PERMUTATION POLYNOMIALS WITH CARLITZ RANK 2

JOSÉ ALVES OLIVEIRA AND F. E. BROCHERO MARTÍNEZ

Abstract. Let \( \mathbb{F}_q \) denote the finite field with \( q \) elements. The Carlitz rank of a permutation polynomial is an important measure of complexity of the polynomial. In this paper we find the sharp lower bound for the weight of any permutation polynomial with Carlitz rank 2, improving the bound found by Gómez-Pérez, Ostafe and Topuzoğlu in that case.

1. Introduction

Let \( \mathbb{F}_q \) denote the finite field with \( q \) elements. A polynomial \( f(x) \in \mathbb{F}_q[x] \) is called a permutation polynomial over \( \mathbb{F}_q \) if the map \( a \mapsto f(a) \) permutes the elements of \( \mathbb{F}_q \). Important early contributions to the general theory can be found in Hermite [1] and Dickson [8]. In recent times, the study of permutation polynomial has intensified by their applications in cryptography and coding theory [3, 4, 5, 6], resulting in the emergence of several new classes of these types of polynomials.

Two polynomials \( f(x), g(x) \in \mathbb{F}_q[x] \) represent the same permutation of \( \mathbb{F}_q \) if \( f(a) = g(a) \) for all \( a \in \mathbb{F}_q \), i.e. \( f(x) \equiv g(x) \pmod{x^q - x} \). Characterizing permutation polynomials with few non null coefficients is one of the main questions involving these polynomials, because they have practical application. Permutation binomials and trinomials, for example, have been extensively explored [10, 11, 12, 13]. Therefore, relating the number of non null coefficients of a permutation polynomial to some other characteristic is an important problem, since this is a way of finding permutations with few coefficients.

Let \( \mathcal{S}_q \) be the set of permutations polynomials of \( \mathbb{F}_q \). A well known result of Carlitz [7] states that \( \mathcal{S}_q \) is generated by linear polynomials \( ax + b, a, b \in \mathbb{F}_q, a \neq 0 \), and \( x^q - 2 \). Thus, any permutation polynomial \( f(x) \) of \( \mathbb{F}_q \) can be represented by a polynomial of the form

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

with \( a_1, a_{n+1} \in \mathbb{F}_q \) and \( a_0, a_2, \ldots, a_n \in \mathbb{F}_q^* \), i.e. \( f(x) = P_n(x) \pmod{x^q - x} \). In fact, the polynomial \( f \) can be represented by several polynomials of the form (1) and thus we can define the following invariant of permutations.

Definition 1.1. Let \( f(x) \) a permutation polynomial of \( \mathbb{F}_q \). The smallest integer \( n \) for which exists a polynomial \( P_n(x) \) of the form (1) such that \( f(x) = P_n(x) \pmod{x^q - x} \) is called Carlitz rank of \( f \). We denote the Carlitz rank by \( \text{Crk}(f) \).

From now we will only use \( P_n(x) \) to denote a representation of a permutation polynomial \( f \) with \( \text{Crk}(f) = n \). Using the fact that

\[
x^{q-2} = \begin{cases} x^{-1}, & \text{se } x \neq 0; \\ 0, & \text{se } x = 0,
\end{cases}
\]

formally, we can see \( P_n(x) \) as

Date: December 11, 2019.
2010 Mathematics Subject Classification. 12E20 (primary) and 11T30(secondary).
Key words and phrases. Permutation Polynomial, Hermite Criteria, Carlitz Rank.
\[ a_{n+1} + \frac{1}{a_n + \ldots + \frac{1}{a_2 + \frac{1}{a_0 x + a_1}}}, \quad (2) \]

and its form the \( n \)th convergent

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

where \( \alpha_k := \alpha_{k-1} a_k + \alpha_{k-2} \) and \( \beta_k := \beta_{k-1} a_k + \beta_{k-2} \) for \( k \geq 2 \), where \( \alpha_0 := 0, \alpha_1 := a_0, \beta_0 := 1 \) and \( \beta_1 := a_1 \).

