On the existence of primitive completely normal bases of finite fields

Theodoulos Garefalakis[a], Giorgos Kapetanakis[b,*]

[a]Department of Mathematics and Applied Mathematics, University of Crete, Voutes Campus, 70013 Heraklion, Greece
[b]Sabanci University, FENS, Orhanli-Tuzla, 34956 Istanbul, Turkey

Abstract

Let $\mathbb{F}_q$ be the finite field of characteristic p with q elements and $\mathbb{F}_{q^n}$ its extension of degree n. We prove that there exists a primitive element of $\mathbb{F}_{q^n}$ that produces a completely normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, provided that $n = p^\ell m$ with $(m, p) = 1$ and $q > m$.

Keywords: finite fields, character sums, primitive elements, normal basis, completely normal basis
2010 MSC: 11T24

1. Introduction

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 prime power 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 [5].

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. For further information we refer to [6] and the references therein.

It is well-known that primitive, see [15, Theorem 2.8], and normal, see [15, Theorem 2.35], elements exist for every q and n. The existence of elements that are simultaneously primitive and normal is also well-known.

Theorem 1.1 (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 $\mathbb{F}_q$.*

*Corresponding author
Email addresses: tgaref@uoc.gr (Theodoulos Garefalakis), gnkapet@gmail.com (Giorgos Kapetanakis)

Lenstra and Schoof [14] were the first to prove Theorem 1.1. Subsequently, Cohen and Huczynska [3] provided a computer-free proof with the help of sieving techniques. Several generalizations of this have also been investigated [2, 4, 11, 12, 13].

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 well-known [1]. Morgan and Mullen [16] conjectured that for any q and n, there exists a primitive completely normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Conjecture 1.2 (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 $\mathbb{F}_q$.*

In order to support their claim, Morgan and Mullen provide examples for such elements for all pairs (q, n) with $q \leq 97$ and $q^n < 10^{50}$, see [16]. This conjecture is yet to be completely resolved. Partial results, covering certain types of extensions have been given, see [9] and the references therein. Recently, Hachenberger [10], using elementary methods, proved the validity of Conjecture 1.2 for $q \geq n^3$ and $n \geq 37$. In this work, we begin by proving the following theorem in Section 4.

Theorem 1.3. *Let $n \in \mathbb{N}$ and q a prime power with $q \geq n$, then there exists a primitive completely normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Then, we extend Theorem 1.3 by pushing our methods further and obtain the following generalization in Section 5.

Theorem 1.4. *Let q a power of the prime p and $\ell, m \in \mathbb{Z}$ with $\ell \geq 0$, $m \geq 1$, $(m, p) = 1$. If $n = p^\ell m$ and $m < q$, then there exists a primitive completely normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Our method is based on the work of Lenstra and Schoof [14]. In particular, we give sufficient conditions, for our existence results, that are progressively easier to check, but harder to satisfy. This way, me manage to prove our theorems theoretically for all pairs (n, q) that satisfy the stated conditions, with the exception of 18 resilient pairs. For all those pairs, however, examples of primitive and completely normal elements have been given in [16]. For the reader's convenience, these pairs are displayed in Table 2.

2. Preliminaries

Before we move on to our results, we note that, in addition to the special cases mentioned in [9], the case when $\mathbb{F}_{q^n}$ is completely basic over $\mathbb{F}_q$ can be excluded from our calculations. Namely, $\mathbb{F}_{q^n}$ is *completely basic over* $\mathbb{F}_q$ if every normal element of F_{q^n} is also completely normal over $\mathbb{F}_q$ and it is clear that in that case, Theorem 1.1 implies Conjecture 1.2. Furthermore, we can characterize such extensions using the following, see [9, Theorem 5.4.18] and, for a proof, see [7, Section 15].

Theorem 2.1. *Let q be a power of the prime p. $\mathbb{F}_{q^n}$ is completely basic over $\mathbb{F}_q$ if and only if for every prime divisor r of n, $r \nmid \operatorname{ord}_{(n/r)'}(q)$, where $(n/r)'$ stands for the p-free part of n/r and $\operatorname{ord}_{(n/r)'}(q)$ for the multiplicative order of q modulo $(n/r)'$.*

With the above and Theorem 1.1 in mind, it is straightforward to check the validity of the following:

Corollary 2.2. *Let q be a power of the prime p and $n = p^\ell m$, where $\ell \geq 0$ and $(m, p) = 1$. If*

1. $m \mid q - 1$ *or*
2. $m = 1$ *or*
3. $n = r$ *or* $n = r^2$ *for some prime* r,

then $\mathbb{F}_{q^n}$ is completely basic over $\mathbb{F}_q$ and there exists a primitive complete normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

The above results imply that $\mathbb{F}_{q^n}$ is completely basic over $\mathbb{F}_q$ when $n \leq 5$ or $m = 1$. They also imply Theorems 1.3 and 1.4 for $q \leq 5$. This is straightforward to check for Theorem 1.3, as our cases of interest are $q > n$ and the case $n \leq 5$ is already settled. For Theorem 1.4 we demonstrate the case $q = 5$ and we notice that the cases $q \leq 4$ are proven in a similar way. Write $n = 5^\ell m$, where $(m, 5) = 1$. Since our cases of interest are $m < q$, we get that $m = 1, 2, 3$ or 4. The cases $m = 1, 2$ and 4 are covered directly from Corollary 2.2, while the case $m = 3$, i.e. when $n = 5^\ell 3$, satisfies the conditions of Theorem 2.1, hence in any case $\mathbb{F}_{5^{5^\ell m}}$ is completely basic over $\mathbb{F}_5$. Summing up, from now on we may assume that $q \geq 7$, $n \geq 6$ and $m > 1$.

