On permutation polynomials over finite fields: differences and iterations

Anbar Meidl, Nurdagül; Odzak, Almasa; Patel, Vandita; Quoos, Luciane; Somoza, Anna; Topuzoglu, Alev

Published in:
Women in Numbers

Publication date:
2017

Document Version
Peer reviewed version

On permutation polynomials over finite fields: differences and iterations

Nurdagül Anbar[1], Almasa Odžak[2], Vandita Patel[3],
Luciane Quoos[4], Anna Somoza[5,6], Alev Topuzoğlu[7]

[1]Otto-von-Guericke University Magdeburg,
Universitätsplatz 2, 39106 Magdeburg, Germany
Email: nurdagulanbar2@gmail.com

[2]University of Sarajevo,
Zmaja od Bosne 35, 71000 Sarajevo, Bosnia and Herzegovina
Email: almasa.odzak@gmail.com

[3]University of Warwick,
Coventry CV4 7AL, UK
Email: vandita.patel@warwick.ac.uk

[4]Universidade Federal do Rio de Janeiro, Cidade Universitária,
Rio de Janeiro, RJ 21941-909, Brazil
Email: luciane@im.ufrj.br

[5]Universitat Politècnica de Catalunya,
Calle Jordi Girona, 1-3, 08034 Barcelona, Spain
[6]Leiden University ,
Snellius building, Niels Bohrweg 1 2300 RA Leiden, Netherlands
Email: anna.somoza@upc.edu

[7]SabancıUniversity,
MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
Email: alev@sabanciuniv.edu

Abstract

The Carlitz rank of a permutation polynomial f over a finite field $\mathbb{F}_q$ is a simple concept that was introduced in the last decade. Classifying permutations over $\mathbb{F}_q$

with respect to their Carlitz ranks has some advantages, for instance f with a given Carlitz rank can be approximated by a rational linear transformation.

In this note we present our recent results on the permutation behaviour of polynomials $f+g$, where f is a permutation over $\mathbb{F}_q$ of a given Carlitz rank, and $g \in \mathbb{F}_q[x]$ is of prescribed degree. We describe the relation of this problem to the well-known Chowla-Zassenhaus conjecture. We also study iterations of permutation polynomials by using the approximation property that is mentioned above.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements, where p is a prime, and $r \geq 1$. We recall that any map from $\mathbb{F}_q$ to itself can be represented uniquely by a polynomial $f \in \mathbb{F}_q[x]$ of degree less than q. A polynomial f is called a *permutation* polynomial if it induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$.

Permutation polynomials over finite fields have been studied widely in the last decades, due to their applications especially in combinatorics, coding theory and symmetric cryptography. In order to meet the specific requirements of individual applications, methods of construction of various types of permutations and/or alternative ways of classifying them are needed. Although the work on permutation polynomials goes back to the 19th century, they still are of theoretical interest also, offering many open problems. We refer to [14, 15, 21] for a detailed exposition of permutation polynomials over finite fields.

We recall that S_q, the symmetric group on q letters, is isomorphic to the group of permutation polynomials over $\mathbb{F}_q$ of degree less than q, under the operation of composition and subsequent reduction modulo $x^q - x$, hence we identify them. A well-known result of Carlitz [3] states that S_q is generated by linear polynomials $ax + b$, $a, b \in \mathbb{F}_q$, $a \neq 0$, and x^{q-2}. Hence any permutation f over $\mathbb{F}_q$ can be represented by a polynomial of the form

$$P_n(x) = \Big(\dots \big((a_0 x + a_1)^{q-2} + a_2 \big)^{q-2} \dots + a_n \Big)^{q-2} + a_{n+1}, \tag{1}$$

for some $n \geq 0$, where $a_i \neq 0$, for $i = 0, 2, \dots, n$. Note that $f(c) = P_n(c)$ holds for all $c \in \mathbb{F}_q$, however this representation is not unique, and n is not necessarily minimal. Accordingly the authors of [2] define the *Carlitz rank* of a permutation polynomial f over $\mathbb{F}_q$ to be the smallest integer $n \geq 0$ satisfying $f = P_n$ for a permutation P_n of the form (1), and denote it by $\mathrm{Crk}(f)$.

The representation of f as in (1) enables approximation of f by a fractional transformation in the following sense.