Let \( O_n \) define the set of poles as

\[ \left\{ \frac{-\beta_i}{\alpha_i} : i = 1 \ldots n \right\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}, \quad (4) \]

Clearly, \( P_n(x) = R_n(x) \) for all \( x \in \mathbb{F}_q \setminus O_n \) and thus

\[ f(x) = \frac{\alpha_{n+1} x + \beta_{n+1}}{\alpha_n x + \beta_n}, \quad \text{for all } x \in \mathbb{F}_q \setminus O_n. \quad (5) \]

In [2], the authors show the following relationship between the Carlitz rank and the degree of a permutation polynomial.

**Proposition 1.2.** Let \( f(x) \) be a permutation polynomial of degree \( d \) and Carlitz rank \( n \). Then

\[ n \geq q - 1 - d. \]

We called weight of \( f(x) \), denoted by \( \omega(f) \), the number of non null coefficients of a polynomial \( f(x) \). The following important result relating the Carlitz rank to the weight of a permutation polynomial was shown by Gómez-Pérez, Ostafe, and Topuzoğlu.

**Theorem 1.3.** [9] Let \( f(x) \) be a permutation polynomial of \( \mathbb{F}_q \) with degree \( \geq 2 \),

\[ f(x) = \sum_{i=1}^{w(f)} a_i x^{c_i} \text{ and } f(x) \neq c_1 + c_2 x^{q-2}, \]

for \( c_1, c_2 \in \mathbb{F}_q, c_2 \neq 0 \). Then

\[ Crk(f) > \frac{q}{\omega(f) + 2} - 1. \]

Fixing \( Crk(f) = n \), this theorem states that the lower bound for the weight of the polynomial is given by

\[ \omega(f) > \frac{q}{n + 1} - 2. \quad (6) \]

But this inequality is not optimal. In this paper, we study the relationship between permutation polynomials with Carlitz rank 2 and the weight of these. In our main result (Theorem 3.1) we present a improvement to the bound (6) in the case \( Crk(f) = 2 \).
Throughout this article, $\mathbb{F}_q$ denotes the finite field with $q$ elements, where $q$ is a power of a prime $p$. For any $a \in \mathbb{F}_q^*$, $\text{ord}_q(a)$ denotes the order of $a$ in the cyclic group $\mathbb{F}_q^*$. From now, $f(x) \equiv g(x)$ means $f(x) \equiv g(x) \pmod{x^t - x}$.

Lemma 2.1. Let $\mathbb{F}_q$ be a finite field with odd characteristic and $f(x) \in \mathbb{F}_q[x]$ be a permutation polynomial of $\mathbb{F}_q$ with $Crk(f) = 2$. Then there exist elements $a_0, a_1, a_2, a_3 \in \mathbb{F}_q$, where $a_0, a_2 \neq 0$, such that

$$f(x) \equiv a_2^{-1} \sum_{i=1}^{q-2} x^i (-a_0)^i [(a_1 - ia_2^{-1}) (a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i}] + a_3 + a_2^{-1} \left[ \frac{a_1}{a_1 + a_2^{-1}} + 1 - a_1^{q-1} \right].$$

Proof: By definition of Carlitz rank, there exists $a_0, a_1, a_2, a_3 \in \mathbb{F}_q$, com $a_0, a_2 \neq 0$, such that $f(x) = ((a_0 x + a_1)^{q-2} + a_2)^{q-2} + a_3$. By Equation (5),

$$f(a_0^{-1} x) \equiv_q \begin{cases} \mathcal{R}_2(x) = \frac{x + a_1}{a_2 x + a_1 a_2 + 1} + a_3, & \text{if } x \notin \{-a_1, -a_1 - a_2^{-1}\}; \\ a_2^{-1} + a_3, & \text{if } x = -a_1; \\ a_3, & \text{if } x = -(a_1 + a_2^{-1}). \end{cases}$$