Characters and their sums play a crucial role in characterizing elements of finite fields with the desired properties and in estimating the number of elements that combine all the desired properties.

Definition 2.3. 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.

The finite field $\mathbb{F}_{q^n}$ is associated with its multiplicative and its additive group. 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. In this work we will use the following well-known results on character sums.

Lemma 2.4 (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 2.5 (Gauss sums). *Let χ be a non-trivial multiplicative character and ψ be a non-trivial additive character. Then*

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

The additive and the multiplicative groups of $\mathbb{F}_{q^n}$ can also be seen as modules. In particular $\mathbb{F}_{q^n}^*$ (the multiplicative group) can be seen as a $\mathbb{Z}$-module and $\mathbb{F}_{q^n}$ (the additive group) as a $\mathbb{F}_{q^l}[X]$-module, where $l \mid n$, under the rules $r \circ x = x^r$ and $F \circ x = \sum_{i=0}^k F_i x^{q^{li}}$, where $r \in \mathbb{Z}$ and $F(X) = \sum_{i=0}^k F_i X^i \in \mathbb{F}_{q^l}[X]$. Since both primitive elements and normal elements over $\mathbb{F}_{q^l}$ are known to exist, it follows that both modules are cyclic.

Let q' be the square-free part of $q^n - 1$. The characteristic function for primitive elements of $\mathbb{F}_{q^n}$ is given by Vinogradov's formula

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

where $\theta(q') = \phi(q')/q'$, μ is the Möbius function, ϕ is the Euler function and the *order* of a multiplicative character is defined as its multiplicative order in $\widehat{\mathbb{F}_{q^n}^*}$. Similarly, the characteristic function for elements of $\mathbb{F}_{q^n}$ that are normal over $\mathbb{F}_{q^l}$ is

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

where $\theta_l(X^{n/l} - 1) := \phi_l(F_l')/q^{l\cdot\deg(F_l')}$, F_l' is the square-free part of $X^{n/l} - 1 \in \mathbb{F}_{q^l}[X]$, μ_l and ϕ_l are the Möbius and Euler functions in $\mathbb{F}_{q^l}[X]$, 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 $\mathbb{F}_{q^l}$. The *order* of an additive character of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^l}$, denoted as ord_l, is defined as the lowest degree monic polynomial $G \in \mathbb{F}_{q^l}[X]$ such that $\psi(G \circ x) = 1$ for all $x \in \mathbb{F}_{q^n}$. We note that the order of an additive character of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^l}$ always divides $X^{n/l} - 1$ in $\mathbb{F}_{q^l}[X]$. Furthermore, an additive or a multiplicative character has order equal to 1 if and only if it is the trivial character. It is easy to see that the above characteristic functions can be written in the following more compact form, which we will use later

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

Let $\mathrm{PCN}_q(n)$ be the number of primitive completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\mathrm{CN}_q(n)$ be the number of completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $\{1=l_1<\ldots<l_k<n\}$ be 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

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

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

$$\sum_{x\in\mathbb{F}_{q^n}}\psi_1\cdots\psi_k(x)=0,\qquad \text{for}\ \ \psi_1\cdots\psi_k\neq\psi_0,$$

we obtain

$$\mathrm{CN}_q(n)=q^n\ \theta(\mathbf{q})\sum_{\substack{(\psi_1,\ldots,\psi_k)\\ \psi_1\cdots\psi_k=\psi_0}}\prod_{i=1}^k\frac{\mu_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}{\phi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}.$$

3. Sufficient conditions

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

Theorem 3.1. *Let q be a prime power, $n\in\mathbb{N}$, 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 $W(q')$ is the number of positive divisors of q' and $W_{l_i}(F'_{l_i})$ is the number of monic divisors of F'_{l_i} in $\mathbb{F}_{q^{l_i}}[X]$.

