

An estimate for incomplete mixed character sums and applications


10th Greek Algebra and Number Theory Conference
May 24, 2025

Giorgos Kapetanakis

Joint work with B.K. Basnet, S. Kala and A.C. Mazumder

 University of Thessaly

 kapetanakis@uth.gr

 <http://gkapet.users.uth.gr/>

Outline

Motivation

An estimate for a mixed incomplete character sum

The weak line property for primitive normal elements

Future work

Primitivity and normality

- Throughout this talk, q is a prime power. We denote by \mathbb{F}_q , the finite field of order q and characteristic p and by \mathbb{F}_{q^m} , the extension field of \mathbb{F}_q of degree m .
- Some $\theta \in \mathbb{F}_{q^m}$ is called a *generator* of $\mathbb{F}_{q^m}/\mathbb{F}_q$, if $\mathbb{F}_{q^m} = \mathbb{F}_q(\theta)$.
- The multiplicative group $\mathbb{F}_{q^m}^*$ is cyclic and a generator of this group is called *primitive*.
- Some $\theta \in \mathbb{F}_{q^m}$ is *normal* over \mathbb{F}_q if the set of its conjugates with respect to \mathbb{F}_q , that is, $\{\theta, \theta^q, \dots, \theta^{q^{m-1}}\}$ forms an \mathbb{F}_q -basis of \mathbb{F}_{q^m} .
- Some $\theta \in \mathbb{F}_{q^m}$ is *primitive normal* if it is both primitive and normal over \mathbb{F}_q .

Translates and lines

- For any generator θ of $\mathbb{F}_{q^m}/\mathbb{F}_q$, the set $\{\theta + x : x \in \mathbb{F}_q\}$ is the *set of translates* of θ over \mathbb{F}_q . We refer to the question of the existence of elements of \mathbb{F}_{q^m} of a certain type in every translate as the *translate problem*. If the answer is positive, the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ possesses the *translate property* (TP) for this type of elements.
- Likewise, for a generator θ of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and some $\alpha \in \mathbb{F}_q^*$, the set $\{\alpha(\theta + x) : x \in \mathbb{F}_q\}$ is the *line* of θ and α over \mathbb{F}_q . In accordance with the previous definitions, we have the *line problem* and the *line property* (LP), respectively.
- If we only consider the case $\alpha \in \mathbb{F}_q^*$, we refer to the *weak line problem* and the *weak line property* (WLP), respectively.
- Clearly, $LP \Rightarrow WLP \Rightarrow TP$.

The Carlitz-Davenport theorem

Theorem (Davenport-Carlitz)

Let $m > 1$ be an integer. There exists some $TP(m)$ such that, if $q > TP(m)$, $\mathbb{F}_{q^m}/\mathbb{F}_q$ possesses the translate property for primitive elements.

- Initially established by Davenport (1937) for q prime and extended by Carlitz (1953) to all prime powers q .
- Both results were obtained using the following.

Lemma (Davenport, 1937)

Let p be a prime, n a positive integer, θ a generator of $\mathbb{F}_{p^n}/\mathbb{F}_p$ and χ a nontrivial multiplicative character of \mathbb{F}_{p^n} . Then

$$\left| \sum_{x \in \mathbb{F}_p} \chi(\theta + x) \right| \ll p^{\left(1 - \frac{1}{2(n+1)}\right)}.$$

Katz's estimate and Cohen's generalization

Theorem (Katz, 1989)

Let χ be any nontrivial multiplicative character of $\mathbb{F}_{q^m}^*$ and θ in \mathbb{F}_{q^m} , a generator $\mathbb{F}_{q^m}/\mathbb{F}_q$. Then

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

- The above does not rely on the Hasse-Weil bound.
- Using this result, Cohen proved the following.

Theorem (Cohen, 2010)

Let $m > 1$ be an integer. There exists some $LP(m)$ such that, if $q > LP(m)$, $\mathbb{F}_{q^m}/\mathbb{F}_q$ possesses the line property for primitive elements.

Yet, another generalization

- Some $b \in \mathbb{F}_{q^m}$ is r -primitive if its multiplicative order is $(q^m - 1)/r$, where necessarily $r \mid q^m - 1$.
- Using Katz's estimate and a novel effective characterization of r -primitive elements, the following was obtained.

