Existence problems of primitive polynomials over finite fields

by

Mateja Prešern

A thesis submitted to the
Faculty of Information and Mathematical Sciences
at the University of Glasgow
for the degree of
Doctor of Philosophy

August 2007

Abstract

This thesis concerns existence of primitive polynomials over finite fields with one coefficient arbitrarily prescribed. It completes the proof of a fundamental conjecture of Hansen and Mullen (1992), which asserts that, with some explicable general exceptions, there always exists a primitive polynomial of any degree n over any finite field with an arbitrary coefficient prescribed. This has been proved whenever $n \geq 9$ or $n \leq 3$, but was unestablished for $4 \leq n \leq 8$.

In this work, we efficiently prove the remaining cases of the conjecture in a self-contained way and with little computation; this is achieved by separately considering the polynomials with second, third or fourth coefficient prescribed, and in each case developing methods involving the use of character sums and sieving techniques. When the characteristic of the field is 2 or 3, we also use p-adic analysis.

In addition to proving the previously unestablished cases of the conjecture, we also offer shorter and self-contained proof of the conjecture when the first coefficient of the polynomial is prescibed, and of some other cases where the proof involved a large amount of computation. For degrees $6 \leq n \leq 8$ and selected values of m, we also prove the existence of primitive polynomials with two coefficients prescribed (the constant term and any other coefficient).

Statement

This thesis is submitted in accordance with the regulations for the degree Doctor of Philosophy in the Faculty of Information and Mathematical Sciences, University of Glasgow. It is the record of research carried out at the University of Glasgow between October 2003 and August 2007. I have not previously submitted any part of this thesis for a degree at any other university.

The main results of this thesis are the outcome of my collaboration with my supervisor, Professor S. D. Cohen; in particular, much of Chapters 4, 5, 6 and 7 is joint work. The material of Chapters 4 and 5 has been published in [12] and [13] respectively, and the material of Chapters 6 and 7 has been accepted for publication in [14].

Acknowledgement

Firstly, I would like to express my gratitude to my supervisor, Professor S. D. Cohen. This thesis would not have been possible without his kind support and inspiration throughout the period of research.

I am grateful to the Faculty of Information and Mathematical Sciences for funding my research and to the Department of Mathematics for making it possible for me to attend and participate at numerous conferences and events, and for years of teaching experience, which was so enjoyable.

Lastly, and most importantly, for reasons so numerous and diverse that it is impossible to list them all, I wish to thank my family and my closest friends. To them I dedicate this thesis.

Contents

Chapter 1

Introduction

A *finite field* is a field containing a finite number of elements. For a prime number p and q a power of p, we will denote a field of q elements (or, equivalently, of *order* q) by $\mathbb{F}_q$, as customary. The multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic of order $q-1$. A generator of $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$ and a (necessarily monic and irreducible) polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is called a *primitive polynomial* over $\mathbb{F}_q$ if any of its roots is a generator of the multiplicative group $\mathbb{F}_{q^n}^*$ of $\mathbb{F}_{q^n}$.

For further details about finite fields please see Section 2.1.

1.1 The Hansen–Mullen primitivity conjecture

In 1992, T. Hansen and G. L. Mullen [19] stated a conjecture on the existence of a primitive polynomial of degree n over $\mathbb{F}_q$ with an arbitrary coefficient prescribed.

Conjecture 1.1.1 (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 $f(x) = x^n + \sum_{j=1}^{n} a_j x^{n-j}$ of degree n over $\mathbb{F}_q$ with $a_m = a$ with (genuine) exceptions when*

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

We shall refer to the Conjecture 1.1.1 as the Hansen–Mullen primitivity conjecture and, for simplicity, use the abbreviation HMPC throughout this work.

Though highly plausible, the conjecture is not easy to prove. There has been much interest in proving the HMPC and a number of researchers have contributed to its proof.

When $m = 1$, it was demonstrated by Cohen, [5] (see also [21]). This was also the only theoretical (non-numerical) evidence at the time the conjecture was published.

For $m = n - 1$, the conjecture follows from the work of Cohen, [6], and Cohen and Huczynska, [9], [20]. The papers of Han [18] and Cohen and Mills [11] cover most cases with $m = 2$ 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 papers by Fan and Han, [15], [16], Mills, [25] and Cohen and King [10]. When $m = 2$ or 3, however, significant computer verification in a large number of cases was necessary to resolve these questions, particularly when $5 \leq n \leq 7$. Next, the HMPC follows from [7] (Cohen) 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 was shown by Fan and Han [27] provided $n \geq 7$. Finally, the conjecture has been established by Cohen whenever $n \geq 9$, [8].

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 [8]). From the above summary, the outstanding cases all have $4 \leq n \leq 8$. In particular, the existence of a primitive quartic and quintic with the second coefficient prescribed ($m = 2$), a primitive quintic ($n = 5$), a primitive sextic ($n = 6$) and a primitive septic ($n = 7$) with the coefficient of x^3 prescribed ($m = 3$), as well as the existence of a primitive octic ($n = 8$) with the coefficient of x^4 prescribed ($m = 4$) has not been settled.

In this work, we consider the cases of the HMPC when $1 \leq m \leq 4$. The conjecture for a prescribed first coefficient ($m = 1$) has already been established by Cohen in 1990, but here we provide a self-contained and minimal computational account of his theorem. The proof of the HMPC for $2 \leq m \leq 4$, where the degrees of the polynomials we consider are $4 \leq n \leq 8$, also contains only a small amount of computation because of the quality of the result.

To provide the complete proof of the HMPC as quickly as possible, the recent results on the $1 \leq m \leq 4$ have already been presented at conferences and published as papers (Cohen, Prešern [12], [13], [14]).

Throughout the proof of the (remaining cases of the) HMPC, our aim is to identify the unique properties of the individual cases and apply up-to-date theory in order to derive efficient machinery to achieve optimal results and minimize the use of a computer.

The general strategy for the effective approach to the proof of the HMPC is to split

the problem into sub-problems:

- with respect to the coefficient we wish to prescribe
- with respect to the degree of the polynomial
- whether the prescribed coefficient is zero or non-zero
- with respect to the characteristic of the field.

Regarding the latter, a novel method employing p-adic analysis is employed.

The treatment of the various subproblems depends on the particular subproblem in question. In the subsection headings of the Chapters 4 - 7 this may be masked by the division into classes by the degree of the polynomial (cubics, quartics, quintics, etc.) since the approach used for a particular degree varies according to the other parameters in question.

The structure of this work follows the proof of the HMPC in a natural way. After introducing the basic theory and the general idea of the proof in Chapters 2 and 3, we prove the HMPC for $1 \leq m \leq 4$. Chapter 4 deals with $m = 1$; a result that has been established before, but here proved in a self-contained way with minimal use of a computer. Chapters 5, 6 and 7 are dedicated to the previously unestablished cases of the HMPC with $m = 2$, 3 and 4 respectively, giving a complete proof and hence establishing the conjecture in full. The final Chapter 8 reflects on the work in the previous chapters and outlines the possibilities for further research. Throughout the work we will be using some bounds for the number of square-free divisors of an integer. All of the bounds used have found their place in Appendix A. Finally, in Appendix B we gather all the primitive polynomials whose existence we could not prove theoretically in Chapters 5, 6 and 7.

Chapter 2

Basic theory and notation

The purpose of this chapter is introducing the notation which will be used throughout this work and assembling some core material. Thus this chapter will provide the foundation for the subsequent chapters by supplying definitions and well-established theoretical results, in general stated without proof. For any further details about the background material the reader may wish to refer to [24] or [22].

2.1 Finite fields

The definition of a finite field has been given at the beginning of the previous chapter; in this section we will gather some basic, though important theorems on finite fields, which provide the underlying foundation to the theory in the chapters that follow.

Theorem 2.1.1. *Let F be a finite field. Then F has p^n elements, where the prime p is the characteristic of F and n is the degree of F over its prime subfield. It is also called the* Galois field *of order p^n.*

A finite field is *prime* if and only if it has no proper subfields. Any field of order p, p prime, is a prime field.

Definition 2.1.2. *Let $f \in \mathbb{F}_q[x]$ be of positive degree and $\mathbb{F}_{q^n}$ an extension of $\mathbb{F}_q$. Then f is said to* split *in $\mathbb{F}_{q^n}$ if f can be written as a product of linear factors in $\mathbb{F}_{q^n}[x]$—that is, if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^n}$ such that*

$$f(x) = \alpha(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n),$$

where α is the leading coefficient of f. The field $\mathbb{F}_{q^n}$ is a splitting field *of f over $\mathbb{F}_q$ if f splits in $\mathbb{F}_{q^n}$ and if, moreover, $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

Theorem 2.1.3 (Existence and uniqueness of finite fields). *For every prime p and every positive integer n, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.*

A direct corollary of this theorem is that any two fields of equal order are isomorphic. This provides the justification for speaking of *the* finite field (or *the* Galois field) with q elements, or of *the* finite field (or *the* Galois field) of order q.

Theorem 2.1.4 (Subfield criterion). *Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^d, where d is a positive divisor of n. Conversely, if d is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with $q = p^d$ elements.*

Theorem 2.1.5 (Existence and uniqueness of splitting field). *If $\mathbb{F}_q$ is a field and f any polynomial of positive degree in $\mathbb{F}_q[x]$, then there exists a splitting field of f over $\mathbb{F}_q$. Any two splitting fields of f over $\mathbb{F}_q$ are isomorphic.*

Definition 2.1.6. *If $\alpha \in \mathbb{F}_{q^n}$ is algebraic over $\mathbb{F}_q$ (that is, if α satisfies a nontrivial polynomial equation with coefficients in $\mathbb{F}_q$), then the uniquely determined monic polynomial $g \in \mathbb{F}_q[x]$ generating the ideal $J = \{f \in \mathbb{F}_q[x] : f(\alpha) = 0\}$ of $\mathbb{F}_q[x]$ is called the* minimal polynomial *of α over $\mathbb{F}_q$ and the* degree *of α over $\mathbb{F}_q$ is the degree of g.*

Theorem 2.1.7. *If $\alpha \in \mathbb{F}_{q^n}$ is algebraic over $\mathbb{F}_q$, then its minimal polynomial g over $\mathbb{F}_q$ has the following properties:*

1. *g is irreducible in $\mathbb{F}_q[x]$.*
2. *For $f \in \mathbb{F}_q[x]$ we have $f(\alpha) = 0$ if and only if g divides f.*
3. *g is the monic polynomial in $\mathbb{F}_q[x]$ of least degree having α as a root.*

Theorem 2.1.8. *If f is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n, then f has a root α in $\mathbb{F}_{q^n}$. Furthermore, all the roots of f are simple and are given by the n distinct elements α, α^q, α^{q^2}, ..., $\alpha^{q^{n-1}}$ of $\mathbb{F}_{q^n}$.*

The elements α, α^q, α^{q^2}, ..., $\alpha^{q^{n-1}}$ of $\mathbb{F}_{q^n}$ are called the *conjugates* of α with respect to $\mathbb{F}_q$. The direct corollaries of the above theorem are that the splitting field of an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree n over $\mathbb{F}_q$ is given by $\mathbb{F}_{q^n}$, and that any two irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree have isomorphic splitting fields.

Theorem 2.1.9. *Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^n}$ a finite extension field. Then $\mathbb{F}_{q^n}$ is a simple algebraic extension of $\mathbb{F}_q$ and every primitive element of $\mathbb{F}_{q^n}$ can serve as a defining element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Corollary 2.1.10. *For every finite field $\mathbb{F}_q$ and every positive integer n, there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.*

Definition 2.1.11. *For $\alpha \in \mathbb{F}_{q^n}$, the* trace $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *over $\mathbb{F}_q$ is defined by*

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

In other words, the trace of α over $\mathbb{F}_q$ is the sum of the conjugates of α with respect to $\mathbb{F}_q$.

Theorem 2.1.12. *The trace function $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ satisfies the following properties:*

1. $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$ *for all* $\alpha, \beta \in \mathbb{F}_{q^n}$;
2. $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *for all* $c \in \mathbb{F}_q$ $\alpha \in \mathbb{F}_{q^n}$;
3. $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = n\alpha$ *for all* $\alpha \in \mathbb{F}_q$;
4. $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *for all* $\alpha \in \mathbb{F}_{q^n}$;
5. *for* $\alpha \in \mathbb{F}_{q^n}$, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ *if and only if* $\alpha = \beta^q - \beta$ *for some* $\beta \in \mathbb{F}_{q^n}$.

Definition 2.1.13. *For $\alpha \in \mathbb{F}_{q^n}$, the* norm $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *over $\mathbb{F}_q$ is defined by*

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}.$$

Theorem 2.1.14. *The norm function $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ satisfies the following properties:*

1. $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha \cdot \beta) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \cdot N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$ *for all* $\alpha, \beta \in \mathbb{F}_{q^n}$;
2. $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ *maps* $\mathbb{F}_{q^n}$ *onto* $\mathbb{F}_q$ *and* $\mathbb{F}_{q^n}^*$ *onto* $\mathbb{F}_q^*$.
3. $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha^n$ *for all* $\alpha \in \mathbb{F}_q$;
4. $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *for all* $\alpha \in \mathbb{F}_{q^n}$.

