Towards the Primitive Completely Normal Basis Theorem

Giorgos Kapetanakis

(Joint work with Theodoulos Garefalakis)

14 May, 2021 – University of Crete Mathematics Seminar

University of Thessaly

Motivation

Introduction - Primitivity

Let $\mathbb{F}_q$ be the finite field of cardinality q and $\mathbb{F}_{q^n}$ its extension of degree n, where q is a power of the prime p, also known as the characteristic of $\mathbb{F}_q$, and n is a positive integer.

- A generator of the multiplicative group $\mathbb{F}_{q^n}^*$ is called primitive. Besides their theoretical interest, primitive elements of finite fields are widely used in various applications, including cryptographic schemes, such as the Diffie-Hellman (1976) key exchange.
- Primitive elements exist for any finite field. However, they are sparse and we do not have any effective way of finding one.

Introduction - Normality

- An $\mathbb{F}_q$-normal basis of $\mathbb{F}_{q^n}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ of the form $\{x, x^q, \ldots, x^{q^{n-1}}\}$ and the element $x \in \mathbb{F}_{q^n}$ is called normal over $\mathbb{F}_q$. These bases bear computational advantages for finite field arithmetic, so they have numerous applications, mostly in coding theory and cryptography (Gao 1993).
- The Normal basis theorem ensures the existence of normal elements over any finite field extension.

Primitive Normal Elements

The existence of elements that are simultaneously primitive and normal is well-known.

Theorem (Primitive normal basis theorem)

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

This was originally proven by Lenstra and Schoof (1987) and Cohen and Huczynska (2003) provided a computer-free proof. Several generalizations of this have been investigated (Cohen-Hachenberger 1999, Cohen-Huczynska 2010, Hsu-Nan 2011, K. 2013, K. 2014).

Primitive nornal elements are also useful in cryptography (Agnew-Mullin-Onyszhuk-Vanstone 1991).

Completely normal elements

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

The existence of such elements for any q and n is known as the Complete normal basis theorem.

This was initially proved by Blessenohl and Johnsen (1986), but Hachenberger (1994) gave a simplified proof.

The Morgan-Mullen conjecture

Morgan and Mullen (1996) went one step further and conjectured that for any q and n, there exists a primitive completely normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Conjecture (Morgan-Mullen)

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

Remark

The conjecture is still open.

Completely basic extensions

The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is completely basic if every normal element of $\mathbb{F}_{q^n}$ is completely normal.

If an extension is completely basic, the Morgan-Mullen conjecture follows from the primitive normal basis theorem.

The study of completely basic extensions dates back to the work of Faith (1957). In particular, we have the following easy characterization:

Theorem (Blessenohl-Johnsen, 1991)

The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ (where q is a power of the prime p) is completely basic if and only if for every prime divisor r of n, we have that $r \nmid \operatorname{ord}_{(n/r)'}(q)$, where $(n/r)'$ is the largest divisor of n/r that is co-prime to p.

First partial results

- Morgan and Mullen (1996) gave examples for such elements for all pairs (q, n) with $q \leq 97$ and $q^n < 10^{50}$ by computer search.
- Hachenberger (2001) settled the case when $\mathbb{F}_{q^n}$ is a regular extension over $\mathbb{F}_q$, given that $4 \mid (q-1)$, q odd and n even. Note that $\mathbb{F}_{q^n}$ is a regular extension over $\mathbb{F}_q$ 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.
- Blessenohl (2005) settled the case $n = 2^l$, $n \mid (q^2-1)$, $l \geq 3$ and $q \equiv 3 \pmod 4$.
- Hachenberger (2012) extended his results to all regular extensions.

