be implemented easily, only sparse polynomials have been considered so far. However permutations of small Carlitz rank can be easily implemented, although they have high degree and large weight, (see [16,23]), providing rare, if not the first examples of such permutations.

For a permutation to be used in cryptography it must also be strong against linear attack, therefore it has to be highly nonlinear. For various measures of nonlinearity we refer to [1,2,7,24] and the references therein. One of the methods is to use the Walsh transform. A justification of this method to be utilized for functions defined over finite abelian groups is given in [7]. Determining nonlinearity of a permutation of Carlitz rank 1 by the use of Walsh transform is equivalent to the evaluation of corresponding Kloosterman sum. Binary Kloosterman sums can be evaluated, see [25]. However obtaining exact values for Kloosterman sums in characteristic other than 2 is a hard problem. By Theorem 5.45 in [26] the absolute value of a Kloosterman sum over $\mathbb{F}_q$ is bounded above by $2q^{1/2}$, at least guaranteeing a flat Walsh spectrum for $\mathcal{P}$ of Carlitz rank 1. More is known in the ternary case, see Theorem 6.4 in [27]. When the Carlitz rank of $\mathcal{P}$ is n and n is small compared to q, then the nonlinearity of $\mathcal{P}$ can be estimated from that of the associated permutation $\mathcal{F}_n$ of Carlitz rank 1. Work on this problem is under progress.

As remarked above, the permutations of Carlitz rank 1 are all APN, since they are EA-equivalent to the inversion, however the values of dispersion vary a lot. This is in accordance with the finding in [10] that the relation between Costas and APN permutations is "quite erratic".

7. Conclusion

We present classes of permutations possessing various properties, that have attracted interest due to diverse applications. Pseudorandom number sequences generated by permutations of Carlitz rank 1 have been widely studied. The cycle structure

of these permutations for instance determine the period lengths of the sequences [28]. The concept of dispersion of a permutation on the other hand is used in coding theory; one generally looks for permutations with normalized dispersion close to 0.8. But so far, the evaluation of the exact value was possible for monomials only, where the normalized dispersion is 0.5. Permutations with favorable cycle structure are either difficult to implement or they lack other useful characteristics like high dispersion. Functions with low differential uniformity are needed for use in cryptography, and in all applications easy implementation is a crucial aspect. We show that permutations with small Carlitz rank provide examples of permutations with many interesting features together, that would be difficult to obtain by the usual approach to permutations. Although we focus on permutations with Carlitz rank 2 only, our methods can be easily extended to the case of larger Carlitz rank, when necessary.

Acknowledgements

We thank the anonymous referees for their valuable comments, which considerably improved the presentation of this paper.

References

[1] C. Carlet, C. Ding, Highly non-linear mappings, J. Complexity 20 (2004) 205–244.
[2] C. Carlet, C. Ding, Nonlinearities of S-boxes, Finite Fields Appl. 13 (2007) 121–135.
[3] K. Nyberg, Perfect nonlinear S-boxes, in: Advances in Cryptology-EUROCRYPT '91 (Brighton, 1991), in: Lecture Notes in Comput. Sci., vol. 547, 1991, pp. 378–386.
[4] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of power functions, Int. J. Inf. Coding Theory 1 (2010) 149–170.
[5] C. Blondeau, A. Canteaut, P. Charpin, Differential properties of $x \to x^{2^t-1}$, IEEE Trans. Inform. Theory 57 (2011) 8127–8137.
[6] C. Bracken, G. Leander, A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, Finite Fields Appl. 16 (2010) 231–242.
[7] K. Drakakis, V. Requena, G. McGuire, On the nonlinearity of exponential Welch Costas functions, IEEE Trans. Inform. Theory 56 (2010) 1230–1238.
[8] D. Panario, B. Stevens, Q. Wang, Ambiguity and deficiency in Costas arrays and APN permutations, in: LATIN 2010: Theoretical Informatics (Mexico, 2010), in: Lecture Notes in Comput. Sci., vol. 6034, 2010, pp. 397–406.
[9] D. Panario, A. Sakzad, B. Stevens, Q. Wang, Two new measures for permutations: ambiguity and deficiency, IEEE Trans. Inform. Theory 57 (11) (2011) 7648–7657.
[10] K. Drakakis, R. Gow, G. McGuire, APN permutations on $\mathbb{Z}_n$ and Costas arrays, Discrete Appl. Math. 157 (2009) 3320–3326.
[11] I.M. Rubio, G.L. Mullen, C. Corrada, F.N. Castro, Dickson Permutation Polynomials that Decompose in Cycles of the Same Length, Finite Fields and Applications, in: Contemp. Math., vol. 461, Amer. Math. Soc., Providence, RI, 2008, pp. 229–239.
[12] I. Rubio, C. Corrada, Cyclic decomposition of permutations of finite fields obtained by using monomials, in: A. Poli, H. Stichtenoth (Eds.), Proc. of Finite Fields and Applications, Vol. 7, in: Lecture Notes in Comput. Sci., vol. 2948, 2004, pp. 254–261.
[13] A. Sakzad, M-R. Sadeghi, D. Panario, Cycle structure of permutation functions over finite fields and their applications, Adv. Math. Comm. 6 (2012) 347–361.
[14] L. Carlitz, Permutations in a finite field, Proc. Amer. Math. Soc. 4 (1953) 538.
[15] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the cycle structure of permutation polynomials, Finite Fields Appl. 14 (2008) 593–614.
[16] E. Aksoy, A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the Carlitz rank of permutation polynomials, Finite Fields Appl. 15 (2009) 418–440.
[17] C. Heegard, S.B. Wicker, Turbo Coding, Kluwer Academic Publishers, Dordrecht, 1999.
[18] C. Avenancio-Leon, Analysis of some properties of interleavers for Turbo codes, in: Proc. of NCUR, Lexington, USA, 2005.
[19] C.J. Corrada-Bravo, I.M. Rubio, Deterministic interleavers for Turbo codes with random-like performance and simple implementation, in: Proc. of the 3rd International Symposium on Turbo Codes and Related Topics, Brest, France, 2003, pp. 555–558.
[20] K. Drakakis, A review of Costas arrays, J. Appl. Math. (2006) 1–32.
[21] S.W. Golomb, G. Gong, The status of Costas arrays, IEEE Trans. Inform. Theory 53 (2007) 4260–4265.
[22] A. Topuzoglu, The Carlitz rank of permutations of $\mathbb{F}_q$: A survey, J. Symbolic Comput. (in press).
[23] D. Gomez-Perez, A. Ostafe, A. Topuzoğlu, On the Carlitz rank of permutations of $\mathbb{F}_q$ and pseudorandom sequences, Preprint.
[24] G.M. Kyureghyan, Special mappings of finite fields, in: P. Charpin, A. Pott, A. Winterhof (Eds.), Finite Fields and Their Applications: Character Sums and Polynomials Radon Series on Computational and Applied Mathematics, vol. 11, de Gruyter, 2013, pp. 117–144.
[25] G. Lachaud, J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inform. Theory 36 (1990) 686–692.
[26] R. Lidl, H. Niederreiter, Finite Fields, second ed., in: Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[27] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, Acta Arith. 132 (2008) 329–350.
[28] W. Meidl, A. Topuzoğlu, On the inversive pseudorandom number generator, in: Recent Developments in Applied Probability and Statistics, Physica-Verlag, Springer, Berlin, Heidelberg, 2010, pp. 103–126.