Complete mappings and Carlitz rank

Leyla Işık¹, Alev Topuzoğlu¹, Arne Winterhof²

¹ Sabancı University, Orhanli, 34956 Tuzla, İstanbul, Turkey
E-mail: {isikleyla,alev}@sabanciuniv.edu

² Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria
E-mail: arne.winterhof@oeaw.ac.at

Abstract

The well-known Chowla and Zassenhaus conjecture, proven by Cohen in 1990, states that for any $d \geq 2$ and any prime $p > (d^2 - 3d + 4)^2$ there is no complete mapping polynomial in $\mathbb{F}_p[x]$ of degree $d$.

For arbitrary finite fields $\mathbb{F}_q$, we give a similar result in terms of the Carlitz rank of a permutation polynomial rather than its degree. We prove that if $n < [q/2]$, then there is no complete mapping in $\mathbb{F}_q[x]$ of Carlitz rank $n$ of small linearity. We also determine how far permutation polynomials $f$ of Carlitz rank $n < [q/2]$ are from being complete, by studying value sets of $f + x$. We provide examples of complete mappings if $n = [q/2]$, which shows that the above bound cannot be improved in general.

Keywords: Permutation polynomials, complete mappings, Carlitz rank, value sets of polynomials

Mathematical Subject Classification: 11T06

1 Introduction

For any prime power $q$ let $\mathbb{F}_q$ be the finite field of $q$ elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial if it induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$. 
A polynomial \( f(x) \in \mathbb{F}_q[x] \) is a complete mapping polynomial (or a complete mapping) if both \( f(x) \) and \( f(x) + x \) are permutation polynomials of \( \mathbb{F}_q \). These polynomials were introduced by Mann in 1942, [12]. A detailed study of complete mapping polynomials over finite fields was carried out by Niederreiter and Robinson (1982, [14]). Complete mappings are pertinent to the construction of mutually orthogonal Latin squares, which can be used for the design of agricultural experiments, see for example [10]. Also due to other recently emerged applications such as check-digit systems [17, 18] and the construction of cryptographic functions [13, 19], complete mappings have attracted considerable attention, see also [8, 9, 15, 21, 22, 23, 24].

By a well-known result of Carlitz (1953), all permutation polynomials over \( \mathbb{F}_q \) with \( q \geq 3 \) can be generated by linear polynomials \( ax + b, \) \( a, b \in \mathbb{F}_q, \) \( a \neq 0, \) and inversions \( x^{q-2} = \begin{cases} 0, & x = 0, \\ x^{-1}, & x \neq 0 \end{cases} \) [2] or [11, Theorem 7.18]. Consequently, as pointed out in [4], any permutation \( f \) of \( \mathbb{F}_q \) can be represented by a polynomial of the form

\[
P_n(a_0, a_1, ..., a_{n+1}; x) = \cdots ((a_0 x + a_1)^{q-2} + a_2)^{q-2} \cdots + a_n)^{q-2} + a_{n+1},
\]

where \( a_i \neq 0, \) for \( i = 0, 2, \ldots, n. \) Note that this representation is not unique, and \( n \) is not necessarily minimal. Accordingly the authors of [1] 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 \( \text{Crk}(f) \). In other words, for \( q \geq 4, \text{Crk}(f) = n \) if \( f \) is a composition of at least \( n \) inversions \( x^{q-2} \) and \( n \) or \( n + 1 \) linear polynomials (depending on \( a_{n+1} \) being zero or not). This concept, introduced in the last decade, has already found interesting applications in diverse areas, see [5, 7, 16].

The following theorem states the well-known conjecture of Chowla and Zassenhaus (1968) [3], which was proven by Cohen [4] 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 \( \mathbb{F}_p. \)

Note that Cohen's theorem is not true for arbitrary finite fields without further restrictions. For example, for any \( 0 \neq a \in \mathbb{F}_p \) with \( a^{(p^r-1)/(p-1)} \neq (-1)^r \) it is easy to see that \( ax^p \) is a complete mapping.

Since the Carlitz rank of a permutation polynomial \( f \) over \( \mathbb{F}_q \) is an invariant of \( f, \) a natural question to ask is whether a non-existence result, similar to that stated in Theorem A, can be obtained in terms of the Carlitz rank.