The extension of the degree is a prime power

The case when n is a prime power has also been settled. Namely, let $\mathrm{PCN}_q(n)$ denote the number of primitive and completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Hachenberger (2010) proved that:

1. $\mathrm{PCN}_q(2^l) \geq 4(q-1)^{2^{l-2}}$, if $q \equiv 3 \pmod 4$ and $l \geq e+3$ (where e is maximal such that $2^e \mid (q^2-1)$), or if $q \equiv 1 \pmod 4$ and $l \geq 5$.
2. $\mathrm{PCN}_q(r^l) \geq r^2(q-1)^{r^{l-2}}$, if $r \neq p$ is an odd prime and $l \geq 2$.
3. $\mathrm{PCN}_q(r^l) \geq r(q-1)^{r^{l-1}} \cdot \varphi(q^{r^{l-1}}-1)$, if $r \geq 7$ and $r \neq p$ is a prime and $l \geq 2$.
4. $\mathrm{PCN}_q(p^l) \geq pq^{p^{l-1}-1}(q-1)$, if $l \geq 2$.
5. $\mathrm{PCN}_q(p^l) \geq pq^{p^{l-1}-1}(q-1) \cdot \varphi(q^{p^{l-1}}-1)$, if $p \geq 7$ and $l \geq 2$.

The first “generic” result

Recently, with elementary combinatorial 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

This is the first result that does not rely on the prime factorization of n.

Our contribution

We employ character sum techniques and prove the following.

Theorem (Garefalakis-K., 2019)

Let $n \in \mathbb{N}$ and q a prime power such that $q > n$, then $\mathrm{PCN}_q(n) > 0$.

Remark

In this talk, we will outline the establishment of this result.

By pushing our techniques further, we generalize our result as follows:

Theorem (Garefalakis-K., 2019)

Let q a power of the prime p and $\ell, m \in \mathbb{Z}$ with $\ell \geq 0$, $m \geq 1$, $(m, p) = 1$. *Then* $\mathrm{PCN}_q(p^\ell m) > 0$ *provided that* $m < q$.

Our contribution

In later work (Garefalakis-K., 2019), we managed to push our techniques even further and obtained the following results:

1. There exists some c, such that if $q > c$ and $q \leq n \leq q^2$ (n odd), or $q - 1 \nmid n$ and $q \leq n \leq 0.43 \cdot q^2$ (n even), then there exists a primitive and completely normal element for the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$.
2. If n is odd and $n < q^{4/3}$ or n is even, $q - 1 \nmid n$ and $n < q^{5/4}$, then there exists a primitive and completely normal element for the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Further computational evidence

By considering the aforementioned results of Garefalakis-K. (2019), Hachenberger and Hackenberg (2019), extended the original computational experiments of Morgan and Mullen (1996) to the extensions

- $\mathbb{F}_{q^n}/\mathbb{F}_q$ (q prime power), when $1 \leq n \leq 202$, and
- $\mathbb{F}_{p^n}/\mathbb{F}_p$ (p prime), when $p \leq 10{,}000$ and $p^n \leq 10^{80}$.

Preliminaries

Characters

Characters and their sums play a crucial role in characterizing elements of finite fields with the desired properties.

Definition

Let $\mathfrak{G}$ be a finite abelian group. A character of $\mathfrak{G}$ is a group homomorphism $\mathfrak{G} \to \mathbb{C}^*$. The characters of $\mathfrak{G}$ form a group under multiplication, which is isomorphic to $\mathfrak{G}$. This group is called the dual of $\mathfrak{G}$ and denoted by $\widehat{\mathfrak{G}}$. Furthermore, the character $\chi_0 : \mathfrak{G} \to \mathbb{C}^*$, where $\chi_0(g) = 1$ for all $g \in \mathfrak{G}$, is called the trivial character of $\mathfrak{G}$.

From now on, we will call the characters of $\mathbb{F}_{q^n}^*$ multiplicative characters and the characters of $\mathbb{F}_{q^n}$ additive characters. Furthermore, we will denote by χ_0 and ψ_0 the trivial multiplicative and additive character respectively.