Recall that $x^{q-2} = x^{-1}$ for $x \neq 0$ and $x^{q-2} = 0$ if $x = 0$. Hence the representation in (1) can be expressed as a continued fraction for suitable $x \in \mathbb{F}_q$, which yields the function

$R_k(x)$ defined as follows. For $0 \leq k \leq n$, put $R_k(x) = (\alpha_{k+1}x + \beta_{k+1})/(\alpha_k x + \beta_k)$, where $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$ and, for $k \geq 2$,

$$\alpha_k = a_k \alpha_{k-1} + \alpha_{k-2} \quad \text{and} \quad \beta_k = a_k \beta_{k-1} + \beta_{k-2} \ . \tag{2}$$

The set

$$\mathcal{O}_n = \left\{ x_k : \ x_k = \frac{-\beta_k}{\alpha_k} \ , \ k = 1, \ldots, n \right\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\} \ , \tag{3}$$

is called the *set of poles* of f. The elements of $\mathcal{O}_n$ may not be distinct. In case $a_{n+1} = 0$ in (1), R_n takes the form

$$R_n(x) = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n} \ . \tag{4}$$

It can easily be verified that

$$f(c) = P_n(c) = R_n(c) \ \text{ for all } \ \mathrm{c} \in \mathbb{F}_q \setminus \mathcal{O}_n \ . \tag{5}$$

Obviously, this property is particularly useful when $\mathrm{Crk}(f)$ is small with respect to the field size. The values that f takes on $\mathcal{O}_n$ can also be expressed in terms of R_n, see [23]. If $\alpha_n = 0$, i.e., the last *pole* $x_n = \infty$, R_n is linear. Following the terminology of [11], we define the *linearity* of $f \in \mathbb{F}_q[x]$ as $\mathcal{L}(f) = \max_{a,b \in \mathbb{F}_q} |\{c \in \mathbb{F}_q : f(c) = ac + b\}|$. Intuitively $\mathcal{L}(f)$ is large when f is a permutation polynomial over $\mathbb{F}_q$ of $\mathrm{Crk}(f) = n$, R_n is linear, and n is small with respect to q.

Various problems concerning the concept of Carlitz rank are tackled in [2, 7, 8]. For instance, the cycle structure of polynomials of a given Carlitz rank, the enumeration of polynomials with small Carlitz rank and of particular cycle structure, or of permutations of a fixed Carlitz rank are studied.

The relation between invariants of a polynomial f and $\mathrm{Crk}(f)$ is of interest. A lower bound for $\mathrm{Crk}(f)$ in terms of the degree of f, denoted by $\deg(f)$, can be found in [2], which shows that non-linear polynomials of small degree have large Carlitz ranks. A similar bound in terms of the weight of f, i.e., the number of nonzero coefficients of f, is given in [9]. The classification of permutations with respect to their Carlitz ranks has already found applications, see [23] and references therein.

This note is concerned with the permutation polynomials over $\mathbb{F}_q$, classified with respect to their Carlitz ranks, and it is structured as follows. In Section 2, we present a recent result of the authors [1] on the difference of permutation polynomials. More precisely, assuming f and $f+g$ to be permutations over $\mathbb{F}_q$, we give lower bounds for the degree of g in terms of q and the Carlitz rank of f, see Theorems 1 and 4. These bounds are analogous to a well-known result of Cohen, Mullen and Shiue where they obtain a lower bound for $\deg(g)$ in terms of $\deg(f) = \deg(f+g) = d$ when the cardinality of the field is sufficiently large with respect to d [6, Theorem 1]. Our bound in Theorem 1 also generalizes the main result of [11] on the non-existence of complete mappings. Section 3 focuses on iterations of permutation polynomials over finite fields of odd characteristic. In particular, we present some preliminary results on the order of a permutation polynomial over $\mathbb{F}_q$ as an element of S_q.

2 On the difference of permutation polynomials

Let f be a permutation polynomial over $\mathbb{F}_q$. If $f(x) + x$ is also a permutation, then f is called a *complete mapping polynomial*, or a complete mapping. We refer the reader to [17] for a detailed study of complete mappings over finite fields. See [13, 16, 19, 20, 22] for various applications, and [11] for some recent work on complete mappings.

Theorem A below was conjectured by Chowla and Zassenhaus [4] in 1968, and proven by Cohen [5] in 1990.

Theorem A. If $d \geq 2$ and $p > (d^2 - 3d + 4)^2$, then there is no complete mapping polynomial of degree d over $\mathbb{F}_p$.

A significant generalization of this result was obtained by Cohen, Mullen and Shiue [6] in 1995, and gives a lower bound for the degree of the difference of two permutation polynomials in $\mathbb{F}_p[x]$ of the same degree d, when $p > (d^2 - 3d + 4)^2$.

Theorem B. Suppose f and $f + g$ are monic permutation polynomials over $\mathbb{F}_p$ of degree $d \geq 3$, where $p > (d^2 - 3d + 4)^2$. If $\deg(g) = t \geq 1$, then $t \geq 3d/5$.

The concept of Carlitz rank was used by Işık, Topuzoğlu and Winterhof [11] recently to obtain a non-existence result, similar to that in Theorem A.

