On the existence of primitive completely normal bases of finite fields

Giorgos Kapetanakis
(Joint work with Theodoulos Garefalakis)

1^{st} Congress of Greek Mathematicians - June, 2018

Sabancı University

Motivation

Let $\mathbf{F}_q$ be the finite field of cardinality q and $\mathbf{F}_{q^n}$ its extension of degree n, where q is a power of the prime p.

- A generator of $(\mathbf{F}_{q^n}^*, \cdot)$ is called *primitive*.
- An $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$ of the form $\{x, x^q, \dots, x^{q^{n-1}}\}$ is called *normal* and $x \in \mathbf{F}_{q^n}$ *normal over* $\mathbf{F}_q$.
- It is well-known that primitive and normal elements exist for every q and n.

The primitive normal basis theorem

Theorem (Primitive normal basis theorem)

Let q be a prime power and $n \in \mathbf{N}$. There exists some $x \in \mathbf{F}_{q^n}$ that is simultaneously primitive and normal over $\mathbf{F}_q$.

- Lenstra and Schoof (1987) provided the first proof.
- Cohen and Huczynska (2003) provided a computer-free proof with the introduction of sieving techniques.
- Several generalizations have been investigated (Cohen-Hachenberger 1999, Cohen-Huczynska 2010, Hsu-Nan 2011, K. 2013, K. 2014).

The completely normal basis theorem

An element of $\mathbf{F}_{q^n}$ that is simultaneously normal over $\mathbf{F}_{q^l}$ for all $l \mid n$ is called *completely normal over* $\mathbf{F}_q$.

Theorem (Completely normal basis theorem)

For every q and n, there exists a completely normal element of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.

- Initially proved by Blessenohl and Johnsen (1986).
- Hachenberger (1994) gave a simplified proof.

The Morgan-Mullen conjecture

Motivated by the primitive normal basis theorem, Morgan and Mullen conjectured the following:

Conjecture (Morgan-Mullen, 1996)

Let q be a prime power and n a positive integer. There exists some $x \in \mathbf{F}_{q^n}$ that is simultaneously primitive and completely normal over $\mathbf{F}_q$.

Known results

- Morgan and Mullen (1996) gave examples for $q \leq 97$ and $q^n < 10^{50}$ by computer search.
- Hachenberger (1997) characterized *completely basic* extensions, that is extensions, that every normal element is also completely normal.
- Hachenberger (2001) settled the case when $\mathbf{F}_{q^n}$ is a regular extension over $\mathbf{F}_q$, given that $4 \mid (q-1)$, q odd and n even. $\mathbf{F}_{q^n}$ is a *regular extension over* $\mathbf{F}_q$ if n and $\mathrm{ord}_{v(n')}(q)$ are co-prime, where $v(n')$ is the square-free part of the p-free part of n.

Known results

- Blessenohl (2005) settled the case $n = 2^l$, $n \mid (q^2 - 1)$, $l \geq 3$ and $q \equiv 3 \pmod 4$.
- Hachenberger (2010) provided lower bounds for the number of primitive and completely normal elements when n is a prime power.
- Hachenberger (2012) extended his results to all regular extensions.

Known results

Recently, with elementary methods, the following was shown.

Theorem (Hachenberger, 2016)

1. *Assume that* $q \geq n^{7/2}$ *and* $n \geq 7$*. Then* $\mathrm{PCN}_q(n) > 0$.
2. *If* $q \geq n^3$ *and* $n \geq 37$*, then* $\mathrm{PCN}_q(n) > 0$.

Remark

The conjecture is still open

Our contribution

In this work, we employ character sum techniques and prove the following.

Theorem (Garefalakis-K.)