Some character sums

Lemma (Orthogonality relations)

Let χ be a non-trivial character of a group $\mathfrak{G}$ and g a non-trivial element of $\mathfrak{G}$. Then

$$\sum_{x \in \mathfrak{G}} \chi(x) = 0 \quad \textit{and} \quad \sum_{\chi \in \widehat{\mathfrak{G}}} \chi(g) = 0.$$

Lemma (Gauss sums)

Let χ be a non-trivial multiplicative character and ψ be a non-trivial additive character. Then

$$\left| \sum_{x \in \mathbb{F}_{q^n}} \chi(x)\psi(x) \right| = q^{n/2}.$$

Vinogradov's formula

- $\mathbb{F}_{q^n}^*$ (the multiplicative group) can be seen as a $\mathbb{Z}$-module under the rule $r \circ x := x^r$ and $\mathbb{F}_{q^n}$ (the additive group), can be seen as an $\mathbb{F}_q[X]$-module, under the rule $F \circ x := \sum_{i=0}^{m} f_i x^{q^i}$ (where $F(X) = \sum_{i=0}^{m} f_i X^i \in \mathbb{F}_q[X]$).
- The fact that primitive and normal elements exist for every finite field extension, imply that both modules are cyclic, while the elements that are interesting for us, i.e. primitive and normal elements, are the generators of those modules.
- It is now clear that we are interested in characterizing generators of cyclic modules over Euclidean domains.

Vinogradov's formula

Define the following functions for $d \in R$, $d \mid r := \mathrm{ord}(g)$:

1. The Euler function is defined as $\varphi(d) := |(R/dR)^*|$,
2. the Möbius function is defined as

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

3. and $\theta(d) := \varphi(d')/|(R/d'R)|$, where d' stands for the square-free part of d.

Proposition (Vinogradov's formula)

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

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

Characteristic functions for normal and primitive elements

By applying Vinogradov's formula, we get that:

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

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

   where the first sum extends over the monic divisors of $X^{n/l} - 1$ in $\mathbb{F}_{q^l}[X]$ and the second sum runs through the additive characters of $\mathbb{F}_{q^n}$ of order F over $\mathbb{F}_{q^l}$.
2. Similarly, the characteristic function for primitive elements of $\mathbb{F}_{q^n}$ is

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

The number of completely normal elements

Let $\mathrm{CN}_q(n)$ be the number of completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Assume that $\{1 = l_1 < \ldots < l_k < n\}$ is the set of proper divisors of n. Since all $x \in \mathbb{F}_{q^n}^*$ are normal over $\mathbb{F}_{q^n}$, it follows that an element of $\mathbb{F}_{q^n}$ is completely normal over $\mathbb{F}_q$ if and only if it is normal over $\mathbb{F}_{q^{l_i}}$ for all $i = 1, \ldots, k$. To simplify our notation, we denote $\mathbf{q} = (X^{n/l_1} - 1, \ldots, X^{n/l_k} - 1)$ and $\theta(\mathbf{q}) = \prod_{i=1}^{k} \theta_{l_i}(X^{n/l_i} - 1)$. We compute

$$\begin{aligned} \mathrm{CN}_q(n) &= \sum_{x \in \mathbb{F}_{q^n}} \left(\Omega_{l_1}(x) \cdots \Omega_{l_k}(x)\right) \\ &= \theta(\mathbf{q}) \sum_{(\psi_1, \ldots, \psi_k)} \prod_{i=1}^{k} \frac{\mu_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}{\varphi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))} \sum_{x \in \mathbb{F}_{q^n}} \psi_1 \cdots \psi_k(x), \end{aligned}$$

where the sums extends over all k-tuples of additive characters.

The number of completely normal elements

Later, we will need a lower bound for $\mathrm{CN}_q(n)$.

Proposition

Let q be a prime power and $n \in \mathbb{N}$. Then the following bounds hold

$$\begin{aligned} \mathrm{CN}_q(n) &\geq q^n \left(1 - \sum_{d|n} \left(1 - \frac{\varphi_d(X^{n/d} - 1)}{q^n}\right)\right) \\ \mathrm{CN}_q(n) &\geq q^n \left(1 - \frac{n(q+1)}{q^2}\right). \end{aligned}$$

We note that the second bound is meaningful for $q \geq n + 1$, which is the case we cover in this work.

