On the multiplicative order of $\alpha + \alpha^{-1}$ in finite fields of characteristic two

Simone Ugolini

Università di Trento

SandGAL 2019
Politecnico di Milano
Cremona, 10 June 2019

Introduction

Problem (Blake et al., 1993)

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p.

Let $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$.

If $\alpha \in \mathbb{F}_q^* \backslash \{1\}$ is an element of order $\mathrm{ord}(\alpha)$, can we find $\mathrm{ord}(\alpha + \alpha^{-1})$ from $\mathrm{ord}(\alpha)$?

Problem (Blake et al., 1993)

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p.
Let $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$.
If $\alpha \in \mathbb{F}_q^* \backslash \{1\}$ is an element of order $\mathrm{ord}(\alpha)$, can we find $\mathrm{ord}(\alpha + \alpha^{-1})$ from $\mathrm{ord}(\alpha)$?

Problem (Blake et al., 1993)

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p.
Let $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$.
If $\alpha \in \mathbb{F}_q^* \setminus \{1\}$ is an element of order $\mathrm{ord}(\alpha)$, can we find $\mathrm{ord}(\alpha + \alpha^{-1})$ from $\mathrm{ord}(\alpha)$?

Some results

Theorem (Shparlinski, 2001)

If $\gamma \in \mathbb{F}_q^*$ does not belong to any proper subfield of $\mathbb{F}_q$, then at least one of the multiplicative orders of γ and $\gamma + \gamma^{-1}$ exceeds $c(p, \varepsilon)(\ln q)^{4/3-\varepsilon}$, where $c(p, \varepsilon) > 0$ depends only on p and arbitrary $\varepsilon > 0$.

Remark

The theorem above is a particular case of Theorem 4.3 in (von zur Gathen-Shparlinski, 1999).

Some results

Theorem (Shparlinski, 2001)

If $\gamma \in \mathbb{F}_q^*$ does not belong to any proper subfield of $\mathbb{F}_q$, then at least one of the multiplicative orders of γ and $\gamma + \gamma^{-1}$ exceeds $c(p, \varepsilon)(\ln q)^{4/3-\varepsilon}$, where $c(p, \varepsilon) > 0$ depends only on p and arbitrary $\varepsilon > 0$.

Remark

The theorem above is a particular case of Theorem 4.3 in (von zur Gathen-Shparlinski, 1999).

Theorem (Shparlinski, 2001)

For any fixed $\varepsilon > 0$ and sufficiently large q, for any positive divisors n and m of $q-1$ with $nm \geq q^{3/2+\varepsilon}$ there exists $\gamma \in \mathbb{F}_q^*$ with

$$\operatorname{ord}(\gamma) = n \quad \text{and} \quad \operatorname{ord}(\gamma + \gamma^{-1}) = m.$$

Dickson polynomials

For each integer $m > 0$ we define the Dickson polynomial of degree m as

$$D_m(x) = \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-1)^i x^{m-2i}$$

Properties

- $D_m(x) \in \mathbb{Z}[x]$.
- $D_m(x + x^{-1}) = x^m + x^{-m}$.

Dickson polynomials

Dickson polynomials

For each integer $m > 0$ we define the Dickson polynomial of degree m as

$$D_m(x) = \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-1)^i x^{m-2i}$$

Properties

- $D_m(x) \in \mathbb{Z}[x]$.
- $D_m(x + x^{-1}) = x^m + x^{-m}$.

Dickson polynomials

Dickson polynomials

For each integer $m > 0$ we define the Dickson polynomial of degree m as

$$D_m(x) = \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-1)^i x^{m-2i}$$

Properties

- $D_m(x) \in \mathbb{Z}[x]$.
- $D_m(x + x^{-1}) = x^m + x^{-m}$.

Dickson polynomials

- In the following $\mathbb{F}_q$ is a finite field with 2^n elements for some positive integer n.
- Dickson polynomials will be considered as polynomials in $\mathbb{F}_q[x]$.

