Finite Fields and Their Applications 28 (2014) 22–42

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Pairs of primitive elements in fields of even order

Stephen D. Cohen

School of Mathematics and Statistics, University of Glasgow, Glasgow G12 8QW, Scotland, United Kingdom

ARTICLE INFO

Article history:
Received 1 August 2013
Received in revised form 16 January 2014
Accepted 25 January 2014
Available online 25 February 2014
Communicated by D. Panario

MSC:
11T06
11T24
11T30

Keywords:
Finite field
Primitive element
Normal element

ABSTRACT

Let $\mathbb{F}_q$ be a finite field of *even* order. Two existence theorems, towards which partial results have been obtained by Wang, Cao and Feng, are now established. These state that (i) for any $q \geqslant 8$, there exists a primitive element $\alpha \in \mathbb{F}_q$ such that $\alpha + 1/\alpha$ is also primitive, and (ii) for any integer $n \geqslant 3$, in the extension of degree n over $\mathbb{F}_q$ there exists a primitive element α with $\alpha + 1/\alpha$ also primitive such that α is a normal element over $\mathbb{F}_q$.

Corresponding results for finite fields of *odd* order remain to be investigated.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q, a power of a prime p. A *primitive element* of $\mathbb{F}_q$ is a generator of the cyclic multiplicative group of $\mathbb{F}_q$ and thus has order $q-1$. We shall consider pairs (α, β) where α $(\neq 0) \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q$ is a rational expression of α. If, for example, $\beta = 1/\alpha$, then β is primitive in $\mathbb{F}_q$ whenever α is, but, for a general function β, if α is primitive in $\mathbb{F}_q$, then β may or may not be primitive in $\mathbb{F}_q$. We shall say that (α, β) is a *primitive pair* in $\mathbb{F}_q$ if both α and β are primitive in $\mathbb{F}_q$. The purpose of this paper is

E-mail address: Stephen.Cohen@glasgow.ac.uk.

http://dx.doi.org/10.1016/j.ffa.2014.01.012
1071-5797/© 2014 Elsevier Inc. All rights reserved.

to clarify and complete existence results of Wang, Cao and Feng [8] with regard to two problems on primitive pairs of the form $(\alpha, \alpha + \alpha^{-1})$ in the case when $\mathbb{F}_q$ is a field of even order, i.e., $p = 2$. We shall refer to the two problems as Problem 1 and Problem 2 (as described below).

Problem 1 is simply whether for a given field $\mathbb{F}_q$ there exists a primitive pair $(\alpha, \alpha + \alpha^{-1})$. Define $\mathcal{P}$ to be the set of prime powers q such that $\mathbb{F}_q$ contains a primitive pair $(\alpha, \alpha + \alpha^{-1})$. Observe that $2 \notin \mathcal{P}$ since $\alpha + \alpha^{-1} = 0$ when $\alpha = 1$, the only primitive element of $\mathbb{F}_2$, and $4 \notin \mathcal{P}$ since $\alpha + \alpha^{-1} = 1$ when α is either of the two primitive elements of $\mathbb{F}_4$. We shall prove that these are the only powers of 2 not in $\mathcal{P}$ by establishing the following theorem.

Theorem 1.1. *Let $q \geqslant 8$ be a power of 2. Then $q \in \mathcal{P}$.*

We summarise the work of Wang, Cao and Feng [8] on Problem 1 (although our notation differs). They suppose that the finite field in question is the field $\mathbb{F}_{q^n}$, an extension of *odd* degree n of the field $\mathbb{F}_q$, where $q = 2^k$ (and k may be even or odd). The main result of [8] on Problem 1 (Theorem 3.2) is that, if $n \geqslant 13$ is odd and $k \geqslant 5$ (so $kn \geqslant 65$), then $q^n = 2^{kn} \in \mathcal{P}$. It is proved by first establishing a sufficient number-theoretic condition on (q, n) for existence (Theorem 3.1) and then using machinery developed by Lenstra and Schoof [7] in establishing the primitive normal basis theorem. A further table (Table 2) is the outcome of applying Mathematica to the problem in some cases when $k \leqslant 4$. This reveals that, whenever $kn \geqslant 63$ with n odd (and $k \leqslant 4$), then $2^{kn} \in \mathcal{P}$. (Presumably Mathematica has been to verify the criterion Theorem 3.1 is valid for a (finite) number of pairs where the general Lenstra–Schoof machinery fails.) In fact, all the results of [8], Theorem 3.2 and Table 2, are immediate from Theorem 1.1; in particular, there is no need to restrict the field to be tested for membership of $\mathcal{P}$ as an extension of odd degree of an intermediate subfield.

Problem 2 of [8] is whether there exists a primitive pair $(\alpha, \alpha + \alpha^{-1})$ in the finite field F in question such that α is *normal* over a given subfield. Specifically, take F to be the extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, where $q = p^k$ and n is any positive integer. An element $\alpha \in \mathbb{F}_{q^n}$ is said to be *normal* over $\mathbb{F}_q$ if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. Define $\mathcal{Q}$ to be the set of pairs (q, n), where q is a prime power and n a positive integer, such that $\mathbb{F}_{q^n}$ contains a primitive pair $(\alpha, \alpha + \alpha^{-1})$ for which additionally α is normal over $\mathbb{F}_q$. If $n = 1$ then this problem reduces to Problem 1, i.e., $(q, 1) \in \mathcal{Q}$ if and only if $q \in \mathcal{P}$. If $n = 2$, then any element of $\mathbb{F}_{q^2}$ that is not in $\mathbb{F}_q$ is a normal element over $\mathbb{F}_q$; in particular, any primitive element of $\mathbb{F}_{q^2}$ is normal over $\mathbb{F}_q$. Hence $(q, 2) \in \mathcal{Q}$ if and only if $q^2 \in \mathcal{P}$. Accordingly, for Problem 2 it suffices to suppose $n \geqslant 3$. We shall establish the following theorem for fields of even order. It represents a strengthening of the primitive normal basis theorem [7] for such fields, namely that any finite field extension contains a primitive element, normal over the base field, cf. [6].

Theorem 1.2. *Let q be a power of 2 and n ($\geqslant 3$) be a positive integer. Then $(q, n) \in \mathcal{Q}$.*

We summarise the work of [8] in relation to Problem 2 in using the above notation with $q = 2^k$ and n *odd*. In Theorem 4.2 it is assumed that $n \geqslant 33$ is a divisor of $q-1$ (thus n is odd and $k \geqslant 6$ with $kn \geqslant 198$). The conclusion of the theorem is that then $(q,n) \in \mathcal{Q}$. Similarly in Theorem 4.3 it is assumed that $n \geqslant 31$ is odd and $k \geqslant 6$ (so that $kn \geqslant 186$). Again, the conclusion is that, in these circumstances, $(q,n) \in \mathcal{Q}$. The authors also tabulate some further ranges of (k,n) for which $(2^k,n) \in \mathcal{Q}$. When $n|q-1$ these all have $k \geqslant 8$. When $n \nmid q-1$ then $(16,n) \in \mathcal{Q}$ if $n \geqslant 111$ (so $kn \geqslant 444$) and $(32,n) \in \mathcal{Q}$ if $n \geqslant 49$ (so $kn \geqslant 245$). None of the results on Problem 2 has $q \leqslant 8$ and all assume n is odd. All the results of [8], Theorems 4.2 and 4.3, and Tables 4 and 5 follow immediately from Theorem 1.2. In [8] (where only *odd* values of n were considered) there was a division of cases according to whether $n|q^n-1$ or not. Likewise, we shall consider a division into two cases, according as to whether the *odd* part of n divides q^n-1 or not.

The techniques used to establish Theorems 1.1 and 1.2 employ multiplicative and additive characters and are developed from previous papers of the author and his collaborators (which should be consulted for more detail). Some indeed are cited in the bibliography of [8] (the items numbered therein as [2–7]). Nevertheless, others are more relevant, including [2–4], which establish the existence of primitive pairs $(\alpha, \alpha+1)$ in $\mathbb{F}_q$ (except when $q \in \{2,3,7\}$), and [6] which establishes the existence of *normal pairs* $(\alpha, 1/\alpha)$ in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for which α is also primitive. (Here a *normal pair in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ is analogous to a *primitive pair in* $\mathbb{F}_{q^n}$ except that "normal over $\mathbb{F}_q$" replaces "primitive".) These papers describe a valuable "sieving" method (ignored in [8]) incorporating a "multiplicative" sieve on the (prime) divisors of q^n-1 and/or an "additive" sieve on the (irreducible) factors of the polynomial x^n-1 over $\mathbb{F}_q$. In particular, [2–4] feature a doubly multiplicative sieve, a version of which will be used in the proof of Theorem 1.1. Whereas [6] features a "multiplicative + doubly additive" sieve (relating to the one primitive and two normal constraints), what is actually needed for Theorem 1.2 is a "doubly multiplicative + additive sieve". Nevertheless, [6] furnishes a helpful comparison as well as a key strategy that will be used in the proof. The proof of Theorem 1.1 is almost entirely theoretical. The proof of Theorem 1.2 is largely theoretical but for a few ("small") pairs (q,n) direct verification by citing explicit examples of pairs $(\alpha, \alpha+\alpha^{-1})$ which guarantee $(q,n) \in \mathcal{Q}$ are required.

Of course, Problems 1 and 2 can equally relate to finite fields of *odd* order (i.e., odd characteristic) and can be tackled by similar methods involving character sums and the sieve. For various reasons they will be more difficult to resolve in odd characteristic. Accordingly, we shall defer an investigation of Problems 1 and 2 in odd characteristic to a future occasion.

2. Preliminaries

In this section q is an arbitrary prime power (though we shall later specialise to powers of 2).

A non-zero element $\alpha \in \mathbb{F}_q$ is primitive if and only if it has order $q-1$. More generally, for any divisor e of $q-1$, call $\alpha \in \mathbb{F}_q^*$ *e-free* if, for any $d|e$, $\alpha = \gamma^d$, $\gamma \in \mathbb{F}_q$, implies $d=1$. We remark that the definition of e-free depends only on the *radical* of e: α is e-free if and only if it is e'-free for any divisor e' of $q-1$ with the same radical, i.e., the same *distinct* prime factors. Hence, in what follows, we blur the distinction between divisors of $q-1$ with the same radical.

