ACTA ARITHMETICA
XCIV.2 (2000)

Kloosterman sums and primitive elements in Galois fields

by

Stephen D. Cohen (Glasgow)

1. Introduction. Let $\mathbb{F}_q$ denote the finite (Galois) field of order q, a power of a prime p. The multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is cyclic of order $q-1$: a generator is known as a *primitive element* of $\mathbb{F}_q$. Hence $\mathbb{F}_q$ contains $\phi(q-1)$ primitive elements, where ϕ is Euler's function. Generally, primitivity is a fragile property that may be destroyed when the element in question is modified through multiplication or addition. Nevertheless, if ξ is a primitive element, then so is $1/\xi$.

When $q = 2$, H. Niederreiter [Ni] has expressed the number of irreducible polynomials of degree n (≥ 3) over the binary field $\mathbb{F}_2$, having the coefficients of x^{n-1} and x both equal to 1, as a formula involving Kloosterman sums over $\mathbb{F}_{2^n}$. Thereby, this number is shown to be positive, except when $n = 3$. An alternative formulation of this conclusion is that, except when $n = 3$, $\mathbb{F}_{2^n}$ contains an element ξ such that $\mathbb{F}_{2^n} = \mathbb{F}_2(\xi)$, and both ξ and $1/\xi$ have $(\mathbb{F}_{2^n}, \mathbb{F}_2)$-trace equal to 1. In this paper we consider extensions $\mathbb{F}_{q^n}$ of a general finite field $\mathbb{F}_q$. The aim is to show that Kloosterman sums are adequate for the stiffer task of generalising the above result (when $n \geq 5$) to yield the existence of a primitive element ξ of $\mathbb{F}_{q^n}$ such that $T_n(\xi) = a$ and $T_n(1/\xi) = b$, where a and b are (arbitrary) given elements of $\mathbb{F}_q$ and $T_n(\xi) := \xi + \xi^q + \ldots + \xi^{q^{n-1}}$ denotes the $(\mathbb{F}_{q^n}, \mathbb{F}_q)$-trace of ξ. The result to be proved is as follows.

Theorem 1.1. *Let q be a prime power and n (≥ 5) be an integer. Suppose that arbitrary elements a and b of $\mathbb{F}_q$ are given. Then there exists a primitive element ξ of $\mathbb{F}_{q^n}$ such that $T_n(\xi) = a$ and $T_n(1/\xi) = b$, except when $a = b = 0$ and $(q, n) = (4, 5), (2, 6),$ or $(3, 6)$.*

Theorem 1.1 is consistent with the pattern that, as n increases, one can expect to guarantee the existence of a primitive element satisfying additional

2000 *Mathematics Subject Classification*: 11L05, 11T24, 11T30.

constraints. Let it be stressed that what are sought are complete results listing *all* exceptions. For example, prior to Theorem 1.1 is the theorem of Cohen [Co1] (see also [JuVa]) that, given $a \in \mathbb{F}_q$ and $n \geq 2$ ($n \geq 3$, if $a = 0$), there exists a primitive element ξ of $\mathbb{F}_{q^n}$ with $T_n(\xi) = a$, except when $n = 3$, $q = 4$, and $a = 0$. Another stage in the scheme is described later in the introduction.

The proof of Theorem 1.1 derives from careful estimates in respect of expressions that combine Kloosterman sums over $\mathbb{F}_{q^n}$ and over $\mathbb{F}_q$. Next, some properties of Kloosterman sums (and Gauss sums) will be developed. For example, whereas the absolute value of a Kloosterman sum over $\mathbb{F}_q$ is bounded by $2\sqrt{q}$, on average, it is less than $\sqrt{q}$ (Corollary 3.2). By means of a sieving process, the proof is completed theoretically, without direct verification, except for a few small values of q (≤ 16) and $n = 5$ or 6, plus $q = 2$ when $n = 8$ (when a and b are not both zero). In fact, when a and b are both zero, then Theorem 1.1 follows from the work of W.-S. Chou and the author [ChCo] and is "best possible" in the sense that it fails for all pairs (q, n) with $n < 5$. Otherwise, the method will succeed, in principle, also when $n = 4$. We defer the study of this case to a further paper, because of the difficulty of identifying efficiently those values of q for which direct verification is required. The question addressed is sensible even when $n = 3$, but the method fails, and it may be difficult to resolve that case.

For $n \geq 2$, the associated (irreducible) minimal polynomial (of degree n) over $\mathbb{F}_q$ of a primitive element ξ of $\mathbb{F}_q$ is itself referred to as *primitive*. Since the $(\mathbb{F}_{q^n}, \mathbb{F}_q)$-norm of such an element ξ is necessarily a primitive element of $\mathbb{F}_q$, and so, when $q = 2$ or 3, is uniquely determined, we have the following consequence of Theorem 1.1.

Corollary 1.2. *Suppose that q is a prime power*, $n \geq 5$, *and a_{n-1} and a_1 are given elements of $\mathbb{F}_q$. Then*, *if either $a_{n-1} = a_1 = 0$ or $q \leq 3$*, *there exists a primitive polynomial of the form*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0. \tag{1.1}$$

More generally, Theorem 1.1 implies that there is a primitive polynomial of the form (1.1) for $n \geq 5$ with both a_{n-1} and the ratio a_1/a_0 prescribed. The Kloosterman sum technique should be instrumental in delivering the next stage in the programme beyond Theorem 1.1, namely, that for given values of a_{n-1}, a_1, and a_0 (with a_0 a primitive element of $\mathbb{F}_q$ and $n \geq 6$ or, perhaps, $n \geq 7$), there is a primitive polynomial (1.1) with prescribed values of a_{n-1}, a_1 and a_0. For other results, conjectures, and data on the existence of primitive elements of $\mathbb{F}_{q^n}$ satisfying further constraints, see, for example, [HaMu], [Mu], [MoMu], [Ha], [CoHa1,2], [Co2]. I also acknowledge some preliminary notes by Dr Wun-Seng Chou (Taipei) on the "fixed traces" question, out of which the considerations of this paper arose.

From the results of [ChCo] we can exclude the case $a = b = 0$ of Theorem 1.1 in what follows. Indeed, by symmetry, we shall assume, without loss of generality, that $a \neq 0$.

2. Character sum formulation.

The number of elements ξ of $\mathbb{F}_q^*$ for which $T_n(\xi) = a$ and $T_n(1/\xi) = b$ can be expressed in terms of (standard) Kloosterman sums over $\mathbb{F}_{q^n}$. The further constraint that ξ can be primitive heralds the introduction of multiplicative characters and more intricate expressions involving generalised (or twisted) Kloosterman sums. Obtaining the relevant formulae in their most transparent form is the object of this section. For the background on Kloosterman sums and Gauss sums for this section and Section 3, Chapter 5 of [LiNi] (including the Exercises) or some other source may be consulted.

Let M be a divisor of $q^n - 1$. If $\xi \in \mathbb{F}_{q^n}^*$ is such that $\xi = \alpha^d$, where $d \mid M$ and $\alpha \in \mathbb{F}_{q^n}$, implies $d = 1$, we shall say that ξ is *not any kind of Mth power in* $\mathbb{F}_{q^n}$. Given q, n, a, b as in Section 1, define $N_{q,n}(M; a, b)$ $(= N_{q,n}(M) = N(M))$ to be the number of elements ξ of $\mathbb{F}_{q^n}^*$, scaled (multiplied) by a factor q^2 (for convenience), such that $T_n(\xi) = a$, $T_n(1/\xi) = b$, and ξ is not any kind of Mth power in $\mathbb{F}_{q^n}$. To establish Theorem 1.1 in respect of q, n, a, b, it is necessary to show that $N_{q,n}(M; a, b)$ for general divisors M of $q^n - 1$. Note, in particular, that the value of $N(M)$ depends only on the distinct prime divisors of M, i.e., on the square-free part of M.

Next, we lay down the basic material on characters. It will be amplified later. Let χ be the canonical additive character of $\mathbb{F}_q$. Thus, for $x \in \mathbb{F}_q$, $\chi(x) = \exp(2\pi i T(x)/p)$, where here T denotes the absolute trace (from $\mathbb{F}_q$ to $\mathbb{F}_p$). Moreover, every additive character $\widehat{\chi}$ of $\mathbb{F}_q$ is such that $\widehat{\chi}(x) = \chi(cx)$ $(x \in \mathbb{F}_q)$ for some $c \in \mathbb{F}_q$; take $c = 0$ to obtain the trivial character χ_0. Further, let $\chi' = \chi(T_n)$ denote the lift of χ to $\mathbb{F}_{q^n}$. Passing to multiplicative characters of $\mathbb{F}_{q^n}$, we shall reserve the symbol ψ for such; more precisely, for any divisor d of $q^n - 1$, ψ_d will denote a typical character of $\mathbb{F}_{q^n}$ of exact order d. Thus, ψ_1 is the trivial character.

Now, for any $\alpha, \beta \in \mathbb{F}_{q^n}$ and any multiplicative character ψ, we define the generalised Kloosterman sum $K_n(\alpha, \beta; \psi)$ $(= K_{q,n}(\alpha, \beta; \psi))$ by

$$K_n(\alpha, \beta; \psi) = \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi'(\alpha\xi + \beta\xi^{-1})\psi(\xi).$$

In particular, we write $K_n(\alpha, \beta)$ for $K_n(\alpha, \beta; \psi_1)$, the (standard) Kloosterman sum.

As a final preliminary to the basic formula, we describe some further notation. In a sum $\sum_u$ (or double sum $\sum_{u,v}$), the variable(s) will be assumed to run over all members of the ground field $\mathbb{F}_q$. If u runs over $\mathbb{F}_q^*$ we will write $\sum_{u \neq 0}$, etc. For any divisor M of $q^n - 1$, abbreviate to $\int_{d \mid M}$ a weighted sum of the form $\sum_{d|M}(\mu(d)/\phi(d))\sum_{(d)}\psi_d$, where μ is the Möbius function, and the inner sum ranges over all $\phi(d)$ characters of order d. Further for any positive integer h, set

$$\Theta(h)=\phi(h)/h=\prod_{l|h,\,l\ \mathrm{prime}}(1-l^{-1}).$$

Moreover, a bar over a symbol signifies complex conjugation.

Proposition 2.1. *Let q be a prime power and n a positive integer. Suppose that elements a,b of $\mathbb{F}_q$ are given. Then, for any divisor M of q^n-1, we have*

$$N_{q,n}(M;a,b)=\Theta(M)\sum_{u,v}\overline{\chi}(au+bv)\int_{d|M}K_n(u,v;\psi_d). \tag{2.1}$$

Proof. The characteristic function for the subset of $\mathbb{F}_{q^n}^*$ comprising elements that are not any kind of Mth power can be expressed as an extension of the Vinogradov formula, [Ju], Lemma 7.5.3. It takes the form $\Theta(M)\int_{d|M}\psi_d(\xi)$. Moreover, that for the subset of $\mathbb{F}_{q^n}$ comprising elements with $T_n(\xi)=a$ is $(1/q)\sum_c\chi(c(T_n(\xi)-a))$. Hence, taking account of the scaling factor q^2, we have

$$\begin{aligned}N_{q,n}(M;a,b)&=\sum_{\xi\in\mathbb{F}_{q^n}^*}\Theta(M)\sum_{u,v}\chi(u(T_n(\xi)-a))\chi(v(T_n(\xi^{-1})-b))\int_{d|M}\psi_d(\xi)\\&=\Theta(M)\sum_{u,v}\overline{\chi}(au+bv)\int_{d|M}\chi(T_n(u\xi+v\xi^{-1}))\psi_d(\xi),\end{aligned}$$

and the result follows from the definition of the Kloosterman sum.