Dickson polynomials

- In the following $\mathbb{F}_q$ is a finite field with 2^n elements for some positive integer n.
- Dickson polynomials will be considered as polynomials in $\mathbb{F}_q[x]$.

Roots of Dickson polynomials

- Any element $\alpha \in \mathbb{F}_q$ can be written as $\alpha = \gamma + \gamma^{-1}$ for some $\gamma \in \mathbb{F}_{q^2}^*$ (i.e. γ is a root of $x^2 + \alpha x + 1$ in $\mathbb{F}_{q^2}$).
- Finding a root $\alpha \in \mathbb{F}_q$ of $D_m(x)$ amounts to finding some $\gamma \in \mathbb{F}_{q^2}^*$ such that

$$D_m(\gamma + \gamma^{-1}) = \gamma^m + \gamma^{-m} = \gamma^{-m}(\gamma^m + 1)^2 = 0$$

or equivalently

$$\gamma^m + 1 = 0$$

namely $\mathrm{ord}(\gamma)$ divides m.

Roots of Dickson polynomials

- Any element $\alpha \in \mathbb{F}_q$ can be written as $\alpha = \gamma + \gamma^{-1}$ for some $\gamma \in \mathbb{F}_{q^2}^*$ (i.e. γ is a root of $x^2 + \alpha x + 1$ in $\mathbb{F}_{q^2}$).
- Finding a root $\alpha \in \mathbb{F}_q$ of $D_m(x)$ amounts to finding some $\gamma \in \mathbb{F}_{q^2}^*$ such that

$$D_m(\gamma + \gamma^{-1}) = \gamma^m + \gamma^{-m} = \gamma^{-m}(\gamma^m + 1)^2 = 0$$

or equivalently

$$\gamma^m + 1 = 0$$

namely $\mathrm{ord}(\gamma)$ divides m.

Roots of Dickson polynomials

A question by Blokhuis et al., 2018

Let m be an integer which divides $q+1 = 2^n + 1$.

Consider the sets

$$S_m := \{\alpha \in \mathbb{F}_q^* : D_m(\alpha) = D_m(\alpha^{-1}) = 0\};$$
$$T_m := \{\alpha \in \mathbb{F}_q^* : D_m(\alpha) = 0, D_m(\alpha^{-1}) \neq 0\}.$$

Are the sets S_m and T_m non-empty?

Roots of Dickson polynomials

A question by Blokhuis et al., 2018

Let m be an integer which divides $q+1 = 2^n+1$.
Consider the sets

$$S_m := \{\alpha \in \mathbb{F}_q^* : D_m(\alpha) = D_m(\alpha^{-1}) = 0\};$$
$$T_m := \{\alpha \in \mathbb{F}_q^* : D_m(\alpha) = 0, D_m(\alpha^{-1}) \neq 0\}.$$

Are the sets S_m and T_m non-empty?

Roots of Dickson polynomials

Some results (Blokhuis et al., 2018)

- Some answers are given for certain values of m in (Blokhuis et al., 2018).
- In the particular case $m = q + 1$ the sets S_{q+1} and T_{q+1} are both non-empty, provided that $q > 4$.

Roots of Dickson polynomials

Some results (Blokhuis et al., 2018)

- Some answers are given for certain values of m in (Blokhuis et al., 2018).
- In the particular case $m = q + 1$ the sets S_{q+1} and T_{q+1} are both non-empty, provided that $q > 4$.

