Noname manuscript No.
(will be inserted by the editor)

Further results on the Morgan-Mullen conjecture

Theodoulos Garefalakis · **Giorgos Kapetanakis**

the date of receipt and acceptance should be inserted later

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. The conjecture of Morgan and Mullen asserts the existence of primitive and completely normal elements (PCN elements) for the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ for any q and n. It is known that the conjecture holds for $n \leq q$. In this work we prove the conjecture for a larger range of exponents. In particular, we give sharper bounds for the number of completely normal elements and use them to prove asymptotic and effective existence results for $q \leq n \leq O(q^{\varepsilon})$, where $\varepsilon = 2$ for the asymptotic results and $\varepsilon = 1.25$ for the effective ones. For n even we need to assume that $q-1 \nmid n$.

Keywords finite fields · completely normal element · primitive element · normal basis · completely normal basis

Mathematics Subject Classification (2000) 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.

Theodoulos Garefalakis
Department of Mathematics and Applied Mathematics, University of Crete, Voutes Campus, 70013 Heraklion, Greece
E-mail: tgaref@uoc.gr
Giorgos Kapetanakis
Sabanci University, FENS, Orhanli-Tuzla, 34956 Istanbul, Turkey
E-mail: gnkapet@gmail.com

It is well-known that primitive and normal elements exist for every q and n, see Chapter 2 of [16]. 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 $\mathbb{F}_q$.*

Lenstra and Schoof [15] 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 [2,4,12–14].

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 [17] 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 [17]. This conjecture is yet to be completely resolved. Partial results, covering certain types of extensions have been given, see [10] and the references therein. Recently, Hachenberger [11], using elementary methods, proved the validity of Conjecture 1.2 for $q \geq n^3$ and $n \geq 37$. In [7], the range was improved to $n \leq q$.

In this work we extend the range for which Conjecture 1.2 holds. In particular, we prove the following theorems:

Theorem 1.3 *There exists $c \in \mathbb{N}$ such that for every prime power $q \geq c$ and every $n \in \mathbb{N}$ satisfying*

1. *n odd, and $q \leq n \leq q^2$, or*
2. *n even, $q-1 \nmid n$ and $q \leq n \leq 0.43 \cdot q^2$,*

there exists a primitive and completely normal element for the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$

Theorem 1.4 *Let q be a prime power and n an integer. There exists a primitive element of $\mathbb{F}_{q^n}$ that is completely normal over $\mathbb{F}_q$ in the following cases:*

1. *n is odd and $n < q^{4/3}$ and*
2. *n is even, $q-1 \nmid n$ and $n < q^{5/4}$.*

In Section 2, we prove our main technical tool, Theorem 2.1. In Section 3, we prove some new bounds for the number of completely normal elements. In Section 4 we combine Theorem 2.1 and the bounds of Section 3 to establish Theorem 1.3. Next, in Section 5, we combine Theorem 2.1 and the bounds of Section 3 to establish Theorem 1.4, for all but a small number of possible exceptions, that are dealt with, either by employing the Cohen-Huczynska [3,4] sieving techniques, or by relying on the Morgan-Mullen [17] examples. We conclude this work with some remarks about possible further improvements in Section 6.

2 Preliminaries

The notion of primitivity can be generalized as follows. We call $x \in \mathbb{F}_{q^n}$ *r-free*, where $r \mid q^n - 1$, if $x = y^d$ for some $d \mid r$ and $y \in \mathbb{F}_{q^n}$ implies $d = 1$. Clearly, the primitive elements are exactly the q'-primitive elements, where q' is the square-free part of $q^n - 1$. In

addition, notice that r-freeness depends solely on the prime divisors of r, that is one may freely interchange between r and its square-free part.

By using Vinogradov's formula for generators of cyclic modules over Euclidean domains, it can be shown that the characteristic function for r-free elements of $\mathbb{F}_{q^n}$, where $r \mid q'$, is

$$\omega_r(x) := \theta(r) \sum_{\chi \in \widehat{\mathbb{F}^*_{q^n}},\ \mathrm{ord}(\chi) \mid r} \frac{\mu(\mathrm{ord}(\chi))}{\phi(\mathrm{ord}(\chi))} \chi(x),$$

where $\theta(r) := \phi(r)/r$, μ is the Möbius function, ϕ is the Euler function and the *order* of the multiplicative character χ, denoted as $\mathrm{ord}(\chi)$, is defined as its multiplicative order in $\widehat{\mathbb{F}^*_{q^n}}$. Also, for the sake of simplicity, we denote $\omega := \omega_{q'}$, thus ω is the characteristic function for primitive elements.

Similarly, the characteristic function for elements of $\mathbb{F}_{q^n}$ that are normal over $\mathbb{F}_{q^l}$ is

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

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 $\mathbb{F}_{q^l}[X]$ respectively and the *order* of an additive character ψ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^l}$, denoted as $\mathrm{ord}_l(\psi)$, is defined as the lowest degree monic polynomial $G = \sum_{i=0}^m G_i X^i \in \mathbb{F}_{q^l}[X]$, such that $\psi\left(\sum_{i=0}^m G_i x^{q^i}\right) = 1$ for all $x \in \mathbb{F}_{q^n}$. It is straightforward to check that $\mathrm{ord}_l(\psi) \mid X^{n/l}-1$ in $\mathbb{F}_{q^l}[X]$.

Let $\mathrm{CN}_q^r(n)$ be the number of r-free completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\mathrm{PCN}_q(n)$ be the number of primitive completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, so that $\mathrm{PCN}_q(n) = \mathrm{CN}_q^{q'}(n)$. Further, 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. Noting that

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

we obtain

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

The following theorem is a direct generalization of [7, Theorem 3.1] and it is the main technical result from which all the sufficient conditions in the proofs of Theorems 1.3 and 1.4 are derived.

