The line and the translate properties for r-primitive elements

Giorgos Kapetanakis
(Joint work with Stephen D. Cohen)

9th Greek Algebra and Number Theory Conference
Thessaloniki, 12–13 May 2023

University of Thessaly

Motivation

Primitivity

- Let $\mathbf{F}_q$ be the finite field of q elements and $\mathbf{F}_{q^n}$ its extension of degree n.
- The generators of $\mathbf{F}_{q^n}^*$ are called primitive elements.
- Primitive elements are important for both theoretical and practical reasons.

r-primitivity

- High-order elements of $\mathbf{F}_{q^n}^*$, are also important, as in several applications they may replace primitive elements.
- The construction of such elements has been studied (Gao 1999, Martínez-Reis 2016, Popovych 2013), since that of primitive elements remains an open problem.
- An element of order $\frac{q^n-1}{r}$ is called r-primitive.
- The existence of 2-primitive elements that also possess other desirable properties has been considered (Cohen-K. 2019, K.-Reis 2018).

The translate property

- Some $\theta \in \mathbf{F}_{q^n}$ is a generator of $\mathbf{F}_{q^n}/\mathbf{F}_q$ if $\mathbf{F}_{q^n} = \mathbf{F}_q(\theta)$.
- If θ is a generator of $\mathbf{F}_{q^n}/\mathbf{F}_q$, the set

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

  the set of translates of θ over $\mathbf{F}_q$. Every element of this set a translate of θ over $\mathbf{F}_q$.
- The extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ 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.

The Carlitz-Davenport theorem

A classical result in the study of primitive elements is the following.

Theorem (Carlitz-Davenport)

There exist some $T_1(n)$ such that for every $q > T_1(n)$, the extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ possesses the translate property.

- This first proved by Davenport (1937), for prime q, while Carlitz (1953) extended it as above.
- Interest in this problem was renewed by recent applications of the translate property in semifield primitivity (Rúa 2015, Rúa 2017).

The line property

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

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

  the line of α and θ over $\mathbf{F}_q$.
- An extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ possesses 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 as the line property.
- It is clear that the line property implies the translate property, i.e., take $\alpha = 1$.

Cohen's theorem

A natural generalization of the Carlitz-Davenport theorem is the following:

Theorem (Cohen)

There exist some $L_1(n)$ such that for $q > L_1(n)$, the extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ possesses the line property.

- Proven by Cohen (2010).
- Clearly, $L_1(n) \geq T_1(n)$.

Explicit results

A handful of values of $T_1(n)$ are known as follows.

- (Cohen 1983): $T_1(2) = L_1(2) = 1$.
- (Cohen 2009): $T_1(3) = 37$.
- (Cohen 2010): $T_1(4), L_1(4) < 25944$ and conjectured that $T_1(4), L_1(4) < 64$ but this work contains errors.
- (Bailey-Cohen-Sutherland-Trudgian 2019): $L_1(3) = 37$ and $73 \leq T_1(4) \leq L_1(4) \leq 102829$.

Our contribution

In this talk, we will outline how

1. we extended the Carlitz-Davenport and Cohen theorems to r-primitive elements and
2. how we obtained explicit results in the case $r = n = 2$, that is, how we calculated $T_2(2)$ and $L_2(2)$.

These works can be found in the following references:

S.D. Cohen and G. Kapetanakis.
Finite field extensions with the line or translate property for r-primitive elements.
Journal of the Australian Mathematical Society, 111(3):313–319, 2021.

S.D. Cohen and G. Kapetanakis.
The translate and line properties for 2-primitive elements in quadratic extensions.
International Journal of Number Theory, 16(9):2029–2040, 2020.

Part I: Asymptotic results

Preliminaries - Freeness

- Let $m \mid q^n - 1$, an element $\xi \in \mathbf{F}_{q^n}^*$ is m-free if $\xi = \zeta^d$ for some $d \mid m$ and $\zeta \in \mathbf{F}_{q^n}^*$ implies $d = 1$.
- Primitive elements are exactly those that are q_0-free, where q_0 is the square-free part of $q^n - 1$.
- The following lemma shows the relation between m-freeness and multiplicative order.

Lemma (Huczynska-Mullen-Panario-Thomson, 2013)

If $m \mid q^n - 1$ then $\xi \in \mathbf{F}_{q^n}^*$ is m-free if and only if $\gcd\left(m, \frac{q^n-1}{\operatorname{ord}\xi}\right) = 1$.

Preliminaries - characteristic functions

Vinogradov's formula yields an expression for the characteristic function of m-free elements in terms of multiplicative characters:

$$\Omega_m(x) := \theta(m) \sum_{d|m} \frac{\mu(d)}{\varphi(d)} \sum_{\text{ord}\,\chi = d} \chi(x),$$

where μ is the Möbius function, φ for the Euler function, $\theta(m) := \varphi(m)/m$ and the inner sum suns through multiplicative characters of order d.