The graph associated with the map $x \mapsto x + x^{-1}$

In (Ugolini, 2012) I studied the structure of the graph associated with the map ϑ defined on $\mathbf{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$ as

$$\vartheta : x \mapsto \begin{cases} \infty & \text{if } x \in \{0, \infty\}; \\ x + x^{-1} & \text{otherwise} \end{cases}$$

The graph associated with the map $x \mapsto x + x^{-1}$

In (Ugolini, 2012) I studied the structure of the graph associated with the map ϑ defined on $\mathbf{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$ as

$$\vartheta : x \mapsto \begin{cases} \infty & \text{if } x \in \{0, \infty\}; \\ x + x^{-1} & \text{otherwise} \end{cases}$$

A note on the graph's construction

If $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{P}^1(\mathbb{F}_q)$ and $\alpha_2 = \vartheta(\alpha_1), \alpha_3 = \vartheta(\alpha_2)$, then

$$\alpha_1 \longrightarrow \alpha_2 \longrightarrow \alpha_3$$

The graph associated with the map $x \mapsto x + x^{-1}$

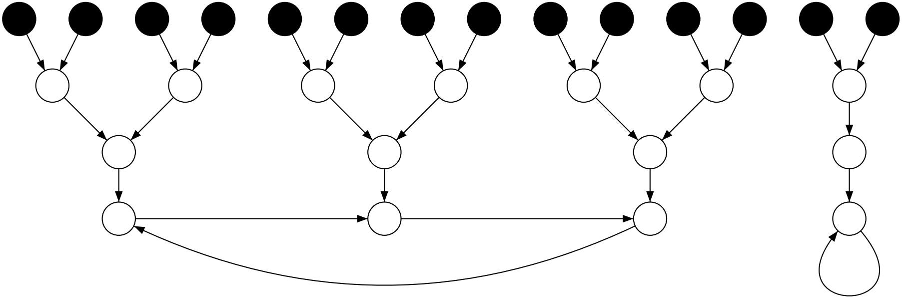
In (Ugolini, 2012) I studied the structure of the graph associated with the map ϑ defined on $\mathbf{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$ as

$$\vartheta : x \mapsto \begin{cases} \infty & \text{if } x \in \{0, \infty\}; \\ x + x^{-1} & \text{otherwise} \end{cases}$$

A remark on the elements in S_{q+1} and T_{q+1}

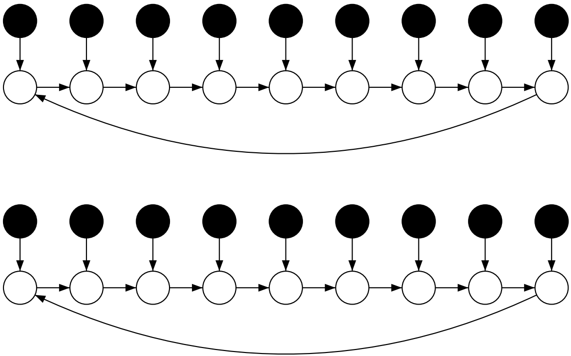
The elements in S_{q+1} and T_{q+1} appear as leaves of the connected components of the graph associated with the map ϑ.

Example: graph associated with ϑ over $\mathbb{F}_q = \mathbb{F}_{2^6}$



Black nodes: elements in S_{q+1}

Example: graph associated with ϑ over $\mathbb{F}_q = \mathbb{F}_{2^6}$



$\boxed{\text{Black nodes: elements in } T_{q+1}}$

About the structure of the graph

The properties of the graph, as

- the depth of the trees (which is the same in any connected component),
- the length of the cycles,

can be explained relating the map ϑ to the duplication map on a certain elliptic curve (a Koblitz curve).

Theorem

If $n := 2^l m$ for some non-negative integer l and some odd integer m, then either all trees in a connected component have depth 1 or $l + 2$.

Example

If $q = 2^6$, then $n = 2 \cdot 3$ and the depths can be either 1 or 3.

About the structure of the graph

The properties of the graph, as

- the depth of the trees (which is the same in any connected component),
- the length of the cycles,

can be explained relating the map ϑ to the duplication map on a certain elliptic curve (a Koblitz curve).

Theorem

If $n := 2^l m$ for some non-negative integer l and some odd integer m, then either all trees in a connected component have depth 1 or $l + 2$.

Example

If $q = 2^6$, then $n = 2 \cdot 3$ and the depths can be either 1 or 3.

