On a conjecture of Morgan and Mullen

Giorgos Kapetanakis
(Joint work with Theodoulos Garefalakis)

Fq13 - June 7, 2017

Sabancı University

Motivation

Definitions

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 $\{x, x^q, \ldots, x^{q^{n-1}}\}$ 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 basis 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

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 (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.
- 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.

Known results

Let $\mathrm{PCN}_q(n)$ denote the number of primitive and completely normal elements of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. Hachenberger (2010) proved:

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 $l \geq 2$.

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 prime power such that $q > n$, 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.

Vinogradov's formula

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

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

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 $\operatorname{CN}_q(n)$ the number of completely normal elements of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.

Sketch of the proof

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

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

Sketch of the proof (cont.)

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

and using character sum estimates, we get

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

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 prime power and $n \in \mathbf{N}$. 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 are the cases of interest in this work.

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

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

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.

Therefore, a condition is:

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

- This 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 $> n$, $t(n)$ by its exact value and exclude the primes n.
- 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.

Another condition would be

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

- This and the estimate $W(q') \leq c_{q',16}q^{n/16}$ reduces the list to 80 pairs. Calculating $W(q')$, reduces it to 65 pairs.
- Morgan and Mullen's calculations reduce the list to 3 pairs (n, q). These pairs are $(36, 37)$, $(48, 49)$ and $(60, 61)$.
- For $(60, 61)$ and $(48, 49)$ we employ Cohen and Huczynska's sieve (on the multiplicative part) and for $(36, 37)$ we find an example.
- The proof is complete.

Conclusions

Outcome

- A step towards resolving Morgan and Mullen Conjecture was taken. Our results, combined with the results of Hachenberger (2010) prove this conjecture for $q \geq n$.
- By using similar techniques, we generalized this result.

Theorem (Garefalakis-K.)

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

Further research

Remark

The restriction $q > n$ is a consequence of our lower bound for $\mathrm{CN}_q(n)$. Tighter bounds for $\mathrm{CN}_q(n)$ or more efficient handling of the character sums would improve our results.

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

Our lower bound and the actual value of $\mathrm{CN}_q(n)$ for some q and n

Thank You!