From Proposition 2.1, $N(M)$ can immediately be estimated using the standard bound for Kloosterman sums that follows.

Lemma 2.2. *Let ψ be a multiplicative character of $\mathbb{F}_{q^n}$. Then*

$$K_n(0,0;\psi)=\begin{cases}q^n-1 & \textit{if } \psi=\psi_1,\\ 0 & \textit{otherwise.}\end{cases}$$

Further, if either $\psi\neq\psi_1$ or $\alpha,\beta\in\mathbb{F}_{q^n}$ are not both zero, then

$$|K_n(\alpha,\beta;\psi)|\le 2q^{n/2}.$$

Nevertheless, before applying Lemma 2.2, it is profitable to develop the formula (2.1). This is the aim in the next sequence of lemmas. They also involve Gauss sums, since some Kloosterman sums reduce to these. The Gauss sum $G_n(\psi)$ is defined by

$$G_n(\psi)=\sum_{\xi\in\mathbb{F}_{q^n}^*}\chi'(\xi)\psi(\xi).$$

LEMMA 2.3. (i) *If* $\alpha\ (\neq 0), \beta \in \mathbb{F}_{q^n}$, *then*

$$K_n(\alpha,\beta;\psi) = \overline{\psi}(\alpha)K_n(1,\alpha\beta;\psi).$$

(ii) *If* $\beta \neq 0$, *then* $K_n(0,\beta;\psi) = \psi(\beta)G_n(\overline{\psi})$.
(iii) *If* $\alpha \neq 0$, *then* $K_n(\alpha,0;\psi) = \overline{\psi}(\alpha)G_n(\psi)$.

LEMMA 2.4. (i) $G_n(\psi_1) = -1$.
(ii) *If* $\psi \neq \psi_1$, *then* $|G_n(\psi)| = q^{n/2}$.
(iii) *If* q *is odd and* $n = 1$, *then* $G_1^2(\psi_2) = (-1)^{(q-1)/2}q$.
(iv) *If* q *is odd and* n *is even*, *then* $G_n(\psi_2) = -(-1)^{n(q-1)/4}q^{n/2}$.
(v) *If* q *and* n *are odd and* λ_2 *is the quadratic character on* $\mathbb{F}_q^*$, *then*

$$\overline{G}_1(\lambda_2)G_n(\psi_2) = (-1)^{(n-1)(q-1)/4}q^{(n+1)/2}.$$

Note that Lemma 2.4 contains information relating to the specific characters ψ_1 and (when q is odd) ψ_2, the quadratic character. Similarly, we can specialise Kloosterman sums to these cases, though the results are more complicated. First, when $\psi = \psi_1$ and u, v are in the ground field $\mathbb{F}_q$, then $K_n(u,v)$ can be expressed in terms of Kloosterman sums over $\mathbb{F}_q$. For $t \in \mathbb{F}_q^*$, set $k_t := K_1(1,t)$. Further, let $D_n(X,c)$ be the Dickson polynomial of the first kind of degree n. Thus, $D_n(X + c/X, c) = X^n + c^n/X^n$.

LEMMA 2.5. *Suppose* $t \in \mathbb{F}_{q^*}$. *Then*

$$K_n(1,t) = (-1)^{n-1}D_n(k_t, q).$$

Define

$$\delta_{q,n} := \left\{\frac{1}{q-1}\sum_{t\neq 0} K_n(1,t)\right\}\Big/q^{n/2}, \quad \delta_{q,n}^* := \left\{\frac{1}{q-1}\sum_{t\neq 0} |K_n(1,t)|\right\}\Big/q^{n/2}.$$

Then, from Lemma 2.2, it follows that

$$|\delta_{q,n}| \leq \delta_{q,n}^* \leq 2. \tag{2.2}$$

The next result indicates that the numbers k_t are essentially uniformly distributed.

LEMMA 2.6. *For a given prime power* q, $\sum_{t\neq 0} k_t = 1$.

Proof.

$$\sum_{t\neq 0} k_t = \sum_{t,u\neq 0} \chi\left(u + \frac{t}{u}\right) = \chi(0) = 1,$$

since, evidently, for any $c \in \mathbb{F}_q$, the equation $u + t/u = c$ (i.e., $t = u(c-u)$) has $q-2$ solution pairs $(t,u) \in (\mathbb{F}_q^*)^2$, unless $c = 0$, when there are $q-1$ solutions.

When q is odd, Kloosterman sums with $\psi = \psi_2$ (the quadratic character) are apparently easier to evaluate than standard sums. The following two results derive, in essence, from Lemma 3.5 and Corollary 3.6 of [ChCo]. For clarity, for any divisor e of $q-1$, we denote a multiplicative character of order e of $\mathbb{F}_q$ by λ_e.

Lemma 2.7. *Let q be an odd prime power. If n is odd and $t \in \mathbb{F}_q^*$ is such that $\lambda_2(t) = -1$, then $K_n(1,t;\psi_2) = 0$. If $\lambda_2(t) = 1$ with $s^2 = t$ ($s \in \mathbb{F}_q$) and $p \nmid n$, then*

$$K_n(1,t;\psi_2) = (\chi(2ns) + \chi(-2ns))G_n(\psi_2).$$

Otherwise, if n is odd, $p \mid n$, and $\lambda_2(t) = 1$, or n is even and either $p \mid n$ or $\lambda_2(t) = -1$, then

$$K_n(1,t;\psi_2) = 2G_n(\psi_2).$$

Lemma 2.8. *Let q be an odd prime power and n be an even integer. Then*

$$\sum_{t \neq 0} K_n(1,t;\psi_2) = -(-1)^{n(q-1)/4}(\varepsilon q - 2)q^{n/2},$$

where

$$\varepsilon = \begin{cases} 2 & \text{if } p \mid n, \\ 1 & \text{if } p \nmid n. \end{cases}$$

Given q, n, define

$$m = m(q,n) := \frac{q^n - 1}{q-1}.$$

The significance of this number is that there are occasions when it is useful to distinguish characters ψ_d for which $d \mid m$. This arises as follows. For *any* divisor d of $q^n - 1$, the restriction to $\mathbb{F}_q^*$ of a character ψ_d (of $\mathbb{F}_{q^n}^*$) will be denoted by $\widehat{\psi}_d$. Then, in fact, $\widehat{\psi}_d = \lambda_{d^*}$, where $d^* = (q-1)/\gcd((q^n-1)/d, q-1)$. In particular, $\widehat{\psi}_d = \lambda_1$ if and only if $d \mid m$. Moreover, if q is odd, then

$$\widehat{\psi}_d = \begin{cases} \lambda_2 & \text{if } n \text{ is odd,} \\ \lambda_1 & \text{if } n \text{ is even.} \end{cases} \tag{2.3}$$

To present refinements of Proposition 2.1, we modify the notation $\int_{d|M}$ used in its statement. First, for a divisor M' of M, write $\int_{d|M,\, d \nmid M'}$ to indicate a similar sum that excludes terms corresponding to divisors d of M'. This is modified further to $\int_{d|M,\, d\nmid M',\, \neq 2}$ to signify that the terms with $d = 2$ are excluded (if there remain any). This makes a difference only if q is odd, M is even, and M' is odd. A frequent choice of M' is $M^* := \gcd(M, m)$.

We come to the main theorems of this section; their statements depend heavily on declared notation. Because the formulae have a different shape according to whether a, b are zero or not, it is from this point on we insist that $a \neq 0$. In the first case, we also suppose that $b \neq 0$.

THEOREM 2.9. *Let q be a prime power and n (≥ 4) an integer. Suppose that $a, b \in \mathbb{F}_q^*$. Then, for any divisor M of q^n-1, we have*

$$(2.4)\quad N_{q,n}(M;a,b) = \Theta(M)\Big\{q^n + 1 + \varDelta_2 + (-1)^{n-1}\sum_{t\neq 0} k_{tab}D_n(k_t,q) \\ + \int_{\substack{d\mid M\\ d\nmid 2}}\sum_{t\neq 0}\overline{K}_1(1,tab;\widehat{\psi}_d)K_n(1,t;\psi_d) - 2\int_{\substack{d\mid M^*\\ d\nmid 2}} G_n(\psi_d) \\ + \int_{\substack{d\mid M\\ d\nmid M^*,\,\neq 2}} (\widehat{\psi}_d(a)+\widehat{\psi}_d(b))\overline{G}_1(\widehat{\psi}_d)G_n(\psi_d)\Big\},$$

where $\varDelta_2 = 0$, unless q is odd and M is even. In the latter event, if n is odd,

$$\varDelta_2 = (-1)^{(n-1)(q-1)/4}\gamma q^{(n+1)/2},$$

where

$$\gamma = \begin{cases} 4 & \textit{if } \lambda_2(a)=\lambda_2(b)=-1, \textit{ but } ab\neq n^2,\\ 2(1-\lambda_2(a))-q & \textit{if } ab=n^2,\\ 0 & \textit{otherwise}, \end{cases}$$

and, if n is even, $\varDelta_2 = (-1)^{n(q-1)/4}\gamma q^{n/2}$, where

$$\gamma = \begin{cases} \big((-1)^{(q+1)/2}+\frac{1}{2}\big)q-\frac{1}{2} & \textit{if } ab=n^2,\\ (-1)^{(q+1)/2}\big(\lambda_2(ab)-\frac{1}{2}\lambda_2(ab-n^2)\big)q-\frac{1}{2} & \textit{otherwise.} \end{cases}$$

Proof. We consider the terms on the right hand side of (2.1) (taking for granted the factor $\Theta(M)$). First, by Lemma 2.2, the contribution of the terms with $u=v=0$ is exactly q^n-1. Next, by Lemma 2.3(i), the contribution of the terms with $uv\neq 0$, on replacement of uv by t, becomes

$$\sum_{t\neq 0}\sum_{u\neq 0}\overline{\chi}\bigg(au+\frac{bt}{u}\bigg)\widehat{\psi}_d(u)K_n(1,t;\psi_d).$$

This yields the first two sums on the right hand side of (2.4) (with $\int_{1\neq d\mid M}$ rather than $\int_{d\mid M,\,d\nmid 2}$) on replacing au by u and separating, with the aid of Lemma 2.5, the contribution arising from ψ_1.

Next, by Lemma 2.3(ii), the contribution of the terms of (2.1) with $u=0$, $v\neq 0$, is

$$\int_{d\mid M}\Big\{\sum_{v\neq 0}\overline{\chi}(bv)\widehat{\psi}_d(v)\Big\}G_n(\overline{\psi}_d).$$

On interchanging ψ_d with its conjugate and replacing bv by v, we obtain

$$\int_{d\mid M}\widehat{\psi}_d(b)G_1(\widehat{\psi}_d)G_N(\psi_d) = 1 - \int_{1\neq d\mid M^*} G_n(\psi_d) + \int_{\substack{d\mid M\\ d\nmid M^*}}\widehat{\psi}_d(b)\overline{G}_1(\psi_d)G_n(\psi_d),$$

by Lemma 2.4(i). There is a similar contribution from the terms with $u \neq 0$, $v = 0$.

As a consequence of the above, it suffices to assume that q is odd and M is even, and prove that the net contribution of the terms in (2.1) corresponding to ψ_2 is the designated expression for Δ_2.

