SOME NOTES ON THE MULTIPLICATIVE ORDER OF $\alpha + \alpha^{-1}$
IN FINITE FIELDS OF CHARACTERISTIC TWO

S. UGOLINI

Abstract. In this paper we prove some results on the possible multiplicative orders of $\alpha + \alpha^{-1}$ when $\alpha$ is a non-zero element of a finite field of characteristic 2. The results of the paper rely on a previous investigation on the structure of the graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic 2.

1. Introduction

Elements of the form $\alpha + \alpha^{-1}$, where $\alpha$ belongs to the multiplicative group $F_q^*$ of a finite field $F_q$ with $q$ elements, play a crucial role in many contexts.

For example, the following nice property holds for the Dickson polynomial $D_n(x)$ of the first kind with parameter 1 and degree $n$ (see [6] or the monograph [5]):

$$D_n(x + x^{-1}) = x^n + x^{-n}.$$ 

Meyn [7] and Varshamov and Garakov [8] employed the $Q$-transform, which takes a polynomial $f(x)$ to $f^Q(x) = x^{|\text{deg}(f)} \cdot f(x + x^{-1})$, for the recursive synthesis of irreducible polynomials.

Shparlinski [9] answered a question posed in [1, Research Problem 3.1] about the possibility of finding the multiplicative order $|\gamma + \gamma^{-1}|$ of $\gamma + \gamma^{-1}$ from the knowledge of the multiplicative order $|\gamma|$ of $\gamma \in F_q^*$. He showed that the orders of $\gamma$ and $\gamma + \gamma^{-1}$ are independent in a certain sense, even though in finite fields of small characteristic it is not possible that $|\gamma|$ and $|\gamma + \gamma^{-1}|$ are both small (see [11, Section 4]).

In this paper we consider finite fields of characteristic 2. If $F_q$ is a finite field of characteristic 2, then we define the map $\vartheta$ over the projective line $\mathbb{P}^1(F_q) := F_q \cup \{\infty\}$ as follows:

$$\vartheta(x) = \begin{cases} 
\infty & \text{if } x \in \{0, \infty\}; \\
x + x^{-1} & \text{otherwise}.
\end{cases}$$

Such a map is strictly related to the duplication map over a Koblitz curve (see [10]). In Section 3 we review some properties of the graph $G_q$ associated with the map $\vartheta$ over $\mathbb{P}^1(F_q)$. The reader can refer to [10] for the proofs of the results. Very briefly, we recall that the vertices of $G_q$ are the elements of $\mathbb{P}^1(F_q)$. Moreover, for any $\alpha \in \mathbb{P}^1(F_q)$ there is an arrow which joins $\alpha$ to $\vartheta(\alpha)$. We say that $\alpha \in \mathbb{P}^1(F_q)$ is $\vartheta$-periodic if $\vartheta^m(\alpha) = \alpha$ for some positive integer $m$ (here $\vartheta^m$ denotes the $m$-fold composition of $\vartheta$ with itself). If $\alpha$ is not $\alpha$-periodic, then it is pre-periodic, namely some iterate of $\alpha$ is $\vartheta$-periodic. The resulting graph is formed by a finite number of

2010 Mathematics Subject Classification. 11T30, 11G20, 37P55.

Key words and phrases. Dickson polynomials, elliptic curves, finite fields, multiplicative order.
connected components. Each component is formed by a cycle, whose vertices are roots of binary trees.

Relying upon some preliminary results presented in Section 3, in Section 4 we prove some restrictions on the multiplicative order of the iterates \( \vartheta^i(\gamma) \) of an element \( \gamma \) in the multiplicative group of a finite field of characteristic 2. The main result of the section is Theorem 4.3. In Section 4.1 we describe three possible scenarios for the order and the absolute trace of the iterates \( \vartheta^i(\gamma) \) of an element \( \gamma \in \mathbb{F}_{q^4} \setminus \{0, 1\} \) whose multiplicative order divides \( q^2 + 1 \). Finally, in Section 4.2 we show how the results of the current paper and [10] can be related to some results on the roots of certain Dickson polynomials presented in [2].

2. Notation

For the reader’s convenience we list here some notations we use along the way.

- If \( G \) is a (multiplicative) group and \( g \) is an element of \( G \), then \( |g| \) is the order of \( g \) in \( G \), namely \( |g| \) is the smallest positive integer \( n \) such that \( g^n = 1 \).
- We denote by \( \mathbb{N} \) the set of natural numbers (0 included). Moreover we define \( \mathbb{N}^* := \mathbb{N} \setminus \{0\} \) and \( \mathbb{N}^{**} := \mathbb{N} \setminus \{0, 1\} \).
- If \( L \) is a finite field, then we denote by \( L^* := L \setminus \{0\} \) its multiplicative group and we define \( L^{**} := L \setminus \{0, 1\} \).
- If \( L_1 \) and \( L_2 \) are two finite fields with \( L_1 \subseteq L_2 \), then we denote by \( [L_2 : L_1] \) the degree of the extension \( L_2 \) over \( L_1 \).
- If \( \alpha \) is an element of a finite field \( L \) of characteristic 2, then we denote by \( \deg(\alpha) \) the degree of the field extension \( \mathbb{F}_2(\alpha) \) over \( \mathbb{F}_2 \). Equivalently, \( \deg(\alpha) \) is the degree of the minimal polynomial of \( \alpha \) over \( \mathbb{F}_2 \).
- If \( \alpha \in \mathbb{F}_{2^t} \) for some positive integer \( t \), then
  \[
  \text{Tr}_t(\alpha) := \sum_{i=0}^{t-1} \alpha^{2^i}
  \]
  is the absolute trace of \( \alpha \). We recall that \( \text{Tr}_t(\alpha) \in \mathbb{F}_2 \).
- If \( f \) is a function from a set \( A \) to a set \( B \), then \( f(A) := \{f(a) : a \in A\} \) is the image set of \( A \) in \( B \).

3. Preliminaries

Throughout this section \( t \) denotes a positive integer, which can be written as

\[
 t = 2^r \cdot s
\]

for some non-negative integer \( r \) and some odd integer \( s \).

We define \( q := 2^t \).

We denote by \( A_t \) and \( B_t \) the following subsets of \( \mathbb{P}^1(\mathbb{F}_q) \):

\[
 A_t := \{ \alpha \in \mathbb{F}_q^* : \text{Tr}_t(\alpha) = \text{Tr}_t(\alpha^{-1}) \} \cup \{0, \infty\};
\]

\[
 B_t := \{ \alpha \in \mathbb{F}_q^* : \text{Tr}_t(\alpha) \neq \text{Tr}_t(\alpha^{-1}) \}.
\]

The set \( A_t \) is strictly related to the ring \( E(\mathbb{F}_q) \) of rational points in \( \mathbb{F}_q \) of the elliptic curve \( E \) defined over \( \mathbb{F}_2 \) by the equation

\[
 y^2 + xy = x^3 + 1.
\]

In fact, the following holds (see [10 Lemma 2.5]).
Lemma 3.1. Let \( x \in \mathbb{F}_q \). Then there exists \( y \in \mathbb{F}_q \) such that \( (x, y) \in E(\mathbb{F}_q) \) if and only if \( x = 0 \) or \( x \neq 0 \) and \( \text{Tr}(x) = \text{Tr}(x^{-1}) \).