Let $n \in \mathbf{N}$ *and* q *a power of the prime* p*, such that* $q > m$*, where* $n = p^\ell m$ *and* $\gcd(p, m) = 1$*. Then* $\mathrm{PCN}_q(n) > 0$*.*

Preliminaries

Module structure

- $(\mathbf{F}_{q^n}^*, \cdot)$ can be seen as a $\mathbf{Z}$-module under the rule $r \circ x := x^r$. $(\mathbf{F}_{q^n}, +)$ can be seen as an $\mathbf{F}_q[X]$-module, under the rule $F \circ x := \sum_{i=0}^{m} f_i x^{q^i}$.
- The fact that primitive and normal elements always exist, implies that both modules are cyclic.
- It is now clear that we are interested in characterizing generators of cyclic modules over Euclidean domains.

Vinogradov's formula

Proposition (Vinogradov's formula)

The characteristic function for the R-generators of $\mathcal{M}$ is

$$\omega(x) := \theta(r) \sum_{d|r} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \widehat{\mathcal{M}},\ \mathrm{ord}(\chi)=d} \chi(x).$$

The *Euler function* is $\varphi(d) = |(R/dR)^*|$, the *Möbius function* is

$$\mu(d) = \begin{cases} (-1)^k, & d \text{ is a product of } k \text{ distinct irreducibles,} \\ 0, & \text{otherwise} \end{cases}$$

and $\theta(d) = \frac{\varphi(d')}{|(R/d'R)|}$, where d' is the square-free part of d.

1. For $l \mid n$, the characteristic function of normal elements of $\mathbf{F}_{q^n}$ over $\mathbf{F}_{q^l}$ is

$$\Omega_l(x) := \theta_l(X^{n/l} - 1) \sum_{F \mid X^{n/l} - 1} \frac{\mu_l(F)}{\varphi_l(F)} \sum_{\psi \in \widehat{\mathbf{F}_{q^n}},\ \mathrm{ord}_l(\psi) = F} \psi(x).$$

2. The characteristic function for primitive elements of $\mathbf{F}_{q^n}$ is

$$\omega(x) := \theta(q^n - 1) \sum_{d \mid q'} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \widehat{\mathbf{F}^*_{q^n}},\ \mathrm{ord}(\chi) = d} \chi(x).$$

Sufficient conditions

Main estimate

Proposition

Let q be a prime power and $n \in \mathbf{N}$, then

$$|\,\mathrm{PCN}_q(n) - \theta(q')\,\mathrm{CN}_q(n)| \leq q^{n/2} W(q') W_{l_1}(F'_{l_1}) \cdots W_{l_k}(F'_{l_k}) \theta(q') \theta(\mathbf{q}),$$

where $W(r)$ is the number of divisors of r, $W_{l_i}(F'_{l_i})$ the number of monic divisors of F'_{l_i} in $\mathbf{F}_{q^{l_i}}[X]$, q' the square-free part of $q^n - 1$, F'_{l_i} the square-free part of $X^{n/l_i} - 1 \in \mathbf{F}_{q^{l_i}}[X]$ and $\mathrm{CN}_q(n)$ the number of completely normal elements of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.

Sketch of the proof

$$\begin{aligned}\mathrm{PCN}_q(n) = &\sum_{x\in\mathbf{F}_{q^n}} \omega(x)\Omega_{l_1}(x)\cdots\Omega_{l_k}(x)\\ =&\theta(q')\theta(\mathbf{q})\sum_{\chi}\sum_{\psi_1,\dots,\psi_k}\frac{\mu(\mathrm{ord}(\chi))}{\varphi(\mathrm{ord}(\chi))}\prod_{i=1}^{k}\frac{\mu_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}{\varphi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}\\ &\sum_{x\in\mathbf{F}_{q^n}}\psi_1\cdots\psi_k(x)\chi(x)\\ =&\theta(q')\theta(\mathbf{q})(S_1+S_2),\end{aligned}$$

where the term S_1 corresponds to $\chi=\chi_0$ and S_2 to $\chi\neq\chi_0$.