To this end, suppose first that n is odd; thus M^* is odd. Observing that the weighting factor $\mu(2)/\phi(2) = -1$, from (2.4) we have

$$\Delta_2 = -\lambda_2(a)(\lambda_2(ab)+1)\overline{G}_1(\lambda_2)G_n(\psi_2) - \sum_{t\neq 0} \overline{K}_1(1, tab; \lambda_2)K_n(1, t; \psi_2).$$

Now, for $t \in \mathbb{F}_q^*$, $\lambda_2(a) = 1$ if and only if $\psi_2(a) = 1$. Consequently, from Lemma 2.7, the product $\overline{K}_1(1, tab; \lambda_2)K_n(1, t; \psi_2)$ is zero unless $\lambda_2(t) = \lambda_2(tab) = 1$. Evidently, therefore, $\Delta_2 = 0$, unless $\lambda_2(ab) = 1$. Moreover, if $\lambda_2(ab) = 1$ and $c^2 = ab$, $c \in \mathbb{F}_q^*$, then, by Lemma 2.7 again, we have

$$\begin{aligned}\sum_{t\neq 0} &\overline{K}_1(1, tab; \lambda_2)K_n(1, t; \psi_2)\\ &= \overline{G}_1(\lambda_2)G_n(\psi_2)\sum_{s\neq 0}\chi(2ns)(\chi(2sc)+\chi(-2sc))\\ &= \overline{G}_1(\lambda_2)G_n(\psi_2)\sum_{s\neq 0}\{\chi(2s(n+c))+\chi(2s(n-c))\}.\end{aligned}$$

The sum in this expression is $q-2$ if $c = \pm n$ (i.e., $ab = n^2$). Otherwise, it is -2. The result for n odd now follows from Lemma 2.4(v).

Finally, suppose n is even, so that M^* is even. Then, by (2.3), $\widehat{\psi}_2 = \lambda_1$, and

$$\begin{aligned}(2.5)\quad \Delta_2 &= 2G_n(\psi_2) - \sum_{t\neq 0} K_1(1, tab)K_n(1, t; \psi_2)\\ &= G_n(\psi_2)\Big(2 - \sum_{t\neq 0}(1-\lambda_2(t))K_1(1, tab) - \sum_{s\neq 0}\chi(2ns)K_1(1, s^2ab)\Big)\\ &= G_n(\psi_2)\Big(1 + \sum_{t\neq 0}\lambda_2(t)K_1(1, tab) - \sum_{s\neq 0}\chi(2ns)K_1(1, s^2ab)\Big),\end{aligned}$$

by Lemmas 2.7 and 2.6. Now, in (2.5), we have

$$\begin{aligned}\sum_{t\neq 0}\lambda_2(t)K_1(1, tab) &= \sum_{t,u\neq 0}\chi\Big(u + \frac{tab}{u}\Big)\lambda_2(t) = \sum_{u\neq 0}\chi(u)\sum_{t\neq 0}\chi\Big(\frac{abt}{u}\Big)\lambda_2(t)\\ &= \lambda_2(ab)\sum_{u\neq 0}\chi(u)\lambda_2(u)G_1(\lambda_2)\\ &= \lambda_2(ab)G_1^2(\lambda_2) = (-1)^{(q-1)/2}\lambda_2(ab)q,\end{aligned}$$

by Lemma 2.4(iii). Also, in (2.5), we have

$$\begin{aligned}S &:= \sum_{s\neq 0}\chi(2ns)K_1(1,s^2ab) = 1+\sum_s\sum_{u\neq 0}\chi\Big(u+\frac{s^2ab}{u}+2ns\Big)\\ &= 1+\sum_{u\neq 0}\chi\Big(u\Big(1-\frac{n^2}{ab}\Big)\Big)\sum_s\chi\Big(\frac{ab}{u}\Big(s-\frac{nu}{ab}\Big)^2\Big)\\ &= 1+\sum_{u\neq 0}\chi\Big(u\Big(1-\frac{n^2}{ab}\Big)\Big)\Big\{\Big[\frac{1}{2}\sum_{v\neq 0}\chi\Big(\frac{ab}{u}v\Big)(1+\lambda_2(v))\Big]+1\Big\}.\end{aligned}$$

Now, if $ab=n^2$, it follows that

$$S = 1+q-1+\frac{1}{2}\sum_{v\neq 0}(1+\lambda_2(v))\sum_{u\neq 0}\chi(abvu) = q-\frac{1}{2}\sum_{v\neq 0}(1+\lambda_2(v)) = \frac{1}{2}(q+1).$$

Hence, in this case,

$$\Delta_2 = G_n(\psi_2)\Big(\frac{1}{2}+(-1)^{(q-1)/2}q-\frac{1}{2}q\Big),$$

as required (by Lemma 2.4(iv)). On the other hand, if $ab\neq n^2$, then

$$\begin{aligned}S &= \frac{1}{2}\sum_{u\neq 0}\chi\Big(u\Big(1-\frac{n^2}{ab}\Big)\Big)\Big\{-1+\sum_{v\neq 0}\chi\Big(\frac{ab}{u}v\Big)\lambda_2(v)\Big\}\\ &= \frac{1}{2}\Big(1+G_1(\lambda_2)\sum_{u\neq 0}\chi\Big(u\Big(1-\frac{n^2}{ab}\Big)\Big)\lambda_2(abu)\Big)\\ &= \frac{1}{2}(1+\lambda_2(ab-n^2)G_1^2(\lambda_2)) = \frac{1}{2}(1+(-1)^{(q-1)/2}\lambda_2(ab-n^2)q).\end{aligned}$$

Again, by Lemma 2.4(iv), this yields the stated expression for Δ_2.

Here now is the corresponding result with $b=0$.

Theorem 2.10. *Let q be a prime power and n (≥ 4) an integer. Suppose that $a\in\mathbb{F}_q^*$. Then, for any divisor M of q^n-1, we have*

$$\begin{aligned}(2.6)\quad N_{q,n}(M;a,0) = \Theta(M)\Big\{q^n-q+1+\Delta_2+(-1)^n\sum_{t\neq 0}D_n(k_t,q)&\\ +\int_{\substack{d|M^*\\ d\nmid 2}}\Big[(q-2)G_n(\psi_d)-\sum_{t\neq 0}K_n(1,t;\psi_d)\Big]&\\ +\int_{\substack{d|M\\ d\nmid M^*,\neq 2}}\psi_d(a)\overline{G}_1(\widehat{\psi}_d)\Big[G_n(\psi_d)+\sum_{t\neq 0}K_n(1,t;\psi_d)\Big]\Big\},&\end{aligned}$$

where $\Delta_2 = 0$, unless q is odd, M is even and $p \mid n$. In the latter event, we have

$$\Delta_2 = \begin{cases} -(-1)^{n(q-1)/4}q^{n/2+1} & \textit{if } n \textit{ is even},\\ -\lambda_2(a)(-1)^{(n-1)(q-1)/4}q^{(n+3)/2} & \textit{if } n \textit{ is odd.}\end{cases}$$

Proof. Again the contribution of the terms in (2.1) with $u = v = 0$ is $q^n - 1$. That from the terms with $u = 0$, $v \neq 0$ is

$$\int_{d|M} G_n(\overline{\psi}_d)\sum_{v\neq 0}\widehat{\psi}_d(v) = -(q-1) + (q+1)\int_{1\neq d|M^*} G_n(\psi_d),$$

by Lemmas 2.3 and 2.4, plus the fact that $\widehat{\psi}_d$ is non-trivial if and only if $d \nmid M^*$. The contribution from the terms with $u \neq 0$, $v = 0$ is

$$\int_{d|M} G_n(\psi_d)\sum_{u\neq 0}\overline{\chi}(au)\overline{\widehat{\psi}}_d(u) = 1 - \int_{1\neq d|M^*} G_n(\psi_d) + \int_{\substack{d|M\\ d|M^*}} \psi_d(a)\overline{G}_1(\widehat{\psi}_d)G_n(\psi_d).$$

This, again, has used the fact that $\widehat{\psi}_d$ is trivial whenever $d \mid M^*$. The contribution of the terms with $uv \neq 0$ is

$$\begin{aligned}\int_{d|M}\sum_{t,u\neq 0}\overline{\chi}(au)\overline{\widehat{\psi}}_d(u)K_n(1,t;\psi_d)\\ = -\int_{d|M^*} K_n(1,t;\psi_d) + \int_{\substack{d|M\\ d\nmid M^*}} \psi_d(a)\overline{G}_1(\widehat{\psi}_d)K_n(1,t;\psi_d).\end{aligned}$$

This yields the remaining terms on the right-hand side of (2.6), apart from the evaluation of the terms arising from ψ_2.

Indeed, we now describe the contribution of the terms involving ψ_2 (when q is odd and M is even). If n is even, then M^* is even and

$$\begin{aligned}\Delta_2 &= -(q-2)G_n(\psi_2) + \sum_{t\neq 0} K_n(1,t;\psi_2)\\ &= \begin{cases} -(-1)^{n(q-1)/4}q^{n/2+1} & \text{if } p \mid n,\\ 0 & \text{otherwise,}\end{cases}\end{aligned}$$

by Lemma 2.8. On the other hand, if n is odd and so M^* is odd, then

$$\begin{aligned}\Delta_2 &= -\lambda_2(a)\overline{G}_1(\lambda_2)\Big(G_n(\psi_2) + \sum_{t\neq 0} K_n(1,t;\psi_d)\Big)\\ &= -\lambda_2(a)\overline{G}_1(\lambda_2)\Big(G_n(\psi_2) + \sum_{s\neq 0}\chi(2ns)G_n(\psi_d)\Big),\end{aligned}$$

by Lemma 2.7. Thus, $\lambda_2 = 0$, unless $p \mid n$, in which event,

$$\Delta_2 = -q\lambda_2(a)\overline{G}_1(\lambda_2)G_n(\psi_2) = -\lambda_2(a)(-1)^{(n-1)(q-1)/4}q^{(n+3)/2},$$

by Lemma 2.4(v). Hence, everything is proved.

3. Inequalities. The sums in the identities of Theorems 2.9 and 2.10 can obviously be estimated by means of the fundamental bounds for Kloosterman sums and Gauss sums stated in Lemmas 2.2 and 2.4(ii). Thus, for example, with regard to the main error terms in Theorem 2.9, we have

$$\Big|\sum_{t\neq 0}\overline{K}_1(1,tab;\widehat{\psi}_d)K_n(1,t;\psi_d)\Big| \le 4(q-1)q^{(n+1)/2}, \qquad d>1.$$

Crucially, we are able to halve this estimate; it then becomes similar to the corresponding estimate for the main error terms in Theorem 2.10, namely

$$\Big|\overline{G}_1(\widehat{\psi}_d)\sum_{t\neq 0}K_n(1,t;\psi_d)\Big| \le 2(t-1)q^{(n+1)/2}, \qquad d>1.$$

Lemma 3.1. *For any multiplicative character λ of $\mathbb{F}_q^*$, we have*

$$\sum_{t\neq 0}|K_1(1,t;\lambda)|^2 = \begin{cases} q(q-1)-1 & \text{if } \lambda=\lambda_1,\\ q(q-2) & \text{if } \lambda\neq\lambda_1.\end{cases}$$

Proof.

$$\begin{aligned}\sum_{t\neq 0}|K_1(1,t;\lambda)|^2 &= \sum_{t,u,v\neq 0}\chi\Big(u+\frac{t}{u}-v-\frac{t}{v}\Big)\lambda\Big(\frac{u}{v}\Big)\\ &= (q-1)^2+\sum_{t\neq u}\sum_{\substack{u,v\neq 0\\ u\neq v}}\chi\Big(u-v-\frac{t(u-v)}{uv}\Big)\lambda\Big(\frac{u}{v}\Big)\\ &= (q-1)^2+\sum_{t\neq u}\sum_{\substack{y\neq 0\\ z\neq 0,1}}\chi\Big(y-\frac{t(z-1)^2}{yz}\Big)\lambda(z)\\ &= (q-1)^2+\sum_{\substack{y\neq 0\\ z\neq 0,1}}\lambda(z)\sum_{t\neq 0}\chi\Big(y-\frac{t(z-1)^2}{yz}\Big)\\ &= (q-1)^2-\sum_{z\neq 0,1}\lambda(z)\sum_{y\neq 0}\chi(y) = (q-1)^2+\sum_{z\neq 0,1}\lambda(z)\\ &= \begin{cases}(q-1)^2+(q-2) & \text{if } \lambda=\lambda_1,\\ (q-1)^2-1 & \text{if } \lambda\neq\lambda_1,\end{cases}\end{aligned}$$

and the result follows.

