Variations of the Primitive Normal Basis Theorem

Giorgos Kapetanakis

Joint work with Lucas Reis

Antalya Algebra Days XX - May 2018

Sabancı University

Supported by TÜBİTAK Project No. 114F432

Motivation

Definitions

- Let $\mathbf{F}_q$ be the finite field of q elements, where q is a power of the prime p and let $n \geq 1$.
- $\mathbf{F}_{q^n}^*$ is cyclic and any generator of this group is called primitive.
- $\mathbf{F}_{q^n}$ is an $\mathbf{F}_q$-vector space of dimension n and $\alpha \in \mathbf{F}_{q^n}$ is normal over $\mathbf{F}_q$ if $\mathcal{B} = \{\alpha, \ldots, \alpha^{q^{n-1}}\}$ is an $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$ and $\mathcal{B}$ is a normal basis
- The Primitive Normal Basis Theorem states that there exists a normal basis composed by primitive elements in any finite field extension.
- Lenstra and Schoof (1987) proved this, while Cohen and Huczynska (2003) gave a computer-free proof.

Introducing k-normal elements

A variation of normal elements was recently introduced by Huczynska et al. (2013).

Definition

For $\alpha \in \mathbf{F}_{q^n}$, consider the set $S_\alpha = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$. Then α is k-normal over $\mathbf{F}_q$ if the $\mathbf{F}_q$-vector space $V_\alpha = \langle S_\alpha \rangle$ has co-dimension k.

- Following this definition, 0-normal elements are the usual normal elements and $0 \in \mathbf{F}_{q^n}$ is the only n-normal element.

Additive order of elements

- For $f \in \mathbf{F}_q[x]$, $f = \sum_{i=0}^{s} a_i x^i$ and $\alpha \in \mathbf{F}_{q^n}$, define $f \circ \alpha = \sum_{i=0}^{s} a_i \alpha^{q^i}$.
- For $\alpha \in \mathbf{F}_{q^n}$, set $\mathcal{I}_\alpha := \{g \in \mathbf{F}_q[x] \mid g \circ \alpha = 0\}$, a non-zero ideal of $\mathbf{F}_q[x]$. Denote by m_α its unique monic generator and call it $\mathbf{F}_q$-order of α.
- For $\alpha \in \mathbf{F}_{q^n}$, $m_\alpha(x) \mid x^n - 1$.

There is a connection between k-normal elements and their $\mathbf{F}_q$-order.

Proposition (Huczynska-Mullen-Panario-Thomson)

Let $\alpha \in \mathbf{F}_{q^n}$. Then α is k-normal if and only if $m_\alpha(x)$ has degree $n - k$.

Previous work on k-normal elements

- Reis has several results about k-normal elements.
- Alizadeh (2017) characterized k-normal elements and gave a recursive construction of 1-normal polynomials.
- Tilenbaev, Saygı and Ürtiş (2017) gave a formula for the number of k-normal elements.
- Reis and Thomson (2018) proved the existence of primitive 1-normal elements of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, for odd q and $n \geq 3$.

Introducing r-primitive elements

Definition

Let $r \mid q^n - 1$. Some $\alpha \in \mathbf{F}_{q^n}^*$ is r-primitive if $\mathrm{ord}(\alpha) = \frac{q^n-1}{r}$, where $\mathrm{ord}(\alpha)$ stands for the multiplicative order of α.

- The 1-primitive elements correspond to the primitive elements in the usual sense.
- For every $r \mid q^n - 1$, there exist exactly $\varphi(r)$ r-primitive elements.

The Anderson-Mullen conjecture

Motivated by the Primitive Normal Basis Theorem, Anderson and Mullen (2014) propose the following.

Conjecture (Anderson-Mullen)

Suppose $p \geq 5$ is a prime and $n \geq 3$. Then for $a = 1, 2$ and $k = 0, 1$ there exists some k-normal element $\alpha \in \mathbf{F}_{p^n}$ with multiplicative order $(p^n - 1)/a$.

- The case $(a, k) = (1, 0)$ is the Primitive Normal Basis Theorem and the case $(a, k) = (1, 1)$ was recently proved by Reis and Thomson (2018).
- In this work, we complete the proof and also consider the missing cases $p = 3$ and $n = 2$.

Preliminaries

Freeness

Definition

1. If m divides $q^n - 1$, an element $\alpha \in \mathbf{F}_{q^n}^*$ is *m-free* if $\alpha = \beta^d$ for any divisor d of m implies $d = 1$.
2. If $m \in \mathbf{F}_q[x]$ divides $x^n - 1$, an element $\alpha \in \mathbf{F}_{q^n}$ is *m-free* if $\alpha = h \circ \beta$ for any divisor h of m implies $h = 1$.

- Primitive elements correspond to the $(q^n - 1)$-free elements.
- Normal elements correspond to the $(x^n - 1)$-free elements.