Moreover, if $x \neq -(a_1 + a_2^{-1})$, it follows that

$$\frac{x + a_1}{a_2 x + a_1 a_2 + 1} + a_3 \equiv_q a_2^{-1} (x + a_1) (x + a_1 + a_2^{-1})^{q-2} + a_3 = a_2^{-1} (x + a_1) \sum_{i=0}^{q-2} \binom{q-2}{i} x^i (a_1 + a_2^{-1})^{q-2-i} + a_3 =: \mathcal{R}_2(x).$$

Thus $f(a_0^{-1} x) - \mathcal{R}_2(x) = 0$ for all elements in $x \in \mathbb{F}_q \setminus \{-a_1, -a_1 - a_2^{-1}\}$. In other hand, the polynomial $f(a_0^{-1} x) - \mathcal{R}_2(x)$ can also be written using the Lagrange’s Interpolation method:

$$f(a_0^{-1} x) - \mathcal{R}_2(x) \equiv_q \sum_{a \in \mathbb{F}_q} [f(a_0^{-1} a) - \mathcal{R}_2(a)] (1 - (x - a)^{q-1})$$

$$= (1 - (x + a_1)^{q-1}) a_2^{-1} + (1 - (x + a_1 + a_2^{-1})^{q-1}) \cdot 0 = (1 - (x + a_1)^{q-1}) a_2^{-1}.$$
So, we recovered a polynomial form of \( f \) as
\[
f(a_0^{-1}x) \equiv_q \mathcal{P}_2(x) + (1 - (x + a_1)^{q-1})a_2^{-1}
\]
\[
= a_2^{-1}(x + a_1) \sum_{i=0}^{q-2} \left( \frac{q-2}{i} \right) x^i \left( a_1 + a_2^{-1} \right)^{q-2-i} + a_3 + (1 - (x + a_1)^{q-1})a_2^{-1}
\]
\[
= a_2^{-1}(x + a_1) \sum_{i=0}^{q-2} \left( \frac{q-2}{i} \right) x^i \left( a_1 + a_2^{-1} \right)^{q-2-i} + a_3 + a_2^{-1} \sum_{i=0}^{q-1} \left( \frac{q-1}{i} \right) x^i a_1^{q-1-i}
\]
\[
\equiv_q a_2^{-1}(x + a_1) \sum_{i=0}^{q-2} (i+1)(-1)^i x^i \left( a_1 + a_2^{-1} \right)^{q-2-i} + a_3 + a_2^{-1} \sum_{i=0}^{q-1} (-1)^i x^i a_1^{q-1-i}
\]
\[
= a_2^{-1} \sum_{i=1}^{q-2} \frac{x^i}{(-1)^i} \left[ (a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i} \right] + a_3 + a_2^{-1} \left[ \frac{a_1}{a_1 + a_2} + 1 - a_1^{q-1} \right].
\]

Hence, we have
\[
f(x) \equiv_q a_2^{-1} \sum_{i=1}^{q-2} (-a_0)^i x^i \left[ (a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i} \right] + a_3 + a_2^{-1} \left[ \frac{a_1}{a_1 + a_2} + 1 - a_1^{q-1} \right],
\]
and the result is shown. \( \square \)

By the last lemma is clearly that we need to determinate which are the elements \( a_1, a_2 \) and \( a_3 \) for which \( (a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i} = 0, \ 1 \leq i \leq q-2 \), have the largest number of solutions. If \( a_1 + a_2^{-1} \neq 0 \), that equation is equivalent to
\[
a_1 + ia_2^{-1} = \left( \frac{a_1 + a_2^{-1}}{a_1} \right)^i (a_1 + a_2^{-1}). \tag{7}
\]

In the following lemmas we present the necessary theory to estimate the largest number of solutions of (7).