Theorem (Cohen-K., 2021)

Let $m > 1$ and r be integers. There exists some $LP_r(m)$ such that, if $q > LP_r(m)$ with the property $r \mid q^m - 1$, $\mathbb{F}_{q^m}/\mathbb{F}_q$ possesses the line property for r -primitive elements. As for the translate property for r -primitive elements, the same is true for some $TP_r(m) \leq LP_r(m)$.

What about similar mixed character sums?

For the *TP* and *LP* for primitive normal elements, we need an estimate for a similar mixed character sum.

Theorem (Perel'muter-Shparlinski, 1990)

Take some prime p , a positive integer n , θ is a generator of the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$, $a \in \mathbb{F}_p$ and χ is a nontrivial multiplicative character of \mathbb{F}_{p^n} . Then

$$\left| \sum_{t \in \mathbb{F}_p} \chi(\theta + t) \exp(2\pi i a t / p) \right| \leq np^{1/2}.$$

- Can the above be generalized to arbitrary finite fields and arbitrary additive characters?
- Can it (after these generalizations) be used to attack the translate, weak line and line problems for primitive normal elements?

Function fields, discrete valuation rings and places

- A field extension F/K is a *function field of one variable over K* , if, for some x transcendental over K , $F/K(x)$ is finite.
- $K(x)/K$ is called *rational* and F/\mathbb{F}_q is called *global*.
- A *discrete valuation ring* of F/K is a ring $K \subsetneq \mathcal{O} \subsetneq F$, such that $a \in \mathcal{O}$ or $a^{-1} \in \mathcal{O}$ for all $a \in F$ and it is a local ring with its (unique) maximal ideal \mathfrak{p} being principal called a *place* of F/K .
- If $\mathfrak{p} = t\mathcal{O}$ is a place of F/K , each $z \in F^*$ has a unique representation of the form $z = t^{\nu_{\mathfrak{p}}(z)}u$, where $\nu_{\mathfrak{p}}(z) \in \mathbb{Z}$ and $u \in \mathcal{O}^*$, and whilst t above is not unique, the number $\nu_{\mathfrak{p}}(z)$ is.
- In particular, $\mathcal{O} = \{z \in F : \nu_{\mathfrak{p}}(z) \geq 0\} \cup \{0\}$,
 $\mathcal{O}^* = \{z \in F : \nu_{\mathfrak{p}}(z) = 0\}$ and $\mathfrak{p} = \{z \in F : \nu_{\mathfrak{p}}(z) > 0\}$, thus $\mathfrak{p} \leftrightarrow \mathcal{O}$.
- The *degree* of \mathfrak{p} is $\deg(\mathfrak{p}) := [\mathcal{O}/\mathfrak{p} : K]$. For all places \mathfrak{p} , $\deg(\mathfrak{p}) < \infty$.

Discrete valuations and the divisor group

- A *discrete valuation* of F is a function $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$, such that
(i) $v(a) = \infty \iff a = 0$, (ii) $v(ab) = v(a) + v(b)$,
(iii) $v(a + b) \geq \min\{v(a), v(b)\}$, (iv) there exists some $c \in F$, such that $v(c) = 1$ and (v) $v(d) = 0$ for all $d \in K^*$.
- Clearly, v_p extended to zero by $v_p(0) = \infty$, is a discrete valuation called the *p-order*.
- The free Abelian group generated by the places of F/K is called the *divisor group* and denoted by $\text{Div}(F)$; its elements are called *divisors*.
- The *degree* of $D = \prod_p p^{d_p}$ is $\deg(D) := \sum_p d_p \deg(p)$ and its *support* is the set $\text{supp}(D) := \{p : d_p \neq 0\}$.

Integral and principal divisors; the divisor class group

- A natural partial ordering is defined in $\text{Div}(F)$ and a divisor $D \geqslant 1_{\text{Div } F}$ is *integral*. Their semigroup is denoted by $\text{Int}(F)$.
- The *group of principal divisors* (denoted by $\text{Prin}(F)$), is the subgroup of $\text{Div}(F)$ comprised by the *principal divisors*, i.e., divisors of the form

$$\text{Prin}(F) = \left\{ [a] = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(a)} : a \in F^* \right\}.$$

- The *divisor class group* of F is the quotient group

$$\text{Cl}(F) := \text{Div}(F) / \text{Prin}(F).$$

Two divisors that are in the same class are *linearly equivalent*.

