Glasgow Math. J. **48** (2006) 281–307. © 2006 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089506003077. Printed in the United Kingdom

PRIMITIVE POLYNOMIALS WITH PRESCRIBED SECOND COEFFICIENT

STEPHEN D. COHEN and MATEJA PREŠERN*

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

(Received 12 November, 2005; revised 20 December, 2005; accepted 12 January, 2006)

Abstract. The Hansen-Mullen Primitivity Conjecture (HMPC) (1992) asserts that, with some (mostly obvious) exceptions, there exists a primitive polynomial of degree n over any finite field with any coefficient arbitrarily prescribed. This has recently been proved whenever $n \geq 9$. It is also known to be true when $n \leq 3$. We show that there exists a primitive polynomial of any degree $n \geq 4$ over any finite field with its second coefficient (i.e., that of x^{n-2}) arbitrarily prescribed. In particular, this establishes the HMPC when $n = 4$. The lone exception is the absence of a primitive polynomial of the form $x^4 + a_1x^3 + x^2 + a_3x + 1$ over the binary field. For $n \geq 6$ we prove a stronger result, namely that the primitive polynomial may also have its constant term prescribed. This implies further cases of the HMPC. When the field has even cardinality 2-adic analysis is required for the proofs.

2000 *Mathematics Subject Classification.* 11T06, 11T30, 11T24, 11L40, 11S85.

1. Introduction. Let $\mathbb{F}_q$ be the finite field of order q, a power of its (prime) characteristic p. Its multiplicative group is cyclic of order $q-1$: a generator is called a *primitive element* of $\mathbb{F}_q$. More generally, a primitive element γ of the unique extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ of degree n is the root of a (monic) *primitive* polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n (automatically irreducible). All roots of f (conjugates $\gamma, \gamma^q, \dots, \gamma^{q^{n-1}}$ of γ) are primitive elements of $\mathbb{F}_{q^n}$. In 1992, T. Hansen and G. L. Mullen [**17**] stated a (natural) conjecture on the existence of a primitive polynomial of degree n over $\mathbb{F}_q$ with an arbitrary coefficient prescribed. (See also [**24**], [**25**] and [**15**].)

Conjecture 1.1 (Hansen and Mullen, 1992). *Let $a \in \mathbb{F}_q$ and let $n \geq 2$ be a positive integer. Fix an integer m with $0 < m < n$. Then there exists a primitive polynomial $f(x) = x^n + \sum_{j=1}^{n} a_jx^{n-j}$ of degree n over $\mathbb{F}_q$ with $a_m = a$ with (genuine) exceptions when*

$$(q, n, m, a) = (q, 2, 1, 0),\ (4, 3, 1, 0),\ (4, 3, 2, 0) \text{ or } (2, 4, 2, 1).$$

In fact, substantial progress has already been made towards a complete proof of Conjecture 1.1. We outline some of these steps. (For a fuller bibliography consult Cohen's survey of the last decade's activity, [**5**].) When $m = 1$, it was demonstrated by Cohen, [**1**]. (See [**10**] for a self-contained exposition.) For $n = m - 1$, it follows from [**2**], [**7**], [**18**]. The papers of Han [**16**] and Cohen and Mills [**9**] cover most cases with $m = 2$

* Supported by a University of Glasgow FIMS Grant.

and $n \geq 5$ (although the situation when q is even and $n = 5$ or 6 is not altogether clear). For $m = 3$, the conjecture holds provided $n \geq 7$ by **[13]**, **[14]**, **[23]** and **[8]**. It has to be said, however, that, when $m = 2$ or 3, some of these items dealt with the stronger requirement that the first m coefficients are prescribed and significant computer verification in a large (though finite) number of cases was necessary to resolve these questions, particularly when $5 \leq n \leq 7$. Next, the HMPC follows from **[3]** whenever $m \leq \frac{n}{3}$ (except that for $q = 2$ the restriction is to $m \leq \frac{n}{4}$). For *even* prime powers q and *odd* degrees n it has been shown by Fan and Han **[12]** provided $n \geq 7$. Finally, the whole conjecture has recently been established by Cohen whenever $n \geq 9$, **[4]**.

To resolve the HMPC for particular values of n and m, it is evidently more delicate when n is small and, less evidently perhaps, when m is around $\frac{n}{2}$ (see **[4]**). From the above summary, the outstanding cases all have $4 \leq n \leq 8$. In particular, the existence of a primitive quartic ($n = 4$) with the coefficient of x^2 prescribed ($m = 2$) has not been settled. For quintics and sextics ($n = 5$ or 6) the existence question when $m = 2$ has been answered affirmatively (at least when q is odd) but this required some considerable computer verification. The problem when $(n, m) = (5, 3), (6, 3)$ or $(6, 4)$ has still to be addressed.

In this paper, we show that there exists a primitive polynomial of any degree $n \geq 4$ over $\mathbb{F}_q$ with its second coefficient (i.e., that of x^{n-2}) arbitrarily prescribed. More precisely, we give a self-contained proof of the following theorem with a minimal amount of computation.

THEOREM 1.2. *Suppose $n \geq 4$. Let a be an arbitrary member of the finite field $\mathbb{F}_q$. Then, except when $q = 2$, $n = 4$ and $a = 1$, there exists a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n with second coefficient prescribed as a.*

A (difficult) case of the HMPC is an immediate consequence of Theorem 1.2.

COROLLARY 1.3. *Suppose $n = 4$. Then the HMPC holds.*

When the degree $n \geq 6$, we prove a stronger version of Theorem 1.2 wherein additionally the constant term of the primitive polynomial is appropriately prescribed as $(-1)^n c \in \mathbb{F}_q$. Here, necessarily c must be a *primitive* element of $\mathbb{F}_q$, since this is the norm of a root of the polynomial.

THEOREM 1.4. *Suppose $n \geq 6$. Let a be an arbitrary non-zero member of the finite field $\mathbb{F}_q$ and c be an arbitrary primitive element of $\mathbb{F}_q$. Then, there exists a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n with second coefficient a and constant term $(-1)^n c$.*

In view of the fact that a monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n with constant term $(-1)^n c$ is primitive if and only if the reciprocal polynomial $\frac{x^n}{(-1)^n c} \cdot f\left(\frac{1}{x}\right)$ is primitive then Theorem 1.2 (for $a = 0$) and Theorem 1.4 (for $a \neq 0$) imply further cases of the HMPC.

COROLLARY 1.5. *Suppose $n \geq 6$ and $a \in \mathbb{F}_q$. Then there exists a primitive polynomial of degree n over $\mathbb{F}_q$ with its coefficient of x^2 equal to a. In particular, the HMPC is established for $(n, m) = (6, 4), (7, 5)$ or $(8, 6)$.*

Granted Theorem 1.4, for $a \neq 0$ we need only consider $n = 4$ or 5 in Theorem 1.2. Generally, for the numerical aspects we can suppose $4 \leq n \leq 8$, though the calculations could easily be extended to larger values of the degree. (Of course, the working becomes easier as n increases).

In the proof of Theorem 1.2, we shall distinguish two cases according to when $a \neq 0$ (the *non-zero problem*) or $a = 0$ (the *zero problem*). In particular, in the non-zero problem we also treat the case when the constant term is prescribed. Furthermore, in each case, we will separately approach fields of odd and even orders. Mainly, this is because, when q is even, the criterion for prescribing the second coefficient has a different shape. Here, based on an important method introduced by Fan and Han (e.g., [**11**]), 2-adic analysis is employed. Accordingly, we shall refer to the *odd non-zero problem*, etc. In every case careful work on expressing the number of desired primitive polynomials in terms of character sum expressions is required, as well as a sieving technique. This outcome is that, except for primitive quartics over fields of *odd* order, the only primitive polynomials that have to be exhibited explicitly are over $\mathbb{F}_q$, where $q \leq 7$. For quartics over odd-order fields, where the prescribed coefficient of x^2 is non-zero, 27 fields have to be checked (the largest is $\mathbb{F}_{103}$). When the prescribed coefficient is zero, 246 polynomials have to be found: the largest field is $\mathbb{F}_{11003}$.

For Theorem 1.4 (so that $n \geq 6$), the main situation where direct checking is required is that of sextics over ten fields of odd order. The largest is $\mathbb{F}_{29}$.

In a sequel, we intend to treat the (remaining cases of the) existence question for primitive polynomials with the *third* or *fourth* coefficient prescribed.

2. Basic notation with applications. Throughout take $Q_n = \frac{q^n-1}{q-1}$ and, for any integer r, denote by $\theta(r)$ the ratio $\frac{\phi(r)}{r}$, ϕ being Euler's function.

Observe that a primitive element of $\mathbb{F}_{q^n}$ is not a d-th power in $\mathbb{F}_{q^n}$ for any divisor d of $q^n - 1$ exceeding 1. More generally, for any divisor k of $q^n - 1$, call a (non-zero) element of $\mathbb{F}_{q^n}$ *k-free* if it is not a d-th power in $\mathbb{F}_{q^n}$ for any divisor d of k exceeding 1.

Given $a \in \mathbb{F}_q$, for a divisor k of $q^n - 1$ denote by $\pi_a(k)$ the number of k-free elements of $\mathbb{F}_{q^n}$ whose characteristic polynomial over $\mathbb{F}_q$ has second coefficient a. It is required to show that $\pi_a(q^n - 1)$ is positive. In particular, in the zero problem ($a = 0$), the number is $\pi_0(q^n - 1)$. Evidently, from the definition of k-free, the value of $\pi_a(k)$ depends only on the square-free part of k, that is, the product of all distinct primes dividing k. Accordingly, we replace k by its square-free part, whenever appropriate.

LEMMA 2.1. *Suppose that an (irreducible) polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n has second coefficient* 0 *and a root $\gamma \in \mathbb{F}_{q^n}$ that is Q_n-free. Then there exists $b \in \mathbb{F}_q^*$, such that the minimal polynomial of $\gamma^* := b\gamma$ is primitive of degree n and also has second coefficient* 0.

Proof. Since γ is Q_n-free, for a fixed primitive element $\xi \in \mathbb{F}_{q^n}$, $\gamma = \xi^e$, where $\gcd(e, Q_n) = 1$. Set $b = \xi^{jQ_n}$ (automatically in $\mathbb{F}_q$) for some j to be chosen. Then, for any choice of j, $\gamma^* := b\gamma$ remains Q_n-free. Write $q - 1 = q_1q_2$, where q_1 and q_2 are co-prime with q_1 the largest factor of $q - 1$ co-prime to Q_n. Thus, for any b, $b\gamma = \gamma^*$ is already q_2-free. It is additionally q_1-free (and so primitive) if j is chosen so that $e + jQ_n \equiv 1 \pmod{q_1}$. This is always possible. The result follows. □

Consequently, from Lemma 2.1, in the zero problem in order to establish that $\pi_0(q^n - 1)$ is positive, it suffices to show that $\pi_0(Q_n)$ is positive.

For Theorem 1.4 (wherein the constant term is also prescribed), introduce E_n, defined as the product of distinct primes in $q^n - 1$ that are *not* factors of $q - 1$. In particular, E_n is an *odd* divisor of Q_n. Further, for $a\ (\neq 0) \in \mathbb{F}_q$, c primitive in $\mathbb{F}_q$ and $k | q^n - 1$, define $\pi_{a,c}(k)$ to be the number of k-free $\gamma \in \mathbb{F}_{q^n}$ whose characteristic polynomial has second coefficient a and constant term $(-1)^n c$. We want to show that when $n \geq 6$, then $\pi_{a,c}(q^n - 1)$ is positive.

LEMMA 2.2. *Suppose that $f(x) \in \mathbb{F}_q[x]$ is an irreducible polynomial of degree n with constant term $(-1)^n c$, where c is a primitive element of $\mathbb{F}_q$. Then f is primitive if and only if any root $\gamma \in \mathbb{F}_{q^n}$ is E_n-free.*

Proof. Since $\gamma^{(q^n-1)/(q-1)} = c$ is a primitive element of $\mathbb{F}_q$, then γ is guaranteed to be $(q-1)$-free. To be primitive (in $\mathbb{F}_{q^n}$) it therefore suffices if it is E_n-free. □

By Lemma 2.2, it suffices to show that $\pi_{a,c}(E_n)$ is positive.

The next items of notation relate to the characteristic function of the set of (non-zero) k-free elements of $\mathbb{F}_{q^n}$. For any $d \mid q^n - 1$, write η_d for a typical multiplicative (complex-valued) character in $\widehat{\mathbb{F}_{q^n}^*}$ of order d. Extend η_d to a function on $\mathbb{F}_{q^n}$ by setting $\eta_d(0) = 0$ (even when $d = 1$). Thus η_1 is the trivial character. We shall however write $\eta = \mathbf{1}$ for the version of the trivial character for which $\eta(0) = 1$. As in other papers, adopt an "integral" notation for weighted sums; namely, for $k \mid q^n - 1$, set

$$\int_{d|k} \eta_d := \sum_{d|k} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \eta_d,$$

where the inner sum runs over all $\phi(d)$ characters of order d. (Once again, only square-free divisors d have any influence.) Then the characteristic function for the subset of k-free elements of $\mathbb{F}_{q^n}$ is

$$\theta(k) \int_{d|k} \eta_d(\gamma), \quad \gamma \in \mathbb{F}_{q^n}, \tag{2.1}$$

with $\theta(k)$ as above.

The next batch of notation relates to the sieving technique. Given k (taken to be square-free), write $k = k_0 p_1 \cdots p_s$, $s \geq 1$, for some divisor k_0 and distinct primes $p_1, \ldots, p_s$. Then (k_0, s) is called a *decomposition* of k. To such a decomposition we associate a number

$$\delta := 1 - \sum_{i=1}^{s} \frac{1}{p_i} \tag{2.2}$$

which is of special significance. To be useful it is essential that k_0 is selected so that δ is positive: it will always be assumed that this is so.