**Lemma 2.2.** Let \( \Omega \) be a finite set and \( f, g : \mathbb{Z} \to \Omega \) be periodic functions with period \( m \) and \( n \), respectively. If \( f|_{[1,m]} \) e \( g|_{[1,n]} \) are injective functions and \( \gcd(m, n) = 1 \), then
\[
|\{i \in [1, mn] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq m\} \cap \{g(i) : 0 \leq i \leq n\}|.
\]

**Proof:** Let \( j \) be a element in \([1, mn]\). If \( f(j) = g(j) \), then \( f(jf) = g(jg) \) for some \( jf \in [1, m] \) and \( jg \in [1, n] \). Reciprocally, if \( jf \in [1, m] \) and \( jg \in [1, n] \) are such that \( f(jf) = g(jg) \), Chinese Remainder Theorem states that exists only one \( j \in [1, mn] \) such that
\[
\begin{align*}
  j &\equiv jf \pmod{m}; \\
  j &\equiv jg \pmod{n}.
\end{align*}
\]
Thus,
\[
|\{i \in [1, mn] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq m\} \cap \{g(i) : 0 \leq i \leq n\}|.
\]
\( \square \)

**Corollary 2.3.** Let \( \Omega \) be a finite set and \( l, k \) be integers. Let \( f, g : \mathbb{Z} \to \Omega \) be periodic functions with period \( m \) and \( n \), respectively. If \( f|_{[1,m]} \) e \( g|_{[1,n]} \) are injective functions and \( \gcd(m, n) = 1 \), then
\[
|\{i \in [k + 1, k + lmn] : f(i) = g(i)\}| \leq l \times \min\{m, n\}.
\]
Lemma 2.4. Let \( \mathbb{F}_q \) be a finite field with odd characteristic and \( \gamma \in \mathbb{F}_q \) and \( c, d \in \mathbb{F}_q \), where \( c \neq 0 \). For \( 3 \leq M \leq p \), we have

\[
|\{1 \leq i \leq M : \gamma^{i+1} = ic + d\}| \leq \sqrt{\frac{3M}{2} - \frac{39}{16} + \frac{5}{4}}.
\]

Proof: For \( \gamma \in \{0, 1\} \) the inequality is trivial. Then let \( \gamma \in \mathbb{F}_q \setminus \{0, 1\} \) and define

\[
C_\gamma := \{1 \leq i \leq M : \gamma^{i+1} = ic + d\}, \quad t := |C_\gamma| \text{ and } l := \text{ord}_{\mathbb{F}_q}(\gamma).
\]

If \( i_1, i_2 \in C_\gamma \), with \( i_1 \neq i_2 \), then \( \gamma^{i_2+1} = i_2c + d \) and \( \gamma^{i_1+1} = i_1c + d \) implies

\[
\gamma^{i_2+1} - \gamma^{i_1+1} = i_2c - i_1c
\]

\[
\gamma^{i_2+1} - \gamma^{i_1+1} = (i_2 - i_1)c
\]

\[
\gamma^{i_2+1}(\gamma^{j_2-j_1} - 1) = (i_2 - i_1)c.
\]

We observe that if \( l|(i_2 - i_1) \), then \( (i_2 - i_1)c = 0 \), hence \( i_1 = i_2 \). Then we can assume \( i_2 - i_1 \equiv 0 \pmod{l} \) to get

\[
\gamma^{i_1+1} = (i_2 - i_1)\frac{c}{\gamma^{j_2-j_1} - 1}.
\]

Now, let \( j_1, j_2 \in C_\gamma \), with \( j_1 \neq j_2 \) and \( j_2 - j_1 = i_2 - i_1 \). Then

\[
j_1c + d = \gamma^{j_1+1} = (j_2 - j_1)\frac{c}{\gamma^{j_2-j_1} - 1} = (i_2 - i_1)\frac{c}{\gamma^{j_2-j_1} - 1} = \gamma^{i_1+1} = i_1c + d.
\]