The rational function field

- In $K(x)/K$ there are only two types of discrete valuations:
 1. For $\pi \in K[x]$ irreducible, define $v_\pi(0) = \infty$ and, for $f \neq 0$, $v_\pi(f) = n$, where n is such that $f = \pi^n g/h$.
 2. Also, define $v_\infty(0) = \infty$ and, for $f \neq 0$, $v_\infty(f) = -\deg(f)$.
- The places of $K(x)$ are exactly the places $\mathfrak{p}_\pi := \langle \pi \rangle$, where $\pi \in K[x]$ is monic irreducible (*finite* places) and \mathfrak{p}_∞ (*infinite* place).
- $\deg(\mathfrak{p}_\pi) = \deg(\pi)$ and $\deg(\mathfrak{p}_\infty) = 1$.
- For every $f \in K[x]$, if $f = \prod_\pi \pi^{f_\pi}$ is its decomposition, define (in addition to its principal divisor)

$$(f) := \prod_\pi \mathfrak{p}_\pi^{f_\pi} \in \text{Int}(K(x)).$$

Characters modulo a divisor

- For $I \in \text{Int}(F)$, $D_I := \{D \in \text{Div}(F) : \text{supp}(D) \cap \text{supp}(I) = \emptyset\}$ and $E_I := \{[a] : a \in F^*, [a] \text{ linearly equivalent to } 1_{\text{Div}(F)}, \text{ and } [a - 1]/I \in \text{Int}(F)\}$.
- E_I is the *ray* of I and $E_I \leq D_I \leq \text{Div}(F)$.
- A homomorphic map $X : \text{Int}(F) \rightarrow \mathbb{C}$, extended to $\text{Div}(F)$, is a *character modulo* I if
 1. $G_X := \{D \in \text{Div}(F) : X(D) \neq 0\} = D_I$ and
 2. $E_I \subseteq G_X^1 := \{D \in \text{Div}(F) : X(D) = 1\}$.
- X is *nonsingular*, if it is nontrivial on divisors of degree 0.

Perel'muter's theorem

Theorem (Perel'muter, 1969)

Let F/K be a global function field of genus g and, if \mathcal{K} is its field of constants, set $m = [\mathcal{K} : K]$. Next take some $I \in \text{Int}(F)$ and X a nonsingular character modulo I . Then

$$\left| \sum_{\deg(\mathfrak{p})|m} (\deg(\mathfrak{p})) X(\mathfrak{p})^{m/\deg(\mathfrak{p})} \right| \leq (2g - 2 + \deg(I)) q^{m/2}.$$

Corollary

Take the function field $\mathbb{F}_q(x)/\mathbb{F}_q$, some $I \in \text{Int}(\mathbb{F}_q(x))$ and X a nonsingular character modulo I . Then

$$\left| \sum_{\deg(\mathfrak{p})=1} X(\mathfrak{p}) \right| \leq (\deg(I) - 2) q^{1/2}.$$

Finite field characters

Definition

Let \mathbb{G} be a finite Abelian group. A *character* of \mathbb{G} is a homomorphism $\chi : \mathbb{G} \rightarrow \mathbb{C}^*$. The *trivial* character is $\chi_o(a) = 1$, for all $a \in \mathbb{G}$.

- In \mathbb{F}_{q^m} there are two main group structures, the additive and the multiplicative. Therefore we have two types of characters, the *additive characters* and the *multiplicative characters*.
- The *canonical* character of \mathbb{F}_{q^m} is defined by $\psi_1(a) = e^{2\pi i \text{Tr}_{q^m/p}(a)/p}$, for $a \in \mathbb{F}_{q^m}$. It is known that all additive characters of \mathbb{F}_{q^m} are of the form $\psi_c(a) = \psi_1(ca)$, for some $c \in \mathbb{F}_{q^m}$.
- The multiplicative characters are extended to \mathbb{F}_{q^m} by the rule

$$\chi(o) := \begin{cases} 0, & \text{if } \chi \neq \chi_o, \\ 1, & \text{if } \chi = \chi_o. \end{cases}$$

The character sum estimate

We have all we need to prove the following:

Theorem

Let χ be a multiplicative character of \mathbb{F}_{q^m} and ψ an additive character of \mathbb{F}_q , respectively, such that not both of them are trivial. Further, let θ be a generator of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$. Then

$$\left| \sum_{t \in \mathbb{F}_q} \chi(\theta + t) \psi(t) \right| \leq m q^{1/2}.$$

Sketch of the proof

We work on the global rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$.

