Character sums estimates over affine spaces applied to existence results in finite fields

Lucas Reis

Federal University of Minas Gerais

August 12

Outline

1. Introduction
2. Bounds on character sums over affine spaces
3. Primitive elements
4. Primitive elements with prescribed digits
5. Primitive k-normal elements

Introduction

Notation

1. $\mathbb{F}_q$ denotes the finite field of q elements, where q is a prime power.
2. $\mathbb{F}_{q^n}$ is the unique n-degree extension of $\mathbb{F}_q$.
3. χ usually denotes a (multiplicative) character of $\mathbb{F}_{q^n}$.
4. $\mathcal{V} \subseteq \mathbb{F}_{q^n}$ usually denotes an $\mathbb{F}_q$-vector space.
5. $\mathcal{A} = u + \mathcal{V} \subseteq \mathbb{F}_{q^n}$ usually denotes an $\mathbb{F}_q$-affine space (we allow $u = 0$).
6. For a set S, $|S|$ denotes its cardinality and $\mathbb{I}_S$ denotes its indicator function.

Some basics

Some basics

Definition

A multiplicative character of $\mathbb{F}_q$ is a homomorphism $\chi : \mathbb{F}_q^* \to \mathbb{C}^\times$. An additive character is defined in a similar way for the group $(\mathbb{F}_q, +)$.

Some basics

Definition

A multiplicative character of $\mathbb{F}_q$ is a homomorphism $\chi : \mathbb{F}_q^* \to \mathbb{C}^\times$. An additive character is defined in a similar way for the group $(\mathbb{F}_q, +)$.

1. The group $\mathbb{F}_q^*$ is cyclic of order $q - 1$, and any generator is called **primitive**.

Some basics

Definition

A multiplicative character of $\mathbb{F}_q$ is a homomorphism $\chi : \mathbb{F}_q^* \to \mathbb{C}^\times$. An additive character is defined in a similar way for the group $(\mathbb{F}_q, +)$.

1. The group $\mathbb{F}_q^*$ is cyclic of order $q-1$, and any generator is called **primitive**.
2. Fix $\theta \in \mathbb{F}_q^*$ a primitive element and let $0 \le k \le q-2$. Then $\chi_k = \chi_{\theta,k} : \mathbb{F}_q^* \to \mathbb{C}^\times$ with $\chi_k(\theta^j) = \zeta^{jk}$, is a multiplicative character of $\mathbb{F}_q$, where $\zeta = \exp\left(\frac{2\pi \mathbf{i}}{q-1}\right)$ is a primitive $(q-1)$-th root of unity.

Some basics

Definition

A multiplicative character of $\mathbb{F}_q$ is a homomorphism $\chi : \mathbb{F}_q^* \to \mathbb{C}^\times$. An additive character is defined in a similar way for the group $(\mathbb{F}_q, +)$.

1. The group $\mathbb{F}_q^*$ is cyclic of order $q-1$, and any generator is called **primitive**.
2. Fix $\theta \in \mathbb{F}_q^*$ a primitive element and let $0 \le k \le q-2$. Then $\chi_k = \chi_{\theta,k} : \mathbb{F}_q^* \to \mathbb{C}^\times$ with $\chi_k(\theta^j) = \zeta^{jk}$, is a multiplicative character of $\mathbb{F}_q$, where $\zeta = \exp\left(\frac{2\pi \mathbf{i}}{q-1}\right)$ is a primitive $(q-1)$-th root of unity.
3. The latter describes the set of multiplicative characters of $\mathbb{F}_q$; this set is a (multiplicative) group with identity χ_0, the trivial character: $\chi_0(a) = 1$ for every $a \in \mathbb{F}_q^*$.
4. We usually extend χ_k to 0 by setting $\chi_k(0) = 0$.

Characters of finite fields have been extensively used to prove remarkable results in finite fields related to topics such as Number Theory, Combinatorics and Arithmetic Dynamics.

Characters of finite fields have been extensively used to prove remarkable results in finite fields related to topics such as Number Theory, Combinatorics and Arithmetic Dynamics.

For a rich source of problems, techniques and results, see [P. Charpin, A. Pott, A. Winterhof, *Finite Fields and Their Applications - Character Sums and Polynomials,* De Grutyer (2013)].

Characters of finite fields have been extensively used to prove remarkable results in finite fields related to topics such as Number Theory, Combinatorics and Arithmetic Dynamics.

For a rich source of problems, techniques and results, see [P. Charpin, A. Pott, A. Winterhof, *Finite Fields and Their Applications - Character Sums and Polynomials*, De Grutyer (2013)].

When proving results with the help of characters (e.g., existence and distribution results), a typical procedure is to obtain a character sum formula for the **indicator function** of sets that are of our interest (squares, normal, primitive, zero trace, etc).

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions.

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions. The number $N = N(\mathbb{F}, A, B)$ of elements in $A \cap B$ equals

$$\sum_{y \in \mathbb{F}} \mathbb{I}_A(y) \cdot \mathbb{I}_B(y) =$$

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions. The number $N = N(\mathbb{F}, A, B)$ of elements in $A \cap B$ equals

$$\sum_{y \in \mathbb{F}} \mathbb{I}_A(y) \cdot \mathbb{I}_B(y) = \sum_{y \in A} \mathbb{I}_B(y) =$$

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions.The number $N = N(\mathbb{F}, A, B)$ of elements in $A \cap B$ equals

$$\sum_{y \in \mathbb{F}} \mathbb{I}_A(y) \cdot \mathbb{I}_B(y) = \sum_{y \in A} \mathbb{I}_B(y) = \sum_{y \in B} \mathbb{I}_A(y).$$

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions. The number $N = N(\mathbb{F}, A, B)$ of elements in $A \cap B$ equals

$$\sum_{y \in \mathbb{F}} \mathbb{I}_A(y) \cdot \mathbb{I}_B(y) = \sum_{y \in A} \mathbb{I}_B(y) = \sum_{y \in B} \mathbb{I}_A(y).$$

1. Existence results: $N(\mathbb{F}, A, B) > 0$;

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions. The number $N = N(\mathbb{F}, A, B)$ of elements in $A \cap B$ equals

$$\sum_{y \in \mathbb{F}} \mathbb{I}_A(y) \cdot \mathbb{I}_B(y) = \sum_{y \in A} \mathbb{I}_B(y) = \sum_{y \in B} \mathbb{I}_A(y).$$

1. Existence results: $N(\mathbb{F}, A, B) > 0$;
2. Distribution results: $N(\mathbb{F}, A, B) = \frac{|A| \cdot |B|}{|\mathbb{F}|} \cdot (1 + o_{|\mathbb{F}|}(1))$.

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions.The number $N = N(\mathbb{F}, A, B)$ of elements in $A \cap B$ equals

$$\sum_{y \in \mathbb{F}} \mathbb{I}_A(y) \cdot \mathbb{I}_B(y) = \sum_{y \in A} \mathbb{I}_B(y) = \sum_{y \in B} \mathbb{I}_A(y).$$

1. Existence results: $N(\mathbb{F}, A, B) > 0$;
2. Distribution results: $N(\mathbb{F}, A, B) = \frac{|A| \cdot |B|}{|\mathbb{F}|} \cdot (1 + o_{|\mathbb{F}|}(1))$.

In particular, sometimes we need to bound (non trivially) a sum of the form

$$s(\chi, S) := \sum_{x \in S} \chi(x),$$

where $S \subseteq \mathbb{F}$ and χ is non trivial.