Proof. Using the characteristic functions, as presented in Section 2 we deduce that

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

where the term S_1 is the part of the above sum for $\chi=\chi_0$,

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

and S_2 is the part for $\chi\neq\chi_0$,

$$S_2 = \sum_{\chi\neq\chi_0} \sum_{(\psi_1,\ldots,\psi_k)} \frac{\mu(\mathrm{ord}(\chi))}{\phi(\mathrm{ord}(\chi))} \prod_{i=1}^{k} \frac{\mu_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}{\phi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))} \sum_{x\in\mathbb{F}_{q^n}} \psi_1\cdots\psi_k(x)\chi(x). \tag{2}$$

In the last sum, note that the summations runs on multiplicative characters χ of order dividing q' and may be restricted to additive characters of order dividing the square-free part of $X^{n/l_i}-1$, which we denoted by F'_{l_i}. For the last sum we have

$$\begin{aligned}
|S_2| &\le \sum_{\chi\neq\chi_0} \sum_{(\psi_1,\ldots,\psi_k)} \frac{1}{\phi(\mathrm{ord}(\chi))} \prod_{i=1}^{k} \frac{1}{\phi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))} \left| \sum_{x\in\mathbb{F}_{q^n}} \psi_1\cdots\psi_k(x)\chi(x) \right| \\
&\le q^{n/2} \sum_{\chi\neq\chi_0} \frac{1}{\phi(\mathrm{ord}(\chi))} \prod_{i=1}^{k} \sum_{\psi_i} \frac{1}{\phi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))} \\
&= q^{n/2}(W(q')-1) \prod_{i=1}^{k} W_{l_i}(F'_{l_i}),
\end{aligned}$$

where we used Lemma 2.4 and Weil's bound, as seen in Lemma 2.5, for the second inequality. The result follows. □

Remark. The sieving techniques of Cohen and Huczynska [3, 4] could be applied here, albeit only on the multiplicative part. The potential advantage of implementing them would be reducing the number of pairs (q,n) that we rely on the examples given in [16] (see Table 2). However, since this number is already small, the current simpler approach was favored.

From the above, it is clear that we will also need the following lemma:

Lemma 3.2. *For any $r \in \mathbb{N}$, $W(r) \le c_{r,a} r^{1/a}$, where $c_{r,a} = 2^s/(p_1 \cdots p_s)^{1/a}$ and $p_1, \dots, p_s$ are the primes $\le 2^a$ that divide r. In particular, $c_{r,4} < 4.9$, $c_{r,8} < 4514.7$ for all $r \in \mathbb{N}$ and $c_{r,4} < 2.9$, $c_{r,8} < 2461.62$ and $c_{r,12} < 5.61 \cdot 10^{23}$ if r is odd.*

Proof. It is clear that it suffices to prove the above for r square-free. Assume that $r = p_1 \cdots p_s q_1 \cdots q_t$, where $p_1, \dots, p_s, q_1, \dots, q_t$ are distinct primes and $p_i \le 2^a$ and $q_j > 2^a$. We have that

$$W(r) = 2^{s+t} = 2^s \cdot \underbrace{2 \cdots 2}_{t \text{ times}} = 2^s (\underbrace{2^a \cdots 2^a}_{t \text{ times}})^{1/a} \le 2^s (q_1 \dots q_t)^{1/a} = c_{r,a} r^{1/a}.$$

The bounds for $c_{r,a}$ can be easily computed. □

Also, in order to apply the results of this section, we need a lower bound for $\mathrm{CN}_q(n)$.

Proposition 3.3. *Let q be a power of the prime p and $n \in \mathbb{N}$, then*

$$\mathrm{CN}_q(n) \ge q^n \left(1 - \sum_{d|n} \left(1 - \frac{\phi_d(X^{n/d} - 1)}{q^n} \right) \right)$$

In particular, for every n and p, we have that

$$\mathrm{CN}_q(n) \ge q^n \left(1 - \frac{n(q+1)}{q^2} \right), \tag{3}$$

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

$$\mathrm{CN}_q(n) \ge q^n \left(1 - m \left(\frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^p} + \frac{4}{q^{2p}} \right) \right), \text{ for } p > 2 \tag{4}$$

$$\mathrm{CN}_q(n) \ge q^n \left(1 - m \left(\frac{1}{q} + \frac{1}{q^2} + \frac{2}{3q^3} + \frac{3}{q^4} \right) \right), \text{ for } p = 2. \tag{5}$$

Proof. For $d|n$, the number of elements of $\mathbb{F}_{q^n}$ that are normal over $\mathbb{F}_{q^d}$ is equal to $\phi_d(X^{n/d} - 1)$. Therefore, the number of elements of $\mathbb{F}_{q^n}$ that are *not* completely normal over $\mathbb{F}_q$ is at most $\sum_{d|n}(q^n - \phi_d(X^{n/d} - 1))$. The first bound follows.

For the bound of Eq. (3), we observe that

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

where the product extends over the prime factors of $X^{n/d} - 1$ in $\mathbb{F}_{q^d}[X]$. Substituting in the first bound we obtain

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

The result follows upon noting that

$$\sum_{d|n} \frac{n}{dq^d} \leq n \left(\frac{1}{q} + \sum_{\substack{d|n \\ d>1}} \frac{1}{dq^d} \right) \leq n \left(\frac{1}{q} + \frac{1}{2} \sum_{d=2}^{n} q^{-d} \right) \leq nq^{-2}(q+1),$$

since $\sum_{d=2}^{n} q^{-d} \leq 2q^{-2}$.