Given $e|q-1$, the characteristic function for the subset of e-free elements $\alpha \in \mathbb{F}_q$ is

$$\theta_e \int\limits_{d|e} \chi_d(\alpha), \tag{2.1}$$

where $\theta_e = \phi(e)/e$ (ϕ is Euler's function) and the integral notation is shorthand for the weighted sum

$$\int\limits_{d|e} \chi_d(\alpha) = \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d(\alpha),$$

with $\sum_{(d)} \chi_d$ (for $d|e$) denoting a sum over all $\phi(d)$ multiplicative characters χ_d of order d over $\mathbb{F}_q$. Again, observe that the only non-zero contributions to this sum can arise from *square-free* values of d and we can assume in what follows that every value of d considered is square-free. (For convenience, the definition of a multiplicative character χ is extended to $\mathbb{F}_q$ by setting $\chi(0)=0$.) For multiplicative characters χ, χ' of $\mathbb{F}_q$ the Jacobi sum $J(\chi,\chi')$ is defined by $J(\chi,\chi') = \sum_{\alpha\in\mathbb{F}_q^*} \chi(\alpha)\chi'(1-\alpha) = \sum_{\alpha\in\mathbb{F}_q} \chi(\alpha)\chi'(1-\alpha)$. Of course, $J(\chi,\chi') = J(\chi',\chi)$. Here are other standard facts about Jacobi sums.

Lemma 2.1. *Suppose $d|q-1$. Then*

$$J(\chi_d, \chi_1) = \begin{cases} q-2, & \textit{if } d=1, \\ -1, & \textit{if } d>1. \end{cases}$$

Suppose $d>1$. Then $J(\chi_d, \chi_d^{-1}) = -\chi_d(-1)$. Hence, if d is odd (e.g., whenever q is even), then $J(\chi_d, \chi_d^{-1}) = -1$.

Suppose $d_1(>1)|q-1$ and $d_2(>1)|q-1$ with $\chi_{d_1} \neq \chi_{d_1}^{-1}$ if $d_2 = d_1$. Then $|J(\chi_{d_1}, \chi_{d_2})| = \sqrt{q}$.

In view of the notion of e-free elements we shall be interested in the number of *square-free* divisors of an integer. Hence given a positive integer e, let $W(e) = 2^{\omega(e)}$ denote the number of square-free divisors of e, where $\omega(e)$ is the number of distinct primes in e.

Lemma 2.2. *Let e be a positive integer. Then*

$$\sum_{d|e} \frac{|\mu(d)|}{\phi(d)} = \frac{1}{\theta_e}.$$

Proof. $|\mu(d)|/\phi(d)$ is a multiplicative function. Moreover, if e is a power of a prime l, then

$$\sum_{d|e} \frac{|\mu(d)|}{\phi(d)} = 1 + \frac{1}{l-1} = \frac{l}{l-1} = \frac{1}{\theta_e}. \qquad \square$$

So far, the material described relates to primitive elements in the given field $\mathbb{F}_q$. Problem 2 relates to an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ and concerns elements that are not only primitive in $\mathbb{F}_{q^n}$ but also normal over $\mathbb{F}_q$. Hence, in the first place all multiplicative concepts we have introduced (such as characters) will be in respect of $\mathbb{F}_{q^n}$. Similarly, e-free will relate to divisors e of $q^n - 1$. The idea of normality over $\mathbb{F}_q$ will require further discussion of additive characters over $\mathbb{F}_{q^n}$. First, we introduce the concept of the $\mathbb{F}_q$-order of an $\alpha \in \mathbb{F}_{q^n}$, which we will refer to as the *Order* of α. The Order of $\alpha \in \mathbb{F}_{q^n}$ is the monic divisor g (over $\mathbb{F}_q$) of $x^n - 1$ of minimal degree such that $g^\sigma(\alpha) = 0$. Here, given a monic polynomial $g(x) \in \mathbb{F}_q[x]$, the polynomial $g^\sigma(x) \in \mathbb{F}_q(x)$ is obtained from g by replacing x^i by x^{q^i}. Note that, if $F(x) = x^n - 1$, then $\alpha \in \mathbb{F}_{q^n} \iff F^\sigma(\alpha) = 0$, so that the definition is sensible. Indeed, if $\alpha \in \mathbb{F}_{q^n}$ has Order g, then $\alpha = h^\sigma(\gamma)$ for some $\gamma \in \mathbb{F}_{q^n}$, where $h = (x^n - 1)/g$. Let $n = p^b n'$, where $p \nmid n'$ and $b \geqslant 0$. Then $x^n - 1 = (x^{n'} - 1)^{p^b}$. Hence, if $p|n$, the Order of $\alpha \in \mathbb{F}_{q^n}$ need not be a square-free polynomial. Let E be a factor of $x^n - 1$. If $\alpha = h^\sigma(\gamma)$ (where $\gamma \in \mathbb{F}_{q^n}$, h is a factor of E) implies $h = 1$ we say that α is *E-free* in $\mathbb{F}_{q^n}$. Again, E may be replaced by its radical. Thus α is normal over $\mathbb{F}_q$ if it is $x^n - 1$-free. Indeed, if $n = p^b n'$ (where $p \nmid n'$), this is equivalent to α being $x^{n'} - 1$-free. At the other extreme, *every* member of $\mathbb{F}_{q^n}$ is 1-free.

The canonical additive character ψ on $\mathbb{F}_{q^n}$ is defined such that $\psi(\alpha)$ is the complex number $\exp(\frac{2\pi i \operatorname{Tr}(\alpha)}{p})$. Thus $\psi(\alpha_1 + \alpha_2) = \psi(\alpha_1)\psi(\alpha_2)$, etc. The character ψ_1, the *trivial character*, maps $\mathbb{F}_{q^n}$ identically onto 1. For any (monic) divisor D of $x^n - 1$, a typical character ψ_D of order D is one such that $\psi_D \circ D^\sigma$ is the trivial character in $\mathbb{F}_{q^n}$, and D is minimal (in respect of degree) with this property. Further, let Δ_D be the subset of $\delta \in \mathbb{F}_{q^n}$ such that ψ_δ has Order D if and only if $\delta \in \Delta_D$, where $\psi_\delta(\alpha) := \psi(\delta\alpha)$, $\alpha \in \mathbb{F}_{q^n}$. Thus, we also write ψ_{δ_D} for ψ_D, where δ_D is a typical element of Δ_D. Note that Δ_D is invariant under multiplication by $\mathbb{F}_q^*$, and that, if $D = 1$, then $\delta_1 = 0$ and $\psi_D = \psi_1$, the trivial character. To obtain a comparison of the number of additive characters of $\mathbb{F}_{q^n}$ of Order $D|x^n - 1$ with that of the multiplicative characters of $\mathbb{F}_{q^n}$ of order $d|q^n - 1$, define $\Phi(D)$ (the Euler function on $\mathbb{F}_q[x]$) as the multiplicative function given by the formula $\Phi(D) = |D| \prod_{P|D}(1 - |P|^{-1})$, where the product is over all (monic) irreducible polynomial divisors of D in $\mathbb{F}_q[x]$ and $|D| = q^{\deg D}$. Then, for $D|x^n - 1$, there are $\Phi(D)$ characters ψ_D having Order D. Similarly, as for e-free elements, in respect of E-free elements, we shall be interested in the number of *square-free* irreducible factors of a polynomial in $\mathbb{F}_q[x]$. Hence given a polynomial $E \in \mathbb{F}_q[x]$, let $W(E) = 2^{\omega(E)}$ denote the number of square-free factors of E.

Given $E|x^n - 1$, where $E(x) \in \mathbb{F}_q[x]$, the characteristic function for the subset of E-free elements. $\alpha \in \mathbb{F}_{q^n}$ is

$$\Theta_E \int_{D|E} \psi_D(\alpha),$$

where $\Theta_E = \Phi(E)/|E|$ and the integral notation is shorthand for the weighted sum

$$\int_{D|E} \psi_D(\alpha) = \sum_{D|E} \frac{\mu(D)}{\Phi(D)} \sum_{(D)} \psi_D(\alpha),$$

with $\sum_{(D)} \psi_D$ (for $D|E$) denoting a sum over all $\Phi(D)$ additive characters ψ_D of order D over $\mathbb{F}_{q^n}$ and where the notation $\mu(D)$ is retained for the Möbius character in $\mathbb{F}_q[x]$. Again, observe that the only non-zero contributions to this sum can arise from *square-free* values of D and we can assume in what follows that every value of D considered is square-free.

The main type of character sum that arises in Problem 2 reduces to a mixed character sum of the following type. For multiplicative characters χ_{d_1}, χ_{d_2}, with d_1, d_2 divisors of $q^n - 1$, and an additive character ψ_D, $D|x^n - 1$ over $\mathbb{F}_{q^n}$, define $L(\chi_{d_1}, \chi_{d_2}, \psi_D)$ by

$$L(\chi_{d_1}, \chi_{d_2}, \psi_D) = \sum_{\alpha \in \mathbb{F}_{q^n}} \chi_{d_1}(\alpha)\chi_{d_2}(1-\alpha)\psi_D(\alpha). \tag{2.2}$$

The basic estimates for the sum L follows conveniently from work of Cochrane and Pinner [1] that summarises and enlarges previous results.

Lemma 2.3. *Suppose $d(>1)|q^n - 1$ and $D(\neq 1)|x^n - 1$. Then $|L(\chi_d, \chi_1, \psi_D)| \leqslant q^{n/2}$. Moreover, for a specific character χ_d of order $d > 1$, $|L(\chi_d, \chi_d^{-1}, \psi_D)| \leqslant q^{n/2}$.*

Suppose $d_1(>1)|q^n - 1$, $d_2(>1)|q^n - 1$ and $D(\neq 1)|x^n - 1$. Suppose also that, if $d_1 = d_2$, then χ_{d_2} is not the same character of order d_1 as either χ_{d_1}, or $\chi_{d_1}^{-1}$. Then $|L(\chi_{d_1}, \chi_{d_2}, \psi_D)| \leqslant 2q^{n/2}$.