Remark 3.2. We notice that in [10] the curve \( E \) was denoted by \( \text{Kob}_0 \) since \( E \) is a Koblitz curve. In the present paper we opted for the shorter notation \( E \).

In [10] we described the structure of the directed graph \( G_q \) associated with the map \( \vartheta \) over \( \mathbb{P}^1(\mathbb{F}_q) \). The following theorem summarizes the results contained in [10, Remark 2.3, Lemma 4.3, Lemma 4.4].

Theorem 3.3. Let \( d := r + 2 \). Then the following hold.

1. The image set \( \vartheta(A_t) \) is contained in \( A_t \), while \( \vartheta(B_t) \) is contained in \( B_t \). In particular, either all the vertices of a connected component are contained in \( A_t \), or all of them are contained in \( B_t \).
2. If \( x \in A_t \) is \( \vartheta \)-periodic, then \( x \) is the root of a binary tree of depth \( d \).
3. If \( x \in B_t \) is \( \vartheta \)-periodic, then \( x \) is the root of a binary tree of depth 1.
4. If \( x \in A_t \setminus \{\infty\} \) is \( \vartheta \)-periodic, then for any positive integer \( k \leq d \) there are \( \lceil 2^{k-1} \rceil \) vertices at the level \( k \) of the tree. Moreover, the root has one child, while all other vertices have two children.
5. \( \infty \) is \( \vartheta \)-periodic and for any positive \( k \leq d \) there are \( \lceil 2^{k-2} \rceil \) vertices at the level \( k \) of the tree. Moreover, \( \infty \) and the vertex at the level 1 have one child, while all other vertices have two children.

Example 3.4. In this example we construct the graph \( G_{2^6} \). The labels are the exponents of the powers \( \alpha^i \), where \( \alpha \) is a root of the Conway polynomial \( x^6 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x] \), with \( 0 \leq i \leq 62 \). Moreover there is one vertex labelled by \( \infty \) and another by \( '0' \), namely the zero of \( \mathbb{F}_{2^6} \).

We notice in passing that the trees of any connected component have the same depth, which is either 1 or 3.
We recall some well-known facts we need in the rest of the paper.

**Lemma 3.5.** The following hold:
- \( \gcd(2^t - 1, 2^t + 1) = 1 \);
- \( \gcd(2^t + 1, 2^{2t} + 1) = 1 \).

**Proof.** If \( d = \gcd(2^t - 1, 2^t + 1) \), then \( d \mid ((2^t + 1) - (2^t - 1)) = 2 \). Since \( d \) cannot be equal to 2, we conclude that \( d = 1 \).

If \( e = \gcd(2^t + 1, 2^{2t} + 1) \), then \( e \mid ((2^{2t} + 1) - (2^t + 1)) = 2^t(2^t - 1) \). Since \( e \) cannot be even, we have that \( e \mid (2^t - 1) \). Hence \( e \mid \gcd(2^t - 1, 2^t + 1) = 1 \). Therefore \( e = 1 \). □

**Lemma 3.6.** Let \( g_1 \) and \( g_2 \) be two elements of a finite commutative group \( G \). If \( \gcd(|g_1|, |g_2|) = 1 \), then \( |g_1g_2| = |g_1| \cdot |g_2| \).

**Lemma 3.7.** The group \( \mathbb{F}_q^* \) is cyclic of order \( 2^t - 1 \). In particular, if \( \alpha \in \mathbb{F}_q^* \) then \( |\alpha| \mid (2^t + 1) \).

**Proof.** For the first part of the claim see for example [6, Theorem 2.8]. For the second part of the claim, we notice that \( |\alpha| > 1 \). Since \( |\alpha| \mid (2^t - 1) \), according to Lemma 3.5 we have that \( |\alpha| \mid (2^t + 1) \).

We recall that \( q + 1 = (2^s)^{2^r} + 1 \) is a generalized Fermat number. The following holds for its divisors.

**Lemma 3.8.** Let \( d \) be a positive divisor of \( q + 1 \). Then \( d \equiv 1 \mod 2^{r+1} \).

**Proof.** Let \( p \) be a prime which divides \( (2^s)^{2^r} + 1 \). According to [3], \( p = k \cdot 2^{r+1} + 1 \) for some \( k \in \mathbb{N}^* \), namely

\[
(3.1) \quad p \equiv 1 \mod 2^{r+1}.
\]

Since \( q + 1 \) can be written as a product of primes satisfying (3.1), we get the result. □

**Lemma 3.9.** If \( \alpha \) has degree \( t \) over \( \mathbb{F}_2 \) and \( \beta := \alpha + \alpha^{-1} \), then either \( \deg(\beta) = t \) or \( \deg(\beta) = \frac{t}{2} \) (provided that \( t \) is even).

**Proof.** Let \( L := \mathbb{F}_2(\beta) \). Then \( \alpha \) is a root of the polynomial \( p(x) := x^2 + \beta x + 1 \in \mathbb{F}_2[x] \). The result follows because

\[
\deg(\beta) = [L : \mathbb{F}_2] = \frac{t}{[\mathbb{F}_2(\alpha) : L]}
\]

with \( 1 \leq [\mathbb{F}_2(\alpha) : L] \leq 2 \). □

The following lemma (see [4, Lemma 4.1]) and Lemma 3.13 will be used repeatedly in the paper.
Lemma 3.10. Let $\alpha$ be an element of order $2^t - 1$ in $F_{2^t}^*$ and $\beta$ an element of order $2^t + 1$ in $F_{2^t}^*$. Let $\Omega$ and $\overline{\Omega}$ be two subsets of $F_{2^t}$ defined as

\[ \Omega = \{ x \in F_{2^t}^* : \text{Tr}_t(x^{-1}) = 0 \}; \]
\[ \overline{\Omega} = \{ x \in F_{2^t}^* : \text{Tr}_t(x^{-1}) = 1 \}. \]

Then

\[ \Omega = \{ x \in F_{2^t}^* : x = \vartheta(\alpha^i) \text{ with } i \in \mathbb{N}, 1 \leq i \leq 2^{t-1} - 1 \}; \]
\[ \overline{\Omega} = \{ x \in F_{2^t}^* : x = \vartheta(\beta^i) \text{ with } i \in \mathbb{N}, 1 \leq i \leq 2^{t-1} \}. \]

Remark 3.11. Let

\[ I := \{ i \in \mathbb{N} : 1 \leq i \leq 2^{t-1} \}; \]
\[ J := \{ j \in \mathbb{N} : 2^{t-1} + 1 \leq j \leq 2^t \}. \]

If $\beta$ is defined as in Lemma 3.10 then $\beta^k + \beta^{-k} \in F_{2^t}^*$ for any $k \in I \cup J$. Indeed, the assertion is true if $k \in I$, according to Lemma 3.13.