LEMMA 2.3. *For any divisor d of $q^n - 1$, let $\pi(k)$ denote the number of k-free elements of $\mathbb{F}_{q^n}$ satisfying prescribed conditions. Suppose that (k_0, s) is a decomposition of k. Then*

$$\pi(k) \geq \left(\sum_{i=1}^{s} \pi(k_0 p_i) \right) - (s-1)\pi(k_0) \tag{2.3}$$

$$= \delta\pi(k_0) + \sum_{i=1}^{s} \left(\pi(k_0 p_i) - \left(1 - \frac{1}{p_i}\right) \pi(k_0) \right). \tag{2.4}$$

Proof. The results are trivial for $s = 1$. The basic sieving inequality (2.3) holds by induction on $s \geq 2$. When $s = 2$, $\mathcal{S}(k_0) \subseteq \mathcal{S}(k_0 p_1) \cup \mathcal{S}(k_0 p_2)$, where $\mathcal{S}(k)$ denotes the set of elements counted by $\pi(k)$.

The expression (2.4) is merely an awkward-looking numerical rearrangement of the right side of (2.3) that will subsequently be efficient in combining estimates for the various quantities. □

In brief, for a given k (such as $q^n - 1$), one starts out by estimating $\pi(k)$ directly (i.e., take $s = 1$ in the above) for sufficiently large q. For smaller values of q, genuine applications of the sieve ($s > 1$) become crucial.

For any positive integer r, denote by $W(r) = 2^{\omega(r)}$ the number of square-free divisors of r, where $\omega(r)$ is the number of distinct prime divisors of r. For a given decomposition (k_0, s) define

$$\Delta_{s,\delta} := \frac{s-1}{\delta} + 2.$$

When $s = 1$, then $\Delta_{s,\delta} = 2$ and $W(k) = 2W(k_0)$.

3. The odd problem.

First we recall a standard general fact.

LEMMA 3.1. *For a field F, let $f(x) \in F[x]$ be a separable monic irreducible polynomial in $F[x]$ with a root $\gamma \in E$, say. For $t = 1, 2$, denote by s_t the E/F-trace of γ^t. Then the second symmetric function σ_2 of the roots of f satisfies*

$$2\sigma_2 = s_1^2 - s_2. \tag{3.1}$$

Proof. Let $\deg f = n$ and $\gamma = \gamma_1, \dots, \gamma_n$ denote all the roots of f (in a splitting field). Then

$$2\sigma_2 = 2\sum_{1 \le i < j \le n} \gamma_i\gamma_j = \sum_{1 \le i,\, j \le n} \gamma_i\gamma_j = \sum_{1 \le i \le n} \gamma_i \sum_{1 \le j \le n} \gamma_j - \sum_{1 \le i \le n} \gamma_i^2,$$

and the result follows. □

As it stands Lemma 3.1 is useful only when the characteristic of F is not 2. Suppose now that q is *odd* and that $a \in \mathbb{F}_q$ is given.

COROLLARY 3.2. *For any $z \in \mathbb{F}_q$, suppose that $f(x) \in \mathbb{F}_q[x]$ is irreducible of degree n and such that $s_1 = z$ and $s_2 = z^2 - 2a$. Then f has second coefficient a.*

From Corollary 3.2 it is useful to have an expression for the characteristic function of the subset of $\mathbb{F}_{q^n}$ comprising elements with prescribed $\mathbb{F}_{q^n}/\mathbb{F}_q$ trace b: in other notation $T_n(\xi) = b$. This is:

$$\frac{1}{q}\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha(T_n(\xi) - b)) = \frac{1}{q}\sum_{\alpha \in \mathbb{F}_q} \bar{\chi}(b)\, \chi_n(\alpha(\xi)), \quad \xi \in \mathbb{F}_{q^n}.$$

Here χ is the canonical additive character on $\mathbb{F}_q$ (so that

$$\chi(b) = \exp\frac{2\pi i T_u(b)}{p},$$

where $q = p^u$) and χ_n is the canonical character on $\mathbb{F}_{q^n}$. Also $\bar{\chi}$ is the complex conjugate character to χ.

Using the characteristic functions defined already we can deduce a basic formula for $\pi_a(k)$ and, when $a \neq 0$, $\pi_{a,c}(k)$.

LEMMA 3.3. *Suppose q is odd, $a \in \mathbb{F}_q$ is given and k divides $q^n - 1$. Then*

$$q^2\pi_a(k) = \theta(k) \int_{d|k} \sum_{\alpha,\beta,z\in\mathbb{F}_q} \bar{\chi}(\alpha(z^2 - 2a) + \beta z)\, S_n(\alpha, \beta; \eta_d), \tag{3.2}$$

where $S_n(\alpha, \beta; \eta)$ denotes the character sum $\sum_{\gamma\in\mathbb{F}_{q^n}} \chi_n(\alpha\gamma^2 + \beta\gamma)\eta(\gamma)$.

More generally, suppose that (k_0, s) is a decomposition of k. Then

$$\begin{aligned} \frac{q^2\pi_a(k)}{\theta(k_0)} &= \delta \int_{d|k_0} \sum_{\alpha,\beta,z\in\mathbb{F}_q} \bar{\chi}(\alpha(z^2 - 2a) + \beta z)\, S_n(\alpha, \beta; \eta_d) \\ &\quad + \sum_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \int_{d|k_0} \sum_{\alpha,\beta,z\in\mathbb{F}_q} \bar{\chi}(\alpha(z^2 - 2a) + \beta z) S_n(\alpha, \beta; \eta_{dp_i}). \end{aligned} \tag{3.3}$$

In particular, the contribution to the right side of (3.3) *attributable to values of $\alpha = \beta = 0$ (the "main term") is $\delta q(q^n - 1)$.*

Proof. For (3.3) use the equivalence of the right sides of (2.3) and (2.4).

For the main term, observe that $S_n(0, 0; \eta_d)$ is zero unless $d = 1$ when the value is $q^n - 1$. Then summing over $z \in \mathbb{F}_q$ we obtain the "main term" in (3.3).

Of course, (3.2) is recovered from (3.3) by setting $s = 1$. □

Recall that, if $\widehat{\mathbb{F}_q^*} \cong \mathbb{F}_q^*$ denotes the group of multiplicative characters of $\mathbb{F}_q^*$, then the characteristic function of elements of $\mathbb{F}_{q^n}$ with $\mathbb{F}_q$-norm c (i.e., $N_n(\gamma) = c$) is $\frac{1}{q-1} \sum_{\nu\in\widehat{\mathbb{F}_q^*}} \nu(N_n(\gamma)c^{-1})$. We obtain the following modification of Lemma 3.3, where $\hat{\nu}$ denotes the lift of ν to $\widehat{\mathbb{F}_{q^n}^*}$ (so that $\hat{\nu}(\gamma) = \nu(N_n(\gamma))$).

LEMMA 3.4. *Suppose q is odd, $a, c \in \mathbb{F}_q^*$ are given, with c a primitive element of $\mathbb{F}_q$, and k divides E_n. Suppose also that (k_0, s) is a decomposition of k. Then*

$$\begin{aligned} \frac{(q-1)q^2\pi_{a,c}(k)}{\theta(k_0)} &= \delta \int_{d|k_0} \sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*} \\ \alpha,\beta,z\in\mathbb{F}_q}} \bar{\nu}(c)\bar{\chi}(\alpha(z^2 - 2a) + \beta z)\, S_n(\alpha, \beta; \eta_d\hat{\nu}) \\ &\quad + \sum_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \int_{d|k_0} \sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*} \\ \alpha,\beta,z\in\mathbb{F}_q}} \bar{\nu}(c)\bar{\chi}(\alpha(z^2 - 2a) + \beta z) S_n(\alpha, \beta; \eta_{dp_i}\hat{\nu}). \end{aligned} \tag{3.4}$$

In particular, the contribution to the right side of (3.4) *attributable to values of $\alpha = \beta = 0$ (the "main term") is $\delta q(q^n - 1)$.*

Estimates for $S_n(\alpha, \beta; \eta_d)$ are standard.

LEMMA 3.5. *Suppose $\alpha, \beta \in \mathbb{F}_q$, not both* 0.

If $\alpha = 0$, then $S_n(0, \beta; \mathbf{1}) = 0$; otherwise

$$|S_n(\alpha, \beta; \mathbf{1})| \le q^{\frac{n}{2}}.$$

Suppose $d|q^n-1$ with $d>1$. Then

$$|S_n(\alpha,\beta;\eta_d)| \le \begin{cases} 2q^{\frac{n}{2}}, & \textit{if } \alpha \neq 0,\\ q^{\frac{n}{2}}, & \textit{if } \alpha = 0.\end{cases}$$

We shall apply Lemma 3.5 not only to character sums over $\mathbb{F}_{q^n}$ but also to character sums over $\mathbb{F}_q$ itself (with $n=1$).

At this point it is convenient to split the discussion into the non-zero or zero problems.

4. The odd non-zero problem.

Suppose now that the prescribed coefficient a is non zero and, where relevant, c is a primitive element of $\mathbb{F}_q$.

PROPOSITION 4.1. *Suppose q is odd and $a\neq 0$. Let $k|q^n-1$ and (k_0,s) be a decomposition of k. Suppose*

$$q^{\frac{n-2}{2}} > 4W(k_0)\Delta_{s,\delta}. \tag{4.1}$$

Then $\pi_a(k)$ is positive. Specifically, when $s=1$ and $k=q^n-1$, the sufficient condition is

$$q^{\frac{n-2}{2}} > 4W(q^n-1). \tag{4.2}$$

Proof. Consider the expression (3.3). We aggregate the contributions to the right side relating to a specific multiplicative character η_d or η_{dp_i} (without the weighting factor implicit in the integral notation). Denote by $\tilde{\eta}_d$ the restriction of η_d to $\mathbb{F}_q$, the significance being that $\tilde{\eta}_d$ has order $\frac{d}{\gcd(d,Q_n)}$.

So suppose $d|k_0$ and take η_d: similar reasoning applies to each η_{dp_i}. Consider the contribution of terms with $\beta\neq 0$. Replace $\gamma\in\mathbb{F}_{q^n}$ by $\frac{\gamma}{\beta}\in\mathbb{F}_{q^n}$, $\alpha\in\mathbb{F}_q$ by $\alpha\beta^2\in\mathbb{F}_q$, and $z\in\mathbb{F}_q$ by $\frac{z}{\beta}\in\mathbb{F}_q$. We obtain

$$\delta\sum_{\alpha\in\mathbb{F}_q}\sum_{\beta\in\mathbb{F}_q^*}\chi(2a\alpha\beta^2)\bar{\tilde{\eta}}_d(\beta)\sum_{z\in\mathbb{F}_q}\bar{\chi}(\alpha z^2+z)\,S_n(\alpha,1;\eta_d),$$

which is the same as

$$\delta\sum_{\alpha\in\mathbb{F}_q} S_1(2a\alpha,0;\bar{\tilde{\eta}}_d)\,\overline{S_1(\alpha,1;\mathbf{1})}\,S_n(\alpha,1;\eta_d). \tag{4.3}$$

In (4.3), if $\alpha=0$, then, by Lemma 3.5, $S_1(\alpha,1;\mathbf{1})=0$. We may therefore suppose that the sum is over $\alpha\in\mathbb{F}_q^*$.

Suppose $d\nmid Q_n$. Then $\tilde{\eta}_d$ has order exceeding 1 on $\mathbb{F}_q$. It follows from Lemma 3.5, that (4.3) is bounded in absolute value by $4\delta(q-1)q^{\frac{n}{2}+1}$.

Now suppose $d|Q_n$ so that $\tilde{\eta}_d$ has order 1. This time Lemma 3.5 yields that (4.3) is bounded in absolute value by $2\delta(1+q^{-\frac{1}{2}})(q-1)q^{\frac{n}{2}+1}$. Here, the constant 2 can be reduced to 1 if $d=1$. It is therefore valid (and convenient) to use the same bound $4\delta(q-1)q^{\frac{n}{2}+1}$ for (4.3) when $d|Q_n$ as when $d\nmid Q_n$. Moreover, the negative quantity $-(q-1)$ from the main term is easily offset by the contribution from η_1.

Next, still with regard to a particular character η_d, we consider the contribution from terms with $\beta=0$ (and $\alpha\neq 0$). First we estimate the contribution from (non-zero) squares $\alpha = A^2,\ A \in \mathbb{F}_q$. Since each such value is counted twice (for A and $-A$), when we replace $\gamma \in \mathbb{F}_{q^n}$ by $\frac{\gamma}{A}$ and $z \in \mathbb{F}_q$ by $\frac{z}{A} \in \mathbb{F}_q$, we obtain

$$\frac{1}{2}\sum_{A\in\mathbb{F}_q^*} \chi(2aA^2)\bar{\tilde{\eta}}_d \sum_{z\in\mathbb{F}_q} \chi(z^2)\, S_n(1,0;\eta_d) = \frac{1}{2} S_1(2a,0;\ \bar{\tilde{\eta}}_d)\, \overline{S_1(1,0;\ \mathbf{1})}\, S_n(1,0;\eta_d).$$

Similarly, for non-squares α, set $\alpha = cA^2,\ A \in \mathbb{F}_q^*$ for a fixed non-square c, and we obtain the expression

$$\frac{1}{2} S_1(2ac,0;\ \bar{\tilde{\eta}}_d)\, \overline{S_1(c,0;\ \mathbf{1})}\, S_n(c,0;\eta_d).$$

Accordingly, we obtain a bound of $4\delta q^{\frac{n}{2}+1}$ from the terms with $\beta = 0$.

Summarising, we obtain an absolute bound of $4\delta q^{\frac{n}{2}+2}$ for the (non-weighted) contribution of all terms corresponding to a character η_d.