3. Counting primitive pairs $(\alpha, \alpha + \alpha^{-1})$

From now on, given α, denote $\alpha + \alpha^{-1}$ by β.

Let q be a power of 2. For any divisors e_1, e_2 of $q - 1$, define $N(e_1, e_2)$ to be the number of $\alpha \in \mathbb{F}_q$ for which α is e_1-free and $\beta = \alpha + \alpha^{-1}$ is e_2-free. In particular, $q \in \mathcal{P}$ if $N(q-1, q-1)$ is positive. We shall see, however, that it is convenient to consider expressions for $N(e_1, e_2)$ more generally. Specifically, given $e|q - 1$, we shall obtain expressions for $N(e, e)$, $N(el, e)$ and $N(e, el)$, where l is any prime dividing $q - 1$ but not e.

Lemma 3.1. *Suppose e_1, e_2 divide $q-1$. Then*

$$N(e_1,e_2)=\theta_{e_1}\theta_{e_2}\int_{d_1|e_1}\int_{d_2|e_2}\sum_{(d_1)}\sum_{(d_2)}J\big(\chi_{d_1}\chi_{d_2}^{-1},\chi_{d_2}^2\big)=:\theta_{e_1}\theta_{e_2}S, \tag{3.1}$$

where, by our convention, the character $\chi_{d_1}\chi_{d_2}^{-1}$ vanishes at zero.

Proof. From (2.1), in characteristic 2,

$$N(e_1,e_2)=\theta_{e_1}\theta_{e_2}\int_{d_1|e_1}\int_{d_2|e_2}\sum_{(d_1)}\sum_{(d_2)}K(\chi_{d_1},\chi_{d_2}),$$

where

$$K(\chi_{d_1},\chi_{d_2})=\sum_{\alpha\in\mathbb{F}_q^*}\chi_{d_1}(\alpha)\chi_{d_2}\big((\alpha+1)^2/\alpha\big)=\sum_{\alpha\in\mathbb{F}_q^*}\big(\chi_{d_1}\chi_{d_2}^{-1}\big)(\alpha)\chi_{d_2}^2(1+\alpha)$$

and the result follows. □

Suppose $e|q-1$. If $e=1$ then $N(1,1)$ is simply the number of $\alpha\in\mathbb{F}_q$ with $\alpha\notin\{0,1\}$, in which case $N(e,e)=q-2$. Otherwise, $N(e,e)$ is bounded as in the next result.

Lemma 3.2. *Suppose q is a power of 2 and $1<e|q-1$. Then*

$$N(e,e)\geqslant\theta_e^2\left(q+1-\frac{2}{\theta_e}-\big(W(e)\big(W(e)-1\big)-2\big(1-\theta_e^{-1}\big)\big)\sqrt{q}\right).$$

Proof. Take $e_1=e_2=e$ in (3.1). By Lemma 2.1 the contribution of the terms in S with $d_2=1$ is $q-2-\sum_{d(>1)|e}\mu(d)=q-1$. The contribution of the terms with $d_1=d_2>1$ and $\chi_{d_1}\chi_{d_2}^{-1}=\chi_1$ (i.e., $\chi_{d_1}=\chi_{d_2}$) is $-\sum_{d(>1)|e}\frac{\mu^2(d)}{\phi(d)}=1-\frac{1}{\theta_e}$, by Lemma 2.2. By Lemmas 2.1 and 2.2 there is a similar contribution (namely $1-\frac{1}{\theta_e}$) from the terms with $d_1=d_2>1$ and $(\chi_{d_1}\chi_{d_2}^{-1})\chi_{d_2}^2=\chi_1$ (i.e., $\chi_{d_2}=\chi_{d_1}^{-1}$).

The remaining Jacobi sums in S all have absolute value $\sqrt{q}$. The contribution of these terms to S is $\sqrt{q}U$, where

$$\begin{aligned}U&\leqslant\sum_{d_1|e}\sum_{d_2|e}\big|\mu(d_1)\mu(d_2)\big|-\sum_{d_1|e}\big|\mu(d_1)\big|-2\sum_{d_1(>1)|e}\frac{\mu^2(d_1)}{\phi(d_1)}\\&=W(e)^2-W(e)-2\left(1-\frac{1}{\theta_e}\right).\end{aligned}$$

The result follows. □

From Lemma 3.2, if $q = 2^{2m}$ (a square), then $3|q-1$ with and $N(3,3) \geqslant \frac{4}{9}(q-2-\sqrt{q})$. In fact, using the explicit evaluation of the cubic Gauss sum over $\mathbb{F}_q$, one obtains the exact evaluation of $N(3,3)$.

Lemma 3.3. *Suppose $q = 2^{2m}$. Then*

$$N(3,3) = \frac{4}{9}\big(q - 2 + (-1)^m\sqrt{q}\big).$$

Lemma 3.2 with $e = q-1$ yields a criterion for $q \in \mathcal{P}$. It represents an improvement of [8], condition (3.1) (when the latter applies).

Theorem 3.4. *Suppose q is even. Then $q \in \mathcal{P}$ whenever*

$$\sqrt{q} > W(W-1) - 2(1 - 1/\theta) + \frac{2/\theta - 1}{\sqrt{q}}, \tag{3.2}$$

where $W = W(q-1)$ and $\theta = \theta_{q-1}$.

If $q-1$ is prime (and so a Mersenne prime), then $\theta_{q-1} = \frac{q-2}{q-1}$, $W = 1$ and (3.2) is satisfied provided $q > 4$. Otherwise, $\theta_{q-1} < 1 - \frac{1}{\sqrt{q}}$, and (3.2) implies the more practical criterion

$$\sqrt{q} > W(W-1) \tag{3.3}$$

for $q \in \mathcal{P}$.

Next, we give a variation of Lemma 3.2 for $N(e_1, e_2)$ for divisors e_1, e_2 of $q-1$.

Lemma 3.5. *Assume e_1, e_2 are divisors of $q-1$. If $e_2 = 1$, then*

$$N(e_1, 1) = \begin{cases} q-2, & \text{if } e_1 = 1, \\ \theta_{e_1}(q-1), & \text{if } e_1 > 1. \end{cases} \tag{3.4}$$

If $e_2 > 1$, then

$$N(e_1, e_2) \geqslant \theta_{e_1}\theta_{e_2}\big\{q - 1 - W(e_1)\big(W(e_2) - 1\big)\sqrt{q}\big\}. \tag{3.5}$$

Proof. Deduce from Lemma 2.1 as in Lemma 3.2 but simply using $J(\chi_{d_1}, \chi_{d_2}) = -1$ if $d_1 > 1$, $d_2 = 1$, and $|J(\chi_{d_1}, \chi_{d_2})| \leqslant \sqrt{q}$, if $d_1 > 1$, $d_2 > 1$. □

Again suppose $e|q-1$ and l is a prime dividing $q-1$ but not e. Then $\theta_{le} = \theta_l\theta_e = (1 - \frac{1}{l})\theta_e$. We give upper bounds for the absolute values of $N(le, e) - \theta_l N(e, e)$ and $N(e, el) - \theta_l N(e, e)$.

Lemma 3.6. *Suppose $e(>1)|q-1$ and l is a prime dividing $q-1$ but not e. Then*

$$\left|N(le,e)-\theta_l N(e,e)\right| \leqslant \theta_l \theta_e^2 W(e)\left(W(e)-1\right)\sqrt{q}$$

and

$$\left|N(e,le)-\theta_l N(e,e)\right| \leqslant \theta_l \theta_e^2 W(e)^2\sqrt{q}.$$

Proof. From Lemma 2.1

$$N(le,e)-\theta_l N(e,e)=\theta_l\theta_e^2 \int\limits_{l|d_1|le} \int\limits_{d_2|e} \sum_{(d_1)}\sum_{(d_2)} J\left(\chi_{d_1}\chi_{d_2}^{-1},\chi_{d_2}^2\right) =: \theta_l\theta_e^2 S.$$

Here, by Lemma 2.1, the contribution to S of the terms with $d_2=1$ is

$$-\sum_{l|d_1|le}\mu(d_1)=\sum_{d_1|e}\mu(d_1)=0$$

(since $\mu(ld_1)=-\mu(d_1)$). The remaining Jacobi sums in S have absolute value $\sqrt{q}$: hence these contribute $\sqrt{q}V$ to S, where $V \leqslant (W(le)-W(e))(W(e)-1)=W(e)(W(e)-1)$, since $W(le)=2W(e)$. The working for $|N(e,le)-\theta_l N(e,e)|$ is similar. Here *all* the Jacobi sums have absolute value $\sqrt{q}$ (except that if $l=1$ then those corresponding to $d_1=1$ have the value -1) so that, generally, we obtain $W(e)^2$ instead of $W(e)(W(e)-1)$. □

Next we give the sieving lemma (as in previous papers such as [6]).

Lemma 3.7. *Suppose $e|q-1$ and that $p_1,\dots,p_s$ are all the primes dividing $q-1$ but not e. Then*

$$N(q-1,q-1) \geqslant \sum_{i=1}^{s} N(p_i e,e)+\sum_{i=1}^{s} N(e,p_i e)-(2s-1)N(e,e).$$

Theorem 3.8. *Assume q is a power of 2. Suppose that $e|q-1$ and $p_1,\dots,p_s$ are the remaining primes dividing $q-1$ (as in Lemma 3.7). Set $\delta=1-2\sum_{i=1}^{s}\frac{1}{p_i}$ and assume $\delta>0$. Then*

$$N(q-1,q-1) \geqslant \delta{\theta_e}^2\sqrt{q}\left\{\sqrt{q}-\left(\frac{2s-1}{\delta}+2\right)W(e)\left(W(e)-\frac{1}{2}\right)\right\}. \tag{3.6}$$

Hence, if

$$\sqrt{q} > W(e)\left(W(e)-\frac{1}{2}\right)\left(\frac{2s-1}{\delta}+2\right), \tag{3.7}$$

then $q \in \mathcal{P}$.

