Existence theorems for r-primitive elements in finite fields

Stephen D. Cohen
(joint work with Giorgos Kapetanakis)

Carleton $\mathbb{F}_q$ eSeminar
7 October 2020

Outline

1 Introduction

2 The trace and line properties

3 Old results, mainly on primitive elements

4 New theorem – trace property

5 New theorems – line property

Table of Contents

1 Introduction

2 The trace and line properties

3 Old results, mainly on primitive elements

4 New theorem – trace property

5 New theorems – line property

Primitive and r-primitive elements in $\mathbb{F}_q$

The multiplicative group of $\mathbb{F}_q$ is cyclic of order $q-1$.
A *primitive element* of $\mathbb{F}_q$ is a generator.

$\mathbb{F}_q$ contains $\phi(q-1)$ primitive elements.

Suppose $r|q-1$.
An *r-primitive element* in $\mathbb{F}_q$ is an element of order $(q-1)/r$.

- primitive = 1-primitive.
- An r-primitive element of $\mathbb{F}_{q^n}$ is the rth power of a primitive element.
- An additive analogue of an r-primitive element is a *k-normal* element ($k \geq 0$).

- The existence theorems being presented involve r-primitive elements in $\mathbb{F}_{q^n}$, $n \geq 2$, regarded as an extension of $\mathbb{F}_q$.

e-free elements of $\mathbb{F}_q^*$

Suppose $e|q-1$.
$\alpha \in \mathbb{F}_q$ is *e-free* if $\alpha \neq \beta^d, \beta \in \mathbb{F}_q, d|e, d > 1$.

Thus a $(q-1)$-free element is the same as a primitive element.

- There are $\theta(e)(q-1)$ e-free elements in $\mathbb{F}_q$, where $\theta(e) = \phi(e)/e$.
- Replace q by q^n in the above for primitive and e-free elements in $\mathbb{F}_{q^n}$.

Another characterisation of r-free elements.
Suppose $r|q-1$ and let $C_{(q-1)/r}$ denote the cyclic subgroup of $\mathbb{F}_q^*$ of order $(q-1)/r$ comprising all rth powers in $\mathbb{F}_q^*$.
Then $\alpha \in \mathbb{F}_q^*$ is r-primitive if

1. $\alpha \in C_{(q-1)/r}$,
2. α is $\dfrac{q-1}{r}$-free in $C_{(q-1)/r}$.

Characteristic function for e-free elements

Let $\alpha \in \mathbb{F}_q^*$. Then

$$\lambda_e(\alpha) := \theta(e) \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{(\eta_d)} \eta_d(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is } e\text{-free,} \\ 0 & \text{otherwise,} \end{cases}$$

where $\sum_{(\eta_d)}$ denotes a sum over all $\phi(d)$ multiplicative characters η_d of $\mathbb{F}_q^*$ of order d.

Hint. Both sides are multiplicative functions of e.

Table of Contents

1 Introduction

2 The trace and line properties

3 Old results, mainly on primitive elements

4 New theorem – trace property

5 New theorems – line property

The trace property for r-primitive elements in $\mathbb{F}_{q^n}$

From now on, assume $n \geq 2$.

For $\alpha \in \mathbb{F}_{q^n}$, $\mathrm{Tr}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} \in \mathbb{F}_q$. In particular, if α is the root of an irreducible polynomial of degree n its trace is the negative of the coefficient of x^{n-1}.

- When $n = 2$ there is no primitive element with trace 0.

$\mathbb{F}_{q^n}$ has the *trace property for r-primitive elements* if for all $a \in \mathbb{F}_q$ (with $a \neq 0$ if $n = 2$), there exists an r-primitive $\alpha \in \mathbb{F}_{q^n}$ with trace a.

- For fixed q and r, the trace property gets easier (less demanding) as n increases. So **hardest** case is $n = 2$.

The line property in $\mathbb{F}_{q^n}$, $n \geq 2$

Let $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma)$ and $\beta \in \mathbb{F}_{q^n}^*$. Call a set of the form

$$L_{\beta,\gamma} = \{\beta(\gamma + b) : b \in \mathbb{F}_q\}$$

the *line* of β and γ in $\mathbb{F}_{q^n}$.