We define the linearity \( \mathcal{L}(f) \) of a polynomial \( f \) over \( \mathbb{F}_q \) by

\[
\mathcal{L}(f) = \max_{a,b \in \mathbb{F}_q} |\{c \in \mathbb{F}_q : f(c) = ac + b\}|.
\]
Note that polynomials of large linearity are highly predictable and thus unsuitable in cryptography.

In this paper we show, see Theorem 1 below, that for any \( n < \left\lfloor \frac{q}{2} \right\rfloor \), there is no complete mapping polynomial of Carlitz rank \( n \) and linearity \( L(f) < \left\lfloor \frac{(q + 5)}{2} \right\rfloor \).

We also answer the following two questions that immediately arise. Firstly one wonders how far the non-complete mapping \( f \) in the above setting is from being complete. This question can be quantified by considering the number \( |V_{f+x}| \) of elements in the image of the polynomial \( f + x \). Theorem 3 presents bounds for \( |V_{f+x}| \). Secondly one would ask if the bound \( q > 2n + 1 \) can be improved. This is not possible in general, see Example 2 below.

2 Preliminaries

Let \( f(x) \) be a permutation polynomial over \( \mathbb{F}_q \). Suppose that \( f \) has a representation \( P_n \) as in (1) for \( n \geq 1 \). We follow the notation of [20] and put

\[
f(x) = P_n(a_0, a_1, ..., a_{n+1}; x).
\]

Since we are interested in complete mapping polynomials, the value of \( a_{n+1} \) is irrelevant. Also, by using the substitution \( x \mapsto x - a_0^{-1}a_1 \), we see that the size of the value set of \( f(x) + x \) does not depend on \( a_1 \). Therefore we may restrict ourselves to the case \( a_1 = a_{n+1} = 0 \). We relabel the coefficients accordingly, as \( c_0 = a_0, c_i = a_{i+1} \) for \( i = 1, ..., n - 1 \), and use the notation

\[
f(x) = P_n(c_0, ..., c_{n-1}; x) =: P_n(x). \tag{2}
\]

The representation of a permutation \( f \) as in (1) (or in (2)) enables approximation of \( f \) by a fractional linear transformation \( R_n \) as described below.

Following the terminology of [1], the \( n \)th convergent \( R_n(x) \) can be associated to \( f \), which is defined as

\[
R_n(x) = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n}, \tag{3}
\]

where

\[
\alpha_k = c_{k-1}x + c_{k-2} \quad \text{and} \quad \beta_k = c_{k-1}x + c_{k-2},
\]

for \( k \geq 2 \) and \( \alpha_0 = 0, \alpha_1 = c_0, \beta_0 = 1, \beta_1 = 0 \).

The set of \textit{poles} \( \mathcal{O}_n \) is defined as

\[
\mathcal{O}_n = \{x_i : x_i = -\frac{\beta_i}{\alpha_i}, i = 1, \ldots, n\} \subset \mathbb{F}_q \cup \{\infty\}.
\]
where the elements of $O_n$ are not necessarily distinct. We note that
\[ f(c) = P_n(c) = R_n(c) \quad \text{for} \ c \in \mathbb{F}_q \setminus O_n. \] (4)

## 3 A non-existence result

In this section we show that any complete mapping must have either high Carlitz rank or high linearity.

**Theorem 1.** If $f(x)$ is a complete mapping of $\mathbb{F}_q$, then we have either
\[
\mathcal{L}(f) \geq \left\lfloor \frac{q+5}{2} \right\rfloor
\]
or
\[
Crk(f) \geq \left\lfloor \frac{q}{2} \right\rfloor.
\]

**Proof.** Let $f(x)$ be of the form (2) with $n = Crk(f)$ and put $F(x) = f(x) + x$. For $n = 0$ we have $\mathcal{L}(f) = q$. Hence, we may assume $n \geq 1$.

If $\alpha_n = 0$, then $R_n(x)$ defined by (3) is a polynomial of degree 1 with $R_n(c) = f(c)$ for all $c \in \mathbb{F}_q \setminus O_n$ by (4) and thus $\mathcal{L}(f) \geq q - n + 1$. Since otherwise the result is trivial, we may assume $n \leq \lfloor q/2 \rfloor - 1$ and thus $\mathcal{L}(f) \geq q + 2 - \lfloor q/2 \rfloor = \lfloor (q+5)/2 \rfloor$.

Now we assume $\alpha_n \neq 0$.