Proof. Start by rearranging Lemma 3.7 as

$$N(q-1,q-1) \geqslant \left(\sum_{i=1}^{s} N(p_i e, e) - \theta_{p_i} N(e,e)\right) + \left(\sum_{i=1}^{s} N(e, p_i e) - \theta_{p_i} N(e,e)\right) + \delta N(e,e),$$

because $\delta = 2\sum_{i=1}^{s} \theta_{p_i} - (2s-1)$. Using Lemma 3.6 and the simpler consequence

$$N(e,e) \geqslant \theta_e^2 \bigl(q - W(e)\bigl(W(e) - 1/2\bigr)\sqrt{q}\bigr)$$

of Lemma 3.2, we deduce that

$$N(q-1,q-1) \geqslant \delta\theta_e^2\sqrt{q}\left\{\sqrt{q} - W(e)\bigl(W(e)-1/2\bigr) - \frac{W(e)(W(e)-1) + W(e)^2}{\delta}\sum_{i=1}^{s}\theta_{p_i}\right\}.$$

This yields (3.6) since $W(e)(W(e)-1) + W(e)^2 = 2W(e)(W(e)-1/2)$ and $\frac{2\sum_{i=1}^{s}\theta_{p_i}}{\delta} = \frac{2s-1}{\delta} + 1$. □

4. Application of criteria for primitive pairs $(\alpha, \alpha + \alpha^{-1})$

We proceed to the proof of Theorem 1.1. Assume $q = 2^k$, $k \geqslant 3$. As remarked following Theorem 3.4, its criterion is satisfied when $q-1$ is a (Mersenne) prime (> 3) and so when $k = 3, 5, 7, 13, 17$.

Lemma 4.1. *Suppose $q = 2^k$, where $k > 12$ or $k = 9, 11$. Then $q \in \mathcal{P}$.*

Proof. Let $\omega = \omega(q-1)$. From (3.3), since $W(W-1) < W^2$, then $q \in \mathcal{P}$ whenever $k \geqslant 4\omega(q-1)$. Assume $\omega = \omega(q-1) \geqslant 13$. Then

$$q > 3 \times 5 \times 7 \times \cdots \times 43 \times 16^{\omega-13} > \bigl(6.541 \times 10^{15}\bigr) \times 16^{\omega-13}.$$

Thus $k > 52.5 + 4(\omega - 13) > 4\omega$ and $q \in \mathcal{P}$.

So assume $\omega \leqslant 12$. If $k \geqslant 48$ then $k \leqslant 4\omega$ and $q \in \mathcal{P}$. By factorising $q-1$ for $13 \leqslant k \leqslant 47$ one sees that $k \geqslant 4\omega$ in every case. The largest value of ω (namely, 8) occurs when $k = 36$ (in which case $q - 1 = 3^3 \times 5 \times 7 \times 13 \times 19 \times 37 \times 73 \times 109$). Moreover, equality occurs precisely when $k = 24$ (when $q - 1 = 3^2 \times 5 \times 7 \times 13 \times 17 \times 241$) and $k = 16$ (when $q - 1 = 3 \times 5 \times 17 \times 257$). Finally, when $k = 11$ then $q - 1 = 23 \times 89$ and when $k = 9$ then $q - 1 = 7 \times 73$ and therefore $k \geqslant 4\omega$ in these cases too. □

As far as membership of $\mathcal{P}$ is concerned there remains the values $q = 2^k$, $k = 4, 6, 8, 10, 12$. We consider each in turn. The discussion hints at a (slight) measure of structure linking primitivity of α with that of β.

$\underline{\mathbb{F}_{\mathbf{16}}.}$ Suppose that $\alpha \in \mathbb{F}_{16}$. Observe that α has order 5 if and only if β has order 3 (because $\alpha^4+\alpha^3+\alpha^2+\alpha+1=0 \iff \beta^2+\beta+1=0$), and that α has order 3 if and only if $\beta=1$. By (3.5), $N(1,15) \geqslant \theta_{15}(15-3\times 4)>0$. Hence there exists $\alpha \in \mathbb{F}_{16}$ with β primitive. Evidently, $\alpha \neq 1$ and, from the above, α cannot have order 3 or 5. Hence (α,β) is a primitive pair and $\mathbb{F}_{16} \in \mathcal{P}$.

$\underline{\mathbb{F}_{\mathbf{64}}.}$ By (3.5), $N(3,63) \geqslant \frac{8}{21}(63-2\times 3\times 8)>0$. Hence there exists a 3-free $\alpha \in \mathbb{F}_{64}$ with β primitive. If α is not primitive it has order 9, whence $\alpha^8+\alpha^7+\cdots+\alpha+1=0$, which yields $\beta^4+\beta^3+\beta^2+1=(\beta+1)(\beta^3+\beta^2+1)=0$. Hence $\beta=1$ or $\beta \in \mathbb{F}_8$, which is not so. Thus (α,β) is a primitive pair and $\mathbb{F}_{64} \in \mathcal{P}$.

$\underline{\mathbb{F}_{\mathbf{256}}.}$ This is the first of two instances when we resort to an explicit example of a primitive pair. Take α to be a root of the primitive polynomial $x^8+x^4+x^3+x^2+1$ over $\mathbb{F}_2$. Then β is a root of the primitive polynomial $x^8+x^6+x^5+x^2+1$. Both these polynomials are primitive. Thus $\mathbb{F}_{256} \in \mathcal{P}$.

$\underline{\mathbb{F}_{\mathbf{1024}}.}$ Here $q-1=3\times 11\times 31$. In Theorem 3.8 take $e=3$. Then the right side of (3.7) is $3(\frac{3}{\delta}+2)<17.95<32=\sqrt{q}$ and (3.7) holds. Hence $\mathbb{F}_{1024} \in \mathcal{P}$.

$\underline{\mathbb{F}_{\mathbf{4096}}.}$ Here is an example of a primitive pair. Take α to be a root of the primitive polynomial $x^{12}+x^7+x^6+x^4+1$ over $\mathbb{F}_2$. Then β is a root of the primitive polynomial $x^{12}+x^8+x^7+x^2+1$. Thus $\mathbb{F}_{4096} \in \mathcal{P}$.

This completes the proof of Theorem 1.1.

5. Primitive normal pairs (α,β) with α normal over $\mathbb{F}_q$

Let q be a power of 2. For $\alpha \in \mathbb{F}_{q^n}$, for convenience in this paper, refer to a pair (α,β) as *primitive normal* if α is both primitive and normal over $\mathbb{F}_q$ and β is primitive. Recall that in the investigation of primitive normal pairs we suppose $n \geqslant 3$.

For any divisors e_1, e_2 of q^n-1 and factor E of $x^n-1 \in \mathbb{F}_q[x]$, define $N(e_1,e_2,E)$ to be the number of $\alpha \in \mathbb{F}_q$ for which α is e_1-free $\beta=\alpha+\alpha^{-1}$ is e_2-free and α is E-free. In particular, the pair $(q,n) \in \mathcal{Q}$ if $N(q^n-1,q^n-1,x^n-1)$ is positive. We shall see however, that it is convenient to consider expressions for $N(e_1,e_2,E)$ in more generality. As in the proof of Lemma 3.1 this number can be expressed in terms of the character sum L defined by (2.2).

Lemma 5.1. *Suppose e_1, e_2 divide q^n-1. Then*

$$N(e_1,e_2,E)=\theta_{e_1}\theta_{e_2}\Theta_E \int\limits_{d_1|e_1}\int\limits_{d_2|e_2}\int\limits_{D|E}\sum_{(d_1)}\sum_{(d_2)}\sum_{(D)} L\big(\chi_{d_1}\chi_{d_2}^{-1},\chi_{d_2}^2,\psi_D\big).$$

Lemma 5.2. *Assume q is a power of 2 and $n \geqslant 3$. Assume also $1 < e | q^n - 1$, and $E | x^n - 1$. Then*

$$N(e, e, E) \geqslant \theta_e^2 \Theta_E q^{\frac{n}{2}} \left\{ q^{\frac{n}{2}} - \left(2W(e)\big(W(e) - 1/2\big)\big(W(E) - 1/2\big) - \frac{W(e)}{2} \right) \right\}.$$

Proof. As for Lemma 3.2 using Lemmas 2.1 and 2.3 (but ignoring the savings arising from characters $\chi_{d_2} = \chi_{d_1}^{-1}$). Specifically, the contribution to the expression for $N(e, e, E)/(\theta_e^2 \Theta_E q^{n/2})$ from characters with $d_2 > 1$ and $D \neq 1$ in absolute value does not exceed $2W(e)(W(e) - 1)(W(E) - 1)$ by the final assertion of Lemma 2.3. Similarly, characters with $d_2 > 1$ and $D = 1$ contribute $W(e)(W(e) - 1)$ (by Lemma 2.1) and characters with $d_2 = 1$ contribute $W(e)(W(E) - 1)$ by the first part of Lemma 2.3. The result follows. □

Remark. When $E = 1$ (so $W(E) = 1$) then $N(e, e, 1) = N(e, e)$ (as in Section 3) and Lemma 5.2 agrees with (3.3).

Now suppose $e | q^n - 1$ and $E | x^n - 1$. Also, suppose P is an irreducible polynomial dividing $x^n - 1$ but not E. Then $\Theta_{PE} = \Theta_P \Theta_E = (1 - \frac{1}{|P|})\Theta_E$. We give an upper bound for the absolute values of $N(e, e, PE) - \Theta_P N(e, e, E)$.