Definition 2.1.15. *Let n be a positive integer. Then the splitting field of the polynomial $x^n - 1$ over a field F is called the* n-th cyclotomic field *over F and denoted by $F^{(n)}$. The roots of $x^n - 1$ in $F^{(n)}$ are called the $n-th$* roots of unity over F *and the set of all these roots is denoted by $E^{(n)}$.*

The structure of $E^{(n)}$ is determined by the relation of n to the characteristic of F. When we refer to the characteristic p of F in this discussion, we permit $p = 0$ as well.

Definition 2.1.16. *Let F be a field of characteristic p and n a positive integer not divisible by p. Then a generator of the cyclic group $E^{(n)}$ is called a* primitive n-th root of unity *over F.*

Definition 2.1.17. *Let F be a field of characteristic p, n a positive integer not divisible by p, and ζ a primitive n-th root of unity over F. Then the polynomial*

$$Q_n(x) = \prod_{\substack{s=1 \\ gcd(s,n)=1}}^{n} (x - \zeta^s)$$

is called the n-th cyclotomic polynomial *over F.*

The polynomial $Q_n(x)$ is clearly independent of the choice of ζ. The degree of $Q_n(x)$ is $\phi(n)$ and its coefficients belong to the n-th cyclotomic field over F (ϕ being the Euler function). The following argument shows that they are actually contained in the prime subfield of F. We use the product symbol $\prod_{d|n}$ to denote a product extended over all positive divisors d of a positive integer n.

Theorem 2.1.18. *Let F be a field of characteristic p and n a positive integer not divisible by p. Then:*

1. $x^n - 1 = \prod_{d|n} Q_d(x)$;
2. *the coefficients of $Q_n(x)$ belong to the prime subfield of F, and to $\mathbb{Z}$ if the prime subfield of F is the field of rational numbers.*

Theorem 2.1.19. *The cyclotomic field $F^{(n)}$ is a simple algebraic extension of F. Moreover:*

1. *If $F = \mathbb{Q}$, then the cyclotomic polynomial Q_n is irreducible over F and $\left[F^{(n)} : F\right] = \phi(n)$.*
2. *If $F = \mathbb{F}_q$ with $\gcd(q, n) = 1$, then Q_n factors into $\frac{\phi(n)}{n}$ distinct monic irreducible polynomials in $F[x]$ of the same degree d, $F^{(n)}$ is the splitting field of any such irreducible factor over F, and $\left[F^{(n)} : F\right] = d$, where d is the least positive integer such that $q^d \equiv 1 \pmod{n}$.*

Theorem 2.1.20. *The finite field $\mathbb{F}_q$ is the $(q-1)$-th cyclotomic field over any of its subfields.*

2.2 Galois rings

The existence of Galois rings was already known to W. Krull in 1924 but it was only after more than forty years that they were independently rediscovered and studied (by G. Janusz and R. Raghavendran).

Generalizing finite fields, Galois rings find applications in similar areas: linear recurrences, cyclic codes, association schemes and character sums.

Here we summon some basic theory on Galois rings, enough to provide the foundations of the theory in Section 2.5. For a more detailed account, including proofs of the theorems given in this section, the reader might wish to refer to [28] or [1].

The definition of a Galois ring is as follows.

Definition 2.2.1. *Let q be a power of a prime p and let f be some monic polynomial modulo q, of degree r, which is irreducible modulo p. The* Galois ring *of characteristic q and rank r is defined as the unique Galois extension of $\mathbb{Z}/q\mathbb{Z}$ of degree n:*

$$GR(q,n) = (\mathbb{Z}/q\mathbb{Z})[x]/f(x).$$

The ring $R = GR(q,n)$ comprises units R^* and zero divisors pR. The multiplicative group R^* is the direct product of $T_n\backslash\{0\}$ by the group of so-called principal units $1+pR$. Here T_n is the Teichmüller set $\left\{0,1,\ldots,\xi,\ldots,\xi^{p^n-2}\right\}$, the set of roots of $x^{p^n-1}-1$. The group of principal units is isomorphic, for $e=2$ or $p>2$ (where $q=p^e$), to the additive group of $(\mathbb{Z}/p^{e-1}\mathbb{Z})^n$. The Galois group of R over $\mathbb{Z}/q\mathbb{Z}$ is isomorphic to the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ and is therefore cyclic of order n.

Let $f(x)$ be a monic polynomial of degree $n \geq 1$ in $\mathbb{Z}_{p^s}[x]$. If $\bar{f}(x)$, the image of $f(x)$ under a ring homomorphism $\mathbb{Z}_{p^s}[x] \to \mathbb{F}_p[x]$, is irreducible in $\mathbb{F}_p[x]$, $f(x)$ is called a *monic basic irreducible* polynomial in $\mathbb{Z}_{p^s}[x]$. (For more details, please see [28], Chapter 13).

Theorem 2.2.2. *Let R be a Galois ring of characteristic $q=p^s$ and cardinality $n=p^{st}$, where p is a prime number and s and t are positive integers. Then R is isomorphic to the ring $\mathbb{Z}_{p^s}[x]/(h(x))$ for any monic basic irreducible polynomial $h(x)$ of degree t over $\mathbb{Z}_{p^s}$.*

Corollary 2.2.3. *Any two Galois rings of the same characteristic and the same cardinality are isomorphic.*

Therefore we can use the notation $GR(q,n)$ to denote any Galois ring of characteristic q and cardinality n.

The following theorem gives an alternative representation of an element of $GR(q,n)$ (expression (2.2)). We call it the *p-adic representation* of the element of $GR(p^s,p^{st})$ and it is a generalization of the power representation of an element of $\mathbb{F}_{p^t}$.

Theorem 2.2.4. *1. In the Galois ring $GR(p^s,p^{st})$ there exists a nonzero element χ of order p^t-1, which is a root of a monic basic primitive polynomial $h(x)$ of degree t over $\mathbb{Z}_{p^s}$ and dividing $x^{p^t-1}-1$ in $\mathbb{Z}_{p^s}[x]$, and*

$$GR(p^s,p^{st})=\mathbb{Z}_{p^s}[\chi]=\left\{a_0+a_1\chi+\cdots+a_{t-1}\chi^{t-1}:a_0,a_1,\ldots,a_{t-1}\in\mathbb{Z}_{p^s}\right\}. \quad (2.1)$$

Moreover, $h(x)$ is the unique monic polynomial of degree $\leq t$ over $\mathbb{Z}_{p^s}$ and having χ as a root.

2. Let $\tau=\left\{0,1,\chi,\chi^2,\ldots,\chi^{p^t-2}\right\}$. Then any element $c\in GR(p^s,p^{st})$ can be written uniquely as

$$c=a_0+a_1p+\cdots+a_{s-1}p^{s-1}, \quad (2.2)$$

where $a_0,a_1,\ldots,a_{s-1}\in\tau$. Moreover, c is a unit if and only if $a_0\neq 0$, and c is a zero divisor or 0 if and only if $a_0=0$.

2.3 Characteristic functions and character sums estimates

A basic role in setting up exponential sums for finite fields (and Galois rings) is played by special group homomorphisms called *characters*. It is necessary to distinguish between two types of characters — namely, additive and multiplicative characters — depending on whether reference is made to the additive or the multiplicative group of the finite field, say. Exponential sums are formed by using the values of one or more characters and possibly combining them with weights or with other function values. If we only sum the values of the single character, we speak of a character sum.

Definition 2.3.1. *Let G be a finite abelian group of order $|G|$ with identity element 1_G. A* character *χ of G is a homomrphism from G into the multiplicative group U of complex numbers of absolute value 1 — that is, a mapping from G into U with $\chi(g_1g_2)=\chi(g_1)\chi(g_2)$ for all $g_1,g_2\in G$.*

Remarks.

1. Since $\chi(1_G)=\chi(1_G)\chi(1_G)$, we must have $\chi(1_G)=1$. Furthermore,

$$(\chi(g))^{|G|}=\chi(g^{|G|})=\chi(1_G)=1$$

for every $g \in G$, so that the values of χ are $|G|$-th roots of unity.

2. Note that $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$, and so $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$ for every $g \in G$, where the bar denotes complex conjugation.

Among the characters of G we have the *trivial* character χ_0 defined by $\chi_0(g) = 1$ for all $g \in G$; all other characters of G are called *nontrivial*. With each character χ of G there is associated the *conjugate* character $\bar{\chi}$ defined by $\bar{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$.

Theorem 2.3.2. *If χ is a nontrivial character of the finite abelian group G, then*

$$\sum_{g \in G} \chi(g) = 0. \tag{2.3}$$

If $g \in G$ with $g \neq 1_G$, then

$$\sum_{\chi \in \widehat{G}} \chi(g) = 0, \tag{2.4}$$

where $\widehat{G}$ is the (finite) set of characters of G.

Remark. The number of characters of a finite abelian group G is equal to $|G|$.

2.4 Gauss sums

Definition 2.4.1. *Let ψ be a multiplicative and χ an additive character of $\mathbb{F}_q$. Then the* Gauss sum $G(\psi, \chi)$ *is defined by*

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c).$$

The absolute value of a Gauss sum over $\mathbb{F}_q$ can be at most $q-1$, but is generally much smaller.

Let ψ_0 be the trivial multiplicative and χ_0 the trivial additive characters which satisfy $\psi_0(c) = 1$ and $\chi_0(c) = 1$ for all $c \in \mathbb{F}_q^*$ and all $c \in \mathbb{F}_q$, respectively.

Theorem 2.4.2. *Let ψ be a multiplicative and χ an additive character of $\mathbb{F}_q$. Then the Gauss sum $G(\psi, \chi)$*

$$G(\psi, \chi) = \begin{cases} q-1 & \text{for } \psi = \psi_0, \chi = \chi_0; \\ -1 & \text{for } \psi = \psi_0, \chi \neq \chi_0; \\ 0 & \text{for } \psi \neq \psi_0, \chi = \chi_0. \end{cases} \tag{2.5}$$

If $\psi \neq \psi_0$ and $\chi \neq \chi_0$, then

$$|G(\psi, \chi)| \ = \ q^{\frac{1}{2}}. \tag{2.6}$$

For proof see [24], Theorem 5.11.

2.5 p-adic analysis

Definition 2.5.1. *Let p be a prime number and x an arbitrary non-zero rational number. Then x can be written in the form*

$$x = p^{v_p(x)} \cdot x_1$$

where $x_1 \in \mathbb{Q}$, x_1 coprime to p. We define the p-adic absolute value of x *as*

$$|x|_p = p^{-v_p(x)}.$$

We (have to) set $|0|_p = 0$. Then $|.|_p$ is a norm on $\mathbb{Q}$.

Remark. It is easy to check that $|.|_p$ is a norm on $\mathbb{Q}$. In fact, $|.|_p$ satisfies the triangular inequality in the sharper form

$$|x + y|_p \leq max\{|x|_p, |y|_p\}. \tag{2.7}$$

Equality holds in (2.7) whenever $|x|_p \neq |y|_p$.

Theorem 2.5.2 (Ostrowski, 1918). *Every non-trivial norm $\|.\|$ on $\mathbb{Q}$ is equivalent to $|.|_p$ for some prime p or the usual absolute value.*

For proof see [26], Theorem 3.1.

Let $R = \{(a_n),\ a_n \in \mathbb{F}, \forall n \in \mathbb{N}, (a_n)$ Cauchy sequence$\}$. One can define addition and multiplication with respect to $|.|_p$ pointwise, by setting

$$\begin{aligned} (a_n) + (b_n) &= (a_n + b_n) \\ (a_n) \cdot (b_n) &= (a_n \cdot b_n) \end{aligned}$$

Then, $(R, +, \cdot)$ is a commutative ring. (This is easy to see.) Moreover, $M = \{(a_n) \in R | \lim_{n\to\infty} a_n = 0\}$ is a maximal ideal.

It is not difficult to see M is an ideal, but let us check it is maximal.

Suppose I is an ideal of ring R, $M \subset I$. Choose $(a_n) \in I, (a_n) \notin M$. Since (a_n) is a Cauchy sequence, so is $(\frac{1}{a_n})$, but $(\frac{1}{a_n}) \notin I$. Since $(a_n) \in I$ and I is an ideal, then $(c_n) = (a_n) \cdot (\frac{1}{a_n}) \in I$ and $\lim_{n\to\infty} c_n = 1$.

Now take any $(b_n) \in R$.

$\lim_{n\to\infty} [(b_n) - (b_n) \cdot (c_n)] = 0$ and therefore $[(b_n) - (b_n) \cdot (c_n)] \in M \ \Rightarrow \ (b_n) \in I \ \Rightarrow \ I = R$.

Consequently, $R/_M$ is a field.

We can embed $\mathbb{F}$ in R via the map

$$a \mapsto (a, a, a, \ldots) \qquad \forall a \in \mathbb{F}$$

which is clearly a Cauchy sequence. We can therefore view $\mathbb{F}$ as a subfield of $R/_M$. We call $R/_M$ *the completion* of $\mathbb{F}$ with respect to $\|.\|$.

Example 2.5.3. *When $\mathbb{F} = \mathbb{Q}$ with the usual absolute value, this construction gives $\mathbb{R}$. When $\mathbb{F} = \mathbb{Q}$ with $|.|_p$, we get* the field of p-adic numbers*: $\mathbb{Q}_p$.*

We can extend the concept of norm to $\mathbb{Q}_p$ in the following way:

$$\forall a = (a_n) \in \mathbb{Q}_p, \quad |a|_p = \lim_{n\to\infty} |a_n|_p$$

(The sequence (a_n) has a limit since it is a Cauchy sequence of real numbers and $\mathbb{R}$ is complete.)