Let $k \in J$. We notice that $\beta^{-k} = \beta^{2^t+1-k}$.

Let $i := 2^t + 1 - k$. Then

\[ 1 \leq i \leq 2^{t-1}. \]

Hence $\beta^k + \beta^{-k} = \beta^i + \beta^{-i} \in \overline{\Omega} \subseteq F_{2^t}^*$.

Remark 3.12. We notice that $\beta^{2t+1} = 1$. Hence $\beta^{2t+1} + \beta^{-(2t+1)} = 0 \notin F_{2^t}^*$.

From Lemma 3.10 and the subsequent remarks we deduce the following results, where $\overline{\Omega}$ is defined as in Lemma 3.10.

Lemma 3.13. We have that $\overline{\Omega} = \{ \vartheta(\gamma) : \gamma \in F_{2^t}^*, |\gamma| \mid (2^t + 1) \}$.

Corollary 3.14. Let $x \in F_q^*$ be a leaf of a connected component of $G_q$.

- If $x \in A_t$, then $\text{Tr}_t(x) = \text{Tr}_t(x^{-1}) = 1$.
- If $x \in B_t$, then $\text{Tr}_t(x) = 0$ and $\text{Tr}_t(x^{-1}) = 1$.

Proof. We notice that $x \in \Omega \cup \overline{\Omega}$. Since $x$ is a leaf, there is no $\tilde{x} \in F_q^*$ such that $x = \vartheta(\tilde{x})$. Therefore $x \in \overline{\Omega}$. \qed

The following property holds for the leaves belonging to $A_t$.

Lemma 3.15. Let $\alpha \in F_q^* \cap A_t$ be a leaf of $G_q$ with $\text{Tr}_t(\alpha) = \text{Tr}_t(\alpha^{-1}) = 1$. If $\vartheta(\gamma) = \alpha$ for some $\gamma \in F_q^*$, then $\text{Tr}_{2t}(\gamma) = \text{Tr}_{2t}(\gamma^{-1}) = 1$.

Proof. First we notice that $q^2 = 2^{2t} = 2^{2t+1}s$. Therefore $\gamma$ belongs to the level $r+3$ of a tree of $G_{q^2}$. According to Theorem 3.3 the trees in $G_{q^2}$ have depth either 1 or $r+3$ and the former holds only for trees whose vertices belong to $B_{2t}$. Since $r+3 > 1$ we conclude that $\gamma$ is a leaf which belongs to $A_{2t}$. \qed
4. DISTRIBUTION OF THE ORDERS IN $G_q$, $G_{q^2}$, $G_{q^4}$ AND SOME IMPLICATIONS

Let $n := 2^l \cdot m$ for some non-negative integer $l$ and some odd integer $m$.

Let $q := 2^n$.

First we prove some results on the degrees of $\alpha$ and its iterates $\vartheta^i(\alpha)$ for an element $\alpha$ belonging to a finite field of characteristic 2.

**Lemma 4.1.** Let $\alpha$ be a leaf of $G_{2^t}$, where $t = 2^r \cdot s$ for some non-negative integer $r$ and some odd integer $s$.

Then $\alpha \notin \{0, \infty\}$ and $\deg(\alpha) = 2^r \cdot v$ for some odd integer $v$ such that $v \mid s$.

**Proof.** First we notice that $\vartheta(0) = \infty$ and $\vartheta(1) = 0$. Hence $\alpha \in \mathbb{F}_{2^t}$.

Let $\deg(\alpha) = 2^u \cdot v$ for some non-negative integer $u$ and some odd integer $v$. Since $\deg(\alpha) \mid t$, we have that $u \leq r$ and $v \mid s$. Indeed, $u = r$. In fact, if $u < r$ and $\gamma$ is an element in the algebraic closure $\overline{\mathbb{F}_2}$ of $\mathbb{F}_2$ such that $\vartheta(\gamma) = \alpha$, then $\gamma \in G_{2^t}$, in contradiction with the fact that $\alpha$ is a leaf of $G_{2^t}$.

**Lemma 4.2.** Let $t := 2^r \cdot s$ and $l := 2^r = 2^r - 1 \cdot s$ for some positive integer $r$ and some odd integer $s$. Let $\alpha \in A_i \cap \mathbb{F}_{2^t}$ and $d := \deg(\alpha)$.

If $\alpha$ is a leaf of $G_{2^t}$ and $\deg(\vartheta(\alpha)) = d$, then one of the following holds:

1. $\deg(\vartheta^i(\alpha)) = d$ for all $i \in \mathbb{N}$.
2. $\vartheta^i(\alpha) \in B_i \cap \mathbb{F}_{2^t}$ for any $i \geq r + 1$, while $\deg(\vartheta^i(\alpha)) = d$ for $1 \leq i \leq r$.

**Proof.** According to Lemma 4.1 we have that $d = 2^s \cdot v$ for some odd integer $v \mid s$.

Now we suppose that $\deg(\vartheta^i(\alpha)) \neq d$ for some $i \in \mathbb{N}$. We define

$$j := \min\{i \in \mathbb{N} : \deg(\vartheta^i(\alpha)) \neq d\}.$$

We notice that $\deg(\vartheta^j(\alpha)) = \frac{d}{2} = 2^{r-1} \cdot v$. Hence

$$\vartheta^j(\alpha) \in \mathbb{F}_{2^t} \text{ and } \vartheta^{j-1}(\alpha) \notin \mathbb{F}_{2^t}.$$

Therefore $\vartheta^j(\alpha)$ is a leaf of the graph $G_{2^t}$, whose connected components have depth either 1 or $r + 1 \geq 2$. Hence either $j = r + 1$ or $j = 1$. This latter is not possible because $\deg(\vartheta(\alpha)) = d$ by hypothesis. Therefore $j = r + 1$.

In the following theorem we investigate the possible orders of the iterates of an element in $\mathbb{F}_{q^4}^*$ whose multiplicative order divides $q^2 + 1$.

**Theorem 4.3.** Let $C_{q^2+1}$ be the cyclic subgroup of $\mathbb{F}_{q^4}^*$ of order $q^2 + 1$ and $H := C_{q^2+1} \setminus \{1\}$. Then $H = H_1 \cup H_2 \cup H_3$, where $H_1$, $H_2$ and $H_3$ are three subsets of $H$, whose pairwise intersections are empty, characterized as follows.