A typical problem: let $A, B \subset \mathbb{F}$ be sets comprising the elements of $\mathbb{F}$ with some special property, and let $\mathbb{I}_A$ and $\mathbb{I}_B$ be their indicator functions.The number $N = N(\mathbb{F}, A, B)$ of elements in $A \cap B$ equals

$$\sum_{y \in \mathbb{F}} \mathbb{I}_A(y) \cdot \mathbb{I}_B(y) = \sum_{y \in A} \mathbb{I}_B(y) = \sum_{y \in B} \mathbb{I}_A(y).$$

1. Existence results: $N(\mathbb{F}, A, B) > 0$;
2. Distribution results: $N(\mathbb{F}, A, B) = \frac{|A| \cdot |B|}{|\mathbb{F}|} \cdot (1 + o_{|\mathbb{F}|}(1))$.

In particular, sometimes we need to bound (non trivially) a sum of the form

$$s(\chi, S) := \sum_{x \in S} \chi(x),$$

where $S \subseteq \mathbb{F}$ and χ is non trivial.

The trivial bound is $|s(\chi, S)| \leq |S|$, but we require something "slightly better". For generic S, this is a **hard** problem.

Some well-known results:

Some well-known results:

1. S is an interval of integers and χ is over $\mathbb{Z}_p = \mathbb{F}_p$:
    - (Polya Vinogradov) $|s(\chi, S)| \ll \sqrt{p} \log p$;
    - (Burgess [1]) $|s(\chi, S)| \ll p^{-\delta(\varepsilon)}|S|$, if $|S| \gg p^{1/4+\varepsilon}$.

Some well-known results:

1. S is an interval of integers and χ is over $\mathbb{Z}_p = \mathbb{F}_p$:
   - (Polya Vinogradov) $|s(\chi, S)| \ll \sqrt{p}\log p$;
   - (Burgess [1]) $|s(\chi, S)| \ll p^{-\delta(\varepsilon)}|S|$, if $|S| \gg p^{1/4+\varepsilon}$.
2. $S \subseteq \mathbb{F}_{p^k}$ is a "box":

$$S = \left\{ \sum_{i=1}^{k} a_i \mathbf{b_i} : a_i \in I_i \right\},$$

each I_i a "nice interval" and $\{\mathbf{b_1}, \ldots, \mathbf{b_k}\}$ an $\mathbb{F}_p$-basis for $\mathbb{F}_{p^k}$. Many results (see [3, 4] and the references therein).

Some well-known results:

1. S is an interval of integers and χ is over $\mathbb{Z}_p = \mathbb{F}_p$:
   - (Polya Vinogradov) $|s(\chi, S)| \ll \sqrt{p} \log p$;
   - (Burgess [1]) $|s(\chi, S)| \ll p^{-\delta(\varepsilon)}|S|$, if $|S| \gg p^{1/4+\varepsilon}$.
2. $S \subseteq \mathbb{F}_{p^k}$ is a "box":

$$S = \left\{ \sum_{i=1}^{k} a_i \mathbf{b_i} : a_i \in I_i \right\},$$

each I_i a "nice interval" and $\{\mathbf{b_1}, \ldots, \mathbf{b_k}\}$ an $\mathbb{F}_p$-basis for $\mathbb{F}_{p^k}$. Many results (see [3, 4] and the references therein).

Remark

The results about "boxes" do not apply to generic affine spaces in a finite field.

Bounds on character sums over affine spaces

Bounds for some special $\mathbb{F}_p$-vector spaces:

Bounds for some special $\mathbb{F}_p$-vector spaces:

1. (Burgess [2]) If θ generates $\mathbb{F}_{p^k}$, i.e., $\mathbb{F}_{p^k} = \mathbb{F}_p(\theta)$, then $|s(\chi, S)| \le p^{m(1-\delta(\varepsilon))}$, where

$$S = \sum_{i=0}^{m-1} \theta^i \cdot \mathbb{F}_p,$$

and $m > k(1/4 + \varepsilon)$.

2. (Chang [4]) For a "sufficiently generic" $\mathbb{F}_p$-vector space $\mathcal{V} \subseteq \mathbb{F}_{p^k}$ of dimension $m \gg k$, the bound

$$|s(\chi, S)| \le |S| \cdot (\log p)^{-\delta},$$

holds under $k \ll p \cdot (\log p)^4$.

A general result:

Theorem (Swaenepoel [16])

Let $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-affine space of dimension t and χ a non trivial multiplicative character of $\mathbb{F}_{q^n}$. Then

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| \le \frac{q^{n-t}-1}{q^{n-t}} q^{n/2}.$$

A general result:

Theorem (Swaenepoel [16])

Let $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-affine space of dimension t and χ a non trivial multiplicative character of $\mathbb{F}_{q^n}$. Then

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| \leq \frac{q^{n-t}-1}{q^{n-t}} q^{n/2}.$$

Main idea:

$$\sum_{a\in\mathcal{A}} \chi(a) = \sum_{y\in\mathbb{F}_{q^n}} \mathbb{I}_{\mathcal{A}}(x)\cdot\chi(x),$$

where the indicator function $\mathbb{I}_{\mathcal{A}}$ can be expressed in terms of additive characters. The latter reduces to estimate Gauss sums (additive+multiplicative characters in the sum) with traditional bounds.

Remark

Obstruction: the bound is trivial for $t \leq n/2$.

A new bound

A new bound

Definition

An element $\alpha \in \mathbb{F}_{q^n}$ has degree n over $\mathbb{F}_q$ (or generates $\mathbb{F}_{q^n}$) if it is not contained in any subfield $\mathbb{F}_{q^d}$, $d < n$.

A new bound

Definition

An element $\alpha \in \mathbb{F}_{q^n}$ has degree n over $\mathbb{F}_q$ (or generates $\mathbb{F}_{q^n}$) if it is not contained in any subfield $\mathbb{F}_{q^d}$, $d < n$.

The following result is crucial:

Theorem (Katz [9])

Let θ be an element of degree n over $\mathbb{F}_q$ and χ a non trivial multiplicative character of $\mathbb{F}_{q^n}$. Then $\left|\sum_{a\in\mathbb{F}_q} \chi(\theta + a)\right| \le (n-1)\sqrt{q}$.

A new bound

Definition

An element $\alpha \in \mathbb{F}_{q^n}$ has degree n over $\mathbb{F}_q$ (or generates $\mathbb{F}_{q^n}$) if it is not contained in any subfield $\mathbb{F}_{q^d}$, $d < n$.

The following result is crucial:

Theorem (Katz [9])

Let θ be an element of degree n over $\mathbb{F}_q$ and χ a non trivial multiplicative character of $\mathbb{F}_{q^n}$. Then $\left|\sum_{a\in\mathbb{F}_q} \chi(\theta + a)\right| \le (n-1)\sqrt{q}$.

Non trivial for $n - 1 < \sqrt{q}$.

A new bound

We obtain the following result:

Theorem (R., 2020)

Let $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-affine space of dimension $t \geq 0$, where $n > 1$. For each divisor d of n, let $n_{\mathcal{A},d}$ be the number of elements in $\mathcal{A}$ whose degree over $\mathbb{F}_q$ equals d. If χ is a nontrivial multiplicative character of $\mathbb{F}_{q^n}$, then

$$\left|\sum_{b\in\mathbb{F}_q}\sum_{a\in\mathcal{A}}\chi(a+b)\right| \leq \sum_{d|n} n_{\mathcal{A},d}\cdot\delta_{\chi,d}, \tag{1}$$

where $\delta_{\chi,d} = q$ if $\chi|_{\mathbb{F}_{q^d}}$ is trivial and $\delta_{\chi,d} = \min\{q, (d-1)\sqrt{q}\}$, otherwise.