We note that the first pole $x_1$ is 0, since $\beta_1 = 0$. Observe that
\[
F(c) = R_n(c) + c = \frac{\alpha_n c^2 + (\alpha_{n-1} + \beta_n)c + \beta_{n-1}}{\alpha_n c + \beta_n}
\] (5)
for any $c \in \mathbb{F}_q \setminus O_n$. It is also easy to show that
\[
\alpha_n \beta_{n-1} - \alpha_{n-1} \beta_n = (-1)^{n-1} c_0, \quad n \geq 1.
\] (6)

First we assume that $q$ is odd.

For any $u \in \mathbb{F}_q$ we study the quadratic equation
\[
R_n(x) + x = u + (\alpha_{n-1} - \beta_n)\alpha_n^{-1},
\] (7)
that is,
\[
x^2 + (2\alpha_n^{-1}\beta_n - u)x + ((-1)^{n-1}c_0 + \beta_n^2 - u\alpha_n\beta_n)\alpha_n^{-2} = 0
\] (8)
by (5) and (6). This equation has at most two different solutions \( c \in \mathbb{F}_q \setminus \{x_n\} \) and we have exactly two solutions if its discriminant

\[
D_u = u^2 + 4(-1)^n c_0 \alpha_n^{-2}
\]  

(9)
is a square in \( \mathbb{F}_q^* \). Note that

\[
\frac{1 + \eta(D_u)}{2} = \begin{cases} 
1, & D_u \text{ is a square in } \mathbb{F}_q^*, \\
0, & D_u \text{ is a nonsquare in } \mathbb{F}_q^*, \\
1/2, & D_u = 0,
\end{cases}
\]

where \( \eta \) is the quadratic character of \( \mathbb{F}_q \). Moreover, either \( D_u = 0 \) for two values of \( u \), that is, \((-1)^n c_0 \) is a square, or there is no value \( u \) with \( D_u = 0 \). Hence, the number \( N \) of the elements \( u \in \mathbb{F}_q \) for which \( D_u \) is a square in \( \mathbb{F}_q^* \) can be expressed as

\[
N = \frac{1}{2} \sum_{u \in \mathbb{F}_q, D_u \neq 0} (1 + \eta(D_u)) = -\frac{1 + \eta((-1)^n c_0)}{2} + \frac{1}{2} \sum_{u \in \mathbb{F}_q} (1 + \eta(D_u)) = \frac{q - 1 - \eta((-1)^n c_0)}{2} + \frac{1}{2} \sum_{u \in \mathbb{F}_q} \eta(D_u) = \frac{q - 2 - \eta((-1)^n c_0)}{2}.
\]

by \[\Xi\] Theorem 5.48.

Now assume that \( F \) is a permutation. Then at least one of these two solutions must be a pole \( c \in \mathcal{O}_n \setminus \{x_n\} \). Hence,

\[
n \geq \frac{q - \eta((-1)^n c_0)}{2} \geq \frac{q - 1}{2}.
\]

For even \( q \) we can argue similarly. Note that a quadratic equation \( x^2 + ax + b \) has exactly two solutions whenever \( a \neq 0 \) and \( \text{Tr}(a^{-2}b) = 0 \), where \( \text{Tr} \) denotes the absolute trace of \( \mathbb{F}_q \), see \[\Xi\] Theorem 2.25. We have to determine the number \( N \) of \( u \) such that (8) has two solutions in \( \mathbb{F}_q \), that is, the number of \( u \neq 0 \) with

\[
0 = \text{Tr} \left( \frac{\alpha_n \beta_n u + \beta_n^2 + c_0}{\alpha_n^2 u^2} \right) = \text{Tr} \left( \frac{\beta_n}{\alpha_n u} + \frac{\beta_n + c_0^{q/2}}{\alpha_n u} \right) = \text{Tr} \left( \frac{c_0^{q/2}}{\alpha_n u} \right). \tag{10}
\]

Since \( u \mapsto u^{-1} \) is a bijection of \( \mathbb{F}_q^* \) and \( \text{Tr} \) is 2-to-1 on \( \mathbb{F}_q \), we get \( N = q/2 - 1 \). Hence, if \( F \) is a permutation, then \( \mathcal{O}_n \) contains at least \( n \geq N + 1 = \frac{q}{2} \) different poles and the result follows. \( \square \)
Remark. Note that complete mappings of high linearity, that is, polynomials $f(x)$ with $n$th convergent $R_n(x)$ and $\alpha_n = 0$ (or $x_n = \infty$) are not suitable for cryptographic applications. Hence, in the following we focus on the case $\alpha_n \neq 0$ (or $x_n \neq \infty$). Note that $\alpha_1 \alpha_2 \neq 0$ and thus $\infty$ is not a pole if $n = 1$ or $n = 2$.