- Let $g(x)$ be the minimum polynomial of θ over \mathbb{F}_q .
- We define a character X modulo $I = \mathfrak{p}_g \mathfrak{p}_\infty^2$ as follows.
- Take some integral $\mathfrak{a} \in D_I$ and a monic $f_{\mathfrak{a}} \in \mathbb{F}_q[x]$, s.t. $(f_{\mathfrak{a}}) = \mathfrak{a}$.
- $g \nmid f_{\mathfrak{a}} \Rightarrow \chi(f_{\mathfrak{a}}(\theta)) \neq 0$.
- Set $S_{\mathfrak{a}} \in \mathbb{F}_q$ the sum of all the roots of $f_{\mathfrak{a}}$ with multiplicities.
- Set $X(\mathfrak{a}) := \chi(f_{\mathfrak{a}}(\theta))\psi(-S_{\mathfrak{a}})$.
- For $\mathfrak{a}, \mathfrak{b} \in D_I$ integral divisors, we have that $X(\mathfrak{a}\mathfrak{b}) = X(\mathfrak{a})X(\mathfrak{b})$, so X can be extended to D_I . Set $X(\mathfrak{a}) = 0$ for all other $\mathfrak{a} \in \text{Div}(\mathbb{F}_q(x))$.
- We have obtained that X is homomorphic and $G_X = D_I$.

Sketch of the proof (cont.)

- We show that $E_I \subseteq G_X^1$, hence X is a character modulo I .
- In order to clarify that X is a nonsingular character, observe that at least one of χ, ψ is nontrivial and they cannot cancel each other.
- The places of degree 1 are \mathfrak{p}_∞ and \mathfrak{p}_{π_t} , where $\pi_t(x) = x + t$. Given that $X(\mathfrak{p}_\infty) = 0$ and $\deg(I) = m + 2$,

$$\left| \sum_{\deg \mathfrak{p}=1} X(\mathfrak{p}) \right| \leq (\deg(I) - 2)q^{1/2} \Rightarrow \left| \sum_{t \in \mathbb{F}_q} X(\mathfrak{p}_{\pi_t}) \right| \leq mq^{1/2}$$

$$\Rightarrow \left| \sum_{t \in \mathbb{F}_q} \chi(\theta + t)\psi(t) \right| \leq mq^{1/2}.$$

The \mathbb{F}_q -order of additive characters

Definition

The \mathbb{F}_q -order of an additive character $\psi \in \widehat{\mathbb{F}_{q^m}}$ is the monic \mathbb{F}_q -divisor g of $x^m - 1$ of minimal degree such that $\psi \circ g$ is the trivial character of $\widehat{\mathbb{F}_{q^m}}$, where $(\psi \circ g)(\alpha) := \psi(g \circ \alpha)$, and $g \circ \alpha = \sum_{i=0}^n a_i \alpha^{q^i}$ if $g(x) = \sum_{i=0}^n a_i x^{q^i}$ for any $\alpha \in \mathbb{F}_{q^m}$ and is denoted by $\text{Ord}_q(\psi)$.

Lemma

Let ψ be an additive character of \mathbb{F}_{q^m} . The restriction of ψ in \mathbb{F}_q , $\psi|_{\mathbb{F}_q}$, is an additive character of \mathbb{F}_q . Also, the following are equivalent:

1. $\psi|_{\mathbb{F}_q}$ is the trivial additive character of \mathbb{F}_q .
2. $\psi = \psi_c$ for some $c \in \mathbb{F}_{q^m}$ such that $\text{Tr}_{q^m/q}(c) = 0$.
3. $\text{Ord}_q(\psi) \mid \frac{x^m - 1}{x - 1}$.