Theorem 2.1 *Let q be a prime power, $n \in \mathbb{N}$ and r a square-free divisor of q^n-1, then*

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

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 $\mathbb{F}_{q^{l_i}}[X]$.

Proof Using the characteristic functions, as presented earlier, we deduce that

$$\begin{aligned}
\mathrm{CN}_q^r(n) &= \sum_{x \in \mathbb{F}_{q^n}} \left(\omega_r(x)\Omega_{l_1}(x)\cdots\Omega_{l_k}(x)\right) \\
&= \theta(r)\theta(\mathbf{q}) \sum_{\chi} \sum_{(\psi_1,\ldots,\psi_k)} \frac{\mu(\chi)}{\phi(\chi)} \prod_{i=1}^{k} \frac{\mu_{l_i}(\mathrm{ord}_{l_i}(\psi_i))}{\phi_{l_i}(\mathrm{ord}_{l_i}(\psi_i))} \sum_{x \in \mathbb{F}_{q^n}} \psi_1 \cdots \psi_k(x)\chi(x) \\
&= \theta(r)\theta(\mathbf{q})(S_1 + S_{2,r}),
\end{aligned}$$

where the term S_1 is the part of the above sum that corresponds to $\chi = \chi_0$, the trivial character. It follows that

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

Also, $S_{2,r}$ is the part that corresponds to $\chi \neq \chi_0$,

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

In the last sum, note that the summations runs on multiplicative characters χ of order dividing r 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

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

where we used the orthogonality relations and the well-known fact that for non-trivial χ and ψ the absolute value of the Gauss sum $\sum_{x \in \mathbb{F}_{q^n}} \psi(x)\chi(x)$ is bounded by $q^{n/2}$. The result follows. □

The following lemma is used to estimate $W(q')$, that appears above.

Lemma 2.2 *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 $p_1, \ldots, p_s$ are the primes $\le 2^a$ that divide r. In particular, $c_{r,4} < 4.9$, $c_{r,12} < 1.06 \cdot 10^{24}$ for all $r \in \mathbb{N}$.*

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 $p_1, \ldots, p_s, q_1, \ldots, q_t$ are distinct primes and $p_i \le 2^a$ and $q_j > 2^a$. We have that

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

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

3 Completely normal elements

In this section, we prove a new lower bound for $\mathrm{CN}_q(n)$. Let p be the characteristic of $\mathbb{F}_q$ and $n = p^\ell m$, with $(m,p) = 1$. The number of elements of $\mathbb{F}_{q^n}$ that are *not* completely normal over $\mathbb{F}_q$ is at most $\sum_{d|n}(q^n - \phi_d(X^{n/d}-1))$. Our starting point is the following bound.

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

Expressing the divisors of n as $p^j d$, $0 \leq j \leq \ell$, $d \,|\, m$, we have

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

We denote $\nu_{p^j d}(k) = \mathrm{ord}_k(q^{p^j d})$ and to simplify notation, we let $\nu(k) = \nu_1(k)$. Then

$$\phi_{p^j d}\left((X^{m/d}-1)^{p^{\ell-j}}\right) = q^{p^\ell m}\prod_{k|(m/d)}\left(1 - \frac{1}{q^{p^j d \nu_{p^j d}(k)}}\right)^{\frac{\phi(k)}{\nu_{p^j d}(k)}}.$$

For $0 \leq j \leq \ell$ and $d \mid m$ we have

$$\begin{aligned}
\phi_{p^j d}\left((X^{m/d}-1)^{p^{\ell-j}}\right) &\geq q^{p^\ell m}\prod_{k|(m/d)}\left(1 - \frac{1}{q^{p^j d}}\right)^{\phi(k)} \\
&\geq q^{p^\ell m}\left(1 - \frac{1}{q^{p^j d}}\right)^{\frac{m}{d}} \\
&\geq q^{p^\ell m}\left(1 - \frac{m}{dq^{p^j d}}\right).
\end{aligned}$$

Therefore,

$$1 - \frac{\phi_{p^j d}\left((X^{m/d}-1)^{p^{\ell-j}}\right)}{q^{p^\ell m}} \leq \frac{m}{dq^{p^j d}}, \quad \text{for } 0 \leq j \leq \ell,\ d \,|\, m. \tag{2}$$

This bound is sufficient for all pairs (j,d), except for $j = 0$ and $d = 1$, which we consider separately.

$$\phi_1\left((X^m-1)^{p^\ell}\right) = q^{p^\ell m}\prod_{k|m}\left(1 - \frac{1}{q^{\nu(k)}}\right)^{\frac{\phi(k)}{\nu(k)}}.$$

Let $g = (m, q-1)$. Then $\nu(k) = 1$ if and only if $q \equiv 1 \pmod{k}$, which holds if and only if $k \,|\, g$. We have

$$\frac{\phi_1\left((X^m-1)^{p^\ell}\right)}{q^{p^\ell m}} = \prod_{k|g}\left(1 - \frac{1}{q}\right)^{\phi(k)}\prod_{\substack{k|m \\ k\nmid g}}\left(1 - \frac{1}{q^{\nu(k)}}\right)^{\frac{\phi(k)}{\nu(k)}}.$$

The first product is equal to $(1-1/q)^g$, while the second is bounded as follows.

$$\begin{aligned}\prod_{\substack{k|m\\ k\nmid g}}\left(1-\frac{1}{q^{\nu(k)}}\right)^{\frac{\phi(k)}{\nu(k)}} &\geq \prod_{\substack{k|m\\ k\nmid g}}\left(1-\frac{1}{q^2}\right)^{\frac{\phi(k)}{2}}\\ &= \prod_{k|m}\left(1-\frac{1}{q^2}\right)^{\frac{\phi(k)}{2}}\prod_{k|g}\left(1-\frac{1}{q^2}\right)^{-\frac{\phi(k)}{2}}\\ &= \left(1-\frac{1}{q^2}\right)^{\frac{m-g}{2}}.\end{aligned}$$