Theorem C. If $f(x)$ is a complete mapping over $\mathbb{F}_q$ and $\mathcal{L}(f) < \lfloor (q+5)/2 \rfloor$, then $\mathrm{Crk}(f) \geq \lfloor q/2 \rfloor$.

Theorems 1 and 4 below give lower bounds for the degree of the difference between two permutation polynomials, analogous to Theorem B, generalizing Theorem C, see [1]. We remark that Theorems A and B hold over prime fields only, while Theorems C, 1 and 4 are true for any finite field.

Let f be a permutation polynomial over $\mathbb{F}_q$, $q \geq 3$, with $\mathrm{Crk}(f) = n \geq 1$. Suppose that f has a representation as in (1) and the fractional linear transformation R_n, which is associated to f as in (5) is not linear. In other words α_n defined as in (2) is not zero. We denote the set of all such permutations by $\mathcal{C}_{1,n}$, i.e., the set $\mathcal{C}_{1,n}$ consists of all permutation polynomials over $\mathbb{F}_q$, satisfying Crk(f) = n ≥ 1 and $\alpha_n \neq 0$. Clearly $\mathcal{L}(f) \leq n + 2$, if $f \in \mathcal{C}_{1,n}$. We note that permutations $f \in \mathbb{F}_q[x]$ with $\alpha_n = 0$ behave very differently. For instance, the polynomial given by $f(x) = \left(\left(\left((-x/(d+1))^{q-2}+1\right)^{q-2}+d\right)^{q-2}-1/(d+1)\right)^{q-2}$ is a complete mapping for every $q \equiv 1 \mod 3$ where d is a primitive 3-rd root of unity, see [12]. Indeed, the condition on the linearity of f in Theorem C corresponds to the case $\alpha_n = 0$. Therefore, we only consider permutations in $\mathcal{C}_{1,n}$.

Theorem 1. *Let f and $f+g$ be permutation polynomials over $\mathbb{F}_q$. If $f \in \mathcal{C}_{1,n}$ and $\deg(g) = k$ satisfies $1 \leq k < q-1$, then*

$$nk + k(k-1)\sqrt{q} \geq q - \nu - n \ , \tag{6}$$

where $\nu = \gcd(k, q-1)$.

For $k = 1$ (and hence $\nu = 1$) we obtain Theorem C, which is the main result in [11].

Corollary 2. *Let f be a permutation polynomial over $\mathbb{F}_q$ with $f \in \mathcal{C}_{1,n}$. If $n < (q-1)/2$, then f is not a complete mapping.*

Remark 3. We note that the bound given in (6) is non-trivial only when $q \geq k(k-1)\sqrt{q} + k + \nu + 1$.

When $g(x) = cx^k \in \mathbb{F}_q[x]$, $\gcd(k+1, q-1) = 1$, and $f \in \mathcal{C}_{1,n}$ where $x_n \in \mathcal{O}_n$ in (3) satisfies $x_n = 0$, the lower bound in (6) can be simplified significantly. We denote by $\mathcal{C}_{2,n}$ the set of $f \in \mathcal{C}_{1,n}$ such that the last pole x_n of f is zero.

Theorem 4. *Let $f(x)$ and $f(x) + cx^k$ be permutation polynomials over $\mathbb{F}_q$, where $f \in \mathcal{C}_{2,n}$, $1 \leq k < q-1$, $c \in {\mathbb{F}_q}^*$. Put $m = \gcd(k+1, q-1)$. Then*

$$k(n+3) + (k-1)(m-1)\sqrt{q} \geq q - n \ .$$

In particular, if $m = 1$, then $k \geq (q-n)/(n+3)$.

The proofs of Theorems 1 and 4 are based on the idea of relating the Carlitz rank n of a permutation polynomial f of $\mathbb{F}_q$ to the number of rational points of an absolutely irreducible projective curve defined over $\mathbb{F}_q$. The fact that f can be approximated by a rational transformation enables us to obtain this relation. Then the well-known Hasse-Weil Theorem yields the stated inequalities.

3 On iterations of permutation polynomials

Dynamical systems generated by polynomials in $\mathbb{F}_q[x]$ have been studied widely. We refer the reader to a recent survey [18] for algebraic and number theoretic properties of algebraic dynamical systems over finite fields and some of their applications. The distribution of elements in orbits of permutation polynomials in $\mathcal{C}_{1,n}$ is studied in [9]. Authors use the approximation property in $\mathcal{C}_{1,n}$, in the sense of (5), to analyse the distribution behaviour of pseudorandom sequences generated by $f \in \mathcal{C}_{1,n}$ efficiently, since this approach enables them to avoid the usual problem of degree growth, encountered when iterations of polynomials are considered.