Freeness

- Take $e \mid q^m - 1$. Some $\alpha \in \mathbb{F}_{q^m}^*$ is e -free, if $d \mid e$ and $\alpha = y^d$, for some $y \in \mathbb{F}_{q^m}^*$ imply $d = 1$. Some $\alpha \in \mathbb{F}_{q^m}^*$ is primitive iff it is $(q^m - 1)$ -free.
- Their characteristic function of e -free elements is

$$\rho_e : \mathbb{F}_{q^m}^* \rightarrow \{0, 1\}; \alpha \mapsto \lambda(e) \sum_{d \mid e} \left(\frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d(\alpha) \right).$$

- For $g \mid x^m - 1$, some $\alpha \in \mathbb{F}_{q^m}$ is g -free if $\alpha = h \circ \beta$ for some $\beta \in \mathbb{F}_{q^m}$ and $h \mid g$ imply $h = 1$. Some $\alpha \in \mathbb{F}_{q^m}$ is normal iff it is $(x^m - 1)$ -free.
- Their characteristic function of g -free elements is

$$\kappa_g : \mathbb{F}_{q^m} \rightarrow \{0, 1\}; \alpha \mapsto \Lambda(g) \sum_{f \mid g} \left(\frac{\mu'(f)}{\Phi(f)} \sum_{(f)} \psi_f(\alpha) \right).$$

When is the additive character trivial?

- A set of elements of \mathbb{F}_{q^m} that will be of interest for us is $(x^m - 1)/(x - 1)$ -free elements.
- These elements do not belong to any intermediate extension of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and if $p \mid m$ they are exactly those that are normal over \mathbb{F}_q .
- If m is a prime such that q is primitive modulo m they are easily characterized.

Lemma

Suppose m is a prime and q is primitive modulo m . Then the $(x^m - 1)/(x - 1)$ -free elements of \mathbb{F}_{q^m} are exactly those that do not belong to any intermediate extension of $\mathbb{F}_{q^m}/\mathbb{F}_q$.

Clean and dirty lines

- Take generator θ of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ and some $\alpha \in \mathbb{F}_q$, such that $\alpha\theta$ is g -free, where $g(x) = (x^m - 1)/(x - 1)$.
- We call the line $\{\alpha(\theta + x) : x \in \mathbb{F}_q\}$ *clean*.
- We refer to a line that is not clean as *dirty*.
- We first focus on clean lines and prove that, for q large enough, every such line contains a primitive normal element.
- As a consequence, we obtain the weak line property for primitive normal elements for a specific types of extensions.

An existence condition

- Take θ a generator of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q$, such that the line of θ and α is clean.
- Set $\mathfrak{N}_{\alpha,\theta}$ the number of elements within the line that are primitive and normal.
- It suffices to show that $\mathfrak{N}_{\alpha,\theta} \neq 0$.

Lemma

$$\mathfrak{N}_{\alpha,\theta} \geq \lambda(q^m - 1)\Lambda(x^m - 1) \left[\frac{q}{\Lambda\left(\frac{x^m - 1}{x - 1}\right)} - W(q^m - 1)W(x^m - 1)q^{1/2} \right],$$

where $W(y)$, if $g \in \mathbb{F}_q[x]$, is the number of squarefree monic divisors of g in $\mathbb{F}_q[x]$ and, for $y \in \mathbb{Z}$, is the number of positive squarefree divisors of a .

Sketch of the lemma's proof

We have that

$$\begin{aligned}
 \mathfrak{N}_{\alpha,\theta} &= \sum_{x \in \mathbb{F}_q} \rho_{q^m-1}(\alpha(\theta+x)) \kappa_{x^m-1}(\alpha(\theta+x)) \\
 &= \lambda(q^m-1) \Lambda(x^m-1) \sum_{\substack{d|q^m-1 \\ f|x^m-1}} \frac{\mu(d)\mu'(f)}{\phi(d)\Phi(f)} \sum_{(d),(f)} \chi_d(\alpha) \psi_f(\alpha\theta) \\
 &\quad \sum_{x \in \mathbb{F}_q} \chi_d(\theta+x) \psi_f(\alpha x) \\
 &= \lambda(q^m-1) \Lambda(x^m-1) [S_1 + S_2 + S_3],
 \end{aligned}$$

where, S_1 stands for the part of the sum that corresponds to $d=1$ and $f \mid (x^m-1)/(x-1)$, S_2 for the part that corresponds to $d=1$ and $f \nmid (x^m-1)/(x-1)$ and S_3 to the part that corresponds to $d \neq 1$.