Moreover, $\mathbb{Q}_p$ is complete with respect to $|.|_p$.

Definition 2.5.4. *The set $\mathbb{Z}_p = \{x \in \mathbb{Q}_p |\ |x|_p \leq 1\}$ is a subring of $\mathbb{Q}_p$, called* the ring of p-adic integers*.*

Remark. The subset $N = \{x \in \mathbb{Z}_p |\ |x|_p < 1\}$ is a maximal ideal of $\mathbb{Z}_p$.

Thus every element $x \in M$ satisfies $v_p(x) \geq 1$ and so we deduce $M = p\mathbb{Z}_p$. Moreover, every non-trivial ideal of $\mathbb{Z}_p$ is a power of M.

Given $x \in \mathbb{Q}$ satisfying $|x|_p \leq 1$ and any $i \in \mathbb{N}$, we can find a positive integer $a_i : \ 0 \leq a_i < p^i$ such that $|x - a_i| \leq p^{-i}$.

Indeed, write $x = \frac{a}{b}$ in its lowest terms. As $|x|_p \leq 1$, p and b are coprime, so there

$$\exists u, v \in \mathbb{Z} : \quad ub + vp^i = 1.$$

Let $a_i = ua$. Then

$$\begin{aligned} |a_i - x|_p &= |ua - x|_p = \\ &= |ua - \frac{a}{b}|_p = \\ &= |\frac{a}{b}|_p \cdot |ub - 1|_p \leq \\ &\leq p^{-i}. \end{aligned}$$

We can translate a_i by a multiple of p^i to ensure $0 \leq a_i < p^i$ and the above inequalities are not altered.

The above observations imply that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Thus, we can think of elements of $\mathbb{Z}_p$ as formal power series

$$\sum_{n=0}^{\infty} b_n p^n, \qquad 0 \leq b_n \leq p-1.$$

Given any $x \in \mathbb{Q}_p$, we can find p^N such that $|p^N \cdot x|_p \leq 1$ so that every element of $\mathbb{Q}_p$ can be thought of as a formal power series

$$\sum_{n=-N}^{\infty} b_n p^n, \qquad 0 \leq b_n \leq p-1.$$

The p-adic expansion of x is easily checked to be unique.

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 $\mathbb{Q}_p$ (the completion of the rational field with respect to the p-adic metric).

Introduce definitions and notation as follows.

- K_n is the splitting field of the polynomial $x^{q^n} - x$ over $\mathbb{Q}_p$.
- 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 $\Gamma_n \subseteq R_n = \left\{ \sum_{i=0}^{\infty} p^i \gamma_i,\ \gamma_i \in \Gamma_n \right\}$. Moreover, R_n is a local ring with unique maximal ideal pR_n and $R_n/pR_n \cong \mathbb{F}_{q^n}$.
- Distinct elements of Γ_n are already distinct modulo p. 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 $\sum_{i=0}^{\infty} p^i \gamma_i$, $\gamma_i \in \mathcal{G}_n$, 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 p^e, i.e., $\Gamma_{n,e} =$

$\left\{\sum_{i=0}^{e-1} p^i\gamma_i,\ \gamma_i \in \mathcal{G}_n\right\}$, 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, $\mathcal{G}_n = \Gamma_{n,1} \cong \mathbb{F}_{q^n}$.

- $R_{n,e} = \left\{\sum_{i=0}^{e-1} p^i\gamma_i, \gamma_i \in \Gamma_{n,e}\right\} \cong R_n/p^eR_n$, so that $R_{n,e}$ is a finite ring with cardinality q^{ne}. Thus $R_{n,e}$ is a *Galois ring* $GR(p^e, n)$ (see Section 2.2). Observe that here $R_{n,e}/pR_{n,e} \cong \mathbb{F}_{q^n}$ also. Moreover, $R_{n,1} = \Gamma_{n,1}$, 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 $\mathbb{F}_{q^n}/\mathbb{F}_q$. 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, $\tau_n\left(\sum_{i=0}^{\infty} p^i\gamma_i\right) = \sum_{i=0}^{\infty} p^i\gamma_i^q$ (where each $\gamma_i \in \Gamma_n$). This induces a ring homomorphism τ_n on $R_{n,e}$ such that $\tau_n\left(\sum_{i=0}^{e-1} p^i\gamma_i\right) = \sum_{i=0}^{e-1} p^i\gamma_i^q$ (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

$$f(x) = (x-\gamma)(x-\gamma^q)\cdots(x-\gamma^{q^{d-1}}) = x^d - \sigma_1 x^{d-1} + \cdots + (-1)^d\sigma_d, \qquad (2.8)$$

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 (2.8) 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 is 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, (2.8) holds with $d = n$. Here σ_i denotes the i-th symmetric function of the roots $\gamma, \gamma^q, \ldots, \gamma^{q^n-1}$. Employing the trace, we have that s_i, the sum of the i-th powers of the roots of f, is given by $s_i = T_n(\gamma^i) \in R$. 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 $R_e[x]$. For our purposes, we require an expression for the p-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 positive integer $\not\equiv 0 \pmod{p}$. Note from above that, for any such t, the value of s_{tp^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 $s_t = \sum_{j=0}^{\infty} s_{t,j} p^j,\ s_{t,j} \in \Gamma_1$, whence $s_t^{(i)} = \sum_{j=0}^{\infty} s_{t,j}^{2^i} p^j$. Since each positive integer L can be uniquely expressed as $L = tp^j$, then any *component* $s_{t,j}$ is uniquely associated with the integer tp^j.

Chapter 3

Prescribing the m-th coefficient: preliminaries

3.1 Bounds for the number of square-free divisors

Throughout Chapters 4 - 7, we will need to estimate the number of square-free divisors of certain factors of $q^n - 1$, the order of $\mathbb{F}_{q^n}^*$. To assist us with that, we will derive bounds for the number of square-free divisors of an integer h. These bounds are, of course, not constant, but depend on h. We will write $W(h)$ for the number of square-free divisors of an integer h. Recall that $W(h) = 2^{\omega(h)}$, where $\omega(h)$ is the number of *distinct* prime divisors of an integer h.

Obtaining a lower bound for $W(q^n - 1)$ (or for the number of square-free divisors of appropriately chosen factors of $q^n - 1$) at a fixed n allows us to prove the HMPC for an infinite number of values of q, giving a tamer set of values of q for which the HMPC is yet to be established. It is therefore important to carefully factor $q^n - 1$ and closely bound the number of square-free divisors of its factors for optimal results.

The choice of the factors of $q^n - 1$ we consider largely, but not solely, depends on the degree n. For example, when $n = 8$ is the degree of the polynomial over $\mathbb{F}_q[x]$, we need not consider the factor $q-1$ of q^8-1 if the m-th coefficient we are prescribing is 0, and we split the rest into $(q^3 + q^2 + q + 1) \cdot (q^4 + 1)$. This factorization is advantageous because, as we will see later, the divisors of $q^4 + 1$ are either 2 or congruent to 1 (mod 8) and taking this into the account, $W((q^3 + q^2 + q + 1)(q^4 + 1))$ can be evaluated more efficiently. Here it is worth pointing out that, when estimating $W(q^3 + q^2 + q + 1)$ and $W(q^4 + 1)$, for example, the lower bounds for $\omega(q^3 + q^2 + q + 1)$ and $\omega(q^4 + 1)$ need to be chosen consistently: so,

that the lower bounds for the value of q they yield are as close as possible.

All the bounds for the number of square-free divisors used in this work are collected in the Appendix A. As an illustration, we below give a sample proofs for two of the bounds used later on; the other estimates are derived analogously.

Lemma 3.1.1. *Let h be a positive integer and $\omega(h) \geq 13$. Then $W(h) < h^{\frac{3}{11}}$.*

Proof. The 13-th prime is 41. For l prime and $l \geq 41$, $l^{\frac{3}{11}} > 2$ and so, by calculation,

$$\frac{2^{\omega(h)}}{h^{\frac{3}{11}}} \leq \prod_{l|h} \frac{2}{l^{\frac{3}{11}}} \leq \prod_{l \leq 41} \frac{2}{l^{\frac{3}{11}}} < 1.$$

□

Lemma 3.1.2. *Let h be a positive integer and $\omega(h) \geq 28$. Then $W(h) < (h-1)^{\frac{1}{5}} < h^{\frac{1}{5}}$.*

Proof. The 28-th 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 $h > \left(1 - \left(\frac{8}{9}\right)^5\right)^{-1} = 2.2468...$, which is trivially true. □

In Chapter 4, we will also use a slightly different bound for $W(h)$ of the following kind. The proof is obvuous, using multiplicativity.

Lemma 3.1.3. *For any positive integer h,*

$$W(h) \leq C \cdot h^{\frac{1}{4}},$$

where $C = \dfrac{2^r}{(p_1 \dots p_r)^{\frac{1}{4}}}$, and $p_1, \dots, p_r$ are the distinct primes less than 16 which divide h.

We will, in particular, require the following bounds for C:

- For h an arbitrary integer,

$$C \leq \frac{2^6}{(2 \cdot 3 \cdots 13)^{\frac{1}{4}}} < 4.9; \tag{3.1}$$

- for r odd,

$$C \leq \frac{2^5}{(3\cdots 13)^{\frac{1}{4}}} < 2.9; \tag{3.2}$$

- for $3 \nmid r$,

$$C \leq \frac{2^5}{(2\cdot 5\cdots 13)^{\frac{1}{4}}} < 3.2. \tag{3.3}$$

3.2 Newton's formula

From a formula of Newton follows a remarkable and important relationship between the symmetric function of the roots of an irreducible polynomial and the traces of powers of the roots.

For a $f(x) \in F[x]$, $f(x) = (x - x_1)(x - x_2)\cdots(x - x_n)$, the *m-th symmetric function* is defined as follows:

$$\sigma_m = \sum_{1\leq i_1<\cdots<i_m\leq n} x_{i_1}\cdots x_{i_m}; \quad m = 1, 2, \ldots, n.$$

Lemma 3.2.1 (Newton's formula). *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 $1 \leq t \leq m$, denote by s_t the E/F-trace of γ^t. Then the m-th symmetric function σ_m of the roots of f satisfies*

$$(-1)^{m-1}m\sigma_m = s_m - s_{m-1}\sigma_1 + s_{m-2}\sigma_2 + \cdots + (-1)^{m-1}s_1\sigma_{m-1}. \tag{3.4}$$

3.3 The sieving method

Throughout take $Q = \dfrac{q^n - 1}{q - 1}$ and, for any integer r, denote by $\Theta(r)$ the ratio $\dfrac{\phi(r)}{r}$, where ϕ is the Euler function.

Let $d|q$. We say an element $\xi \in \mathbb{F}_{q^n}$ is not a d-th power in $\mathbb{F}_{q^n}$, if, for any $\alpha \in \mathbb{F}_{q^n}$, $\xi = \alpha^d$ yields $d = 1$. 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 3.3.1. *Suppose that an (irreducible) polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n has m-th 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 m-th 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 $q - 1 = q_1 q_2$, 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 3.3.1, 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.

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

$$\delta \;:=\; 1 - \sum_{i=1}^{s} \frac{1}{p_i}, \tag{3.5}$$

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 3.3.2. *For any divisor k 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*

$$\pi(k) \geq \left(\sum_{i=1}^{s} \pi(k_0 p_i)\right) - (s-1)\pi(k_0) \tag{3.6}$$

$$= \delta\pi(k_0) + \sum_{i=1}^{s} \left(\pi(k_0 p_i) - \left(1 - \frac{1}{p_i}\right)\pi(k_0)\right). \tag{3.7}$$

Proof. The results are trivial for $s = 1$. The basic sieving inequality (3.6) 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 (3.7) is a useful rearrangement of the right side of (3.6). □

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 a given decomposition (k_0, s) define

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

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

Chapter 4

The trace coefficient

In this chapter, we show the existence of a primitive polynomial of a given degree n over a given finite field $\mathbb{F}_q$ with the first coefficient (i.e. that of x^{n-1}) arbitrarily prescribed. We call that coefficient the *trace coefficient*, or simply the *trace* (of a polynomial). The reason for that is because, for $\alpha \in \mathbb{F}_{q^n}$, the coefficient of x^{n-1} of a minimal polynomial of α over $\mathbb{F}_q$ is $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

This chapter stands apart from the subsequent ones, not only because the result here has already been proved almost two decades ago (although the proof we offer here is much sleeker and requires very little computation), but also because we use a surprisingly different approach in showing the existence of primitive polynomials. While the basic idea behind the proof is the same, we have to employ results like the Stickelberger's and the Davenport-Hasse theorem, and need to separately treat a fan of distinct cases - perhaps more than one would expect at first. On the other hand, the use of p-adic analysis is not required here.

Our aim in this chapter is to give a self-contained, instantly-checkable version of the proof of Theorem 4.1.1 below. Although it suffices as to its truth in [5], as part of a greater programme it is preferable that it should be derived in an efficient and transparent manner. Until 2005 (when the results presented in this chapter have been published in a paper (see [12])) this was not so for the following reasons.

- The most delicate cases, namely primitive polynomials of degree two and primitive polynomials with zero trace, were deduced from prior separate investigations on quadratic extensions [3] and on cyclic difference sets [4]. It was desirable that there should be a unified proof: this is now fulfilled.

- Larger values of n are given scant attention in [5]. It should be obvious that the method extends to these (and indeed it does). Nevertheless, they can be settled by short conclusive arguments, which are now given.