A new bound

We obtain the following result:

Theorem (R., 2020)

Let $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-affine space of dimension $t \geq 0$, where $n > 1$. For each divisor d of n, let $n_{\mathcal{A},d}$ be the number of elements in $\mathcal{A}$ whose degree over $\mathbb{F}_q$ equals d. If χ is a nontrivial multiplicative character of $\mathbb{F}_{q^n}$, then

$$\left|\sum_{b\in\mathbb{F}_q}\sum_{a\in\mathcal{A}}\chi(a+b)\right| \leq \sum_{d|n} n_{\mathcal{A},d}\cdot\delta_{\chi,d}, \tag{1}$$

where $\delta_{\chi,d} = q$ if $\chi|_{\mathbb{F}_{q^d}}$ is trivial and $\delta_{\chi,d} = \min\{q, (d-1)\sqrt{q}\}$, otherwise.In particular, if $n_{\mathcal{A},n} > 0$, we have that

$$\left|\sum_{b\in\mathbb{F}_q}\sum_{a\in\mathcal{A}}\chi(a+b)\right| < n\cdot q^{t+1/2}. \tag{2}$$

Alternative version of the previous theorem

Definition

An affine space $\mathcal{A} = u + \mathcal{V} \subseteq \mathbb{F}_{q^n}$ is *n*-good if there exist $y \in \mathcal{V}$ and $z \in \mathcal{A}$ such that zy^{-1} has degree n over $\mathbb{F}_q$.

Alternative version of the previous theorem

Definition

An affine space $\mathcal{A} = u + \mathcal{V} \subseteq \mathbb{F}_{q^n}$ is n-good if there exist $y \in \mathcal{V}$ and $z \in \mathcal{A}$ such that zy^{-1} has degree n over $\mathbb{F}_q$.

Theorem (R., 2020)

Let $\mathcal{A}$ be an n-good affine space of dimension $t \geq 1$. If χ is a non trivial multiplicative character of $\mathbb{F}_{q^n}$, we have that

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| \leq n \cdot q^{t-1/2}. \tag{3}$$

Proof.

Let $y \in \mathcal{V}$ such that zy^{-1} has degree n for some $z \in \mathcal{A}$ and set $\mathcal{A}_y = \{ay^{-1} : a \in \mathcal{A}\}$.

Proof.

Let $y \in \mathcal{V}$ such that zy^{-1} has degree n for some $z \in \mathcal{A}$ and set $\mathcal{A}_y = \{ay^{-1} : a \in \mathcal{A}\}$. Since χ is multiplicative,

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|.$$

Proof.

Let $y \in \mathcal{V}$ such that zy^{-1} has degree n for some $z \in \mathcal{A}$ and set $\mathcal{A}_y = \{ay^{-1} : a \in \mathcal{A}\}$. Since χ is multiplicative,

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|.$$

1. $\mathcal{A}_y = u_y + V_y$, where V_y is an $\mathbb{F}_q$-vector space of dimension t containing $\mathbb{F}_q$;

Proof.

Let $y \in \mathcal{V}$ such that zy^{-1} has degree n for some $z \in \mathcal{A}$ and set $\mathcal{A}_y = \{ay^{-1} : a \in \mathcal{A}\}$. Since χ is multiplicative,

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|.$$

1. $\mathcal{A}_y = u_y + V_y$, where V_y is an $\mathbb{F}_q$-vector space of dimension t containing $\mathbb{F}_q$;
2. $\mathcal{A}_y = \mathbb{F}_q \oplus \mathcal{B}$, where $\mathcal{B}$ is an $\mathbb{F}_q$-affine space of dimension $t-1$;

Proof.

Let $y \in \mathcal{V}$ such that zy^{-1} has degree n for some $z \in \mathcal{A}$ and set $\mathcal{A}_y = \{ay^{-1} : a \in \mathcal{A}\}$. Since χ is multiplicative,

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|.$$

1. $\mathcal{A}_y = u_y + V_y$, where V_y is an $\mathbb{F}_q$-vector space of dimension t containing $\mathbb{F}_q$;
2. $\mathcal{A}_y = \mathbb{F}_q \oplus \mathcal{B}$, where $\mathcal{B}$ is an $\mathbb{F}_q$-affine space of dimension $t-1$;

Therefore, the following holds:

$$\sum_{a\in\mathcal{A}_y} \chi(a) = \sum_{b\in\mathbb{F}_q} \sum_{a\in\mathcal{B}} \chi(a+b).$$

Proof.

Let $y \in \mathcal{V}$ such that zy^{-1} has degree n for some $z \in \mathcal{A}$ and set $\mathcal{A}_y = \{ay^{-1} : a \in \mathcal{A}\}$. Since χ is multiplicative,

$$\left| \sum_{a \in \mathcal{A}} \chi(a) \right| = \left| \sum_{a \in \mathcal{A}_y} \chi(a) \right|.$$

1. $\mathcal{A}_y = u_y + V_y$, where V_y is an $\mathbb{F}_q$-vector space of dimension t containing $\mathbb{F}_q$;
2. $\mathcal{A}_y = \mathbb{F}_q \oplus \mathcal{B}$, where $\mathcal{B}$ is an $\mathbb{F}_q$-affine space of dimension $t-1$;

Therefore, the following holds:

$$\sum_{a \in \mathcal{A}_y} \chi(a) = \sum_{b \in \mathbb{F}_q} \sum_{a \in \mathcal{B}} \chi(a+b).$$

From hypothesis, $\mathcal{B}$ contains an element whose degree over $\mathbb{F}_q$ equals n, and so the result follows by the previous theorem. □

Theorem

Let $\mathcal{A}$ be an n-good affine space of dimension $t \geq 1$. If χ is a non trivial multiplicative character of $\mathbb{F}_{q^n}$, we have that

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| \leq n \cdot q^{t-1/2}. \quad (4)$$

Theorem

Let $\mathcal{A}$ be an n-good affine space of dimension $t \geq 1$. If χ is a non trivial multiplicative character of $\mathbb{F}_{q^n}$, we have that

$$\left|\sum_{a\in\mathcal{A}} \chi(a)\right| \leq n \cdot q^{t-1/2}. \quad (4)$$

Non trivial for $n < \sqrt{q}$.

The "*n*-goodness" property is **not restrictive** within the non trivial range $n \leq \sqrt{q}$:

The "n-goodness" property is **not restrictive** within the non trivial range $n \leq \sqrt{q}$:

Proposition

Fix q a prime power and $n \leq q$. Then either $\mathcal{A}$ is n-good or $\mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}$ for some $d | n$ with $d < n$ and some $y \in \mathbb{F}_{q^n}$.

The "n-goodness" property is **not restrictive** within the non trivial range $n \leq \sqrt{q}$:

Proposition

Fix q a prime power and $n \leq q$. Then either $\mathcal{A}$ is n-good or $\mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}$ for some $d|n$ with $d < n$ and some $y \in \mathbb{F}_{q^n}$.

So if $n \leq \sqrt{q}$ and $\mathcal{A}$ is not n-good, we have that $\mathcal{A}_y := y^{-1} \cdot \mathcal{A} \subseteq \mathbb{F}_{q^d}$.