About the structure of the graph

The properties of the graph, as

- the depth of the trees (which is the same in any connected component),
- the length of the cycles,

can be explained relating the map ϑ to the duplication map on a certain elliptic curve (a Koblitz curve).

Theorem

If $n := 2^l m$ for some non-negative integer l and some odd integer m, then either all trees in a connected component have depth 1 or $l + 2$.

Example

If $q = 2^6$, then $n = 2 \cdot 3$ and the depths can be either 1 or 3.

About the structure of the graph

The properties of the graph, as

- the depth of the trees (which is the same in any connected component),
- the length of the cycles,

can be explained relating the map ϑ to the duplication map on a certain elliptic curve (a Koblitz curve).

Theorem

If $n := 2^l m$ for some non-negative integer l and some odd integer m, then either all trees in a connected component have depth 1 or $l + 2$.

Example

If $q = 2^6$, then $n = 2 \cdot 3$ and the depths can be either 1 or 3.

About the structure of the graph

The properties of the graph, as

- the depth of the trees (which is the same in any connected component),
- the length of the cycles,

can be explained relating the map ϑ to the duplication map on a certain elliptic curve (a Koblitz curve).

Theorem

If $n := 2^l m$ for some non-negative integer l and some odd integer m, then either all trees in a connected component have depth 1 or $l + 2$.

Example

If $q = 2^6$, then $n = 2 \cdot 3$ and the depths can be either 1 or 3.

About the structure of the graph

The properties of the graph, as

- the depth of the trees (which is the same in any connected component),
- the length of the cycles,

can be explained relating the map ϑ to the duplication map on a certain elliptic curve (a Koblitz curve).

Theorem

If $n := 2^l m$ for some non-negative integer l and some odd integer m, then either all trees in a connected component have depth 1 or $l + 2$.

Example

If $q = 2^6$, then $n = 2 \cdot 3$ and the depths can be either 1 or 3.

- In (Ugolini, 2018) some results on the orders of the iterates are given.
- Let γ be an element of $\mathbb{F}_{q^4} \backslash \{0, 1\}$ such that $\mathrm{ord}(\gamma) \mid (q^2 + 1)$.
- It can be proved that γ is a leaf of a tree having depth $l + 4$ in the graph associated with ϑ over $\mathbf{P}^1(\mathbb{F}_{q^4})$.

On the multiplicative orders of the iterates

- In (Ugolini, 2018) some results on the orders of the iterates are given.
- Let γ be an element of $\mathbb{F}_{q^4} \backslash \{0, 1\}$ such that $\text{ord}(\gamma) \mid (q^2 + 1)$.
- It can be proved that γ is a leaf of a tree having depth $l + 4$ in the graph associated with ϑ over $\mathbf{P}^1(\mathbb{F}_{q^4})$.

On the multiplicative orders of the iterates

- In (Ugolini, 2018) some results on the orders of the iterates are given.
- Let γ be an element of $\mathbb{F}_{q^4} \backslash \{0, 1\}$ such that $\text{ord}(\gamma) \mid (q^2 + 1)$.
- It can be proved that γ is a leaf of a tree having depth $l + 4$ in the graph associated with ϑ over $\mathbf{P}^1(\mathbb{F}_{q^4})$.

- Let γ_i be the i-th iterate of γ, e.g.

$$\begin{aligned}\gamma_1 &= \vartheta(\gamma),\\ \gamma_2 &= \vartheta(\gamma_1) = \vartheta^2(\gamma),\\ \gamma_3 &= \vartheta(\gamma_2) = \vartheta^3(\gamma),\\ &\dots\end{aligned}$$

- One of the following 3 cases is possible for the iterates of γ.

On the multiplicative orders of the iterates

- Let γ_i be the *i*-th iterate of γ, e.g.

$$\begin{aligned} \gamma_1 &= \vartheta(\gamma), \\ \gamma_2 &= \vartheta(\gamma_1) = \vartheta^2(\gamma), \\ \gamma_3 &= \vartheta(\gamma_2) = \vartheta^3(\gamma), \\ &\dots \end{aligned}$$

- One of the following 3 cases is possible for the iterates of γ.