- Implicitly, in [5] (in the difference set discussion), there are a few cases which, effectively, were treated by direct verification. In every other case it is shown that some (theoretically established) numerical criterion for existence is indeed satisfied. Nevertheless, the reader has to take on trust thousands of numerical calculations. We here improve the sieving techniques, and the reader with a basic calculator can quickly check everything within the course of studying this chapter. Moreover, there are no longer instances where existence of a primitive polynomial with a prescribed trace has to be verified by direct construction.

4.1 Main results

When the HMPC was originally published in 1992, the only non-numerical evidence underpinning the conjecture was the following theorem (1990). (In [21], D. Jungnickel and S.A. Vanstone give an independent result in the same direction, but though substantial, it is incomplete.) It establishes the conjecture for a prescribed first coefficient (that is, the coefficient of x^{n-1} or *trace* coefficient) and exposes genuine exceptions when $q = 4$ and $n = 3$, or when $n = 2$ and the prescribed coefficient is zero.

Theorem 4.1.1 (Cohen, [5]). *Let $n \geq 2$ and a be an arbitrary member of $\mathbb{F}_q$, with $a \neq 0$ if $n = 2$ or if $n = 3$ and $q = 4$. Then there exists a primitive element in $\mathbb{F}_{q^n}$ with trace a. Equivalently, there exists a primitive polynomial of degree n over $\mathbb{F}_q$ with trace a.*

4.2 Expressions and sieving bounds for $\pi(k)$

For any $k|q^n - 1$, let $\pi(k)$ and $\pi_0(k)$ denote the number of k-free elements of $\mathbb{F}_{q^n}$ whose characteristic polynomial has trace coefficient $a \neq 0$ and $a = 0$, respectively. We will derive expressions for $\pi(k)$ and $\pi_0(k)$ and apply the sieving theorem (Lemma 3.3.2). In the derivation, we use two standard results as follows.

Lemma 4.2.1 (Davenport-Hasse Theorem; [24], Theorem 5.14**).** *Let χ be an additive and ψ a multiplicative character of $\mathbb{F}_q$, not both of them trivial. Suppose χ and ψ are lifted to characters χ' and ψ', respectively, of the finite extension field E of $\mathbb{F}_q$ with $[E:\mathbb{F}_q]=s$. Then*

$$G(\psi',\chi') = (-1)^{s-1}G(\psi,\chi)^s.$$

Lemma 4.2.2 (Stickelberger's Theorem; [24], Theorem 5.16**).** *Let q be a prime power, let ψ be a nontrivial multiplicative character of $\mathbb{F}_{q^2}$ of order k dividing $q+1$, and let χ_1 be a canonical additive character of $\mathbb{F}_{q^2}$. Then,*

$$G(\psi,\chi_1) = \begin{cases} q & \text{if } k \text{ odd or } \frac{q+1}{k} \text{ even,} \\ -q & \text{if } k \text{ even and } \frac{q+1}{k} \text{ odd.} \end{cases}$$

Now recall that, as a consequence of Lemma 3.3.1, we can assume that $k|Q=\frac{q^n-1}{q-1}$ if $a=0$, and that k_Q signifies the greatest divisor of k such that Q and $\frac{k}{k_Q}$ are co-prime. Furthermore, we introduce the following notation.

For $d|k$, we will use η_d for a (typical) multiplicative character of $\mathbb{F}_{q^n}$ of (exact) order d with the convention that $\eta_d(0)=0$ (even when $d=1$). Let $G_n(\eta_d)$ be the Gauss sum on $\mathbb{F}_{q^n}$ formed from η_d and the canonical additive character χ on $\mathbb{F}_{q^n}$: thus $G_n(\eta_d)=\sum_{x\in\mathbb{F}_{q^n}}\eta_d(x)\chi(x)$ (see Section 2.4). In particular, if χ_d is trivial (i.e., $d=1$), then $G_n(\eta_d)=\sum_{x\in\mathbb{F}_{q^n}^*}\chi(x)=-\chi(0)=-1$.

By $\hat{\eta}_d$, we denote the restriction of η_d to $\mathbb{F}_q$: as such it is a multiplicative character of order $\dfrac{d}{\gcd\left(d,\frac{q^n-1}{q-1}\right)}$. It follows that, if $d|k_Q$, then $\hat{\eta}_d$ is the trivial character on $\mathbb{F}_q$.

From now on (also in the subsequent chapters), we will adopt the following notation for weighted sums:

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

where the sum $\sum_{(d)}\eta_d$ runs over all $\phi(d)$ multiplicative characters of $\mathbb{F}_{q^n}$ of order d and μ is the Möbius function given by

$$\mu(d) = \begin{cases} 1 & \text{if } d=1, \\ (-1)^s & \text{if } d \text{ is a product of } s \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

Observe that only square-free divisors d have any influence in $\int_{d|k}\eta_d$.

Lemma 4.2.3. *For k a divisor of q^n-1 and $\xi \in \mathbb{F}_{q^n}$,*

$$\int_{d|k} \eta_d(\xi) = \begin{cases} \frac{k}{\phi(k)} & \text{if } \xi \text{ is not a } k\text{-th power,} \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

Proof. Let k be a divisor of q^n-1 and $\xi \in \mathbb{F}_{q^n}$. Let l run through all the distinct prime divisors of k and suppose ξ is not a k-th power in $\mathbb{F}_{q^n}$. Then

$$\begin{aligned} \int_{d|k} \eta_d(\xi) &= \prod_{l|k} \left(1 + \frac{\mu(l)}{\phi(l)} \sum_{(l)} \eta_l(\xi)\right) \\ &= \prod_{l|k} \left(1 + \frac{1}{\phi(l)}\right) \\ &= \frac{k}{\phi(k)} \ . \end{aligned}$$

Now suppose that ξ is a k-th power in $\mathbb{F}_{q^n}$. Then there exists a prime l such that $l|\frac{k}{\mathrm{ord}(\xi)}$ so that $\sum_{(l)} \eta_l(\xi) = \phi(l)$, thus

$$\int_{d|k} \eta_d(\xi) = \prod_{l|k} \left(1 + \frac{\mu(l)}{\phi(l)} \sum_{(l)} \eta_l(\xi)\right) = 0 \ .$$

□

The following lemma is an important tool in estimating the number of k-free elements.

Lemma 4.2.4. *Suppose $a \neq 0$ is given and $k|q^n-1$. Then*

$$\pi(k) = \frac{\Theta(k)}{q} \left(q^n \ + \ \int_{\substack{d|k \\ d\nmid k_Q}} \hat{\eta}_d(a) \bar{G}_1\left(\hat{\eta}_d\right) G_n(\eta_d) \ - \ \int_{\substack{d|\, k_Q \\ d>1}} G_n\left(\eta_d\right) \right).$$

Suppose $a = 0$ and $k|Q$. Then

$$\pi_0(k) = \frac{\Theta(k)}{q} \left(q^n - q + (q-1) \int_{\substack{d|k \\ d>1}} G_n\left(\eta_d\right) \right).$$

Proof. By multiplying the characteristic function over the field $\mathbb{F}_{q^n}$, of elements that have trace a over $\mathbb{F}_q$, with that for elements that are k-free, we obtain

$$\begin{aligned} \pi(k) &= \frac{\Theta(k)}{q} \sum_{d|k} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \sum_{c\in\mathbb{F}_q} \sum_{w\in\mathbb{F}_{q^n}} \lambda\left(c\cdot(T(w)-a)\right) \eta_d(w) \\ &= \frac{\Theta(k)}{q} \int_{d|k} \sum_{c\in\mathbb{F}_q} \sum_{w\in\mathbb{F}_{q^n}} \lambda\left(c\cdot(T(w)-a)\right) \eta_d(w) \\ &= \frac{\Theta(k)}{q} \int_{d|k} \sum_{c\in\mathbb{F}_q} \sum_{w\in\mathbb{F}_{q^n}} \left[\lambda\left(c\cdot T(w)\right)\cdot\bar{\lambda}(ca)\right] \eta_d(w). \end{aligned} \tag{4.2}$$

Here λ is the canonical additive character on $\mathbb{F}_q$: $\lambda(x) = e^{\frac{2\pi i T_0(x)}{p}}$ (q is a power of the prime p), where T_0 denotes the absolute trace $T_0 : \mathbb{F}_q \to \mathbb{F}_p$.

The contribution to

$$\int_{d|k} \sum_{c\in\mathbb{F}_q} \sum_{w\in\mathbb{F}_{q^n}} \left[\lambda\left(c\cdot T(w)\right)\cdot\bar{\lambda}(ca)\right]\eta_d(w)$$

in (4.2) of the terms with $c = 0$ or $d = 1$ is

$$\sum_{d|k}\frac{\mu(d)}{\phi(d)}\sum_{(d)}\sum_{w\in\mathbb{F}_{q^n}}\eta_d(w) + \sum_{c\in\mathbb{F}_q^*}\bar{\lambda}(ac)\sum_{w\in\mathbb{F}_{q^n}^*}\chi(cw) = q^n - 1 + \sum_{c\in\mathbb{F}_q*}\bar{\lambda}(ac),$$

which has value q^n when $a \neq 0$, and $q^n - q$ when $a = 0$.

Now assume $c \neq 0$ and $d \neq 1$. Write $\lambda\left(c\cdot T(w)\right) = \lambda\left(T(cw)\right) = \chi(cw)$, χ being the canonical additive character on $\mathbb{F}_{q^n}$. Then (4.2) takes the form

$$\begin{aligned}\pi(k) &= \frac{\Theta(k)}{q}\left(q^n + \int_{\substack{d|k\\ d>1}}\sum_{c\in\mathbb{F}_q^*}\bar{\lambda}(ac)\sum_{w\in\mathbb{F}_{q^n}}\chi(cw)\eta_d(w)\right)\\ &\text{and, replacing } cw \text{ by } w,\\ \pi(k) &= \frac{\Theta(k)}{q}\left(q^n + \int_{\substack{d|k\\ d>1}}\sum_{c\in\mathbb{F}_q^*}\bar{\lambda}(ac)\hat{\eta}_d(c)G_n(\eta_d)\right),\end{aligned}$$

where $G_n(\eta_d) = \sum_{x\in\mathbb{F}_{q^n}}\eta_d(x)\chi(x)$ and $\hat{\eta}_d$ is η_d, restricted to $\mathbb{F}_q$.

When $a = 0$ and $k|Q$, the result is evident since $\hat{\eta}_d(c) = 1$ and $c \in \mathbb{F}_q^*$ in that case. We may therefore suppose $a \neq 0$, whereupon the desired formula follows when ac is replaced by c. We also use the fact that $G_1(\hat{\eta}_d) = -1$ when $d|\, k_Q$. □

Corollary 4.2.5. *Suppose that q^n is a square, thus either q is a square or n is even. Assume that k (> 1) is a square-free divisor of $q^{\frac{n}{2}} + 1$. Then, provided $k > 2$ if $q^{\frac{n}{2}} \equiv 1 \pmod 4$, the following hold:*

$$\pi(k) = \Theta(k)\, q^{\frac{n}{2}-1}\,(q^{\frac{n}{2}} + 1); \tag{4.3}$$

$$\pi_0(k) = \Theta(k)\,(q^{\frac{n}{2}-1} - 1)\,(q^{\frac{n}{2}} + 1). \tag{4.4}$$

Further, suppose that q^n is a 4-th power. Assume that k (> 1) is a divisor of $q^{\frac{n}{4}} + 1$. Then, provided $k > 2$ if $q^{\frac{n}{4}} \equiv 1 \pmod 4$,

$$\pi(k) = \Theta(k)\, q^{\frac{n}{2}-1}\,(q^{\frac{n}{2}}-1); \tag{4.5}$$

$$\pi_0(k) = \Theta(k)\,(q^{\frac{n}{2}-1}+1)\,(q^{\frac{n}{2}}-1). \tag{4.6}$$

If q^n is a square, $k=2$ and $q^{\frac{n}{2}} \equiv 1 \pmod 4$, then (4.5) and (4.6) hold.

Finally, for completeness,

$$\pi(1) = q^{n-1}; \tag{4.7}$$

$$\pi_0(1) = q^{n-1}-1. \tag{4.8}$$

Proof. Observe that, under the given assumptions, $k|Q$. Define $M(k,q,n)$ by

$$M(k,q,n) := \begin{cases} q^n - \dfrac{q\cdot\pi(k)}{\Theta(k)}, & a \neq 0, \\ \dfrac{q\cdot\pi(k)-(q^n-q)}{(q-1)\cdot\Theta(k)}, & a = 0. \end{cases}$$

By Lemma 4.2.4, $M(k,q,n) = \int_{\substack{d|\,k \\ d>1}} G_n(\eta_d)$. On the other hand, for (4.3) and (4.4), it is necessary to show that $M(k,q,n) = -q^{\frac{n}{2}}$, whereas for (4.5) and (4.6), it is needed to show that $M(k,q,n) = q^{\frac{n}{2}}$. It follows that for (4.3) and (4.4), one can replace $q^{\frac{n}{2}}$ by q and n by 2. Similarly, for (4.5) and (4.6), replace $q^{\frac{n}{4}}$ by q and n by 4.