The remaining terms on the right side of (3.3) (involving characters like η_{dp_i}) are estimated in the same way: we have used no special properties for $d|k_0$. Taking into account that there are $\phi(d)$ characters of order d for each divisor d we deduce that numerically the right side of (3.3) exceeds

$$\delta\left(q^{n+1} - 4q^{\frac{n}{2}+2}\Delta_{s,\delta}\right),$$

with $\Delta_{s,\delta}$ as in Section 2, since $\sum_{i=1}^{s}(1 - \frac{1}{p_i}) = s - 1 + \delta$. □

Similarly, taking the $q-1$ characters in $\widehat{\mathbb{F}_q^*}$ into account we obtain an analogous criterion for the positivity of $\pi_{a,c}(E_n)$.

Proposition 4.2. *Suppose q is odd, $a \neq 0$ and c is a primitive element of $\mathbb{F}_q$. Let $k|E_n$ and (k_0, s) be a decomposition of k. Suppose*

$$q^{\frac{n-4}{2}} > 4\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{4.4}$$

Then $\pi_{a,c}(k)$ is positive. Specifically, when $s = 1$ and $k = E_n$, the sufficient condition is

$$q^{\frac{n-4}{2}} > 4\left(1 - \frac{1}{q}\right) W(E_n). \tag{4.5}$$

4.1. Quartics. Take $n = 4$. Then (4.1) takes the form

$$q > 4W(k_0)\Delta_{s,\delta}. \tag{4.6}$$

To assist in the application of the criterion (4.1) we employ some auxiliary results. The first is an easy fact that was also quoted as Lemma 4.2 in [**10**].

Lemma 4.3. *Suppose n and l are odd primes such that $l|Q_n = \frac{q^n-1}{q-1}$. Then either $l = n$ or $l \in L_{2n}$ (with $l \nmid (q-1)$). Here L_{2n} denotes the set of primes congruent to* 1 (mod $2n$).

Here (and throughout) we use some explicit bounds for the number of square-free divisors of an integer h (see Section 9).

Remark. We will use l to denote a prime number throughout.

Express the product of distinct primes in $q^4 - 1$ as $K_1 \cdot K_2$, where K_1 (an *even* factor of $q^2 - 1$) is the product of all distinct prime divisors of $q^2 - 1$ and K_2 (an *odd* divisor of $q^2 + 1$) is the product of distinct prime divisors of $q^2 + 1$ that do not divide $q^2 - 1$. Easily (or by Lemma 4.3), any prime divisor l of K_2 is $\equiv 1 \pmod 4$, i.e., $l \in L_4$. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2. In fact, $\omega_1 = \omega(\frac{q^2-1}{4})$: indeed $16 | q^4 - 1 = (q-1)(q+1)(q^2+1)$.

LEMMA 4.4. *Suppose that $n = 4$, q odd and $\omega_1 \geq 15$ or $\omega_2 \geq 11$. Let $a \ (\neq 0) \in \mathbb{F}_q$. Then there exists a primitive polynomial of degree 4 over $\mathbb{F}_q$ with the coefficient of x^2 prescribed as a.*

Proof. First suppose $\omega_1 \geq 15$ and $\omega_2 \geq 11$. By Lemma 9.1, the number of square-free divisors of h, an integer such that $\omega(h) \geq 15$, is bounded by $W(h) < h^{\frac{13}{50}}$. Therefore $W(K_1) < (q^2 - 1)^{\frac{13}{50}} < q^{\frac{13}{25}}$. Also, by Lemma 9.2, when an integer h is a product of primes $l \equiv 1 \pmod 4$ and $\omega(h) \geq 11$, then $W(h) < h^{\frac{1}{5}}$. That yields $W(K_2) < (\frac{q^2+1}{2})^{\frac{1}{5}} < q^{\frac{2}{5}}$. It follows that $W(q^4 - 1) < q^{\frac{23}{25}}$. Consequently, by (4.2), to show existence it suffices that $q > 4q^{\frac{23}{25}}$, i.e. $q \geq 4^{\frac{25}{2}} = 33554432$, which obviously holds as $\omega_1 \geq 15, \omega_2 \geq 11$ yield $q > 10^8$.

Next, suppose $\omega_1 \leq 14$ and $\omega_2 \geq 11$. First assume $\omega_1 \geq 4$. Let (k_0, s) be the decomposition where k_0 is the product of K_2 and the smallest three primes in K_1. Thus $s \leq 11$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{43} > 0.392$ and $\Delta_{s,\delta} < 27.52$. By the above, $W(k_0) < 8q^{\frac{2}{5}}$ and (4.6) is satisfied whenever $q \geq 80910$. This is the case since $\omega_2 \geq 11$, whence $q > 10^8$. Assume, on the other hand, that $\omega_1 \leq 3$. Then $W(k_0) = W(q^4 - 1) < 8q^{\frac{2}{5}}$ (again) and the same conclusion follows by (4.1) (equivalent to (4.6) with $s = 1$). (We omit similar obvious modifications in subsequent arguments.)

Finally, suppose $\omega_1 \geq 15$ and $\omega_2 \leq 10$. Take $k_0 = K_1$. Then $s \leq 10$, $\delta \geq 1 - \sum_{\substack{l \leq 89 \\ l \equiv 1 \pmod 4}} \frac{1}{l} > 0.518$ and $\Delta_{s,\delta} < 19.38$. Now (4.6) is satisfied whenever $q \geq 8636$, which completes the proof since $\omega_1 \geq 15$ implies $q > 10^8$. □

After Lemma 4.4, we assume $\omega_1 \leq 14$, $\omega_2 \leq 10$ and run the full sieving process.

Consider the (k_0, s) decomposition with $k_0 = \gcd(q^4 - 1, 30)$. Thus, $k_0 = 30$ unless the characteristic p is 3 ($k_0 = 10$) or 5 ($k_0 = 6$). When $p \neq 5$, the prime 5 will be a divisor of one of K_1 or K_2: observe that in either case δ is bounded below by

$$\delta \geq \min\left(1 - \sum_{\substack{i=2 \\ l_i \equiv 3 \pmod 4}}^{\omega_1 - 2} \frac{1}{l_i} - \sum_{\substack{i=2 \\ l_i \equiv 1 \pmod 4}}^{\omega_2 + 1} \frac{1}{l_i}, \quad 1 - \sum_{\substack{i=2 \\ l_i \equiv 3 \pmod 4}}^{\omega_1 - 1} \frac{1}{l_i} - \sum_{\substack{i=2 \\ l_i \equiv 1 \pmod 4}}^{\omega_2} \frac{1}{l_i}\right),$$

where in each sum the prime l_i indicates the i-th prime in the given congruency class mod 4. It is an empirical (rather than theoretical) observation that this value of δ yields the notional minimal for the bounded values of ω_1, ω_2 in the current application. When $p = 5$, for minimal δ it can be supposed that all odd prime divisors of K_1 are $\equiv 3 \pmod 4$. Write q_{min} for the minimal integral value of q for which (4.6) with the above minimum value of δ holds. The sieving steps are shown in the table below.

#	q	$\omega_1 \le$	$\omega_2 \le$	k_0	$\omega(k_0)$	$s \le$	$\delta \ge$	$\Delta_{s,\delta} \le$	q_{min}
1		14	10	30	3	21	0.242	84.65	2709
2	≤ 2707	7	5	6	2	10	0.240	39.50	633
3	≤ 631	6	4	6	2	8	0.299	25.24	407
4	≤ 405	6	3	6	2	7	0.334	19.97	320
5	≤ 319	5	3	6	2	6	0.377	15.27	245

In the final two lines of the above table we have supposed $\omega_2 \le 3$: although numerically $\omega_2 = 4$ is possible, there are no integers $\frac{q^2+1}{2}$, $q \le 405$ odd, with this value of ω_2.

Next, for all odd prime powers $q \le 243$ the computer algebra package Maple is used to check whether (4.6) (with $k_0 = \gcd(6, q)$) holds. This is so, except for those in $\{3, 5, \dots, 73, 83, 89, 103\}$, a set of cardinality 27. For each of these remaining values primitive quartics with prescribed coefficient of x^2 were found directly.

We do not list all of these polynomials here, only those for $q = 83$, which turns out to have the most (and very small) different prime divisors of $q^4 - 1 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 41 \cdot 53$. We string the 82 pairs (a, c), one example for each primitive quartic $x^4 + ax^2 + x + c$, $a \ne 0$:
$(1, 18)$, $(2, 14)$, $(3, 5)$, $(4, 35)$, $(5, 14)$, $(6, 24)$, $(7, 20)$, $(8, 34)$, $(9, 14)$, $(10, 2)$, $(11, 2)$, $(12, 8)$, $(13, 15)$, $(14, 6)$, $(15, 14)$, $(16, 80)$, $(17, 6)$, $(18, 32)$, $(19, 19)$, $(20, 43)$, $(21, 15)$, $(22, 32)$, $(23, 32)$, $(24, 8)$, $(25, 62)$, $(26, 18)$, $(27, 2)$, $(28, 19)$, $(29, 14)$, $(30, 19)$, $(31, 14)$, $(32, 15)$, $(33, 54)$, $(34, 35)$, $(35, 24)$, $(36, 32)$, $(37, 35)$, $(38, 20)$, $(39, 14)$, $(40, 22)$, $(41, 6)$, $(42, 34)$, $(43, 2)$, $(44, 6)$, $(45, 8)$, $(46, 5)$, $(47, 8)$, $(48, 8)$, $(49, 6)$, $(50, 8)$, $(51, 39)$, $(52, 15)$, $(53, 8)$, $(54, 6)$, $(55, 55)$, $(56, 18)$, $(57, 2)$, $(58, 24)$, $(59, 14)$, $(60, 34)$, $(61, 2)$, $(62, 5)$, $(63, 22)$, $(64, 18)$, $(65, 53)$, $(66, 5)$, $(67, 43)$, $(68, 2)$, $(69, 39)$, $(70, 66)$, $(71, 5)$, $(72, 2)$, $(73, 19)$, $(74, 8)$, $(75, 15)$, $(76, 15)$, $(77, 14)$, $(78, 8)$, $(79, 50)$, $(80, 18)$, $(81, 60)$, $(82, 67)$.

In summary, the above examples suffice to complete the proof (for odd q) of Theorem 1.2 for $n = 4$, $m = 2$ and $a \ne 0$.

4.2. Quintics. Take $n = 5$. Then (4.1) takes form

$$q^{\frac{3}{2}} > 4W(k_0)\Delta_{s,\delta}. \tag{4.7}$$

Express the product of distinct primes in $q^5 - 1$ as $K_1 \cdot K_2$, where K_1 (a factor of $q - 1$) is the product of all distinct prime divisors of $q - 1$ and K_2 (a factor of Q_5) is the product of distinct prime divisors of Q_5 that do not divide $q - 1$. Observe that $5|(q - 1)$ if and only if $5|Q_5$ and therefore all prime divisors of K_2 are $\equiv 1 \pmod{10}$. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2.

LEMMA 4.5. *Suppose that $n = 5$, q odd and $\omega_1 \ge 6$ or $\omega_2 \ge 10$. Let $a\ (\ne 0) \in \mathbb{F}_q$. Then there exists a primitive polynomial of degree 5 over $\mathbb{F}_q$ with the coefficient of x^3 prescribed as a.*

Proof. First suppose $\omega_1 \ge 6$ and $\omega_2 \ge 10$. Then, by (9.1), $W(K_1) < q^{\frac{3}{7}}$, and by (9.6), $W(K_2) < (q^4 + q^3 + q^2 + q + 1)^{\frac{1}{6}} < (q^5)^{\frac{1}{6}} = q^{\frac{5}{6}}$. It follows that $W(q^5 - 1) < q^{\frac{53}{42}}$. Consequently, by (4.2) to show existence it suffices that $q^{\frac{3}{2}} > 4q^{\frac{53}{42}}$, so certainly whenever $q \ge 338$. The latter evidently holds since $\omega_1 \ge 6$ implies $q \ge 30030$.

Next, suppose $\omega_1 \leq 5$ and $\omega_2 \geq 10$. Let (k_0, s) be the decomposition where k_0 is the product of K_2 and the least three primes in K_1. Thus $s \leq 2$. Hence, in (2.2), $\delta \geq 1 - \frac{1}{7} - \frac{1}{11} > 0.766$ and consequently $\Delta_{s,\delta} < 3.31$. By the above reasoning, $W(k_0) < 8q^{\frac{5}{6}}$ and (4.7) is satisfied whenever $q \geq 1091$. This suffices since $q > 45000$ as $\omega_2 \geq 10$.

Finally, suppose $\omega_1 \geq 6$ and $\omega_2 \leq 9$. Then $s \leq 9$, $\delta \geq 1 - \sum_{\substack{l \leq 181 \\ l \equiv 1 (\bmod 10)}} \frac{1}{l} > 0.792$ and $\Delta_{s,\delta} < 12.11$, when k_0 is taken to be $k_0 = K_1$. Now (4.7) is satisfied whenever $q \geq 38$, which holds since $\omega_1 \geq 6$ yields $q \geq 30030$. □

After Lemma 4.5, we can assume $\omega_1 \leq 5$ and $\omega_2 \leq 9$ and begin the full sieving process.