Corollary 3.2. *For λ as in Lemma* 3.1,

$$\sum_{t\neq 0}|K_1(1,t;\lambda)| < (q-1)\sqrt{q}.$$

Hence, if d (>1) is a divisor of q^n-1 and $ab\in\mathbb{F}_q^*$, then

$$\Big|\sum_{t\neq 0}\overline{K}_1(1,tab;\widehat{\psi}_d)K_n(1,t;\psi_d)\Big|<2(q-1)q^{(n+1)/2}.$$

Proof. By Cauchy's inequality and Lemma 3.1,

$$\sum_{t\neq 0}|K_1(1,t;\lambda)|\le\sqrt{q-1}\Big(\sum_{t\neq 0}|K_1(1,t;\lambda)|^2\Big)^{1/2}<\sqrt{q-1}\sqrt{q(q-1)}$$
$$=(q-1)\sqrt{q}.$$

Granted Lemma 2.2, the other inequality is immediate.

Taking $\lambda=\lambda_1$ in Corollary 3.2, we see that $\delta_q^*:=\delta_{q,1}^*$ (see Section 2) satisfies $\delta_q^*<1$ (cf. (2.2)). Indeed, for a range of prime values of q tested (with $7<q<200$), δ_q^* lay within the interval $(0.82, 0.89)$.

Moreover, we can effectively improve further on Corollary 3.2 under the following circumstances: q,n odd, d even, $d\,|\,2m$ (so that $\widehat{\psi}_d=\lambda_2$).

Lemma 3.3. *Let q be an odd prime power and χ be the canonical additive character on $\mathbb{F}_q$. Then*

$$\sum_s|\chi(s)+1|=\frac{2q}{p}\operatorname{cosec}\left(\frac{\pi}{2p}\right).$$

Proof. Suppose $q=p$, an odd prime. Then

$$\sum_s|\chi(s)+1|=\sum_s 2|\cos(\pi s/p)|=2\Big(1+2\sum_{s=0}^{(p-1)/2}\cos(\pi s/p)\Big)$$
$$=2\operatorname{cosec}(\pi/(2p)).$$

This implies the result for a prime power q, since the elements of $\mathbb{F}_q$ are uniformly distributed with respect to absolute trace.

Lemma 3.4. *Let q be an odd prime power. Define κ_q by*

$$\kappa_q=\begin{cases}\dfrac{4}{\pi} & \text{if } q=p \text{ or } p^2,\\[2mm] \dfrac{4}{\pi}\left(1+\dfrac{2}{p^2}\right) & \text{otherwise.}\end{cases}$$

Then

$$\sum_{s\neq 0}|\chi(s)+1|<\kappa_q(q-1).$$

Proof. Using Lemma 3.3 and setting $x=\pi/(2p)$, we obtain

$$\sum_{s\neq 0}|\chi(s)+1|=2\Big(\frac{q}{p}\operatorname{cosec}x-1\Big)<2\Big(\frac{q}{p(x-x^3/6)}\Big)-1<\frac{4}{\pi}(q-1),$$

provided

$$\frac{q}{p^2} < \frac{12}{\pi}\left(1 - \frac{2}{\pi}\right)\left(1 - \frac{x^2}{6}\right).$$

Because $x = \pi/(2p) \le \pi/6$, the right side of this inequality exceeds 1.3, and so the inequality holds whenever $q = p$ or p^2. The adjustment shown suffices for general values of q.

LEMMA 3.5. *For any $\alpha \in \mathbb{F}_{q^n}^*$ and multiplicative character ψ,*

$$K_n(1, \alpha; \psi) = \psi(\alpha) K_n(1, \alpha; \overline{\psi}).$$

Proof. Replace ξ by α/ξ in the definition of $K_n(1, \alpha; \psi)$.

The climax of the preceding few lemmas comes next. In it, for a character ψ, set

$$S(\psi) := \sum_{t \neq 0} \overline{K}_1(1, t; \widehat{\psi}) K_n(1, t; \psi).$$

LEMMA 3.6. *Let q be an odd prime power and n an odd integer. Suppose that $a, b \in \mathbb{F}_q^*$ and d is an even divisor of $2m$. If $\lambda_2(ab) = -1$, then $S(\psi_d) + S(\overline{\psi}_d) = 0$, whereas if $\lambda_2(ab) = 1$, then*

$$|S(\psi_d) + S(\overline{\psi}_d)| < 2\kappa_q (q-1) q^{(n+1)/2},$$

where κ_q is as defined in Lemma 3.4; in particular, $\kappa_q = 4/\pi$ whenever $q = p$ or p^2.

Proof. By Lemma 3.5, and the fact that $\widehat{\psi}_d = \lambda_2$,

$$S(\psi_d) + S(\overline{\psi}_d) = \sum_{t \neq 0} (1 + \lambda_2(t)) K_1(1, tab; \lambda_2) K_n(1, t; \psi_d).$$

If $\lambda_2(ab) = -1$, then either $\lambda_2(t) = -1$ or $\lambda_2(tab) = -1$ whenever $t \in \mathbb{F}_q^*$. Hence, the above expression is zero by Lemma 2.7. If $\lambda_2(ab) = 1$, with $c^2 = ab$ ($c \in \mathbb{F}_q^*$), then, again by Lemma 2.7,

$$\begin{aligned} |S(\psi_d) + S(\overline{\psi}_d)| &= 2|G_1(\lambda_2)| \Big| \sum_{s \neq 0} \chi(2cs) K_n(1, s^2; \psi_d) \Big| \\ &= \sqrt{q} \Big| \sum_{s \neq 0} (\chi(2cs) + \chi(-2cs)) K_n(1, s^2; \psi_d) \Big| \\ &\le 2q^{(n+1)/2} \sum_{s \neq 0} |\chi(2cs) + \chi(-2cs)|, \end{aligned}$$

by Lemma 2.2. The result follows from Lemma 3.4, since

$$\sum_{s \neq 0} |\chi(2cs) + \chi(-2cs)| = \sum_{s \neq 0} |\chi(s/2) + \chi(-s/2)| = \sum_{s \neq 0} |\chi(s) + 1|.$$

Lemma 3.5 can be exploited for other characters χ, but not with such generality. The consequences tend to depend on the order of ab more specifically.

The remaining inequality is of a different nature and derives from a sieving process. The aim is to obtain a lower bound for $N_{q,n}(M)$ that may not be good asymptotically (as $q \to \infty$) but is especially effective for small values of q.

As noted in Section 2, given q, n, a, b, the value of $N(M)$ (M is a divisor of $q^n - 1$) depends only on the distinct prime factors of M. Accordingly, divisors $M_1, \ldots, M_r$ ($r \geq 1$) of M will be called *complementary divisors of M with common divisor M_0* if the set of distinct prime divisors of $\operatorname{lcm}\{M_1, \ldots, M_r\}$ is the same as that of M, and, for any pair (i, j) with $1 \leq i \neq j \leq r$, the set of distinct prime divisors of $\gcd(M_i, M_j)$ is that of M_0. When $r = 1$, we have $M_1 = M_0 = M$. Though easy to prove (see [ChCo], Proposition 6.1), the following inequality is extremely useful.

Proposition 3.7. *Let q be a prime power and n (≥ 1) an integer. Suppose that $a, b \in \mathbb{F}_q$. Let $M_1, \ldots, M_r$ be complementary divisors of M (itself a divisor of $q^n - 1$) with common divisor M_0. Then, with $N(M) = N_{q,n}(M; a, b)$, etc., we have*

$$N(M) \geq \Big\{ \sum_{i=1}^{r} N(M_i) \Big\} - (r-1) N(M_0).$$

Proposition 3.7 motivates a generalisation of the ratio $\Theta(M)$ defined in Section 2. With the same notation, define

$$\Theta(M_1, \ldots, M_r) := \Big\{ \sum_{i=1}^{r} \Theta(M_i) \Big\} - (r-1) \Theta(M_0).$$

This number represents the coefficient of q^n on the right hand side of the inequality when Theorems 2.9 or 2.10 are applied to each of the constituents. To be useful, therefore, it is vital that $\Theta(M_1, \ldots, M_r)$ be positive. Indeed, preferably the ratio $\widehat{\Theta}(M_1, \ldots, M_r) := \Theta(M_1, \ldots, M_r)/\Theta(M_0)$ should not be too small. For this reason, when q is odd we suppose (except in one place) that M_0 is even, because of the effect of the prime 2 otherwise. Consequently, we say that the complementary divisors are *regular* if qM_0 is even.

4. Criteria for success. These criteria are effective only if $n \geq 4$, which we assume from now on. Again, assume also that the prime power q and a $(\neq 0), b \in \mathbb{F}_q$ are given. Also, from now on, fix M as $q^n - 1$; $M_1, \ldots, M_r$ will be regular complementary divisors of M with common divisor M_0. We supplement the previously defined integer $m = (q^n - 1)/(q - 1)$ with the definitions $m_i := \gcd(M_i, m)$, $i = 0, 1, \ldots, r$. For any positive integer h, let

$W(h) = 2^{\omega(h)}$ be the number of square-free divisors of h (where $\omega(h)$ is the number of distinct prime factors of h).

We derive criteria for $N_{q,n}(M; a, b)$ to be positive. First, we suppose $b \neq 0$.

PROPOSITION 4.1. *Let q be a prime power and n (≥ 4) be an integer. Suppose that $a, b \in \mathbb{F}_q$. Let $M_1, \ldots, M_r$ be regular complementary divisors of M with common divisor M_0. Assume that $\Theta := \Theta(M_1, \ldots, M_r)$ is positive. If the following condition* (*labelled $A_{q,n}(M_1, \ldots, M_r)$*) *is satisfied*, *then $N_{q,n}(M; a, b)$ is positive*:

$$\begin{aligned} (4.1)\quad & q^{(n-3)/2} \\ & > 2\Big\{W(M_0) - W(m_0) + \delta_q^*\Big(1 - \frac{1}{q}\Big)(W(m_0) - \eta_1) + \frac{1}{q^{3/2}}(W(m_0) - 1)\Big\} \\ & \quad + \eta_1 \frac{3}{2\sqrt{q}} - \eta_2\Big[\Big(2 - \kappa_q\Big(1 - \frac{1}{q}\Big)\Big)(W(m_0) - 1) + 1\Big] \\ & \quad + \Theta^{-1} \sum_{i=1}^{r} \Theta(M_i) \Big\{ 2\Big[W(M_i) - W(M_0) - W(m_i) + W(m_0) \\ & \quad + \Big(\delta_q^*\Big(1 - \frac{1}{q}\Big) + \frac{1}{q^{3/2}}\Big)(W(m_i) - W(m_0))\Big] \\ & \quad - \eta_2\Big[\Big(2 - \kappa_q\Big(1 - \frac{1}{q}\Big)\Big)(W(m_i) - W(m_0))\Big]\Big\}, \end{aligned}$$

where κ_q $(\sim 4/\pi)$ and δ_q^* (< 1) are as in Section 3, *and*

$$\eta_1 = \begin{cases} 1 & \text{if } q \text{ is odd and } n \text{ is even}, \\ 0 & \text{otherwise}; \end{cases} \qquad \eta_2 = \begin{cases} 1 & \text{if } q \text{ and } n \text{ are odd}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Proposition 3.7 and Theorem 2.9,

$$\begin{aligned} (4.2)\quad N(M) = \Theta N(M_0) + \sum_{i=1}^{r} \Theta(M_i) \Big\{ & \int_{\substack{d \mid M_i \\ d \nmid M_0}} \sum_{t \neq 0} \overline{K}_1 K_n - 2 \int_{\substack{d \mid m_i \\ d \nmid m_0}} G_n \\ & + \int_{\substack{d \mid M_i \\ d \nmid M_0}} (\widehat{\psi}_d(a) + \widehat{\psi}_d(b)) \overline{G}_1 G_n \Big\}, \end{aligned}$$

where we have employed an abbreviated notation based on (2.4). Further, $N(M_0)$ itself is given by (2.4) with $M = M_0$, $M^* = m_0$. In particular, since the complementary divisors are regular, all contributions relating to ψ_2 are counted within $N(M_0)$. Now, for each of the $\phi(d)$ characters ψ_d, we have an absolute bound of $2q^{(n+3)/2}$ for $\sum_{t \neq 0} \overline{K}_1 K_n + (\widehat{\psi}_d(a) + \widehat{\psi}_d(b)) \overline{G}_1 G_n$

in (4.2), by Corollary 3.2 and Lemma 2.4(iii). Indeed, for those d that are divisors of m_i, but not m_0 (so that $\widehat{\psi}_d$ is trivial), we have the improvement that the factor 2 may be replaced by $2(1-q^{-1})\delta_q^*$, and we have a further contribution (bounded absolutely by $2q^{n/2}$) from the minor term $-2\int_{d|m_i,\, d\nmid m_0} G_n$.