The "n-goodness" property is **not restrictive** within the non trivial range $n \leq \sqrt{q}$:

Proposition

Fix q a prime power and $n \leq q$. Then either $\mathcal{A}$ is n-good or $\mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}$ for some $d|n$ with $d < n$ and some $y \in \mathbb{F}_{q^n}$.

So if $n \leq \sqrt{q}$ and $\mathcal{A}$ is not n-good, we have that $\mathcal{A}_y := y^{-1} \cdot \mathcal{A} \subseteq \mathbb{F}_{q^d}$.

However, $\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|$, reducing the problem to a character sum over $\mathbb{F}_{q^d}$.

The "n-goodness" property is **not restrictive** within the non trivial range $n \leq \sqrt{q}$:

Proposition

Fix q a prime power and $n \leq q$. Then either $\mathcal{A}$ is n-good or $\mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}$ for some $d|n$ with $d < n$ and some $y \in \mathbb{F}_{q^n}$.

So if $n \leq \sqrt{q}$ and $\mathcal{A}$ is not n-good, we have that $\mathcal{A}_y := y^{-1} \cdot \mathcal{A} \subseteq \mathbb{F}_{q^d}$.

However, $\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|$, reducing the problem to a character sum over $\mathbb{F}_{q^d}$.We then try to apply the theorem for $\mathcal{A}_y$, checking if $\chi|_{\mathbb{F}_{q^d}}$ is trivial or if $\mathcal{A}_y$ is d-good, and so on ...

The "n-goodness" property is **not restrictive** within the non trivial range $n \le \sqrt{q}$:

Proposition

Fix q a prime power and $n \le q$. Then either $\mathcal{A}$ is n-good or $\mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}$ for some $d|n$ with $d < n$ and some $y \in \mathbb{F}_{q^n}$.

So if $n \le \sqrt{q}$ and $\mathcal{A}$ is not n-good, we have that $\mathcal{A}_y := y^{-1} \cdot \mathcal{A} \subseteq \mathbb{F}_{q^d}$.

However, $\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|$, reducing the problem to a character sum over $\mathbb{F}_{q^d}$.We then try to apply the theorem for $\mathcal{A}_y$, checking if $\chi|_{\mathbb{F}_{q^d}}$ is trivial or if $\mathcal{A}_y$ is d-good, and so on ...

After some iterations of this procedure we reduce to a character sum over an affine space $\mathcal{A}^* \subseteq \mathbb{F}_{q^e}$ such that either $\mathcal{A}^*$ is e-good or $\chi|_{\mathbb{F}_{q^e}}$ is trivial.

The "n-goodness" property is **not restrictive** within the non trivial range $n \leq \sqrt{q}$:

Proposition

Fix q a prime power and $n \leq q$. Then either $\mathcal{A}$ is n-good or $\mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}$ for some $d|n$ with $d < n$ and some $y \in \mathbb{F}_{q^n}$.

So if $n \leq \sqrt{q}$ and $\mathcal{A}$ is not n-good, we have that $\mathcal{A}_y := y^{-1} \cdot \mathcal{A} \subseteq \mathbb{F}_{q^d}$.

However, $\left|\sum_{a\in\mathcal{A}} \chi(a)\right| = \left|\sum_{a\in\mathcal{A}_y} \chi(a)\right|$, reducing the problem to a character sum over $\mathbb{F}_{q^d}$.We then try to apply the theorem for $\mathcal{A}_y$, checking if $\chi|_{\mathbb{F}_{q^d}}$ is trivial or if $\mathcal{A}_y$ is d-good, and so on ...

After some iterations of this procedure we reduce to a character sum over an affine space $\mathcal{A}^* \subseteq \mathbb{F}_{q^e}$ such that either $\mathcal{A}^*$ is e-good or $\chi|_{\mathbb{F}_{q^e}}$ is trivial.

Conclusion: either the theorem can be applied or $|\sum_{a\in\mathcal{A}} \chi(a)| = |\mathcal{A}|$.

Let p_n be the smallest prime divisor of n. If $d|n$ and $d < n$, then $d \leq \frac{n}{p_n}$.

Let p_n be the smallest prime divisor of n. If $d|n$ and $d < n$, then $d \leq \frac{n}{p_n}$.

In particular, any $\mathbb{F}_q$-affine space $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ of dimension $t > \frac{n}{p_n}$ is n-good.

Let p_n be the smallest prime divisor of n. If $d|n$ and $d < n$, then $d \leq \frac{n}{p_n}$.

In particular, any $\mathbb{F}_q$-affine space $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ of dimension $t > \frac{n}{p_n}$ is n-good.

Corollary

Let p_n be the smallest prime divisor of n, then for every $\mathbb{F}_q$-affine space $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ of dimension $t > n/p_n$ and every non trivial character χ of $\mathbb{F}_{q^n}$, we have that

$$\left| \sum_{a \in \mathcal{A}} \chi(a) \right| \leq nq^{t-1/2}.$$

Let p_n be the smallest prime divisor of n. If $d|n$ and $d < n$, then $d \leq \frac{n}{p_n}$.

In particular, any $\mathbb{F}_q$-affine space $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ of dimension $t > \frac{n}{p_n}$ is n-good.

Corollary

Let p_n be the smallest prime divisor of n, then for every $\mathbb{F}_q$-affine space $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ of dimension $t > n/p_n$ and every non trivial character χ of $\mathbb{F}_{q^n}$, we have that

$$\left|\sum_{a \in \mathcal{A}} \chi(a)\right| \leq nq^{t-1/2}.$$

Remark

Our bound is "nice" if n is fixed and $q \to +\infty$: we improved the trivial bound by $\frac{\sqrt{q}}{n}$.

Primitive elements

Recall that an element $\theta \in \mathbb{F}_{q^n}$ is primitive if it generates the cyclic group $\mathbb{F}_{q^n}^*$.

Recall that an element $\theta \in \mathbb{F}_{q^n}$ is primitive if it generates the cyclic group $\mathbb{F}_{q^n}^*$.
Vinogradov obtained the following formula for the indicator function of primitivity: for every $w \in \mathbb{F}_{q^n}$, we have that

$$\mathbb{I}_P(w) = \frac{\varphi(q^n-1)}{q^n-1} \sum_{d \mid q^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(w) = 1,$$

if and only if w is primitive. Otherwise, this sum equals 0.

Recall that an element $\theta \in \mathbb{F}_{q^n}$ is primitive if it generates the cyclic group $\mathbb{F}_{q^n}^*$.
Vinogradov obtained the following formula for the indicator function of primitivity: for every $w \in \mathbb{F}_{q^n}$, we have that

$$\mathbb{I}_P(w) = \frac{\varphi(q^n - 1)}{q^n - 1} \sum_{d | q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi) = d} \chi(w) = 1,$$

if and only if w is primitive. Otherwise, this sum equals 0.

1. $\varphi(t)$ is the Euler Totient function;
2. $\mu(t)$ is the Mobius function.

We obtain the following:

Proposition

Let n be a positive integer and $\varepsilon > 0$. Then there exists a constant $c = c(\varepsilon, n)$ such that for every $q > c$ and every n-good affine space $\mathcal{A} \subseteq \mathbb{F}_{q^n}$ of dimension $t \geq 1$, the number $\mathcal{P}(\mathcal{A})$ of primitive elements in $\mathcal{A}$ satisfies

$$\mathcal{P}(\mathcal{A}) \geq q^{t-\varepsilon}.$$

Proof.

