J. Aust. Math. Soc. **111** (2021), 313–319
doi:10.1017/S1446788720000099

FINITE FIELD EXTENSIONS WITH THE LINE OR TRANSLATE PROPERTY FOR r-PRIMITIVE ELEMENTS

STEPHEN D. COHEN and GIORGOS KAPETANAKIS

(Received 6 July 2019; accepted 7 January 2020; first published online 2 March 2020)

Communicated by I. Shparlinski

Abstract

Let $r, n > 1$ be integers and q be any prime power q such that $r \mid q^n - 1$. We say that the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the line property for r-primitive elements property if, for every $\alpha, \theta \in \mathbb{F}_{q^n}^*$ such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$, there exists some $x \in \mathbb{F}_q$ such that $\alpha(\theta + x)$ has multiplicative order $(q^n - 1)/r$. We prove that, for sufficiently large prime powers q, $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the line property for r-primitive elements. We also discuss the (weaker) translate property for extensions.

2010 *Mathematics subject classification*: primary 11T30; secondary 11T06.

Keywords and phrases: primitive element, high-order element, line property, translate property.

1. Introduction

Let q be a prime power and $n \geq 2$ an integer. We denote by $\mathbb{F}_q$ the finite field of q elements and by $\mathbb{F}_{q^n}$ its extension of degree n. It is well known that the multiplicative group $\mathbb{F}_{q^n}^*$ is cyclic; its generators are called *primitive elements*. The theoretical importance of primitive elements is complemented by their numerous applications in practical areas such as cryptography.

In addition to their theoretical interest, elements of $\mathbb{F}_{q^n}^*$ that have high order, without necessarily being primitive, are of great practical interest because in several applications they may replace primitive elements. Accordingly, recently researchers have worked on the effective construction of such high-order elements [9, 14, 15], since that of primitive elements themselves remains an open problem.

With that in mind, we call an element of order $(q^n - 1)/r$, where $r \mid q^n - 1$, *r-primitive*, that is, the primitive elements are exactly the 1-primitive elements. In this line of work, the existence of 2-primitive elements that also possess other desirable properties has recently been considered [7, 12].

The first author is Emeritus Professor of Number Theory, University of Glasgow.

We call some $\theta \in \mathbb{F}_{q^n}$ a *generator* of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ if $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$ and, if θ is a generator of $\mathbb{F}_{q^n}/\mathbb{F}_q$, we call the set

$$\mathcal{T}_\theta := \{\theta + x \,:\, x \in \mathbb{F}_q\}$$

the *set of translates* of θ over $\mathbb{F}_q$ and every element of this set a *translate* of θ over $\mathbb{F}_q$. We say that an extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the *translate property for r-primitive elements*, if every set of translates contains an r-primitive element. In particular, for $r = 1$ we simply call it the *translate property*. A classical result in the study of primitive elements is as follows.

Theorem 1.1 (Carlitz and Davenport). *Let n be an integer. There exists some $T_1(n)$ such that, for every prime power $q > T_1(n)$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the translate property.*

Theorem 1.1 was first proved by Davenport [8], for prime q, while Carlitz [3] extended it to the stated form. Interest in this problem has been renewed by recent applications of the translate property in semifield primitivity [11, 16, 17].

Let θ be a generator of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and take some $\alpha \in \mathbb{F}_{q^n}^*$. We call the set

$$\mathcal{L}_{\alpha,\theta} := \{\alpha(\theta + x) \,:\, x \in \mathbb{F}_q\}$$

the *line* of α and θ over $\mathbb{F}_q$. An extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is said to possess the *line property for r-primitive elements* if every line of this extension contains an r-primitive element. When $r = 1$, we refer to this property as the *line property*. A natural generalization of Theorem 1.1 is as follows [6, Corollary 2.4].

Theorem 1.2 (Cohen). *Let n be an integer. There exists some $L_1(n)$ such that, for every prime power $q > L_1(n)$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the line property.*

It is clear that all the sets of translates are actually lines (where $\alpha = 1$), that is, the line property implies the translate property. Thus, $L_1(n) \geq T_1(n)$. In this work, we extend Theorems 1.1 and 1.2 to r-primitive elements, by proving the following.