Therefore, we have

$$\begin{aligned}\frac{\phi_1\left((X^m-1)^{p^\ell}\right)}{q^{p^\ell m}} &\geq \left(1-\frac{1}{q}\right)^g\left(1-\frac{1}{q^2}\right)^{\frac{m-g}{2}}\\ &= \left(1-\frac{1}{q}\right)^{\frac{g}{2}}\left(1+\frac{1}{q}\right)^{-\frac{g}{2}}\left(1-\frac{1}{q^2}\right)^{\frac{m}{2}}\\ &= \left(1-\frac{2}{q+1}\right)^{\frac{g}{2}}\left(1-\frac{1}{q^2}\right)^{\frac{m}{2}}\\ &\geq \left(1-\frac{g}{q+1}\right)\left(1-\frac{m}{2q^2}\right),\end{aligned}$$

and we get

$$1-\frac{\phi_1\left((X^m-1)^{p^\ell}\right)}{q^{p^\ell m}} \leq \frac{g}{q+1}+\frac{m}{2q^2}-\frac{gm}{2q^2(q+1)}. \tag{3}$$

Combining Eqs. (1), (2) and (3), we obtain

$$\frac{\mathrm{CN}_q(p^\ell m)}{q^{p^\ell m}} \geq 1-\frac{g}{q+1}-\frac{m}{2q^2}+\frac{gm}{2q^2(q+1)}-\sum_{\substack{d|m\\ d>1}}\sum_{j=0}^{\ell}\frac{m}{dq^{p^j d}}-\sum_{j=1}^{\ell}\frac{m}{q^{p^j}}. \tag{4}$$

We proceed to upper bound the sums in the last expression.

$$\sum_{j=1}^{\ell}\frac{m}{q^{p^j}} \leq \frac{m}{q^p}+\sum_{j=2}^{\infty}\frac{m}{q^{pj}} = \frac{m}{q^p}+\frac{m}{q^{2p}(1-q^{-p})},$$

and

$$\begin{aligned}\sum_{j=0}^{\ell}\frac{m}{dq^{p^j d}} &\leq \frac{m}{d}\left(\frac{1}{q^d}+\sum_{j=1}^{\infty}\frac{1}{q^{pdj}}\right)\\ &\leq \frac{m}{d}\left(\frac{1}{q^d}+\frac{1}{q^{pd}(1-q^{-pd})}\right)\\ &\leq \frac{m}{d}\left(\frac{1}{q^d}+\frac{64}{63q^{pd}}\right),\end{aligned}$$

where we used the fact that $pd \geq 6$, therefore $1/(1-q^{-pd}) \leq 64/63$.

We now consider two cases. For m odd, we have

$$\begin{aligned}\sum_{\substack{d|m\\ d>1}}\sum_{j=0}^{\ell}\frac{m}{dq^{p^j d}} &\le \sum_{\substack{d|m\\ d>1}}\frac{m}{dq^d}+\sum_{\substack{d|m\\ d>1}}\frac{64m}{63dq^{pd}}\\ &\le \frac{m}{3q^3}+\sum_{d=5}^{\infty}\frac{m}{5q^d}+\sum_{d=3}^{\infty}\frac{64m}{63\cdot 3q^{pd}}\\ &\le \frac{m}{3q^3}+\frac{2m}{5q^5}+\frac{m}{2q^6}.\end{aligned}$$

Therefore,

$$\sum_{\substack{d|m\\ d>1}}\sum_{j=0}^{\ell}\frac{m}{dq^{p^j d}}+\sum_{j=1}^{\ell}\frac{m}{q^{p^j}} \le \frac{m}{q^p}+\frac{m}{3q^3}+\frac{2m}{q^4}+\frac{2m}{5q^5}+\frac{m}{2q^6}. \tag{5}$$

For m even, we have $p \ge 3$ and

$$\sum_{\substack{d|m\\ d>1}}\sum_{j=0}^{\ell}\frac{m}{dq^{p^j d}} \le \sum_{d\ge 2}\frac{m}{dq^d}+\sum_{d\ge 2}\frac{64m}{63dq^{pd}}.$$

For the sums involved, we have

$$\sum_{d\ge 2}\frac{m}{dq^d} \le \frac{m}{2q^2}+\frac{m}{3q^3}+\frac{m}{4q^4}\sum_{d\ge 0}\frac{1}{q^d} \le \frac{m}{2q^2}+\frac{m}{3q^3}+\frac{m}{2q^4},$$

where we used the fact that $q/(q-1) < 2$. Similarly,

$$\sum_{d\ge 2}\frac{64m}{63dq^{pd}} \le \frac{64m}{63\cdot 2}\sum_{d\ge 2}\frac{1}{q^{3d}} \le \frac{32}{63}\cdot\frac{m}{q^6}\cdot\frac{q^3}{q^3-1} \le \frac{48m}{91q^6},$$

since $q^3/(q^3-1) \le 27/26$. We conclude that

$$\sum_{\substack{d|m\\ d>1}}\sum_{j=0}^{\ell}\frac{m}{dq^{p^j d}} \le \frac{m}{2q^2}+\frac{m}{3q^3}+\frac{m}{2q^4}+\frac{48m}{91q^6}.$$

Therefore,

$$\sum_{\substack{d|m\\ d>1}}\sum_{j=0}^{\ell}\frac{m}{dq^{p^j d}}+\sum_{j=1}^{\ell}\frac{m}{q^{p^j}} \le \frac{m}{2q^2}+\frac{4m}{3q^3}+\frac{m}{2q^4}+\frac{8m}{5q^6}. \tag{6}$$

We are now ready to prove the following proposition.