Now apply the Stickelberger's theorem and the Hasse-Davenport theorem. For d a square-free divisor of $q+1$, these yield

$$\begin{aligned} G_2(\eta_d) &= \sum_{x\in\mathbb{F}_{q^2}} \eta_d(x)\chi_1(x) \\ &= G(\eta_d,\chi_1) \\ &= \begin{cases} -q, & \text{if } d \text{ is even and } \frac{q+1}{d} \text{ odd}, \\ q, & \text{if } d \text{ odd or } \frac{q+1}{d} \text{ even}; \end{cases} \\ &= \begin{cases} -q, & \text{if } d \text{ is even and } q \equiv 1 \pmod 4, \\ q, & \text{otherwise}; \end{cases} \end{aligned}$$

$$G_4(\eta_d) = \begin{cases} q^2, & \text{if } d \text{ is even and } q \equiv 1 \pmod 4, \\ -q^2, & \text{otherwise.} \end{cases}$$

Assume that k is odd or $q \not\equiv 1 \pmod 4$. Then

$$\begin{aligned} M(k,q,2) &= \int_{\substack{d|k \\ d>1}} G_2(\eta_d) \\ &= \sum_{\substack{d|k \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{(d)} q \\ &= q \sum_{\substack{d|k \\ d>1}} \frac{\mu(d)}{\phi(d)} \\ &= -q, \end{aligned}$$

as required.

Similarly, $M(k,q,4) = q^2$.

Now, assume $k > 2$ is even and $q \equiv 1 \pmod 4$. Then

$$\begin{aligned} M(k,q,2) &= \int_{\substack{d|k \\ d>1}} G_2(\eta_d) \\ &= \sum_{\substack{d|k \\ d>1 \\ d \text{ odd}}} \frac{\mu(d)}{\phi(d)} \sum_{(d)} q + \sum_{\substack{d|k \\ d>2 \\ d \text{ even}}} \frac{\mu(d)}{\phi(d)} \sum_{(d)} (-q) \ + \ q \\ &= 2q \sum_{\substack{d|k \\ d>1 \\ d \text{ odd}}} \frac{\mu(d)}{\phi(d)} \ + \ q \ = \ -2q + q \\ &= -q, \end{aligned}$$

as required. Evidently, the sign is reversed for $M(2,q,2)$.

Similarly, $M(k,q,4) = q^2$. □

The identities of Lemma 4.2.4 can be extended by using a sieving inequality. First, observe that, from the definition of k-free, it is evident that the value of $\pi(k)$ depends only on the square-free part of k, that is, the set of (or product of) the distinct primes in k. Accordingly, we freely replace k by its square-free part in what follows.

As defined previously in Section 3.3, $\delta := 1 - \sum_{i=1}^{s} \frac{1}{p_i}$ and $\Theta(p_i) = 1 - \frac{1}{p_i}$, where $\{p_1, \ldots, p_s\}$ is the set of (all) distinct prime divisors of k not dividing k_0, a divisor of k.

The basic sieving inequality (4.9) below is equivalent to Lemma 3.3.2. The other inequalities in the next result follow simply from this section.

Lemma 4.2.6. *Let k be a divisor of q^n-1 and let (k_0,s) be a decomposition of k. Then*

$$\begin{aligned}\pi(k) &\geq \left(\sum_{i=1}^{s}\pi(k_0p_i)\right)-(s-1)\pi(k_0)\\ &= \left(1-\sum_{i=1}^{s}\frac{\Theta(k_0)-\Theta(k_0p_i)}{\Theta(k_0)}\right)\pi(k_0)+\sum_{i=1}^{s}\left(\pi(k_0p_i)-\frac{\Theta(k_0p_i)}{\Theta(k_0)}\pi(k_0)\right). \quad (4.9)\end{aligned}$$

If $a\neq 0$, then

$$\pi(k) \geq \frac{\Theta(k_0)}{q}\left(\delta\cdot q^n+\left[\left(\sum_{i=1}^{s}\Theta(p_i)\int_{\substack{d|k_i\\ d\nmid k_0}}\right)+\delta\int_{\substack{d|k_0\\ d>1}}\right]\hat{\eta}_d(a)\bar{G}_1(\hat{\eta}_d)G_n(\eta_d)\right) \quad (4.10)$$

Otherwise, if $a=0$ and $k|Q$, then

$$\pi(k)\geq\frac{\Theta(k_0)}{q}\left(\delta\cdot(q^n-q)+(q-1)\cdot\left[\left(\sum_{i=1}^{s}\Theta(p_i)\int_{\substack{d|k_i\\ d\nmid k_0}}\right)+\delta\int_{\substack{d|k_0\\ d>1}}\right]G_n(\eta_d)\right). \quad (4.11)$$

4.3 Estimates for k-free elements with specified trace

Suppose that $d|(q^n-1)$ but $d>1$. Then (see Section 2.4) $|G_n(\eta_d)|=q^{\frac{n}{2}}$ and $|G_1(\hat{\eta}_d)|=q^{\frac{1}{2}}$, unless $d|\,Q$, in which case $G_1(\hat{\eta}_d)=-1$.

Let $W(k)$ be the number of square-free divisors of k, as defined in Section 3.1. The following results are immediate consequences of Lemma 4.2.4 and (when $n=2$) Corollary 4.2.5.

Lemma 4.3.1. *Suppose that $a\neq 0$ and k divides q^n-1. Then*

$$\begin{aligned}\pi(k) &\geq \Theta(k)\cdot q^{\frac{n-2}{2}}\cdot\left[q^{\frac{n}{2}}-\Big(W(k)-W(k_Q)\Big)q^{\frac{1}{2}}-\Big(W(k_Q)-1\Big)\right] \quad (4.12)\\ &\geq \Theta(k)\cdot q^{\frac{n-1}{2}}\cdot\left[q^{\frac{n-1}{2}}-\Big(W(k)-1\Big)\right]. \quad (4.13)\end{aligned}$$

More precisely, when $n=2$ (and $Q=q+1$), then

$$\pi(k) \geq \Theta(k)\left[q-\Big(W(k)-W(k_Q)\Big)q^{\frac{1}{2}}+(1-\varepsilon_{k_Q})\right], \quad (4.14)$$

where

$$\varepsilon_{k_Q}=\begin{cases}1; & k_Q=1,\\ 0; & \text{otherwise.}\end{cases}$$

Lemma 4.3.2. *Suppose that k divides Q. Then*

$$\pi_0(k) \;\geq\; \Theta(k)\cdot q^{\frac{n}{2}}\cdot\left[q^{\frac{n}{2}-1}-\left(1-\frac{1}{q}\right)\Big(W(k)-1\Big)-\frac{1}{q^{\frac{n}{2}}}\right]. \tag{4.15}$$

To efficiently apply these results, we prefer to have them in 'sieve versions' given below. They are obtained by the same means from Lemma 4.2.6; however in applying (4.10), we use again the fact that $G_1(\hat{\eta}_d)=-1$ when $d|\, k_{iQ},\ i=0,\dots,s$, where $k_{iQ}:=\gcd(k_0p_i,\,Q)$.

Lemma 4.3.3. *Assume that $a\neq 0$. Let k divide q^n-1 and let (k_0,s) be a decomposition of k. Suppose that the primes $p_1,\dots,p_s$ are ordered so that $p_i\nmid Q$ for $i>t$ (possibly $t=0$) and $p_i|Q$ for $i\leq t\,(\leq s)$. Then*

$$\begin{aligned}\frac{\pi(k)}{\delta\cdot\Theta(k_0)} \;\geq\; & q^{n-1}-\left[W(k_0)\left(\frac{s-1}{\delta}+2\right)-W(k_{0Q})\left(\frac{t-1+\delta_t}{\delta}+1\right)\right]q^{\frac{n-1}{2}}\\ & -\left[W(k_{0Q})\left(\frac{t-1+\delta_t}{\delta}+1\right)-1\right]q^{\frac{n}{2}-1},\end{aligned} \tag{4.16}$$

where $\delta_t:=1-\sum_{i=1}^{t}\frac{1}{p_i},\ t\geq 1$, and $\delta_0:=1$.

More precisely, when $n=2$, then

$$\begin{aligned}\frac{\pi(k)}{\delta\cdot\Theta(k_0)} \;\geq\; & q+1+\varepsilon_{k_{0Q}}\left(\frac{t-1+\delta_t}{\delta}-1\right)\\ & -\left[W(k_0)\left(\frac{s-1}{\delta}+2\right)-W(k_{0Q})\left(\frac{t-1+\delta_t}{\delta}+1\right)\right]q^{\frac{1}{2}}.\end{aligned} \tag{4.17}$$

(Here, as in Lemma 4.14, $\varepsilon_{k_{0Q}}=1$ if $k_{0Q}=1$ and 0 otherwise.)

Lemma 4.3.4. *Suppose k divides Q and (k_0,s) is a decomposition of k. Then*

$$\frac{\pi_0(k)}{\delta\cdot\Theta(k_0)\cdot q^{\frac{n}{2}}} \;\geq\; q^{\frac{n}{2}-1}-\left(1-\frac{1}{q}\right)\left[W(k_0)\left(\frac{s-1}{\delta}+2\right)-1\right]-\frac{1}{q^{\frac{n}{2}}}. \tag{4.18}$$

4.4 Primitive elements with non-zero trace

Now that the required machinery has been attained, we can begin to establish the existence of primitive polynomials with prescribed trace.

Throughout this section we suppose that the trace $a \neq 0$. Polynomials with zero trace will be treated separately in the following section.

Take $k = q^n - 1$ in Lemma 4.3.1. A criterion for existence is that the right-hand side of the inequality (4.13) is positive, i.e., that

$$q^{\frac{n-1}{2}} > W(q^n - 1) - 1. \tag{4.19}$$

When, specifically, $q = 2$, then necessarily $k | Q$ and, by the inequality (4.12), it suffices that

$$2^{\frac{n}{2}} > W(2^n - 1) - 1. \tag{4.20}$$

4.4.1 Degree $n \geq 4$

We shall begin by demonstrating that conditions (4.19) and (4.20) guarantee existence when $n \geq 4$. From Lemma 3.1.3, we have that $W(q^n - 1) < C \cdot q^{\frac{n}{4}}$, where always $C < 4.9$, but, for instance, when q is even (so that $q^n - 1$ is odd), we may suppose $C < 2.9$. Moreover, if q is odd and n is even, then $8 | q^n - 1$: indeed

$$q^n - 1 = (q^{\frac{n}{2}} - 1)(q^{\frac{n}{2}} + 1)$$

where the two factors are consecutive even positive integers and as such one of them is neccessarily divisible by 4.

Hence, evidently $W(q^n - 1) < \frac{C}{\sqrt{2}} \cdot q^{\frac{n}{4}}$ (we can divide $q^n - 1$ by 4 without losing 2 as a factor). We therefore have the following sufficient criteria for existence, where C is at most 4.9:

$$q^{\frac{n-2}{4}} > C; \tag{4.21}$$

$$q^{\frac{n-2}{4}} > \frac{C}{\sqrt{2}}, \quad q \text{ odd } n \text{ even}; \tag{4.22}$$

$$2^{\frac{n}{4}} > 2.9, \quad q = 2. \tag{4.23}$$

Evidently, (4.21) and (4.23) suffice to yield existence for $n \geq 7$; in particular, in (4.21) we have $C < 3.2$ when $q = 3$.

With the additional use of (4.22) for $q = 3$, (4.21) suffices for $n = 6$, except when $q = 2$.

Next, we dispose of all remaining cases when $q = 2$ via (4.20). Observe that

$$\begin{aligned} 2^3 &> W(2^6 - 1) - 1 = 3; \\ 2^{\frac{n}{2}} &> W(2^n - 1) - 1 = 0, \text{ for } n = 2, 3, 5; \\ 2^2 &> W(2^4 - 1) - 1 = 3. \end{aligned}$$

Suppose $n = 5$ (with $q > 2$). From (4.21), we can suppose first that $q \leq 8$ ($q^{\frac{3}{4}} > 4.9$ is satisfied for $q \geq 9$) and then, using $C \leq \frac{2^4}{(2 \cdot 3 \cdot 5 \cdot 7)^{\frac{1}{4}}} < 4.21$, that $q \leq 5$. For the remaining cases we have

$$\begin{aligned} 5^2 &> W(5^5 - 1) - 1 = 7; \\ 4^2 &> W(4^5 - 1) - 1 = 7; \\ 3^2 &> W(3^5 - 1) - 1 = 3. \end{aligned}$$

Finally, take $n = 4$. Since $16 | q^4 - 1$ when q is odd, we may replace (4.22) by $\sqrt{q} > \dfrac{C}{2^{\frac{3}{4}}}$. With (4.21) for q even ($q^{\frac{1}{2}} > 2.9$), existence is established for $q > 8$. Otherwise (4.19) is always satisfied. Indeed,

$$\begin{aligned} 8^{\frac{3}{2}} &> W(4095) - 1 = 15; \\ 7^{\frac{3}{2}} &> W(2400) - 1 = 7; \\ 5^{\frac{3}{2}} &> W(624) - 1 = 7; \\ 4^{\frac{3}{2}} &> W(255) - 1 = 7; \\ 3^{\frac{3}{2}} &> W(80) - 1 = 3. \end{aligned}$$

When the prescribed trace coefficient is non-zero, it now only remains to show existence of primitive polynomials of degrees $n = 3$ and $n = 2$.

4.4.2 Cubics

Take $n = 3$, so that $Q = q^2 + q + 1$. To identify the possible prime factors Q, use the case $n = 3$ of the following easily-proved result.