We denote the m-th iteration of $f \in \mathbb{F}_q[x]$ by

$$f^{(m)}(x) = f^{(m-1)}(f(x)) \text{ for } m \geq 1, \text{where } f^{(0)}(x) = x.$$

In connection with complete mappings, one may wonder if $f^{(m)}$, $m > 1$, is complete while f is not. Such polynomials are called $\{m\}$-complete mappings, see [24] for results on the $\{m\}$-completeness of some classes of polynomials over $\mathbb{F}_q$.

In this section we consider finite fields $\mathbb{F}_q$ of odd characteristic and study iterations of permutation polynomials over $\mathbb{F}_q$ of a given Carlitz rank n. Iterations of permutations of Carlitz rank 1 are easy to determine since their cycle structures can be described in a simple manner, see [7, Theorem 2]. On the contrary, the cycle structure of permutations of higher rank are difficult to describe, see [7, Theorems 6, 7, 11, 13 and 15] for the cases $n = 2, 3$. Therefore in what follows we consider $n \geq 2$.

For simplicity we consider monic polynomials only, and take $f \in \mathcal{C}_{2,n}$. Without loss of generality, we also assume throughout that $a_{n+1} = 0$ in the representation (1) of f. For $f(x) \in \mathcal{C}_{2,n}$, consider the associated rational fraction $R_n(x)$ as in (4) and (5). We denote the m-th iteration of $R_n(x)$ by $R_n^{(m)}(x)$. Note that

$$R_n^{(m)}(x) = \frac{\alpha_{nm-1}x + \beta_{nm-1}}{\alpha_{nm}x + \beta_{nm}},$$

where α_k, β_k, $k \geq 2$, are defined as in Equation (2) and $a_i = a_j$ for $i \equiv j \mod n$, $i, j \geq 1$. Hence we have $f^{(m)}(c) = R_n^{(m)}(c)$ for all $c \in \mathbb{F}_q \setminus \mathcal{O}_{nm}$.

If $f(x) = ((x + a)^{q-2} + b)^{q-2}$ for some $a, b \in \mathbb{F}_q$, $b \neq 0$, then by Theorem C, $f^{(2)}$ is not complete for $q > 9$. However, as we see in the following example, $f^{(3)}$ is trivially complete since $f^{(3)}(x) \equiv x$. Using the terminology of [24], $f(x)$ therefore is not $\{2\}$-complete, but it is $\{3\}$-complete.

Example 5. Let $f(x) = ((x + a)^{q-2} + b)^{q-2}$ be a permutation polynomial over $\mathbb{F}_q$ with $f(0) = 0$. Then $f^{(3)}(x) \equiv x$.

Proof. Since $b \neq 0$, the property $f(0) = 0$ implies that $a \neq 0$ and $ab + 1 = 0$. Note that $\mathcal{O}_2 = \{-a, 0\}$. For any $x \in \mathbb{F}_q \setminus \mathcal{O}_6$ we have

$$\begin{aligned} f^{(3)}(x) = R_2^{(3)}(x) &= \frac{\alpha_5 x + \beta_5}{\alpha_6 x + \beta_6} \\ &= \frac{((ab)^2 + 3ab + 1)x + a((ab)^2 + 4ab + 3)}{(b((ab)^2 + 4ab + 3)x + ((ab)^3 + 5(ab)^2 + 6ab + 1))} = x, \end{aligned}$$

where $\mathcal{O}_6 = \{-a, 0, \infty\}$. We see by straightforward calculations that $f^{(3)}(0) = 0$ and $f^{(3)}(-a) = -a$. This finishes the proof of our claim. □

Consider $f \in \mathcal{C}_{1,n}$. Obviously if $q > 2mn + 1$, then $f^{(m)}(x) \in \mathbb{F}_q[x]$ is not complete unless $f^{(m)}$ is linear. However the Carlitz rank of $f^{(m)}$ may be smaller than mn. Hence one may obtain better bounds for $\{m\}$-completeness of special types of permutation polynomials in $\mathcal{C}_{1,n}$, when $f^{(m)}$ is also in $\mathcal{C}_{1,n}$.

Here we focus on extending the property of permutations of Carlitz rank 2, which is observed in Example 5 above, to those of arbitrary Carlitz rank $n > 2$. Therefore we search for the cases where f is trivially $\{m\}$-complete, i.e., $f^{(m)}(x) \equiv x$. This, of course, leads to the problem of determining the order of $f \in \mathcal{C}_{1,n}$ as an element of the group S_q. Our approach is similar to that in Example 5, i.e., first finding when $R_n^{(m)}(x) \equiv x$. We need to determine the values of α_{nm}, α_{nm-1}, β_{nm} and β_{nm-1}. Lemmas 6 and 10 below enable us to express them in terms of eigenvalues of the matrix corresponding to R_n.