Characterizing 1-normal elements

Proposition

Let q be a power of a prime p and $n = p^k u$, where $k \geq 0$ and $\gcd(u,p) = 1$. Write $T(x) = \frac{x^u - 1}{x-1}$. Then $\alpha \in \mathbf{F}_{q^n}$ is such that $m_\alpha(x) = \frac{x^n - 1}{x-1}$ if and only if α is $T(x)$-free and $\mathrm{Tr}_{q^n/q^{p^k}}(\alpha) = \beta$, where β is such that $m_\beta(x) = \frac{x^{p^k} - 1}{x-1}$.

In the case when $p^2 \mid n$, we have an alternative characterization for such 1-normal elements.

Proposition

Suppose that $n = p^2 s$ and let $\alpha \in \mathbf{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q^{ps}}(\alpha) = \beta$. Then $m_\alpha = \frac{x^n - 1}{x-1}$ if and only if $m_\beta = \frac{x^{ps} - 1}{x-1}$.

Characteristic functions

We are interested in the characteristic functions of the properties. Vinogradov's formula is an expression of the above that involves characters.

1. For $w \in \mathbf{F}_{q^n}^*$ and t be a positive divisor of $q^n - 1$,

$$\omega_t(w) = \theta(t) \sum_{d|t} \frac{\mu(t)}{\varphi(t)} \sum_{\operatorname{ord} \chi = t} \chi(w) = \begin{cases} 1, & \text{if } w \text{ is } t\text{-free,} \\ 0, & \text{otherwise.} \end{cases}$$

2. For $w \in \mathbf{F}_{q^n}$ and D be a monic divisor of $x^n - 1$,

$$\Omega_D(w) = \Theta(D) \sum_{E|D} \frac{\mu(D)}{\varphi(D)} \sum_{\operatorname{ord} \psi = D} \psi(w) = \begin{cases} 1, & \text{if } w \text{ is } D\text{-free,} \\ 0, & \text{otherwise.} \end{cases}$$

Characteristic function for traces

For any divisor m of n, $\mathbf{F}_{q^m}$ is a subfield of $\mathbf{F}_{q^n}$. Let

$$T_{m,\beta}(w) = \begin{cases} 1, & \text{if } \mathrm{Tr}_{q^n/q^m}(w) = \beta, \\ 0, & \text{otherwise.} \end{cases}$$

We need a character sum formula for $T_{m,\beta}$. The orthogonality relations yield:

$$T_{m,\beta}(w) = \frac{1}{q^m} \sum_{\psi \in \widehat{\mathbf{F}_{q^m}}} \widetilde{\psi}(w)\overline{\psi}(\beta),$$

where $\widetilde{\psi}(w) = \psi(\mathrm{Tr}_{q^n/q^m}(w))$ is the lift of ψ and $\overline{\psi}$ is the inverse of ψ.

Sufficient conditions

The quantities we are interested in

1. Let $\mathcal{N}(r, f, m, \beta)$ be the number of primitive elements $w \in \mathbf{F}_{q^n}$ such that w^r is f-free and $\mathrm{Tr}_{q^n/q^m}(w^r) = \beta$. Then

$$\mathcal{N}(r, f, m, \beta) = \sum_{w \in \mathbf{F}_{q^n}} \Omega_f(w^r) T_{m,\beta}(w^r) \omega_{q^n-1}(w).$$

2. Let $\mathcal{N}(r)$ be the number of primitive elements $w \in \mathbf{F}_{q^n}$ such that w^r is normal. Then

$$\mathcal{N}(r) = \sum_{w \in \mathbf{F}_{q^n}} \Omega_{x^n-1}(w^r) \omega_{q^n-1}(w).$$

Inequality conditions

Let $W(t)$ be the number of square-free factors of t. By using exponential sums, we prove the following:

Proposition

Write $n = p^t u$, *where* $\gcd(u, p) = 1$ *and* $t \geq 0$.

(a) *If* $q^{p^t(u/2-1)} > W(q^n - 1)W(x^u - 1)$ *there exist* 2*-primitive,* 1*-normal elements in* $\mathbf{F}_{q^n}$.

(b) *If* $q^{n/2} > 2W(q^n - 1)W(x^u - 1)$ *there exist* 2*-primitive, normal elements in* $\mathbf{F}_{q^n}$.

(c) *If* $t \geq 1$, $q^{n/2-n/p} > 2W(q^n - 1)$ *and* $\beta \in \mathbf{F}_{q^{n/p}}$, *there exists a* 2*-primitive element* $\alpha \in \mathbf{F}_{q^n}$, *with* $\mathrm{Tr}_{q^n/q^{n/p}}(\alpha) = \beta$.

A special case

Remark

The first inequality of the last proposition is always false for $n = p, 2p$. For these cases, we employ a refinement of our main result, using simple combinatorial arguments.