Proposition 3.1 *Let $\mathbb{F}_q$ be the finite field of characteristic p, and $n = p^\ell m$, with $\ell \ge 1$, $m \ge 1$, $(m,p) = 1$.*

1. *For m even*

$$\mathrm{CN}_q(n) \ge q^n\left(1-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}-\frac{m}{q^2}-\frac{4m}{3q^3}-\frac{m}{2q^4}-\frac{8m}{5q^6}\right).$$

2. *For m odd*

$$\mathrm{CN}_q(n) \ge q^n\left(1-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}-\frac{m}{2q^2}-\frac{m}{q^p}-\frac{m}{3q^3}-\frac{2m}{q^4}-\frac{2m}{5q^5}-\frac{m}{2q^6}\right).$$

Proof For m even, Eq. (4) combined with the bound in Eq. (6), we have

$$\begin{aligned}\frac{\mathrm{CN}_q(n)}{q^n} &\geq 1-\frac{g}{q+1}-\frac{m}{2q^2}+\frac{gm}{2q^2(q+1)}-\frac{m}{2q^2}-\frac{4m}{3q^3}-\frac{m}{2q^4}-\frac{8m}{5q^6}\\ &\geq 1-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}-\frac{m}{q^2}-\frac{4m}{3q^3}-\frac{m}{2q^4}-\frac{8m}{5q^6}.\end{aligned}$$

The bound for m odd follows similarly from Eqs. (4) and (5). □

For $\ell = 0$, that is, $(n,p) = 1$, we have slightly tighter bounds.

Proposition 3.2 *Let $\mathbb{F}_q$ be the finite field of characteristic p, and $n \geq 1$, $(n,p) = 1$.*

1. *For n even*
$$\mathrm{CN}_q(n) \geq q^n\left(1-\frac{g}{q+1}+\frac{gn}{2q^2(q+1)}-\frac{n}{q^2}-\frac{n}{2q^3}\right).$$
2. *For n odd*
$$\mathrm{CN}_q(n) \geq q^n\left(1-\frac{g}{q+1}+\frac{gn}{2q^2(q+1)}-\frac{n}{2q^2}-\frac{n}{3q^3}-\frac{n}{2q^4}\right).$$

Proof For the first bound,

$$\begin{aligned}\mathrm{CN}_q(n) &\geq q^n\left(1-\frac{g}{q+1}+\frac{gn}{2q^2(q+1)}-\frac{n}{2q^2}-\sum_{\substack{d\mid n\\ d>1}}\frac{n}{dq^d}\right)\\ &\geq q^n\left(1-\frac{g}{q+1}+\frac{gn}{2q^2(q+1)}-\frac{n}{q^2}-\frac{n}{2q^3}\right)\end{aligned}$$

For the second bound,

$$\begin{aligned}\mathrm{CN}_q(n) &\geq q^n\left(1-\frac{g}{q+1}+\frac{gn}{2q^2(q+1)}-\frac{n}{2q^2}-\sum_{\substack{d\mid n\\ d>1}}\frac{n}{dq^d}\right)\\ &\geq q^n\left(1-\frac{g}{q+1}+\frac{gn}{2q^2(q+1)}-\frac{n}{2q^2}-\frac{n}{3q^3}-\frac{n}{2q^4}\right).\end{aligned}$$

□

Corollary 3.3 *Let $\mathbb{F}_q$ be the finite field of characteristic p, and $n = p^\ell m$, with $\ell \geq 1$, $1 \leq m < 2q^2$, $(m,p) = 1$, and $(q-1) \nmid m$.*

1. *For m even, $q \geq 9$*
$$\mathrm{CN}_q(n) \geq q^n\left(\frac{1}{2}+\frac{1}{q+1}-\frac{0.96\cdot m}{q^2}\right).$$
2. *For m odd, $q \geq 8$ and $p = 2$*
$$\mathrm{CN}_q(n) \geq q^n\left(\frac{2}{3}+\frac{2}{3(q+1)}-\frac{1.45\cdot m}{q^2}\right).$$

Proof We proceed to prove the first bound. In the RHS expressions of the inequalities of Proposition 3.1, the quantity

$$-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}=-\frac{g}{q+1}\left(1-\frac{m}{2q^2}\right)$$

is a decreasing function of g, since $m<2q^2$. Assuming that $g\leq(q-1)/2$, we have

$$\begin{aligned}
&1-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}-\frac{m}{q^2}-\frac{4m}{3q^3}-\frac{m}{2q^4}-\frac{8m}{5q^6}\\
\geq\ &1-\frac{q-1}{2(q+1)}+\frac{(q-1)m}{4q^2(q+1)}-\frac{m}{q^2}-\frac{4m}{3q^3}-\frac{m}{2q^4}-\frac{8m}{5q^6}\\
=\ &\frac{1}{2}+\frac{1}{q+1}-\frac{m}{q^2}\left(-\frac{q-1}{4(q+1)}+1+\frac{4}{3q}+\frac{1}{2q^2}+\frac{8}{5q^4}\right)\\
\geq\ &\frac{1}{2}+\frac{1}{q+1}-\frac{0.96\cdot m}{q^2}.
\end{aligned}$$