We next move on to the next two inequalitites. Let $n = p^\ell m$, with $(m,p) = 1$. Then the by the first bound we have

$$\mathrm{CN}_q(p^\ell m) \geq q^{p^\ell m} \left(1 - \sum_{j=0}^{\ell} \sum_{d|m} \left(1 - \frac{\phi_{p^j d}(X^{p^{\ell-j} m/d} - 1)}{q^{p^\ell m}} \right) \right).$$

Since p is the characteristic of $\mathbb{F}_q$, $X^{p^{\ell-j} m/d} - 1 = (X^{m/d} - 1)^{p^{\ell-j}}$, and we may compute

$$\phi_{p^j d}(X^{p^{\ell-j} m/d} - 1) \geq q^{p^\ell m} \left(1 - \frac{1}{q^{dp^j}} \right)^{m/d} \geq q^{p^\ell m} \left(1 - \frac{m}{dq^{dp^j}} \right).$$

Therefore,

$$\mathrm{CN}_q(p^\ell m) \geq q^{p^\ell m} \left(1 - m \sum_{j=0}^{\ell} \sum_{d|m} \frac{1}{dq^{dp^j}} \right). \tag{6}$$

First, we consider the case $p > 2$. We compute,

$$\sum_{d|m} \frac{1}{dq^{dp^j}} \leq \frac{1}{q^{p^j}} + \frac{1}{2} \sum_{d=2}^{m} \frac{1}{q^{dp^j}} \leq \frac{1}{q^{p^j}} + \frac{1}{q^{2p^j}}.$$

Substituting in Eq. (6), and using the fact that

$$\sum_{j=0}^{\ell} \frac{1}{q^{p^j}} \leq \frac{1}{q} + \frac{1}{q^p} + \frac{2}{q^{2p}},$$

we have

$$\begin{aligned} \mathrm{CN}_q(p^\ell m) &\geq q^{p^\ell m} \left(1 - m \sum_{j=0}^{\ell} \left(\frac{1}{q^{p^j}} + \frac{1}{q^{2p^j}} \right) \right) \\ &\geq q^{p^\ell m} \left(1 - m \left(\frac{1}{q} + \frac{1}{q^p} + \frac{2}{q^{2p}} + \frac{1}{q^2} + \frac{2}{q^{2p}} \right) \right), \end{aligned}$$

which immediately yields Eq. (4).

In the case $p = 2$, we note that m is odd. Then

$$\sum_{d|m} \frac{1}{dq^{d2^j}} \leq \frac{1}{q^{2^j}} + \frac{1}{3} \sum_{d=3}^{m} \frac{1}{q^{d2^j}} \leq \frac{1}{q^{2^j}} + \frac{2}{3q^{3 \cdot 2^j}}.$$

Substituting in Eq. (6), and using the bound

$$\sum_{j=0}^{\ell} \frac{1}{q^{2^j}} \leq \frac{1}{q} + \frac{1}{q^2} + \frac{2}{q^4},$$

we obtain

$$\begin{aligned} \mathrm{CN}_q(2^\ell m) &\geq q^{2^\ell m}\left(1 - m\sum_{j=0}^{\ell}\left(\frac{1}{q^{2^j}} + \frac{2}{3q^{3\cdot 2^j}}\right)\right) \\ &\geq q^{2^\ell m}\left(1 - m\left(\frac{1}{q} + \frac{1}{q^2} + \frac{2}{q^4} + \frac{2}{3q^3} + \frac{4}{3q^6}\right)\right). \end{aligned}$$

The last bound of the statement follows. □

We note that the bound of Eq. (3) is meaningful for $q \geq n+1$ and the ones in Eqs. (4) and (5) are meaningful for $q > m > 1$, with the sole exception of $q = 4$ and $m = 3$. This covers all our cases of our interest that are not covered directly by Corollary 2.2.

4. Proof of Theorem 1.3

In this section, we use the theory developed earlier to prove Theorem 1.3. All the described computations were performed with the SageMath software. From Theorem 3.1, we get $\mathrm{PCN}_q(n) > 0$ provided that

$$\mathrm{CN}_q(n) > q^{n/2} W(q') \prod_{i=1}^{k} W_{l_i}(F'_{l_i})\theta_{l_i}(F'_{l_i}). \tag{7}$$

Clearly, $\theta_{l_i}(F'_{l_i}) < 1$ for all i and $W_{l_i}(F'_{l_i}) \leq 2^{n/l_i}$, so we have that

$$\prod_{i=1}^{k} W_{l_i}(F'_{l_i})\theta_{l_i}(F'_{l_i}) < 2^{\sum_{i=1}^{k} n/l_i} = 2^{t(n)-1}.$$