Consider the decomposition (k_0, s), where $k_0 | K_1$. Where applicable, to minimise δ, the prime 11 is notionally taken to divide K_2 rather than K_1. The sieving steps are summarized below:

#	q	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		5	9	30	3	11	0.572	19.49	73
2	≤ 71	3	4	6	2	5	0.636	8.29	27
3	≤ 25	2	3	2	1	4	0.519	7.79	16

For $q = 13, 11$ and 9, consider decompositions with $k_0 = 2$. Here $s = 2$ in each case with $\delta > 0.666$, 0.799 and 0.892 respectively. Then (4.7) is satisfied because

$$13 > (4 \cdot\ 2 \cdot 3.51)^{\frac{2}{3}} = 9.23\ldots ; \quad 11 > (4 \cdot\ 2 \cdot 3.26)^{\frac{2}{3}} = 8.79\ldots ;$$
$$9 > (4 \cdot\ 2 \cdot 3.13)^{\frac{2}{3}} = 8.55\ldots .$$

The only values of q left to check are 7, 5 and 3. Because these are small, we list the relevant primitive polynomials below, one for each pair (q, a).

a	$q = 7$	$q = 5$	$q = 3$
1	$x^5 + x^3 + 4x + 4$	$x^5 + x^3 + 2x + 2$	$x^5 + x^3 + x + 1$
2	$x^5 + 2x^3 + x + 2$	$x^5 + 2x^3 + x + 2$	$x^5 + 2x^3 + x^2 + 1$
3	$x^5 + 3x^3 + x + 4$	$x^5 + 3x^3 + 2$	—
4	$x^5 + 4x^3 + x + 2$	$x^5 + 4x^3 + x^2 + 3$	—
5	$x^5 + 5x^3 + 4$	—	—
6	$x^5 + 6x^3 + 2$	—	—

4.3. Degrees 6, 7 and 8. In this section we prove a stronger result and show the existence of primitive polynomials of degrees $6 \leq n \leq 8$ where, in addition to their second coefficients, their constant terms are also prescribed as primitive elements of $\mathbb{F}_q$. The main tool here is Proposition 4.2. This yields the sufficient condition

$$q,\ q^{\frac{3}{2}},\ q^2 > 4\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta} \quad \text{when } n = 6, 7, 8, \text{ respectively.}$$

4.3.1. Sextics. Write the product of distinct primes in E_6 as $K_1 \cdot K_2$, where K_1 is the product of all distinct prime divisors of $q + 1$ (that do not divide $q - 1$) and K_2 is the product of distinct prime divisors of $\frac{q^6-1}{q^2-1}$ that do not divide $q^2 - 1$. Notice that 3 is never a factor of K_2 and so (by an analogue of Lemma 4.3) any prime divisor l of K_2 is $\equiv 1 \pmod 6$, i.e., $l \in L_6$. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2.

LEMMA 4.6. *Suppose that $n = 6$, q odd and $\omega_1 \geq 10$ or $\omega_2 \geq 24$. Let $a\ (\neq 0) \in \mathbb{F}_q$ and c be a primitive element of $\mathbb{F}_q$. Then there exists a primitive polynomial of degree* 6 *over $\mathbb{F}_q$ with the coefficient of x^4 prescribed as a and constant term c.*

Proof. First suppose $\omega_1 \geq 10$ and $\omega_2 \geq 24$. By (9.2), $W(K_1) < q^{\frac{5}{18}}$, and by (9.5), $W(K_2) < (q^4 + q^2 + 1)^{\frac{10}{63}} < (2q^4)^{\frac{10}{63}}$. Therefore $W(E_6) < 2^{\frac{10}{63}} q^{\frac{115}{126}}$ and, putting $s = 1$, (4.4) guarantees existence when $q > 4 \cdot 2^{\frac{10}{63}} q^{\frac{115}{126}}$, so certainly whenever $q \geq 27774792$ (as $\omega_1 \geq 10$ implies $q > 10^{11}$).

Next, suppose $\omega_1 \leq 9$ and $\omega_2 \geq 24$. Let (k_0, s) be the decomposition where k_0 is the product of K_2 and the smallest three primes in K_1. Hence, $s \leq 6$, $\delta \geq 1 - \frac{1}{11} - \ldots - \frac{1}{29} > 0.642$ and consequently $\Delta_{s,\delta} < 9.79$. Reasoning as above, $W(k_0) < 2^{\frac{199}{63}} q^{\frac{40}{63}}$ and (4.4) is satisfied whenever $q \geq 4322937$. This suffices since $q > 10^{11}$ as $\omega_2 \geq 24$.

At last, suppose $\omega_1 \geq 10$ and $\omega_2 \leq 23$. Take $k_0 = K_1$. Then $s \leq 23$, $\delta \geq 1 - \sum_{\substack{l \leq 223 \\ l \equiv 1 (\mathrm{mod}\ 6)}} \frac{1}{l} > 0.499$ and $\Delta_{s,\delta} < 48.10$. Now (4.4) is satisfied whenever $q \geq 1455$, which holds since $\omega_1 \geq 10$ yields $q \geq 10^{11}$. □

Consequently to the above lemma, we may assume $\omega_1 \leq 9$ and $\omega_2 \leq 23$ and run the sieve, which is represented in the table below.

#	q	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		9	23	105	3	29	0.364	78.93	2526
2	≤ 2525	4	8	15	2	10	0.436	21.44	344
3	≤ 343	3	6	3	1	8	0.354	21.78	175
4	≤ 173	2	6	3	1	7	0.445	15.49	124
5	≤ 123	2	5	3	1	6	0.468	12.69	102

At this place, q_{min} is not small enough to lessen the values of ω_1, ω_2, therefore we use Maple to search for all the $q \leq 101$ with $\omega_1 = 2$. Five such values are found: 29, 41, 59, 83, 101. All but 29 satisfy (4.4) with $k_0 = 1$. We will deal with $q = 29$, but for all the other values of $q \leq 101$ we can now (rightfully) assume $\omega_1 \leq 1$ and continue the sieve.

#	q	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
6	≤ 101	1	5	3	1	5	0.668	7.99	64
7	≤ 63	1	4	3	1	4	0.695	6.32	51
8	≤ 49	1	3	3	1	3	0.727	4.76	39

In line 7 of the table, $q \leq 63$ implies $\omega_2 \leq 5$, but there are no primes or prime powers of that size with $\omega_2 = 5$. We proceeded similarly in the next step, where three such values with $\omega_2 = 4$ exist: 37, 47 and 49. They all fit into (4.4) with $k_0 = 1$. So also does $q = 31, 27$ and 25, but for all the smaller values, and for $q = 29$, we have to search for polynomials explicitly.

For illustration, we give here two polynomials of degree 6 over $\mathbb{F}_3$ with the coefficient of x^4 prescribed as $a \neq 0$ and constant term c (which necessarily equals 2):

$$a = 1 : \ x^6 + x^4 + 2x^2 + x + 2, \qquad a = 2 : \ x^6 + 2x^4 + x^2 + x + 2.$$

4.3.2. Septics.

LEMMA 4.7. *Suppose that $n = 7$, q odd and $\omega(E_7) \geq 6$. Let $a\ (\neq 0) \in \mathbb{F}_q$ and c be a primitive element of $\mathbb{F}_q$. Then there exists a primitive polynomial of degree 7 over $\mathbb{F}_q$ with the coefficient of x^5 prescribed as a and constant term $-c$.*

Proof. Suppose $\omega(E_7) \geq 6$. Lemma 9.5 then provides $W(E_7) < (E_7)^{\frac{1}{6}} \leq (Q_7)^{\frac{1}{6}} < (q^7)^{\frac{1}{6}} = q^{\frac{7}{6}}$. Criterion (4.4) is then certainly sufficient whenever $q^{\frac{3}{2}} > 4q^{\frac{7}{6}}$, i.e. $q > 64$. This holds since $\omega(E_7) \geq 6$. □

We may now suppose $\omega(E_7) \leq 5$. Set $k_0 = 1$ and so $s \leq 5$. Recall Lemma 4.3, by which all the prime divisors of E_7 are $\equiv 1 \pmod{14}$. Therefore $\delta \geq 1 - \frac{1}{29} - \frac{1}{43} - \frac{1}{71} - \frac{1}{113} - \frac{1}{127} > 0.911$ and (4.4) is satisfied for $q \geq 9$. Among the remaining values, $q = 7$ and 5 satisfy (4.4) with $k_0 = 1$, whereas when $q = 3$, the polynomials need to be found explicitly:

$$a = 1 : \ x^7 + x^5 + x + 1, \qquad a = 2 : \ x^7 + 2x^5 + 1.$$

4.3.3. Octics. Express the product of distinct primes in E_8 as $K_1 \cdot K_2$, where K_1 is the product of all distinct odd prime divisors of $(q + 1)(q^2 + 1)$ and K_2 is the product of distinct odd prime divisors of $q^4 + 1$. By an analogue of Lemma 4.3 any prime divisor l of K_2 is $\equiv 1 \pmod 8$, i.e., $l \in L_8$. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2.

LEMMA 4.8. *Suppose that $n = 8$, q odd, $\omega_1 \geq 8$ or $\omega_2 \geq 6$. Let $a\ (\neq 0) \in \mathbb{F}_q$ and c be a primitive element of $\mathbb{F}_q$. Then there exists a primitive polynomial of degree 8 over $\mathbb{F}_q$ with the coefficient of x^6 prescribed as a and constant term c.*

The proof of Lemma 4.8 is analogous to that of Lemma 4.6, so we do not lay it out for the reader. We now assume $\omega_1 \leq 7$ and $\omega_2 \leq 5$ and continue the sieving process. This stops at $q \leq 9$. We check that $q = 9, 7, 5$ and 3 all satisfy criterion (4.4) with $k_0 = 1$. For example, (4.1) holds when $q = 3$, because $q^2 = 9 > 8.78$.

5. The odd zero problem.

Suppose that q remains odd but that the prescribed coefficient a is *zero*. By Lemma 2.1, it suffices to prove that $\pi_0(Q_n)$ is positive.

PROPOSITION 5.1. *Let $k|Q_n$ and let (k_0, s) be a decomposition of k. Suppose q is odd and*

$$q^{\frac{n-3}{2}} > 2\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{5.1}$$

Then $\pi_0(k)$ is positive.

Specifically, when $s = 1$ and $k = Q_n$, the sufficient condition is

$$q^{\frac{n-3}{2}} > 2\left(1 - \frac{1}{q}\right) W(Q_n). \tag{5.2}$$

Proof. Suppose $k|Q_n$ and again consider the expression (3.3). Once more we aggregate the contributions to the right side relating to a specific multiplicative character η_d or η_{dp_i}.

For $d|k_0$ again we obtain (4.3) (with $a = 0$) as the contribution of terms with $\beta \neq 0$. As before we can ignore contributions from terms with $\alpha = 0$. The difference this time is that, since $a = 0$ and $\tilde{\eta}_d$ has order 1, then $S_1(2a\alpha, 0; \bar{\tilde{\eta}}_d) = q - 1$, always. Further $|S_n(\alpha, 1; \eta_d)| \leq 2q^{\frac{n}{2}}$, where the constant 2 can be replaced by 1 if $d = 1$. We therefore obtain $2\delta(q-1)^2 q^{\frac{n+1}{2}}$ as a bound for the sum (4.3) in this situation, where the constant 2 can be replaced by 1 when $d = 1$. Similarly, we obtain $2\delta(q-1)q^{\frac{n+1}{2}}$ as a bound for the contribution of terms with $\beta = 0$. In total therefore the "non-main terms" on the right side of (3.3) are bounded by $2\delta(q-1)W(k_0)\Delta_{s,\delta} q^{\frac{n+3}{2}}$. Since the "main term" is δq^{n+1}, the result follows. □

In what follows, we focus on quartics and quintics. It is then routine to establish Theorem 1.2 for $6 \leq n \leq 8$.

5.1. Quartics. Take $n = 4$. Then, for a decomposition (k_0, s) of $Q_4 = (q+1)(q^2+1)$, (5.1) takes the form

$$q^{\frac{1}{2}} > 2\left(1 - \frac{1}{q}\right) W(k_0)\, \Delta_{s,\delta}. \tag{5.3}$$

Write the product of distinct primes in Q_4 as $K_1 \cdot K_2$, where K_1 (a factor of $q+1$) is the product of all distinct prime divisors of $q+1$ (and so is even) and K_2 (an *odd* divisor of q^2+1) is the product of distinct prime divisors of q^2+1 that do not divide $q+1$. Thus every prime factor l of K_2 has $l \equiv 1 \pmod 4$. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2.

LEMMA 5.2. *Suppose that $n = 4$, q odd and $\omega_1 \geq 28$ or $\omega_2 \geq 40$. Then there exists a primitive polynomial of degree* 4 *over $\mathbb{F}_q$ with the coefficient of x^2 prescribed as $a = 0$.*

Proof. First suppose $\omega_1 \geq 28$ and $\omega_2 \geq 40$. Then, by (9.1) and (9.3), $W(Q_4) < q^{\frac{1}{5}+\frac{7}{25}} = q^{\frac{12}{25}}$. Consequently, by (5.2) to show existence it suffices that $q^{\frac{1}{2}} > 2q^{\frac{12}{25}}$, i.e. $q > 2^{50}$. This holds here because $\omega_1 \geq 28$ implies $q > 10^{42}$.

Next, suppose $\omega_1 \leq 27$ and $\omega_2 \geq 40$. Let (k_0, s) be the decomposition where k_0 is the product of K_2 and the smallest three primes in K_1. Thus $s \leq 24$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{103} > 0.210$ and $\Delta_{s,\delta} < 111.53$. By the above reasoning, $W(k_0) < 8q^{\frac{7}{25}}$ and criterion (5.3) is satisfied whenever $q \geq 6.1 \cdot 10^{14}$. Since $\omega_2 \geq 40$, however, then $q > 10^{43}$.

Finally, suppose $\omega_1 \geq 28$ and $\omega_2 \leq 39$. Take $k_0 = K_1$. Then $s \leq 39$, $\delta \geq 1 - \sum_{\substack{l \equiv 1 \pmod 4 \\ l \leq 409}} \frac{1}{l} > 0.379$ and $\Delta_{s,\delta} < 102.27$. Now (5.3) is satisfied whenever $q \geq 50418994$. This holds since $\omega_1 \geq 28$ yields $q \geq 10^{42}$. □

As a consequence of Lemma 5.2, we can assume $\omega_1 \leq 27$ and $\omega_2 \leq 39$ and run the full sieving process.