For the second bound, letting $g\leq(q-1)/3$, we have

$$\begin{aligned}
&1-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}-\frac{m}{2q^2}-\frac{m}{q^p}-\frac{m}{3q^3}-\frac{2m}{q^4}-\frac{2m}{5q^5}-\frac{m}{2q^6}\\
\geq\ &1-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}-\frac{3m}{2q^2}-\frac{m}{3q^3}-\frac{2m}{q^4}-\frac{2m}{5q^5}-\frac{m}{2q^6}\\
\geq\ &1-\frac{q-1}{3(q+1)}+\frac{(q-1)m}{6q^2(q+1)}-\frac{3m}{2q^2}-\frac{m}{3q^3}-\frac{2m}{q^4}-\frac{2m}{5q^5}-\frac{m}{2q^6}\\
=\ &\frac{2}{3}+\frac{2}{3(q+1)}-\frac{m}{q^2}\left(-\frac{q-1}{6(q+1)}+\frac{3}{2}+\frac{1}{3q}+\frac{2}{q^2}+\frac{2}{5q^3}+\frac{1}{2q^4}\right)\\
\geq\ &\frac{2}{3}+\frac{2}{3(q+1)}-\frac{1.45\cdot m}{q^2}
\end{aligned}$$

□

Corollary 3.4 *Let $\mathbb{F}_q$ be of characteristic p, $n=p^\ell m$, with $\ell\geq 1$, $(m,p)=1$. Assume that $m<2q^2$ is odd, $p\geq 3$ and $q\geq 9$. Then*

$$\mathrm{CN}_q(n)\geq q^n\left(\frac{2}{q+1}-\frac{2.735\cdot m}{q^2(q+1)}\right).$$

Proof The proof is very similar to that of Corollary 3.3. We compute

$$\begin{aligned}
&1-\frac{g}{q+1}+\frac{gm}{2q^2(q+1)}-\frac{m}{2q^2}-\frac{m}{q^p}-\frac{m}{3q^3}-\frac{2m}{q^4}-\frac{2m}{5q^5}-\frac{m}{2q^6}\\
\geq\ &1-\frac{q-1}{q+1}+\frac{(q-1)m}{2q^2(q+1)}-\frac{m}{2q^2}-\frac{4m}{3q^3}-\frac{2m}{q^4}-\frac{2m}{5q^5}-\frac{m}{2q^6}\\
=\ &\frac{2}{q+1}-\frac{m}{q^2(q+1)}\left(-\frac{q-1}{2}+\frac{q+1}{2}+\frac{4(q+1)}{3q}+\frac{2(q+1)}{q^2}+\frac{2(q+1)}{5q^3}+\frac{q+1}{2q^4}\right)\\
\geq\ &\frac{2}{q+1}-\frac{2.735\cdot m}{q^2(q+1)}.
\end{aligned}$$

□

The next corollary follows similarly from Proposition 3.2.

Corollary 3.5 *Let $\mathbb{F}_q$ be of characteristic p, and $1 \leq n < 2q^2$, $(n,p) = 1$.*

1. *For n even, $q \geq 9$ and $q-1 \nmid n$,*
$$\mathrm{CN}_q(n) \geq q^n \left(\frac{1}{2} + \frac{1}{q+1} - \frac{0.86 \cdot n}{q^2} \right).$$
2. *For n odd, $q \geq 8$*
$$\mathrm{CN}_q(n) \geq q^n \left(\frac{2}{q+1} - \frac{1.45 \cdot n}{q^2(q+1)} \right).$$

Proof For the first item, in Proposition 3.2, we assume that $g \leq (q-1)/2$, hence

$$\begin{aligned} \mathrm{CN}_q(n) &\geq q^n \left(1 - \frac{q-1}{2(q+1)} + \frac{(q-1)n}{4q^2(q_1)} - \frac{n}{q^2} - \frac{n}{2q^3} \right) \\ &= q^n \left(\frac{1}{2} + \frac{1}{q+1} - \frac{n}{q^2} \left(\frac{3}{4} + \frac{1}{2(q+1)} + \frac{1}{2q} \right) \right) \\ &\geq q^n \left(\frac{1}{2} + \frac{1}{q+1} - \frac{0.86 \cdot n}{q^2} \right). \end{aligned}$$

□

Theorem 3.6 *Let $\mathbb{F}_q$ be of characteristic p, $n \in \mathbb{N}$ odd and $q \geq 8$. Then*

1. *For n odd, $q \geq 8$,*
$$\mathrm{CN}_q(n) \geq q^n \left(\frac{2}{q+1} - \frac{1.45 \cdot n}{q^2(q+1)} \right). \tag{7}$$
2. *For n even, $q \geq 9$, $q-1 \nmid n$,*
$$\mathrm{CN}_q(n) \geq q^n \left(\frac{1}{2} + \frac{1}{q+1} - \frac{0.86 \cdot n}{q^2} \right). \tag{8}$$

Proof We first note that we may assume that $n < 2q^2$, since otherwise the bounds hold trivially. For the bound in Eq. (7), let $n = p^\ell m$, with $(m,p) = 1$. First we consider the case $\ell \geq 1$. In this case, $p \geq 3$, $n \geq 3m$ and Corollary 3.4 implies that

$$\mathrm{CN}_q(n) \geq q^n \left(\frac{2}{q+1} - \frac{0.92 \cdot n}{q^2(q+1)} \right).$$

Suppose now that $\ell = 0$, so that $(n,p) = 1$. In this case, the stated bound is that of Corollary 3.5.