Employing Vinogradov's formula, we obtain that

$$\begin{aligned} \frac{(q^n-1)\cdot\mathcal{P}(\mathcal{A})}{\varphi(q^n-1)} &= \sum_{a\in\mathcal{A}}\sum_{d\mid q^n-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(a) \\ &= \sum_{a\in\mathcal{A}}\chi_0(a)+\sum_{\substack{d\mid q^n-1\\ d\neq 1}}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)}\sum_{a\in\mathcal{A}}\chi(a). \end{aligned} \tag{5}$$

Proof.

Employing Vinogradov's formula, we obtain that

$$
\begin{aligned}
\frac{(q^n-1)\cdot\mathcal{P}(\mathcal{A})}{\varphi(q^n-1)} &= \sum_{a\in\mathcal{A}}\sum_{d\mid q^n-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(a) \\
&= \sum_{a\in\mathcal{A}}\chi_0(a)+\sum_{\substack{d\mid q^n-1\\ d\neq 1}}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)}\sum_{a\in\mathcal{A}}\chi(a).
\end{aligned} \tag{5}
$$

We have the bounds $\sum_{a\in\mathcal{A}}\chi_0(a)\geq q^t-1$ and $\left|\sum_{a\in\mathcal{A}}\chi(y)\right|\leq nq^{t-1/2}$

Proof.

Employing Vinogradov's formula, we obtain that

$$\begin{aligned}\frac{(q^n-1)\cdot\mathcal{P}(\mathcal{A})}{\varphi(q^n-1)} &= \sum_{a\in\mathcal{A}}\sum_{d|q^n-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(a) \\ &= \sum_{a\in\mathcal{A}}\chi_0(a) + \sum_{\substack{d|q^n-1\\ d\neq 1}}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)}\sum_{a\in\mathcal{A}}\chi(a).\end{aligned} \tag{5}$$

We have the bounds $\sum_{a\in\mathcal{A}}\chi_0(a)\geq q^t-1$ and $\left|\sum_{a\in\mathcal{A}}\chi(y)\right|\leq nq^{t-1/2}$, hence

$$\frac{(q^n-1)\cdot\mathcal{P}(\mathcal{A})}{\varphi(q^n-1)} > q^t - n\cdot W(q^n-1)\cdot q^{t-1/2}.$$

Proof.

Employing Vinogradov's formula, we obtain that

$$\begin{aligned}\frac{(q^n-1)\cdot\mathcal{P}(\mathcal{A})}{\varphi(q^n-1)} &= \sum_{a\in\mathcal{A}}\sum_{d\mid q^n-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(a)\\ &= \sum_{a\in\mathcal{A}}\chi_0(a)+\sum_{\substack{d\mid q^n-1\\ d\neq 1}}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)}\sum_{a\in\mathcal{A}}\chi(a).\end{aligned} \tag{5}$$

We have the bounds $\sum_{a\in\mathcal{A}}\chi_0(a)\geq q^t-1$ and $\left|\sum_{a\in\mathcal{A}}\chi(y)\right|\leq nq^{t-1/2}$, hence

$$\frac{(q^n-1)\cdot\mathcal{P}(\mathcal{A})}{\varphi(q^n-1)} > q^t - n\cdot W(q^n-1)\cdot q^{t-1/2}.$$

To finish, we observe that if n is fixed and q is large, $W(q^n-1)<q^{\varepsilon}$ and $\varphi(q^n-1)>q^{n-\varepsilon}$.

□

A general result

Remark

From now and on, all the results are asymptotic in the following way: n is **fixed** *and q is* **large***.*

A general result

Remark

From now and on, all the results are asymptotic in the following way: n is **fixed** *and q is* **large**.

Theorem

For each $n \geq 2$, and $q > c(n)$ is large enough, an $\mathbb{F}_q$-affine space $\mathcal{A} =\subseteq \mathbb{F}_{q^n}$ contains a primitive element if and only if one of the following holds:

1. *$\mathcal{A}$ is n-good;*
2. *there exists a primitive element $y \in \mathbb{F}_{q^n}$ and divisor $d < n$ of n such that*

$$y \in \mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}.$$

A general result

Remark

From now on, all the results are asymptotic in the following way: n is **fixed** *and q is* **large**.

Theorem

For each $n \geq 2$, and $q > c(n)$ is large enough, an $\mathbb{F}_q$-affine space $\mathcal{A} = \subseteq \mathbb{F}_{q^n}$ contains a primitive element if and only if one of the following holds:

1. *$\mathcal{A}$ is n-good;*
2. *there exists a primitive element $y \in \mathbb{F}_{q^n}$ and divisor $d < n$ of n such that*
$$y \in \mathcal{A} \subseteq y \cdot \mathbb{F}_{q^d}.$$

In particular, for q large, every $\mathcal{A}$ of dimension $t > \frac{n}{p_n}$ contains a primitive element.

Primitive elements with prescribed digits

Motivated by works of Mauduit and Rivat [11, 12] on the famous Gelfond Problems about digits over the integers, Dartyge and Sarkozy [7] introduced the notion of digits over finite fields.

Motivated by works of Mauduit and Rivat [11, 12] on the famous Gelfond Problems about digits over the integers, Dartyge and Sarkozy [7] introduced the notion of digits over finite fields.

Definition

If $\mathcal{B} = \{b_1, \dots, b_n\}$ is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$, then every $y \in \mathbb{F}_{q^n}$ is written uniquely as

$$y = \sum_{i=1}^{n} a_i b_i,$$

where $a_i \in \mathbb{F}_q$. The elements $a_1, \dots, a_n$ are called the *digits* of y with respect to the basis $\mathcal{B}$.

Motivated by works of Mauduit and Rivat [11, 12] on the famous Gelfond Problems about digits over the integers, Dartyge and Sarkozy [7] introduced the notion of digits over finite fields.

Definition

If $\mathcal{B} = \{b_1, \ldots, b_n\}$ is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$, then every $y \in \mathbb{F}_{q^n}$ is written uniquely as

$$y = \sum_{i=1}^{n} a_i b_i,$$

where $a_i \in \mathbb{F}_q$. The elements $a_1, \ldots, a_n$ are called the *digits* of y with respect to the basis $\mathcal{B}$.

Prescribing digits: $S = \{\sum_{i=1}^{n} a_i b_i : \ a_i = \mathbf{c_i} \in \mathbb{F}_q \text{ for } i = j_1, \ldots, j_k\}$.

Motivated by works of Mauduit and Rivat [11, 12] on the famous Gelfond Problems about digits over the integers, Dartyge and Sarkozy [7] introduced the notion of digits over finite fields.

Definition

If $\mathcal{B} = \{b_1, \ldots, b_n\}$ is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$, then every $y \in \mathbb{F}_{q^n}$ is written uniquely as

$$y = \sum_{i=1}^{n} a_i b_i,$$

where $a_i \in \mathbb{F}_q$. The elements $a_1, \ldots, a_n$ are called the *digits* of y with respect to the basis $\mathcal{B}$.

Prescribing digits: $S = \left\{\sum_{i=1}^{n} a_i b_i \,:\, a_i = \mathbf{c_i} \in \mathbb{F}_q \text{ for } i = j_1, \ldots, j_k\right\}.$

Many questions on the existence of special elements (squares, polynomial values, primitive elements, etc) with **prescribed digits** have been discussed: see [16] and the references therein.

Natural question:

Problem

For fixed n and large q, for what values of $k \leq n$ we can prescribe k digits of a primitive element in $\mathbb{F}_{q^n}$ (with respect to an arbitrary basis)?

Natural question:

Problem

For fixed n and large q, for what values of $k \leq n$ we can prescribe k digits of a primitive element in $\mathbb{F}_{q^n}$ (with respect to an arbitrary basis)?