More significantly, when q and n are odd (so that $\eta_2 = 1$) and d is an even divisor of $2m_i$, we can, on average (when ψ_d is paired with $\overline{\psi}_d$), replace the factor 2 by $\kappa_q(1-q^{-1})$, by Lemma 3.6. Because each d in $\int_{d|M_i,\, d\nmid M_0}$, say, appears with a weighting factor $\mu(d)/\phi(d)$ (so that only square-free d matter, and each carries an absolute weight $1/\phi(d)$), and because the main term in $\Theta N(M_0)$ is Θq^n, we deduce that (4.1) is correct insofar as the terms under the sum $\sum_{i=1}^r$ are concerned.

The estimate for the remaining terms of $N(M_0)$ is similar. The only modifications are as follows. There is no contribution from $d = 1$ to $-2\int_{d|M_0,\, d\nmid 2} G_n$. Also, when q is odd, then M_0 is even and we need to adjust the terms with ψ_2 using the expression for Δ_2 in Theorem 2.9. Thus, if n (and so m_0) are even, then $\eta_1 = 1$ and $|\Delta_2| < \frac{3}{2}q^{n/2+1}$, whereas, if n (and so m_0) are odd, the contribution in the worst case (when $ab = n^2$) is halved to $q^{(n+1)/2}$. This completes the proof.

When $b = 0$, we analogously employ Theorem 2.10.

Proposition 4.2. *Let q be a prime power and n (≥ 4) an integer. Suppose that $a \in \mathbb{F}_q^*$. Let $M_1, \ldots, M_r$ be regular complementary divisors of M with common divisor M_0. Assume that Θ is positive. If the following condition* (*labelled $B_{q,n}(M_1, \ldots, M_r)$*) *is satisfied, then $N_{q,n}(M; a, 0)$ is positive*:

$$\begin{aligned}(4.3)\quad & q^{(n-3)/2} - \frac{q-1}{q^{(n+3)/2}} \\ & > \left(2 - \frac{1}{q}\right)(W(M_0) - W(m_0) - \eta_2) + (-1)^{(n-1)(q-1)/4}\lambda_2(a)\varepsilon_2 \\ & \quad + \frac{1}{\sqrt{q}}\left\{(W(m_0) - 1 - \eta_1) + \left(1 - \frac{1}{q}\right)\delta_{q,n} + (-1)^{n(q-1)/4}\varepsilon_1\right\} \\ & \quad + \Theta^{-1}\sum_{i=1}^{r}\Theta(M_i)\left\{\left(2 - \frac{1}{q}\right)(W(M_i) - W(M_0) - W(m_i) + W(m_0)) \right. \\ & \quad \left. + \frac{1}{\sqrt{q}}\left(3 - \frac{4}{q}\right)(W(m_i) - W(m_0))\right\}\end{aligned}$$

where η_1 and η_2 are as in Proposition 4.1, *$\delta_{q,n}$* (*with absolute value at most* 2) *is as defined in Section* 2, *and ε_1 and ε_2 are zero*, *unless q is odd and*

$p \mid n$, *in which case*,

$$\varepsilon_1 = \begin{cases} 1 & \text{if } n \text{ is even}, \\ 0 & \text{otherwise}; \end{cases} \qquad \varepsilon_2 = \begin{cases} 1 & \text{if } n \text{ is odd}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This is similar to Proposition 4.1. But note the extra (minor) term on the left hand side of (4.3) springing from terms of the shape $-\Theta(M_i)(q-1)$ on the right side of (2.6). Further, for d a divisor of M_i (say), but neither of m_i nor M_0, the contribution from $\widehat{\psi}_d(a)\overline{G}_1(G_n+\sum_{t\neq 0} K_n)$ is $(1+2(q-1))q^{(n+1)/2} = (2-q^{-1})q^{(n+3)/2}$, and, for d a divisor of m_i, but not m_0, that of $(q-2)G_n - \sum_{t\neq 0} K_n$ is $((q-2)+2(q-1))q^{n/2} = (3-4/q)q^{n/2+1}$. In this way, the result is proved.

We shall sometimes abbreviate $A_{q,n}(M_1,\ldots,M_r)$, say, to $A_{q,n}$. We also use $R_{q,n}(M_1,\ldots,M_r)$ (possibly abbreviated) and $L_{q,n}$ to denote the right and left sides of (4.1) or (4.3) as appropriate to the context. Note that, even for $B_{q,n}$, $L_{q,n}$ is essentially $q^{(n-3)/2}$ as the other term is generally negligible. Although these conditions seem complicated, for larger values of q and n, it suffices to use the coarser estimate obtained by selecting only the terms involving $M_0, M_1, \ldots, M_r$. Note finally that, because the terms in respect of divisors of m are generally diminished in $B_{q,n}$ by a factor of order $\sqrt{q}$, the condition $A_{q,n}$ is essentially more stringent than $B_{q,n}$ and therefore, as a rule, $B_{q,n}$ holds whenever $A_{q,n}$ does.

5. Theorem 1.1 for "almost all" pairs (q,n).

In this section we shall take $r = 1$ and show that $A_{q,n}(M)$ and $B_{q,n}(M)$ hold for all but finitely many pairs (q,n). Nevertheless, in interpreting this conclusion, caution must be exercised because the number of potential exceptions is huge. Hence, properly understood, this is merely the first stage in the application of the theory. Note that, in $A_{q,n}(M)$, say, all the "Θ-terms" are absent.

We begin with a weak, but convenient, lemma to bound the function W. Note that $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13 = 30030$.

Lemma 5.1. *Set* $\gamma := 64/30030^{1/4} < 4.9$. *Suppose that* h *is an integer indivisible by a prime* p. *Then*

$$W(h) \le \gamma_p h^{1/4}, \quad \text{where} \quad \gamma_p = \begin{cases} \frac{1}{2}p^{1/4}\gamma & \text{if } p < 16, \\ \gamma & \text{if } p > 16. \end{cases}$$

In particular, $\gamma_2 < 2.9$, $\gamma_3 < 3.2$, $\gamma_5 < 3.7$.

Proof. Granted that W is multiplicative, the proof is easy.

Now, we resume the assumption that q, n, a, b are given as in Section 4 with $M = q^n - 1$, etc. We shall denote $\omega(M)$ by $\omega_{q,n}$. From now on we shall also suppose $n \ge 5$, as in Theorem 1.1.

LEMMA 5.2. *Let q be a prime power and $n \geq 5$. Suppose that $A_{q,n}(M)$ does not hold. Then $n \leq 9$ and $q < 2^{2(\omega+1)/(n-3)}$, where $\omega = \omega_{q,n}$. Moreover, if n has the specified value, then*

$$\omega_{q,5} \leq 17, \quad \omega_{q,6} \leq 17, \quad \omega_{q,7} \leq 6, \quad \omega_{q,8} \leq 11, \quad \omega_{q,9} \leq 7.$$

Further, identical conclusions hold in respect of the condition $B_{q,n}(M)$.

Proof. For both $A_{q,n}$ and $B_{q,n}$, for most of the proof it suffices to use the rough bounds

$$R_{q,n}(M) < 2\left(W(M) - \frac{1}{q}\right), \qquad L_{q,n} > q^{(n-3)/2} - \frac{1}{q^4}.$$

It follows that, if the relevant condition fails, then

$$q^{(n-3)/2} < 2W(M). \tag{5.1}$$

From Lemma 5.1, (5.1) implies that

$$q^{(n-6)/4} < 2\gamma_p < 9.8. \tag{5.2}$$

Suppose $n \geq 10$. It follows from (5.2) that $q \leq 9$. Indeed, substituting bounds for γ_3, γ_2, we deduce that $q \leq 7$. Moreover, $n = 10$ if $q = 7$ or 5 (using γ_5); $n \leq 11$ if $q = 4$; $n \leq 12$ if $q = 3$; $n \leq 16$ if $q = 2$. But $\omega_{2,11} = 2$ and $\omega_{2,n} \leq 4$ for $13 \leq n \leq 16$; consequently, by (5.1), if $q = 2$, then $n = 10$ or 12. For $q = 3$, $\omega_{3,10} = \omega_{3,11} = 3$, $\omega_{3,12} = 5$; hence (5.1) is false in each case. Further, for $q = 4, 5$ or 7, $\omega_{q,n} \leq 5$ in the relevant cases (with $n = 10$ or 11). Hence, again (5.1) cannot hold. This leaves only the aforementioned possibilities, that $q = 2$ and $n = 10$ or 12.

Now, for $A_{2,n}(M)$, we have

$$R_{2,n} = \delta_2^* W(M) + \frac{1}{\sqrt{2}}(W(M) - 1) = \sqrt{2}W(M) - \frac{1}{\sqrt{2}}$$

since, trivially, $\delta_2^* = 1/\sqrt{2}$. Since $\omega_{2,10} = 3$, $\omega_{2,12} = 5$, we deduce that

$$R_{2,10} = 2^{7/2} - 1/\sqrt{2} < L_{2,10} = 2^{7/2},$$
$$R_{2,12} = 2^{9/2} - 1/\sqrt{2} < L_{2,12} = 2^{9/2}.$$

Hence, $A_{2,n}(M)$ holds in both cases.

Similarly, for $B_{2,n}(M)$, we have

$$R_{2,n} = \frac{1}{\sqrt{2}}\left[W(M) - 1 + \frac{\delta_{2,n}}{2}\right] < \frac{W(M)}{\sqrt{2}}$$

and it is evident that $B_{2,n}(M)$ holds for $n = 10, 12$.