We shall consider decompositions (k_0, s) of Q_4, where k_0 (even) is the product of the least primes in Q_4. Suppose, for example, $\omega(k_0) = 4$. Then k_0 is at least $2 \cdot 3 \cdot 5 \cdot 7$. Here, for example, 5 may be a factor of K_1 or K_2 or neither (when $q \equiv 1 \pmod{10}$). But evidently δ is bounded below as

$$\delta \geq \min\left(1 - \sum_{\substack{i=3 \\ l_i \equiv 3 \pmod 4}}^{\omega_1 - 2} \frac{1}{l_i} - \sum_{\substack{i=2 \\ l_i \equiv 1 \pmod 4}}^{\omega_2 + 1} \frac{1}{l_i},\ 1 - \sum_{\substack{i=3 \\ l_i \equiv 3 \pmod 4}}^{\omega_1 - 1} \frac{1}{l_i} - \sum_{\substack{i=2 \\ l_i \equiv 1 \pmod 4}}^{\omega_2} \frac{1}{l_i}\right).$$

The sieving steps are shown in the table below. As usual q_{min} denotes the minimum integer q satisfying (5.3) numerically.

#	q	$\omega_1 \leq$	$\omega_2 \leq$	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		27	39	4	62	0.159	385.65	152295345
2	$\leq$ 152295343	8	10	3	15	0.332	44.17	499454
3	$\leq$ 499453	6	7	2	11	0.229	45.67	133488
4	$\leq$ 133487	6	6	2	10	0.248	38.30	93881
5	$\leq$ 93879	5	6	2	9	0.291	29.50	55696
6	$\leq$ 55695	5	5	2	8	0.316	24.13	37258
7	$\leq$ 62773	6	4	2	8	0.299	25.35	41101
8	$\leq$ 55324	4	6	2	8	0.344	22.32	31868
9	$\leq$ 37257	5	4	2	7	0.343	19.48	24271
10	$\leq$ 37257	4	5	2	7	0.368	18.27	24343
11	$\leq$ 41100	6	3	2	7	0.334	19.95	25457
12	$\leq$ 31867	3	6	2	7	0.435	15.78	15932
13	$\leq$ 24270	4	4	2	6	0.396	14.62	13692
14	$\leq$ 24372	5	3	2	6	0.377	15.24	14850
15	$\leq$ 24372	3	5	2	6	0.459	12.88	10466

The first three lines of figures in the above table were obtained through the method of maximising ω_1 and ω_2 for the indicated range of q. For the fourth line, the values of ω_2 for integers q in this range were calculated and shown to not to exceed 7. Then in the fifth line, the values of ω_1 for integers q in the relevant range were calculated and 30029, 43889, 51862, 53129, 67829, 81509, 84629 and 85469 were found with $\omega_1 = 6$. However, they all satisfy criterion (5.3) with k_0 chosen to be 6. As indicated, this establishes Theorem 1.2 for $q \leq 55696$. Moreover, there are no integers q with $\omega_1 \geq 5$ or $\omega_2 \geq 5$ that lie outside the scope of the next five lines. Hence, we can suppose $q \leq 41100$. Although $\omega_1 = \omega_2 = 5$ when $q = 31709$, this value of q is not a prime power. Altogether 8 prime powers q (all actually primes) with $q > 15000$ lie outside the scope of the remainder of the table. These are 19469, 19739, 20747, 21419, 21713, 24023 (all with $\omega_1 = 5, \omega_2 = 4$) and 15287, 23873 (both with $\omega_1 = 4, \omega_2 = 5$). Not surprisingly, when δ is calculated explicitly for these it is seen that (5.3) is indeed satisfied in these cases.

More systematically, Maple (with $k_0 = \gcd(6, Q_4)$) was used to check (5.3) for prime powers $q < 15000$. Virtually instantaneously it returns a positive answer for all but a set of 246 prime powers q comprising 233 primes and 13 composite prime powers. The largest (prime) failure is 11003. The composite failures are $3^2 = 9$, $5^2 = 25$, $3^3 = 27$, $7^2 = 49$, $3^4 = 81$, $11^2 = 121$, $5^3 = 125$, $13^2 = 169$, $3^5 = 243$, $17^2 = 289$, $7^3 = 343$, $11^3 = 1331$, $17^3 = 4913$. For each failure $q = p^n$, Maple was again used to prove the existence of a primitive quartic with zero coefficient of x^2. For details see the table below. The field $\mathbb{F}_{q^4}$ was defined as $\mathbb{F}_p(\alpha)$ where $f_q(x)$ is the minimal polynomial of α. Then γ is a primitive element of $\mathbb{F}_{q^4}$ (in terms of α) with minimal polynomial of γ over $\mathbb{F}_q$ having second coefficient 0. There were no special preferences when chosing α and γ; the choice was random. The primitive quartics themselves are not given in the table below, as they take a long time to compute. More explicitly, an appropriate quartic for

$q = 9$ is $x^4 + x + 2\alpha + 2$, where $\mathbb{F}_9$ is defined as $\mathbb{F}_3(\alpha)$ where α satisfies $f(x) = 0$ with $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$.

$$\begin{array}{lc}
q = 3^2 & f_q(x) = x^8 + 2x^7 + x^6 + x^5 + x^2 + 2 \\
 & \gamma = \alpha^7 + 2\alpha^6 + \alpha^4 + \alpha^3 + 2\alpha^2 + 1 \\
q = 5^2 & f_q(x) = x^8 + 4x^6 + x^5 + 3x^4 + 4x^3 + 4x^2 + 1 \\
 & \gamma = 4\alpha^7 + 3\alpha^6 + 2\alpha^4 + 3\alpha^3 + 2\alpha^2 + 4 \\
q = 3^3 & f_q(x) = x^{12} + 2x^{11} + x^{10} + 2x^7 + x^6 + x^5 + 2x^4 + 2x^3 + x + 1 \\
 & \gamma = \alpha^{11} + 2\alpha^9 + 2\alpha^8 + 2\alpha^6 + 2\alpha^4 + 2\alpha^3 + 2\alpha^2 + 2\alpha + 1 \\
q = 7^2 & f_q(x) = x^8 + x^7 + x^6 + 5x^5 + 4x^3 + 4x^2 + 3 \\
 & \gamma = \alpha^7 + \alpha^6 + 5\alpha^5 + 6\alpha^4 + 5\alpha^2 + 6\alpha \\
q = 3^4 & f_q(x) = x^{16} + 2x^{15} + 2x^{14} + 2x^{11} + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2 \\
 & \gamma = \alpha^{15} + \alpha^{13} + \alpha^{12} + 2\alpha^{10} + \alpha^8 + \alpha^7 + 2\alpha^6 + 2\alpha^5 + 2\alpha^4 + 2\alpha^3 + \alpha^2 + \alpha + 2 \\
q = 11^2 & f_q(x) = x^8 + 10x^7 + 10x^6 + 5x^5 + 4x^4 + 7x^3 + 5x^2 + 5x + 2 \\
 & \gamma = 8\alpha^7 + 6\alpha^5 + 8\alpha^4 + 5\alpha^3 + 7\alpha^2 + 3\alpha + 6 \\
q = 5^3 & f_q(x) = x^{12} + 2x^{11} + 2x^{10} + 3x^9 + x^8 + 2x^7 + 2x^6 + x^5 + 3x + 2 \\
 & \gamma = 4\alpha^{10} + 3\alpha^9 + \alpha^8 + 3\alpha^6 + 3\alpha^5 + 4\alpha^3 + 2\alpha^2 + 3\alpha + 3 \\
q = 13^2 & f_q(x) = x^8 + 10x^7 + x^6 + 10x^5 + 9x^3 + 9x^2 + 6x + 5 \\
 & \gamma = 10\alpha^7 + 4\alpha^6 + 10\alpha^5 + 9\alpha^4 + 2\alpha^3 + 9\alpha^2 + 11\alpha + 11 \\
q = 3^5 & f_q(x) = x^{20} + 2x^{17} + 2x^{15} + x^{14} + x^{12} + 2x^{11} + 2x^{10} + x^7 + 2x^6 + x^5 + x^4 + x^3 + 2x + 1 \\
 & \gamma = 2\alpha^{19} + 2\alpha^{18} + \alpha^{17} + 2\alpha^{16} + 2\alpha^{15} + \alpha^{14} + \alpha^{13} + \alpha^{12} + 2\alpha^7 + 2\alpha^6 + \alpha^5 + 2\alpha^2 + 2\alpha + 2 \\
q = 17^2 & f_q(x) = x^8 + 10x^7 + 11x^6 + 8x^5 + 5x^4 + 8x^3 + 12x^2 + 3x + 5 \\
 & \gamma = 4\alpha^7 + 2\alpha^4 + 2\alpha^2 + 4 \\
q = 7^3 & f_q(x) = x^{12} + 4x^{11} + 3x^{10} + 3x^9 + 3x^8 + x^7 + 3x^6 + 4x^4 + 4x^3 + 5x + 4 \\
 & \gamma = 4\alpha^{11} + 3\alpha^{10} + 2\alpha^9 + 6\alpha^8 + \alpha^7 + 3\alpha^6 + 4\alpha^5 + 6\alpha^4 + 6\alpha^3 + 4\alpha + 5 \\
q = 11^3 & f_q(x) = x^{12} + 5x^{11} + 4x^{10} + 10x^9 + 10x^8 + 8x^7 + x^6 + 2x^5 + 5x^4 + 6x^2 + 1 \\
 & \gamma = 7\alpha^{11} + 5\alpha^{10} + \alpha^9 + 2\alpha^8 + 10\alpha^7 + 9\alpha^5 + 6\alpha^4 + 10\alpha + 4 \\
q = 17^3 & f_q(x) = x^{12} + 16x^{11} + 9x^9 + 5x^8 + 14x^7 + 13x^6 + 8x^5 + 3x^4 + 3x^3 + 11x^2 + 12x + 6 \\
 & \gamma = 10\alpha^{11} + 11\alpha^{10} + 12\alpha^9 + 14\alpha^8 + 14\alpha^7 + \alpha^6 + 2\alpha^5 + 11\alpha^4 + \alpha^3 + 11\alpha^2 + 13
\end{array}$$

Except for $q = 5, 7, 13, 19$ and 31, when q is prime, a primitive quartic of the simple form $x^4 + x + c$ exists. The largest value of c obtained is 103 when $q = 1559$. Suitable quartics in the excepted cases are as follows.

$q = 5$	$x^4 + x^3 + x + 3$
$q = 7$	$x^4 + x^3 + x + 3$
$q = 13$	$x^4 + x^3 + x + 2$
$q = 19$	$x^4 + x^3 + 3x + 13$
$q = 31$	$x^4 + x^3 + x + 21$

5.2. Quintics. Take $n = 5$. Then (5.1) becomes

$$q > 2\left(1 - \frac{1}{q}\right) W(k_0)\, \Delta_{s,\delta}. \tag{5.4}$$

Suppose l (prime) divides Q_5. Then either $l = 5$ (which occurs if and only if $q \equiv 1 \pmod{10}$) or $l \equiv 1 \pmod{10}$. In this subsection, denote $\omega(Q_5)$ by ω.

LEMMA 5.3. *Suppose that $n = 5$, q is odd and that $\omega \geq 18$ if $q \equiv 1 \pmod{10}$ and $\omega \geq 17$, otherwise. Then there exists a primitive polynomial of degree* 5 *over $\mathbb{F}_q$ with the coefficient of x^3 prescribed as* 0.

Proof. Since $\omega \geq 18$, even when $5|Q_5$, the number of prime divisors $l \equiv 1 \pmod{10}$ of Q_5 is at least 17. By (9.6) it follows that

$$W(Q_5) \, < \, 2\left(\sqrt{\frac{Q_5}{5}} - 1\right)^{\frac{23}{80}} \, < \, \frac{2}{5^{\frac{23}{160}}}\,(q^2 + 1 \, - 1)^{\frac{23}{80}} < 1.6 \cdot q^{\frac{23}{40}}.$$

Hence (5.4) holds whenever $q > 3.2^{\frac{40}{23}} = 7.558\ldots$, which is trivially the case. □

To continue with the sieving process, take $k_0 = 1$. Then by Lemma 5.3 we can suppose $s = \omega \leq 18$ (or 17). The outcome is summarised in the following table where the figures focus on the more testing case when $5|Q_5$ until $q < 11$. Here q_{min} denotes the minimal integral value of q for which (5.4) holds with the displayed value of δ.

#	q	$\omega \leq$	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		18	0.560	32.32	65
2	≤ 64	6	0.621	10.04	21
3	≤ 20	4	0.652	6.599	14
4	≤ 13	3	0.676	4.96	10
5	≤ 9	2	0.876	3.15	7

For $q = 5$, then $Q_5 = 11 \cdot 71$ so that $\delta = 1 - \frac{1}{11} - \frac{1}{71} > 0.895$, $\Delta_{s,\delta} < 3.12$. Thus the right side of (5.4) is less than $4.992 < 5$, as required. Finally, for $q = 3$, $Q_5 = 11^2$ and (5.4) holds (with $s = 1$) since $3 > \frac{8}{3}$. Hence, in this case, Theorem 1.2 holds without the need for any direct verification.

Similar considerations could be applied to degrees $n = 6, 7, 8$ but Theorem 1.2 in these cases when $a = 0$ follows, for instance, from [**9**].

6. The even problem.

Suppose that $p = 2$ so that q is *even*. In this section, 2-adic analysis will be used. The fields $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ will be identified with subsets (or finite quotient rings) of an extension of the field $\mathbb{Q}_2$ (the completion of the rational field with respect to the 2-adic metric).

Introduce definitions and notation as follows.