Lemma 5.3. *Suppose $e | q^n - 1$ and $E | x^n - 1$. Suppose also P is an irreducible polynomial dividing $x^n - 1$ but not E. Then*

$$\big| N(e, e, PE) - \Theta_P N(e, e, E) \big| \leqslant 2{\theta_e}^2 \Theta_{PE} W(e)\big(W(e) - 1/2\big) W(E) q^{\frac{n}{2}}.$$

Proof. From Lemma 5.1

$$N(e, e, PE) - \Theta_P N(e, e, E) = {\theta_e}^2 \Theta_{PE} \int_{d_1|e_1} \int_{d_2|e_2} \int_{D|E} \sum_{(d_1)} \sum_{(d_2)} \sum_{(D)} L\big(\chi_{d_1}\chi_{d_2}^{-1}, \chi_{d_2}^2, \psi_{PD}\big).$$

Using Lemma 2.3 as in Lemma 5.2 we find that the contribution to the expression $(N(e, e, PE) - \Theta_P N(e, e, E))/({\theta_e}^2 \Theta_{PE} q^{n/2})$ from characters with $d_2 > 1$ in absolute value does not exceed $2W(e)(W(e) - 1)(W(PE) - W(E)) = 2W(e)(W(e) - 1)W(E)$, since $W(PE) = 2W(E)$. Similarly, the contribution from characters with $d_2 = 1$ is $W(e)W(E)$. The result follows. □

For this problem we shall in the first place concentrate on sieving with respect to the factors of E ("additive sieving"). The sieving inequality which follows is established by the elementary combinatorial argument of Proposition 4.1 of [5] translated verbatim to Problem 2.

Lemma 5.4. *Assume $e|q^n - 1$ and $E|x^n - 1$. Suppose that $P_1, \dots, P_t$ are the distinct irreducible factors of $x^n - 1$ not dividing E. Then*

$$N\bigl(e, e, x^n - 1\bigr) \geqslant \sum_{i=1}^{t} N(e, e, P_i E) - (t-1)N(e, e, E).$$

Theorem 5.5. *Assume q is a power of 2 and $n \geqslant 3$. Suppose that $E|x^n - 1$ and $P_1, \dots, P_t$ are the remaining irreducible polynomials dividing $x^n - 1$ (as in Lemma 5.4). Set $\delta = 1 - \sum_{i=1}^{t} \frac{1}{|P_i|}$ and $S = \frac{t-1}{\delta} + 2$. Assume $\delta > 0$. Then*

$$\begin{aligned} &N\bigl(q^n - 1, q^n - 1, x^n - 1\bigr) \\ &\quad \geqslant \delta \theta_{q^n-1}^2 \Theta_E q^{\frac{n}{2}} \bigl\{q^{\frac{n}{2}} - 2SW\bigl(q^n - 1\bigr)\bigl(W\bigl(q^n - 1\bigr) - 1/2\bigr)W(E)\bigr\}. \end{aligned} \tag{5.1}$$

Hence, if

$$q^{\frac{n}{2}} > 2W\bigl(q^n - 1\bigr)\bigl(W\bigl(q^n - 1\bigr) - 1/2\bigr)W(E)S, \tag{5.2}$$

then $(q, n) \in \mathcal{Q}$. Often it is convenient to use the (weaker) criterion

$$q^{\frac{n}{2}} > 2W^2\bigl(q^n - 1\bigr)W(E)S \tag{5.3}$$

for the pair (q, n) to be in $\mathcal{Q}$.

Later, for some specific pairs, (q, n) we will use the "additive-multiplicative" sieve involving sieving with respect to primes in $q^n - 1$ (as in Theorem 3.8, applied to $\mathbb{F}_{q^n}$) as well as irreducible polynomials dividing $x^n - 1$ as in Theorem 5.5. The proof is by combining the essential features of those of Theorems 3.8 and 5.5.

Theorem 5.6. *Assume q is a power of 2 and $n \geqslant 3$. Suppose that $e|q^n - 1$ and $p_1, \dots, p_s$ are the remaining primes dividing $q - 1$. Suppose also that $E|x^n - 1$ and $P_1, \dots, P_t$ are the remaining irreducible polynomials dividing $x^n - 1$. Set $\delta = 1 - 2\sum_{i=1}^{s} \frac{1}{p_i} - \sum_{i=1}^{t} \frac{1}{|P_i|}$ and $S = \frac{2s+t-1}{\delta} + 2$. Assume $\delta > 0$. If*

$$q^{\frac{n}{2}} \geqslant 2SW(e)\bigl(W(e) - 1/2\bigr)W(E), \tag{5.4}$$

then $(q, n) \in \mathcal{Q}$. In particular, if

$$q^{\frac{n}{2}} > 2W^2(e)W(E)S, \tag{5.5}$$

then $(q, n) \in \mathcal{Q}$.

We stress that the constraint that $\delta > 0$ for the validity of (5.4) and (5.5) is demanding. Nevertheless, it is useful for some particular pairs. Because the factorisation pattern of

$x^n - 1$ is more predictable than the prime decomposition of $q^n - 1$ additive sieving, based on Theorem 3.8, is more valuable for the systematic theory. As in Section 2, write $n = 2^b n'$, where n' is odd and $b \geqslant 0$. Recall that, the notion of an E-free polynomial depends only on the radical of E, a factor of $x^{n'} - 1$. We divide the proof of Theorem 1.2 into cases depending on the nature of the factors of $x^{n'} - 1$.

6. Values of n for which n' divides $q - 1$

Suppose $n'|q-1$. Then $x^{n'} - 1$ splits into a product of n' distinct linear factors over $\mathbb{F}_q$.

Lemma 6.1. *Suppose $n'|q-1$. If, in the statement of Theorem 5.5, $n' = (q-1)/u$ and $E = 1$, then $S = \frac{q^2-3q+uq+2}{uq-q+1}$.*

To apply Theorem 5.5 systematically one also needs an upper bound on $W(q^n - 1)$ (however extravagant) without having to factorise $q^n - 1$.

Lemma 6.2. *Let m be an odd positive integer. Then $W(m) < 6.46m^{1/5}$.*

Proof. Taking a product over odd primes less than 32 we have

$$\frac{W(m)}{m^{1/5}} \leqslant \prod_{3 \leqslant l \leqslant 31} \frac{2}{l^{1/5}} < 6.46. \qquad \square$$

Lemma 6.3. *Assume q is a power of 2 and n satisfies $n'|q-1$. If $q \geqslant 32$ and $n' \geqslant 15$, then $(q, n) \in \mathcal{Q}$.*

Proof. From Lemma 6.2, $W(q^n - 1) < 6.46q^{n/5}$ and (5.3) (with $E = 1$) is satisfied whenever $q^{\frac{n}{10}} > 83.5 \times S$.

Suppose $n' = q - 1$. Then, in Lemma 6.1, $S = q^2 - 2q + 2 < 2q^2$ and (5.3) is satisfied whenever $q^{\frac{q-1}{10}-2} > 167$, which holds (easily) if $q \geqslant 32$ except when $q = 32$ and $n = n' = 31$. In the exceptional case $\omega(q^n - 1) = 7$ and (5.3) holds since $q^{\frac{31}{2}-2} > 2^{15}$.

Hence we can assume $q \geqslant 64$ and $15 \leqslant n' \leqslant (q-1)/3$ which implies (from Lemma 6.1) that $S \leqslant \frac{q^2+1}{2q+1} < q/2$. Hence (5.3) is satisfied provided $q^{\frac{n'}{10}-1} > 41.8$ which always holds under the given constraints on q and n'. $\square$

It follows from Lemma 6.3 that, to complete the proof of Theorem 1.2 when $n'|q-1$, it suffices to consider odd values of $n' \leqslant 13$.

$n' = 1$. Here, we have $n = 2^j$, $j \geqslant 2$. We need to bound below the number of primitive pairs $(\alpha, \beta) \in \mathbb{F}_{q^n}$ with α $(x-1)$-free over $\mathbb{F}_q$. To satisfy (5.3) with $E = x - 1$ $(= x^{n'} - 1)$ it is enough if $q^{2^j/10} > 83.5$. This holds for $j \geqslant 2$ whenever $q \geqslant 2^{16}$. Conversely, if it fails then necessarily $q^{2^j} \leqslant 2^{48}$. Using exact values of $\omega(q^n - 1)$ we find that (5.3) is satisfied except when $(q, n) = (2, 16), (2, 8), (2, 4), (4, 8), (4, 4), (8, 4), (8, 8), (16, 4), (32, 4)$.

Amongst these pairs, those with $q^n \geqslant 2^{16}$ satisfy (5.4) for appropriate choice of e and E. For example, for $(2,16)$, $(4,8)$ and $(16,4)$ (for which $q^n = 2^{16}$), $q^n - 1 = 3 \times 5 \times 17 \times 257$. Take $e = 3$ and $E = 1$. Then $\delta > 0.4745$, $S < 14.7$ and (5.4) holds since $q^{n/2} = 256 > 177 > 12S$.

For the pair $(2,4)$, easily an element $\alpha \in \mathbb{F}_{16}$ in the proof of Theorem 1.1 such that (α, β) is a primitive pair can be either a root of $x^4 + x + 1$ or $x^4 + x^3 + 1$. Choosing the latter we see that $(2,4) \in \mathcal{Q}$.

In summary for $n' = 1$ this leaves the pairs $(2,8)$, $(4,4)$ and $(8,4)$ to be checked directly (using MAGMA) for membership of $\mathcal{Q}$. In each case we give an example of a primitive normal pair using f, g for the minimal polynomials over $\mathbb{F}_q$ of α, β, respectively.

$(2,8)$. $f = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$, $g = x^8 + x^6 + x^5 + x^3 + 1$.

$(4,4)$. $f = x^4 + x^3 + ux^2 + ux + u$, $g = x^4 + ux^2 + ux + u$, where $u^2 + u + 1 = 0$.

$(8,4)$. $f = x^4 + ux^3 + x^2 + (u^2+1)x + u^2 + u$, $g = x^4 + (u^2+u)x^3 + x^2 + (u^2+u+1)x + u^3$, where $u^3 + u + 1 = 0$.