1. $\gamma \in H$ belongs to $H_1$ if and only if $\mid \vartheta(\gamma) \mid$ divides $q + 1$ and $\mid \vartheta^i(\gamma) \mid$ divides $q - 1$ for all the integers $i \geq 2$.
2. $\gamma \in H$ belongs to $H_2$ if and only if
   - for any $i \in \mathbb{N}$ with $1 \leq i \leq l + 1$ there are two positive integers $d_i$ and $e_i$ greater than 1 with $d_i \mid (q + 1)$ and $e_i \mid (q - 1)$ such that $\mid \vartheta^i(\gamma) \mid = d_i e_i$;
   - $\mid \vartheta^{i+2}(\gamma) \mid$ divides $q + 1$;
   - $\mid \vartheta^i(\gamma) \mid$ divides $q - 1$ for all $i \geq l + 3$.
3. $\gamma \in H$ belongs to $H_3$ if and only if for any positive integer $i$ there are two positive integers $d_i$ and $e_i$ greater than 1 with $d_i \mid (q + 1)$ and $e_i \mid (q - 1)$ such that $\mid \vartheta^i(\gamma) \mid = d_i e_i$. 


Proof. First we notice that $q^2 = 2^{2n}$.

We prove that the pairwise intersections of the sets $H_1, H_2$ and $H_3$ are empty. If $\gamma \in H_1$, then $|\vartheta(\gamma)|$ divides $q + 1$. By definition, if $\gamma \in H_2 \cup H_3$, then $|\vartheta(\gamma)|$ does not divide $q + 1$. Therefore $H_1 \cap H_2 = \emptyset$ and $H_1 \cap H_3 = \emptyset$. Finally, if $\gamma \in H_2$, then $|\vartheta^{l+3}(\gamma)|$ is a divisor of $q - 1$. Therefore $\gamma \notin H_3$.

Now we prove that, if $\gamma \in H$, then $h \in H_1 \cup H_2 \cup H_3$. We deal separately with some cases.

- **Case 1:** $|\vartheta(\gamma)|$ divides $q + 1$.

  Then $\vartheta^2(\gamma) \in \mathbb{F}_q^*$ according to Lemma 3.13 and any iterate $\vartheta^i(\gamma)$ belongs to $\mathbb{F}_q^*$ for $i \geq 2$. Hence $\gamma \in H_1$.

- **Case 2:** $|\vartheta(\gamma)|$ does not divide $q + 1$.

  Let $t := 2n$. According to Lemma 3.10 we have that $\vartheta(\gamma) \in \mathbb{F}_q^*$. Nevertheless, $\vartheta(\gamma) \notin \mathbb{F}_q^*$. In fact, according to Lemma 3.13 any element in $\mathbb{F}_q^*$ can be expressed as

  $$\vartheta(\alpha^i) \text{ or } \vartheta(\beta^i)$$

  for some positive integer $i$, where $|\alpha| = 2^n - 1$ and $|\beta| = 2^n + 1$. Since $|\gamma| \mid (2^n + 1)$ with $|\gamma| > 1$ and $\gcd(2^n + 1, 2^{2n} - 1) = 1$, we conclude that $\gamma \notin \mathbb{F}_q^*$. Hence

  $$\gamma \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}.$$

  Moreover $\vartheta(\gamma)$ is a leaf of $G_{q^2}$ because $\gamma \notin \mathbb{F}_q^*$ and either $\vartheta(\gamma) \in A_{2n}$ or $\vartheta(\gamma) \in B_{2n}$.

  - **Sub-case 1:** $\vartheta(\gamma) \in A_{2n}$.

    Let $\alpha := \vartheta(\gamma)$. According to Lemma 4.1 we have that $d := \deg(\alpha) = 2^{l+1} \cdot v$ for some odd integer $v \mid s$.

    Let $r := l + 1$, $s := m$, $t := 2^n \cdot s$ and $\deg(\alpha) = d$. According to Lemma 3.9 we have that $\deg(\vartheta(\alpha)) \in \{1, 2\}$. If $\deg(\vartheta(\alpha)) = 2$, then $\vartheta(\alpha) \in \mathbb{F}_q^*$ and $|\vartheta(\alpha)| \mid (q - 1)$. This latter is not possible because $|\alpha| \mid (q + 1)$. Hence $\deg(\vartheta(\alpha)) = d$.

    Therefore the hypotheses of Lemma 4.2 are satisfied.

    If $\deg(\vartheta^i(\alpha)) = d$ for all $i \in \mathbb{N}$, then there is no $i \in \mathbb{N}$ such that $|\vartheta^i(\alpha)| \mid (q - 1)$. In fact, if $|\vartheta^i(\alpha)| \mid (q - 1)$ for some $i \in \mathbb{N}$, then $\vartheta^i(\alpha) \in \mathbb{F}_q^*$ and $\deg(\vartheta^i(\alpha)) < d$.

    Moreover, if $|\vartheta^i(\alpha)| \mid (q + 1)$ for some $i \in \mathbb{N}$, then $|\vartheta^{i+1}(\alpha)| \mid (q - 1)$ according to Lemma 3.13 namely $\vartheta^{i+1}(\alpha) \in \mathbb{F}_q^*$. Since this latter is not possible, we conclude that $|\vartheta^i(\gamma)| = d_i e_i$ for some positive integers $d_i$ and $e_i$ greater than 1 with $d_i \mid (q + 1)$ and $e_i \mid (q - 1)$. Therefore $\gamma \in H_3$.

    If $\deg(\vartheta^i(\alpha)) = d$ for some $i \in \mathbb{N}$, then $\vartheta^i(\alpha) \in B_{2n/2} \cap \mathbb{F}_q^*$ for any $i \geq r + 1 = l + 2$, namely $\vartheta^i(\gamma) \in B_{2n/2} \cap \mathbb{F}_q^*$ for any $i \geq l + 3$. Moreover $\deg(\vartheta^i(\gamma)) = d$ for any $i$ with $1 \leq i \leq l + 2$. Since $\vartheta^{l+3}(\gamma) \in \mathbb{F}_q^*$, according to Lemma 3.13 we have that $|\vartheta^{l+2}(\gamma)|$ divides $q + 1$. Finally, we can prove as above that $|\vartheta^i(\gamma)|$ is neither a divisor of $q + 1$ nor a divisor of $q - 1$ for all $i$ with $1 \leq i \leq l + 1$. Hence $\gamma \in H_2$.