Theorem 1.3. *Let n and r be integers. There exists some $L_r(n)$ such that, for every prime power $q > L_r(n)$ with the property $r \mid q^n - 1$, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ possesses the line property for r-primitive elements. If we confine ourselves to the translate property for r-primitive elements, the same is true for some $T_r(n) \leq L_r(n)$.*

A natural, but apparently challenging, related question is to identify the exact value of the numbers $T_1(n)$ and $L_1(n)$ for given n. Indeed, only a handful of these are known. In particular, the first author, in [4], proved that $T_1(2) = L_1(2) = 1$ and, in [5], that $T_1(3) = 37$. Bailey *et al.* [2] proved that $L_1(3) = 37$ and estimated $T_1(4) \leq L_1(4) \leq 102\,829$. By means of more specialized theoretical and computational techniques, the authors have now proved that $T_2(2) = L_2(2) = 41$. The details will be given in a further paper.

https://doi.org/10.1017/S1446788720000099 Published online by Cambridge University Press

2. Preliminaries

We begin by introducing the notion of freeness. Let $m \mid q^n - 1$. An element $\xi \in \mathbb{F}_{q^n}^*$ is *m-free* if $\xi = \zeta^d$ for some $d \mid m$ and $\zeta \in \mathbb{F}_{q^n}^*$ implies $d = 1$. It is clear that primitive elements are exactly those that are q_0-free, where q_0 is the square-free part of $q^n - 1$. It is also evident that there is some relation between m-freeness and multiplicative order.

Lemma 2.1 [10, Proposition 5.3]. *If $m \mid q^n - 1$ then $\xi \in \mathbb{F}_{q^n}^*$ is m-free if and only if* $\gcd(m, (q^n - 1)/\mathrm{ord}\xi) = 1$.

Throughout this work, a *character* is a multiplicative character of $\mathbb{F}_{q^n}^*$, while we denote by χ_0 the trivial multiplicative character. Vinogradov's formula yields an expression for the characteristic function of m-free elements in terms of multiplicative characters, namely,

$$\Omega_m(x) := \theta(m) \sum_{d \mid m} \frac{\mu(d)}{\phi(d)} \sum_{\mathrm{ord}\chi = d} \chi(x), \tag{2-1}$$

where μ stands for the Möbius function, ϕ for the Euler function, $\theta(m) := \phi(m)/m$ and the inner sum sums through multiplicative characters of order d. Furthermore, a direct consequence of the orthogonality relations is that the characteristic function for the elements of $\mathbb{F}_{q^n}^*$ that are k th powers, where $k \mid q^n - 1$, can be written as

$$w_k(x) := \frac{1}{k} \sum_{d \mid k} \sum_{\mathrm{ord}\chi = d} \chi(x). \tag{2-2}$$

We will use character sums to establish our results. The following estimate is a direct consequence of the main result of [13] and, notably, is one of the few nontrivial character sum estimates not relying on Weil's results [18].

Proposition 2.2 (Katz). *Let $\theta \in \mathbb{F}_{q^n}$ be such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$ and χ is a nontrivial character. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(\theta + x) \right| \leq (n - 1)\sqrt{q}.$$

Let $d(R)$ be the number of divisors of R. The following result provides an asymptotic estimate for this function.

Proposition 2.3 [1, page 296]. *For every $\delta > 0$, $d(n) = o(n^\delta)$, where o signifies the little-o notation.*

3. Characterization of r-primitive elements

From now on, fix the positive integers r and n and let q be some prime power such that $r \mid q^n - 1$. Let Γ be the characteristic function for r-primitive elements of $\mathbb{F}_{q^n}$, that is, for $x \in \mathbb{F}_{q^n}^*$,

$$\Gamma(x) := \begin{cases} 1 & x \text{ is } r\text{-primitive}, \\ 0 & \text{otherwise}. \end{cases}$$

The aim of this section is to express $\Gamma(x)$ in a convenient way, using characters.

https://doi.org/10.1017/S1446788720000099 Published online by Cambridge University Press

Let $\mathcal{P}$ be the set of distinct primes dividing $q^n - 1$. It follows that $q^n - 1 = \prod_{p\in\mathcal{P}} p^{a_p}$, where $a_p \geq 1$ for all $p \in \mathcal{P}$. Additionally, we have that $r = \prod_{p\in\mathcal{P}} p^{b_p}$, where, for every $p \in \mathcal{P}$, $0 \leq b_p \leq a_p$.

