Sabancı Üniversitesi

FACULTY OF ENGINEERING AND NATURAL SCIENCES

On a conjecture of Morgan and Mullen

Giorgos Kapetanakis

Joint work with T. Garefalakis

May 4, 2017

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 key exchange.
- 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.
- It is well-known that primitive and normal elements exist for every q and n.

The existence of elements that are simultaneously primitive and normal is also 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 $\mathbb{F}_q$.

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

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.

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 $\mathbb{F}_q$.

- The conjecture is still open.
- Morgan and Mullen provide 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 $\mathrm{ord}_{\nu(n')}(q)$ are co-prime, where $\nu(n')$ 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 case when n is a prime power have 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. $\mathrm{PCN}_q(r^l) \geq r(q-1)^{r^{l-1}} \cdot \phi(q^{r^{l-1}}-1)$, 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. $\mathrm{PCN}_q(p^l) \geq pq^{p^{l-1}-1}(q-1) \cdot \phi(q^{p^{l-1}}-1)$, if $p \geq 7$ and $l \geq 2$.

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

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

Theorem (Garefalakis-K.)

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

The main idea behind our techniques dates back to the 50's and the work of Carlitz and remains popular among authors. Roughly, our method is:

1. We express the characteristic function for an element with the desired properties with help of characters,
2. this leads us to a sufficient condition for the existence of our desired polynomial.
3. With the the help of characters sum estimates, we end up with asymptotic results, for the existence of the elements we seek.
4. If necessary and desirable, we deal with the remaining cases with a case-by-case approach.

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 $\mathfrak{G}$. Finally, by $\bar{\chi}$ we denote the inverse of χ.

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 and we will extend the multiplicative characters to zero with the rule

$$\chi(0) := \begin{cases} 0, & \text{if } \chi \in \widehat{\mathbb{F}_{q^n}^*} \setminus \{\chi_0\}, \\ 1, & \text{if } \chi = \chi_0. \end{cases}$$

A character sum is a sum that involves characters.

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

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

- $\mathbb{F}_{q^n}^*$ (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.

- Let R be a Euclidean domain and $\mathcal{M}$ a cyclic finite R-module and g a generator. $\mathcal{M}$ has also the structure of an abelian group, hence $\widehat{\mathcal{M}}$ is well-defined and can also be seen as an R-module under the rule $F \circ \chi(x) := \chi(F \circ x)$ for all $\chi \in \widehat{\mathcal{M}}$, $x \in \mathcal{M}$ and $F \in R$, while it is not hard to show that $\widehat{\mathcal{M}}$ is also cyclic.
- Let $x \in \mathcal{M}$. The annihilator of x is an ideal or R and, as such, has a generator called the order of x and denoted by $\mathrm{ord}(x)$.
- The order of a character is defined accordingly.

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

1. The Euler function is defined as $\phi(d) := |(R/dR)^*|$,
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 $\theta(d) := \phi(d')/|(R/d'R)|$, 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

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

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
$$\Omega_l(x) := \theta_l(X^{n/l}-1) \sum_{F \mid X^{n/l}-1} \frac{\mu_l(F)}{\phi_l(F)} \sum_{\psi\in\widehat{\mathbb{F}_{q^n}},\ \mathrm{ord}_l(\psi)=F} \psi(x),$$
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
$$\omega(x) := \theta(q^n-1) \sum_{d \mid q'} \frac{\mu(d)}{\phi(d)} \sum_{\chi\in\widehat{\mathbb{F}_{q^n}^*},\ \mathrm{ord}(\chi)=d} \chi(x).$$

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

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

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

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

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

We note that the second bound is meaningful for $q \geq n+1$, which are the cases of interest in this work.

Sketch of the proof

The number of normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^d}$ is $\phi_d(X^{n/d}-1)$. So, $\mathbb{F}_{q^n}$ has $\leq \sum_{d|n}(q^n - \phi_d(X^{n/d}-1))$ elements that are *not* completely normal over $\mathbb{F}_q$. The first bound follows.
For the second bound, observe that

$$\phi_d(X^{n/d}-1) = q^n \prod_P \left(1 - \frac{1}{q^{d\deg(P)}}\right) \geq q^n \left(1 - \frac{1}{q^d}\right)^{n/d}.$$

Substituting in the first bound we obtain

$$\mathrm{CN}_q(n) \geq q^n \left(1 - \sum_{d|n} \left(1 - \left(1 - \frac{1}{q^d}\right)^{n/d}\right)\right) \geq q^n \left(1 - \sum_{d|n} \frac{n}{dq^d}\right).$$

The second bound follows upon noting that $\sum_{d|n} \frac{n}{dq^d} \leq nq^{-2}(q+1)$, since $\sum_{d=2}^{n} q^{-d} \leq 2q^{-2}$.