$\mathbb{F}_{q^n}$ has the *line property for r-primitive elements* if every line in $\mathbb{F}_{q^n}/\mathbb{F}_q$ contains an r-primitive element.

- For a fixed prime power q and r, the line property gets harder as n increases. So **easiest** case is $n = 2$.

The line property implies the **non-zero** trace property

Lemma 1

Suppose $\mathbb{F}_{q^n}$ has the line property for r-primitive elements. Then it has the non-zero trace property.

Easily, there exist linearly independent members $\{\alpha, \beta\}$ of $\mathbb{F}_{q^n}$ with $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha), \mathrm{Tr}(\alpha) = 1, \mathrm{Tr}(\beta) = 0$.
Given $a \in \mathbb{F}_q^*$, then on the line

$$\{a\alpha + b\beta : b \in \mathbb{F}_q\} = \{\beta(a\alpha/\beta + b) : b \in \mathbb{F}_q\}$$

there is an r-primitive element with trace a.

Table of Contents

1. Introduction
2. The trace and line properties
3. Old results, mainly on primitive elements
4. New theorem – trace property
5. New theorems – line property

The trace property for **primitive** elements in $\mathbb{F}_{q^n}$

Theorem 1 (SDC 1990 [1], with M Prešern 2005 [2])

For any $n \geq 2$, $\mathbb{F}_{q^n}$ has the trace property, except for $\mathbb{F}_{4^3}$.

- Theorem 1 is a **complete** existence theorem.
- The revised proof establishes the result theoretically,
  i.e., no direct verification by computation in any case is required.

The line property for **primitive** elements in $\mathbb{F}_{q^2}, \mathbb{F}_{q^3}$

Theorem 2 (SDC 1983 [3], 2010 [4])

Every line in $\mathbb{F}_{q^2}$ contains a primitive element.

- Theorem 2 is a **complete** existence theorem.
- The revised proof establishes the result theoretically, i.e., no direct verification by computation in any case is required.

Theorem 3 (SDC,G Bailey,N Sutherland,T Trudgian 2019 [5])

Every line in $\mathbb{F}_{q^3}$ contains a primitive element, except when $q = 3, 4, 5, 7, 9, 11, 13, 31, 37$.

- Theorem 3 is a **complete** existence theorem.
- The proof involves a theoretical refinement of an incomplete one of SDC [4]; nevertheless 82 values of q between 103 and 4951 had to be verified by (extensive!) computation.

The trace property for r-primitive elements: an old result

For fixed q, n both the trace and line properties get harder as r increases (because the number of r-primitive elements decreases).
In particular, r cannot be too close to q^n.

The following is from an alternative proof of a theorem of Ozbudak [6].

Theorem 4 (SDC 2005 [7])

Suppose $r | q^n - 1$ *and*

$$r < \frac{q^{\frac{n-4}{3}}}{21}.$$

Then $\mathbb{F}_{q^n}$ *has the trace property for* r*-primitive elements.*

- The bound could easily be improved!
- Theorem 4 is vacuous unless $n \geq 5$.
- It implies $\mathbb{F}_{q^5}$ has the trace property for 2-primitive elements provided $q > 74088$.

Table of Contents

1. Introduction
2. The trace and line properties
3. Old results, mainly on primitive elements
4. New theorem – trace property
5. New theorems – line property

Existence theorem for **2-primitive** elements in $\mathbb{F}_{q^n}$

Necessarily, let q be odd.

Theorem 5 (SDC, GK 2020 [8])

Suppose $n \geq 2$ and q is an odd prime power. Then $\mathbb{F}_{q^n}$ has the trace property, except when $n = 2$ and $q = 3, 5, 7, 9, 11, 13, 31$.

Special case. $\frac{q^n-1}{2}$ is odd, i.e., n is odd and $q \equiv 3 \bmod 4$.
Here $\alpha \in \mathbb{F}_{q^2}$ is 2-primitive if and only if $-\alpha$ is primitive and result follows from Theorem 1.