The characteristic function for the elements of $\mathbf{F}_{q^n}^*$ that are k-th powers is

$$w_k(x) := \frac{1}{k} \sum_{d|k} \sum_{\text{ord}\,\chi = d} \chi(x).$$

Proposition (Katz, 1989)

Let θ be a generator of $\mathbf{F}_{q^n}/\mathbf{F}_q$ and $\chi \neq \chi_0$ a character. Then

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

Proposition

For every $\delta > 0$, $d(n) = o(n^{\delta})$, where $d(n)$ is the number of divisors of n and o signifies the little-o notation.

Characterization of r-primtive elements

Fix r, n and q, such that $r \mid q^n - 1$. We will express $\Gamma(x)$, the characteristic function for r-primitive elements of $\mathbf{F}_{q^n}$ in a convenient way, using characters.

Let $\mathcal{P}$ be the set of primes dividing $q^n - 1$, i.e., $q^n - 1 = \prod_{p \in \mathcal{P}} p^{a_p}$. Assume $r = \prod_{p \in \mathcal{P}} p^{b_p}$. For every $p \in \mathcal{P}$, $0 \le b_p \le a_p$.

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

$$\begin{aligned}
\mathcal{P}_s &:= \{p \in \mathcal{P} \,:\, a_p = b_p > 0\}, \\
\mathcal{P}_t &:= \{p \in \mathcal{P} \,:\, a_p > b_p > 0\} = \{p_1, \ldots, p_k\}, \\
\mathcal{P}_u &:= \{p \in \mathcal{P} \,:\, a_p > b_p = 0\}.
\end{aligned}$$

Characterization of r-primitive elements

Set

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

- The set of u-free elements, contains all the σ-primitive elements, where
$$\sigma = \prod_{p \in \mathcal{P}_s \cup \mathcal{P}_t} p^{\sigma_p},$$
for some $0 \leq \sigma_p \leq a_p$.
- For $i = 1, \ldots, k$ set $e_i := p_i^{b_{p_i}}$ and $f_i := p_i^{b_{p_i}+1}$.
- From the set of u-free elements, that are also r-th powers, exclude those that are not f_i-th powers for every i.
- We are left with the r-primitive elements.

Characterization of r-primitive elements

Thus, the characteristic function for r-primitive elements of $x \in \mathbf{F}_{q^n}^*$ can be expressed as

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

Further,

$$w_{e_i}(x) - w_{f_i}(x) = \frac{1}{e_i}\sum_{d|e_i}\sum_{\operatorname{ord}\chi=d}\chi(x) - \frac{1}{f_i}\sum_{d|f_i}\sum_{\operatorname{ord}\chi=d}\chi(x)$$
$$= \frac{1}{e_i}\sum_{d|f_i}\sum_{\operatorname{ord}\chi=d}\ell_{i,d}\chi(x),$$

where, for $d \mid f_i$,

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

Characterization of r-primitive elements

Putting everything together, we obtain

$$\Gamma(x) = \frac{\theta(u)}{r} \sum_{\substack{d_1|u, d_2|s \\ \delta_1|f_1,\dots,\delta_k|f_k}} \frac{\mu(d_1)}{\varphi(d_1)} \ell_{1,\delta_1} \cdots \ell_{k,\delta_k} \sum_{\substack{\mathrm{ord}\,\chi_j = d_j \\ \mathrm{ord}\,\psi_i = \delta_i}} (\chi_1 \chi_2 \psi_1 \cdots \psi_k)(x),$$

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

Main result

Let $\mathcal{N}(\theta, \alpha)$ be the number of r-primitive elements of the form $\alpha(\theta + x)$, where $x \in \mathbf{F}_q$. It suffices to show that

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

We have that

$$\frac{\mathcal{N}(\theta, \alpha)}{\theta(u)} = \frac{1}{r} \sum_{\substack{d_1 | u,\, d_2 | s, \\ \delta_1 | f_1, \ldots, \delta_k | f_k}} \frac{\mu(d_1)}{\varphi(d_1)} \ell_{1,\delta_1} \cdots \ell_{k,\delta_k} \sum_{\substack{\text{ord } \chi_j = d_j \\ \text{ord } \psi_i = \delta_i}} \mathcal{X}_{\alpha,\theta}(\chi_1, \chi_2, \psi_1, \ldots, \psi_k),$$

where

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

Main result

- 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.
- Hence, Katz's theorem implies that, unless all the characters χ_1, χ_2, ψ_1,...,ψ_k are trivial,

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

- Clearly,

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

Main result

We separate the term that corresponds to $d_1 = d_2 = \delta_1 = \ldots = \delta_k = 1$ and obtain

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

For all $1 \leq i \leq k$, $|\ell_{i,\delta_i}| \leq \ell_{i,1}$, hence $\mathcal{N}(\theta,\alpha) \neq 0$ if