Next, we prove some sufficient conditions that ensure $\mathrm{PCN}_q(n) > 0$.

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

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

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.)

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

and

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

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

Next, we adjust Cohen and Huczynska's (2013) sieve in our setting.

Proposition

Let $\{p_1, \ldots, p_t\}$ *a set of prime divisors of* $q^n - 1$, *such that* $\delta := 1 - \sum_{i=1}^{t} p_i^{-1} > 0$. *If*

$$\mathrm{CN}_q(n) \geq q^{n/2}\, W(q_0)\, W_{l_1}(F'_{l_1}) \cdots W_{l_k}(F'_{l_k}) \left(\frac{t-1}{\delta} + 2 \right) \theta(\mathbf{q}),$$

where $q_0 := q' / p_1 \cdots p_t$, *then* $\mathrm{PCN}_q(n) > 0$.

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. *In particular, we are interested in* $d_r := c_{r,8}$. *Moreover, for all* $r \in \mathbb{N}$ *we have that* $d_r < 4514.7$.

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

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

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

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

- 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.

n	q_0	q_1	n	q_0	q_1	n	q_0	q_1	n	q_0	q_1
4	5	4391	6	7	1259	8	9	431	9	11	149
10	11	223	12	13	419	14	16	107	15	16	79
16	17	137	18	19	179	20	23	139	21	23	49
22	23	59	24	25	243	25	27	29	26	27	49
27	29	41	28	29	89	30	31	173	32	37	79
34	37	41	36	37	193	40	41	113	42	43	121
44	47	61	45	47	49	48	49	191	50	53	59
52	53	59	54	59	97	56	59	81	60	61	256
66	67	83	70	71	73	72	73	211	78	79	81
80	81	101	84	89	181	90	97	163	96	97	163
108	109	151	120	121	311	126	127	128	132	137	139
144	149	211	168	169	229	180	181	311	240	241	343
360	361	439									

Table: Non-prime values for $2 \leq n \leq 1016$ not satisfying our condition for q_0, the least prime power $\geq n+1$, where q_1 stands for the least prime power satisfying our condition for that n.

Another condition would be

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

- 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 $(60, 61)$.

For those pairs, we will employ the sieve. In particular, we choose a set $\{p_1, \ldots, p_t\}$ of prime divisors of $q^n - 1$ and check whether $\delta := 1 - \sum_{i=1}^t 1/p_i > 0$ and then if

$$q^{n/2} \left(1 - \sum_{d|n} \left(1 - \frac{\phi_d(X^{n/d} - 1)}{q^n} \right) \right) > W\left(\frac{q'}{p_1 \cdots p_t} \right) \prod_{i=1}^{k} W_{l_i}(F'_{l_i}) \theta_{l_i}(F'_{l_i}) \left(\frac{t-1}{\delta} + 2 \right).$$

If both are true, then we have proved that $\mathrm{PCN}_q(n) > 0$ for that pair (n, q).

- For the pair $(60, 61)$ we choose $\{907838335136559038161, 188565401138641, 4674531865001, 32096761, 13842121, 1238411, 61261, 28771, 21491, 1861, 661, 523, 211, 131, 97, 41, 31\}$.
- For the pair $(48, 49)$ we choose $\{108604397663266369, 33232924804801, 47072139617, 104837857, 169553, 1201, 409, 353, 193, 181, 97\}$.
- For the pair $(36, 37)$ this method fails to provide the desired result, but an explicit computer search reveals that $a^2 + 12 \in \mathbb{F}_{37^{36}}$ is primitive and completely normal over $\mathbb{F}_{37}$, where a is a root of the irreducible $X^{36}+5X^{35}+36X^{34}+11X^{33}+28X^{32}+31X^{31}+32X^{30}+13X^{29}+25X^{28}+4X^{27}+7X^{26}+X^{25}+17X^{24}+20X^{23}+30X^{22}+5X^{21}+8X^{20}+11X^{19}+20X^{18}+3X^{17}+21X^{15}+33X^{14}+30X^{13}+27X^{12}+30X^{11}+X^{10}+26X^{9}+23X^{8}+11X^{7}+31X^{6}+7X^{5}+34X^{4}+14X^{3}+34X^{2}+36X+20 \in \mathbb{F}_{37}[X]$.

Now the proof is complete.

- 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 as follows:

Theorem (Garefalakis-K.)

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 $m < q$.

Remark

The restriction $q > n$ is a direct consequence of the lower bound for $\mathrm{CN}_q(n)$ we employed. For our methods to work for $q < n$, new bounds for $\mathrm{CN}_q(n)$ or better handling of the character sums that arise are needed. 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

Thank You!