  - **Sub-case 2:** $\vartheta(\gamma) \in B_{2n}$. Then $\vartheta(\gamma)$ is a leaf of a tree of depth 1 in $G_{q^2}$ and both the elements $\vartheta(\gamma)$ and $(\vartheta(\gamma))^{-1}$ do not belong to $\mathbb{F}_q^*$.
Moreover \((d(\gamma))^{-1}\) is \(d\)-periodic and belongs to the same cycle of the iterates \(d^i(\gamma)\) for any positive integer \(i\). Therefore \(d^i(\gamma) \in \mathbb{F}_q^*\) for any positive integer \(i\) and \(|d^i(\gamma)|\) does not divide \(q - 1\). Moreover, if \(|d^i(\gamma)|\) divided \(q + 1\) for some positive integer \(i\), then \(d^{i+1}(\gamma)\) would belong to \(\mathbb{F}_q^*\) according to Lemma 3.13 in contradiction with the fact that no iterate of \(\gamma\) belongs to \(\mathbb{F}_q^*\). Since \(|d^i(\gamma)|\) divides \(q^2 - 1\), we conclude that for any positive integer \(i\) there are two positive integers \(d_i\) and \(e_i\) greater than 1 with \(d_i \mid (q + 1)\) and \(e_i \mid (q - 1)\) such that \(|d^i(\gamma)| = d_ie_i\).

Hence \(\gamma \in H_3\).

\[\square\]

**Corollary 4.4.** If \(H, H_1, H_2\) and \(H_3\) are defined as in Theorem 4.3 then the following hold.

1. If \(\gamma \in H_1\), then \(\text{Tr}_n(d^2(\gamma)) = \text{Tr}_n((d^2(\gamma))^{-1}) = 1\), while \(\text{Tr}_n(d^i(\gamma)) = \text{Tr}_n((d^i(\gamma))^{-1}) = 0\) for all \(i \geq 2\).

2. If \(\gamma \in H_2\), then \(\text{Tr}_n(d^{l+3}(\gamma)) = 0\) and \(\text{Tr}_n((d^{l+3}(\gamma))^{-1}) = 1\). Moreover \(\text{Tr}_n(d^i(\gamma)) = 1\) and \(\text{Tr}_n((d^i(\gamma))^{-1}) = 0\) for all \(i \geq l + 4\).

**Proof.** We prove separately the claims.

1. If \(\gamma \in H_1\) then, according to Theorem 4.3,

\[
\gamma \in \mathbb{F}_q^* \setminus \mathbb{F}_q^2, \\
d(\gamma) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^2, \\
d^2(\gamma) \in \mathbb{F}_q^*.
\]

We notice that \(d^2(\gamma)\) cannot be \(d\)-periodic. In fact, if \(d^2(\gamma)\) were \(d\)-periodic, then \(d^2(\gamma)\) would be the root of a tree of depth at least 1 in \(G_q\) and \(d(\gamma)\), which is not \(d\)-periodic, would be a child of \(d^2(\gamma)\) in \(G_q\). This latter is absurd because \(d(\gamma) \notin \mathbb{F}_q^* \setminus \mathbb{F}_q^2\).

Since \(d^2(\gamma)\) is not \(d\)-periodic, \(d(\gamma)\) is not \(d\)-periodic too. Therefore \(\gamma\) belongs to a level not smaller than 4 of a tree in \(G_{q^2}\). Consequently \(d^2(\gamma)\) is a leaf of a tree having depth at least 2 in \(G_q\). Therefore \(d^2(\gamma) \in A_n\).

2. If \(\gamma \in H_2\), then \(d(\gamma)\) is a leaf of a tree in \(G_{q^2}\). Since \(d(\gamma) \notin \mathbb{F}_q\) and \(d^{l+2}(\gamma) \notin \mathbb{F}_q\), while \(d^{l+3}(\gamma) \in \mathbb{F}_q\), we can say that neither \(d(\gamma)\) nor \(d^{l+2}(\gamma)\) are \(d\)-periodic. Therefore \(d(\gamma)\) is a leaf of a tree of depth \(l + 3\) in \(G_{q^2}\), while \(d^{l+3}(\gamma)\) is a leaf of a tree of depth 1 in \(G_q\). Therefore \(d^{l+3}(\gamma)\) and all its iterates are in \(B_n\).

\[\square\]

### 4.1. Distribution of orders and traces in \(G_q\), \(G_{q^2}\) and \(G_{q^4}\)

As a consequence of Theorem 4.3 and Corollary 4.4 we have three possible scenarios for the iterates of an element \(\gamma \in \mathbb{F}_{q^2}^*\) such that \(d := |\gamma|\) divides \((q^2 + 1)\). The data are collected in three distinct tables.

For the sake of brevity, we introduce the following notations:

- \(\gamma_i\) is the \(i\)-th iterate \(d^i(\gamma)\) of \(\gamma\);
- \(d_i := |\gamma_i|\);
- \(d_i \nmid (q \pm 1)\) stands for \(d_i \nmid (q + 1)\) and \(d_i \nmid (q - 1)\).

Moreover we conventionally define \(0^{-1} = 0\), \(\infty^{-1} = \infty\), \(|0| = 1\), \(|\infty| = 1\) and \(\text{Tr}_n(\infty) = 0\).

The levels refer to the graph \(G_{q^i}\).
4.1.1. Case 1: \( d_1 \mid (q + 1) \).

| Level | Order | Trace |
|-------|-------|-------|
| \( l + 4 \) | \( d \mid (q^2 + 1) \) | \( \text{Tr}_{4n}(\gamma) = \text{Tr}_{4n}(\gamma^{-1}) = 1 \) |
| \( l + 3 \) | \( d_1 \mid (q + 1) \), \( d_2 \mid (q + 1) \) | \( \text{Tr}_{2n}(\gamma_1) = \text{Tr}_{2n}(\gamma_1^{-1}) = 1 \) |
| \( l + 2 \) | \( d_2 \mid (q^2 - 1), d_1 \mid (q + 1) \) | \( \text{Tr}_{2n}(\gamma_2) = \text{Tr}_{2n}(\gamma_2^{-1}) = 0 \) |
| \( l + 1 \) | \( \vdots \) | \( \text{Tr}_n(\gamma_3) = \text{Tr}_n(\gamma_3^{-1}) = 0 \) |
| \( 0 \) | \( \vdots \) | \( \vdots \) |