Lemma 6. *Let $R(x) = (ax + b)/(cx + d) \in \mathbb{F}_q(x)$, $\gamma = ad - bc \neq 0$. If $h(T) = T^2 - (a + d)T + \gamma$ has two distinct roots λ_1 and λ_2 in $\mathbb{F}_{q^2}$, then $R^{(m)}(x) \equiv x$ if and only if $\lambda_1^m = \lambda_2^m$.*

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, q)$ be the matrix associated to $R(x)$. Then $h(T)$ is the characteristic polynomial of M. By our assumption, M has two distinct eigenvalues. That is, there exists $P \in \mathrm{GL}(2, q^2)$ such that $M = PDP^{-1}$ for the diagonal matrix $D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. Then the m-th iteration $R^{(m)}(x)$ of $R(x)$ is obtained by

$$M^m = PD^mP^{-1} = P \begin{pmatrix} \lambda_1^m & 0 \\ 0 & \lambda_2^m \end{pmatrix} P^{-1} \ . \tag{7}$$

By Equation (7), we conclude that $R^{(m)}(x) \equiv x$ if and only if $\lambda_1^m = \lambda_2^m$. □

Remark 7. We recall that the set of fractional transformations $(ax + b)/(cx + d)$, for $a, b, c, d \in \mathbb{F}_q$ with $ad - bc \neq 0$, forms the projective general linear group $\mathrm{PGL}(2, q)$. Up to conjugacy, a complete list of its subgroups is known, see [10, Theorem A.8]. This classification implies that the order m of $R_n(x)$ is a divisor of $q \pm 1$.

Now we turn our attention to polynomials $f \in \mathcal{C}_{2,n}$, and consider the corresponding rational transformations R_n. Since $f \in \mathcal{C}_{2,n}$, i.e., $\beta_n = 0$, the associated matrix $M \in \mathrm{GL}(2, q)$ is given by

$$M = \begin{pmatrix} \alpha_{n-1} & \beta_{n-1} \\ \alpha_n & 0 \end{pmatrix} \ . \tag{8}$$

Remark 8. For $f(x) \in \mathcal{C}_{2,n}$, by straightforward calculations, we see that the determinant of M associated to $R_n(x)$ is $(-1)^n$. Therefore the characteristic polynomial of M, which is given in Equation (8), is $h_M(T) = T^2 - \alpha_{n-1}T + (-1)^n$.

Corollary 9. *Let $f(x) \in \mathcal{C}_{2,n}$ and $R_n(x)$ be the corresponding rational transformation. Suppose α_{n-1} satisfies $\alpha_{n-1}^2 - 4(-1)^n \neq 0$. Let λ_1, λ_2 be the distinct eigenvalues of M in (8). Then $R_n^{(m)}(x) \equiv x$ if and only if $\lambda_1^m = \lambda_2^m$.*

The criteria given in Corollary 9 can be used to identify polynomials in $\mathcal{C}_{2,n}$, with $R_n^{(m)}(x) \equiv x$. Lemma 10 below indicates the choices for α_{n-1}. Moreover, it enables us to construct permutations of prescribed Carlitz rank n with $R_n^{(m)}(x) \equiv x$, see Remark 12 and Example 13.

Lemma 10. *Let $h_1(T) = T^2 - \gamma T - 1$ and $h_2(T) = T^2 - \delta T + 1$ be in $\mathbb{F}_q[T]$.*

(i) Let λ_1, λ_2 be the roots of h_1 in $\mathbb{F}_{q^2}$. Then γ satisfies

$$\lambda_1^m - \lambda_2^m = (\lambda_1 - \lambda_2)H_m(\gamma), \text{ with } H_m(T) = \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-i-1}{i} T^{m-2i-1} \tag{9}$$

for $m \geq 1$.

(ii) Let λ_1, λ_2 be the roots of h_2 in $\mathbb{F}_{q^2}$. Then δ satisfies

$$\lambda_1^m - \lambda_2^m = (\lambda_1 - \lambda_2)G_m(\delta), \text{ with } G_m(T) = \sum_{i=0}^{m-1} \binom{m+i}{2i+1} (T-2)^i \tag{10}$$

for $m \geq 1$.