- K_n is the splitting field of the polynomial $x^{q^n} - x$ over $\mathbb{Q}_2$.
- Γ_n ($\subseteq K_n$) is the set of roots of the polynomial above (the Teichmüller points of K). The non-zero elements of Γ_n form a cyclic group of order $q^n - 1$.
- R_n denotes the ring of integers of K_n. Then $\Gamma_n \subseteq R_n = \{\sum_{i=0}^{\infty} 2^i \gamma_i,\ \gamma_i \in \Gamma_n\}$. Moreover, R_n is a local ring with unique maximal ideal $2R_n$ and $R_n/2R_n \cong \mathbb{F}_{q^n}$.
- Distinct elements of Γ_n are already distinct modulo 2. For a set isomorphic to $\mathbb{F}_{q^n}$, temporarily denoted by $\mathcal{G}_n$, all q^n members of Γ_n can be expressed uniquely in the form $\sum_{i=0}^{\infty} 2^i \gamma_i,\ \gamma_i \in \mathcal{G}_n$, where $\gamma \in \Gamma_n$ is already fixed by specifying γ_0. For any integer $e \geq 1$, $\Gamma_{n,e}$ is the set (of cardinality q^n) of elements of Γ_n mod 2^e, i.e.,

$\Gamma_{n,e} = \{\sum_{i=0}^{e-1} 2^i\gamma_i,\ \gamma_i \in \mathcal{G}_n\}$, where we retain the notation γ for the member associated with $\gamma \in \Gamma_{n,e}$. In particular, $\gamma^{q^n} = \gamma$ for $\gamma \in \Gamma_{n,e}$. Moreover, $\mathcal{G}_n = \Gamma_{n,1} \cong \mathbb{F}_{q^n}$.

- $R_{n,e} = \{\sum_{i=0}^{e-1} 2^i\gamma_i, \gamma_i \in \Gamma_{n,e}\} \cong R_n/2^eR_n$, so that $R_{n,e}$ has cardinality q^{ne}. (Thus $R_{n,e}$ is a *Galois ring*.) Observe that here $R_{n,e}/2R_{n,e} \cong \mathbb{F}_{q^n}$ also, and $R_{n,1} = \Gamma_{n,1}$, which can be identified with $\mathbb{F}_{q^n}$. Conversely, each $\gamma \in \Gamma_{n,1}$ yields a unique lift, also denoted by γ, to every $\Gamma_{n,e}$ and to Γ_n itself. An element of (multiplicative) order r in $\Gamma_{n,1}$ lifts to an element of the same order in each $\Gamma_{n,e}$ and in Γ_n; in particular, a primitive element lifts to a primitive element.

Next, consider objects relating to the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. The field K_1 is a subfield of K_n, with $\Gamma_1 \subseteq \Gamma_n$, and R_1 a subring of R_n. Similar relationships apply to the Galois rings. Further, note that the Galois group of K_n/K_1 is isomorphic to that of $\mathbb{F}_{q^n}/\mathbb{F}_q$, being cyclic of order n and generated by the Frobenius automorphism τ_n, where $\tau_n(\gamma) = \gamma^q$, $\gamma \in \Gamma_n$. More generally, on R_n, $\tau_n(\sum_{i=0}^{\infty} 2^i\gamma_i) = \sum_{i=0}^{\infty} 2^i\gamma_i^q$ (where each $\gamma_i \in \Gamma_n$). This induces a ring homomorphism τ_n on $R_{n,e}$ such that $\tau_n(\sum_{i=0}^{e-1} 2^i\gamma_i) = \sum_{i=0}^{e-1} 2^i\gamma_i^q$ (where now each $\gamma_i \in \Gamma_{n,e}$).

Now we discuss polynomials. The polynomial $x^{q^n} - x$ over $\mathbb{F}_q$ (and so over R_1) is the product of all monic irreducible polynomials of degree a divisor of n. A typical monic irreducible polynomial $f(x)$ of degree d (a divisor of n) in $R_{1,1}[x]$ has the form

$$f(x) = (x-\gamma)(x-\gamma^q)\cdots(x-\gamma^{q^{d-1}}) = x^d - \sigma_1x^{d-1} + \cdots + (-1)^d\sigma_d, \qquad (6.1)$$

where $\gamma \in \Gamma_{n,1}$ and each $\sigma_j \in \Gamma_{1,1}$. The polynomial f *lifts* to a (unique) irreducible polynomial of degree d over each $R_{1,e}$, and over R_1 having the same form, except that γ is the corresponding lifted element of $\Gamma_{1,e}$ or Γ_1. But note that, in general, the coefficients σ_j in (6.1) lie in $R_{1,e}$ (or R_1), but may not be in $\Gamma_{1,e}$ (or Γ_1). From the above, the *order* of the polynomial f (which equals the order of any of its roots) or any of its lifts has the same value (a divisor of $q^n - 1$). In particular, f is *primitive* if it is irreducible of degree n and has order $q^n - 1$: this holds if and only if any of its lifts are primitive.

For any $\gamma \in \Gamma_n$, define its trace (over R_1) as $T_n(\gamma) := \gamma + \tau_n(\gamma) + \cdots + \tau_n^{n-1}(\gamma) = \gamma + \gamma^q + \cdots + \gamma^{q^{n-1}} \in R_1$. Observe that $T_n(c\gamma) = cT_n(\gamma)$, $c \in \Gamma_1$. A trace function T_n with similar properties is induced on $\Gamma_{n,e}$.

Next, let $\gamma \in \Gamma_n$ be a root of a lifted irreducible polynomial $f(x) \in R_1[x]$. Eventually, we can suppose γ is *primitive*: for the moment it suffices that f has degree n. Thus, (6.1) holds with $d = n$. Here σ_i denotes the i-th symmetric function of the roots $\gamma, \gamma^q, \dots, \gamma^{q^n-1}$. Employing the trace, we have that s_i, the sum of the i-th powers of the roots of f, is given by $s_i = T_n(\gamma^i) \in R_1$. Of course, each s_i depends only on f and not on the specific root γ: moreover, all this translates to the expansion of f as a polynomial in $R_{1,e}[x]$. For our purposes, we require an expression for the 2-adic expansion of s_i.

We proceed to work with a lifted irreducible polynomial f of degree n in $R_1[x]$ and eventually its reduction to $R_{1,2}$. Henceforth, the letter t is reserved for an *odd* positive integer. Note from above that, for any such t, the value of s_{t2^i} for any $i \geq 0$ is already determined by s_t, and is given by $s_t^{(i)} := \tau^i(s_t)$. For any t, write $s_t = \sum_{j=0}^{\infty} s_{t,j}2^j$, $s_{t,j} \in \Gamma_1$, whence $s_t^{(i)} = \sum_{j=0}^{\infty} s_{t,j}^{2^i}2^j$. Since each positive integer L can be uniquely expressed as $L = t2^j$, then any *component* $s_{t,j}$ is uniquely associated with the integer $t2^j$.

In this context Lemma 3.1 assumes the following shape.

LEMMA 6.1. *Let* $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \in R_1[x]$ *be a (lifted) irreducible polynomial with* σ_i *being a symmetric function of the roots of* f, $\sigma_1, \ldots, \sigma_n \in \Gamma_1$. *Let* s_i *be the sum of the i-th powers of the roots of* f. *Then*

$$2\sigma_2 = s_1^2 - s_2. \tag{6.2}$$

LEMMA 6.2. *Let* f, σ_i *and* s_i *be as in Lemma* 6.1. *Then* $\sigma_2 \equiv s_{1,1}^2 \pmod 2$.

Proof. Over $R_{1,2}$, equality (6.2) translates to $2\sigma_2 = (s_{1,0} + 2s_{1,1})^2 - (s_{1,0}^2 + 2s_{1,1}^2)$ which, modulo 4, is congruent to $-2s_{1,1}^2$. Hence $\sigma_2 \equiv s_{1,1}^2 \pmod 2$. □

As a consequence of Lemma 6.2, for σ_2 to be prescribed (mod 2), it suffices to prescribe $s_{1,1} \in \Gamma_1$ alone. The value of $s_{1,0}$ appears to be irrelevant. Nevertheless, in practice we cannot prescribe $s_{1,1}$ without assigning a value (say $z \in \Gamma_{1,1}$) to $s_{1,0}$. The situation is therefore comparable to that in odd characteristic. In view of Lemma 6.2, given $a \in \mathbb{F}_q \cong \Gamma_{1,1}$, write $a = A^2$, $A \in \mathbb{F}_q$. We wish to prescribe $s_1 = s_{1,0} + 2s_{1,1} \in R_{1,2}$ as $z + 2A$.

In order to apply Lemma 6.2, we require to work with the multiplicative characters of $\Gamma_{n,2}^*$, a cyclic group of order $q^n - 1$, and the additive characters of $R_{n,2}$. So now, for any divisor d of $q^n - 1$, η_d is a character of order d. It is extended to $\Gamma_{n,2}$ by setting $\eta_d(0) = 0$. In particular, η_1 is the trivial character: for an alternative version with $\eta(0) = 1$ we write $\eta = \mathbf{1}$. For additive characters, write $\chi_{(n)}$ for the canonical additive character of $R_{n,2}$: thus

$$\chi_{(n)}(\gamma) = \exp\left(\frac{2\pi T_{nu}(\gamma)}{4}\right), \quad q = 2^u, \quad \gamma \in R_{n,2}.$$

Here $T_{nu}(\gamma)$ yields the *absolute trace* of γ. In particular, set $\chi_{(1)} = \chi$. The characteristic function for the set of elements $\gamma \in \Gamma_{n,2}$ for which $s_1 (= s_{1,0} + 2s_{1,1}) = z + 2A$ is

$$\begin{aligned} &\frac{1}{q^2} \sum_{\xi \in R_{1,2}} \chi(\xi(T_n(\gamma) - (z + 2A))) \\ &\quad = \frac{1}{q^2} \sum_{\alpha_0, \alpha_1 \in \Gamma_{1,1}} \chi_{(n)}((\alpha_0 + 2\alpha_1)(\gamma))\, \chi(-(\alpha_0 + 2\alpha_1)z - 2\alpha_0 A). \end{aligned} \tag{6.3}$$

For the (eventual) sum over $z \in \Gamma_{1,1}$ we require a lemma.

LEMMA 6.3. *Let* $\xi = \alpha_0 + 2\alpha_1 \in R_{1,2}^*$, *where* $\alpha_0, \alpha_1 \in \Gamma_{1,1}$. *Set* $U_\xi = \sum_{z \in \Gamma_{1,1}} \chi(\xi z)$. *Then* $U_\xi = 0$ *unless* $\xi = \pm\alpha_0$ $(\neq 0)$, *in which case* $U_\xi = \frac{1 \pm i}{2} \cdot q$, *respectively.*

Proof. Replacing z by $\alpha_i z$, $i = 1, 2$, as appropriate, we may assume that either $\xi = 1 + 2x$ or $\xi = 2x$, $x \neq 0$, where $x \in \Gamma_{1,1}$. Moreover, from the definition, the value of $\chi(\xi z)$ depends on the absolute trace $T_u(\xi z)$.

First let $\xi = 1 + 2x$. Then with $i = \sqrt{-1}$, $\chi(\xi z) = i^j \cdot (-1)^k$, where $j = T_u(z)$, $k = T_u(xz)$. The map $z \longmapsto (T_u(z), T_u(xz))$ is obviously an additive homomorphism from $\Gamma_{1,1} \cong \mathbb{F}_q$ onto $\mathbb{F}_2 \times \mathbb{F}_2$. In particular, it attains each value in its image set equally often. Because $T_u(\Gamma_{1,1}) = \mathbb{F}_2$, if this map is not an epimorphism, then it must be one of the subgroups $\{(0,0), (1,0)\}$ or $\{(0,0), (1,1)\}$.

In the former case, this means that $T_u(xz) = 0$ for all $z \in \Gamma_{1,1}$ which implies that $x = 0$ (i.e., $\xi = 1$) and $U_\xi = \frac{1+i}{2} \cdot q$. In the latter case, it must be that $T_u(xz) = T_u(z)$

for all $z \in \Gamma_{1,1}$ which implies that $x = 1$ (i.e., $\xi = 3 = -1 \in R_{1,2}$) and $U_\xi = \frac{1-i}{2} \cdot q$. Otherwise, the map is surjective: $\chi(\xi z)$ attains the values $1,\ i-1, -i$ with equal frequency, whence $U_\xi = 0$.

Now take $\xi = 2x \neq 0$. Then the map $z \longmapsto T_u(xz)$ from $\Gamma_{1,1}$ to $\mathbb{F}_2$ is surjective and $\chi(\xi z)$ attains the values ± 1 equally often. This completes the proof. □

LEMMA 6.4. *Assume q is even and $a = A^2 \in \mathbb{F}_q \cong \Gamma_{1,1}^*$. Let $k|q^n - 1$ and (k_0, s) be a decomposition of k. Then*

$$\frac{q\pi_a(k)}{\theta(k_0)} = \delta\left(q^n - 1 + \frac{1}{2}\int_{d|k_0} \sum_{\alpha\in\Gamma_{1,1}^*} \bar{\chi}(2\alpha a)\bar{\tilde{\eta}}_d(\alpha)\,\{(1-i)S_n(1;\eta_d) + (1+i)S_n(-1;\eta_d)\}\right)$$
$$+\frac{1}{2}\sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right)\int_{d|k_0}\sum_{\alpha\in\Gamma_{1,1}^*} \bar{\chi}(2\alpha a)\bar{\tilde{\eta}}_d(\alpha)\big\{(1-i)S_n\big(1;\eta_{dp_i}\big)$$
$$+(1+i)S_n\big(-1;\eta_{dp_i}\big)\big\},$$

where, for $\xi \in R_{1,2}$, $S_n(\xi;\eta_d) := \sum_{\gamma\in\Gamma_{n,2}} \chi_{(n)}(\xi\gamma)\eta_d(\gamma)$ and $\tilde{\eta}_d$ is the restriction of η_d to $\Gamma_{1,1}$.

Proof. Consider the trivial decomposition of k with $s = 1$. (The difficulty in extending to a general decomposition is merely notational.) Write $\xi = \alpha_0 + 2\alpha_1$ for a typical element of $R_{1,2}$.