In 2018, Swaenepoel [16] proved that any $k < n/2$ is admissible.

Natural question:

Problem

For fixed n and large q, for what values of $k \leq n$ we can prescribe k digits of a primitive element in $\mathbb{F}_{q^n}$ (with respect to an arbitrary basis)?

In 2018, Swaenepoel [16] proved that any $k < n/2$ is admissible.

If we prescribe k digits (in certain k positions in $\{1, \ldots, n\}$), the resulting set is an $\mathbb{F}_q$-affine space $\mathcal{A}$ of dimension $n-k$, that is n-**good** if

$$n - k > \frac{n}{p_n} \iff k \leq n - \frac{n}{p_n} - 1.$$

Natural question:

Problem

For fixed n and large q, for what values of $k \le n$ we can prescribe k digits of a primitive element in $\mathbb{F}_{q^n}$ (with respect to an arbitrary basis)?

In 2018, Swaenepoel [16] proved that any $k < n/2$ is admissible.

If we prescribe k digits (in certain k positions in $\{1, \dots, n\}$), the resulting set is an $\mathbb{F}_q$-affine space $\mathcal{A}$ of dimension $n-k$, that is n-**good** if

$$n - k > \frac{n}{p_n} \iff k \le n - \frac{n}{p_n} - 1.$$

1. n even: we just recover the range $k < n/2$;

Natural question:

Problem

For fixed n and large q, for what values of $k \leq n$ we can prescribe k digits of a primitive element in $\mathbb{F}_{q^n}$ (with respect to an arbitrary basis)?

In 2018, Swaenepoel [16] proved that any $k < n/2$ is admissible.

If we prescribe k digits (in certain k positions in $\{1, \ldots, n\}$), the resulting set is an $\mathbb{F}_q$-affine space $\mathcal{A}$ of dimension $n-k$, that is n-**good** if

$$n - k > \frac{n}{p_n} \iff k \leq n - \frac{n}{p_n} - 1.$$

1. n even: we just recover the range $k < n/2$;
2. for n odd, we have a significant improvement: $p_n = 3 \Rightarrow k < \frac{2n}{3}$

The bound $n - \frac{n}{p_n} - 1$ is **sharp**:

The bound $n - \frac{n}{p_n} - 1$ is **sharp**:

Let $\mathcal{B}_0 = \{b_1, \ldots, b_{n/p_n}\}$ an $\mathbb{F}_q$-basis for the field $\mathbb{F}_{q^{n/p_n}} \subseteq \mathbb{F}_{q^n}$ and extend it to an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$:

$$\mathcal{B} = \{b_1, \ldots, b_{n/p_n}, c_1, \ldots, c_{n-n/p_n}\}.$$

The bound $n - \frac{n}{p_n} - 1$ is **sharp**:

Let $\mathcal{B}_0 = \{b_1, \ldots, b_{n/p_n}\}$ an $\mathbb{F}_q$-basis for the field $\mathbb{F}_{q^{n/p_n}} \subseteq \mathbb{F}_{q^n}$ and extend it to an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$:

$$\mathcal{B} = \{b_1, \ldots, b_{n/p_n}, c_1, \ldots, c_{n-n/p_n}\}.$$

In particular, if we prescribe the last $n - n/p_n$ digits to be $= 0$, the corresponding elements are combinations of the b_i's, hence all lie in $\mathbb{F}_{q^{n/p_n}}$ and so none of them can be primitive!

Primitive k-normal elements

For $\beta \in \mathbb{F}_{q^n}$, let $\mathcal{V}_\beta$ be the $\mathbb{F}_q$-vector space generated by the $\mathbb{F}_q$-conjugates of β:

$$\beta, \beta^q, \ldots, \beta^{q^{n-1}},$$

and let $d(\beta)$ be the dimension of $\mathcal{V}_\beta$.

For $\beta \in \mathbb{F}_{q^n}$, let $\mathcal{V}_\beta$ be the $\mathbb{F}_q$-vector space generated by the $\mathbb{F}_q$-conjugates of β:

$$\beta, \beta^q, \dots, \beta^{q^{n-1}},$$

and let $d(\beta)$ be the dimension of $\mathcal{V}_\beta$.

An element $\beta \in \mathbb{F}_{q^n}$ is **normal** over $\mathbb{F}_q$ if $d(\beta) = n$, i.e., $\mathcal{V}_\beta$ is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$.

For $\beta \in \mathbb{F}_{q^n}$, let $\mathcal{V}_\beta$ be the $\mathbb{F}_q$-vector space generated by the $\mathbb{F}_q$-conjugates of β:

$$\beta, \beta^q, \dots, \beta^{q^{n-1}},$$

and let $d(\beta)$ be the dimension of $\mathcal{V}_\beta$.

An element $\beta \in \mathbb{F}_{q^n}$ is **normal** over $\mathbb{F}_q$ if $d(\beta) = n$, i.e., $\mathcal{V}_\beta$ is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$.

The Primitive Normal Basis Theorem (PNBT) ensures the existence of an element $\beta \in \mathbb{F}_{q^n}$ that is **primitive and normal** for every $q \geq 2$ and every $n \geq 1$.

For $\beta \in \mathbb{F}_{q^n}$, let $\mathcal{V}_\beta$ be the $\mathbb{F}_q$-vector space generated by the $\mathbb{F}_q$-conjugates of β:

$$\beta, \beta^q, \ldots, \beta^{q^{n-1}},$$

and let $d(\beta)$ be the dimension of $\mathcal{V}_\beta$.

An element $\beta \in \mathbb{F}_{q^n}$ is **normal** over $\mathbb{F}_q$ if $d(\beta) = n$, i.e., $\mathcal{V}_\beta$ is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$.

The Primitive Normal Basis Theorem (PNBT) ensures the existence of an element $\beta \in \mathbb{F}_{q^n}$ that is **primitive and normal** for every $q \geq 2$ and every $n \geq 1$.

First proof by Lenstra and Schoof [10] (1987),

For $\beta \in \mathbb{F}_{q^n}$, let $\mathcal{V}_\beta$ be the $\mathbb{F}_q$-vector space generated by the $\mathbb{F}_q$-conjugates of β:

$$\beta, \beta^q, \ldots, \beta^{q^{n-1}},$$

and let $d(\beta)$ be the dimension of $\mathcal{V}_\beta$.

An element $\beta \in \mathbb{F}_{q^n}$ is **normal** over $\mathbb{F}_q$ if $d(\beta) = n$, i.e., $\mathcal{V}_\beta$ is an $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$.

The Primitive Normal Basis Theorem (PNBT) ensures the existence of an element $\beta \in \mathbb{F}_{q^n}$ that is **primitive and normal** for every $q \geq 2$ and every $n \geq 1$.

First proof by Lenstra and Schoof [10] (1987), computer-free proof was later given by Cohen and Huczynska [6] (2003).

Following the concept of normal elements, Huczynska, Mullen, Panario and Thomson [8] introduced the notion of k-normal elements:

$\beta \in \mathbb{F}_{q^n}$ is k-**normal** over $\mathbb{F}_q$ if $d(\beta) = n - k$.

Following the concept of normal elements, Huczynska, Mullen, Panario and Thomson [8] introduced the notion of k-normal elements:

$\beta \in \mathbb{F}_{q^n}$ is k-**normal** over $\mathbb{F}_q$ if $d(\beta) = n - k$.