Proof. If $\lambda_1 = \lambda_2$, then Equations (9) and (10) are clearly satisfied. Therefore we assume that $\lambda_1 \neq \lambda_2$. For $m \geq 1$, we define

$$L_m = \frac{\lambda_1^m - \lambda_2^m}{\lambda_1 - \lambda_2} .$$

(i) It can be seen easily that

$$L_1 = H_1(\gamma) = 1 \quad \text{and} \quad L_2 = H_2(\gamma) = \gamma . \tag{11}$$

Since λ_1, λ_2 are the roots of h_1, for $m \geq 1$, L_m satisfies

$$L_{m+2} - \gamma L_{m+1} - L_m = 0 .$$

By Equation (11), it is enough to show that $H_m(T)$ satisfies the same recurrence for $T = \gamma$ and $m \geq 1$. For $m = 2k, 2k+1$ we can write $H_m(\gamma)$ as follows:

$$H_{2k}(\gamma) = \sum_{i=0}^{k-1} \binom{2k-i-1}{i} \gamma^{2k-2i-1} = \sum_{i=0}^{k-1} \binom{k+i}{k-i-1} \gamma^{2i+1} = \sum_{i=0}^{k-1} \binom{k+i}{2i+1} \gamma^{2i+1},$$

$$H_{2k+1}(\gamma) = \sum_{i=0}^{k} \binom{2k-i}{i} \gamma^{2k-2i} = \sum_{i=0}^{k} \binom{k+i}{k-i} \gamma^{2i} = \sum_{i=0}^{k} \binom{k+i}{2i} \gamma^{2i} .$$

Hence for $m = 2k$ we have

$$\begin{aligned} &H_{2k+2}(\gamma) - \gamma H_{2k+1}(\gamma) - H_{2k}(\gamma) \\ &= \sum_{i=0}^{k} \binom{k+i+1}{2i+1} \gamma^{2i+1} - \gamma \sum_{i=0}^{k} \binom{k+i}{2i} \gamma^{2i} - \sum_{i=0}^{k-1} \binom{k+i}{2i+1} \gamma^{2i+1} . \end{aligned} \tag{12}$$

Since the identity

$$\binom{k+i+1}{2i+1} - \binom{k+i}{2i} - \binom{k+i}{2i+1} = 0$$

holds, the coefficient of γ^{2i+1} in Equation (12) is equal to zero for all $i = 0, \ldots, k$. The same argument holds for $m = 2k-1$ as the coefficient of γ^{2i} in

$$H_{2k+1}(\gamma) - \gamma H_{2k}(\gamma) - H_{2k-1}(\gamma)$$

satisfies

$$\binom{k+i}{2i} - \binom{k+i-1}{2i-1} - \binom{k+i-1}{2i} = 0$$

for all $i = 0, \ldots, k$.

(i) Similarly, we have $L_1 = G_1(\delta) = 1$ and $L_2 = G_2(\delta) = \delta$ and we replace Equation (12) by

$$G_{m+2}(\delta) - (\delta-2)G_{m+1}(\delta) - 2G_{m+1}(\delta) + G_m(\delta) . \tag{13}$$

Then by similar calculations we observe that the coefficient of $(\delta-2)^i$ in Equation (13) satisfies

$$\binom{m+2+i}{2i+1} - \binom{m+i}{2i-1} - 2\binom{m+1+i}{2i+1} + \binom{m+i}{2i+1} = 0$$

for all $i = 0, \ldots, m+1$, which proves the desired result.

□

As mentioned earlier, a permutation polynomial f over $\mathbb{F}_q$ can be regarded as an element of the symmetric group S_q. We denote the order of f in S_q by $\operatorname{ord}_{S_q}(f)$. Next theorem provides a lower bound for $\operatorname{ord}_{S_q}(f)$.

Theorem 11. *Let $f \in \mathcal{C}_{2,n}$ with $\alpha_{n-1}^2 - 4(-1)^n \neq 0$. We define*

$$A_m(T) = \begin{cases} H_m(T), & \text{if } n \text{ is odd,} \\ G_m(T), & \text{if } n \text{ is even,} \end{cases}$$

where H_m, G_m are given as in Equations (9) *and* (10)*. If $A_m(\alpha_{n-1}) = 0$, then $R_n^{(m)}(x) \equiv x$. Moreover, putting $\operatorname{ord}_{S_q}(f) = m_f$, $q > nm_f + 2$ implies $m_f \geq m_0$, where $m_0 = \min\{\, m \mid A_m(\alpha_{n-1}) = 0 \,\}$. In particular, $m_f = \ell m_0$ for some $\ell \geq 1$.*

Proof. The first claim follows from Remark 8, Corollary 9 and Lemma 10. For the second claim we note that $f^{(m)}(x)$ and $R_n^{(m)}(x)$ differ at most at nm elements of $\mathbb{F}_q$. Therefore if $q > nm_f+2$, then $R_n^{(m_f)}(c) = c$ for at least three distinct elements c in $\mathbb{F}_q$. But this implies that $R_n^{(m_f)}(x) \equiv x$. Therefore $f^{(m_f)}(x) \equiv x$ and $q > nm_f+2$ imply that $R_n^{(m_f)}(x) \equiv x$. □

Remark 12. One can construct permutations f, represented as in Equation (1), by an algorithm given in [2] when $R_n(x)$ and the poles $x_1, \ldots, x_n \in \mathbb{P}^1(\mathbb{F}_q)$ are prescribed.