Using the fact that \( c \neq 0 \), we have \( j_1 = i_1 \) and \( j_2 = i_2 \), so the difference between two distinct pairs of elements in \( C_\gamma \) is never the same. Therefore, assuming \( C_\gamma = \{i_1 < \cdots < i_t\} \), the values

\[
(i_2 - i_1), (i_3 - i_2), \ldots, (i_t - i_{t-1}),
\]

\[
(i_3 - i_1), (i_5 - i_3), \ldots, (i_2\frac{3}{2}i|1 + 1 - i_2\frac{3}{2}i|1 - 1),
\]

\[
(i_4 - i_2), (i_6 - i_4), \ldots, (i_2\frac{3}{2}i| - i_2\frac{3}{2}i| - 2)
\]

are all different. The quantity of values above is \( 2t - 3 \). Besides that,

\[
L_1 := (i_2 - i_1) + (i_3 - i_2) + \cdots + (i_t - i_{t-1}) \leq M - 1,
\]

\[
L_2 := (i_3 - i_1) + \cdots + (i_2\frac{3}{2}i| + 1 - i_2\frac{3}{2}i| - 1) + (i_4 - i_2) + \cdots + (i_2\frac{3}{2}i| - i_2\frac{3}{2}i| - 2) \leq 2M - 4
\]

Thus,

\[
\frac{(2t - 3)(2t - 2)}{2} = 1 + 2 + \cdots + (2t - 3) \leq L_1 + L_2 \leq 3M - 5,
\]

it follows that

\[
t \leq \sqrt{\frac{3M}{2} - \frac{39}{16} + \frac{5}{4}}.
\]

Observe that this inequality is not optimal. In fact, we do not know a sharp version for this result. We checked via computer that there exists a constant \( k > 0 \) such that

\[
|\{1 \leq i \leq p \leq 2 : \gamma^{i+1} = ic + d\}| < k \cdot \log(p)
\]

for \( p < 10^6 \).

Lemma 2.5. Let \( p \) be an odd prime and \( n > 1 \) an integer. Let \( \mathbb{F}_q \) be a finite field with \( q = p^n \) and let \( \gamma \in \mathbb{F}_q \setminus \mathbb{F}_p \). Then

\[
|\{1 \leq i \leq q - 2 : \gamma^{i+1} = i(1 - \gamma + 1)\}| \leq \frac{q}{p}.
\]
Proof: We define \( l = \text{ord}_{\mathbb{F}_q}(\gamma) \). In order to prove the result, we consider two cases: \( l > p \) and \( l < p \).

Firstly, we assume \( l > p \). We note that \( \gamma^{i+1} \) have period \( l \) and \( i(1 - \gamma) + 1 \) have period \( p \). Let \( f(i) := \gamma^{i+1} - i(1 - \gamma) - 1 \). By Corollary 2.3, the number of roots of \( f(i) \) in \([1, lp\lfloor\frac{q-2}{lp}\rfloor]\) is at most \( p\lfloor\frac{q-2}{lp}\rfloor \). In the interval \([lp\lfloor\frac{q-2}{lp}\rfloor, q-2]\) the number of roots of \( f(i) \) is at most \( p \), since \( q - 2 - lp\lfloor\frac{q-2}{lp}\rfloor < lp \). Therefore, we divide the problem in the following subcases:

If \( n = 2 \), since \( l > p \),
\[
\left\lfloor\frac{q-2}{lp}\right\rfloor + p = \left\lfloor\frac{p^2-2}{lp}\right\rfloor + p = \frac{q}{p}.
\]

If \( n = 3 \), since \((p+1) \nmid (p^3-1)\), then \( l \) is at least \( p + 2 \). Thus
\[
p \left\lfloor\frac{q-2}{lp}\right\rfloor + p = p \left\lfloor\frac{p^3-2}{lp}\right\rfloor + p < p\frac{p^3-2}{lp} + p \leq \frac{p^3-2}{p} + p \leq p^3 = \frac{p^3}{p} = \frac{q}{p}.
\]

If \( n \geq 4 \), since \( l \geq p + 1 \), we have
\[
p \left\lfloor\frac{q-2}{lp}\right\rfloor + p = p \left\lfloor\frac{p^n-2}{lp}\right\rfloor + p < p\frac{p^n-2}{lp} + p \leq \frac{p^n-2}{p+1} + p \leq p^{n-1} = \frac{p^n}{p} = \frac{q}{p}.
\]