Sketch of the proof (cont.)

$$S_1 = \sum_{\psi_1,\ldots,\psi_k} \prod_{i=1}^{k} \frac{\mu_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}{\varphi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))} \sum_{x\in\mathbf{F}_{q^n}} \psi_1\cdots\psi_k(x) = \frac{\mathrm{CN}_q(n)}{\theta(\mathbf{q})}$$

and using character sum estimates, we get

$$|S_2| \leq q^{n/2}(W(q')-1)\prod_{i=1}^{k} W_{l_i}(F'_{l_i}).$$

The result follows.

A useful corollary

Corollary

If

$$\mathrm{CN}_q(n) \geq q^{n/2} W(q') W_{l_1}(F'_{l_1}) \cdots W_{l_k}(F'_{l_k}) \theta(\mathbf{q}),$$

then $\mathrm{PCN}_q(n) > 0$.

A lower bound for $\mathrm{CN}_q(n)$

Proposition

Let q be a power of the prime p and $n \in \mathbf{N}$, then

$$\mathrm{CN}_q(n) \geq q^n \left(1 - \frac{n(q+1)}{q^2}\right),$$

while for $n = p^\ell m$, with $\ell \geq 1$ and $(m, p) = 1$, we get

$$\mathrm{CN}_q(n) \geq \begin{cases} q^n \left(1 - m\left(\frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^p} + \frac{4}{q^{2p}}\right)\right), & \text{for } p > 2 \\ q^n \left(1 - m\left(\frac{1}{q} + \frac{1}{q^2} + \frac{2}{3q^3} + \frac{3}{q^4}\right)\right), & \text{for } p = 2. \end{cases}$$

The bounds are meaningful for $q > m$.

Proof of the main theorem

Since $\prod_{i=1}^{k} W_{l_i}(F'_{l_i})\theta_{l_i}(F'_{l_i}) < 2^{t(n)-1}$, where $t(n) := \sum_{d|n} d$, it suffices to show that

$$\mathrm{CN}_q(n) \geq W(q')2^{t(n)-1}.$$

Lemma

For $r \in \mathbf{N}$, $W(r) \leq c_{r,a} r^{1/a}$, where $c_{r,a} = 2^s/(p_1 \cdots p_s)^{1/a}$ and $p_1, \ldots, p_s$ the prime divisors $\leq 2^a$ of r. Also, $d_r = c_{r,8} < 4514.7$.

Theorem (Robin, 1984)

$$t(n) \leq e^{\gamma} n \log\log n + \frac{0.6483n}{\log\log n}, \ \forall n \geq 3,$$

where γ is the Euler-Mascheroni constant.

We distinguish three separate cases:

1. $(n, p) = 1$.
2. $(n, p) > 1$ and $p \neq 2$.
3. $(n, p) > 1$ and $p = 2$.

For each case we roughly follow the below steps:

1. Deal with all but a finite number of possible exceptions with the generic bounds for the various W's.
2. For the possible exceptions, try validating the conditions after replacing all quantities with their exact values.
3. Check if the remaining pairs (q, n) correspond to a completely basic extension.

The above strategy worked for all but the below possible exception pairs (q, n):

n	q	n	q	n	q	n	q	n	q	n	q
6	8	6	11	6	17	6	23	6	29	8	11
8	19	12	17	12	23	12	29	12	41	24	29
24	41	21	9	12	8	20	8	24	8		

But for all of them Morgan and Mullen have provided examples of primitive and completely normal elements.

The proof is complete.

Conclusions

Further research

The restriction $q > m$ is a consequence of our lower bound for $\mathrm{CN}_q(n)$ and the fact that we were unable to fully handle the behavior of the additive characters.

1. Tighter bounds for $\mathrm{CN}_q(n)$ or
2. more efficient handling of the character sums

would improve our results.

This work is available at:

arXiv:1709.03141 [math.NT]

DOI:10.1016/j.jpaa.2018.05.005

Thank You!