If $\frac{q^n-1}{2}$ is even then

1. $\alpha \in \mathbb{F}_{q^2}$ is 2-primitive if and only if $-\alpha$ is 2-primitive,
2. the number of 2-primitive elements in $\mathbb{F}_{q^2}$ is half the number of primitive elements.

Idea of proof of Theorem 5

Assume $(q^n - 1)$ even. Given $a \in \mathbb{F}_q$ we want to count the number of primitive $\alpha \in \mathbb{F}_q$ whose **square** has trace a.
Define $N_a(e)$ to be twice the number of e-free $\alpha \in \mathbb{F}_{q^n}$ for which α^2 has trace a.
We want to show $N_a := N_a(q^n - 1)$ is positive. simplified expressions

$$N_a(e) = \frac{\theta(e)}{q} \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{(\eta_d)} \sum_{u \in \mathbb{F}_q} \psi(ua) S_u(\eta_d),$$

where

$$S_u(\eta_d) = \sum_{\alpha \in \mathbb{F}_{q^n}} \eta_d(\alpha) \psi(u\alpha^2)$$

and ψ is the canonical additive character in $\mathbb{F}_{q^n}$.

Bounds for $S_u(\eta_d)$

$$N_a(e) = \frac{\theta(e)}{q} \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{(\eta_d)} \sum_{u \in \mathbb{F}_q} \psi(ua) S_u(\eta_d), \quad e | q^n - 1,$$

where $S_u(\eta_d) = \sum_{\alpha \in \mathbb{F}_{q^n}} \eta_d(\alpha)\psi(u\alpha^2)$.

$S_0(\eta_1) = q^n - 1$;
$S_u(\eta_1) = \varepsilon q^{n/2} - 1$, $u \neq 0$, n even, $\varepsilon = \pm 1$; quadratic Gauss sum
$S_u(\eta_1)$ terms cancel out, $u \neq 0$, n odd;
$|S_u(\eta_d)| \leq 2q^{n/2}$, $d > 1, u \neq 0$.

The case $a \neq 0$

$$N_a(e) = \frac{\theta(e)}{q} \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{(\eta_d)} \sum_{u \in \mathbb{F}_q} \psi(ua) S_u(\eta_d)$$

$$\frac{N_a(e)}{\theta(e)} - q^{n/2-1}(q^{n/2} + \varepsilon q)) = \frac{1}{2q} \sum_{\substack{d|e \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{(\eta_d)} s_1(\hat{\eta}_d)(S_1(\eta_d) + S_c(\eta_d)),$$

where c is a fixed non-square in $\mathbb{F}_q$ and $s_1(\hat{\eta}_d) = \sum_{u \in \mathbb{F}_q} \hat{\eta}_d(u)\psi(u^2 a)$.

This leads to:

$$N_a(e) \geq \theta(e) q^{(n-1)/2} \{q^{(n-1)/2} + \varepsilon q^{1/2} - 4W(e)\},$$

where $\varepsilon = 0, n$ odd, $W(m) = 2^{\omega(m)} =$ number of squarefree divisors of m. So, for example, $N_a > 0$ whenever $q^{(n-1)/2} > -\varepsilon q^{1/2} + 4W(q^n - 1)$.

- Method fails when $n = 2$ and $\varepsilon = -1$, i.e., if $q \equiv 1 \mod 4$.

The case $n > 4, a \neq 0$

Simplifying: $N_a > 0$ if

$$q^{(n-1)/2} > 4W(q^n - 1). \tag{1}$$

- Using the elementary estimate $W(m) < 4515m^{1/8}$, (1) is satisfied if $q^{3n/8} > 18060$.
- This fails to establish the trace property for 4222 values of q^n.
- With a more careful bound for $W(q^n - 1)$, (1) holds for all but 12 values of q^n, including $37^5, 13^6, 3^8$.
- For these 12 q^n, use the exact value of $W(q^n - 1)$ to show that (1) is satisfied in every case.

The prime sieve

Let the product of the distinct primes in $q^n - 1$ be $kp_1 \dots p_s$, where $p_1, \dots, p_s$ are distinct primes not dividing k (sieving primes) while k involves small primes.