Plugging this and Eq. (3) of Proposition 3.3 into Eq. (7), it suffices to show that

$$q^{n/2}\left(1 - \frac{n(q+1)}{q^2}\right) \geq W(q')2^{t(n)-1}. \tag{8}$$

We combine the above with Lemma 3.2, applied for $a = 8$, and a sufficient condition for $\mathrm{PCN}_q(n) > 0$ would be

$$q^{3n/8}\left(1 - \frac{n(q+1)}{q^2}\right) \geq 4514.7 \cdot 2^{t(n)-1}. \tag{9}$$

By Robin's theorem [17],

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

where γ is the Euler-Mascheroni constant, therefore the condition of Eq. (9) becomes

$$q^{3n/8}\left(1-\frac{n(q+1)}{q^2}\right) > 4514.7\cdot 2^{n\left(\log\log n\cdot e^{0.578}+\frac{0.6483}{\log\log n}\right)-1}.$$

Since the cases $q=n$ and $q=n+1$ are already settled by Corollary 2.2, we check the above for $q\geq n+2$ and verify that it holds for $n>1212$.

A quick computation shows that, within the range $2\leq n\leq 1212$, Eq. (9) is satisfied for all but 42 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 cases when n is a prime or a square of a prime, as in those cases n Theorem 1.3 is implied by Corollary 2.2. For those values for n, we compute the smallest prime power q that satisfies Eq. (9), where $t(n)$ is replaced by its exact value. The results are presented in Table 1. In this region, there is a total of 1162 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
6	8	1259	8	11	431	10	13	223	12	16	419
14	16	107	15	17	79	16	19	137	18	23	179
20	23	139	21	23	49	22	25	59	24	27	243
26	29	49	27	29	41	28	31	89	30	32	173
32	37	79	34	37	41	36	41	193	40	43	113
42	47	121	44	47	61	45	47	49	48	53	191
50	53	59	54	59	97	56	59	81	60	64	256
66	71	83	72	79	211	80	83	101	84	89	181
90	97	163	96	101	163	108	113	151	120	125	311
132	137	139	144	149	211	168	173	229	180	191	311
240	243	343	360	367	439						

Table 1: Values for $2\leq n\leq 984$ that are not primes or square of primes, not satisfying Eq. (9) for q_0, the least prime power $\geq n+2$, where q_1 stands for the least prime power satisfying Eq. (9) for that n.

By combining Eq. (7) and the first bound of Proposition 3.3, we get another condition, namely

$$q^{n/2}\left(1-\sum_{d\mid n}\left(1-\frac{\phi_d(X^{n/d}-1)}{q^n}\right)\right) > W(q')\prod_{i=1}^{k} W_{l_i}(F'_{l_i})\theta_{l_i}(F'_{l_i}). \qquad (10)$$

By using the estimate $W(q')\leq c_{q',16}q^{n/16}$ from Lemma 3.2 and Eq. (10) the list is furtherer reduced to a total of 47 pairs, if we compute all appearing quantities explicitly, in particular the constant $c_{q',16}$ is computed exactly for each value of q' of interest. The list can be shrinked even more, to a total of 37 pairs, if we replace $W(q')$ by its exact value in Eq. (10). These pairs (n,q) are

$(6,8)$, $(6,9)$, $(6,11)$, $(6,13)$, $(6,16)$, $(6,17)$, $(6,19)$, $(6,23)$, $(6,25)$, $(6,29)$, $(6,31)$, $(6,37)$, $(6,43)$, $(6,49)$, $(6,61)$, $(8,11)$, $(8,13)$, $(8,17)$, $(8,19)$, $(8,25)$, $(12,17)$, $(12,19)$, $(12,23)$, $(12,25)$, $(12,29)$, $(12,31)$, $(12,37)$, $(12,41)$, $(12,43)$, $(12,49)$, $(12,61)$, $(12,73)$, $(18,37)$, $(24,29)$, $(24,37)$, $(24,41)$ and $(24,49)$.

However, 24 of those pairs correspond to completely basic extensions, as we directly check the conditions of Theorem 2.1. The remaining 13 pairs are

$(6,8)$, $(6,11)$, $(6,17)$, $(6,23)$, $(6,29)$, $(8,11)$, $(8,19)$, $(12,17)$, $(12,23)$, $(12,29)$, $(12,41)$, $(24,29)$ and $(24,41)$

and they all satisfy $q \leq 97$ or $q^n < 10^{50}$ and examples of primitive completely normal elements are given in [16]. This completes the proof of Theorem 1.3.

5. Proof of Theorem 1.4

Let $n = p^\ell m$, with $(m,p) = 1$ and $m < q$. Our goal is to prove that $\mathrm{PCN}_q(p^\ell m) > 0$ for $\ell \geq 0$ and $m \geq 1$. First, we notice that if $\ell = 0$, then Theorem 1.3 implies Theorem 1.4, hence we only need to consider the case $\ell \geq 1$. Also, the case $m = 1$ is settled by Corollary 2.2, so from this point on, we assume that $\ell \geq 1$ and $m \geq 2$.