This prove the result for \( l > p \). Now, we assume \( l < p \) and observe that \( \gamma^{i+1} = i(1-\gamma) + 1 \) is the same as \( \gamma^i + \ldots + \gamma + 1 = -i \). We define \( f(i) = \sum_{j=0}^{i} \gamma^j \) and \( g(i) = -i \), then by Lemma 2.2, we get
\[
|\{i \in [1, lp] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq l\} \cap \{g(i) : 0 \leq i \leq p\}|
= |\{f(i) : 0 \leq i \leq l\} \cap \{-i : 0 \leq i \leq p\}|
= |\{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p|.
\]

Assuming that \( k \in \mathbb{N} \), where \( 0 \leq k \leq l-1 \), such that \( f(k), f(k+1) \in \{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p \), we have
\[
f(k) = \gamma^k + \ldots + \gamma + 1 = c_k \in \mathbb{F}_p, \quad (8)
\]
\[
f(k + 1) = \gamma^{k+1} + \ldots + \gamma + 1 = c_{k+1} \in \mathbb{F}_p. \quad (9)
\]

Since \( c_k \neq 0 \) and \( k < l = \text{ord}_{\mathbb{F}_q}(\gamma) \), the Equations (8) and (9) imply
\[
\gamma = \frac{c_{k+1} - 1}{c_k} \in \mathbb{F}_p,
\]
which is a contradiction. Therefore, if \( f(k) \in \{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p \), then \( f(k+1) \notin \{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p \). So we have a bound for the number of elements in \( \{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p \), given by
\[
|\{i \in [1, lp] : f(i) = g(i)\}| = |\{f(i) : 0 \leq i \leq l\} \cap \mathbb{F}_p| \leq \left\lfloor\frac{l}{2}\right\rfloor.
\]

Hence the number of roots of \( f(i) - g(i) \) in \([1, lp\lfloor\frac{q-2}{lp}\rfloor]\) is at most \( \left\lfloor\frac{l}{2}\right\rfloor\lfloor\frac{q-2}{lp}\rfloor \) and the number of roots in \([lp\lfloor\frac{q-2}{lp}\rfloor, q-2]\) is at most \( \left\lfloor\frac{l}{2}\right\rfloor \), since \( q - 2 - lp\lfloor\frac{q-2}{lp}\rfloor < lp \). Hence
\[
|\{1 \leq i \leq q - 2 : \gamma^{i+1} = i(1-\gamma) + 1\}| \leq \left\lfloor\frac{l}{2}\right\rfloor\left\lfloor\frac{q-2}{lp}\right\rfloor + \left\lfloor\frac{l}{2}\right\rfloor < \frac{q}{2p} + \frac{p}{2} \leq \frac{q}{p},
\]
this proof the result. \( \square \)
3. The main Theorem

Note that in case \( Crk(f) = 2 \), Theorem 1.3 states that
\[
\omega(f) > \frac{q}{3} - 2.
\]

The following theorem improve the bound in this case.

**Theorem 3.1.** Let \( \mathbb{F}_q \) be with odd characteristic \( p \) and let \( f(x) \) be a permutation polynomial of \( \mathbb{F}_q \) with \( Crk(f) = 2 \). Then
\[
\omega(f) \geq q - \frac{q}{p} - \sqrt{\frac{3p}{2}} - \frac{39}{16} - \frac{1}{4}.
\]

**Proof:** By Lemma 2.1, there exist \( a_0, a_1, a_2, a_3 \in \mathbb{F}_q \), where \( a_0, a_2 \neq 0 \), such that
\[
f(x) = a_2^{-1} \sum_{i=1}^{q-2} x^i(-a_0)^i[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i}] + a_3 + a_2^{-1} \left[ \frac{a_1}{a_1 + a_2^{-1}} + 1 - a_1^{q-1} \right].
\]

In order to calculate the smaller number of non null coefficients of \( f \), we consider
\[a_3 := -\frac{a_2^{-1}a_1}{a_1 + a_2^{-1}} - a_2^{-1}a_1^{q-1} \text{ and } a_0 = -1.\]

Thus,
\[
f(x) = a_2^{-1} \sum_{i=1}^{q-2} x^i[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i}]. \tag{10}
\]