For the bound in Eq. (8), we first consider the case $p = 2$, that is $n = 2^\ell m$, $\ell \geq 1$, m odd. In this case, from Corollary 3.3,

$$\mathrm{CN}_q(n) \geq q^n \left(\frac{2}{3} + \frac{2}{3(q+1)} - \frac{1.45 \cdot m}{q^2} \right) \geq q^n \left(\frac{2}{3} + \frac{2}{3(q+1)} - \frac{0.725 \cdot n}{q^2} \right).$$

Next, we consider the case $p \geq 3$ and $n = p^\ell m$, with $\ell \geq 1$ and m even. From Corollary 3.3,

$$\mathrm{CN}_q(n) \geq q^n \left(\frac{1}{2} + \frac{1}{q+1} - \frac{0.96 \cdot m}{q^2} \right) \geq q^n \left(\frac{1}{2} + \frac{1}{q+1} - \frac{0.32 \cdot n}{q^2} \right).$$

Finally, we consider the case $p \geq 3$, n even and $(n,p) = 1$. From Corollary 3.5, we have

$$\mathrm{CN}_q(n) \geq q^n \left(\frac{1}{2} + \frac{1}{q+1} - \frac{0.86 \cdot n}{q^2} \right).$$

One easily checks that among the last three bounds, the latter is the weakest. □

4 Proof of Theorem 1.3

From Theorem 2.1, we get $\mathrm{PCN}_q(n) > 0$ provided that

$$\mathrm{CN}_q(n) > q^{n/2} W(q') \prod_{i=1}^{k} W_{l_i}(F'_{l_i}) \theta_{l_i}(F'_{l_i}). \tag{9}$$

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

$$\prod_{i=1}^{k} W_{l_i}(F'_{l_i}) \theta_{l_i}(F'_{l_i}) < 2^{\sum_{i=1}^{k} n/l_i} = 2^{t(n)-1}, \tag{10}$$

where t stands for the sum-of-divisors function. We now consider the case n odd. From Theorem 3.6, Lemma 2.2 and Eqs. (9) and (10), we obtain the sufficient condition

$$q^{n/4} \left(\frac{2}{q+1} - \frac{1.45 \cdot n}{q^2(q+1)} \right) \geq 4.9 \cdot 2^{t(n)-1}.$$

By Robin's theorem [18],

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

where γ is the Euler-Mascheroni constant, hence the latter becomes

$$q^{n/4} \left(\frac{2}{q+1} - \frac{1.45 \cdot n}{q^2(q+1)} \right) \geq 4.9 \cdot 2^{n\left(\log\log n \cdot e^{0.578} + \frac{0.6483}{\log\log n}\right) - 1}. \tag{11}$$

Assuming $n \geq 285$, a simple calculation shows that

$$4.9 \cdot 2^{n\left(\log\log n \cdot e^{0.578} + \frac{0.6483}{\log\log n}\right) - 1} \leq 2.5 \cdot 2^{2n\log\log n},$$

and since $n \leq q^2$ we obtain the condition

$$\frac{0.55 \cdot q^{n/4}}{q+1} \geq 2.5 \cdot 2^{2n\log\log n}. \tag{12}$$

Since $q^2 \geq n \geq 285$, we have $q \geq 16$, so that $q+1 \leq 1.0625 \cdot q$ and the condition becomes

$$q^{n/4-1} \geq 4.83 \cdot 4^{n\log\log n}.$$

Since $q \geq \sqrt{n}$, it suffices

$$\frac{n-4}{8} \log n \geq n \log\log n \cdot \log 4 + \log 4.83,$$

which is true for n large enough.

For n even, a similar argument leads to the sufficient condition

$$q^{n/4} \left(\frac{1}{2} + \frac{1}{q+1} - \frac{0.86 \cdot n}{q^2} \right) \geq 2.5 \cdot 4^{n\log\log n}.$$

For $n \leq 0.43 \cdot q^2$ we obtain the sufficient condition

$$\frac{q^{n/4}}{q+1} \geq 2.5 \cdot 4^{n\log\log n}$$

which is actually weaker than Eq.(12), and holds for n large enough. The proof of Theorem 1.3 is now complete.

5 Proof of Theorem 1.4

Before we move on to the proof, we note that, in addition to the special cases mentioned in [10], 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 $\mathbb{F}_{q^n}$ 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 [10, Theorem 5.4.18] and, for a proof, see [8, Section 15].

Theorem 5.1 ([8], Section 15) *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 $(n/r)'$.*

The proof of Theorem 1.4 relies on computations performed with SAGEMATH. We describe our steps for each item separately.

Case 1: n odd Following the same steps as those that led us to Eq. (11), except that we now choose $a = 12$ for the constant of Lemma 2.2, we obtain the condition

$$q^{5n/12}\left(\frac{2}{q+1}-\frac{1.45\cdot n}{q^2(q+1)}\right) \geq 1.06\cdot 10^{24}\cdot 2^{n\left(\log\log n\cdot e^{0.578}+\frac{0.6483}{\log\log n}\right)-1}.$$

First, notice that the LHS of the latter is an increasing function of q in the interval $n^{3/4} < q < n$, so it suffices to check its validity for $q = n^{3/4}$. It follows that the case $n \geq 14561$ is settled.

Then we replace the term $2^{n\left(\log\log n\cdot e^{0.578}+\frac{0.6483}{\log\log n}\right)-1}$ by $2^{t(n)-1}$ and, as before, q by $n^{3/4}$ and check the resulting inequality for every $n < 14561$, where $t(n)$ is computed explicitly for every n. The resulting inequality holds for every n, with the exception of 51 odd integers, with 135 being the largest among them and for those n, we list all possible pairs (q,n), where q is a prime power with $n^{3/4} < q < n$. This leads to a list of 590 possible exceptional pairs.

This list is immediately reduced to a list of 31 pairs, once $1.06\cdot 10^{24}$ is replaced by the exact value of $c_{q',12}$, as described in Lemma 2.2, while all, but the 7 pairs (q,n)

$$(9,21),\ (11,21),\ (16,21),\ (17,21),\ (11,27),\ (13,27) \text{ and } (16,27)$$

correspond to completely basic extensions.