The set of proper divisors of n is $\{p^j d \ : \ 0 \leq j \leq \ell,\ d|m\} \setminus \{n\}$. From Theorem 3.1, we get $\mathrm{PCN}_q(n) > 0$ provided that

$$\mathrm{CN}_q(n) > q^{n/2} W(q') \prod_{\substack{j=0,\ldots,\ell,\ d|m \\ (j,d)\neq(\ell,m)}} W_{p^j d}(F'_{p^j d}) \theta_{p^j d}(F'_{p^j d}), \tag{11}$$

where $F'_{p^j d} = X^{m/d} - 1$. Clearly, $\theta_{p^j d}(F'_{p^j d}) < 1$ for all $0 \leq j \leq \ell$, $d|m$ and $W_{p^j d}(X^{m/d} - 1) \leq 2^{m/d}$, so we have

$$\prod_{\substack{j=0,\ldots,\ell,\ d|m \\ (j,d)\neq(\ell,m)}} W_{p^j d}(F'_{p^j d}) \theta_{p^j d}(F'_{p^j d}) < 2^{(\ell+1)\sum_{d|m} m/d - 1} = 2^{(\ell+1)t(m)-1},$$

where $t(m)$ denotes the sum of divisors of m. So a sufficient condition is

$$\mathrm{CN}_q(n) \geq q^{n/2} W(q') 2^{(\ell+1)t(m)-1}. \tag{12}$$

The $p > 2$ case. For $p > 2$, using Eq. (4) from Proposition 3.3 and Lemma 3.2, applied for $a = 8$, we obtain the sufficient condition,

$$q^{3p^\ell m/8} \left(1 - m\left(\frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^p} + \frac{4}{q^{2p}}\right)\right) \geq 2257.35 \cdot 2^{(\ell+1)t(m)}. \tag{13}$$

The RHS of Eq.(13) does not depend on q, while the LHS is an increasing function of q, so, since we are interested in $q > m$ and the case $q = m+1$ or $q \leq 5$ is settled by Corollary 2.2, it suffices to prove Eq. (13) for $q = \max(m+2, 7)$.

First we consider the case $m = 2$. A short calculation shows that the condition becomes

$$q^{3p^\ell/4}\left(1 - 2\left(\frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^p} + \frac{4}{q^{2p}}\right)\right) \geq 2257.35 \cdot 2^{3(\ell+1)},$$

which is satisfied for $q \geq 7$ and $\ell \geq 1$, with the exceptions $(\ell, m, q) = (1, 2, 7)$ or $(1, 2, 9)$.

For $m \geq 3$, we upper bound $t(m)$ by Robin's theorem [17],

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

where γ is the Euler-Mascheroni constant. Furthermore, for $m \leq q - 1$ we have

$$1 - m\left(\frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^p} + \frac{4}{q^{2p}}\right) \geq \frac{m}{q^4}$$

and the condition becomes

$$mq^{3p^\ell m/8-4} \geq 2257.35 \cdot 2^{(\ell+1)\left(e^\gamma m \log\log m + \frac{0.6483m}{\log\log m}\right)}.$$

Since $q \geq m + 2$ and $p \geq 3$, it suffices to show that

$$m(m+2)^{3^{\ell+1}m/8-4} \geq 2257.35 \cdot 2^{(\ell+1)\left(e^\gamma m \log\log m + \frac{0.6483m}{\log\log m}\right)},$$

which is true for $\ell \geq 4$ and $m \geq 3$. The inequality is violated for the following 54 pairs

$$(\ell, m) = (1, 3 \leq m \leq 49), (2, 3 \leq m \leq 8), (3, 3).$$

For those pairs (ℓ, m) we go back to Eq. (13), and check for which prime powers q it is violated. Since the LHS is an increasing function of q, this process will produce one more exceptional triple (ℓ, m, q), namely $(1, 7, 9)$). So, in total there are 3 exceptional triples (ℓ, m, q),

$$(1, 2, 7), (1, 2, 9), (1, 7, 9),$$

but only $(1, 7, 9)$ corresponds to a non completely basic extension, by Theorem 2.1. For this case, an example of primitive completely normal basis is given in [16].

The $p = 2$ case. For $p = 2$, the argument is nearly identical, the only difference being the choice of the bound of Eq. (5) from Proposition 3.3. Since $m > 1$ and $(m, 2) = 1$ we consider only $m \geq 3$, while from Corollary 2.2, it suffices to work with $q \geq 8$.