We partition $\mathcal{P}$ as follows:

$$\mathcal{P}_s := \{p \in \mathcal{P} : a_p = b_p > 0\},$$
$$\mathcal{P}_t := \{p \in \mathcal{P} : a_p > b_p > 0\},$$
$$\mathcal{P}_u := \{p \in \mathcal{P} : a_p > b_p = 0\}.$$

It is clear that the above sets are pairwise disjoint and that $\mathcal{P}_s \cup \mathcal{P}_t \cup \mathcal{P}_u = \mathcal{P}$. Further, set

$$s := \prod_{p\in\mathcal{P}_s} p^{b_p}, \quad t := \prod_{p\in\mathcal{P}_t} p^{b_p} \quad \text{and} \quad u := \prod_{p\in\mathcal{P}_u} p.$$

It is straightforward to check that $r = st$ and that u is the radical of the part of $q^n - 1$ that is relatively prime with r.

Lemma 2.1 implies that the set of u-free elements, contains all the σ-primitive elements, where

$$\sigma = \prod_{p\in\mathcal{P}_s\cup\mathcal{P}_t} p^{\sigma_p}, \tag{3-1}$$

for some $0 \leq \sigma_p \leq a_p$. In addition, the u-free elements that are rth powers are the σ-primitive elements with σ as in (3-1) with $b_p \leq \sigma_p \leq a_p$. Next, let $\mathcal{P}_t = \{p_1, \ldots, p_k\}$ and, for $i = 1, \ldots, k$, set $e_i := p_i^{b_{p_i}}$ and $f_i := p_i^{b_{p_i}+1}$. Note that $b_{p_i} + 1 \leq a_{p_i}$. Now, from the set of u-free elements that are also rth powers, exclude those that are not f_ith powers for every $i = 1, \ldots, k$. We are left with exactly the σ-primitive elements, where σ is as in (3-1), with

$$\begin{cases} b_p \leq \sigma_p \leq a_p = b_p & \text{if } p \in \mathcal{P}_s, \\ b_p \leq \sigma_p < b_p + 1 \leq a_p & \text{if } p \in \mathcal{P}_t. \end{cases}$$

In particular, in any case $\sigma_p = b_p$, that is, $\sigma = r$.

In other words, with the notation of Section 2, the characteristic function for r-primitive elements of $\mathbb{F}_{q^n}^*$ can be expressed as

$$\begin{aligned} \Gamma(x) &= \Omega_u(x) w_r(x) \prod_{i=1}^{k} (1 - w_{f_i}(x)) \\ &= \Omega_u(x) w_s(x) \prod_{i=1}^{k} w_{e_i}(x)(1 - w_{f_i}(x)), \end{aligned} \tag{3-2}$$

where $x \in \mathbb{F}_{q^n}^*$. Moreover, for every $i = 1, \ldots, k$, notice that since $e_i \mid f_i$, we have that an f_ith power is also an e_ith power, that is, for $x \in \mathbb{F}_{q^n}^*$, $w_{e_i}(x) w_{f_i}(x) = w_{f_i}(x)$. Thus (3-2) yields

$$\Gamma(x) = \Omega_u(x) w_s(x) \prod_{i=1}^{k} (w_{e_i}(x) - w_{f_i}(x)). \tag{3-3}$$

https://doi.org/10.1017/S1446788720000099 Published online by Cambridge University Press

Next, recall that, for $i = 1, \dots, k$, $e_i = p_i^{b_{p_i}}$ and $f_i = p_i^{b_{p_i}+1} = e_i p_i$. It follows that, for every $x \in \mathbb{F}_{q^n}^*$,

$$\begin{aligned} w_{e_i}(x) - w_{f_i}(x) &= \frac{1}{e_i} \sum_{d \mid e_i} \sum_{\operatorname{ord}\chi = d} \chi(x) - \frac{1}{f_i} \sum_{d \mid f_i} \sum_{\operatorname{ord}\chi = d} \chi(x) \\ &= \frac{1}{e_i} \sum_{d \mid f_i} \sum_{\operatorname{ord}\chi = d} \ell_{i,d} \chi(x), \end{aligned}$$

where, for $d \mid f_i$,

$$\ell_{i,d} := \begin{cases} 1 - 1/p_i & \text{if } d \neq f_i, \\ -1/p_i & \text{if } d = f_i. \end{cases}$$

Finally, we insert the above and the expressions (2-1) and (2-2) into (3-3), and obtain

$$\Gamma(x) = \frac{\theta(u)}{r} \sum_{d_1 \mid u} \sum_{d_2 \mid s} \sum_{\delta_1 \mid f_1} \cdots \sum_{\delta_\lambda \mid f_k} \frac{\mu(d_1)}{\phi(d_1)} \ell_{1,\delta_1} \cdots \ell_{k,\delta_k} \sum_{\substack{\operatorname{ord}\chi_j = d_j \\ \operatorname{ord}\psi_i = \delta_i}} (\chi_1 \chi_2 \psi_1 \cdots \psi_k)(x), \tag{3-4}$$

where $x \in \mathbb{F}_{q^n}^*$ and $(\chi_1 \chi_2 \psi_1 \cdots \psi_\lambda)$ stands for the product of the corresponding characters, itself a character.