Finally, all 7 pairs satisfy the condition

$$q^{n/2}\left(\frac{2}{q+1}-\frac{1.45\cdot n}{q^2(q+1)}\right) > W(q')\prod_{i=1}^{k} W_{l_i}(F'_{l_i})\theta_{l_i}(F'_{l_i})$$

if we compute every appearing value explicitly.

Case 2: n even As in the previous case, we begin with the condition

$$q^{5n/12}\left(\frac{1}{2}+\frac{1}{q+1}-\frac{0.86\cdot n}{q^2}\right) \geq 1.06\cdot 10^{24}\cdot 2^{n\left(\log\log n\cdot e^{0.578}+\frac{0.6483}{\log\log n}\right)-1}.$$

Again, we replace q by $n^{4/5}$ and verify that the latter holds for $n \geq 5719$.

Then we replace the term $2^{n\left(\log\log n\cdot e^{0.578}+\frac{0.6483}{\log\log n}\right)-1}$ by $2^{t(n)-1}$ and, as before, q by $n^{4/5}$ and check the resulting inequality for every $n < 5719$, where $t(n)$ is computed explicitly for

every n. The resulting inequality holds for every n, with the exception of 114 even integers, with 1680 being the largest among them and for those n, we list all possible pairs (q,n), where q is a prime power with $n^{4/5} < q < n$. This leads to a list of 3250 possible exceptional pairs.

This list is furtherly reduced to 536 pairs, once $1.06 \cdot 10^{24}$ is replaced by the exact value of $c_{q',12}$, as described in Lemma 2.2 and, consequently, to 441 pairs if we exclude the pairs that turn out to correspond to completely normal extensions.

Our next step is to check the condition

$$q^{n/2}\left(\frac{1}{2}+\frac{1}{q+1}-\frac{0.86\cdot n}{q^2}\right) \geq W(q')\cdot 2^{t(n)-n-1}W_1(F_1')\theta_1(F_1'), \tag{13}$$

which, as in Eq. (10), derives from the fact

$$\prod_{i=1}^{k} W_{l_i}(F_{l_i}')\theta_{l_i}(F_{l_i}') < W_1(F_1')\theta_1(F_1')\cdot 2^{\Sigma_{i=2}^{k} n/l_i} = W_1(F_1')\theta_1(F_1')\cdot 2^{t(n)-n-1}.$$

First, we use Lemma 2.2 and Eq. (13) yields the condition

$$q^{5n/12}\left(\frac{1}{2}+\frac{1}{q+1}-\frac{0.86\cdot n}{q^2}\right) \geq c_{q',12}\cdot 2^{t(n)-n-1}W_1(F_1')\theta_1(F_1'),$$

By checking the last condition, the list of possible exceptions reduces further to 47 pairs. Then, we explicitly compute $\prod_{i=1}^{k} W_{l_i}(F_{l_i}')\theta_{l_i}(F_{l_i}')$ and use this number over the above estimation and, this way, we reduce the number of possible exception pairs even more, to 26.

In the mentioned list of 26 pairs (q,n), one finds the 18 pairs that are listed in Table 1 that are the pairs that fail to satisfy Eq. (13) even after $W(q')$ is computed explicitly.

q	5	7	8	9	11	13	17	19	23	29	41
n	6	8, 10	12	10	12, 16	16, 20	18, 24, 36	24, 30	24, 48	60	60

Table 1 Pairs (q,n) on which the non-sieving methods were inadequate.

5.1 The sieve

To deal with the persistent pairs (q,n) of Table 1, we employ the Cohen-Huczynska [3,4] sieving techniques. In principle, those pairs can be handled by brute force, i.e., by finding appropriate examples and in fact such examples are already known for most of those pairs [17], while for the rest, namely $(23,48)$, $(29,60)$ and $(41,60)$, a modern computer is able to find such examples within a few minutes. Nonetheless, disposing of such pairs in a theoretical way, such as sieving, is desirable and we choose this path in this work.

Proposition 5.2 (Sieving inequality) *Let $\{r_1,\dots,r_t\}$ be some divisors of r, where $r \mid q'$, such that $(r_i,r_j) = r_0$ for all $i \neq j$ and $\operatorname{lcm}(r_1,\dots,r_t) = r$, then*

$$\mathrm{CN}_q^r(n) \geq \sum_{i=1}^{t} \mathrm{CN}_q^{r_i}(n) - (t-1)\,\mathrm{CN}_q^{r_0}(n).$$

Proof We denote by $\mathbb{S}(l)$ the set of l-primitive completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where l may be any r_i. The statement is obvious for $t=1$. For $t=2$, we get that $\mathbb{S}(r_1)\cup\mathbb{S}(r_2)\subseteq\mathbb{S}(r_0)$ and $\mathbb{S}(r_1)\cap\mathbb{S}(r_2)=\mathbb{S}(q')$. The result follows after considering the cardinalities of the above sets.

Next, suppose the desired result holds for some $t=m\geq 2$. For $t=m+1$, if we denote by r' the least common multiple of $r_2,\dots r_{t+1}$, we observe that $\{r_1,r'\}$ satisfy the conditions for $t=2$. The desired result follows from the induction hypothesis. □

Proposition 5.3 *Let q be a prime power, $n\in\mathbb{N}$ and $\{p_1,\dots,p_t\}$ a set of prime divisors of q^n-1 (this set may be empty, in which case $t=0$), 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 $\mathrm{PCN}_q(n)>0$.