In this context, 0-normal elements are the original normal elements and $0 \in \mathbb{F}_{q^n}$ is the unique n-normal element.

Following the concept of normal elements, Huczynska, Mullen, Panario and Thomson [8] introduced the notion of k-normal elements:

$\beta \in \mathbb{F}_{q^n}$ is k-**normal** over $\mathbb{F}_q$ if $d(\beta) = n - k$.

In this context, 0-normal elements are the original normal elements and $0 \in \mathbb{F}_{q^n}$ is the unique n-normal element.

Motivated by the PNBT, they proposed a challenging problem (see Problem 6.3 in [8]).

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Some basic tools

Lemma

For each element $\alpha \in \mathbb{F}_{q^n}$, *the set of polynomials* $g(x) = \sum_{i=0}^{t} a_i x^i \in \mathbb{F}_q[x]$ *such that*

$$0 = g \circ \alpha := \sum_{i=0}^{t} a_i \alpha^{q^i},$$

is an ideal of $\mathbb{F}_q[x]$. *This ideal is generated by a monic polynomial* $m_{\alpha,q}(x)$, *the* $\mathbb{F}_q$*-order of* α. *Moreover, the following hold:*

Some basic tools

Lemma

For each element $\alpha \in \mathbb{F}_{q^n}$*, the set of polynomials* $g(x) = \sum_{i=0}^{t} a_i x^i \in \mathbb{F}_q[x]$ *such that*

$$0 = g \circ \alpha := \sum_{i=0}^{t} a_i \alpha^{q^i},$$

is an ideal of $\mathbb{F}_q[x]$*. This ideal is generated by a monic polynomial* $m_{\alpha,q}(x)$*, the* $\mathbb{F}_q$*-order of* α*. Moreover, the following hold:*

1. $m_{\alpha,q}$ *is a divisor of* $x^n - 1$*;*

Some basic tools

Lemma

For each element $\alpha \in \mathbb{F}_{q^n}$, *the set of polynomials* $g(x) = \sum_{i=0}^{t} a_i x^i \in \mathbb{F}_q[x]$ *such that*

$$0 = g \circ \alpha := \sum_{i=0}^{t} a_i \alpha^{q^i},$$

is an ideal of $\mathbb{F}_q[x]$. *This ideal is generated by a monic polynomial* $m_{\alpha,q}(x)$, *the* $\mathbb{F}_q$*-order of* α. *Moreover, the following hold:*

1. $m_{\alpha,q}$ *is a divisor of* $x^n - 1$;
2. α *is k-normal over* $\mathbb{F}_q$ *if and only if* $m_{\alpha,q}(x)$ *has degree* $n - k$.

Some remarks

Problem

Determine the pairs (n, k) *such that there exist primitive* k*-normal elements in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$*.*

Some remarks

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Observe that k-normals (not necessarily primitive) exist if and only if $x^n - 1$ admits a k-degree divisor over $\mathbb{F}_q$:

Some remarks

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Observe that k-normals (not necessarily primitive) exist if and only if $x^n - 1$ admits a k-degree divisor over $\mathbb{F}_q$: this is always ensured only for $k = 0, 1, n-1, n$ ([8]).

Some remarks

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Observe that k-normals (not necessarily primitive) exist if and only if $x^n - 1$ admits a k-degree divisor over $\mathbb{F}_q$: this is always ensured only for $k = 0, 1, n-1, n$ ([8]).

1. Case $k = 0$ of the problem is the PNBT.

Some remarks

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Observe that k-normals (not necessarily primitive) exist if and only if $x^n - 1$ admits a k-degree divisor over $\mathbb{F}_q$: this is always ensured only for $k = 0, 1, n-1, n$ ([8]).

1. Case $k = 0$ of the problem is the PNBT.
2. Positive answer for $k = 1$ (R., Thomson [14]).

Some remarks

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Observe that k-normals (not necessarily primitive) exist if and only if $x^n - 1$ admits a k-degree divisor over $\mathbb{F}_q$: this is always ensured only for $k = 0, 1, n-1, n$ ([8]).

1. Case $k = 0$ of the problem is the PNBT.
2. Positive answer for $k = 1$ (R., Thomson [14]).
3. Negative answer for $k = n, n-1$ ([8]).

Some remarks

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Observe that k-normals (not necessarily primitive) exist if and only if $x^n - 1$ admits a k-degree divisor over $\mathbb{F}_q$: this is always ensured only for $k = 0, 1, n-1, n$ ([8]).

1. Case $k = 0$ of the problem is the PNBT.
2. Positive answer for $k = 1$ (R., Thomson [14]).
3. Negative answer for $k = n, n-1$ ([8]).

Techniques employed so far: Vinogradov's formula + additive character sums for k-normality.

Problem

Determine the pairs (n, k) *such that there exist primitive* k*-normal elements in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$*.*

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Assuming that k-normal elements actually exist.

Theorem (R., [15])

If n is fixed and q is large, we have positive answer provided that $0 \leq k < n/2$ and k-normal elements exist in $\mathbb{F}_q$.

Problem

Determine the pairs (n, k) such that there exist primitive k-normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Assuming that k-normal elements actually exist.

Theorem (R., [15])

If n is fixed and q is large, we have positive answer provided that $0 \leq k < n/2$ and k-normal elements exist in $\mathbb{F}_q$.

It is sharp for $n = 4$ and $q \equiv 3 \pmod 4$: no 2-normal element in $\mathbb{F}_{q^4}$ is primitive.

The non existence of primitive k-normal elements if $k = n - 1$ ([8]) or $(n, k) = (4, 2)$ and $q \equiv 3 \pmod 4$ ([15]), use the fact that the $\mathbb{F}_q$-order of such elements are **binomials**.

The non existence of primitive k-normal elements if $k = n - 1$ ([8]) or $(n, k) = (4, 2)$ and $q \equiv 3 \pmod 4$ ([15]), use the fact that the $\mathbb{F}_q$-order of such elements are **binomials**. This is extended as follows:

The non existence of primitive k-normal elements if $k = n - 1$ ([8]) or $(n, k) = (4, 2)$ and $q \equiv 3 \pmod 4$ ([15]), use the fact that the $\mathbb{F}_q$-order of such elements are **binomials**.This is extended as follows:

Lemma

Suppose that the $\mathbb{F}_q$-order of α divides a binomial $x^d - \delta \in \mathbb{F}_q[x]$ with $d < n$. Then α cannot be a primitive element of $\mathbb{F}_{q^n}$.

The non existence of primitive k-normal elements if $k = n - 1$ ([8]) or $(n, k) = (4, 2)$ and $q \equiv 3 \pmod 4$ ([15]), use the fact that the $\mathbb{F}_q$-order of such elements are **binomials**.This is extended as follows:

Lemma

Suppose that the $\mathbb{F}_q$-order of α divides a binomial $x^d - \delta \in \mathbb{F}_q[x]$ with $d < n$. Then α cannot be a primitive element of $\mathbb{F}_{q^n}$.

Proof.

$$\alpha^{q^d} - \delta\alpha = (x^d - \delta) \circ \alpha = 0 \Rightarrow \alpha^{(q^d-1)(q-1)} = 1.$$

And $(q^d - 1)(q - 1) < q^n - 1$ for every $d < n$. □

Motivated by the previous result, we have the following definition:

Definition

An element $\alpha \in \mathbb{F}_{q^n}$ is **free of binomials** if its $\mathbb{F}_q$-order $m_{\alpha,q}(x)$ does not divide any binomial in $\mathbb{F}_q[x]$ of degree $< n$. .