The prime sieve

$$N_a \geq \sum_{i=1}^{s} N_a(kp_i) - (s-1)N_a(k).$$

Thus, to ensure N_a positive, instead of the sufficient condition
$q^{(n-1)/2} > 4W(q^n - 1)$
we have the the condition
$q^{(n-1)/2} > 4W(k)\left(\frac{s-1}{\delta} + 2\right)$
where
$\delta = 1 - \sum_{i=1}^{s} \frac{1}{p_i}$
and the sieving primes are chosen so that δ **is positive**.

The cases $n = 4, 3, a \neq 0$

$n = 4$

Use (1) to resolve the situation when $\omega(q^4 - 1) \geq 24$.

Then use the prime sieve:

- generally (without knowing the factorisation of $q^4 - 1$) – leaves 114 cases $3 \leq q \leq 4217$ undecided.
- specifically (using the factorisation) – leaves $q = 3, 5, 7, 11, 13$.

$n = 3$ (necessarily with $q \equiv 1 \mod 4$)

The character sum $|S_u(\eta_d)| \leq \sqrt{2}q^{n/2}$, on average; thus (1) is improved to

$$q^{(n-1)/2} > 2\sqrt{2}W(q^n - 1).$$

Use the prime sieve

- generally – leaves 4459 cases, $3 \leq q \leq 511033$.
- specifically – leaves $q = 5, 9, 13, 25$.

Note. For the case $a = 0$ apply a modified treatment.

The case $n = 2$ and completion

As noted in Lemma 1, the line property implies the non-zero trace property. So, using such theoretical means, when $n = 2$, the trace property holds except possibly for 101 values of q, $3 \leq q \leq 3541$. see later

More generally, after applying all theoretical means, all that are left are 118 possible exceptions with $2 \leq n \leq 6$.

By calculation (5 minutes computer time), the only q^n that do not have the trace property have $q = n = 2$ and $q = 2, 3, 5, 7, 11, 13, 31$ and in these cases the values of the missing trace values are exhibited.

For example, if $q = 31$, there are no 2-primitive elements with traces 0, 11, 20.

Table of Contents

1 Introduction

2 The trace and line properties

3 Old results, mainly on primitive elements

4 New theorem – trace property

5 New theorems – line property

Asymptotic existence theorem

Reminder.

Let $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma)$ and $\beta \in \mathbb{F}_{q^n}^*$.
A line is a set of the form $L_{\beta,\gamma} = \{\beta(\gamma + b) : b \in \mathbb{F}_q\}$.
$\mathbb{F}_{q^n}$ has the line property if every line contains an r-primitive element.

Theorem 6 (SDC, GK 2020 [9])

Fix integers n, r. There exists $L_r(n)$ such that, whenever $q > L_r(n)$ for any prime power q (with $r|q^n - 1$), then $\mathbb{F}_{q^n}$ has the line property for r-primitive elements.

- Proof depends on the factorisation of $q^n - 1$ and r. Thus if $p^{a_p}|(q^n - 1)$ and $p^{b_p}|r$ (exactly), does
  1. $a_p = b_p > 0$,
  2. $a_p > b_p > 0$,
  3. $a_p > b_p = 0$?
- Primes of type (2) are the most awkward!
- Uses Katz' theorem [10]: $|\sum_{x\in\mathbb{F}_q} \eta(\gamma + x)| \leq (n-1)\sqrt{q}$.

Existence theorem for **2-primitive** elements in $\mathbb{F}_{q^2}$

Theorem 7 (SDC, GK 2020 [11])

Suppose q is an odd prime power. Then $\mathbb{F}_{q^2}$ has the line property for 2-primitive elements, except when $q = 3, 5, 7, 9, 11, 13, 31, 41$.

Idea of proof

Let Q be the odd part of q^2-1.

$\alpha \in \mathbb{F}_{q^2}$ is 2-primitive if it is Q-free and a square but not a 4th power.