Proof Under the assumptions of the statement, Proposition 5.2 implies

$$\mathrm{PCN}_q(n)\geq\sum_{i=1}^{t}\mathrm{CN}_q^{q_0p_i}(n)-(t-1)\,\mathrm{CN}_q^{q_0}(n).$$

Next, we use the notation of the proof of Theorem 2.1 and by taking into account the analysis performed in its proof, the latter gives

$$\begin{aligned}\mathrm{PCN}_q(n)&\geq\sum_{i=1}^{t}\theta(q_0)\theta(p_i)\theta(\mathbf{q})(S_1+S_{2,q_0p_i})-(t-1)\theta(q_0)\theta(\mathbf{q})(S_1+S_{2,q_0})\\&=\theta(q_0)\theta(\mathbf{q})\left(\delta S_1+\sum_{i=1}^{t}\theta(p_i)S_{2,q_0p_i}-(t-1)S_{2,q_0}\right),\end{aligned}$$

which in turn yields

$$\frac{\mathrm{PCN}_q(n)}{\theta(q_0)\theta(\mathbf{q})}\geq\delta S_1+q^{n/2}W_{l_1}(F'_{l_1})\cdots W_{l_k}(F'_{l_k})W(q_0)\left(1+\sum_{i=1}^{t}(\theta(p_i)\frac{W(q_0p_i)}{W(q_0)}-1)\right)$$

and by considering the fact that $W(q_0p_i)/W(q_0)=2$, we get that

$$\frac{\mathrm{PCN}_q(n)}{\theta(q_0)\theta(\mathbf{q})}\geq\delta S_1+q^{n/2}W_{l_1}(F'_{l_1})\cdots W_{l_k}(F'_{l_k})W(q_0)(t-1+2\delta).$$

The last inequality combined with the fact that $S_1=\mathrm{CN}_q(n)/\theta(\mathbf{q})$ completes the proof. □

The latter implies that one may replace the term $W(q')$ in Eq. (13) by $W(q'/s_1\cdots s_k)\cdot\Delta$, where $s_1,\dots,s_k$ are prime divisors of q' such that $\delta:=1-\sum_{i=1}^{k}1/s_i>0$ and $\Delta:=(k-1)/\delta+2$, so one has to look for appropriate prime divisors of q'. We attempt to find such divisors for all the pairs of Table 1. It turns out that this is possible for the pairs (q,n) that are listed in Table 2, along with the appropriate primes.

The remaining pairs (listed in Table 3) were not dealt with theoretically. However, those pairs (q,n) satisfy $q\leq 97$ and $q^n<10^{50}$, i.e. Morgan and Mullen [17] have identified examples of primitive elements of $\mathbb{F}_{q^n}$ that are completely normal over $\mathbb{F}_q$. The proof of Theorem 1.4 is now complete.

q	n	Sieving primes	#
8	12	109, 73, 37, 19, 13	5
11	16	6304673, 7321, 61, 17, 5	5
13	16	407865361, 14281, 17	3
13	20	30941, 2411, 641	3
17	18	1270657, 5653, 1423, 307, 19	5
19	30	2460181, 1081291, 2251, 911, 271, 211, 151, 127, 61, 31, 11, 7	12
23	24	83575993, 139921, 7549, 937, 79, 53, 37, 13, 11, 7	10
23	48	483563163219889, 83575993, 12682129, 623009, 139921, 7549, 3697, 937	8
29	60	4140278225341, 517475046481, 470925821, 111855481, 732541, 120691, 22111, 1061, 541, 421, 401	11
41	60	8179560752161, 22616035021, 103826101, 11228251, 4555261, 579281, 382021, 22381, 4111, 1993, 1723, 1621, 761	13

Table 2 Pairs (q,n) from Table 1 that admit sieving, along with their sieving primes.

q	5	7	9	11	17	19
n	6	8, 10	10	12	24, 36	24

Table 3 Pairs (q,n) that were not dealt with theoretically.

6 Conclusions

The aim of this work is to establish the existence of primitive and completely normal elements for a larger range for the parameters q,n. We prove new sharper bounds for the number of completely normal elements of a given extension and use it to establish the existence of primitive and completely normal elements, using the method laid out in [7]. Our results hold asymptotically for n up to roughly q^2 with the additional assumption that $q-1 \nmid n$ when n is even in Theorem 1.3. Our method can be used to obtain effective results, as shown in Theorem 1.4. We believe that the range in Theorem 1.3 cannot be significantly improved, without improving Theorem 2.1. However, one should be able to improve Theorem 1.4 at the expense of significantly heavier computations. An interesting problem for further work could be to remove the condition $q-1 \nmid n$ for n even and, more generally, to establish the existence of primitive and completely normal elements for any n and q such that $q-1 \mid n$.

Acknowledgements We are grateful to the anonymous reviewers for their valuable comments. Theodoulos Garefalakis was supported by the University of Crete Research Grant No. 10316.

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. 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.
8. 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.
9. D. Hachenberger. Primitive complete normal bases: Existence in certain 2-power extensions and lower bounds. *Discrete Math.*, 310(22):3246–3250, 2010.
10. 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.
11. D. Hachenberger. Asymptotic existence results for primitive completely normal elements in extensions of Galois fields. *Des. Codes Cryptogr.*, 80(3):577–586, 2016.
12. C. Hsu and T. Nan. A generalization of the primitive normal basis theorem. *J. Number Theory*, 131(1):146–157, 2011.
13. G. Kapetanakis. An extension of the (strong) primitive normal basis theorem. *Appl. Algebra Engrg. Comm. Comput.*, 25(5):311–337, 2014.
14. G. Kapetanakis. Normal bases and primitive elements over finite fields. *Finite Fields Appl.*, 26:123–143, 2014.
15. H. W. Lenstra, Jr and R. J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.
16. R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, second edition, 1997.
17. I. H. Morgan and G. L. Mullen. Completely normal primitive basis generators of finite fields. *Util. Math.*, 49:21–43, 1996.
18. G. Robin. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann. *J. Math. Pures Appl.*, 63(2):187–213, 1984.