4.1.2. Case 2: \( d_1 \nmid (q + 1), d_{i+2} \mid (q + 1) \).

| Level | Order | Trace |
|-------|-------|-------|
| \( l + 4 \) | \( d \mid (q^2 + 1) \) | \( \text{Tr}_{4n}(\gamma) = \text{Tr}_{4n}(\gamma^{-1}) = 1 \) |
| \( l + 3 \) | \( d_1 \mid (q^2 - 1), d_1 \mid (q + 1) \) | \( \text{Tr}_{2n}(\gamma_1) = \text{Tr}_{2n}(\gamma_1^{-1}) = 1 \) |
| \( l + 2 \) | \( d_2 \mid (q^2 - 1), d_2 \mid (q + 1) \) | \( \text{Tr}_{2n}(\gamma_2) = \text{Tr}_{2n}(\gamma_2^{-1}) = 0 \) |
| \( l + 1 \) | \( \vdots \) | \( \vdots \) |
| \( 2 \) | \( d_{i+2} \mid (q + 1) \) | \( \text{Tr}_{2n}(\gamma_{i+2}) = \text{Tr}_{2n}(\gamma_{i+2}^{-1}) = 0 \) |
| \( 1 \) | \( d_{i+3} \mid (q - 1) \) | \( \text{Tr}_n(\gamma_{i+3}) = 0, \text{Tr}_n(\gamma_{i+3}^{-1}) = 1 \) |
| \( 0 \) | \( d_{i+4} \mid (q - 1) \) | \( \text{Tr}_n(\gamma_{i+4}) = 1, \text{Tr}_n(\gamma_{i+4}^{-1}) = 0 \) |

4.1.3. Case 3: \( d_1 \nmid (q + 1), d_{i+2} \nmid (q + 1) \).

| Level | Order | Trace |
|-------|-------|-------|
| \( l + 4 \) | \( d \mid (q^2 + 1) \) | \( \text{Tr}_{4n}(\gamma) = \text{Tr}_{4n}(\gamma^{-1}) = 1 \) |
| \( l + 3 \) | \( d_1 \mid (q^2 - 1), d_1 \mid (q + 1) \) | \( \text{Tr}_{2n}(\gamma_1) = \text{Tr}_{2n}(\gamma_1^{-1}) = 1 \) |
| \( l + 2 \) | \( \vdots \) | \( \text{Tr}_{2n}(\gamma_2) = \text{Tr}_{2n}(\gamma_2^{-1}) = 0 \) |
| \( l + 1 \) | \( \vdots \) | \( \vdots \) |
| \( 0 \) | \( \vdots \) | \( \text{Tr}_{2n}(\gamma_{l+4}) = \text{Tr}_{2n}(\gamma_{l+4}^{-1}) = 0 \) |

In Case 1 we can have different sub-cases.

**Lemma 4.5.** In Case 1, if \( l \geq 1 \) and \( \tilde{q} := \sqrt{q} \), then one of the following holds.

- Sub-case 1: \( d_2 \nmid (\tilde{q} + 1) \). Then \( d_i \nmid (\tilde{q} \pm 1) \) for all \( i \) such that \( 2 \leq i \leq l + 1 \).
- Sub-case 2: \( d_2 \mid (\tilde{q} + 1) \). Then \( d_i \mid (\tilde{q} - 1) \) for all \( i \geq 3 \).

**Proof.** We deal separately with the two sub-cases.

- **Sub-case 1:** if \( d_2 \nmid (\tilde{q} + 1) \), then \( d_2 \nmid (\tilde{q} - 1) \) too. In fact, if \( d_2 \mid (\tilde{q} + 1) \), then \( d_1 \mid (\tilde{q} + 1) \) according to Lemma 3.13. This latter is not possible since \( \gcd(q + 1, \tilde{q} + 1) = 1 \). Hence, if we define

\[
q := \tilde{q}, \quad n := \frac{n}{2}, \quad \gamma := \gamma_1, \quad l := l - 1,
\]

we have that either Case 2 or Case 3 holds for \( \gamma \).

- **Sub-case 2:** if \( d_2 \mid (\tilde{q} + 1) \), then \( d_3 \mid (\tilde{q} - 1) \) according to Lemma 3.13. Therefore \( d_i \mid (\tilde{q} - 1) \) for all \( i \geq 3 \).

\( \square \)
Proof. The first part of the claim follows from the fact that \( q \) divides \( G \) connected component of \( l \) the level \( \gamma \). Then Case 1 holds for Lemma 4.10. Let \( n := \frac{n}{2}, \gamma := \gamma_1, l := l - 1 \).

Then Case 1 holds for \( \gamma \).

Lemma 4.7. If \( \alpha \in \mathbb{F}_{q^2}^* \) is an element of a connected component of \( G_{q^2} \) such that \(|\alpha|\) divides \( q + 1 \), then \( \alpha \) lies on the level \( l + 3 \) or 2 of \( G_{q^2} \). Moreover, if \( \alpha \) lies on the level \( l + 3 \) (resp. 2), then the order of any vertex at the level \( l + 3 \) (resp. 2) divides \( q + 1 \).

Proof. The first part of the claim follows from the fact that \( \vartheta(\alpha) \) is a leaf of a connected component of \( G_q \) and any tree in \( G_q \) has depth \( l + 2 \) or 1. According to Lemma 3.13 any leaf of \( G_q \) can be expressed in the form \( \vartheta(\gamma) \) for some \( \gamma \in \mathbb{F}_{q^2}^* \) with \(|\gamma| \mid (q + 1)\). Since the depth is the same for any tree in a given component, we get the second part of the claim.

From Lemma 4.7 we get the following.

Corollary 4.8. Let \( C_{q+1} \) and \( C_{q^2+1} \) be the cyclic subgroups of order \( q + 1 \) and \( q^2 + 1 \) in \( \mathbb{F}_{q}^* \) and \( \mathbb{F}_{q^2}^* \) respectively. Then
\[
C_{q+1} \subseteq \vartheta(C_{q^2+1}) \cup \vartheta^{l+2}(C_{q^2+1}).
\]

Proof. Let \( \alpha \in C_{q+1} \). Then \( \alpha \in \mathbb{F}_{q^2}^*, \alpha \notin \mathbb{F}_q \) and \( \vartheta(\alpha) \in \mathbb{F}_q \). Since \( \vartheta(\alpha) \) is a leaf of a connected component of \( G_q \), we have that \( \alpha \) lies on the level 2 or \( l + 3 \) of \( G_{q^2} \). In the latter case \( \alpha \) is a leaf of \( G_{q^2} \) and \( \alpha = \vartheta(\gamma) \) for some \( \gamma \in C_{q^2+1} \). In the first case \( \alpha \) belongs to a tree of \( G_{q^2} \) having depth \( l + 3 \), whose leaves have predecessors in \( C_{q^2+1} \), namely \( \alpha \in \vartheta^{l+2}(C_{q^2+1}) \).

Lemma 4.9. Let \( \gamma \) be an element of \( \mathbb{F}_{q^2}^* \) such that \(|\gamma| \mid (q^2 + 1) \) but \(|\vartheta(\gamma)| \mid (q \pm 1)\). Let \( p_1 \) be the smallest prime which divides \( q + 1 \) and \( p_2 \) the smallest prime which divides \( q - 1 \). Then
\[
|\vartheta^i(\gamma)| \geq p_1 \cdot p_2 \geq (1 + 2^{l+1}) \cdot p_2
\]
for any integer \( i \) such that \( 1 \leq i \leq l + 1 \). Moreover, if \(|\vartheta^{l+2}(\gamma)| \) does not divide \( q + 1 \), the inequality \( (4.1) \) holds also for \( l + 2 \leq i \leq l + 4 \).