4. Proof of Theorem 1.3

Fix some $\alpha, \theta \in \mathbb{F}_{q^n}^*$ such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$. Let $\mathcal{N}(\theta, \alpha)$ be the number of r-primitive elements of the form $\alpha(\theta + x)$, where $x \in \mathbb{F}_q$. It suffices to show that

$$\mathcal{N}(\theta, \alpha) = \sum_{x \in \mathbb{F}_q} \Gamma(\alpha(\theta + x)) \neq 0.$$

With (3-4) in mind, we have that

$$\frac{\mathcal{N}(\theta, \alpha)}{\theta(u)} = \frac{1}{r} \sum_{\substack{d_1 \mid u,\, d_2 \mid s, \\ \delta_1 \mid f_1, \dots, \delta_k \mid f_k}} \frac{\mu(d_1)}{\phi(d_1)} \ell_{1,\delta_1} \cdots \ell_{k,\delta_k} \sum_{\substack{\operatorname{ord}\chi_j = d_j \\ \operatorname{ord}\psi_i = \delta_i}} \mathcal{X}_{\alpha,\theta}(\chi_1, \chi_2, \psi_1, \dots, \psi_k), \tag{4-1}$$

where

$$\mathcal{X}_{\alpha,\theta}(\chi_1, \chi_2, \psi_1, \dots, \psi_k) := \sum_{x \in \mathbb{F}_q} (\chi_1 \chi_2 \psi_1 \cdots \psi_k)(\alpha(\theta + x)).$$

In addition, notice that the orders of all the factors of the character product $(\chi_1 \chi_2 \psi_1 \cdots \psi_k)$ are relatively prime. Hence the product itself is trivial if and only if all its factors are trivial. With this in mind, Proposition 2.2 implies that, unless all the characters $\chi_1, \chi_2, \psi_1, \dots, \psi_k$ are trivial,

$$|\mathcal{X}_{\alpha,\theta}(\chi_1, \chi_2, \psi_1, \dots, \psi_k)| \leq \sqrt{q},$$

while it is clear that

$$\mathcal{X}_{\alpha,\theta}(\chi_0, \chi_0, \chi_0, \dots, \chi_0) = q.$$

https://doi.org/10.1017/S1446788720000099 Published online by Cambridge University Press

In (4-1), we separate the term that corresponds to $d_1 = d_2 = \delta_1 = \cdots = \delta_k = 1$ and, with the above in mind, we obtain

$$\left|\frac{\mathcal{N}(\theta,\alpha)}{\theta(u)} - \frac{q}{r}\cdot \ell_{1,1}\cdots\ell_{k,1}\right| \le \frac{1}{r} \sum_{\substack{d_1\mid u,\, d_2\mid s,\\ \delta_1\mid f_1,\ldots,\delta_k\mid f_k\\ \text{not all equal to 1}}} \frac{|\ell_{1,\delta_1}\cdots\ell_{k,\delta_k}|}{\phi(d_1)} \sum_{\substack{\operatorname{ord}\chi_j = d_j\\ \operatorname{ord}\psi_i=\delta_i}} \sqrt{q}. \tag{4-2}$$

Notice that, for all $1 \le i \le k$, $|\ell_{i,\delta_i}| \le \ell_{i,1}$. It follows from (4-2) that $\mathcal{N}(\theta,\alpha) \ne 0$ if

$$q > \sum_{\substack{d_1\mid u,\, d_2\mid s,\\ \delta_1\mid f_1,\ldots,\delta_k\mid f_k}} \frac{1}{\phi(d_1)} \sum_{\substack{\operatorname{ord}\chi_j = d_j\\ \operatorname{ord}\psi_i=\delta_i}} \sqrt{q}.$$

Furthermore, it is well known that, for every $d \mid q^n - 1$, there exist exactly $\phi(d)$ characters of order d. Hence the latter condition can be also written as

$$q > sf_1\cdots f_k \cdot d(u)\cdot \sqrt{q}, \tag{4-3}$$

where we recall that $d(m)$ stands for the number of divisors of $m \in \mathbb{Z}$. Now observe that $u \mid q^n - 1$, as a result of which Proposition 2.3 implies that

$$d(u) \le d(q^n - 1) = o(q^{1/4}).$$

Further, observe that

$$sf_1\cdots f_k \le A_r := \prod_{p\in\mathcal{P}_s\cup\mathcal{P}_t} p_i^{b_i+1},$$

where the left-hand side of the above inequality depends solely on r. It follows that, for q large enough, (4-3) holds. Hence $\mathcal{N}(\theta,\alpha) \ne 0$.