Sufficient conditions

The main condition

Next, we prove some sufficient conditions that ensure $\mathrm{PCN}_q(n) > 0$, where $\mathrm{PCN}_q(n)$ stands for the number of primitive completely normal elements of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Theorem

Let q be a prime power and $n \in \mathbb{N}$, 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 positive divisors of r and $W_{l_i}(F'_{l_i})$ is the number of monic divisors of F'_{l_i} in $\mathbb{F}_{q^{l_i}}[X]$.

- Here, q' stands for the square-free part of $q^n - 1$ and F'_{l_i} stands for the square-free part of $X^{n/l_i} - 1$ in $\mathbb{F}_{q^{l_i}}$.

Sketch of the proof

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

where the term S_1 is the part of the above sum for $\chi=\chi_0$ and S_2 is the part for $\chi\neq\chi_0$.

Sketch of the proof (cont.)

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

and

$$S_2 = \sum_{\chi \neq \chi_0} \sum_{(\psi_1,\ldots,\psi_k)} \frac{\mu(\mathrm{ord}(\chi))}{\varphi(\mathrm{ord}(\chi))} \prod_{i=1}^{k} \frac{\mu_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}{\varphi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))} \sum_{x \in \mathbb{F}_{q^n}} \psi_1 \cdots \psi_k(x)\chi(x).$$

Using the character sum results we presented earlier, we get

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

and the result follows.

The main condition

The latter implies.

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

Proof of the theorem

Putting things together

Lemma

For any $r \in \mathbb{N}$, $W(r) \leq c_{r,a} r^{1/a}$, where $c_{r,a} = 2^s/(p_1 \cdots p_s)^{1/a}$ and $p_1, \ldots, p_s$ are the primes $\leq 2^a$ that divide r.

We get $\mathrm{PCN}_q(n) > 0$ provided that

$$\mathrm{CN}_q(n) > q^{n/2} W(q') \prod_{i=1}^{k} W_{l_i}(F'_{l_i}) \theta_{l_i}(F'_{l_i}).$$

It is not hard to see that $\prod_{i=1}^{k} W_{l_i}(F'_{l_i}) \theta_{l_i}(F'_{l_i}) < 2^{t(n)-1}$, where $t(n) := \sum_{d|n} d$. Plugging this and a bound of $\mathrm{CN}_q(n)$, it suffices to show that

$$q^{n/2} \left(1 - \frac{n(q+1)}{q^2}\right) \geq W(q') 2^{t(n)-1}.$$

Putting things together

We combine the above and a sufficient condition for $\mathrm{PCN}_q(n) > 0$ would be

$$q^{3n/8}\left(1 - \frac{n(q+1)}{q^2}\right) \geq 4514.7 \cdot 2^{t(n)-1}.$$

By Robin's (1984) theorem $t(n) \leq e^{\gamma} n \log\log n + \frac{0.6483n}{\log\log n}$, $\forall n \geq 3$, where γ is the Euler-Mascheroni constant, therefore the above becomes

$$q^{3n/8}\left(1 - \frac{n(q+1)}{q^2}\right) > 4514.7 \cdot 2^{n\left(\log\log n \cdot e^{0.558} + \frac{0.6483}{\log\log n}\right)-1}.$$

Putting things together

- The latter is satisfied for all $q \geq n + 1$, given that $n > 1016$.
- Within the range $2 \leq n \leq 1016$ it is satisfied for all but 49 values of n, if we substitute q by the least prime power greater or equal to $n + 1$, $t(n)$ by its exact value and we exclude the values of n that are a prime number.
- For those values for n, we compute the smallest prime power q that satisfies our condition. In this region, there is a total of 1868 pairs (n, q) to deal with.