Sketch of the lemma's proof (cont.)

We prove that

$$S_1 = \frac{q}{\Lambda\left(\frac{x^m-1}{x-1}\right)},$$

$$|S_2| \leq \left(W(x^m - 1) - W\left(\frac{x^m - 1}{x - 1}\right) \right) m q^{1/2},$$

$$|S_3| \leq (W(q^m - 1) - 1) W(x^m - 1) m q^{1/2}.$$

The result follows.

The (clean) line property for primitive normal elements

The above lemma combined with known bounds for the quantities $W(q^m - 1)$ and $W(x^m - 1)$ yield the following.

Theorem

Fix an integer m . There exists some number \mathfrak{L}_m , such that for every prime power $q \geq \mathfrak{L}_m$, every clean line of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ contains a primitive normal element.

The weak line property for primitive normal elements

Then we show that if q is primitive modulo m (m prime), $q \geq \mathfrak{L}_m$, θ is a generator of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, then the line $\{a(\theta + x) : x \in \mathbb{F}_q\}$ is clean. So, we get the following:

Theorem

Fix a prime m . There exists an integer $WLPN(m) = \mathfrak{L}_m$, such that for every prime power $q \geq WLPN(m)$ that is primitive modulo m , the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ possesses the weak line property for primitive normal elements. The same is true for some $TPN(m) \leq WLPN(m)$ regarding the translate property for primitive normal elements.

Additional research on existence results

- What is going on with the dirty lines?
- Can we extend to the (nonweak) line property?
- Can we generalize to r -primitive and/or k -normal elements? Some \mathbb{F}_{q^m} is called k -normal over \mathbb{F}_q if its \mathbb{F}_q -conjugates produce an \mathbb{F}_q -vector space of dimension $m - k$.
- Recent effective characterizations for r -primitive and k -normal elements, were recently established by the speaker with Cohen and Reis (2022) and with Reis (2025), respectively.

Additional research from a geometric point of view

- In this work we studied the existence of primitive normal elements of $\mathbb{F}_{q^m}/\mathbb{F}_q$ within the set $\mathcal{A}_f := \{f(x) : x \in \mathbb{F}_q\}$, where $f \in \mathbb{F}_q[x]$ is linear.
- Perel'muter and Shparlinski (1990) work with the prime extension $\mathbb{F}_{p^m}/\mathbb{F}_p$ and study the existence of primitive elements within \mathcal{A}_f where $f \in \mathbb{F}_p[x]$ is required to be irreducible.
- In that spirit, we believe that establishing the existence of primitive normal elements of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ within \mathcal{A}_f , for irreducible $f \in \mathbb{F}_q[x]$, would be feasible but nontrivial.

Additional research from a computational point of view

Finally, an intriguing question on this line of research is computing the exact value of the numbers that are proven asymptotically to exist. For example, we have the following:

- (Cohen, 1983): $TP(2) = LP(2) = 1$.
- (Cohen, 2009): $TP(3) = 37$.
- (Bailey-Cohen-Sutherland-Trudgian, 2019): $LP(3) = 37$ and $73 \leq TP(4) \leq LP(4) \leq 10282$.
- (Cohen-K., 2020): $TP_2(2) = LP_2(2) = 41$.
- It follows from this work that $TPN(2) = LPN(2) = 1$.
- What about the numbers $TPN(m)$ and $LPN(m)$, for $m \geq 3$?

References I



T. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, New York Heidelberg Berlin, 1976.



G. Bailey, S. Cohen, N. Sutherland, and T. Trudgian. Existence results for primitive elements in cubic and quartic extensions of a finite field. *Math. Comp.*, 88(316):931–947, 2019.