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

For every $d \mid q^n - 1$, there are exactly $\varphi(d)$ characters of order d. Hence the latter can be rewritten as

$$q > s\cdot f_1\cdots f_k \cdot d(u)\cdot\sqrt{q},$$

Main result

Also $u \mid q^n - 1$, thus $d(u) \leq d(q^n - 1) = o(q^{1/4})$. Further,

$$s \cdot f_1 \cdots f_k \leq A_r := \prod_{p \in \mathcal{P}_s \cup \mathcal{P}_t} p_i^{b_i+1},$$

where the left side of the above inequality depends solely on r. It follows that, for q large enough, the latter condition holds. Hence $\mathcal{N}(\theta, \alpha) \neq 0$. We have proven the following:

Theorem (Cohen-K., 2021)

There exist some $L_r(n)$ such that for every prime power $q > L_r(n)$, with the property $r \mid q^n - 1$, the extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ 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 $T_r(n) \leq L_r(n)$.

Part II: Explicit results

First results

- Since $2 \mid q^2 - 1$, q is odd and $4 \mid q^2 - 1$.
- Thus, following the previous notation, $s = 1$, $t = 2$ and u is the square-free part of the odd part of $q^2 - 1$.
- Set $W(q^2 - 1) = 2^{t(q^2-1)}$, where $t(R)$ stands for the number of prime divisors of R. Clearly, $W(q^2 - 1) = 2d(u)$.
- Hence a sufficient condition for $\mathbf{F}_{q^2}/\mathbf{F}_q$ to possess the line property is

$$\sqrt{q} \geq 2W(q^2 - 1).$$

- We have that $W(R) \leq d_R R^{1/8}$, where $d_R < 4514.7$.
- We obtain the desired result when

$$q \geq (2 \cdot 4514.7)^4 \simeq 6.65 \cdot 10^{15}.$$

- This implies that the case $t(q^2 - 1) \geq 14$ is settled.

Cohen's evaluation

In the special case $n = 2$, Katz's theorem can be improved as follows

Lemma (Cohen, 2010)

Let θ be a generator of $\mathbf{F}_{q^2}/\mathbf{F}_q$ and $\chi \neq \chi_0$ a character. Set

$$B := \sum_{x \in \mathbf{F}_q} \chi(\theta + x).$$

1. *If* $\operatorname{ord} \chi \nmid q + 1$, *then* $|B| = \sqrt{q}$.
2. *If* $\operatorname{ord} \chi \mid q + 1$, *then* $B = -1$.

Further theoretical reductions

With the above in mind we:

1. Distinguish the cases $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$.
2. Employ the Cohen-Huczynska (2003) sieve.
3. Use an algorithm that settles the case $\alpha \leq t(q^2-1) \leq \beta$ and successfully use it when $(\alpha, \beta) = (11, 13)$ and $(10, 10)$.
4. We are left with the case $t(q^2-1) \leq 9$, i.e., $q \leq (2 \cdot 2^9)^2 = 1048576$.
5. The interval $3 \leq q \leq 1048576$ contains exactly 82247 odd prime powers.
6. We first replace d_{q^2-1} by its exact value and then $W(q^2-1)$ by its exact value we reduce the list to a total of 2425 possible exceptions.

Final theoretical reductions

The sieve reduces that list to a total of 101 possible exceptions as follows:

q	#
3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 79, 81, 83, 89, 97, 101, 103, 109, 113, 121, 125, 127, 131, 137, 139, 149, 151, 157, 169, 173, 181, 191, 197, 199, 211, 229, 239, 241, 269, 281, 307, 311, 331, 337, 349, 361, 373, 379, 389, 409, 419, 421, 461, 463, 509, 521, 529, 569, 571, 601, 617, 631, 659, 661, 701, 761, 769, 841, 859, 881, 911, 1009, 1021, 1231, 1289, 1301, 1331, 1429, 1609, 1741, 1849, 1861, 2029, 2281, 2311, 2729, 3541	101

Direct verification

1. We first verified the translate property for the 101 exceptional prime powers. It turns out that the only genuine exceptions are $q = 5, 7, 11, 13, 31$ and 41. We spent about 2.5 hours of computer time for this.
2. A direct verification of the line property revealed the additional genuine exceptions $q = 3$ and 9.
3. The direct verification of the line property turned out to be exceptionally expensive in terms of computer time. For example, $q = 3541$ required 45 days of computer time, $q = 2729$ required 20 days and $q = 2029$ required 14 days.

Main results

Summing up, we proved the following:

Theorem (Cohen-K., 2020)

For every odd prime power $q \neq 5, 7, 11, 13, 31$ *or* 41 *the extension* $\mathbf{F}_{q^2}/\mathbf{F}_q$ *possesses the translate property for 2-primitive elements. In particular,* $T_2(2) = 41$.

Theorem (Cohen-K., 2020)

For every odd prime power $q \neq 3, 5, 7, 9, 11, 13, 31$ *or* 41 *the extension* $\mathbf{F}_{q^2}/\mathbf{F}_q$ *possesses the line property for 2-primitive elements. In particular,* $L_2(2) = 41$.

Thank You!