From the characteristic functions (in particular (6.3)) one obtains

$$\frac{q^2\pi_a(k)}{\theta(k)} = \int_{d|k}\sum_{\xi\in R_{1,2}} \chi(2\alpha_0 A)\ U_\xi\ S_n(\xi;\eta_d), \tag{6.4}$$

with U_ξ as in Lemma 6.3. Since $S_n(0;\eta_d) = 0$ unless $d = 1$, the contribution to (6.4) from $\xi = 0$ (the "main term") is $q(q^n - 1)$. Since $U_\xi = 0$ unless $\xi = \pm\alpha_0$ all contributions from other values of ξ are zero.

Hence consider the contribution from $\xi = \pm\alpha_0 \neq 0$. Replace $\gamma \in \Gamma_{n,2}$ by $\frac{\gamma}{\alpha_0} \in \Gamma_{n,2}$ and $z \in \Gamma_{1,1}$ by $\alpha_0 z \in \Gamma_{1,1}$ to obtain

$$\int_{d|k}\sum_{\alpha_0\in\Gamma_{1,1}^*} \chi(2\alpha_0 A)\bar{\tilde{\eta}}_d(\alpha_0)\ U_{-1}\ S_n(1;\eta_d) + \int_{d|k}\sum_{\alpha_0\in\Gamma_{1,1}^*} \chi(2\alpha_0 A)\bar{\tilde{\eta}}_d(\alpha_0)\ U_1\ S_n(-1;\eta_d).$$

The result follows using Lemma 6.3 for $U_{\pm 1}$ and dividing the ensuing identity by q. □

Multiplicatively, $\mathbb{F}_{q^n}^* \cong \Gamma_{n,2}^*$. Take c to be a primitive element of $\mathbb{F}^* \cong \Gamma_{1,1}^*$ as well as $a \neq 0$ ($\in \mathbb{F} \cong \Gamma_{1,1}$). Then, with $k|E_n$ (by Lemma 2.2), there is an analogous expression for $\frac{(q-1)q\pi_{a,c}}{\theta(k_0)}$ to that of Lemma 6.4 comparable to the relationship Lemma 3.4 bears to Lemma 3.3. In particular, each "integral" on the right side is also over a sum over characters $\nu \in \widehat{\Gamma_{1,2}^*}$ and each character such as η_d or η_{dp_i} replaced by a product $\eta_d\hat{\nu}$ $\eta_{dp_i}\hat{\nu}$, where $\hat{\nu}$ is the lift of ν to $\Gamma_{n,2}^*$.

In the expressions for $\frac{q\pi_a}{\theta(k_0)}$ or $\frac{(q-1)q\pi_{a,c}}{\theta(k_0)}$, the relevant bounds for $|S_n(\xi;\eta_d)|$ are as follows.

LEMMA 6.5. *Suppose* $\xi \in R^*_{1,2}$. *Then* $S_n(\xi; \mathbf{1}) = 0$. *Further, if* d (> 1) *divides* $q^n - 1$, *then* $|S_n(\xi; \eta_d)| \le 2q^{\frac{n}{2}}$. *Indeed, if* $\alpha_1 \in \Gamma_{1,1}$ *then* $|S_n(2\alpha_1; \eta_d)| \le q^{\frac{n}{2}}$.

Proof. This follows from Corollary 6.1 of **[21]**. The significant point is that the polynomial $(\alpha_0 + 2\alpha_1)x \in R^*_{1,2}[x]$ has *weighted degree* 2 (if $\alpha_0 \neq 0$) or 1 (if $\alpha_0 = 0$). □

Again it is now convenient to split the discussion into the non-zero or zero problems.

7. The even non-zero problem. Suppose that q is even and that the prescribed coefficient $a \in \mathbb{F}_2 \cong \Gamma_{1,1}$ is non-zero.

PROPOSITION 7.1. *Assume that* q *is even and* $a \in \mathbb{F}_2$ *is non-zero. Assume also that* $k|q^n - 1$ *and that* (k_0, s) *is a decomposition of* k. *Suppose also that*

$$q^{\frac{n-1}{2}} > 2\sqrt{2}\, W(k_0)\Delta_{s,\delta}. \tag{7.1}$$

Then $\pi_a(k)$ *is positive.*

Specifically, when $s = 1$ *and* $k = q^n - 1$, *the sufficient condition is*

$$q^{\frac{n-1}{2}} > 2\sqrt{2}\, W(q^n - 1). \tag{7.2}$$

Proof. The sums over $\alpha \in \Gamma^*_{1,1}$ in (6.4) can be written as $\tilde{\eta}_d(a)S_1(1; \bar{\tilde{\eta}}_d)$. Then use Lemma 6.5 both for S_n and S_1. (The savings when $\tilde{\eta}_d$ is trivial easily compensate for the -1 in the main term.) □

PROPOSITION 7.2. *Assume that* q *is even,* $a \in \mathbb{F}_2$ *is non-zero and* c *is a primitive element of* $\mathbb{F}_2$. *Assume also that* $k|E_n$ *and that* (k_0, s) *is a decomposition of* k. *Suppose also that*

$$q^{\frac{n-3}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{7.3}$$

Then $\pi_{a,c}(k)$ *is positive.*

Specifically, when $s = 1$ *and* $k = q^n - 1$, *the sufficient condition is*

$$q^{\frac{n-3}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(E_n). \tag{7.4}$$

7.1. Quartics. Take $n = 4$. Then, for any decomposition of Q_4, (7.1) takes the form

$$q^{\frac{3}{2}} > 2\sqrt{2}\, W(k_0)\Delta_{s,\delta}. \tag{7.5}$$

As in Section 4.1, express the product of distinct primes in the odd coprime integers $q^2 - 1$ and $q^2 + 1$ as K_1, K_2, respectively, and $\omega_i = K_i$, $i = 1, 2$. In particular, $3|K_1$ and all prime divisors of K_2 are $\equiv 1 \pmod 4$.

LEMMA 7.3. *Suppose that* $n = 4$, q *even and* $\omega_1 \ge 8$ *or* $\omega_2 \ge 6$. *Let* a $(\neq 0) \in \mathbb{F}_q$. *Then there exists a primitive quartic over* $\mathbb{F}_q$ *with the coefficient of* x^2 *prescribed as* a.

Proof. First suppose $\omega_1 \geq 8$ and $\omega_2 \geq 6$. Then, by (9.2) and (9.4), $W(q^4-1) < q^{\frac{2}{3}+\frac{2}{4}} = q^{\frac{7}{6}}$. Consequently, by (7.2), to show existence it suffices that $q^{\frac{1}{3}} > 2\sqrt{2}$. This holds since, evidently $\omega_1 \geq 8$ and hence $q > 10^4$.

Next, suppose $\omega_1 \leq 7$ and $\omega_2 \geq 6$. Take the decomposition with $k_0 = 3K_2$. Thus $s \leq 6$, $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \cdots - \frac{1}{19} > 0.377$ and $2\sqrt{2}\Delta_{s,\delta} < 43.17$. Moreover $W(k_0) < 2 \cdot q^{\frac{1}{2}}$ and (7.5) is satisfied whenever $q \geq 87$. This holds since $\omega_2 \geq 6$, whence $q > 6900$.

Finally, suppose $\omega_1 \geq 8$ and $\omega_2 \leq 5$. Take $k_0 = K_1$. Then $s \leq 5$ and $\delta \geq 1 - \frac{1}{5} - \frac{1}{13} - \frac{1}{17} - \frac{1}{29} - \frac{1}{37} > 0.602$ and $2\sqrt{2}\Delta_{s,\delta} < 24.46$. Hence (7.5) is satisfied whenever $q \geq 24.46^{\frac{6}{5}} = 46.36\ldots$. Necessarily however $q > 10^4$. □

As a consequence of Lemma 7.3 we can assume $\omega_1 \leq 7$ and $\omega_2 \leq 5$.

Take the decomposition with $k_0 = 3$, so that $s \leq 11$. Then $\delta > 1 - \frac{1}{5} - \frac{1}{7} - \cdots - \frac{1}{41} \geq 0.216$, so that $2W(k_0)\sqrt{2}\Delta_{s,\delta} < 273.21$. Hence (7.5) is satisfied whenever $q > 273.21^{\frac{2}{3}} = 42.10\ldots$.

We can therefore suppose $q \leq 32$, whence $\omega_1 \leq 3$, $\omega_2 \leq 2$. Repeating the previous procedure (now with $s \leq 4$) we have $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \frac{1}{11} - \frac{1}{13} \geq 0.489$, $2W(k_0)\sqrt{2}\Delta_{s,\delta} < 46.02$. Hence (7.5) is satisfied whenever $q > 46.02^{\frac{2}{3}} = 12.84\ldots$. For $q \leq 8$, criterion (7.5) cannot be satisfied. Yet for $q = 8$ and 4 the necessary primitive quartics exist and are listed in the table below. Here $\mathbb{F}_4$ is defined by $x^2+x+1 \in \mathbb{F}_2[x]$ and $\mathbb{F}_8$ by $x^3+x^2+1 \in \mathbb{F}_2[x]$ and in each case α is a root of the defining polynomial. On the other hand, when $q = 2$, no primitive quartic with coefficient of x^2 equal to 1 exists!

a	$q = 8$	$q = 4$
1	$x^4+x^2+\alpha^2x+\alpha^2+\alpha+1$	$x^4+x^2+\alpha x+\alpha^2$
α	$x^4+\alpha x^2+x+6$	$x^4+\alpha x^2+\alpha x+\alpha$
$\alpha+1$	$x^4+(\alpha+1)x^2+(\alpha^2+\alpha)x+\alpha^2+1$	$x^4+(\alpha+1)x^2+\alpha x+\alpha$
α^2	$x^4+\alpha^2x^2+x+\alpha+1$	—
α^2+1	$x^4+(\alpha^2+1)x^2+(\alpha+1)x+\alpha^2+\alpha$	—
$\alpha^2+\alpha+1$	$x^4+(\alpha^2+\alpha+1)x^2+x+\alpha^2+1$	—
$\alpha^2+\alpha$	$x^4+(\alpha^2+\alpha)x^2+(\alpha^2+\alpha)x+(\alpha^2+\alpha)$	—

7.2. Quintics. Take $n = 5$. Then, for any decomposition (k_0, s) of q^5-1, (7.1) takes the form

$$q^2 > 2\sqrt{2}\, W(k_0)\Delta_{s,\delta}. \tag{7.6}$$

Write the product of distinct primes in q^5-1 as $K_1 \cdot K_2$, where K_1 (a factor of $q-1$) is the product of all distinct prime divisors of $q-1$ and K_2 (a factor of Q_5) is the product of distinct prime divisors of Q_5 that do not divide $q-1$. All prime divisors of K_2 are $\equiv 1 \pmod{10}$. Denote $\omega(q-1)$ by ω_1 and $\omega(K_2)$ by ω_2.

LEMMA 7.4. *Suppose q is even and $a \in \mathbb{F}_q^*$. Then there exists a primitive quintic over $\mathbb{F}_q$ with the coefficient of x^3 prescribed as a.*

Proof. First suppose $\omega_1 \geq 3$ and $\omega_2 \geq 2$. Then, by (9.2), and (9.6), $W(q^5-1) < q^{\frac{3}{2}} < \frac{q^2}{2\sqrt{2}}$ provided $q > 8$. Criterion (7.1) with $s = 1$ is satisfied since $q > 8$ when $\omega_1 \geq 3$.

Next, suppose $\omega_1 \leq 2$ and $\omega_2 \geq 2$. Take $k_0 = K_2$ so that $s \leq 2$, $\delta \geq 1 - \frac{1}{3} - \frac{1}{5} > 0.466$ and $2\sqrt{2}\Delta_{s,\delta} < 11.73 < q$ whenever $q \geq 12$. Thus (7.6) is satisfied unless $q \leq 8$.

Next, suppose $\omega_1 \geq 3$ (whence $q > 105$) and $\omega_2 \leq 1$. Criterion (7.6) (with $s = 1$) holds provided $q > 4$, which is the case.

Now, suppose $\omega_1 \leq 2$ and $\omega_2 \leq 1$. Take $k_0 = 1$ so that $s \leq 3$. Then $\delta > 0.375$ and $2\sqrt{2}\Delta_{s,\delta} < 20.75$. Thus (7.1) holds when $q > 4.6$. It also holds when $q = 2$ because of the factor $1 - \frac{1}{q}$ on the right side.

There remain $q = 8$ and 4. For $q = 8$, $q^5 - 1 = 7 \cdot 31 \cdot 151$ and (7.6) (with $s = 1$) holds since $64 > 16\sqrt{2}$. Although (7.6) cannot be satisfied, there does exist a primitive quintic $\mathbb{F}_4[x]$ with arbitrary coefficient of x^2. Over $\mathbb{F}_2$, any irreducible quintic is primitive: it is enough to quote the example $x^5 + x^3 + 1$. □

For $q = 2^m$, we again consider degrees 6, 7 and 8, but however, we do not present that to the reader in detail. The main reason is that, applying methods used with these degrees in Section 4, in only a couple of steps shows that Proposition 7.2 is satisfied for any value of q. The only exception is the value $q = 4$ for sextics, where polynomials are found explicitly. Let $\mathbb{F}_4$ be defined by $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ and let α be a root of f. Then the relevant primitive polynomials are:

a	$c = \alpha$	$c = \alpha + 1$
1	$x^6 + x^5 + x^4 + x^3 + \alpha x^2 + (\alpha+1)x + \alpha$	$x^6 + x^5 + x^4 + x^3 + \alpha x^2 + (\alpha+1)x + (\alpha+1)$
α	$x^6 + x^5 + \alpha x^4 + x^3 + \alpha$	$x^6 + x^5 + \alpha x^4 + x^3 + (\alpha+1)x + (\alpha+1)$
$\alpha + 1$	$x^6 + x^5 + (\alpha+1)x^4 + x^3 + \alpha x + \alpha$	$x^6 + x^5 + (\alpha+1)x^4 + x^3 + (\alpha+1)$

8. The even zero problem.

By Lemma 2.1, when the prescribed coefficient $a = 0$, it suffices to show that $\pi_0(Q_n)$ is positive, where $Q_n = \frac{q^n-1}{q-1}$.