In Eq. (12), q' is odd and an application of Lemma 3.2 for $a = 8$ yields

$$W(q') \leq 2461.62 \cdot (q')^{1/8} \leq 2461.62 \cdot q^{n/8}.$$

Using this, Eq. (5) from Proposition 3.3 and Eq. (12), we obtain the sufficient condition

$$q^{3\cdot 2^{\ell} m/8}\left(1-m\left(\frac{1}{q}+\frac{1}{q^2}+\frac{2}{3q^3}+\frac{3}{q^4}\right)\right)\geq 2461.62\cdot 2^{(\ell+1)t(m)-1}. \qquad (14)$$

Using Robin's bound and the fact that

$$1-m\left(\frac{1}{q}+\frac{1}{q^2}+\frac{2}{3q^3}+\frac{3}{q^4}\right)\geq \frac{m}{12q^3}$$

we obtain the condition

$$m\cdot q^{3\cdot 2^{\ell} m/8-3}\geq 6\cdot 2461.62\cdot 2^{(\ell+1)\left(e^{\gamma} m\log\log m+\frac{0.6483m}{\log\log m}\right)}.$$

Since $q\geq m+2$, it suffices to show that

$$m\cdot (m+2)^{3\cdot 2^{\ell} m/8-3}\geq 6\cdot 2461.62\cdot 2^{(\ell+1)\left(e^{\gamma} m\log\log m+\frac{0.6483m}{\log\log m}\right)},\ \text{for } m\geq 7$$

and

$$m\cdot 8^{3\cdot 2^{\ell} m/8-3}\geq 6\cdot 2461.62\cdot 2^{(\ell+1)\left(e^{\gamma} m\log\log m+\frac{0.6483m}{\log\log m}\right)},\ \text{for } 3\leq m\leq 5.$$

The above inequalities are true for $\ell\geq 2$ with the exceptions

$$(\ell,m)=(2,3\leq m\leq 157),(3,3\leq m\leq 19),(4,3),(4,5),(5,3),(6,3).$$

For those pairs (ℓ,m) we go back to Eq. (14), and check for which values of $q\geq 8$ that are powers of 2 the condition is violated. Those triples (ℓ,m,q) are

$$(2,3,8),(2,3,16),(2,5,8),(2,7,8),(3,3,8),$$

but only $(2,3,8)$, $(2,5,8)$ and $(3,3,8)$ correspond to a non-completely basic extension, by Theorem 2.1. Examples of primitive completely normal bases for the corresponding extensions are given in [16].

The remaining cases to check are for $\ell=1$, $m\geq 3$ and $q\geq 8$. An application of Lemma 3.2 for $a=12$ yields

$$W(q')\leq 5.61\cdot 10^{23}\cdot (q')^{1/12}\leq 5.61\cdot 10^{23}\cdot q^{n/12}.$$

Using this, Eq. (5) from Proposition 3.3 and Eq. (12), we obtain the sufficient condition

$$q^{5\cdot 2\cdot m/12}\left(1-m\left(\frac{1}{q}+\frac{1}{q^2}+\frac{2}{3q^3}+\frac{3}{q^4}\right)\right)\geq \frac{5.61\cdot 10^{23}}{2}\cdot 2^{2t(m)}.$$

Using Robin's bound it is sufficient to show that for $q\geq m+2$, and $q\geq 8$,

$$q^{5m/6}\frac{m}{12q^3}\geq 2.81\cdot 10^{23}\cdot 4^{e^{\gamma} m\log\log m+\frac{0.6483m}{\log\log m}}.$$

This leads to the conditions

$$m8^{5m/6-3} \geq 12 \cdot 2.81 \cdot 10^{23} \cdot 4^{e^{\gamma} m \log\log m + \frac{0.6483m}{\log\log m}}, \text{ for } 3 \leq m \leq 5,$$
$$m(m+2)^{5m/6-3} \geq 12 \cdot 2.81 \cdot 10^{23} \cdot 4^{e^{\gamma} m \log\log m + \frac{0.6483m}{\log\log m}}, \text{ for } m \geq 7.$$

The conditions are satisfied for $m > 873$. For $3 \leq m \leq 873$, we obtain the following 116 exceptions

$$\begin{aligned}(\ell, m, q) =& (1, 3, 2^3 \leq q \leq 2^{34}), (1, 5, 2^3 \leq q \leq 2^{21}), (1, 7, 2^4 \leq q \leq 2^{16}),\\ & (1, 9, 2^4 \leq q \leq 2^{13}), (1, 11, 2^4 \leq q \leq 2^{11}), (1, 13, 2^4 \leq q \leq 2^9),\\ & (1, 15, 2^5 \leq q \leq 2^{10}), (1, 17, 2^5 \leq q \leq 2^8), (1, 19, 2^5 \leq q \leq 2^7),\\ & (1, 21, 2^5 \leq q \leq 2^8), (1, 23, 2^5 \leq q \leq 2^6), (1, 25, 2^5 \leq q \leq 2^6),\\ & (1, 27, 2^5 \leq q \leq 2^7), (1, 29, 2^5), (1, 33, 64), (1, 35, 64), (1, 45, 64).\end{aligned}$$

After removing the triples which are covered by Corollary 2.2, that is where $m \mid q-1$, the list shrinks to the following list of 85 possible exceptions:

$(1,3,8)$, $(1,3,32)$, $(1,3,128)$, $(1,3,512)$, $(1,3,2048)$, $(1,3,8192)$, $(1,3,32768)$, $(1,3,131072)$, $(1,3,524288)$, $(1,3,2097152)$, $(1,3,8388608)$, $(1,3,33554432)$, $(1,3,134217728)$, $(1,3,536870912)$, $(1,3,2147483648)$, $(1,3,8589934592)$, $(1,5,8)$, $(1,5,32)$, $(1,5,64)$, $(1,5,128)$, $(1,5,512)$, $(1,5,1024)$, $(1,5,2048)$, $(1,5,8192)$, $(1,5,16384)$, $(1,5,32768)$, $(1,5,131072)$, $(1,5,262144)$, $(1,5,524288)$, $(1,5,2097152)$, $(1,7,16)$, $(1,7,32)$, $(1,7,128)$, $(1,7,256)$, $(1,7,1024)$, $(1,7,2048)$, $(1,7,8192)$, $(1,7,16384)$, $(1,7,65536)$, $(1,9,16)$, $(1,9,32)$, $(1,9,128)$, $(1,9,256)$, $(1,9,512)$, $(1,9,1024)$, $(1,9,2048)$, $(1,9,8192)$, $(1,11,16)$, $(1,11,32)$, $(1,11,64)$, $(1,11,128)$, $(1,11,256)$, $(1,11,512)$, $(1,11,2048)$, $(1,13,16)$, $(1,13,32)$, $(1,13,64)$, $(1,13,128)$, $(1,13,256)$, $(1,13,512)$, $(1,15,32)$, $(1,15,64)$, $(1,15,128)$, $(1,15,512)$, $(1,15,1024)$, $(1,17,32)$, $(1,17,64)$, $(1,17,128)$, $(1,19,32)$, $(1,19,64)$, $(1,19,128)$, $(1,21,32)$, $(1,21,128)$, $(1,21,256)$, $(1,23,32)$, $(1,23,64)$, $(1,25,32)$, $(1,25,64)$, $(1,27,32)$, $(1,27,64)$, $(1,27,128)$, $(1,29,32)$, $(1,33,64)$, $(1,35,64)$ and $(1,45,64)$

Each of the above triples, with the sole exception of $(1,3,8)$, satisfy the initial condition of Eq. (11), but the latter is already covered by the examples provided in [16]. This concludes the proof of Theorem 1.4.

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	6	8

Table 2: Pairs (n,q) that were not dealt with theoretically.

6. Conclusions

In this work, a step towards the proof of Conjecture 1.2 was taken. We note that our restrictions $q < n$ and $q < m$ are direct consequences of the lower bounds for $\mathrm{CN}_q(n)$ from Proposition 3.3. For our methods to work more generally, new bounds for $\mathrm{CN}_q(n)$ are required. We believe that this would be an interesting and challenging direction for further research.

Acknowledgments

The authors are grateful to the anonymous referee for his/her comments that significantly improved the quality and readability of this paper.

References

[1] D. Blessenohl and K. Johnsen. Eine verschärfung des satzes von der normalbasis. *J. Algebra*, 103(1):141–159, 1986.

[2] S. D. Cohen and D. Hachenberger. Primitive normal bases with prescribed trace. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):383–403, 1999.

[3] S. D. Cohen and S. Huczynska. The primitive normal basis theorem – without a computer. *J. London Math. Soc.*, 67(1):41–56, 2003.

[4] S. D. Cohen and S. Huczynska. The strong primitive normal basis theorem. *Acta Arith.*, 143(4):299–332, 2010.

[5] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.

[6] S. Gao. *Normal Basis over Finite Fields.* PhD thesis, University of Waterloo, 1993.

[7] D. Hachenberger. *Finite Fields: Normal Bases and Completely Free Elements*, volume 390 of *Kluwer Internat. Ser. Engrg. Comput. Sci.* Kluwer Academic Publishers, Boston, MA, 1997.

[8] D. Hachenberger. Primitive complete normal bases: Existence in certain 2-power extensions and lower bounds. *Discrete Math.*, 310(22):3246–3250, 2010.

[9] D. Hachenberger. Completely normal bases. In G. L. Mullen and D. Panario, editors, *Handbook of Finite Fields*, pages 128–138. CRC Press, Boca Raton, 2013.

[10] D. Hachenberger. Asymptotic existence results for primitive completely normal elements in extensions of Galois fields. *Des. Codes Cryptogr.*, 80(3):577–586, 2016.

[11] C. Hsu and T. Nan. A generalization of the primitive normal basis theorem. *J. Number Theory*, 131(1):146–157, 2011.

[12] G. Kapetanakis. An extension of the (strong) primitive normal basis theorem. *Appl. Algebra Engrg. Comm. Comput.*, 25(5):311–337, 2014.

[13] G. Kapetanakis. Normal bases and primitive elements over finite fields. *Finite Fields Appl.*, 26:123–143, 2014.

[14] H. W. Lenstra, Jr and R. J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.

[15] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, Cambridge, second edition, 1997.

[16] I. H. Morgan and G. L. Mullen. Completely normal primitive basis generators of finite fields. *Util. Math.*, 49:21–43, 1996.

[17] G. Robin. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann. *J. Math. Pures Appl.*, 63(2):187–213, 1984.