Lemma 4.4.1. *Suppose n and l are odd primes such that $l \mid Q = \frac{q^n-1}{q-1}$. Then, either $l = n$ or l $(\nmid (q-1)) \in L_n$:= the set of primes $\equiv 1 \pmod{2n}$.*

By Lemma 4.4.1, with $l|q^2+q+1$, either $l = 3$ or $l \in L_3 = \{7, 13, 19, 31, 37, 43, 61, \ldots\}$. In order to effectively use this knowledge, we will attack the polynomials with coefficients in $\mathbb{F}_q$, where $q \equiv 1 \pmod 3$, separately from those where $q \not\equiv 1 \pmod 3$.

Assume that $q \equiv 1 (\mathbf{mod}\ 3)$.

Then $9 \mid (q^3 - 1)$ and so, from Lemma 3.1.3,

$$W\left(q^3-1\right) = W\left(\frac{q^3-1}{3}\right) < C \cdot \frac{q^{\frac{3}{4}}}{3^{\frac{1}{4}}}. \tag{4.24}$$

We deduce from (4.19) that $\pi(q^3 - 1)$ is positive whenever $q > \frac{C^4}{3}$. Since $C < 4.9$, existence is proven for $q \geq 193$. Indeed for $q = 2^r$ even (where necessarily r also is even), $C < 2.9$ and $\pi(q^3 - 1)$ is certainly positive for $q \geq 24$. Hence we may assume $q \leq 181$, q odd, or $q = 4$, 16.

The following table shows that the latter two satisfy the criterion (4.19), which, for $n = 3$, takes the form $q > W(q^3 - 1) - 1$.

q	$q^3 - 1$	$W(q^3 - 1) - 1$
4	$3^2 \cdot 7$	3
16	$3^2 \cdot 5 \cdot 7 \cdot 13$	15

Suppose now that q $(\equiv 1 \pmod 3) \leq 181$ is *odd*: thus, by Lemma 4.4.1, we can assume that $3 \mid Q$ (where $Q \leq 32943 = 3 \cdot 10981$). We aim to apply Lemma 4.3.3. Since the product of the four smallest primes in $L_3 = \{7, 13, 19, 31, \ldots\}$ exceeds 10981, then, by Lemma 4.4.1, $\omega(Q) \leq 4$. Similarly, since the product of the four smallest primes exceeds 181, then $\omega(q-1) \leq 3$ and therefore $\omega\left(q^3-1\right) \leq 6$.

Now, as q is odd, $q \equiv 1 \,(\mathrm{mod}\ 6)$ and $q^3 - 1 = 2 \cdot 3^2 \cdot p_1 \cdots p_s$ (observe that $3|Q$ and $3|q-1$), where $s \leq 4$ and $p_i \geq 5$, $1 \leq i \leq s$. We apply Lemma 4.3.3 with $k_0 = 6$; thus $k_{0Q} = 3$ and $t \leq 3$. Moreover, $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \frac{1}{13} - \frac{1}{19} > 0.527$. By (4.16) it is sufficient that

$$q^2 > \left[4\left(\frac{s-1}{\delta} + 2\right) - 2\left(\frac{t-1+\delta_t}{\delta} + 1\right)\right] q + \left[2\left(\frac{t-1+\delta_t}{\delta} + 1\right) - 1\right] \sqrt{q},$$

which is equivalent to

$$q > 4\left(\frac{s-1}{\delta}\right) + 6 + \frac{1}{\sqrt{q}} - 2\left(1 - \frac{1}{\sqrt{q}}\right)\left(\frac{t-1+\delta_t}{\delta}\right). \tag{4.25}$$

Ignoring the negative term in (4.25) and noting that $q \geq 7$, we deduce the sufficient condition

$$q > 4\left(\frac{s-1}{\delta}\right) + 6 + \frac{1}{\sqrt{7}}. \tag{4.26}$$

With $s \leq 4$ and $\delta > 0.527$, this yields existence for $q \geq 30$.

Hence, for q odd, we may assume $q \leq 25$. Then $Q \leq 651 = 3 \cdot 217$. It follows that $\omega(Q) \leq 3$ and similarly $\omega(q-1) \leq 2$, whence $\omega(q^3 - 1) \leq 4$. We may therefore apply the sufficient condition (4.26) with $s \leq 2$ and $\delta \geq 1 - \frac{1}{7} - \frac{1}{13} > 0.780$. This establishes existence for $q \geq 13$. This leaves only $q = 7$, in which case criterion (4.12) is satisfied, since

$$q^{\frac{3}{2}} > \Big(W(k) - W(k_Q)\Big) q^{\frac{1}{2}} - \Big(W(k_Q) - 1\Big),$$

as we can see below:

$$\begin{aligned} 7 &> \Big(W(342) - W(57)\Big) - \frac{W(57) - 1}{\sqrt{7}} \\ &= 4 + \frac{3}{\sqrt{7}} = 5.133\ldots. \end{aligned}$$

Assume that $q \not\equiv 1$ (mod 3).

In place of (4.24), Lemma 3.1.3 now provides the sufficient criterion

$$q > C^4$$

$\left(W(q^3-1) < C \cdot q^{\frac{3}{4}} \quad \text{and} \quad q > W(q^3-1) - 1 \quad \text{yield} \quad q > C \cdot q^{\frac{3}{4}}\right)$, which holds for *odd* $q \geq 577$ (using $C < 4.9$) and *even* $q \geq 71$ (using $C < 2.9$). The remaining even values $q = 8$ and $q = 32$ satisfy the criterion (4.19) $\left(q > W(q^3-1) - 1\right)$, as shown in the table below.

q	$q^3 - 1$	$W(q^3-1) - 1$
8	$7 \cdot 73$	3
32	$7 \cdot 31 \cdot 151$	7

Accordingly, we may suppose $q \leq 571$ is odd; thus $Q \leq 326613$. Moreover, 3 is *not* a factor of $q^3 - 1$. Since the product of the five smallest primes in L_3 exceeds 326613, it follows that $\omega(Q) \leq 4$. Similarly (because the product of the four smallest primes (excluding 3) is $2 \cdot 5 \cdot 7 \cdot 11 > 571$), $\omega(q-1) \leq 3$ and therefore $\omega(q^3-1) \leq 7$, with at most two of the odd prime divisors of $q^3 - 1$ *not* members of L_3. Apply Lemma 4.3.3 with $k_0 = 2$; thus $k_{0Q} = 1$ and $t \leq 4$. Now, $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \frac{1}{11} - \frac{1}{13} - \frac{1}{19} - \frac{1}{31} > 0.404$. On the other hand, the right-hand side of the inequality (4.16) is positive whenever

$$q^2 > \left[2\left(\frac{s-1}{\delta} + 2\right) - 2\left(\frac{t-1+\delta_t}{\delta} + 1\right)\right] q + \left(\frac{t-1+\delta_t}{\delta}\right)\sqrt{q}.$$

It suffices that

$$q > 2\left(\frac{s-1}{\delta}\right) + 3 - \left(1 - \frac{1}{\sqrt{q}}\right)\left(\frac{t-1+\delta_t}{\delta}\right). \tag{4.27}$$

Since $s \leq 6$ and $\delta > 0.404$, (4.27) holds for $q \geq 28$ (even if we omit the negative term on the right-hand side). We may therefore assume $q \leq 27$ and $Q \leq 757$. Repeating the process ($k_0 = 2$, $k_{0Q} = 1$), we see that $t = \omega(Q) \leq 2$, $\omega(q-1) \leq 2$ (since $2 \cdot 5 \cdot 7 > 27$) and $\omega(q^3-1) \leq 4$, whence $s \leq 3$, $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \frac{1}{13} > 0.580$. Now, we suppose $9 \leq q \leq 27$ and apply the criterion (4.27) in full (that is, without omitting the negative term):

$$q > 2\left(\frac{s-1}{\delta}\right) + 3 - \frac{1}{\delta}\left(1 - \frac{1}{\sqrt{q}}\right)\left(2 - \frac{1}{7} - \frac{1}{13}\right) = 7.850\ldots.$$

Existence for $q \geq 9$ is a consequence.

The values $q = 3$ and $q = 5$ remain. For $q = 3$ we have $Q = 13$ and $q^3 - 1 = 2 \cdot 13$. Setting $k = 26$ (and thus $k_Q = 13$) in (4.12) yields $\pi(q^3-1)$ positive since

$$\begin{aligned} 3 &> W(26) - W(13) + \frac{W(13)-1}{\sqrt{3}} \\ &= 2 + \frac{1}{\sqrt{3}} = 2.577\ldots. \end{aligned}$$

For $q = 5$, criterion (4.19) is enough since

$$5 > W(5^3 - 1) - 1 = 3.$$

This completes the proof of existence of primitive polynomials of degree $n = 3$ with prescribed non-zero trace coefficient. It now only remains to show the same for primitive polynomials of degree $n = 2$.

4.4.3 Quadratics

Take $n = 2$ (thus $Q = q + 1$) and set $\omega := \omega(q^2 - 1)$. We will proceed by separately considering the cases when q is even or odd. This brings the advantage of knowing that q^2-1 is odd if q is even, and that $8|q^2-1$ if q is odd, which yields that $\omega(q^2-1) = \omega(\frac{q^2-1}{4})$.

Suppose $8|k$ and $\omega(k) \geq 15$. Then $W(k) < k^{\frac{1}{4}}$, since

$$\frac{W(k)}{k^{\frac{1}{4}}} < \frac{2^{15}}{(8 \cdot 3 \cdot 5 \cdot \cdots \cdot 47)^{\frac{1}{4}}} < 1.$$

For k odd it suffices that $\omega(k) \geq 13$. Thus, whenever $\omega \geq 15$ (q odd), or $\omega \geq 13$ (q even), then

$$q^{\frac{1}{2}} > W(q^2 - 1) - 1,$$

meaning that the condition (4.19) is satisfied.

Assume that q is odd.

From the above, we can assume that $\omega \leq 14$. In (4.17), take k_0 *even* so that $\varepsilon_{k_{0Q}} = 0$ (as $k_{0Q} > 1$). Trivially also $\frac{t-1+\delta_t}{\delta} \geq 0$ when $\delta > 0$. It follows that $\pi(q^2 - 1)$ is positive whenever

$$q^{\frac{1}{2}} > W(k_0)\left(\frac{s-1}{\delta} + 2\right) - 2. \tag{4.28}$$

Set k_0 to be the product of the three smallest primes dividing q^2-1. Then $s \le 11$, $\delta \ge 1 - \frac{1}{7} - \frac{1}{11} - \ldots - \frac{1}{43} > 0.392$ and (4.28) is satisfied for $q \ge 47560$. Hence, we can assume $q \le 47559$. Recalling that $8|q^2-1$ and thus $\omega(q^2-1) = \omega\left(\frac{q^2-1}{4}\right)$, we repeat the sieving process two times based on (4.28), now setting k_0 to be the product of the two least prime divisors of q^2-1. Each of the two steps produces a value q_{min} such that (4.28) holds provided $q \ge q_{min}$. The outcome is tabulated as follows.

$q \le$	$\omega \le$	$s \le$	$\delta >$	q_{min}
47559	9	7	0.334	6062
6061	7	5	0.430	1868

We can therefore assume that $q \le 1867$, $\omega(q-1) \le 4$ and $\omega \le 7$.

If $3|\, q$, i.e., $p = 3$, then in the last line of the table above, we have $\delta \ge 1 - \frac{1}{7} - \frac{1}{11} - \frac{1}{13} - \frac{1}{17} - \frac{1}{19} > 0.577$ and $q_{min} = 1138$. Hence, we can assume $q \le 3^6 = 729$: thus $\omega \le 5$ $\left(2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 > \frac{729^2-1}{4}\right)$ with $\omega(q-1) \le 3$. In this case, take $k_0 = 2$ in (4.28): then $\delta \ge 1 - \frac{1}{5} - \frac{1}{7} - \frac{1}{11} - \frac{1}{13} > 0.489$, $s \le 4$ and the criterion is satisfied whenever $q \ge 204$, i.e., unless $q \le 81$.

From now on we have regard to the value of t in (4.17) (or use exact values). Given δ, we have to minimise $t - 1 + \delta_t$. Accordingly, it suffices that $q > V^2$, where

$$V := W(k_0)\left(\frac{s-1}{\delta} + 2\right) - W(k_{0Q})\left(\frac{t-1+\delta_t}{\delta} + 1\right). \tag{4.29}$$

Suppose $\omega = 7$. Then $q^2 - 1 \ge 8 \cdot 3 \cdot 5 \cdot \cdots \cdot 17$ so that $q \ge 1429$. (In fact, equality is possible!) Set $k_0 = 6$, so that $\delta > 0.430$, as before.

If $3|\, q-1$, then $k_{0Q} = 2$ and, in (4.17), we can suppose $t \ge 3$ and $t - 1 + \delta_t \ge t - \frac{1}{5} - \frac{1}{7} - \frac{1}{11} > 2.566$. Hence $V < 31.27$, whence $V^2 < 978 < q$.

On the other hand, if $3|\, q+1$, then we have $k_{0Q} = 4$ and $t \ge 2$ with $t - 1 + \delta_t \ge t - \frac{1}{5} - \frac{1}{7} > 1.657$. Hence $V < 25.6$, whence $V^2 < 665 < q$. Again this is sufficient.

Suppose $\omega = 6$. Now $q \ge 347$. As before, set $k_0 = 6$ so that $\delta > 0.489$.