Now we provide examples of complete mappings of Carlitz rank $n = \lfloor q/2 \rfloor$ with $L(f) < \lfloor (q + 5)/2 \rfloor$.

**Example 2.** It is easy to check that $f(x) = \gamma(x^4 + 1) + \gamma^{-1}(x^2 + x) \in \mathbb{F}_8[x]$ is a complete mapping of $\mathbb{F}_8 = \mathbb{F}_2(\gamma)$, where $\gamma$ is a root of the polynomial $x^3 + x + 1$ which is irreducible over $\mathbb{F}_2$. As a polynomial of degree 4 its linearity is at most 4 and by Theorem 1 its Carlitz rank is at least 4. Verifying

$$f(c) = (((\gamma c)^6 + 1)^6 + \gamma^{-3})^6 + 1)^6,$$

we see that $Crk(f) = 4$ and Theorem 1 is in general tight in the case of even $q$.

Analogously, $f(x) = x^4 - x^3 + 3x^2 - x + 1 \in \mathbb{F}_7[x]$ satisfies

$$f(c) = (((c^5 + 3)^5 + 3)^5,$$

and has Carlitz rank 3. Hence, the bound of Theorem 1 is attained for odd $q$, as well.

Many similar examples lead the authors to believe that there is a complete mapping of $\mathbb{F}_q$ of Carlitz rank $n = \lfloor q/2 \rfloor$ and small linearity for infinitely many prime powers $q \geq 7$. This can be checked for $7 \leq q \leq 25$.

### 4 The size of $V_{f+x}$

In this section we study the set $V_{f+x} = \{f(\delta) + \delta : \delta \in \mathbb{F}_q\}$ for any $f$ satisfying (II) with $\alpha_n \neq 0$. Theorem 1 implies that if $n < \lfloor q/2 \rfloor$, we have $|V_{f+x}| < q$. Here we aim to determine how large the gap between $q$ and $|V_{f+x}|$ is. Theorem 3 below shows that $q - |V_{f+x}| \geq (q - 2 \cdot Crk(f) - 1)/2$, that is, it is large if the Carlitz rank of $f$ is small, as one would expect. We present the result in a slightly more general form.

**Theorem 3.** For $\alpha_{n-1}, \beta_{n-1}, \alpha_n, \beta_n \in \mathbb{F}_q$ with $\alpha_n \neq 0$ and $\alpha_{n-1}\beta_n - \alpha_n\beta_{n-1} \neq 0$, let $F$ be any self-mapping of $\mathbb{F}_q$ satisfying

$$F(c) = \frac{\alpha_{n-1}c + \beta_{n-1}}{\alpha_nc + \beta_n} + c \quad (11)$$
for at least \( q - n \) different \( c \in \mathbb{F}_q \). Then we have

\[
\left\lceil \frac{q-n}{2} \right\rceil \leq |V_F| \leq \min \left\{ n + \left\lfloor \frac{q+1}{2} \right\rfloor, q \right\}.
\]

**Proof.** Consider the set \( S \) of elements \( c \in \mathbb{F}_q \) satisfying (11), which has cardinality \( |S| \geq q - n \). At most two different elements of \( S \) can have the same value \( u \) since \( F(c) = u \) is a quadratic equation in \( c \) because of the conditions on \( \alpha_{n-1}, \beta_{n-1}, \alpha_n, \beta_n \). Therefore, \( |V_F| \geq (q - n)/2 \). Now the elements of \( \mathbb{F}_q \setminus S \) can attain at most \( n \) different values of \( F \). If \( q \) is odd, the discriminant \( D_u \) of \( F(c) = u \) is a quadratic polynomial in \( u \) and is 0 for at most two different values \( u \in V_F \). For these two possible \( u \) we have exactly one solution \( c \) of \( F(c) = u \). For all other \( u \) we have either two or no solutions. Hence, we get similarly \( |V_F| \leq n + (q + 1)/2 \). If \( q \) is even, the quadratic equation \( F(c) = u \) has a unique solution for exactly one \( u \) and two or no solutions otherwise. Hence, we get similarly \( |V_F| \leq n + q/2 \).

For the special cases \( n = 1 \) and \( n = 2 \) one can provide exact formulas for \( |V_{f+x}| \).