Inequality checking methods

Lemma

Let t, a be positive integers and let $p_1, \ldots, p_j$ be the distinct prime divisors of t such that $p_i \leq 2^a$. Then $W(t) \leq c_{t,a} t^{1/a}$, where

$$c_{t,a} = \frac{2^j}{(p_1 \cdots p_j)^{1/a}}.$$

In particular, for $c_t := c_{t,4}$ and $d_t := c_{t,8}$ we have the bounds $c_t < 4.9$ and $d_t < 4514.7$ for every positive integer t.

Estimates for $W(t)$, t polynomial

Lemma (Lenstra-Schoof)

For every positive integer n, $W(x^n - 1) \leq 2^{(\gcd(n,q-1)+n)/2}$. Additionally, the bound $W(x^n - 1) \leq 2^{s(n)}$ holds in the following cases:

1. $s(n) = \frac{\min\{n,q-1\}+n}{2}$ *for every q,*
2. $s(n) = \frac{n+4}{3}$ *for $q = 3$ and $u \neq 4, 8, 16$,*
3. $s(n) = \frac{n}{3} + 6$ *for $q = 5$.*

Outline of our method

Next, we explore the pairs (q, n) satisfying the above inequalities. Our method is based on two main steps.

Step 1. Use the bounds for $W(q^n - 1)$ and $W(x^u - 1)$. After this point, only a finite number of pairs (q, n) does not satisfy the inequalities.

Step 2. Check the inequalities by direct computations. After this step, the remaining pairs that do not satisfy the inequalities have small q and n.

For all our computations, the SageMath software was used.

2-primitive, normal elements

For this case, the condition is

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

We prove it to hold for all but 68 pairs (q, n), where q is any odd prime power and $n \geq 3$.

2-primitive elements with prescribed trace

This case is useful for the 2-primitive, 1-normal case, when $p^2 \mid n$. The resulting inequality to check is

$$q^{n_0(p^2/2-p)} > 2W(q^{p^2 n_0} - 1),$$

where $n = p^2 n_0$. This is true for all but 6 pairs (q, n), where q is any power of some odd prime p and $p^2 \mid n$.

2-primitive, 1-normal elements

Write $n = p^t \cdot u$ with $\gcd(p, u) = 1$. We are interested in the cases $t < 2$. The resulting inequality is

$$q^{p^t(u/2-1)} > W(q^n - 1)W(x^u - 1).$$

We consider the cases:

1. $t = 0$: We prove the above inequality for all but 483 pairs (q, n), where q may be any odd prime power and $n \geq 4$.
2. $t = 1$, $u \geq 3$: We prove the validity of the inequality for all but 7 pairs (q, n).
3. $n = p, 2p$: We prove the existence of 2-primitive, 1-normal elements, with the exception of 3 pairs (q, n), where $p \neq 5$ if $n = p$.

Completion of the proofs

The cases $n = 2, 3$

The proof of the following is elementary.

Lemma

If $q > 3$ is an odd prime power, then all 2-primitive $c \in \mathbf{F}_{q^2}$ are normal over $\mathbf{F}_q$. In contrast, all 2-primitive elements of $\mathbf{F}_{3^2}$ are 1-normal over $\mathbf{F}_3$.

Based on Cohen's (1990) results about primitive elements with prescribed trace, we prove the following.

Proposition

Let q be a power of an odd prime. Then there exists a 2-primitive, 1-normal element in $\mathbf{F}_{q^3}$ over $\mathbf{F}_q$.

The main result

Next, we write a script that verifies the pairs (q, n) that were not dealt with theoretically. This completes our proof.

Theorem

Let q be a power of an odd prime p and $n \geq 2$.

1. *There exists some $\alpha \in \mathbf{F}_{q^n}$ that is simultaneously 2-primitive and normal over $\mathbf{F}_q$, unless $(q, n) = (3, 2), (3, 4)$.*
2. *If $n \geq 3$, there exists some $\alpha \in \mathbf{F}_{q^n}$ that is simultaneously 2-primitive and 1-normal over $\mathbf{F}_q$. Such an element exists also in the case $(q, n) = (3, 2)$ and it does not exist when $n = 2$ and $q > 3$.*

A by-product

- Following our proof, all 2-primitive, 1-normal elements that we theoretically proved to exist when $n \geq 3$, are zero-traced over $\mathbf{F}_q$.
- For the remaining pairs (q, n), we verify by computer the existence of zero-traced 2-primitive, 1-normal of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. So we have proved the following.

Theorem

Let q be a power of an odd prime and let $n \geq 3$ be a positive integer. Then there exists a 2-primitive, 1-normal element $\alpha \in \mathbf{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q}(\alpha) = 0$.

This work is available at:

`arXiv:1712.09861 [math.NT]`

Thank You!