PROPOSITION 8.1. *Assume that q is even. Let (k_0, s) be a decomposition of Q_n. Suppose that*

$$q^{\frac{n}{2}-1} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{8.1}$$

Then $\pi_0(Q_n)$ is positive.

Proof. This follows from Lemma 6.4 as in the proof of Lemma 7.1. The difference is that now the sum over α_0 is (trivially) $q - 1$ in every case. □

Degrees 6, 7 and 8 here are routine, therefore we focus on quartics and quintics.

8.1. Quartics.

Take $n = 4$. Then, for a decomposition (k_0, s) of Q_4, (8.1) has the form

$$q > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{8.2}$$

Express the product of distinct primes in Q_4 as $K_1 \cdot K_2$, where K_1 (a factor of $q + 1$) is the product of all distinct prime divisors of $q + 1$ and K_2 is the product of distinct prime divisors of $q^2 + 1$. Observe that K_1 and K_2 are coprime and all prime divisors of K_2 are $\equiv 1 \pmod 4$. Set $\omega_i = \omega(K_i)$, $i = 1, 2$.

LEMMA 8.2. *Suppose that $n = 4$, q even and $\omega_1 \geq 5$ or $\omega_2 \geq 7$. Then there exists a primitive polynomial of degree 4 over $\mathbb{F}_q$ with the coefficient of x^2 prescribed as $a = 0$.*

Proof. Suppose $\omega_1 \geq 5$ and $\omega_2 \geq 7$. Then, by (9.2) and Lemma (9.4), $W(Q_4) < q^{\frac{7}{5}}$. Consequently, by (5.2) to show existence it suffices that $q > 2^{15} = 32768$. This holds since $\omega_2 \geq 7$ and accordingly $q > 50000$.

Next, suppose $\omega_1 \leq 4$ and $\omega_2 \geq 7$. Let $k_0 = K_2$. Thus $s \leq 4$, $\delta \geq 1 - \frac{1}{3} - \frac{1}{5} - \frac{1}{7} - \frac{1}{11} > 0.232$ and $2\sqrt{2}\Delta_{s,\delta} < 42.24$. By the above reasoning, (5.3) is satisfied whenever $q \geq 42.24^2 = 1784.21\ldots.$ This is the case since $\omega_2 \geq 7$, whence $q > 50000$.

Finally, suppose $\omega_1 \geq 5$ and $\omega_2 \leq 6$. Take $k_0 = K_1$. Thus $s \leq 6$, $\delta \geq 1 - \frac{1}{5} - \frac{1}{13} - \frac{1}{17} - \frac{1}{29} - \frac{1}{37} - \frac{1}{41} > 0.578$ and $2\sqrt{2}\Delta_{s,\delta} < 30.13$. Now (5.3) is satisfied whenever $q \geq 30.13^{\frac{10}{11}} = 22.10\ldots$, which trivially is the case. □

We may now suppose $\omega_1 \leq 4$ and $\omega_2 \leq 6$. Take $\omega(k_0) = 1$; then $s \leq 9$, $\delta \geq 1 - \frac{1}{5} - \frac{1}{13} - \frac{1}{17} - \frac{1}{29} - \frac{1}{37} - \frac{1}{41} - \frac{1}{7} - \frac{1}{11} - \frac{1}{19} > 0.291$ and $2\sqrt{2}\Delta_{s,\delta} < 83.42$. Thus (5.3) is satisfied when $q \geq 83.42^{\frac{2}{3}} = 19.09$.

Finally, suppose $q \leq 16$. Then $\omega_1 = 1$ and $\omega_2 \leq 2$. Take k_0; then $s \leq 3$, $\delta > 0.389$ and $2\sqrt{2}\Delta_{s,\delta} < 20.2$. Thus (5.3) is satisfied when $q > 20.2^{\frac{2}{3}} = 7.41\ldots.$ Hence the theorem holds for $q \geq 4$. In fact, for $q = 4$, $Q_4 = 5 \cdot 17$ and $\delta > 0.741$ and $\Delta_{s,\delta} < 3.35$. Then (5.3) holds since $4 > (\frac{3}{4} \cdot 2\sqrt{2} \cdot 3.35)^{\frac{2}{3}} = 3.69\ldots.$ Over $\mathbb{F}_2$, $x^4 + x + 1$ is the desired primitive quartic.

8.2. Quintics. Take $n = 5$. For a decomposition (k_0, s) of $k|Q_5$, (8.1) now takes the form

$$q^{\frac{3}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{8.3}$$

Define $\omega = \omega(Q_5)$. Suppose $\omega \geq 4$. Then $W(Q_5) < 5^{\frac{5}{4}}$ (by (9.7)). To satisfy (8.3) (with $s = 1$) we require $q^{\frac{1}{4}} > 2\sqrt{2} > 64$. This certainly holds if $\omega \geq 6$ (so that $Q_5 \geq 5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 71$).

Accordingly, assume $\omega \leq 5$. Take $k_0 = 1$. Thus $s \leq 5$ and $\delta \geq 1 - \frac{1}{5} - \frac{1}{11} - \frac{1}{31} - \frac{1}{41} - \frac{1}{61} > 0.636$ and $2\sqrt{2}\Delta_{s,\delta} < 23.35$. Hence (8.3) is satisfied for $q \geq 23.35^{\frac{2}{3}} = 8.1\ldots.$ For $q \leq 8$, necessarily $5 \nmid Q_5$ and $\omega \leq 2$. Repeat the last process so that $\delta \geq 1 - \frac{1}{11} - \frac{1}{31} \geq 0.876$ and $2\sqrt{2}\Delta_{s,\delta} < 8.9$. Thus (8.3) is satisfied when $q > C := ((1 - \frac{1}{q})8.9)^{\frac{2}{3}}$. In fact, $C < 3.93$ so that the result holds for $q = 8, 4$. When $q = 2$ then $\omega = 1$ and (8.3) with $s = 1$ holds since $2\sqrt{2} > \sqrt{2}$.

9. Bounds for the number of square-free divisors.

Recall $W(h) = 2^{\omega(h)}$ denotes the number of square-free divisors of an integer h. In this section we provide some bounds for $W(h)$, used throughout the paper.

In this paper, we do not refer to all of the results below, for example the first two bounds in Lemma 9.3. However, they are stated here as the reader might find them useful when checking results for which explicit procedures are not given.

LEMMA 9.1. *Let the integer h be such that $\omega(h) \geq r$. Then the following statements hold*:

$$W(h) < \begin{cases} h^{\frac{3}{7}}, & when\ r = 6; \\ h^{\frac{1}{3}}, & when\ r = 9; \\ h^{\frac{13}{50}}, & when\ r = 15; \\ (h-1)^{\frac{1}{5}}, & when\ r = 28. \end{cases} \tag{9.1}$$

Furthermore, for an odd integer h with $\omega(h) \geq r$,

$$W(h) < \begin{cases} h^{\frac{1}{2}}, & when\ r = 3; \\ (h-1)^{\frac{2}{5}}, & when\ r = 5; \\ h^{\frac{1}{3}}, & when\ r = 8; \\ (h-1)^{\frac{5}{18}}, & when\ r = 10. \end{cases} \tag{9.2}$$

Proof. We illustrate (9.1) by proving, for the last part, $W(h) < (h-1)^{\frac{1}{5}} < h^{\frac{1}{5}}$. The 28th prime is 107. Let l be a prime number. Then

$$\frac{2^{\omega(h)}}{(h)^{\frac{1}{5}}} \leq \prod_{l|h} \frac{2}{l^{\frac{1}{5}}} \leq \prod_{l \leq 107} \frac{2}{l^{\frac{1}{5}}} < \frac{8}{9}.$$

It follows that $W(h) < (h-1)^{\frac{1}{5}}$ provided $h > (1 - (\frac{8}{9})^5)^{-1} = 2.2468\ldots$, which is trivially true. The rest of the bounds in Lemma 9.1 are proved analogously. □

The following lemmas feature slight refinements. Their proofs, however, are parallels to the proof of Lemma 9.1.

LEMMA 9.2. *Suppose that the integer h is a product of primes $l \equiv 1 \pmod 4$ and $\omega(h) \geq r$. Then the following statement holds*:

$$W(h) < \begin{cases} \left(h^{\frac{1}{2}} - 1\right)^{\frac{1}{2}}, & when\ r = 2; \\ h^{\frac{1}{5}}, & when\ r = 11; \\ h^{\frac{7}{50}}, & when\ r = 40. \end{cases} \tag{9.3}$$

Furthermore, for an odd integer h with $\omega(h) \geq 6$,

$$W(h) < (h-1)^{\frac{1}{4}}. \tag{9.4}$$

LEMMA 9.3. *Suppose that the integer h is a product of primes $l \equiv 1 \pmod 6$ and $\omega(h) \geq r$. Then the following is true*:

$$W(h) < \begin{cases} h^{\frac{1}{5}}, & when\ r = 12; \\ h^{\frac{9}{50}}, & when\ r = 15; \\ h^{\frac{10}{63}}, & when\ r = 24. \end{cases} \tag{9.5}$$

LEMMA 9.4. *Suppose that the integer h is a product of primes $l \equiv 1 \pmod{10}$ and $\omega(h) \geq r$. Then the statements below hold*:

$$W(h) < \begin{cases} \left(h^{\frac{1}{2}} - 1\right)^{\frac{1}{2}}, & \text{when } r = 2; \\ h^{\frac{1}{6}}, & \text{when } r = 10; \\ \left(h^{\frac{1}{2}} - 1\right)^{\frac{23}{80}}, & \text{when } r = 17. \end{cases} \tag{9.6}$$

Furthermore, when h is a product of primes $l \equiv 1 \pmod{10}$ or $l = 5$ and $\omega(h) \geq 4$, then

$$W(h) < \left(h^{\frac{1}{2}} - 1\right)^{\frac{1}{2}}. \tag{9.7}$$

LEMMA 9.5. *Suppose that the integer h is a product of primes $l \equiv 1 \pmod{14}$ and $\omega(h) \geq 6$. Then $W(h) < h^{\frac{1}{6}}$.*

LEMMA 9.6. *Suppose that the integer h is a product of primes $l \equiv 1 \pmod 8$ and $\omega(h) \geq 6$. Then $W(h) < (h-1)^{\frac{17}{100}}$.*

REFERENCES

1. S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discr. Math.* **83** (1990), 1–7.

2. S. D. Cohen, Gauss sums and a sieve for generators of Galois fields, *Publ. Math. Debrecen* **56** (2000), 293–312.

3. S. D. Cohen, Primitive polynomials over small fields, *Finite Fields and Applications. 7th International Conference, Toulouse* (2003), Lecture Notes in Mathematics No. 2948 (Springer-Verlag, 2004), 197–214.

4. S. D. Cohen, Primitive polynomials with a prescribed coefficient, *Finite Fields Appl.*, to appear.

5. S. D. Cohen, Explicit results on generator polynomials, *Finite Fields Appl.* **11** (2005), 337–357.

6. S. D. Cohen and S. Huczynska, The primitive normal basis theorem—without a computer, *J. London Math. Soc (2)* **67** (2003), 41–56.

7. S. D. Cohen and S. Huczynska, Primitive free quartics with specified norm and trace, *Acta Arith.* **109** (2003), 359–385.

8. S. D. Cohen and C. King, The three fixed coefficient primitive polynomial theorem, *JP J. Algebra Number Theory Appl.* **4** (2004), 79–87.

9. S. D. Cohen and D. Mills, Primitive polynomials with first and second coefficients prescribed, *Finite Fields Appl.* **9** (2003), 334–350.

10. S. D. Cohen and M. Prešern, Primitive finite field elements with prescribed trace, *Southeast Asian Bull. Math.* **29** (2005), 283–300.

11. S-Q. Fan and W-B. Han, p-adic formal series and primitive polynomials over finite fields, *Proc. Amer. Math. Soc.* **132** (2004), 15–31.

12. S-Q. Fan and W-B. Han, Primitive polynomials over finite fields of characteristic two, *Appl. Algebra Engrg. Comm. Comput.* **14** (2004), 381–395.

13. S.-Q. Fan and W.-B. Han, Character sums over Galois rings and primitive polynomials over finite fields, *Finite Fields Appl.* **10** (2004), 36–52.

14. S.-Q. Fan and W.-B. Han, Primitive polynomials with three coefficients prescribed, *Finite Fields Appl.* **10** (2004), 506–521.

15. K. H. Ham and G. L. Mullen, Distribution of irreducible polynomials of small degrees over finite fields, *Math. Comp.* **67** (1998), 337–341.

16. Han Wenbao, The coefficients of primitive polynomials over finite fields, *Math. Comp.* **65** (1996), 331–340.

17. T. Hansen and G. L. Mullen, Primitive polynomials over finite fields, *Math. Comp.* **59** (1992), 639–643, S47–S50.

18. S. Huczynska and S. D. Cohen, Primitive free cubics with specified norm and trace, *Trans. Amer. Math. Soc.* **355** (2003), 3099–3116.

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

20. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions* (Springer-Verlag, 1984).

21. W-C. W. Li, Character sums over p-adic fields, *J. Number Theory* **74** (1999), 181–229.

22. R. Lidl and H. Niederreiter, *Finite fields* (Addison-Wesley, 1983), *2nd edition* (Cambridge University Press, 1997).

23. D. Mills, Existence of primitive polynomials with three coefficients prescribed, *JP J. Algebra Number Theory Appl.* **4** (2004), 36–52.

24. G. L. Mullen, Open problems in finite fields, *Congr. Numer.* **111** (1995), 97–103.

25. G. L. Mullen and I. Shparlinski, Open problems and conjectures in finite fields, in *Finite fields and applications (Glasgow, 1995)*, London Math. Soc. Lecture Note Series No 233 (Cambridge University Press, 1996), 243–268.