Before to resolve the general case, we consider some special cases. Firstly, we assume \( a_1 = 0 \) and then
\[
f(x) = a_2^{-1} \sum_{i=1}^{q-2} x^i[-i(a_2^{-1})^{q-1-i}] = -a_2^{-1} \sum_{i=1}^{q-2} ix^i a_2^i.
\]

Note that \( ia_2^i = 0 \) only when \( i \equiv 0 \) (mod \( p \)). Thus, in this case we have
\[
\omega(f) = q - 2 - \left( \frac{q}{p} - 1 \right) = q - \frac{q}{p} - 1,
\]

Now, we assume that \( a_1 + a_2^{-1} = 0 \) and in this case
\[
f(x) = -a_2^{-1} \sum_{i=1}^{q-2} x^i a_1^{q-1-i}.
\]

Since \( a_2 \neq 0 \), we have \( a_1 \neq 0 \) and thus \( \omega(f) = q - 2 \). Now we consider the general case, where \( a_1 \neq 0 \) and \( a_1 + a_2^{-1} \neq 0 \). Hence
\[
f(x) = a_2^{-1} \sum_{i=1}^{q-2} x^i[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{q-2-i} - a_1^{q-1-i}]
\]
\[= a_2^{-1} \sum_{i=1}^{q-2} x^i[(a_1 - ia_2^{-1})(a_1 + a_2^{-1})^{(i+1)} - a_1^{i}]
\]
\[= a_2^{-1} \sum_{i=1}^{q-2} x^ia_1(a_1 + a_2^{-1})^{-(i+1)} \left[ 1 - i \left( \frac{a_1 + a_2^{-1}}{a_1} - 1 \right) - \left( \frac{a_1 + a_2^{-1}}{a_1} \right)^{i+1} \right].
\]
Let \( \gamma := \frac{a_1 + a_2^{-1}}{a_1} \) and by hypothesis \( \gamma \not\in \{0, 1\} \). In the same way that particular cases, we estimate the number of indices \( i \) for which
\[
\gamma^{i+1} = i(1 - \gamma) + 1. \tag{11}
\]
In the case \( \gamma \in \mathbb{F}_q \setminus \mathbb{F}_p \), the result follows by Lemma 2.5. Now, we assume \( \gamma \in \mathbb{F}_p \), thus \( l := \text{ord}_{\mathbb{F}_q}(\gamma) \mid (p-1) \). By Corollary 2.3, the number of elements \( i \) in \([p-1, q-2]\) for which \( \gamma^{i+1} = i(1 - \gamma) + 1 \) is exactly \( p - 1 \). Finally, by Lemma 2.4, the number of such \( i \) in the interval \([1, p-2]\) is at most
\[
\sqrt{\frac{3p}{2} - \frac{39}{16}} + \frac{5}{4}.
\]
Hence, we get
\[
\omega(f) \geq q - 2 - \left( \frac{q}{p} - 1 \right) - \left( \sqrt{\frac{3p}{2} - \frac{39}{16}} + \frac{5}{4} \right) = q - \frac{q}{p} - \sqrt{\frac{3p}{2} - \frac{39}{16}} - \frac{1}{4}.
\]
As we wanted to prove. \( \square \)

**Corollary 3.2.** Let \( \mathbb{F}_{p^n} \) be a finite field with odd characteristic \( p \) and let \( f(x) \) be a permutation polynomial of \( \mathbb{F}_{p^n} \) with \( \text{Crk}(f) = 2 \). Then for all \( p \) there exists an integer \( \nu_p \in \mathbb{N} \), with \( 0 \leq \nu_p \leq \sqrt{\frac{3p}{2} - \frac{39}{16}} + \frac{5}{4} \), such that
\[
\omega(f) \geq p^n - p^{n-1} - 1 - \nu_p,
\]
where this inequality is sharp, i.e. for all \( n \in \mathbb{N} \) there exists a polynomial \( f(x) \in \mathbb{F}_{p^n} \) such that \( \text{Crk}(f) = 2 \) and \( \omega(f) = p^n - p^{n-1} - 1 - \nu_p \).