If $3|\, q-1$, then $t = 2$ (exactly) and $t - 1 + \delta_t \ge t - \frac{1}{5} - \frac{1}{7} > 1.657$. Hence

$$V < 4\left(\frac{3}{0.489} + 2\right) - 2\left(\frac{1.657}{0.489} + 1\right) < 23.8$$

and the existence is guaranteed for $q \geq 567$. A systematic check, considering possible products of three or four primes together with 2 or 4, yields that there no prime powers in the range $349 \leq q \leq 559$ with $\omega = 6$.

If $3 | q+1$, then $t \geq 1$ and $t - 1 + \delta_t \geq 0.8$. Hence

$$V < 4\left(\frac{3}{0.489} + 2\right) - 4\left(\frac{0.8}{0.489} + 1\right) < 22$$

and so existence is guaranteed for $q \geq 484$. Otherwise, if $q \leq 479$, then $\omega(q-1) \leq 3$, whence $t \geq 2$ and $t - 1 + \delta_t > 1.657$, yielding $V < 14.98$, which suffices.

Suppose $\omega = 5$. Set k_0 to be product of the least two prime divisors of $q^2 - 1$. Then $s \leq 3$, $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \frac{1}{11} > 0.566$ and (4.28) is satisfied for $q \geq 406$.

We can therefore assume that $q \leq 403$. The only possible prime powers with $\omega(q-1) = 4$ are $q = 211 (= 2 \cdot 3 \cdot 5 \cdot 7 + 1)$ or $q = 331 (= 2 \cdot 3 \cdot 5 \cdot 11 + 1)$. In the latter case, $s = 3$, $\delta = 1 - \frac{1}{5} - \frac{1}{11} - \frac{1}{83} > 0.697$ and (4.28) is satisfied. For $q = 211$, temporarily write π_k for $\pi(k)$. Then, by Lemma 4.2.6, the identity (4.3), and the estimates used in Section 4.3,

$$\begin{aligned}
\pi(q^2-1) &\geq \pi_{210} + \pi_{212} - \pi_2 \\
&\geq (\pi_{30} + \pi_{42} - \pi_6) + \pi_{212} - \pi_2 \\
&\geq \left(\pi_{30} - \frac{4}{5}\pi_6\right) + \left(\pi_{42} - \frac{6}{7}\pi_6\right) + \frac{23}{35}\left(\pi_6 - \frac{2}{3}\pi_2\right) + \pi_{212} - \frac{59}{105}\pi_2 \\
&\geq -\left(4\left(\frac{4}{15} + \frac{2}{7}\right) + \frac{23}{15} \cdot \frac{2}{3}\right)\sqrt{211} + 104 - \frac{59}{105} \cdot 106 \\
&> 5.9.
\end{aligned}$$

Therefore we may assume $\omega(q-1) \leq 3$. It is quickly seen that no arrangement of five prime powers into factors of $q-1$ and $q+1$ can have $q + 1 < 140$.

Suppose $3 | q - 1$, $q \geq 139$. This time set $k_0 = 2$. Then, $\delta > 0.232$, $t \geq 2$ and $t - 1 + \delta_t \geq 1.657$. Hence

$$V < 2\left(\frac{3}{0.232} + 2\right) - 2\left(\frac{1.657}{0.232} + 1\right) < 13.6$$

and so the existence is guaranteed for $q \geq 185$. Easily, the only possibilities that remains are $q = 139$ or 169. For these $\delta > 0.280$ or 0.264, respectively. Also $t = 2$ and $t - 1 + \delta_t >$ 1.657 and 1.741, whence

$$V < 2\left(\frac{3}{0.280} + 2\right) - 2\left(\frac{1.657}{0.280} + 1\right) < 11.6$$

or

$$V \;<\; 2\left(\frac{3}{0.264}+2\right)-2\left(\frac{1.741}{0.264}+1\right) \;<\; 11.6,$$

so that $V^2 < 135 < q$ in each case.

Suppose $3|\, q+1,\ q \geq 155$ (since $\omega = 4$ when $q = 149$). Resume the choice $k_0 = 6$. Then $\delta > 0.566$, $t \geq 1$ and $\delta_t \geq 0.8$. Thus

$$V \;<\; 4\left(\frac{2}{0.566}+2\right)-4\left(\frac{0.8}{0.566}+1\right) \;<\; 12.48,$$

so that $V^2 < 156 < q$, as required.

Suppose $\omega \leq 4$. Then, with $k_0 = 6,\ s \leq 3,\ \delta > 0.6571$, the criterion (4.28) is satisfied provided $q \geq 147$: indeed, with $k_0 = 1$ it suffices that $q \geq 36$, whenever $q \leq 3$.

Suppose $\omega = 4,\ q \leq 139$. Assume $3|q-1$ and take $k_0 = 6$ (as before). Then $t \geq 1$ and $t - 1 + \delta_t \geq 0.8$, whence $V < 9.66$: this is sufficient if $q \geq 94$. Now, assume $3|q+1$ and take $k_0 = 2$, so that $\delta > 0.3238$: again $t \geq 1$ and $V < 9.42$. This suffices if $q \geq 89$.

From the above, we conclude the existence of a suitable primitive quadratic in every case provided $q > 83$. To complete the proof we give a supplementary criterion for $\pi(q^2-1)$ to be positive that is useful for small values of q. Its origins lie in [17].

Lemma 4.4.2. *Let $\Theta_O(k)$ denote $\Theta\,(k_{odd})$, where k_{odd} is the odd part of k.*

Then $\pi\left(q^2-1\right) > 0$ whenever

$$\Theta_O(q-1)+\frac{1}{2}\Theta_O(q+1) \;>\; 1. \tag{4.30}$$

Proof. Assume q is odd. (The result is not needed when q is even.)

Let S denote the set of $(q-1)$-free elements of $\mathbb{F}_{q^2}$ with trace $a \neq 0$, that are *not* primitive. Then $|S| \;\geq\; \pi(q-1)-\pi\left(q^2-1\right)$. Moreover, for any α in S, its $\mathbb{F}_q$-norm $\mathrm{N}(\alpha) = \alpha^{q+1} \in \mathbb{F}_q$ is a non-square, non-primitive element of $\mathbb{F}_q$. Conversely, given a non-square, non-primitive element $c \in \mathbb{F}_q$, there are at most two elements $\alpha \in S$ such that $\mathrm{N}(\alpha) = c$: these would be roots of $\alpha^2 - a\alpha + c = 0$. It follows that S does not exceed twice the number of non square, non-primitive elements of $\mathbb{F}_q$. We conclude that

$$\pi(q-1)-\pi\left(q^2-1\right) \;\leq\; |S| \;\leq\; q-1-2(q-1)\Theta(q-1).$$

It follows (using (4.3)) that

$$\begin{aligned}\pi\left(q^2-1\right) &\geq \pi(q+1)+2(q-1)\Theta(q-1)-(q-1)\\ &\geq (q-1)\Theta(q+1)+2(q-1)\Theta(q-1)-(q-1)\\ &= (q-1)\left(\frac{1}{2}\Theta_O(q+1)+\Theta_O(q-1)-1\right).\end{aligned}$$

This yields the criterion (4.30). □

To apply Lemma 4.4.2 for $q \leq 83$ (so that $\omega \leq 4$), we will write the product of the distinct *odd* primes in $q-1$ and $q+1$ as $l_1 \cdot l_2$ and $l_3 \cdot l_4$, respectively, where each l_i ($i \leq 4$) is a prime (in which case, set $L_i = 1 - \frac{1}{l_i}$), or is 1 (in which case, set $L_i = 1$). We can then rewrite condition (4.30) as

$$L_1 \cdot L_2 + \frac{1}{2} \cdot L_3 \cdot L_4 \ > \ 1,$$

where at least one of the L_i has to be 1. Evidently, this is satisfied unless $\{l_1, l_2\} = \{3, 5\}$ and $\{l_3, l_4\} = \{1, 7\}$ or $\{1, 11\}$; or $\{l_1, l_2\} = \{3, 7\}$ and $\{l_3, l_4\} = \{1, 5\}$. This cannot happen for any $q \leq 83$. For instance, $\{l_1, l_2\} = \{3, 5\}$ implies $q = 31$ or 61, etc.

This concludes the consideration of primitive quadratics (with prescribed non-zero trace coefficient) over the fields of odd characteristic.

Assume that q is even.

Suppose $\omega \leq 12$. In place of (4.28), we now have the sufficient condition

$$q^{\frac{1}{2}} \ > \ W(k_0)\left(\frac{s-1}{\delta}+2\right)-1. \tag{4.31}$$

We set k_0 to be the product of the least two primes dividing q^2-1. Then $s \leq 10$, $\delta \ \geq \ 1-\frac{1}{7}-\frac{1}{11}-\ldots-\frac{1}{41} \ > \ 0.416$ and (4.31) is satisfied for $q \geq 8750$. Hence we can assume $q \leq 8192$ and $\omega\left(q^2-1\right) \leq 7$. Set k_0 to be the least prime divisor of q^2-1. Then $s \leq 6$, $\delta \ \geq \ 1-\frac{1}{5}-\frac{1}{7}-\ldots-\frac{1}{19} \ > \ 0.377$ and (4.31) is satisfied for $q \geq 872$.

We can assume $q \leq 512$. For $q = 512$, 256, 128 and 2, the criterion (4.19) is satisfied, as shown below: $q > \left(W(q^2-1)-1\right)^2$.

q	q^2-1	$\big(W(q^2-1)-1\big)^2$
512	$3^3 \cdot 7 \cdot 19 \cdot 73$	225
256	$3 \cdot 5 \cdot 17 \cdot 257$	225
128	$3 \cdot 43 \cdot 127$	49
2	3	1

Three further powers of 2 satisfy an even stronger criterion (derived from (4.14)), namely,

$$q \;\geq\; \big(W(q^2-1) \;-\; W(q+1)\big)^2 .$$

(Here equality suffices because $\varepsilon_{q+1} = 0$.) This is satisfied for $q = 32$, $q = 8$ and $q = 4$, and tabulated below:

q	q^2-1	$q+1$	$\big(W(q^2-1) \;-\; W(q+1)\big)^2$
32	$3 \cdot 11 \cdot 31$	$3 \cdot 11$	16
8	$3^2 \cdot 7$	3^2	4
4	$3 \cdot 5$	5	4

For the remaining two powers of 2, we apply condition (4.17) to guarantee existence. It suffices that $q > V^2$, where V is the expression given by (4.29). Here are the results.

q	q^2-1	k_0	k_{0Q}	s	$\delta \geq$	t	$\delta_t \geq$	$V^2 <$
64	$3^2 \cdot 5 \cdot 7 \cdot 13$	3	1	3	0.580	2	0.723	48
16	$3 \cdot 5 \cdot 17$	1	1	3	0.407	1	0.941	13

This concludes the case of primitive polynomials with prescribed non-zero trace coefficient, and this section.

4.5 Primitive elements with zero trace

Take $a = 0$ and, necessarily, $n \geq 3$. From Lemma 4.3.2 we have the following core sufficient condition for $\pi_0(Q)$ (and so $\pi_0(q^n - 1)$) to be positive, namely

$$q^{\frac{n}{2}-1} > \left(1 - \frac{1}{q}\right)(W(Q) - 1) + \frac{1}{q^{\frac{n}{2}}}. \tag{4.32}$$

Thus, since Lemma 3.1.3 implies that $W(Q) \leq C \cdot Q^{\frac{1}{4}} < C \cdot q^{\frac{n-1}{4}} \cdot \left(1 - \frac{1}{q}\right)^{-\frac{1}{4}}$, it suffices that

$$q^{\frac{n-3}{4}} > C \cdot \left(1 - \frac{1}{q}\right)^{\frac{3}{4}}. \tag{4.33}$$

4.5.1 Degree $n \geq 5$

First we consider polynomials of degree $n \geq 7$. Then the left-hand side of the sufficient criterion(4.33) is at least q and (4.33) is satisfied by using

- $C < 4.9$ for $q \geq 4$: $5 > 4.9$ for $q \geq 5$ and $4 > 4.9 \cdot \frac{3}{4}^{\frac{3}{4}}$ for $q \geq 4$;
- $C < 3.7$ for $q = 3$: $3 > 3.7 \cdot \frac{2}{3}^{\frac{3}{4}}$ and
- $C < 2.9$ for $q = 2$: $2 > 2.9 \cdot \frac{1}{2}^{\frac{3}{4}}$.

Now we assume $n = 6$. It then suffices that $q\left(1 - \frac{1}{q}\right)^{-1} > C^{\frac{4}{3}}$. This holds for $q > 3$ using $C < 4.9$ for $q \geq 8$ and the appropriate (smaller) value of C, otherwise. For $q \leq 3$, inequality (4.32) is satisfied since

$$\begin{aligned} 3^2 &> \frac{2}{3}(W(40) - 1) + \frac{1}{27} = \frac{127}{27}; \\ 2^2 &> \frac{1}{2}(W(15) - 1) + \frac{1}{8} = \frac{29}{8}. \end{aligned}$$

Next, we assume $n = 5$. By Lemma 4.4.1, all prime factors of Q lie in $L_5 \cup \{5\}$: indeed, 5 and 11 are the only possible prime factors below 16. Accordingly, we may suppose $C < 1.5$ and the inequality

$$\frac{q^{\frac{1}{2}}}{\left(1 - \frac{1}{q}\right)^{\frac{3}{4}}} > 1.5$$

evidently holds. This implies (4.33).

4.5.2 Quartics

Now we consider polynomials of degree $n = 4$. For even values of q , the criterion (4.33) certainly holds whenever $q > C^4$, $C < 2.9$, i.e., if $q > 70.8$.