Case 1

- ord$(\gamma) \mid (q^2+1)$;
- ord$(\gamma_1) \mid (q+1)$;
- ord$(\gamma_2) \mid (q-1)$;
- $\ldots$;
- ord$(\gamma_{l+4}) \mid (q-1)$.

Case 1

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q+1)$;
- $\mathrm{ord}(\gamma_2) \mid (q-1)$;
- $\ldots$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 1

- $\mathrm{ord}(\gamma) \mid (q^2 + 1)$;
- $\mathrm{ord}(\gamma_1) \mid (q + 1)$;
- $\mathrm{ord}(\gamma_2) \mid (q - 1)$;
- $\ldots$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q - 1)$.

Case 1

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q+1)$;
- $\mathrm{ord}(\gamma_2) \mid (q-1)$;
- $\ldots$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 1

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q+1)$;
- $\mathrm{ord}(\gamma_2) \mid (q-1)$;
- $\ldots$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 2

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\ldots$
- $\mathrm{ord}(\gamma_{l+2}) \mid (q+1)$;
- $\mathrm{ord}(\gamma_{l+3}) \mid (q-1)$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 2

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\ldots$
- $\mathrm{ord}(\gamma_{l+2}) \mid (q+1)$;
- $\mathrm{ord}(\gamma_{l+3}) \mid (q-1)$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 2

- ord$(\gamma) \mid (q^2+1)$;
- ord$(\gamma_1) \mid (q^2-1)$, ord$(\gamma_1) \nmid (q+1)$, ord$(\gamma_1) \nmid (q-1)$;
- ord$(\gamma_2) \mid (q^2-1)$, ord$(\gamma_2) \nmid (q+1)$, ord$(\gamma_2) \nmid (q-1)$;
- $\ldots$
- ord$(\gamma_{l+2}) \mid (q+1)$;
- ord$(\gamma_{l+3}) \mid (q-1)$;
- ord$(\gamma_{l+4}) \mid (q-1)$.

Case 2

- ord$(\gamma) \mid (q^2+1)$;
- ord$(\gamma_1) \mid (q^2-1)$, ord$(\gamma_1) \nmid (q+1)$, ord$(\gamma_1) \nmid (q-1)$;
- ord$(\gamma_2) \mid (q^2-1)$, ord$(\gamma_2) \nmid (q+1)$, ord$(\gamma_2) \nmid (q-1)$;
- $\ldots$
- ord$(\gamma_{l+2}) \mid (q+1)$;
- ord$(\gamma_{l+3}) \mid (q-1)$;
- ord$(\gamma_{l+4}) \mid (q-1)$.

Case 2

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\dots$
- $\mathrm{ord}(\gamma_{l+2}) \mid (q+1)$;
- $\mathrm{ord}(\gamma_{l+3}) \mid (q-1)$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 2

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\ldots$
- $\mathrm{ord}(\gamma_{l+2}) \mid (q+1)$;
- $\mathrm{ord}(\gamma_{l+3}) \mid (q-1)$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 2

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\dots$
- $\mathrm{ord}(\gamma_{l+2}) \mid (q+1)$;
- $\mathrm{ord}(\gamma_{l+3}) \mid (q-1)$;
- $\mathrm{ord}(\gamma_{l+4}) \mid (q-1)$.

Case 3

- $\operatorname{ord}(\gamma) \mid (q^2+1)$;
- $\operatorname{ord}(\gamma_1) \mid (q^2-1)$, $\operatorname{ord}(\gamma_1) \nmid (q+1)$, $\operatorname{ord}(\gamma_1) \nmid (q-1)$;
- $\operatorname{ord}(\gamma_2) \mid (q^2-1)$, $\operatorname{ord}(\gamma_2) \nmid (q+1)$, $\operatorname{ord}(\gamma_2) \nmid (q-1)$;
- $\dots$
- $\operatorname{ord}(\gamma_{l+4}) \mid (q^2-1)$, $\operatorname{ord}(\gamma_{l+4}) \nmid (q+1)$, $\operatorname{ord}(\gamma_{l+4}) \nmid (q-1)$.