$n' = 3$, q an even power of 2. In Lemma 6.1 (with $E = 1$) we have $S = \frac{4(q-3/2)}{q-3} = 4 + \frac{6}{q-3} < 9/2$ for $q \geqslant 16$. Write $q^n = 2^{3 \cdot 2^j}$. As before, for (5.3) to hold it suffices that $2^{2^{j-1}} > (9 \times 6.46^2)^{10/3} = 3.82\ldots \times 10^8$, which holds if $j \geqslant 6$. If $j = 5$, then $\omega(q^n - 1) = \omega(2^{96} - 1) = 12$ and (5.3) holds since $2^{48} > 9 \times 2^{24}$. Similarly, if $j = 4$, then $\omega(q^n - 1) = \omega(2^{48} - 1) = 9$ and the inequality $2^{24} > 9 \times 2^{18}$ holds. The pairs that remain are $(4,12)$, $(4,6)$, $(4,3)$, $(16,6)$, $(16,3)$.

$(4,12)$. $f = x^{12} + (u+1)x^{11} + x^{10} + (u+1)x^9 + ux^6 + x^5 + x^4 + x^3 + x^2 + x + u$, $g = x^{12} + x^9 + x^7 + (u+1)x^5 + x^4 + (u+1)x^3 + x^2 + u + 1$, where $u^2 + u + 1 = 0$.

$(4,6)$. $f = x^6 + (u+1)x^5 + ux^4 + (u+1)x^3 + x + u + 1$, $g = x^6 + x^5 + (u+1)x^4 + u$, where $u^2 + u + 1 = 0$.

$(4,3)$. $f = x^3 + x^2 + x + u$, $g = x^3 + ux^2 + ux + u$, where $u^2 + u + 1 = 0$.

$(16,6)$. $f = x^6 + (u^3+1)x^5 + (u^3+u)x^4 + (u^3+u^2+u+1)x^3 + (u^3+u^2+u+1)x + u^3 + u^2 + u$, $g = x^6 + (u^2+u+1)x^4 + (u+1)x^3 + (u^3+u^2)x^2 + (u^3+u^2)x + u^3 + u^2 + u$, where $u^4 + u + 1 = 0$.

$(16,3)$. $f = x^3 + (u^2+1)x^2 + (u+1)x + u$, $g = x^3 + (u+1)x^2 + u^2x + u$, where $u^4 + u + 1 = 0$.

$n' = 5$, q a $4m$th power of 2. In Lemma 6.1 we have $S = \frac{2(3q-5)}{q-5} = 6 + \frac{20}{q-5} < 8$ for $q \geqslant 16$. Write $q^n = 2^{5 \cdot 2^j}$. As before, for (5.3) to hold it suffices that $2^{2^{j-1}} > 16 \times 6.46^2 = 667.7\ldots$, which holds if $j \geqslant 5$. If $j = 4$, then $\omega(q^n - 1) = 9$ and (5.3) holds since $2^{40} > 16 \times 2^{18}$. If $j = 3$, then $\omega(q^n - 1) = 7$ and (5.3) holds since $2^{20} > 16 \times 2^{14}$. For $n' = 5$, this leaves $(16,5)$.

$(16,5)$. $f = x^5 + ux^4 + u^2x^3 + (u^2+1)x^2 + (u+1)x + u$, $g = x^5 + (u^3+u)x^4 + (u^3 + u^2 + 1)x^3 + u^2x^2 + (u^3+u^2+u+1)x + u^3 + u + 1$, where $u^4 + u + 1 = 0$.

$\underline{n' = 7,\ q \text{ a } 3m\text{th power of } 2}$. Only the pair $(8,7)$ needs to be examined. Then $q^n - 1 = 7^2 \times 127 \times 337$, $\omega(q^n - 1) = 3$. In Theorem 5.6 take $e = 7$, $E = 1$ so that $s = 2$, $t = 7$. Then $\delta > 0.1033$ and $S = 10/\delta + 2 < 98.9$ and $(8,7) \in \mathcal{Q}$ since $8^{7/2} > 1448 > 792 > 8S$.

It is easily checked that when $n' = 9, 11, 13$ there are no pairs that require verification for membership of $\mathcal{Q}$.

7. Values of n' that do not divide $q - 1$

Given q, n, define u to be the order of q mod n'. Then the irreducible factors of $x^{n'} - 1$ in $\mathbb{F}_q[x]$ of maximal degree have degree u. In particular, if $n' \nmid q - 1$ (as we are now supposing), then $u \geqslant 2$. Define $\rho(q,n)$ to be such that $n\rho(q,n) = n'\rho(q,n')$ is the number of *distinct* irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ having degree *less than* u. It is important to use the following upper bounds for $\rho(q,n)$.

Lemma 7.1. *Assume that q is an even power of 2 and n is an odd integer.*

(i) *Suppose $q = 2$. Then $\rho(2,3) = 1/3$; $\rho(2,5) = 1/5$; $\rho(2,9) = 2/9$; $\rho(2,21) = 4/21$; otherwise $\rho(2,n) \leqslant 1/6$.*
(ii) *Suppose $q = 4$. Then $\rho(4,9) = 1/3$; $\rho(4,45) = 11/45$; otherwise $\rho(4,n) \leqslant 1/5$.*
(iii) *Suppose $q = 8$. Then $\rho(8,3) = \rho(8,21) = 1/3$; otherwise $\rho(8,n) \leqslant 1/5$.*
(iv) *Suppose $q \geqslant 16$. Then $\rho(q,n) \leqslant 1/3$.*

Except for part (iii), Lemma 7.1 is implied by Proposition 5.3 of [5]. When $q = 8$ the proof is similar to that of the latter (particularly with reference to the case $q = 4$). Thus, suppose in the first place, that $n = n'$ and the product of the irreducible factors of $x^n - 1$ of degree less than u is $x^{n_{s/l}} - 1$ for some prime l. Here s is the order of 8 modulo n and $n_{s/l} = \gcd(8^{s/l} - 1, n) < n$. Then by (7.1) of Lemma 7.1 of [5], in the notation of that lemma,

$$\rho(8,n) = \frac{\sigma(8, n_{s/l})}{t_{s/l}} = \frac{\sigma}{t},$$

say, where $n\sigma$ is the total number of irreducible factors of $x^{n_{s/l}} - 1$ in $\mathbb{F}_q[x]$ and $t = n/n_{s/l} > 1$. Hence it may be assumed that $t = 3$. Moreover, $\sigma = 1$ only if $n | 21$, leading eventually to the sole exceptional cases $n = 3, 21$. In the general case, use also (7.2) of Lemma 7.1 of [5]. Following [5], the details are awkward but routine and the idea should be clear. (Similarly, the possibility $t = 5$ leads to the two cases, $n = 5, 35$, where we have equality in the bound of Lemma 7.1(iii).)

Lemma 7.2. *Assume that q is an even power of 2 and n is an integer such that n' does not divide $q - 1$. Then, in Theorem 5.5 with E the product of irreducible factors of $x^n - 1$ of degree less than u, $S \leqslant n'$.*

Proof. We can assume n is odd (with $n' = n$). The number of irreducible factors of $x^n - 1$ does not exceed $\frac{n-\rho(q,n)}{u} \leqslant n/u$. Hence $\delta \geqslant 1 - \frac{n-\rho(q,n)}{uq^u} \geqslant 1 - \frac{n}{uq^u} > 1 - 1/u$, since $n \leqslant q^u - 1$. Thus $S < \frac{\frac{n}{u}-1}{\frac{u-1}{u}} \leqslant n$, since $u \geqslant 2$. □

We suppose from now on that $n' \nmid (q-1)$ and discuss the values of q as delineated in Lemma 7.1 in turn.

$\underline{q \geqslant 16}$. Take E in Theorem 5.5 as in Lemma 7.2. Conclude (also using Lemma 6.2) that, to ensure (5.1) holds, it suffices that $q^{\frac{n}{2}} > 2(6.46)^2 q^{\frac{2n}{5}} 2^{\rho(n)} S$. By Lemma 7.1(iv), $2^{\rho n} \leqslant q^{\rho(n)/4} \leqslant q^{n/12}$ and so, by Lemma 7.2, it suffices that

$$q^{\frac{n}{60}} > 83.5n.$$

This holds if $n \geqslant 212$ for all $q \geqslant 16$. So we can assume $n \leqslant 211$ and $q^n \leqslant 16^{211} < 1.2 \times 10^{254}$. Hence $\omega = \omega(q^n - 1) \leqslant 111$. Therefore (5.1) would be satisfied if

$$q^{\frac{5n}{12}} \geqslant n2^{2\omega+1} \tag{7.1}$$

with $\omega \leqslant 111$. In fact, (7.1) holds if $n \geqslant 139$ and $q^n \geqslant 16^{139}$, since $\omega \leqslant 111$. Hence, we suppose $n \leqslant 138$ and $q^n \leqslant 1.5 \times 10^{166}$, whence $\omega \leqslant 79$. Now, with $\omega = 79$, (7.1) is satisfied if $n \geqslant 100$. Thus $n \leqslant 99$ and $q^n \leqslant 1.7 \times 10^{119}$ and therefore $\omega \leqslant 60$. Repeating this process several times we can assume finally that $n \leqslant 38$ and $q^n \leqslant 5.8 \times 10^{45}$. Call such a process a *sieving cycle*.

For the pairs (q,n) that remain (of the order of 200 in number), $\omega = \omega(q^n - 1)$ was evaluated exactly and tested to see whether $q^{\frac{n}{2}} > 2^{n/3+2\omega+1}$ (which would imply (5.3)). This occurred except for the pairs $(16,7)$, $(16,9)$, $(16,11)$, $(32,3)$, $(32,6)$, $(32,12)$, $(64,5)$. One can routinely show that each of these pairs is in $\mathcal{Q}$ since criterion (5.4) is satisfied for an appropriate choice of e, E. (The method is akin to that demonstrated at greater length in more delicate cases treated below.)