**Proposition 4.** The size of the value set \( V_F \) of the polynomial

\[
F(x) = (c_0 x)^{q-2} + x \in \mathbb{F}_q[x],
\]

\( q > 2 \), with \( c_0 \neq 0 \) is

\[
|V_F| = \begin{cases} 
(q + 1 + \eta(c_0) - \eta(-c_0))/2, & q \text{ odd}, \\
q/2, & q \text{ even},
\end{cases}
\]

where \( \eta \) denotes the quadratic character of \( \mathbb{F}_q \).

**Proof.** We start with odd \( q \). We have \( F(0) = 0 = F(\pm(-c_0)^{-1/2}) \) and thus \( F(c) = 0 \) is attained for \( 2 + \eta(-c_0) \) different \( c \in \mathbb{F}_q \). The discriminant

\[
D_u = u^2 - 4c_0^{-1}
\]

of \( x^2 - ux + c_0^{-1} \) has no zeros if \( c_0 \) is a non-square. If \( c_0 \) is a square, for the two zeros of \( D_u \) there is a unique solution \( c = u/2 \) of \( F(c) = u \). For the remaining \( u \) there are two or no solutions of \( F(c) = u \). Collecting everything we get the result.

For even \( q \) we have \( F(0) = F(c_0^{-q/2}) = 0 \) and no further zeros of \( F \). For all \( u \neq 0 \) there are either two or no solutions of \( F(c) = u \) and we get the result. \( \square \)
Proposition 5. The size of the value set of \( F(x) = ((c_0 x)^{q-2} + c_1)^{q-2} + x \), \( q > 2 \), with \( c_0, c_1, 4c_0 + 1, c_0 + 4 \neq 0 \) is

\[
|V_F| = \begin{cases} 
\frac{q + 2 - \eta(4c_0+1) - \eta(c_0^2 + 4c_0) + \eta(-c_0)}{2}, & c_0 \neq -1, \\
\frac{q - \eta(-3)}{2}, & c_0 = -1,
\end{cases}
\]

if \( q \) is odd. For even \( q \) and \( c_0, c_1 \neq 0 \), we get

\[
|V_F| = \frac{q}{2} + \begin{cases} 
Tr(c_0) + Tr(c_0^{-1}), & c_0 \neq 1, \\
Tr(1) - 1, & c_0 = 1,
\end{cases}
\]

where \( Tr \) is the absolute trace of \( \mathbb{F}_q \) and we identify \( \mathbb{F}_2 \) with the integers \( \{0, 1\} \).

Proof. Note that \( O_2 = \{0, -(c_0c_1)^{-1}\} \). We have \( F(0) = c_1^{-1} \) and

\[
F(-(c_0c_1)^{-1}) = -(c_0c_1)^{-1}.
\]

Note that both values coincide if \( c_0 = -1 \). \( \{7\} \) simplifies to \( R_2(x) + x = u + c_1^{-1} - (c_0c_1)^{-1} \). Hence, we get \( R_2(c) + c = F(0) \) if \( u = (c_0c_1)^{-1} =: u_1 \) and \( R_2(c) + c = F(-(c_0c_1)^{-1}) \) if \( u = c_1^{-1} =: u_2 \).

Again we deal with odd \( q \) first.

By \( \{9\} \) we get the discriminants

\[
D_{u_1} = (4c_0 + 1)(c_0 c_1)^{-2} \quad \text{and} \quad D_{u_2} = (c_0 + 4)c_0(c_0 c_1)^{-2}.
\]

Hence there are \( 1 + \eta(4c_0 + 1) \) additional \( c \) with \( R_2(c) + c = F(0) \) and \( 1 + \eta((c_0 + 4)c_0) \) additional \( c \) with \( R_2(c) + c = F(-(c_0c_1)^{-1}) \). Now verify that there is a \( u \), namely \( u = (1 - c_0)(c_0c_1)^{-1} \), such that \( x = 0 \) is a solution of \( \{8\} \). If \( c_0 = -1, x = 0 \) is the unique solution for this \( u \). However, for \( x = -(c_0c_1)^{-1} \) there is no such \( u \). Finally, there are \( 1 + \eta(-c_0) \) values \( u \) with \( D_u = 0 \) such that \( \{8\} \) has a unique solution. Altogether we have

\[
4 + \eta(-c_0) + \frac{q - 6 - \eta(4c_0 + 1) - \eta((c_0 + 4)c_0) - \eta(-c_0)}{2}
\]

values in \( V_F \) if \( c_0 \neq -1 \) and the first result follows. For \( c_0 = -1 \) we get

\[
|V_F| = 2 + \frac{q - 4 - \eta(-3)}{2}.
\]