Given a line $\{\beta(\gamma+b) : b \in \mathbb{F}_q\} \in \mathbb{F}_{q^2}$, let N be the number of 2-primitive α on the line. Then

$$N = \frac{\theta(Q)}{4} \sum_{d|Q} \frac{\mu(d)}{\phi(d)} \sum_{(\eta_d)} \{T(\eta_d\eta_1) + T(\eta_d\eta_2) - T(\eta_d\eta_4) - T(\eta_d\eta_4')\}.$$

Here η_1 is the principal character, η_2 is the quadratic character, η_4, η_4' are the two characters of order 4 and

$$T(\eta) = \sum_{x\in\mathbb{F}_q} \eta(\beta(\gamma+x))$$

.

If $d>1$, $|T(\eta_d\eta_i)| \leq \sqrt{q}$. elementary!

Hence N is positive if

$$\sqrt{q} > 4W(Q) = 2W(q^2-1)$$ (actual condition is stronger)

Numerical aspects

N is positive if
$$\sqrt{q} > 2W(q^2-1) \qquad (2)$$

- using (2) directly: succesful for $q > 10^6$ (approx);
  fails for 2425 smaller prime powers q.
- using sieving version of (2) and algorithm:
  fails for 101 prime powers, largest being 3541.
  (the same set as for Theorem 5)
- direct computer verification by computer for these 101 prime powers.
  - **Key feature.** No need to check all lines $L_{\beta,\gamma}, \beta \neq 0 \in \mathbb{F}_{q^2}$:
    suffices to take $\beta = \alpha$ or $\zeta\alpha$, where $\alpha^{q+1} = 1$ and ζ is a primitive fth root of unity, where f is the power of 2 in $q^2 - 1$ ($q+1$ values of β in all).
- 3541 alone took 45 days of computer time.

Open questions

1. Which cubic extensions $\mathbb{F}_{q^3}$ have the line property for 2-primitive elements?
2. What extensions $\mathbb{F}_{q^n}$ have the trace property for 3-primitive elements?
   - In particular, which quadratic extensions $\mathbb{F}_{q^2}$?
   - Which cubic extensions $\mathbb{F}_{q^3}$?
3. Which quadratic extensions have the line property for 3-primitive elements?
4. If $q > L_r(n)$ then $\mathbb{F}_{q^n}$ has the line property for r-primitive elements. We have

$$L_1(2) = 1; \quad L_1(3) = 37; \quad L_1(4) \leq 102829[5]; \quad L_2(2) = 41.$$

Can we add any exact values or bounds to this list?

References

[1] S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discrete Math.*, **83** (1990), 1–7.

[2] S. D. Cohen and M. Prešern, Primitive finite field elements with prescribed trace, *Southeast Asian Bull. Math.*, **27** (2005), 283–300.

[3] S. D. Cohen, Primitive roots in the quadratic extension of a finite field, *J. London Math. Soc.* (2), **27** (1983), 221–228.

[4] S. D. Cohen, Primitive elements on lines in extensions of finite field, Finite fields: theory and applications, *Contemp. Math.* **518**, (2010), 113–127.

[5] G. Bailey, S. D. Cohen, N. Sutherland, T. Trudgian, Existence results for primitive elements in cubic and quartic extensions of a finite field, *Math. Comp.* **88**, (2019), 931–947.

[6] F. Ozbudak, Elements of prescribed order, prescribed traces and systems of rational functions over finite fields, em Des. Codes Cryptogr., **34**, (2005)), 331–340.

[7] S. D. Cohen, Finite field elements with specified order and traces, *Des. Codes Cryptogr.*, **36**, (2005)), 35–54.

[8] S. D. Cohen, G. Kapetanakis, The trace of 2-primitive elements of finite fields, *Acata Arith.*, **192**, (2020) 397–419.

[9] S. D. Cohen, G. Kapetanakis, Finite field extensions with the line or translate property for r-primitive elements, *J. Aust. Math. Soc.*, published online 2020, 7 pages.

[10] N. M. Katz An estimate for character sums, *J. Amer. Math. Soc.*, **2**, (1989), 197–200.

[11] S. D. Cohen, G. Kapetanakis, The translate and line properties for 2-primitive elements in quadratic extensions, *Intern. J. Number Th.*, **16** (2020), 2027–2040.