$\underline{q = 8}$. First suppose $n' = 3$. Then $x^{n'} - 1$ is the product of a linear and quadratic factor over $\mathbb{F}_q$. Assume first that $n' < n$. In Theorem 5.5 take $E = 1$. Write $n = 3 \cdot 2^b$, $b \geqslant 1$. Then $\delta = 1 - 1/8 - 1/64 = 55/64$ and $S = 174/55 < 3.17$. Since $n/2 - 2n/5 = n/10$, to ensure that (5.3) holds it suffices that $8^{\frac{3 \cdot 2^b}{10}} > 83.7 \times 3.17 = 265.32\ldots$. This holds if $b \geqslant 4$. For $1 \leqslant b \leqslant 3$, as it happens, $\omega(8^n - 1) = 4b$ (exactly) and (5.1) holds if $8^{n/2} > 2^{4b+1} \times 3.17$, which is true. So assume $n = 3$ in which case $q^n - 1 = 7 \times 73$. In Theorem 5.6, take $e = 1$ and $E = 1$, so that $s = 2$, $t = 2$ and $\delta = 1 - 1/8 - 1/64 - 2/7 - 2/73 > 0.5462$. Hence $S < 11.155$. In this case (5.5) holds because $8^{3/2} > 22.62 > 22.31 > 2S$.

Next take $n' = 21$. Then $x^{n'} - 1$ factors as a product of 14 irreducible polynomials (7 linear and 7 quadratic) over $\mathbb{F}_q$. In Theorem 5.5 take E to be the product of the 7 linear factors, in which case $\delta = 57/64 = 0.8906\ldots$ and $S < 8.74$. Then, without knowing the factorisation of $8^n - 1$, it suffices to show that $8^{n/10} > 83.7 \times 2^7 \times S$, which holds if $n \geqslant 84$. On the other hand, knowing the factorisation of $8^n - 1$, it suffices that $8^{n/2} > 2^{2\omega+8}S$, where $\omega = \omega(8^n - 1)$. In fact, $\omega(8^{42} - 1) = 11$ and $\omega(8^{21} - 1) = 6$ which and (5.5) is easily satisfied. Thus $(8, n) \in \mathcal{Q}$ whenever $n' = 21$.

Assume therefore that $n \neq 3, 21$. By Lemma 7.1(iii), $2^{\rho(8,n)} \leqslant 8^{1/15}$. Since $1/10 - 1/15 = 1/30$, by Theorem 5.5, to ensure that (5.1) holds it suffices that $8^{\frac{n}{30}} > 83.5n$. This would be guaranteed if $n \geqslant 135$. So assume, $n \leqslant 134$, whence $\omega(8^n - 1) \leqslant 61$ and (5.1) holds if $n \geqslant 100$. Having performed a sieving cycle (as for $q \geqslant 16$) we can assume $n \leqslant 49$. Then, after using the exact value of $\omega(8^n - 1)$, we are left with the pairs $n = 5, 10, 20$, for all of which $n' = 5$. For these $x^{n'} - 1$ is a product over $\mathbb{F}_q$ of a linear factor and an irreducible quartic so that, with $E = 1$, $\delta = 1 = 1/8 - 1/4096 > 0.8747$, $S < 3.15$ and it suffices that $8^{n/2} > 3.15 \times 2^{2\omega+1}$. This holds if $n = 10$ or 20 (for which $\omega = 6, 11$, respectively). Finally, if $n = 5$, then $8^n - 1 = 7 \times 31 \times 151$. In Theorem 5.6, sieve completely into primes/irreducibles (i.e., take $e = 1$, $E = 1$). Then $s = 3$, $t = 2$, $\delta > 0.5112$ and $2S < 27.4$, whereas $8^{n/2} > 181$. Hence $(8, 5) \in \mathcal{Q}$.

$q = 4$. Suppose $n' = 45$. Then $x^{n'} - 1$ is a product of 3 linear factors, 6 quadratics, 2 cubics and 4 sextics. In Theorem 5.5 take E to be the product of the three linear factors. Then $\delta = 1 - 6/16 - 2/64 - 4/1024 > 0.5922$ and $S < 20.58$. Hence (5.3) holds if $4^{n/10} > (2^3 \times 83.7 \times 20.58) = 16\,036.17\ldots$, which holds if $n \geqslant 90$. But, if $n = 45$, then $\omega(4^n - 1) = 11$ and (5.3) holds since $4^{45/2} > 3.51 \times 10^{13}$ and $2^{2\omega+4}S < 2^{26} \times 20.58 < 1.39 \times 10^9$. Hence $(4, n) \in \mathcal{Q}$ when $n' = 45$.

Suppose $n' = 9$. Then $x^{n'} - 1$ factorises as a product of 3 linear factors and 2 irreducible cubics. In Theorem 5.5 again take E to be the product of the three linear factors so that $\delta = 31/32$ and $S < 3.033$. As before, it suffices that $4^{n/10} > 2^3 \times 83.7 \times 3.033 = 2030.8\ldots$, which holds if $n \geqslant 72$. Knowledge of $\omega = \omega(8^n - 1)$ would allow us to check whether $4^{n/2} > 2^{2\omega+4}$. Indeed this holds with $n = 36$, because $\omega = 12$. Suppose $n = 18$. Then $4^n - 1 = 3^3 \times 5 \times 7 \times 13 \times 19 \times 37 \times 73 \times 109$. Now apply Theorem 5.6 with $e = 105$ and E as before so that $s = 5$, $t = 2$ and $\delta = 0.6098\ldots$. Then (5.5) holds since $4^9 = 262\,144 > 20\,521 > 2^{10} \times S$. Thus $(4, 18) \in \mathcal{Q}$. When $n = 9$, then $4^n - 1 = 3^3 \times 7 \times 19 \times 73$, too many factors to allow successful application of Theorem 5.6. So $(4, 9)$ has to be checked directly for membership of $\mathcal{Q}$.

$(4, 9)$. $(4, 9) \in \mathcal{Q}$ using $f = x^9 + x^8 + ux^7 + ux^6 + (u + 1)x^5 + ux^3 + x + u + 1$, $g = x^9 + (u + 1)x^8 + x^7 + ux^6 + ux^5 + x^4 + ux^3 + x^2 + u + 1$, where $u^2 + u + 1 = 0$.

Suppose $n' \neq 9, 45$; thus $\rho(q, n) \leqslant 1/5$. First assume n is even (and so $n' < n$). Then $\rho(q, n) \leqslant 1/10$ and $2^{\rho(n)} \leqslant q^{n/20}$. Since $1/10 - 1/20 = 1/20$, as before, for $(4, n) \in \mathcal{Q}$ it suffices that $4^{n/20} > 83.7n$ which holds when $n \geqslant 135$. Indeed, a sieving cycle (as before when $q = 8$) allows us to suppose $n \leqslant 44$. Thus $n = 10, 20$. In these cases $x^{n'} - 1 = x^5 - 1$ factorises as a product of a linear and two quadratic factors. We treat the (more delicate) case $n = 10$ so that $4^n - 1 = 3 \times 5^2 \times 11 \times 31 \times 41$. In Theorem 5.6 take $e = 75$, $E = 1$ so that $s = t = 3$ and $\delta > 0.3298$, $S < 24.26$. It suffices if $4^5 = 1024 > 26.26 \times 2^5 = 840.3\ldots$. By (5.5), $(4, 10) \in \mathcal{Q}$. More easily, $(4, 20) \in \mathcal{Q}$.

Next suppose $n \neq 9, 45$ is odd. We need a variation of Lemma 6.2.

Lemma 7.3. *Suppose $m = 4^n - 1$, where n is odd. Then $W(m) < 6.04 \times m^{1/6}$.*

Proof. Suppose a prime l divides $m = 4^n - 1$. Then $4^n \equiv 1 \bmod l$ so that the order of 4 mod l is odd. The set of primes less than 64 which have this property is $U = \{3, 7, 11, 19, 23, 31, 43, 47, 59\}$, whence $W(m) < \prod_{l \in U} \frac{2}{l^{1/6}} \times m^{1/6} < 6.04 \times m^{1/6}$. □

Remark. For a prime factor l of $4^n - 1$ it is not necessary that $l \equiv 3 \bmod 4$; for example $281 | 4^{35} - 1$.

Now to ensure that (5.1) holds it suffices that $4^{\frac{n}{2}} > 2(6.04)^2 \cdot 4^{\frac{2n}{6}} \cdot 2^{\rho(n)} S$, i.e., $4^{\frac{n}{15}} > 73n$ which is the case if $n > 95$. So assume $n \leqslant 95$. Using the exact value of $\omega(4^n - 1)$ we deduce that $(4, n) \in \mathcal{Q}$ if $n \neq 5, 7, 11, 15$. We treat these briefly via (5.5) in turn. Set $R = 2^{2\omega(e)+\omega(E)+1} S$.

(4, 15). $4^{15} - 1 = 3^2 \times 7 \times 11 \times 31 \times 151 \times 331$, $x^{15} - 1$ is a product of a linear factor and 7 irreducible quadratics. Take $e = 63$, $E = x + 1$. Thus, $s = 4$, $t = 7$, $\delta > 0.2968$ and $R < 3146.9$, whereas $4^{15/2} = 32\,768$. Hence $(4, 15) \in \mathcal{Q}$.

(4, 11). $4^{11} - 1 = 3 \times 23 \times 89 \times 683$, $x^{11} - 1$ is a product of a linear factor and 2 irreducible quintics. Easily (as for $(4, 7)$ below), $(4, 11) \in \mathcal{Q}$.

(4, 7). $4^7 - 1 = 3 \times 43 \times 127$, $x^7 - 1$ is a product of a linear factor and 2 irreducible cubics. Take $e = 3$, $E = 1$. Thus, $s = 2$, $t = 3$, $\delta > 0.6564\ldots$ and $R < 89.2$, whereas $4^{7/2} = 128$. Hence $(4, 7) \in \mathcal{Q}$.

(4, 5). $4^5 - 1 = 3 \times 11 \times 31$, $x^5 - 1$ is a product of a linear factor and 2 irreducible quadratics. This time sieving fails and $(4, 5)$ has to be checked directly for membership of $\mathcal{Q}$, as follows. $f = x^5 + ux^4 + ux^3 + x^2 + u$, $g = x^5 + ux^4 + x^2 + ux + u$, where $u^2 + u + 1 = 0$.