Motivated by the previous result, we have the following definition:

Definition

An element $\alpha \in \mathbb{F}_{q^n}$ is **free of binomials** if its $\mathbb{F}_q$-order $m_{\alpha,q}(x)$ does not divide any binomial in $\mathbb{F}_q[x]$ of degree $< n$. .

So the existence of a k-normal element, free of binomials, is necessary.

For fixed n, and q large, this is also sufficient!

For fixed n, and q large, this is also sufficient!

Theorem

Let $n \geq 2$ be a positive integer. Then there exists a constant $c(n) > 0$ such that, for every $q > c(n)$ and every $0 \leq k \leq n-2$, the following are equivalent:

1. *there exists a k-normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ that is free of binomials;*
2. *there exists a k-normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ that is primitive.*

Proof.

We have proved (2)$\to$ (1).

Proof.

We have proved (2)$\to$ (1).

Sketch of the proof of (1)$\to$ (2): let α be a k-normal element free of binomials.

Proof.

We have proved (2)→ (1).

Sketch of the proof of (1)→ (2): let α be a k-normal element free of binomials.

1. Let $\mathcal{A}_\alpha \subseteq \mathbb{F}_{q^n}$ be the $\mathbb{F}_q$-vector space generated by all the conjugates of α: $\mathcal{A}_\alpha$ has dimension $n-k$.

Proof.

We have proved (2)$\rightarrow$ (1).

Sketch of the proof of (1)$\rightarrow$ (2): let α be a k-normal element free of binomials.

1. Let $\mathcal{A}_\alpha \subseteq \mathbb{F}_{q^n}$ be the $\mathbb{F}_q$-vector space generated by all the conjugates of α: $\mathcal{A}_\alpha$ has dimension $n-k$.
2. α is free of binomials $\Rightarrow \alpha^{-1} \cdot \alpha^q = \alpha^{q-1}$ has degree n over $\mathbb{F}_q$.

Proof.

We have proved (2)$\rightarrow$ (1).

Sketch of the proof of (1)$\rightarrow$ (2): let α be a k-normal element free of binomials.

1. Let $\mathcal{A}_\alpha \subseteq \mathbb{F}_{q^n}$ be the $\mathbb{F}_q$-vector space generated by all the conjugates of α: $\mathcal{A}_\alpha$ has dimension $n-k$.
2. α is free of binomials $\Rightarrow \alpha^{-1}\cdot\alpha^q=\alpha^{q-1}$ has degree n over $\mathbb{F}_q$.
3. Conclusion: $\mathcal{A}_\alpha$ is n-good!

Proof.

We have proved (2)$\rightarrow$ (1).

Sketch of the proof of (1)$\rightarrow$ (2): let α be a k-normal element free of binomials.

1. Let $\mathcal{A}_\alpha \subseteq \mathbb{F}_{q^n}$ be the $\mathbb{F}_q$-vector space generated by all the conjugates of α: $\mathcal{A}_\alpha$ has dimension $n-k$.
2. α is free of binomials $\Rightarrow \alpha^{-1}\cdot\alpha^q = \alpha^{q-1}$ has degree n over $\mathbb{F}_q$.
3. Conclusion: $\mathcal{A}_\alpha$ is n-good!
4. For q large, it contains at least $q^{n-k-1/2}$ primitive elements.

Proof.

We have proved (2)$\rightarrow$ (1).

Sketch of the proof of (1)$\rightarrow$ (2): let α be a k-normal element free of binomials.

1. Let $\mathcal{A}_\alpha \subseteq \mathbb{F}_{q^n}$ be the $\mathbb{F}_q$-vector space generated by all the conjugates of α: $\mathcal{A}_\alpha$ has dimension $n-k$.
2. α is free of binomials $\Rightarrow \alpha^{-1} \cdot \alpha^q = \alpha^{q-1}$ has degree n over $\mathbb{F}_q$.
3. Conclusion: $\mathcal{A}_\alpha$ is n-good!
4. For q large, it contains at least $q^{n-k-1/2}$ primitive elements.
5. For q large, the number of elements in $\mathcal{A}_\alpha$ that are not k-normal is $< q^{n-k-1/2}$: it suffices to take $q > 4^n$.

□

A natural question:

Problem

Determine the pairs (n, k) such that $x^n - 1$ has a divisor $f \in \mathbb{F}_q[x]$ of degree k that does not divide any binomial of degree $< n$.

A natural question:

Problem

Determine the pairs (n, k) such that $x^n - 1$ has a divisor $f \in \mathbb{F}_q[x]$ of degree k that does not divide any binomial of degree $< n$.

Example: $n = p$, the characteristic of $\mathbb{F}_q$ and $0 \leq k \leq p - 2$.

A natural question:

Problem

Determine the pairs (n, k) *such that* $x^n - 1$ *has a divisor* $f \in \mathbb{F}_q[x]$ *of degree* k *that does not divide any binomial of degree* $< n$.

Example: $n = p$, the characteristic of $\mathbb{F}_q$ and $0 \leq k \leq p - 2$.

In particular, for q large, there exist primitive $(p-2)$-normal elements in $\mathbb{F}_{q^p}$ (not expected).

[1] D.A. Burgess.
Character sums and primitive roots in finite fields.
Proc. London Math. Soc. (3) 37: 11–35, 1967.

[2] D.A. Burgess.
A note on character sums over finite fields.
J. Reine Angew. Math. 255: 80–82, 1972.

[3] M. C. Chang.
On a question of Davenport and Lewis and new character sum bounds in finite fields.
Duke Math. J. 145(3): 409–442, 2008.

[4] M. C. Chang.
Character Sums in Finite Fields.
in *Finite Fields: Theory and Applications* (Am. Math. Soc., Providence, RI): 83–98, 2010.

[5] P. Charpin, A. Pott, A. Winterhof.
Finite Fields and Their Applications - Character Sums and Polynomials.
De Grutyer, Radon Series on Computational and applied mathematics (11), 2013.

[6] S. D. Cohen and S. Huczynska.
The primitive normal basis theorem – without a computer.
J. London Math. Soc., 67(1):41–56, 2003.

[7] C. Dartyge, A. Sárközy.
The sum of digits function in finite fields.
Proc. Amer. Math. Soc. 141: 4119–4124, 2013.

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

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

[10] H. W. Lenstra Jr. and R. J. Schoof.
Primitive normal bases for finite fields.
Math. Comp., 48(177):217–231, 1987.

[11] C. Mauduit, J. Rivat.
La somme des chiffres des carrés.
Acta Math. 203 (1): 107–148, 2009.

[12] C. Mauduit and J. Rivat.
Sur un probléme de Gelfond: la somme des chiffres des nombres premiers.
Ann. of Math. 171 (3): 1591–1646, 2010.

[13] C. Pomerance, L. Thompson, A. Weingartner.
On integers n for which $x^n - 1$ has a divisor of every degree.
Acta Arith. 175: 225–243, 2016.

[14] L. Reis, D. Thomson.
Existence of primitive 1-normal elements in finite fields
Finite Fields Appl. 51: 238–269, 2018.

[15] L. Reis.
Existence results on k-normal elements over finite fields.
Rev. Mat. Iberoam. 35: 805–822, 2019.

[16] C. Swaenepoel.
Prescribing digits in finite fields.
J. Number Theory 189: 97–114, 2018.

[17] L. Thompson.
On the divisors of $x^n - 1$ in $\mathbb{F}_p[x]$.
Int. J. Number Theory 9: 421–430, 2013.

Obrigado! Thank you!