Example 13. For $q = 29$, we fix $n = 4$, and choose $R_4(x) = (x-5)/6x$, with $\alpha_3 = -1$, being a root of $A_3(T)$, i.e., $m_0 = 3$, (and hence of $A_6(T)$). Therefore $R_4^{(3)}(x) \equiv x$. We prescribe the poles as $(x_1, x_2, x_3, x_4) = (27, 16, 5, 0)$, and as in [2] we determine $(a_1, a_2, a_3, a_4) = (2, 8, 7, 14)$, so that, $f(x) = ((((x+2)^{27} + 8)^{27} + 7)^{27} + 14)^{27}$. It can also be checked in this case that $\operatorname{ord}_{S_q}(f) = 6$.

In the special case of polynomials f in $\mathcal{C}_{2,3}$ we obtain the following corollary.

Corollary 14. *Consider the permutation polynomial $f = (((x+a)^{q-2}+b)^{q-2}+c)^{q-2}$ with $f(0) = 0$ and $a(b^2+4) \neq 0$. Then $R_3^{(m)} \equiv x$ if and only if b is a root of the polynomial*

$$A_m(T) = \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-j-1}{j} T^{m-2j-1} \,. \tag{14}$$

In particular, putting $m_0 = \min\{m \mid A_m(b) = 0\}$, and $\operatorname{ord}_{S_q}(f) = m_f$, we have $m_f \geq m_0$, when $q > 3m_f + 2$.

Another result on $\operatorname{ord}_{S_q}(f)$ for a polynomial f with $\operatorname{Crk}(f) = 3$ can be given as follows.

Proposition 15. *Let $f(x) = (((x+a)^{q-2}+b)^{q-2}+c)^{q-2} \in \mathbb{F}_q[x]$, with $f(0)=0$ and $a(b^2+4) \neq 0$. Put $m_f = \mathrm{ord}_{S_q}(f)$. Suppose $q > 3m_f + 2$. If the order of $(b+\gamma(b))/2$ in the multiplicative group $\mathbb{F}_{q^2}^*$ is k, where $\gamma(b)^2 = b^2+4$, then $m_f \geq m$, where m is given by*

$$m = \begin{cases} k/2, & \text{if } k \equiv 0 \mod 8, \\ k, & \text{if } k \equiv 2, 6 \mod 8, \\ k/4, & \text{if } k \equiv 4 \mod 8, \\ 2k, & \text{if } k \equiv 1, 3, 5, 7 \mod 8. \end{cases}$$

Proof. Since $a \neq 0$, the assumption $f(0) = 0$ implies that $abc + a + c = 0$, i.e., $\beta_3 = 0$. This shows that $f \in \mathcal{C}_{2,3}$. Since $\alpha_4 = b$ and $b^2 + 4 \neq 0$, Lemma 6 implies that $R_3^{(m)} \equiv x$ if and only if the distinct eigenvalues satisfy $\lambda_1^m = \lambda_2^m$. Then the argument follows from $\lambda_1^{2m} = (-1)^m$ as $\lambda_1\lambda_2 = -1$. □

Example 16. (1) Let $f(x) = (((x+7)^{71}+14)^{71}+25)^{71}$ be a permutation over $\mathbb{F}_{73}$. In this case, we have $b^2+4 = 54$. Then for $\gamma(b) = 28$, the order k of the element $(b+\gamma(b))/2$ is 24 and $\mathrm{ord}_{S_q}(f) = 12 = k/2$. Note that $b = 14$ is a root of $A_{12}(T)$ given in Equation (14), but it is not root of $A_m(T)$ for any $m < 12$.

(2) Let $f(x) = (((x+13)^{41}+13)^{41}+28)^{41}$ be a permutation over $\mathbb{F}_{43}$. In this case, we have $b^2+4 = 1$. Then for $\gamma(b) = 1$, the order k of the element $(b+\gamma(b))/2$ is 6 and $\mathrm{ord}_{S_q}(f) = 6 = k$. We remark that $b = 13$ is not a root of A_m for any $m < 6$.

(3) If we choose $\gamma(b) = -1$ in Example (2), then we have $\mathrm{ord}_{S_q}(f) = 6 = 2k$.