L. Carlitz. Distribution of primitive roots in a finite field. *Quart. J. Math. Oxford Ser. (2)*, 4(1):4–10, 1953.



F. Chung. Diameters and eigenvalues. *J. Amer. Math. Soc.*, 2(2):187–196, 1989.



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



S. Cohen. Generators of the cubic extension of a finite field. *J. Combin. Number Theory*, 1(3):189–202, 2009.

References II



S. Cohen. Primitive elements on lines in extensions of finite fields. In D. Panario, G. McGuire, G. Mullen, and I. Shparlinski, eds., *Finite Fields: Theory and Applications*, vol. 518 of *Contemp. Math.*, pp. 113–127, AMS, 2010.



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



S. Cohen and G. Kapetanakis. Finite field extensions with the line or translate property for-primitive elements. *J. Aust. Math. Soc.*, 111(3):313–319, 2021.



S. Cohen, G. Kapetanakis, and L. Reis. The existence of \mathbb{F}_q -primitive points on curves using freeness. *Comptes Rendus Math.*, 360(G6):641–652, 2022.



H. Davenport. On primitive roots in finite fields. *Quart. J. Math. Oxford*, 8(1):308–312, 1937.



S. Huczynska, G. Mullen, D. Panario, and D. Thomson. Existence and properties of k -normal elements over finite fields. *Finite Fields Appl.*, 24:170–183, 2013.



G. Kapetanakis and L. Reis. Normal points on Artin-Schreier curves over finite fields. To appear, 2025.

References III



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



R. Lidl and H. Niederreiter. *Finite Fields*, vol. 20 of *Enycl. Math. Appl.*. Cambridge University Press, Cambridge, second ed., 1997.



G. Perel'muter. Estimate of a sum along an algebraic curve. *Mat. Zametki*, 5:373–380, 1969.



G. Perel'muter and I. Shparlinski. The distribution of primitive roots in finite fields. *Russ. Math. Surv.*, 45(1):223–224, 1990.



I. Rúa. On the primitivity of four-dimensional finite semifields. *Finite Fields Appl.*, 33:212–229, 2015.



I. Rúa. Primitive semifields of order 2^{4e} . *Des. Codes Cryptogr.*, 83(2):345–356, 2017.



H. Stichtenoth. *Algebraic Function Fields and Codes*, vol. 254 of *Grad. Texts in Math.*. Springer, Berlin Heidelberg, second ed., 2009.

Shameless Advertisment:




30th APPLICATIONS OF COMPUTER ALGEBRA

14-18 JULY HERAKLION CRETE / GREECE 2025

Invited Speakers

Giampaolo Nicotri
University of Palermo

Isabelle Sten
University of Athens, Greece

Daniel Renshaw
Carleton University, Canada

Yannick Dierker
University of Würzburg, Germany

Organization

General Chair:
Sami Tzavara
University of Crete, Greece

Program Chair:
Giorgos Kuperelis
University of Thessaly, Greece

ACA WG co-chairs:
Rico Janssens
UNIFRAX, Austria
Michael Wüster
University of Bonn, Germany

Scientific Committee:
ACA Working Group

Local Committees

Theodoros Gontikas
University of Crete, Greece

Zafra Malik
University of Cyprus, Cyprus

Special Sessions including (but not limited to)

- Computer Algebra in Education
- Computer Algebra Software in the Life Sciences (CAS4Life)
- Computer algebra in group theory and representation theory
- Computational Differential and Difference Algebra and Their Applications
- Computer algebra modelling in physics, classical and celestial mechanics, and engineering
- Symbolic Linear Algebra and its Applications
- History of Computer Algebra
- D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic
- Algebraic geometry from an algorithmic point of view
- Algebraic and Algorithmic Aspects of Differential and Integral Operators Session
- Sparse Interpolation and Technology
- Symbolic-Numeric Computation
- Advances in Coding Theory: Algebraic, Combinatorial and Computational Methods
- Finite Fields and Applications

Deadlines

Early registration: 1 June 2025
Special session proposal deadline: 30 April 2025
Talk submission deadline: 30 May 2025
Camera-ready: 1 July 2025

The ACA conference series is devoted to bringing leading computer algebra researchers and encourage the interaction of advances of computer algebra research and practice with mathematicians, scientists, and industrialists.

<https://aca2025.github.io/>






Thank you for your attention!