Proof. The first inequality in \( (4.1) \) for the indices \( i \) with \( 1 \leq i \leq l + 1 \) follows from the tables corresponding to Case 2 and 3 and from the fact that \( \gcd(q+1, q-1) = 1 \). If \(|\vartheta^{l+2}(\gamma)| \) does not divide \( q + 1 \), then the only possible case is Case 3.

The second inequality in \( (4.1) \) follows from Lemma 3.8.

From the tables above we deduce the following characterizations of some subsets of \( A_n \) and \( B_n \).

Lemma 4.10. Let
\[
A_{n_1} := \{ x \in A_n : \text{Tr}_n(x) = \text{Tr}_n(x^{-1}) = 1 \};
\]
\[
A_{n_0} := \{ x \in A_n : \text{Tr}_n(x) = \text{Tr}_n(x^{-1}) = 0 \};
\]
\[
B_{n_{10}} := \{ x \in B_n : \text{Tr}_n(x) = 0, \text{Tr}_n(x^{-1}) = 1 \};
\]
\[
B_{n_{10}} := \{ x \in B_n : \text{Tr}_n(x) = 1, \text{Tr}_n(x^{-1}) = 0 \}.
\]
Then
\[ A_{n_1} := \vartheta^2 \{ \gamma \in \mathbb{F}_q^* : |\gamma| \mid (q^2 + 1) \text{ and } |\vartheta(\gamma)| \mid (q + 1) \}; \]
\[ A_{n_0} := \bigcup_{i=3}^{t+4} \vartheta^i \{ \gamma \in \mathbb{F}_q^* : |\gamma| \mid (q^2 + 1) \text{ and } |\vartheta(\gamma)| \mid (q + 1) \}; \]
\[ B_{n_1} := \vartheta^{l+3} \{ \gamma \in \mathbb{F}_q^* : |\gamma| \mid (q^2 + 1) \text{ and } |\vartheta^{l+2}(\gamma)| \mid (q + 1) \}; \]
\[ B_{n_0} := \vartheta^{l+4} \{ \gamma \in \mathbb{F}_q^* : |\gamma| \mid (q^2 + 1) \text{ and } |\vartheta^{l+2}(\gamma)| \mid (q + 1) \}. \]

Finally we deduce the following.

**Lemma 4.11.** The map \( \vartheta \) acts as a permutation on the set
\[ \vartheta^{l+4} \{ \gamma \in \mathbb{F}_q^* : |\gamma| \mid (q^2 + 1) \}. \]

**Proof.** If \( \gamma \in \mathbb{F}_q^* \), then \( \vartheta(\gamma) \) is a leaf of \( G_{q^2} \) and belongs to the level \( l + 3 \) of a tree in \( G_{q^2} \). Hence \( \vartheta^{l+4}(\gamma) \) is \( \vartheta \)-periodic. \( \square \)

### 4.2. Roots of Dickson polynomials

Elements of the form \( x + x^{-1} \) play a crucial role in Dickson polynomials.

Let \( q := 2^n \) for some positive integer \( n \). We recall that the Dickson polynomial \( D_m(x) \in \mathbb{F}_q[x] \) of the first kind of degree \( m > 0 \) with parameter 1 is
\[ D_m(x) := \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-1)^i x^{m-2i}. \]

The following property holds:
\[ D_m(x + x^{-1}) = x^m + x^{-m}. \]

Equivalently,
\[ D_m(x + x^{-1}) = x^{-m} \cdot (x^m + 1)^2. \]

For any \( \alpha \in \mathbb{F}_q \) we can find some \( \gamma \in \mathbb{F}_{q^2} \) such that \( \alpha = \gamma + \gamma^{-1} \). Therefore, finding a root \( \alpha \) in \( \mathbb{F}_q \) of \( D_m(x) \) amounts to finding an element \( \gamma \in \mathbb{F}_{q^2} \) such that
\[ D_m(\gamma + \gamma^{-1}) = \gamma^{-m} \cdot (\gamma^m + 1)^2 = 0, \]
which is equivalent to saying that \( \gamma \) is an element of \( \mathbb{F}_{q^2}^* \) such that \( |\gamma| \) divides \( m \).

Let \( m \) be an integer such that \( m > 1 \) and \( m \mid (q + 1) \).

We define the following sets:
\[ S_m := \{ \alpha \in \mathbb{F}_q^* : D_m(\alpha) = D_m(\alpha^{-1}) = 0 \}; \]
\[ T_m := \{ \alpha \in \mathbb{F}_q^* : D_m(\alpha) = 0, D_m(\alpha^{-1}) \neq 0 \}. \]

In [2] the authors investigated the existence of elements \( \alpha \in \mathbb{F}_q^* \) belonging to \( S_m \) or \( T_m \). In [2] Section 2] they gave some existence and non-existence results. First they considered the case \( m := q + 1 \), defining
\[ N_{q+1} := |S_{q+1}|. \]

Then they proved the following result (see [2] Theorem 2.1)).

**Theorem 4.12.** We have
\[ N_{q+1} = \frac{q + 1 + K(\chi_q)}{4}, \]
where \( K(\chi_q) = \sum_{x \in \mathbb{F}_q^*} \chi_q(x + x^{-1}) \) is a Kloosterman sum.
Therefore, we have that Lemma 4.14.

**Corollary 4.13.** Let \( n \) be a positive integer and \( q = 2^n \). There is \( \alpha \in \mathbb{F}_q^* \) such that both \( \alpha \) and \( \alpha^{-1} \) are roots of \( D_{q+1}(x) \). When \( q > 4 \), there is \( \alpha \in \mathbb{F}_q^* \) such that \( \alpha \) is a root of \( D_{q+1}(x) \), but \( \alpha^{-1} \) is not. For \( q = 2, 4 \), there is no \( \alpha \in \mathbb{F}_q^* \) such that \( \alpha \) is a root of \( D_{q+1}(x) \), but \( \alpha^{-1} \) is not.

Indeed, the fact that \( S_{q+1} \neq \emptyset \) can be proved without computing \( N_{q+1} \), just relying upon the Koblitz curve \( E \) and on the graph \( G_q \). We notice in passing that

\[
S_{q+1} = \{ \vartheta(\gamma) : \gamma \in \mathbb{F}_q^{**}, |\gamma| \mid (q + 1) \}.
\]

In the following we denote by \( L_{A_n} \) and \( L_{B_n} \) the sets of leaves of \( G_q \) contained in \( A_n \) and \( B_n \) respectively.