Acknowledgement

The initial work on this project began during “Women in Numbers Europe 2 (WIN-E2)” workshop, held in the Lorentz Centre, Leiden in September 2016. The authors are grateful to the Lorentz Centre and all supporting institutions for making this conference and collaboration possible. They would especially like to thank the organisers of WIN-E2, Irene Bouw, Rachel Newton and Ekin Özman for all of their hard work, as this resulted in an extremely fruitful and enjoyable meeting.

The authors N.A.; A.O.; V.P.; L.Q. and A.T. are partially supported by H.C. Ørsted COFUND Post-doc Fellowship from the project “Algebraic curves with many rational points”; Federal Ministry of Education and Science, grant No.05-39-3663-1/14; an EPSRC studentship; CNPq, PDE grant number 200434/2015-2 and TUBİTAK project number 114F432, respectively.

References

[1] N. Anbar, A. Odžak, V. Patel, L. Quoos, A. Somoza, A. Topuzoğlu, 'On the difference of permutation polynomials', preprint.

[2] E. Aksoy, A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, 'On the Carlitz rank of permutation polynomials', *Finite Fields and Their Applications*, **15** (2009), 428–440.

[3] L. Carlitz, 'Permutations in a finite field', *Proc. Amer. Math. Soc.*, **4** (1953), 538.

[4] S. Chowla, H. Zassenhaus, 'Some conjectures concerning finite fields', *Nor. Vidensk. Selsk. Forh. (Trondheim)*, **41** (1968), 34–35.

[5] S.D. Cohen, 'Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials', *Can. Math. Bull.*, **33** (1990), 230–234.

[6] S.D. Cohen, G.L. Mullen, P.J.-S. Shiue, 'The difference between permutation polynomials over finite fields', *Proc. Amer. Math. Soc.*, **123** (1995), 2011–2015.

[7] A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, 'On the cycle structure of permutation polynomials', *Finite Fields and Their Applications*, **14** (2008), 593–614.

[8] A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, 'Permutations with prescribed properties', Journal of Computational and Applied Mathematics, **259** (2014), 536–545.

[9] D. Gomez-Perez, A. Ostafe, A. Topuzoğlu, ' On the Carlitz rank of permutations of $\mathbb{F}_q$ and pseudorandom sequences', Journal of Complexity, **30** (2014), 279–289.

[10] J.W.P. Hirschfeld, G. Korchmros, F. Torres, *Algebraic curves over a finite field*, Princeton University Press, 2013.

[11] L. Işık, A. Topuzoğlu and A. Winterhof, 'Complete mappings and Carlitz rank', *Des. Codes Cryptogr.*, DOI 10.1007/s10623-016-0293-5.

[12] L. Işık, A. Topuzoğlu, 'A note on value set of polynomials over finite fields', preprint.

[13] C.F. Laywine, G. Mullen, 'Discrete mathematics using Latin squares', Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.

[14] R. Lidl and H. Niederreiter, 'Finite fields', Cambridge University Press, Cambridge, 1997.

[15] G. L. Mullen, 'Permutation polynomials over finite fields', Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991), vol. 141 of Lecture Notes in Pure and Appl. Math., 131–151, 1993.

[16] A. Muratovic-Ribic, E. Pasalic, 'A note on complete mapping polynomials over finite fields and their applications in cryptography', *Finite Fields Appl.*, **25** (2014), 306–315.

[17] H. Niederreiter, K.H. Robinson, 'Complete mappings of finite fields', *J. Aust. Math. Soc. A*, **33** (1982), 197–212.

[18] A. Ostafe, 'Iterations of rational functions: some algebraic and arithmetic aspects', Finite fields and their applications, 197–231, Radon Ser. Comput. Appl. Math., 11, De Gruyter, Berlin, 2013.

[19] R.-H. Schulz, 'On check digit systems using anti-symmetric mappings', in: Numbers, Information and Complexity (Bielefeld, 1998), 295–310, Kluwer Acad. Publ., Boston, MA, 2000.

[20] R. Shaheen, A. Winterhof, 'Permutations of finite fields for check digit systems', *Des. Codes Cryptogr.*, **57** (2010), 361–371.

[21] I.E. Shparlinski, 'Finite fields: theory and computation. The meeting point of number theory, computer science, coding theory and cryptography', *Mathematics and its Applications* **477**, Kluwer Academic Publishers, Dordrecht (1999).

[22] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, 'Investigations on bent and negabent functions via the nega-Hadamard transform', *IEEE Trans. Inf. Theory*, **58** (2012), 4064–4072.

[23] A. Topuzoğlu, 'Carlitz rank of permutations of finite fields: A survey', *J. Symb. Comput.*, **64** (2014), 53–66.

[24] A. Winterhof, 'Generalizations of complete mappings of finite fields and some applications', *Journal of Symbolic Computation*, **64** (2014), 42–52.