From here, an open question is what is the value of
\[
\nu_p = \max_{\gamma \in \mathbb{F}_p} |\{1 \leq i \leq p-2 : \gamma^{i+1} = i(1 - \gamma) + 1\}| - 1? \tag{12}
\]

**Example 3.3.** It is easy to verify that \( \nu_{11} = 3 \), where the maximum value in (12) is attained by \( \gamma = 7 \). For each positive integer \( n \) we let
\[
f(x) = \sum_{i=1}^{11^n-2} [4^{i+1}(2 - i) - 6^i] x^i
\]
be a permutation polynomial with Carlitz rank 2 in \( \mathbb{F}_{11^n} \). The coefficients of \( f \) has been choosing using Equation (10) and the fact that \( \gamma = \frac{a_1 + a_2^{-1}}{a_1} \). The polynomial \( f(x) \) also can be seen as
\[
f(x) \equiv (\text{mod } 11^n - x).
\]
By the proof of Theorem 3.1 we know the \( \omega(f) = 11^n - 11^{n-1} - 4 \). In addition, any permutation polynomial \( g(x) \) with Carlitz rank 2 over \( \mathbb{F}_{11^n} \) satisfies \( \omega(g) \geq 11^n - 11^{n-1} - 4 \).

**References**

[1] C. Hermite, *Sur Les Fonctions de Sept Lettres*, C. R. Acad. Sci. Paris 57 (1863), pp. 750-757.
[2] E. Aksoy, A. Çeşmelioğlu, W. Meidl, and A. Topuzoğlu, *On the Carlitz Rank of Permutation Polynomials*, Finite Fields and Their Applications, 15 (2009), pp. 428-440.
[3] W. Chu and S. W. Golomb, *Circular Tuscan-k Arrays From Permutation Binomials*, J. Comb. Theory A 97 (2002), 195-202.
[4] J. Sun, O. Y. Takeshita and M. P. Fitz, *Permutation Polynomial Based Deterministic Interleavers for Turbo Codes*, Proceedings 2003 IEEE International Symposium on Information Theory (Yokohama, Japan, 2003), 319.
[5] J. F. Dillon and H. Dobbertin, *New Cyclic Difference Sets with Singer Parameters*, Finite Fields Appl. 10 (2004), pp. 342-389.
[6] C. J. Colbourn, T. Klove and A. C. H. Ling, *Permutation Arrays for Powerline Communication and Mutually Orthogonal Latin Squares*, IEEE Trans. Inf. Theory 50 (2004), pp. 1289-1291.

[7] L. Carlitz, *Permutations in a Finite Field*, Proc. Amer. Math. Soc, vol. 4, 1953, p. 194.

[8] L. E. Dickson, *The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group*, The Annals of Mathematics, 11 (1896), pp. 65-120.

[9] D. Gómez-Pérez, A. Ostafe, and A. Topuzo˘ glu, *On the Carlitz Rank of Permutations of \( \mathbb{F}_q \) and Pseudorandom Sequences*, Journal of Complexity, 30 (2014), pp. 279-289.

[10] A. Masuda and M. Zieve, *Permutation Binomials over Finite Fields*, Transactions of the American Mathematical Society, 361 (2009), pp. 4169-4180.

[11] Xing-D. Hou, S. D. Lappano, *Determination of a Type of Permutation Binomials over Finite Fields*, Journal of Number Theory, vol. 147 (2015), pp. 14-23.

[12] Xing-D. Hou, *Determination of a type of permutation trinomials over finite fields, II*, Finite Fields and Their Applications, vol. 35 (2015), pp. 16-35.

[13] K. Li, L. Qu, X. Chen, *New classes of permutation binomials and permutation trinomials over finite fields*, Finite Fields and Their Applications, vol. 43 (2017), pp. 69-85.

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 31270-901, Brazil,

E-mail address: jose-alvesoliveira@hotmail.com
E-mail address: fbrocher@mat.ufmg.br