**Lemma 4.14.** \( L_{A_n} \) is not empty and \( S_{q+1} = L_{A_n} \).

**Proof.** We notice that \( E(\mathbb{F}_2) \subseteq E(\mathbb{F}_{2^n}) \) for all positive integers \( n \). Since

\[
E(\mathbb{F}_2) = \{ O, (0, 1), (1, 1), (1, 0) \},
\]

we have that \( |E(\mathbb{F}_{2^n})| \geq 4 \). Therefore \( A_n \) is not empty and the same holds for \( L_{A_n} \).

If \( \alpha \in S_{q+1} \), then there exist two elements \( \beta, \gamma \in \mathbb{F}_q^{**} \) such that \( |\beta| \mid (q + 1) \) and \( |\gamma| \mid (q + 1) \) with \( \vartheta(\beta) = \alpha \) and \( \vartheta(\gamma) = \alpha^{-1} \). In particular, \( \alpha \) and \( \alpha^{-1} \) are leaves of \( G_q \) and are not \( \vartheta \)-periodic. Moreover \( \vartheta(\alpha) \) is not \( \vartheta \)-periodic too. In fact, if \( \alpha = 1 \), then \( \vartheta(\alpha) = 0 \), which belongs to the tree rooted in \( \infty \). If \( \alpha \neq 1 \), then \( \alpha \neq \alpha^{-1} \).

If \( \vartheta(\alpha) \) were \( \vartheta \)-periodic, then the in-degree of \( \vartheta(\alpha) \) in \( G_q \) would be greater than 2, which is absurd. Hence \( \alpha \) and \( \alpha^{-1} \) belong to a tree of depth at least 2. We conclude that \( \alpha, \alpha^{-1} \in L_{A_n} \).

If \( \alpha \in L_{A_n} \), then \( \alpha^{-1} \in L_{A_n} \) too. According to Lemma 3.13 there exist two elements \( \beta \) and \( \gamma \) in \( \mathbb{F}_q^{**} \) such that \( |\beta| \mid (q + 1) \) and \( |\gamma| \mid (q + 1) \) with \( \vartheta(\beta) = \alpha \) and \( \vartheta(\gamma) = \alpha^{-1} \). Hence \( \alpha \in S_{q+1} \).

In Lemma 4.15 we prove that \( T_{q+1} \neq \emptyset \).

We recall that, for any \( x \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{ 0, \infty \} \), there are two distinct points in \( E(\mathbb{F}_q) \) having the same \( x \)-coordinate, while \( (0, 1) \) is the only point with \( x = 0 \). In fact, if \( P := (x_P, y_P) \in E(\mathbb{F}_q), y_P \neq 0 \), then \( -P = (x_P, x_P + y_P) \) (see [10] Section 2). Moreover, \( -P \) is the only point having the same \( x \)-coordinate of \( P \) and \( P = -P \) if and only if \( x_P = 0 \).

**Lemma 4.15.** \( L_{B_n} \) is not empty and \( T_{q+1} = L_{B_n} \), provided that \( n > 2 \).

**Proof.** First we prove that \( B_n \neq \emptyset \). Indeed,

\[
|A_n \cap \mathbb{F}_q^*| = \frac{|E(\mathbb{F}_q)| - 2}{2}.
\]

We recall that, according to Hasse bound,

\[
|E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}.
\]

Therefore

\[
|A_n \cap \mathbb{F}_q^*| \leq \frac{q - 1 + 2\sqrt{q}}{2}.
\]

We have that

\[
\frac{q - 1 + 2\sqrt{q}}{2} < q - 1 \iff 0 < q - 1 - 2\sqrt{q}.
\]
This latter is true if $n > 2$. In fact, the real function $f(x) = x - 1 - 2\sqrt{x}$ is strictly increasing for $x > 1$ and $f(8) > 0$.

Since $B_n \neq \emptyset$, also $L_{B_n} \neq \emptyset$.

If $\alpha \in T_{q+1}$, then there exists $\gamma \in \mathbb{F}_q^*$ such that $\vartheta(\gamma) = \alpha$ and $|\gamma| \mid (q + 1)$ but there is no $\beta \in \mathbb{F}_q^*$ such that $\vartheta(\beta) = \alpha^{-1}$ and $|\beta| \mid (q + 1)$. Therefore $\alpha^{-1} = \vartheta(\delta)$ for some $\delta \in \mathbb{F}_q^*$, according to Lemma 3.10. Hence $\Tr_n(\alpha) = 0$, while $\Tr_n(\alpha^{-1}) = 1$. Therefore $\alpha \in L_{B_n}$.

If $\alpha \in L_{B_n}$, then $\Tr_n(\alpha^{-1}) = 1$, while $\Tr_n(\alpha) = 0$. According to Lemma 3.10 there exists $\beta \in \mathbb{F}_q^*$ such that $\vartheta(\beta) = \alpha$. Moreover, according to Lemma 3.10 there exists $\gamma \in \mathbb{F}_q^*$ such that $\vartheta(\gamma) = \alpha^{-1}$. Therefore $D_{q+1}(\alpha) = 0$, while $D_{q+1}(\alpha^{-1}) \neq 0$. Hence $\alpha \in T_{q+1}$ according to Lemma 3.10. □

REFERENCES

1. I. F. Blake, X. Gao, A. J. Menezes, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of finite fields*, Kluwer Academic Publishers, Boston, MA, 1993.
2. A. Blokhuis, X. Cao, W.-S. Chou, and X.-D. Hou, *On the roots of certain Dickson polynomials*, J. Number Theory 188 (2018), 229–246.
3. H. Dubner and W. Keller, *Factors of generalized Fermat numbers*, Math. Comp. 64 (1995), no. 209, 397–405.
4. G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory 36 (1990), no. 3, 686–692.
5. R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Longman Scientific & Technical, Harlow, 1993.
6. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, 1997.
7. H. Meyn, *On the construction of irreducible self-reciprocal polynomials over finite fields*, AAECC 1 (1990), 43–53.
8. G. A. Garakov R. R. Varshamov, *On the theory of selfdual polynomials over a Galois field (Russian)*, Bull. Math. Sci. Math. R. S. Roumanie (N. S.) 13 (1969), 403–415.
9. I. Shparlinski, *On the multiplicative orders of $\gamma$ and $\gamma + 1$ over finite fields*, Finite Fields Appl. (2001), no. 7, 327–331.
10. S. Ugolini, *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two*, Theory and Applications of Finite Fields, Contemp. Math., vol. 579, Amer. Math. Soc., Providence, RI, 2012, pp. 187–204.
11. J. von zur Gathen and I. Shparlinski, *Gauss periods in finite fields*, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 162–177.

E-mail address: s.ugolini@unitn.it