$\underline{q = 2}$. The following easy result deals, for example, with $n = 3, 5, 7, 13$.

Lemma 7.4. *Suppose $2^n - 1 \geqslant 7$ is a (Mersenne) prime. Then $(2, n) \in \mathcal{Q}$.*

Proof. Choose $\alpha \in \mathbb{F}_{2^n}$ normal. Then $\alpha \notin \mathbb{F}_2$ and so α is primitive. Indeed, $\beta = \alpha + 1/\alpha$ also is primitive (since $\beta \in \mathbb{F}_2 \implies \alpha = 1$ or $\alpha^2 + \alpha + 1 = 0$, not so). □

Now suppose $n' = 3$. Since $x^{n'} - 1$ is the product of a linear factor and a quadratic factor, by (5.3) of Theorem 5.5 (with $e = 2^n - 1$ and $E = x^{n'} - 1$) for membership of $\mathcal{Q}$, it suffices to show that $2^{n/10} > 83.5 \times 3 = 250.5$ which holds if $n \geqslant 96$. Similarly, if $n = 48$, then $\omega = 9$ and it suffices that $2^{n/2 - 2\omega - 3} = 8 > 1$. Otherwise, knowing the factorisation of $2^n - 1$ one can employ Theorems 5.5 or 5.6. If $n = 24$, then $q^n - 1 = 3^2 \times 5 \times 7 \times 13 \times 17 \times 241$. Take $e = 105$, $E = x + 1$. Then $s = 3$, $t = 1$, $\delta > 0.4702$,

$S < 14.77$ and $2^{n/2} = 4096 > 3779 > 2^8 S$. Hence $(2,24) \in \mathcal{Q}$. This leaves $(2,6)$, $(2,12)$ to be checked directly.

$(2,6)$. $f = x^6 + x^5 + 1$, $g = x^6 + x^5 + x^3 + x^2 + 1$.

$(2,12)$. $f = x^{12} + x^{11} + x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$, $g = x^{12} + x^9 + x^8 + x^6 + x^5 + x^4 + 1$.

Suppose next $n' = 5$. $x^{n'} - 1$ is the product of a linear factor and an irreducible quartic. As for $n' = 3$ it suffices if $2^{n/10} > 83.5 \times 3 = 250.5$ and certainly if $n \geqslant 80$. Alternatively, it suffices that $q^{n/2-2\omega-3} = 8 > 1$, which holds if $n = 40$ when $\omega = 7$. Take $n = 20$. Then $2^{20} - 1 = 3 \times 5^2 \times 11 \times 31 \times 41$. Take $e = 15$, $E = x + 1$. Thus, $s = 3$, $t = 1$, $\delta > 0.4548$, $S < 15.193$ and $q^{n/2} = 1024 > 973 > 2^6 S$. Hence $(2,20) \in \mathcal{Q}$. The pair $(2,10)$ requires direct treatment.

$(2,10)$. $f = x^{10} + x^9 + x^4 + x^2 + 1$, $g = x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 + 1$.

Suppose $n' = 9$. $x^9 - 1$ is a product of a linear, quadratic and sextic polynomial. As before, it suffices that $2^{n/10} > 83.5 \times 7.5 = 626.25$, which is satisfied if $n \geqslant 144$. For smaller values of n use Theorem 5.6 with $E = (x+1)(x^2+1)$. In particular, when $n = 72$ or 36, then $\omega = 12$ or 8, respectively, and one can take $e = 135$ so that $\delta > 0.2091$ or 0.3397, respectively. Easily, (5.5) is satisfied. We give more detail for $n = 18$. Then $2^n - 1 = 3^3 \times 7 \times 19 \times 73$. Take $e = 27$ and $E = (x+1)(x^2+x+1)$. Then $s = 3$, $t = 2$, $\delta > 0.3160$ and $S < 24.16 < 32 = 2^{n/2-4}$. Hence $(2,18) \in \mathcal{Q}$. The pair $(2,9)$ requires direct treatment.

$(2,9)$. $f = x^9 + x^8 + x^5 + x^4 + 1$, $g = x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + 1$.

The final special value of n' is 21. Then $x^{21} - 1 = (x+1)(x^2+x+1)(x^3+x^2+1)(x^3+x+1)(x^6+x^5+x^4+x^2+1)(x^6+x^4+x^2+x+1)$. As in the previous cases, $(2,n) \in \mathcal{Q}$ for $n \geqslant 168$ and then, having factorised $2^n - 1$, for $n = 84, 42$. Finally, suppose $n = 21$ so that $2^n - 1 = 7^2 \times 127 \times 337$. Take $e = 1$, $E = (x+1)(x^2+x+1)$: thus $s = 3$ and $t = 4$. Then $\delta = 0.4113$ and $S < 23.9$. For $(2,21)$ it is sufficient that $2^{21/2} > 1448 > 8S$, which is so.

Now suppose $n' \neq 3, 5, 9, 21$; thus $\rho(q,n) \leqslant 1/6$. First assume n is divisible by 4. Then $2^{\rho(n)} \leqslant 2^{n/24}$. Since $1/10 - 1/24 = 7/120$, as before, for $(2,n) \in \mathcal{Q}$ it suffices that $2^{7n/120} > 83.7n$ which holds when $n \geqslant 246$. Hence we may assume $n \leqslant 244$. Indeed, after performing a sieving cycle we can conclude $n \leqslant 120$. After taking exact value of $\omega(2^n - 1)$ we are left with the single pair $(2,28)$. In this case $2^n - 1 = 3 \times 5 \times 29 \times 43 \times 113 \times 127$, $x^7 - 1$ is a product of a linear factor and an irreducible sextic. Take $e = 3$, $E = x + 1$. Thus, $s = 5$, $t = 1$, $\delta > 0.4354$ and $S < 25$. Thus $2^{n/2} = 16\,384 > 64S$ and $(2,28) \in \mathcal{Q}$.

Now, assume n is even but indivisible by 4 (with $n' \neq 3, 5, 9, 21$). Then $\rho(n) \leqslant 1/12$. On the other hand, we may assume $\omega(2^n - 1) < 6.04 \times 2^{n/6}$ by Lemma 7.3. Since $1/2 - 2/6 - 1/12 = 1/12$, for $(2,n) \in \mathcal{Q}$ it suffices that $2^{n/12} > 73n$ which holds when $n \geqslant 163$. Hence we may assume $n \leqslant 162$. After substituting exact value of $\omega(2^n - 1)$, we are left to check for membership of $\mathcal{Q}$ the pairs $(2,n)$ for $n = 14, 22, 30$. To illustrate, consider $(2,14)$ so that $2^n - 1 = 3 \times 43 \times 127$, $x^7 - 1$ is a product of a linear factor and an irreducible sextic. Take $e = 1$, $E = x + 1$. Thus, $s = 3$, $t = 1$, $\delta > 0.2554$ and $S < 25$. Hence $2^7 = 128 > 4S$ and $(2, 14) \in \mathcal{Q}$.

Finally, assume $n \neq 3, 5, 9, 21$ is odd. Then $\rho(n) \leqslant 1/6$. We need a variation of Lemma 7.3.

Lemma 7.5. *Suppose n is odd. Then $W(2^n - 1) < 3.76 \times 2^{n/7}$.*

Proof. Suppose a prime l divides $2^n - 1$. Then $2^n \equiv 1 \bmod l$ so that the order of 2 mod l is odd. The set of primes less than 128 which have this property is $V = \{7, 23, 47, 71, 73, 79, 89, 103, 127\}$, whence $W(2^n - 1) < \prod_{l \in V} \frac{2}{l^{1/7}} \times 2^{n/7} < 3.76 \times 2^{n/7}$. □

Since $1/2 - 2/7 - 1/6 = 1/21$ and $3.76^2 = 14.15$, by Lemma 7.5, for $(2, n) \in \mathcal{Q}$ it suffices that $2^{n/21} > 28.3n$, which holds if $n \geqslant 271$. So assume $n \leqslant 271$. Taking into account that all prime divisors l of $2^n - 1$, n odd are such that 2 has odd order modulo l it follows that $\omega \leqslant 38$, whence $n \leqslant 247$. Having performed a sieving cycle (on the same basis) we conclude that, if $n > 205$ then $(2, n) \in \mathcal{Q}$. So, assume $n \leqslant 205$. By using the exact value of $\omega(2^n - 1)$, we conclude that $(2, n) \in \mathcal{Q}$ unless, $n = 11, 15$. Using, Theorem 5.6 with $e = 1$ in each case, easily, $(2, 15), (2, 11) \in \mathcal{Q}$.

This completes the proof of Theorem 1.2.

Acknowledgment

The author is grateful to the referees for a number of corrections and improvements to the original manuscript.

References

[1] T. Cochrane, C. Pinner, Using Stepanov's method for exponential sums involving rational functions, J. Number Theory 116 (2006) 270–292.
[2] S.D. Cohen, Consecutive primitive roots in a finite field, Proc. Am. Math. Soc. 93 (1985) 189–197.
[3] S.D. Cohen, Consecutive primitive roots in a finite field, II, Proc. Am. Math. Soc. 94 (1985) 605–611.
[4] S.D. Cohen, Pairs of primitive roots, Mathematika 32 (1985) 276–285.
[5] S.D. Cohen, S. Huczynska, The primitive normal basis theorem – without a computer, J. Lond. Math. Soc. 67 (2003) 41–56.
[6] S.D. Cohen, S. Huczynska, The strong primitive normal basis theorem, Acta Arith. 143 (2010) 299–322.
[7] H.W. Lenstra, R.J. Schoof, Primitive normal bases for finite fields, Math. Comput. 48 (1987) 217–231.
[8] P. Wang, X. Cao, R. Feng, On the existence of some specific elements in finite fields of characteristic 2, Finite Fields Appl. 18 (2012) 800–813.