The proof of the first statement of Theorem 1.3 is now complete, while the second statement (about $T_r(n)$) follows immediately from the fact that all the sets of translates of an extension are simultaneously lines of this extension.

Remark 4.1. The reader will note that, in the statement of Theorem 1.3, n and r are fixed integers and q is any (sufficiently large) prime power such that $r \mid q^n - 1$. We are indebted to the referee for the observation that it would be possible to allow the integer r with this property to vary as a (suitably small) function of q. To avoid unnecessary technical complication we have refrained from a precise formulation of the ensuing result at this juncture.

Acknowledgement

We are grateful to Michel Lavrauw whose suggested terminology we have adopted.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory* (Springer, New York, 1976).
[2] G. Bailey, S. D. Cohen, N. Sutherland and T. Trudgian, 'Existence results for primitive elements in cubic and quartic extensions of a finite field', *Math. Comp.* **88**(316) (2019), 931–947.

https://doi.org/10.1017/S1446788720000099 Published online by Cambridge University Press

[3] L. Carlitz, 'Distribution of primitive roots in a finite field', *Quart. J. Math. Oxford Ser. (2)* **4**(1) (1953), 4–10.
[4] S. D. Cohen, 'Primitive roots in the quadratic extension of a finite field', *J. Lond. Math. Soc. (2)* **27**(2) (1983), 221–228.
[5] S. D. Cohen, 'Generators of the cubic extension of a finite field', *J. Comb. Number Theory* **1**(3) (2009), 189–202.
[6] S. D. Cohen, 'Primitive elements on lines in extensions of finite fields', in: *Finite Fields: Theory and Applications*, Contemporary Mathematics, 518 (eds. G. McGuire, G. L. Mullen, D. Panario and I. E. Shparlinski) (American Mathematical Society, Province, RI, 2010), 113–127.
[7] S. D. Cohen and G. Kapetanakis, 'The trace of 2-primitive elements of finite fields', *Acta Arith.* **192**(4) (2020), 397–419.
[8] H. Davenport, 'On primitive roots in finite fields', *Quart. J. Math. Oxford* **8**(1) (1937), 308–312.
[9] S. Gao, 'Elements of provable high orders in finite fields', *Proc. Amer. Math. Soc.* **127**(6) (1999), 1615–1623.
[10] S. Huczynska, G. L. Mullen, D. Panario and D. Thomson, 'Existence and properties of k-normal elements over finite fields', *Finite Fields Appl.* **24** (2013), 170–183.
[11] G. Kapetanakis and M. Lavrauw, 'A geometric condition for primitive semifields', 2019, in preparation.
[12] G. Kapetanakis and L. Reis, 'Variations of the primitive normal basis theorem', *Des. Codes Cryptogr.* **87**(7) (2019), 1459–1480.
[13] N. M. Katz, 'An estimate for character sums', *J. Amer. Math. Soc.* **2**(2) (1989), 197–200.
[14] F. E. B. Martínez and L. Reis, 'Elements of high order in Artin-Schreier extensions of finite fields $\mathbb{F}_q$', *Finite Fields Appl.* **41** (2016), 24–33.
[15] R. Popovych, 'Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$', *Finite Fields Appl.* **19**(1) (2013), 92–96.
[16] I. F. Rúa, 'On the primitivity of four-dimensional finite semifields', *Finite Fields Appl.* **33** (2015), 212–229.
[17] I. F. Rúa, 'Primitive semifields of order 2^{4e}', *Des. Codes Cryptogr.* **83**(2) (2017), 345–356.
[18] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent* (Hermann, Paris, 1948).

STEPHEN D. COHEN, 6 Bracken Road,
Portlethen, Aberdeen AB12 4TA, UK
e-mail: Stephen.Cohen@glasgow.ac.uk

GIORGOS KAPETANAKIS, Department of Mathematics
and Applied Mathematics, University of Crete,
Voutes Campus, 70013 Heraklion, Greece
e-mail: gnkapet@gmail.com

https://doi.org/10.1017/S1446788720000099 Published online by Cambridge University Press