Accordingly, we may assume that $\omega \leq 9$ and (5.1) holds. In particular, $q < 2^{2(\omega+1)/(n-3)}$. We establish the displayed bounds for ω in the most delicate case, namely, when $n = 5$, so that (5.1) has the form

$$q < 2W(M).$$

In this proof, let $r = \omega(q-1)$, $s = \omega(m)$. Now, primes that are candidates for the divisors of m must lie in the set $\mathcal{S}_5 = \{5, 11, 31, 41, \ldots\}$ whose members (other than 5) are congruent to $1 \pmod{10}$. Moreover, $5 \mid m$ if and only if $5 \mid q-1$; indeed $\gcd(m, q-1) = 1$ or 5. Hence,

$$q < 2W(M) = \begin{cases} 2^{r+s} & \text{if } q \equiv 1 \pmod{5}, \\ 2^{r+s+1} & \text{if } q \not\equiv 1 \pmod{5}. \end{cases} \tag{5.3}$$

On the other hand, any prime (other than p) is a potential factor of $q-1$. We use P_r for the product of the smallest r primes, possibly excluding some that cannot be factors of $q-1$, as specified by context. Similarly, let P_s^* be the product of the smallest (relevant) s primes in $\mathcal{S}_5$, and set $Q_s = (P_s^*)^{1/4} - 1$. Then, evidently, $(q+1)^4 > m \geq P_s^*$, and hence

$$\max(P_r, Q_s) < q < 2W(M),$$

where the latter is given in (5.3).

Suppose $\omega_{q,5} \geq 18$. A pivotal case occurs when $r = 7$, $s = 12$. By (5.3), we have

- $8.8 \cdot 10^5 < P_7 < q < 2^{19} < 5.3 \cdot 10^5$ if $q \equiv 1 \pmod{5}$, $q \not\equiv 1 \pmod{55}$,
- $5.4 \cdot 10^5 < Q_{12} < q < 5.3 \cdot 10^5$ if $q \equiv 1 \pmod{55}$,
- $1.9 \cdot 10^6 < P_7 < q < 2^{20} < 1.1 \cdot 10^6$ if $q \not\equiv 1 \pmod{5}$,

a contradiction in each case. A similar argument rules out the possibilities that $r = 6$, $s = 13$, $q \equiv 1 \pmod{5}$, and $r = 7$, $s = 11$, $q \not\equiv 1 \pmod{5}$. More generally, we distinguish two cases.

Case (i): $s \leq 3(r+1)/2$. First, suppose $q \equiv 1 \pmod{5}$ so that $r + s = \omega + 1 \geq 19$. Having excluded $(r, s) = (7, 12)$, we deduce that $r \geq 8$. By assumption, $2^{r+s} \leq 2^{(5r+3)/2}$, and we obtain

$$3.2 < P_8/2^{43/2} \leq P_r/2^{(5r+3)/2} \leq q/2^{r+s} < 1,$$

a contradiction. For justification, note that $P_r/2^{(5r+3)/2}$ is increasing for $r \geq 8$, since the new prime factor of P_{r+1}, not a factor of P_r, exceeds $2^{5/2} = 4\sqrt{2}$.

Now, suppose $q \not\equiv 1 \pmod{5}$, so that $r + s = \omega \geq 18$. Similarly, we can suppose $r \geq 8$, and derive a contradiction, namely

$$7 < P_8/2^{45/2} \leq P_r/2^{5(r+1)/2} \leq q/2^{r+s+1} < 1.$$

Case (ii): $s > 3(r+1)/2$. Again, first suppose $q \equiv 1 \pmod{5}$. Then $s \geq 13$. From the preliminary step, $s = 13$ implies $r = 7$, whence $q < 2^{20} < 1.05 \cdot 10^6$. If $q \equiv 1 \pmod{11}$, then $11 \nmid m$ and $Q_{13} > 2.1 \cdot 10^6$, a contradiction. Hence, $q \not\equiv 1 \pmod{11}$ and $q \geq P_7 + 1 = 881791$, which, in fact, is not a prime power. Indeed, the next admissible candidate for P_7 is 1067430; since this exceeds q (from the above), this is a contradiction. We conclude that $s \geq 14$.

If $s = 14$, then $r = 7$ or 8. In these cases,

$$1.86 < Q_{14}/2^{21}, \qquad 2.3 < P_8/2^{22},$$

respectively, yield contradictions. Similarly, if $s = 15$, then $r \le 8$, and we obtain the contradiction

$$1.89 < Q_{15}/2^{23} < q/2^{r+s} < 1.$$

For $s \ge 16$, we similarly use

$$1.2 < Q_{16}/2^{77/3} \le Q_5/2^{(55-3)/3} < q/2^{r+s} < 1.$$

When $q \not\equiv 1 \pmod 5$, the corresponding work is easier. Granted the preliminary step, we may suppose $s \ge 13$. If $s = 13$, then $r \le 7$, and

$$1.2 < Q_{13}/2^{21} < q/2^{r+s+1} < 1;$$

if $s \ge 14$, then

$$1.005 < Q_{14}/2^{70/3} < Q_s/2^{55/3} < q/2^{r+s+1} < 1,$$

a contradiction in every case.

Summarising, we have shown that $\omega_{q,5} \le 17$ as claimed. For $6 \le n \le 9$, similar (but simpler) reasoning leads to the displayed bounds for $\omega_{q,n}$. When $n = 7$, we can exploit the fact that all prime factors of m lie in the set $\mathcal{S}_7 = \{7, 29, 43, 71, \ldots\}$ whose members (> 7) are all congruent to $1 \pmod{14}$. In the other cases, the bounds were obtained without making special allowance for the form of prime factors of m.

6. More complementary divisors. From Section 5, towards the goal of Theorem 1.1, we may suppose $5 \le n \le 9$ and $q < 2^{2(\omega+1)/(n-3)}$, with $\omega = \omega_{q,n}$ bounded as indicated in Lemma 5.2. In this section we (almost) complete the proof by describing other choices of complementary divisors such that $A_{q,n}(M_1, \ldots, M_r)$ and $B_{q,n}(M_1, \ldots, M_r)$ are satisfied. The method fails only for a tiny set of prime powers q, with $q \le 16$, $n = 5$, $q \le 11$, $n = 6$, or $q = 2$, $n = 8$. Within the framework of the above parameters, we deal with larger values of ω and q in sizeable batches, based on convenient weaker forms of Propositions 4.1 and 4.2.

A key principle that will operate is the following. Let $M_1^*, \ldots, M_r^*$ be obtained by replacing each prime in M by one that is smaller (or the same). Then $A_{q,n}(M_1, \ldots, M_r)$ holds whenever $A_{q,n}(M_1^*, \ldots, M_r^*)$ does (as a formal inequality). This is obvious, as can be seen by replacing the primes one at a time: its merit is that large numbers of individual cases can be dealt with simultaneously. In particular, the value of $\widehat{\Theta} = \Theta/\Theta(M_0)$, where $\Theta = \Theta(M_1, \ldots, M_r)$, is especially influential, and replacement by $\widehat{\Theta}^* = \Theta^*/\Theta(M_0^*)$, where $\Theta^* = \Theta(M_1^*, \ldots, M_r^*)$ is a significant component of this broad approach. For smaller values of ω and q, we make specific application of Propositions 4.1 and 4.2, taking advantage of the more delicate refinements these offer.

We reduce the length of the proof (perhaps, by one half) by illustrating some of the procedures, but always in the most unfavourable cases, so that their wider validity will be apparent. As it turns out, we focus on degrees $n = 5$ or 6, which are of comparable difficulty, because the advantage of the extra factor $\sqrt{q}$ in $L_{q,6}$ is offset by the restricted candidate set $\mathcal{S}_5$ for prime factors of m when $n = 5$ (as in Lemma 5.2). From this working, it becomes apparent that it is unnecessary to consider the cases $n \geq 7$ in full detail.

First, we suppose $n = 5$.

LEMMA 6.1. *Let q be a prime power and $n = 5$.*

(A) *There are regular complementary divisors $M_1, \ldots, M_r$ of M such that $A_{q,5}(M_1, \ldots, M_r)$ is valid, except when $q \leq 8$ or $q = 16$.*

(B) *There are complementary divisors such that $B_{q,5}(M_1, \ldots, M_r)$ holds, except when $q = 4, 5$ or 7.*

Proof. We suppress subscripts relating to the degree $n = 5$. When q is odd, we shall have $M_0 = 2$; when q is even, $M_0 = 1$. By Lemma 5.2, we can assume $\omega \leq 17$.

(A) We break the argument into a series of stages.

I: *q odd*, $11 \leq \omega \leq 17$. Note that, in Proposition 4.1, $\eta_1 = 0$, $\eta_2 = 1$. We select complementary divisors M_1, M_2 $(r = 2)$ with $M_0 = 2$ (and $m_0 = 1$). Observe that, here, the portion of R_q involving M_0, m_0, but not Θ, is

$$1 + 2\delta_q^*(1 - 1/q) < 3.$$

To illustrate, suppose $\omega = 11$ and $q \equiv 1 \pmod 5$, so that $q < 2^{12} = 4096$ and $\omega(q-1) \leq 5$. The more difficult case is when $q \not\equiv 1 \pmod{11}$ (so that 11 may be a factor of m). Assume first that $\omega(q-1) = 5$ so that $q > 2\cdot 3\cdot 5\cdot 7\cdot 13 = 2730$. Take $M_1 = 2p_1 \ldots p_5$, $M_2 = 2p_6 \ldots p_{10}$, where $p_1, \ldots, p_4$ are the odd primes in $q - 1$ (including 5) and $p_5, \ldots, p_{10}$ are the primes (> 5) dividing m (in increasing order). Replace $p_1, \ldots, p_{10}$ by the members of $S = \{3, 5, 7, 13, 11, 31, 41, 61, 71, 101\}$ (in order) to yield M_1^*, M_2^*, with $m_1^* = 5 \cdot 11$, $m_2^* = \frac{1}{2}M_2^*$. Moreover, $\widehat{\Theta}(M_1^*) = \Theta(M_1^*)/\Theta(M_0) = 2\Theta(M_1^*) = 0.3836\ldots$, $\widehat{\Theta}(M_2^*) = 0.9065\ldots$, and $\widehat{\Theta} \geq \widehat{\Theta}^* > 0.2901$. Using the trivial bound $\delta_q^*(1 - 1/q) + 1/q^{3/2} < 1$, we have

$$\begin{aligned} R_q(M_1, M_2) &\leq R_q(M_1^*, M_2^*) \\ &< 3 + \frac{\widehat{\Theta}(M_1^*)(59 \cdot 2 + 3\kappa_q) + (\widehat{\Theta}(M_2^*) \cdot 31)(2 + \kappa_q)}{0.2901} \\ &< 481 < q = L_q, \end{aligned}$$

since $q > 2730$. Here we have substituted $\kappa_q = 4/\pi$. The adjustment when $q \neq p$ or p^2 (p small) is offset by the exclusion of p as a possible factor of M_i, $i = 1, 2$.

Still with $q \equiv 1 \pmod 5$ but $q \equiv 1 \pmod{11}$, next suppose $\omega(q-1) = 4$, so that $\omega(m) = 8$ and, as in the proof of Lemma 5.2, $q > (5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 71 \cdot 101 \cdot 131)^{1/4} - 1 > 1413$. Proceed as before, except that p_1, p_2, p_3 are the odd primes in $q-1$, and $p_4, \ldots, p_{10}$ the primes (> 5) in m (in order). The replacement set S becomes $\{3, 5, 7, 11, 31, 41, 61, 71, 101, 131\}$. Further, $m_1^* = 5 \cdot 11 \cdot 31$, $m_2^* = \frac{1}{2} M_2^*$, and $\widehat{\Theta}(M_1^*) = 0.4021\ldots$, $\Theta(M_2^*) = 0.9295\ldots$, and $\widehat{\Theta}^* > 0.3317$. Then

$$\begin{aligned} R_q(M_1, M_2) &< 3 + \frac{\widehat{\Theta}(M_1^*)(55 \cdot 2 + 7\kappa_q) + (\widehat{\Theta}(M_2^*) \cdot 31)(2 + \kappa_q)}{0.3317} \\ &< 449 < q. \end{aligned}$$

Thus $A_q(M_1, M_2)$ holds in the above cases. When $q \equiv 1 \pmod{55}$, with $\omega(q-1) = 5$, then $q > 2310$ and the argument proceeds as in the last case, with the same S and $\widehat{\Theta}^*$, and only the slight change that $m_1^* = 5 \cdot 31$. In all other cases with $\omega = 11$, similar arguments, with more comfortable margins, succeed.