Putting things together

Another condition would be

$$q^{n/2}\left(1-\sum_{d|n}\left(1-\frac{\varphi_d(X^{n/d}-1)}{q^n}\right)\right) > W(q')\prod_{i=1}^{k} W_{l_i}(F'_{l_i})\theta_{l_i}(F'_{l_i}).$$

- By using this and the estimate $W(q') \leq c_{q',16}q^{n/16}$ the list is furtherer reduced to a total of 80 pairs. The list can be shrinked even more, to a total of 65 pairs, if we replace $W(q')$ by its exact value.
- By taking into account the fact that Morgan and Mullen (1996) found examples for $q \leq 97$ and $q^n < 10^{50}$, we are left with just 3 pairs (n, q) to investigate. These pairs are $(36, 37)$, $(48, 49)$ and $(60, 61)$.

Completing the proof

- For the pairs $(60, 61)$ and $(48, 49)$ we succesfully apply the Cohen-Huczynska (1999) sieve.
- For the pair $(36, 37)$ we explicitly find an example.

Now the proof is complete.

Conclusion

Further research

For our methods to work for arbitrary n there seems to be two paths:

- new bounds for $\mathrm{CN}_q(n)$ or
- better handling of the character sums that arise.

We believe that this would be an interesting and challenging direction for further research.

q	n	Lower bound	Exact value
7	4	1630	1728
5	6	7165	8448
2	14	1666	6272

References

References

G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone.

An implementation for a fast public-key cryptosystem.

J. Cryptology, 3(2):63–79, 1991.

S. D. Cohen and D. Hachenberger.

Primitive normal bases with prescribed trace.

Appl. Algebra Engrg. Comm. Comput., 9(5):383–403, 1999.

S. D. Cohen and S. Huczynska.

The primitive normal basis theorem – without a computer.

J. London Math. Soc., 67(1):41–56, 2003.

S. D. Cohen and S. Huczynska.

The strong primitive normal basis theorem.

Acta Arith., 143(4):299–332, 2010.

W. Diffie and M. Hellman.

New directions in cryptography.

IEEE Trans. Information Theory, 22(6):644–654, 1976.

C. C. Faith.

Extensions of normal bases and completely basic fields.

Trans. Amer. Math. Soc., 85(2):406–427, 1957.

S. Gao.

Normal Basis over Finite Fields.

PhD thesis, University of Waterloo, 1993.

References

T. Garefalakis and G. Kapetanakis.

Further results on the Morgan-Mullen conjecture.

Des. Codes Cryptogr., 87(11):2639–2654, 2019.

T. Garefalakis and G. Kapetanakis.

On the existence of primitive completely normal bases of finite fields.

J. Pure Appl. Algebra, 223(3):909–921, 2019.

D. Hachenberger.

Primitive complete normal bases for regular extensions.

Glasgow Math. J., 43(3):383–398, 2001.

D. Hachenberger.

Primitive complete normal bases: Existence in certain 2-power extensions and lower bounds.

Discrete Math., 310(22):3246–3250, 2010.

D. Hachenberger.

Primitive complete normal bases for regular extensions II: the exceptional case.

Unpublished, 2012.

D. Hachenberger.

Asymptotic existence results for primitive completely normal elements in extensions of Galois fields.

Des. Codes Cryptogr., 80(3):577–586, 2016.

D. Hachenberger and S. Hackenberg.

Computational results on the existence of primitive complete normal basis generators.

arXiv:1912.07541 [math.NT], 2019.

References

C. Hsu and T. Nan.

A generalization of the primitive normal basis theorem.

J. Number Theory, 131(1):146–157, 2011.

G. Kapetanakis.

An extension of the (strong) primitive normal basis theorem.

Appl. Algebra Engrg. Comm. Comput., 25(5):311–337, 2014.

G. Kapetanakis.

Normal bases and primitive elements over finite fields.

Finite Fields Appl., 26:123–143, 2014.

H. W. Lenstra, Jr and R. J. Schoof.

Primitive normal bases for finite fields.

Math. Comp., 48(177):217–231, 1987.

I. H. Morgan and G. L. Mullen.

Completely normal primitive basis generators of finite fields.

Util. Math., 49:21–43, 1996.

G. Robin.

Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann.

J. Math. Pures Appl., 63(2):187–213, 1984.

Thank You!