Case 3

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\ldots$
- $\mathrm{ord}(\gamma_{l+4}) \mid (q^2-1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q+1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q-1)$.

Case 3

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\dots$
- $\mathrm{ord}(\gamma_{l+4}) \mid (q^2-1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q+1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q-1)$.

Case 3

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- ...
- $\mathrm{ord}(\gamma_{l+4}) \mid (q^2-1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q+1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q-1)$.

Case 3

- $\mathrm{ord}(\gamma) \mid (q^2+1)$;
- $\mathrm{ord}(\gamma_1) \mid (q^2-1)$, $\mathrm{ord}(\gamma_1) \nmid (q+1)$, $\mathrm{ord}(\gamma_1) \nmid (q-1)$;
- $\mathrm{ord}(\gamma_2) \mid (q^2-1)$, $\mathrm{ord}(\gamma_2) \nmid (q+1)$, $\mathrm{ord}(\gamma_2) \nmid (q-1)$;
- $\ldots$
- $\mathrm{ord}(\gamma_{l+4}) \mid (q^2-1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q+1)$, $\mathrm{ord}(\gamma_{l+4}) \nmid (q-1)$.

Final remarks

- For other properties, see (Ugolini, 2018).
- For example, we can deduce that any element in the cyclic group C_{q+1} of order $q+1$ in $\mathbb{F}_{q^2}^*$ is expressible as

$$\vartheta(\alpha) \quad \text{or} \quad \vartheta^{l+2}(\alpha)$$

for some α in the cyclic group C_{q^2+1} of order q^2+1 in $\mathbb{F}_{q^4}^*$.
- There are also some relations between the order and the trace of the iterates.

Final remarks

- For other properties, see (Ugolini, 2018).
- For example, we can deduce that any element in the cyclic group C_{q+1} of order $q+1$ in $\mathbb{F}_{q^2}^*$ is expressible as

$$\vartheta(\alpha) \quad \text{or} \quad \vartheta^{l+2}(\alpha)$$

  for some α in the cyclic group C_{q^2+1} of order q^2+1 in $\mathbb{F}_{q^4}^*$.
- There are also some relations between the order and the trace of the iterates.

Final remarks

- For other properties, see (Ugolini, 2018).
- For example, we can deduce that any element in the cyclic group C_{q+1} of order $q+1$ in $\mathbb{F}_{q^2}^*$ is expressible as

$$\vartheta(\alpha) \quad \text{or} \quad \vartheta^{l+2}(\alpha)$$

  for some α in the cyclic group C_{q^2+1} of order q^2+1 in $\mathbb{F}_{q^4}^*$.
- There are also some relations between the order and the trace of the iterates.

References I

I. F. Blake, X. Gao, A. J. Menezes, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian
Applications of finite fields
Kluwer Academic Publishers, 1993.

A. Blokhuis, X. Cao, W.-S. Chou, X.-D. Hou
On the roots of certain Dickson polynomials
Journal of Number Theory, 188, pp. 229–246, 2018.

J. von zur Gathen and I. Shparlinski
Gauß periods in finite fields
Proceedings of the fifth International Conference on Finite Fields and Applications, Augsburg, 1999, pp. 162–177, 2001.

I. Shparlinski
On the multiplicative orders of γ and $\gamma + \gamma^{-1}$ over finite fields
Finite Fields and Their Applications, 7, pp. 327–331, 2001.

References II

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., 579, pp. 187–204, 2012.

S. Ugolini
Some notes on the multiplicative order of $\alpha + \alpha^{-1}$ in finite fields of characteristic two
Preprint ArXiv, 2018.