II: *q even*, $10 \le \omega \le 17$. Since $q < 2^{\omega+1}$, we have $q \le 2^{17}$ and these powers of 2 could be tackled individually. But a general argument, independent of the actual factorisation of M, works. To illustrate take $\omega = 10$ so that $q \le 1024 < 3 \cdot 5 \cdot 7 \cdot 11$ and hence $\omega(q-1) \le 3$. As in I, if $q \equiv 1 \pmod 5$, then $q > 1413$. Thus, $q \not\equiv 1 \pmod 5$, and $q > (11 \cdot 31 \cdot \ldots \cdot 131)^{1/4} - 1 > 945$. Necessarily, also, $\omega(q-1) = 3$. Set $M_1 = p_1 \ldots p_5$, $M_2 = p_6 \ldots p_{10}$, where p_1, p_2, p_3 divide $q-1$, and $p_4, \ldots, p_{10}$ divide m. The replacement set S may be taken to be $\{3, 7, 13, 11, 31, \ldots, 131\}$, yielding $\Theta(M_1^*) = 0.4640\ldots$, $\Theta(M_2^*) = 0.9295\ldots$, and $\Theta^* > 0.3936$. Since the Θ-free part of R_q is now $2\delta_q^*(1 - 1/q) < 2$, we derive

$$R_q(M_1, M_2) < 2 + \frac{2 \cdot 31\Theta(M_1^*) + \Theta(M_2^*)}{0.3936} < 222 < q.$$

III: *q odd*, $6 \le \omega \le 10$. We have $q < 2048$, $\omega(q-1) \le 4$. First suppose $\omega \ge 7$. By actually factorising numbers of the form $M = q^5 - 1$, with q a prime power ≤ 223, we see that $q \ge 223$. Take $r = \omega - 1$ and complementary divisors $M_i = 2p_i$, $i = 1, \ldots, r$, where $p_1, \ldots, p_r$ are the odd divisors of M. Hence $m_i = p_i$ if $p_i \mid m$; otherwise, $m_i = 1$. Further, $W(M_i) = 4$, $W(m_i) = 1$ or 2, $i = 1, \ldots, r$. Clearly, $R_q(M_1, \ldots, M_r)$ is maximised under these conditions when $r = 9$ and $S = \{3, 5, 7, 11, 31, 41, 61, 71, 101\}$ (with 13 instead of 5, if $q \not\equiv 1 \pmod 5$, etc). Thus $\widehat{\Theta}^*$ exceeds 0.1358 if $q \equiv 1 \pmod 5$.

It is considerably larger (> 0.2589) if $q \not\equiv 1 \pmod 5$, or if $\omega(q-1) = 3$, etc. So, we illustrate with the most delicate case with $q \equiv 1 \pmod 5$ and $\omega(q-1) = 4$. With S as above, we deduce

$$R_q(M_1, \ldots, M_r) < 3 + \frac{1.538 \cdot 4 + 6.6121(2+\kappa_q)}{0.1358} < 208 < q.$$

In all other cases, the bound for R_q is (much) smaller, and $A_q(M_1, M_2)$ holds.

The above general discussion did not extend to cover the case $\omega = 6$, but a similar argument, specifically with $r = 6$, works. For then, $q < 128$ and $\omega(q-1) \le 3$. Furthermore, the least relevant prime power of q is 59. To illustrate, suppose $q \equiv 1 \pmod 5$ and $\omega(q-1) = 3$. Then we can take $S = \{3, 5, 11, 31, 41\}$, $\widehat{\Theta}^* > 0.3751$, and obtain

$$R_q(M_1, \ldots, M_r) < 3 + \frac{4 \cdot \frac{2}{3} + 3.6525(2+\kappa_q)}{0.3751} < 49 < q.$$

IV: *q even*, $6 \le \omega \le 9$. A general argument with $r = \omega$ and $M_1, \ldots, M_r$ the primes in M succeeds for $7 \le \omega \le 9$. For $\omega = 6$, we have $q \le 64$, with equality, in fact, precisely when $q = 64$. In this case

$$R_{64}(3, 7, 11, 31, 151, 331) < \frac{2 \cdot 5.391}{0.391} + 2 < 30 < q,$$

and A_{64} holds.

V: $q < 64$, $\omega \le 5$. We identify the relevant prime powers q for each value of ω. For $\omega = 5$, $q \in \{16, 25, 31, 37, 47\}$. Bounding R_{31} more accurately from (4.1), we have

$$\begin{aligned} R_{31}(6, 10, 22, 34702) &< 1 + \frac{60}{31}\delta_{31}^* + \frac{4 \cdot \frac{2}{3} + \left[\frac{30}{31}\left(2\delta_{31}^* + \frac{4}{\pi}\right) + \frac{2}{31^{3/2}}\right]}{0.3751} \\ &< 30.7 < q, \end{aligned}$$

using the easily calculated bound $\delta_{31}^* < 0.8503$. This yields A_{31} with little to spare. In fact, A_{37} and A_{47} hold more readily because, in these cases, $q \not\equiv 1 \pmod 5$ and $\widehat{\Theta} > 0.55$. For $q = 25$, simply using $\frac{24}{25}\delta^* < 1$, we have

$$R_{25}(6, 22, 142, 1042) < \frac{4 \cdot \frac{2}{3} + 2.894\left(2 + \frac{4}{\pi}\right)}{0.5597} + 3 < 24.7 < q.$$

On the other hand, when $q = 16$, M agrees with its minimal theoretical value of $3 \cdot 5 \cdot 11 \cdot 31 \cdot 41$ and $A_{16}(3, 5, 11, 31, 41)$ does not hold. Although, with care, A_{16} can be modified to yield a positive result when $ab \ne 1$, we have to list this case as an exception.

For $\omega = 4$, $q < 31$, we have $q \in \{19, 27\}$ and A_q holds. For,

$$R_{19}(6, 302, 1822) < \frac{4 \cdot \frac{2}{3} + 1.993\bigl(2 + \frac{4}{\pi}\bigr)}{0.6589} + 3 < 17;$$

$$R_{27}(22, 26, 9122) < \frac{4 \cdot \frac{12}{13} + 1.909(2 + \kappa_{27})}{0.8319} + 3 < 16,$$

using $\kappa_{27} = \frac{4}{\pi}\bigl(1 + \frac{2}{9}\bigr) < 1.5562$.

For $\omega \le 3$, $q < 16$, we have $q \le 8$ or $q \in \{11, 13\}$. The largest pair of these can be eliminated because

$$R_{11}(10, 6442) < \frac{4 \cdot \frac{4}{5} + 0.9997\bigl[\frac{10}{11}\bigl(2 + \frac{4}{\pi}\bigr) + \frac{2}{11^{3/2}}\bigr]}{0.7996} + 1 + \frac{20}{11} < 10.7;$$

$$R_{13}(6, 61882) < \frac{4 \cdot \frac{2}{3} + \bigl(2 + \frac{4}{\pi}\bigr)}{0.666} + 3 < 12.$$

Prime powers $q \le 8$ are listed as exceptions to (A).

(B) If the bound $\delta_q^*(1 - 1/q) + 1/q^{3/2}$ is used in (4.1) (as it was through most of the working in (A)), then the coefficient of $\Theta(M_i)$ in (4.1) (relating to A_q) exceeds that in (4.3) (relating to B_q) by an amount

$$q^{-1}(W(M_i) - W(M_0) - W(m_i) + W(m_0)) + \nu(W(m_i) - W(m_0)),$$

where

$$\nu = \begin{cases} \kappa_q\left(1 - \dfrac{1}{q}\right) - \dfrac{1}{\sqrt{q}}\left(3 - \dfrac{4}{q}\right), & q \text{ odd,} \\ 2 - \dfrac{1}{\sqrt{q}}\left(3 - \dfrac{4}{q}\right), & q \text{ even,} \end{cases}$$

and this is positive (whenever $M_i \ne M_0$). Hence A_q implies B_q in virtually every case treated in (A), and it suffices to check B_q for values of q such as 31 and 11, and those listed as exceptional for A_q.

When $q = 31$, the only odd prime divisor of M, not a divisor of m, is 3 and, in (4.3), we have $\eta_1 = 1, \eta_2 = \varepsilon_1 = \varepsilon_2 = 0$ and

$$\begin{aligned} R_{31}(6, 10, 22, 34702) &< \frac{2\bigl(\frac{4}{3} + 2.71\bigr) + \frac{3}{\sqrt{31}} \cdot 2.71}{0.3751} + \frac{2}{\sqrt{31}} \\ &< 26 < L_{31} = 30.99\ldots \end{aligned}$$

Further

$$\begin{aligned}
R_{16}(3,5,11,31,41) &= \frac{\frac{4}{3}+\frac{3}{4}\cdot 3.6525}{0.319}+\frac{1}{2}<13.3,\\
R_{11}(10,6442) &< \frac{2\left(\frac{8}{3}+1\right)+\frac{3}{\sqrt{11}}}{0.7996}+\frac{2}{\sqrt{11}}<8.3,\\
R_{8}(7,31,151) &< \frac{\frac{12}{7}+\frac{3}{\sqrt{8}}\cdot 1.961}{0.818}+\frac{2}{\sqrt{8}}<5.4,
\end{aligned}$$

which is less than L_q ($> q-1/q^3$) in each case. We even obtain a positive result for $q\in\{2,3\}$. Thus,

$$R_2(31)=\frac{1}{\sqrt{2}}(1+12\delta_{2,5})<\sqrt{2}<L_2=31/16.$$

For $q=3$, we use *non-regular* complementary divisors $2,11$ and (4.3) (slightly modified), with $\eta_2=1,\varepsilon_1=\varepsilon_2=\eta_1=0$, to yield

$$R_3(2,11)<\frac{\frac{10}{11}\cdot\frac{5}{3\sqrt{3}}}{0.409}+\frac{2}{3\sqrt{3}}\delta_{3,5}<2.83<L_3=2.975\ldots$$

This completes the verification in every case not listed as exceptional.

Lemma 6.2. *Let q be a prime power and $n=6$.*

(A) *There are regular complementary divisors $M_1,\ldots,M_r$ of M such that $A_{q,6}(M_1,\ldots,M_r)$ is valid, except when $q\le 5$ or $q=11$.*

(B) *There are regular complementary divisors such that $B_{q,6}(M_1,\ldots\ldots,M_r)$ holds, except when $q=4$.*

Proof. We suppress subscripts relating to the degree $n=6$, and assume $\omega\le 17$.

(A) Note that $L_q=q^{3/2}$.

I: *q odd*, $10\le\omega\le 17$. In Proposition 4.1 we have $\eta_1=1$, $\varepsilon_1=1$ if and only if $p=3$, and $\eta_2=\varepsilon_2=0$. Of course, m is even; m is also divisible by 3 if and only if $q\equiv 1 \pmod 3$. Note also that M is divisible by 8.

Given ω, we select complementary divisors M_1,M_2, with common divisor $2l$, where l is the least odd prime factor of M. Then $m_0=2$ (unless $l=3$, when $m_0=6$). Thus, from Proposition 4.1,

$$R_q<2\Theta^{-1}\Big(\sum_{i=1}^{2}\Theta(M_i)(W(M_i)-4)\Big)+7, \tag{6.1}$$

where the final 7 may be replaced by 3 when $l=3$.