Now we consider even \( q \). By \( \{10\} \) and

\[
Tr \left( \frac{c_0}{c_0}^{q/2} \right) = Tr(c_0) \quad \text{and} \quad Tr \left( \frac{c_0}{c_0}^{q/2} \right) = Tr(c_0^{-1})
\]
the number of $c$ with $F(c) = F(0)$ (including $c = 0$) is $3 - 2Tr(c_0)$ and the number of $c$ with $F(c) = F((c_0c_1)^{-1})$ is $3 - 2Tr(c_0^{-1})$. For $u = 0$ there is a unique solution $x \neq 0$ of (8) if $c_0 \neq 1$. Moreover, $x = 0$ is a solution of (8) for one $u$ which has already been counted above. Hence, we get

$$|V_F| = 4 + \frac{q - 8 + 2Tr(c_0) + 2Tr(c_0^{-1})}{2}$$

if $c_0 \neq 1$ and the result follows.

If $c_0 = 1$ we have $F(0) = F((c_0c_1)^{-1}) = c_1^{-1}$ and $c_1^{-1}$ is attained $4 - 2Tr(c_0)$ times. Moreover, the $u$ with unique solution (8) corresponds to the solution $x = 0$. Hence we get

$$|V_F| = 1 + \frac{q - 4 + 2Tr(1)}{2}$$

and the result follows. 

5 Acknowledgement

L.I. and A.T. were supported by TUBITAK project number 114F432. A.W. is partially supported by the Austrian Science Fund FWF Project F5511-N26 which is part of the Special Research Program ”Quasi-Monte Carlo Methods: Theory and Applications”.

References

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

[2] L. Carlitz, Permutations in a finite field, Proc. American Mathematical Society 4 (1953), 538.

[3] S. Chowla, H. Zassenhaus, Some conjectures concerning finite fields, Norske Videnskabers Selskabs Forhandlinger (Trondheim) 41 (1968), 34–35.

[4] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the cycle structure of permutation polynomials. Finite Fields and Their Applications 14 (2008), 593–614.
[5] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, Permutations with prescribed properties, Journal of Computational and Applied Mathematics 259 B (2014), 536–545.

[6] S.D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, Canada Mathematical Bulletin 33 (1990), 230–234.

[7] 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.

[8] X. Guangkui, X. Cao, Complete permutation polynomials over finite fields of odd characteristic, Finite Fields and Their Applications 31 (2015), 228–240.

[9] L. Işik, On complete mappings and value sets of polynomials over finite fields, PhD Thesis. Sabancı University, 2015.

[10] 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.

[11] R. Lidl, H. Niederreiter, Finite fields. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[12] H.B. Mann, The construction of orthogonal Latin squares, Annals of Mathematical Statistics 13 (1942), 418–423.

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

[14] H. Niederreiter, K.H. Robinson, Complete mappings of finite fields, Journal of Australian Mathematical Society A 33 (1982), 197–212.

[15] H. Niederreiter, A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, Discrete Mathematics 295 (2005), 161–171.

[16] F. Pausinger, A. Topuzoğlu, Permutations of finite fields and uniform distribution modulo 1, in H. Niederreiter, A. Ostafe, D. Panario, A. Winterhof (eds.), Algebraic Curves and Finite Fields, Radon Series on Applied and Computational Mathematics 16 (2014), 145–160.
[17] 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.

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

[19] 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.

[20] A. Topuzoğlu, *Carlitz rank of permutations of finite fields: A survey*, Journal of Symbolic Computation 64 (2014), 53–66.

[21] Z. Tu, X. Zeng, L. Hu, *Several classes of complete permutation polynomials*, Finite Fields and Their Applications 25 (2014), 182–193.

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

[23] G. Wu, N. Li, T. Helleseth, Y. Zhang, *Some classes of monomial complete permutation polynomials over finite fields of characteristic two*, Finite Fields and Their Applications 28 (2014), 148–165.

[24] Z. Zha, L. Hu, X. Cao, *Constructing permutations and complete permutations over finite fields via subfield-valued polynomials*, Finite Fields and Their Applications 31 (2015), 162–177.