To illustrate, we treat the most delicate case, namely, $\omega=10$, $l=3$ (i.e., $q\equiv 1 \pmod 6$). Set $M_1=6p_1\ldots p_4$, $M_2=6p_5\ldots p_8$, where $p_1,\ldots,p_8$ are the odd primes (>3) dividing M (in increasing order). Thus $W(M_1)=$

$W(M_2) = 64$, and $R_q(M_1, M_2) \leq R_q(M_1^*, M_2^*)$, where M_1^*, M_2^* are obtained by replacing $p_1, \ldots, p_8$ by the smallest 8 primes exceeding 3, i.e., by $5, 7, \ldots, 29$. Moreover, $\widehat{\Theta} = \Theta/\Theta(6) = 3\Theta \geq \widehat{\Theta}^* = 3\Theta^* > 0.3988$. Hence, by (6.1),

$$R_q(M_1, M_2) < \frac{120(\widehat{\Theta}(M_1^*) + \widehat{\Theta}(M_2^*))}{0.3988} + 7 < 428.$$

On the other hand, from M, $q > (8 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot 29)^{1/6} - 1 > 53$. Thus, because q is a prime power, $q \geq 59$ and $L_q > 453 > R_q(M_1, M_2)$ (by the above). Consequently, $A_q(M_1, M_2)$ holds. For $11 \leq \omega \leq 17$, the argument is similar, but there is no need for a step analogous to the one above which allowed 53 to be replaced by 59.

II: *q even*, $10 \leq \omega \leq 17$. Take complementary divisors M_1, M_2 with common divisor l, the least (odd) prime factor of M and proceed as in I. The working is more comfortable because $W(M_i)$ is approximately halved, in general.

III: *q odd* (≥ 29), $\omega \leq 9$. Take $r = \omega - 2 \leq 7$ and $M_i = 2lp_i$, $i = 1, \ldots, r$, where l is the least odd prime divisor of M and $p_1, \ldots, p_r$ the remaining odd prime divisors (as in I). Then $M_0 = 2l$, $m_0 = 2$ (unless $l = 3$, when $m_0 = 6$). To illustrate, take $l = 3$, so that $q \equiv 1 \pmod 6$. Clearly, R_q is maximised when $r = 9$ and $p_1, \ldots, p_7$ are replaced by the primes in $[5, 23]$. Thus $\widehat{\Theta} \geq \widehat{\Theta}^* > 0.3443$ and, extending (6.1) to r complementary divisors, we obtain

$$R_q < \frac{8 \cdot 6.3443}{0.3443} + 7 < 155 < L_q = q^{3/2},$$

since $q \geq 29$, and so $q^{2/3} > 156$. Thus A_q holds.

IV: *q even* (≥ 32), $\omega \leq 9$. This is similar to III, except that $r = \omega - 1$, $M_i = lp_i, i = 1, \ldots, r$, and $M_0 = l$.

V: $q \leq 27$. We deal with the remaining powers in order of decreasing ω, taking $M_0 = 2$ or 1 according as q is odd or even. In fact, $\omega \leq 6$ for all $q \leq 27$, and, hence, by Lemma 5.2, $q < 2^{14/3} < 25.4$, i.e., $q \leq 25$.

For $\omega = 6$, there remains $q \in \{11, 16, 23, 25\}$. Indeed, we have

$$R_{25}(6, 14, 26, 62, 1202) < \frac{4 \cdot 4.413}{0.413} + 3 < 46 < L_{25} = 125;$$
$$R_{23}(6, 14, 22, 26, 158) < \frac{4 \cdot 4.344}{0.344} + 3 < 54 < L_{23} = 110.3\ldots;$$
$$R_{16}(3, 5, 7, 13, 17, 24) < \frac{2 \cdot 5.1839}{0.1839} + 2 < 59 < L_{16} = 64.$$

Unfortunately, when $q = 11$, then $M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 37$, and A_{11} appears not to hold for any choice of complementary divisors. Hence, this value is listed as an exception.

For $\omega = 5$, we can suppose $q < 2^4 = 16$. This leaves $q \in \{9, 13\}$. For $q = 9$, all prime factors of M divide m (so that $M_i = m_i$ in every case). We obtain

$$R_9(10, 14, 26, 146) < \frac{4\left(\frac{8}{9} + \frac{1}{27}\right) \cdot 3.566}{0.566} + 2.5 < 26 < L_9 = 27,$$

since $2(\delta_9^*(1 - 1/9)) + 3/(2\sqrt{9}) < 2.5$;

$$R_{13}(6, 14, 122, 314) < \frac{4 \cdot 3.501}{0.501} + 3 < 31 < L_{13} = 46.8\ldots$$

For $\omega \le 4$, we can assume $q < 2^{10/3} < 10.1$, and hence $q \le 8$. We can eliminate $q \in \{7, 8\}$. When $q = 8$, we have

$$R_8(3, 7, 19, 73) < \frac{2 \cdot 3.457}{0.457} + 2 < R_8 = 22.6\ldots$$

When $q = 7$, all prime factors of M divide m, and, using more care, we have

$$\begin{aligned} R_7(6, 38, 86) &< \frac{\left(\frac{6}{7}\delta_7^* + \frac{1}{7^{3/2}}\right) \cdot 2.5907}{0.5907} + 2\left(\frac{6}{7}\delta_7^* + \frac{1}{7^{3/2}}\right) + \frac{3}{2\sqrt{7}} \\ &< 18.4 < L_7 = 18.52\ldots, \end{aligned}$$

simply using $\delta_7^* < 1$. (In fact, $\delta_7^* < 0.902$.)

Values of q remaining are listed as exceptions. This completes the proof for A_q.

(B) Since A_q generally implies B_q, it suffices to check $q \in \{2, 3, 5, 7, 9, 11\}$, which includes all exceptions to (A), except $q = 4$.

First, we verify $B_{11}(6, 10, 14, 38, 74)$, observing that 5 is the only prime divisor of M, not a divisor of m. Thus $M_i = m_i$, except for $M_i = 10$. Thus,

$$\begin{aligned} R_{11}(6, 10, 14, 38, 74) &< \frac{\frac{21}{11} \cdot \frac{8}{5} + \frac{1}{\sqrt{11}}\left(2 \cdot \frac{29}{11} \cdot 3.445\right)}{0.2441} + \frac{20}{11}\delta_{11,5} \\ &< 35.5 < L_{11} = 36.48\ldots \end{aligned}$$

Further

$$R_9(10, 14, 26, 146) < \frac{1}{3}\left(\frac{\left(2 \cdot \frac{23}{9}\right) \cdot 3.566}{0.566} + \frac{16}{9} + 1\right) < 12 < L_9 = 26.99\ldots;$$

$$R_7(6, 38, 86) < \frac{1}{\sqrt{7}}\left(\frac{\left(2 \cdot \frac{17}{7}\right) \cdot 2.591}{0.591} + \frac{12}{7}\right) < 8.7 < L_7 = 18.51\ldots;$$

$$R_5(6, 14, 62) < \frac{1}{\sqrt{5}}\left(\frac{\left(2 \cdot \frac{11}{5}\right) \cdot 2.491}{0.491} + \frac{8}{5}\right) < 10.7 < L_5 = 11.17\ldots;$$

$$R_3(14, 26) < \frac{1}{\sqrt{3}}\left(\frac{\left(2 \cdot \frac{5}{3}\right) \cdot 1.7802}{0.7802} + \frac{4}{3} - 1\right) < 4.6 < L_3 = 5.18\ldots,$$

exploiting the fact that here the ε_1-term is negative;

$$R_2(3,7) < \frac{1}{\sqrt{2}}\left(\frac{1.5238}{0.5238}+1\right) < 2.765 < L_2 = 2.784\ldots$$

This completes the proof of the lemma.

Lemma 6.3. *Let q be a prime power and n (≥ 7) be an integer.*

(A) *There are regular complementary divisors $M_1,\ldots,M_r$ of M such that $A_{q,n}(M_1,\ldots,M_r)$ holds, except for $A_{2,8}$.*

(B) *There are regular complementary divisors such that $B_{q,n}(M_1,\ldots \ldots,M_r)$ holds.*

Proof. By Lemmas 5.2, 6.1 and 6.2, it suffices to suppose $n=7$ (with $\omega \leq 6$), $n=8$ (with $\omega \leq 11$), or $n=9$ (with $\omega \leq 7$). From the working of this section so far, plus the fact that (essentially) $L_{q,n+1}=\sqrt{q}L_{q,n}$, it is clear that only extremely small values of q (say, $q \leq 5$) could be in doubt. Moreover, when $n=7$, because the bulk of the prime factors of M divide m and so lie in $\mathcal{S}_7=\{7,29,43,71,\ldots\}$, the result easily holds in this case. The only pair (q,n) for which the result is delicate is $(2,8)$. This was an exceptional case for the corresponding condition in [ChCo] for $a=b=0$ and, again, $A_{2,8}$ fails here. But $B_{2,8}$ holds. For, then,

$$R_{2,8}(3,5,17) < \frac{1}{\sqrt{2}}\left(\frac{2.407}{0.407}+\frac{\delta_{2,8}}{2}\right) < 4.9 < L_{2,8} = 5.63\ldots$$

7. Completion of proof of Theorem 1.1.

We used MAPLE (Version 5, Release 3) to test the results for the twelve pairs (q,n) not (wholly) covered by Lemmas 6.1–6.3. Specifically, in each case, we generated $\mathbb{F}_{q^n}$ over the prime field $\mathbb{F}_p$ by means of the primitive polynomial P of $\mathbb{F}_{q^n}$ listed in [HaMu]. Using the MAPLE Galois Field package and a root α of P, a representation was obtained for each pair $(T_n(\alpha^i),T_n(1/\alpha^i)), i=1,2,3,\ldots,$ proceeding as far as was necessary for the cardinality of the set of such pairs (and their reflections) to reach q^2. This occurred within a few minutes in every case, except for the three exceptional pairs listed in Theorem 1.1, when, following a complete run, we found that the set of pairs was deficient by $(0,0)$ in each case.

References

[ChCo] W.-S. Chou and S. D. Cohen, *Primitive elements with zero traces*, Finite Fields Appl., to appear.

[Co1] S. D. Cohen, *Primitive elements with arbitrary trace*, Discrete Math. 83 (1990), 1–7.

[Co2] S. D. Cohen, *Gauss sums and a sieve for generators of Galois fields*, Publ. Math. Debrecen 56 (2000) (Kálmán Győry 60th birthday issue), to appear.

[CoHa1] S. D. Cohen and D. Hachenberger, *Primitive normal bases with prescribed trace*, Appl. Algebra Engrg. Comm. Comput. 9 (1999), 383–403.

[CoHa2] —, —, *Primitivity*, *freeness*, *norm and trace*, Discrete Math. 214 (2000), 135–144.

[Ha] W. B. Han, *The coefficients of primitive polynomials over finite fields*, Math. Comp. 65 (1996), 331–340.

[HaMu] T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields*, ibid. 59 (1992), 639–643.

[Ju] D. Jungnickel, *Finite Fields. Structures and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[JuVu] D. Jungnickel and S. A. Vanstone, *On primitive polynomials over finite fields*, J. Algebra 124 (1989), 337–353.

[LiNi] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983; 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[MoMu] I. H. Morgan and G. L. Mullen, *Primitive normal polynomials over finite fields*, Math. Comp. 63 (1994), 759–765.

[Mu] G. L. Mullen, *Bases and the distribution of irreducible and primitive polynomials over finite fields*, in: Applications of Finite Fields, Inst. Math. Appl. Conf. Ser. New Ser. 59, 1996, 1–18.

[Ni] H. Niederreiter, *An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary fields*, Appl. Algebra Engrg. Comm. Comput. 1 (1990), 119–124.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW, Scotland
E-mail: sdc@maths.gla.ac.uk

Received on 4.8.1999
and in revised form on 21.12.1999 (3668)