For odd values of q, we can assume that $4|Q = (q+1)\left(q^2+1\right)$ and so C may be replaced by $\frac{C}{2^{\frac{1}{4}}}$; $C < 4.9$. Hence it suffices that $q > \frac{C^4}{2}$, $C < 4.9$, i.e., $q > 288.2$.

It remains to show existence for *odd* $q \leq 283$ and *even* $q \leq 64$. As in Lemma 4.4.1, all odd prime divisors of q^2+1 are $\equiv 1 \pmod 4$. Since the odd part of q^2+1 does not exceed 40045 and $\omega(q^2+1) \leq 4$ with equality if and only if it equals $5 \cdot 13 \cdot 17 \cdot 31$ (in which case the odd part of $q-1$ has at most 2 prime factors since $2 \cdot 3 \cdot 7 \cdot 11 = 462$), then $\omega(Q) \leq 7$.

Now we apply Lemma 4.3.4 with k_0 being the product of the least two primes in Q, $s \leq 5$ and $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \ldots - \frac{1}{17} > 0.430$. Since the right-hand side of (4.16) is certainly positive whenever

$$q > 4 \cdot \frac{s-1}{\delta} + 7, \tag{4.34}$$

then (4.34) is satisfied when $q \geq 45$.

Accordingly, we may assume $q \leq 43$. Thus $q^2+1 \leq 1850$ so that $\omega(q^2+1) \leq 3$, $\omega(q+1) \leq 3$ and $\omega(Q) \leq 5$. We repeat the previous procedure with k_0 taken to be the product of the smallest pair of primes in Q, $s \leq 3$ and $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \frac{1}{11} > 0.566$. Now (4.34) is satisfied provided $q \geq 22$.

We may now assume $q \leq 19$, whence $q^2+1 \leq 362$, $\omega(q^2+1) \leq 3$. Easily, in the above procedure $\omega(Q) \leq 4$, $s \leq 2$, and $\delta \geq 1 - \frac{1}{5} - \frac{1}{13} > 0.723$. (We recall that only odd primes $\equiv 1 \pmod 4$ may divide q^2+1.) Now (4.34) is satisfied provided $q \geq 13$.

Suppose $7 \leq q \leq 11$. Thus $q^2+1 \leq 122$ and $\omega(q^2+1) \leq 2$ and $\omega(Q) \leq 3$. Hence the right-hand side of the condition (4.32) is at most 8; indeed, when $q = 7$ it is $6 + \frac{1}{7} < 7$.

For $q = 5$, take $k_0 = 1$, $p_1 = 3$ and $p_2 = 13$ ($s = 2$) in Lemma 4.2.6. Since $3|q+1$ and $2 \cdot \mathbf{1}3 = 26|q^2+1$, then (4.4), (4.6) and (4.8) yield

$$\pi_0(Q) \geq \pi_0(3) + \pi_0(26) - \pi_0(1) = 96 + 48 - 124 = 20.$$

For $q = 3$, $\pi_0(Q) = \pi_0(q^2+1) > 0$, by Corollary (4.4).

Finally, (4.32) is satisfied when $q = 4$ and $q = 2$, since $\omega(Q) = 2$ in both cases and we have

$$\begin{aligned} 4 &> \frac{3}{4}\cdot 3+\frac{1}{16}; \\ 2 &> \frac{1}{2}\cdot 3+\frac{1}{4}. \end{aligned}$$

4.5.3 Cubics

Assume $n=3$. Now the basic sufficient condition (4.32) is implied by the stronger one

$$q^{\frac{1}{2}} > \left(1-\frac{1}{q}\right) W(Q). \tag{4.35}$$

Crucially, in these circumstances, $Q=q^2+q+1$ is odd and, indeed from Lemma 4.4.1, all prime factors lie in the set $\{3\}\cup L_3$. By considering the product of the first 8 primes in this set, we deduce that, when $\omega(Q)\geq 8$, then $W(Q) < Q^{\frac{1}{4}} < q^{\frac{1}{2}}\left(1-\frac{1}{q}\right)^{-\frac{1}{4}}$ and (4.35) is automatically satisfied.

Hence, we can assume $\omega(Q)\leq 7$. Recall from Lemma 4.3.4 the sufficient condition

$$q^{\frac{1}{2}} > \left(1-\frac{1}{q}\right)\left[W(k_0)\left(\frac{s-1}{\delta}+2\right)-1\right]-\frac{1}{q^{\frac{3}{2}}}. \tag{4.36}$$

If we apply this with k_0 as the smallest prime divisor of Q, $s\leq 6$ and $\delta \geq 1-\frac{1}{7}-\frac{1}{13}-\frac{1}{19}-\frac{1}{31}-\frac{1}{37}-\frac{1}{43} > 0.646$. It is enough to satisfy

$$q^{\frac{1}{2}} \geq 2\left(\frac{s-1}{\delta}\right)+3. \tag{4.37}$$

Evidently, (4.37) holds for $q\geq 343$.

Next, we suppose $q\leq 341$ and repeat the above procedure. Since the product of the five smallest possible prime divisors of Q already exceeds $Q\leq 116623$, then $\omega(Q)\leq 4$, $s\leq 3$ and $\delta \geq 1-\frac{1}{7}-\frac{1}{13}-\frac{1}{19} > 0.727$. It follows that (4.37) holds for $q\geq 73$. When $q\leq 71$ a further repetition of this procedure is possible. Then $\omega(Q)\leq 3$, $s\leq 2$ and $\delta \geq 1-\frac{1}{7}-\frac{1}{13} > 0.780$ and (4.37) holds for $q\geq 31$.

Next, we assume $9\leq q\leq 29$ so that $Q\leq 871$. If $\omega(Q)\leq 2$, then (4.32) holds. This is necessarily the case when $q\not\equiv 1 \pmod 3$. It also occurs when $q=19$ ($Q=3\cdot 127$), and $q=13$ ($Q=3\cdot 61$).

For $q = 25$, $Q = 651 = 3 \cdot 7 \cdot 31$. The right-hand side of (4.36) with $k_0 = 1,\ s = 3$ and $\delta = 1 - \frac{1}{3} - \frac{1}{7} - \frac{1}{31}$ (> 0.491) is less than 4.88 so that (4.36) holds.

For $q = 16$, $Q = 273 = 3 \cdot 7 \cdot 13$. We apply the condition (4.9) with $k_0 = 1,\ p_1 = 3,\ p_2 = 13$ and $p_3 = 7$ ($s = 3$). Since $3|q^{\frac{3}{4}} + 1$ and $13|q^{\frac{3}{2}} + 1$, by Corollary 4.2.5 we have

$$\begin{aligned}
\pi_0(Q) &\geq \pi_0(3) + \pi_0(13) + \pi_0(7) - 2\pi_0(1) \\
&= \pi_0(3) + \pi_0(13) - \frac{8}{7}\pi_0(1) + \left(\pi_0(7) - \frac{6}{7}\pi_0(1)\right) \\
&\geq 2 \cdot 5 \cdot 21 + 12 \cdot 3 \cdot 5 - \frac{8 \cdot 255}{7} - \frac{6}{7} \cdot \frac{15}{16} \cdot 64 \\
&> 47.
\end{aligned}$$

For $q = 7$, the right side of (4.32) is $\frac{6}{7} \cdot 3 + 7^{-\frac{3}{2}} < 2.626 < \sqrt{7}$ so that this condition is satisfied. More easily, the inequality (4.32) is satisfied for $q = 2,\ 3$ and 5, since Q is prime in each case and $q^{\frac{1}{2}} > q^{-\frac{3}{2}}$ trivially holds.

Finally, observe that none of the sufficient conditions are satisfied when $q = 4$: indeed, the conclusion of Theorem 5.1.1 is false in this case. There are also no primitive polynomials of degree $n = 3$ with zero first coefficient in existence.

Chapter 5

The second coefficient

This chapter is dedicated to prescribing the second coefficient (that is, the coefficient of x^{n-2}) of a primitive polynomial. Recall that it has been proved that the HMPC holds whenever $n \geq 9$ (see [8]) and $n \leq 3$ (covered by [5] and [20]). We will show that there exists a primitive polynomial of degree n, $4 \leq n \leq 8$, over any finite field, with its second coefficient arbitrarily prescribed; 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. In particular, this establishes the HMPC when $n = 4$ (the remaining case of prescribing the third coefficient follows from [9]).

When the degree n is 6 or higher, we additionally prescribe the constant coefficient. While this constraint yields stricter criteria for existence of a primitive polynomial of the desired form, it enables the use of the reciprocal polynomial, which means the existence of polynomials with prescribed $(n-2)$-nd coefficient is proved at the same time. Another new and very important feature here is the use of p-adic analysis when the characteristic of the field is 2.

The papers of Han [18] and Cohen and Mills [11] cover most cases with $m = 2$ and $n \geq 5$ (although the situation when q is even and $n = 5$ or 6 is not altogether clear, and significant computer verification in a large number of cases was necessary). In spite of some work having been done in this area, we will here give not only a detailed and complete account of the case when $n = 4$, but also when $n = 5$, and the cases when the prescribed coefficient is non-zero and $6 \leq n \leq 8$. Like in the previous chapter, we here aim for a self-contained proof with a minimal amount of computation. Nevertheless, sometimes a primitive polynomial (usually over a very small field) has to be explicitly found to show it exists.

5.1 Main results

The following theorem asserts the existence of a primitive polynomial of degree higher than 3, with arbitrarily prescribed second coefficient.

Theorem 5.1.1. *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 5.1.1.

Corollary 5.1.2. *Suppose $n = 4$. Then the HMPC holds.*

We have already announced that, for the degree $n \geq 6$, we will prove a stronger version of Theorem 5.1.1 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 5.1.3. *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 5.1.1 (for $a = 0$) and Theorem 5.1.3 (for $a \neq 0$) imply further cases of the HMPC, as stated in the Corollary below.

Corollary 5.1.4. *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 5.1.3, for $a \neq 0$ we need only consider $n = 4$ or 5 in Theorem 5.1.1. 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).

For Theorem 5.1.3 (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 5.1.5. *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 $\gamma^{\frac{q^n-1}{q-1}} = c$ 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 5.1.5, it suffices to show that $\pi_{a,c}(E_n)$ is positive.

In order to prove Theorems 5.1.1 and 5.1.3 as efficiently as we possibly can, we will separately treat fields of odd and fields of even characeristics. The reason for this lies, as we will see later, in the fact that the method used when the characteristic of the field is odd, fails when the characteristic of the field is 2, due to prescribing the second coefficient.

5.2 The odd problem

By the Newton's formula (Lemma 3.2.1), the second symmetric function σ_2 of the roots of a separable monic irreducible polynomial satisfies

$$2\sigma_2 = s_1^2 - s_2, \tag{5.1}$$

where σ_2, s_1 and s_2 are as defined in Lemma 3.2.1. The following result follows immediately from (5.1).

Lemma 5.2.1. *For any $z \in \mathbb{F}_q$, suppose that $f(x) \in \mathbb{F}_q[x]$ is irreducible of degree n is such that $s_1 = z$ and $s_2 = z^2 - 2a$. Then f has second coefficient a.*

From Lemma 5.2.1 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.

For $\alpha,\ \beta \in \mathbb{F}_q$ and η a multiplicative character of $\mathbb{F}_{q^n}^*$, we introduce the following character sum notation:

$$S_n(\alpha,\beta;\eta) \;:=\; \sum_{\gamma\in\mathbb{F}_{q^n}} \chi_n(\alpha\gamma^2+\beta\gamma)\eta(\gamma). \tag{5.2}$$

We summarize standard estimates for $S_n(\alpha,\beta;\eta_d)$ (see [2], (1.3)) in a lemma.

Lemma 5.2.2. *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

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

We shall apply Lemma 5.2.2 not only to character sums over $\mathbb{F}_{q^n}$ but also to character sums over $\mathbb{F}_q$ itself (with $n=1$).

Recall that $\int_{d|k}\eta_d$ stands for $\sum_{d|k}\frac{\mu(d)}{\phi(d)}\sum_{(d)}\eta_d$, as defined in Section 4.2. Using characteristic functions, we can deduce basic formulas for $\pi_a(k)$ and, when $a\neq 0$, $\pi_{a,c}(k)$.

Lemma 5.2.3. *Suppose q is odd, $a\in\mathbb{F}_q$ is given and k divides q^n-1. Then*

$$q^2\pi_a(k) \;=\; \theta(k)\int_{d|k}\sum_{\alpha,\beta,z\in\mathbb{F}_q}\bar{\chi}(\alpha(z^2-2a)+\beta z)\ S_n(\alpha,\beta;\eta_d). \tag{5.3}$$

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

$$\begin{aligned}\frac{q^2\pi_a(k)}{\theta(k_0)} \;&=\; \delta\int_{d|k_0}\sum_{\alpha,\beta,z\in\mathbb{F}_q}\bar{\chi}(\alpha(z^2-2a)+\beta z)\ S_n(\alpha,\beta;\eta_d)\\ &+\; \sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right)\int_{d|k_0}\sum_{\alpha,\beta,z\in\mathbb{F}_q}\bar{\chi}(\alpha(z^2-2a)+\beta z)S_n(\alpha,\beta;\eta_{dp_i}).\end{aligned} \tag{5.4}$$

In particular, the contribution to the right-hand side of (5.4) attributable to values of $\alpha=\beta=0$ (the "main term") is $\delta\cdot q(q^n-1)$.

Proof. We derive (5.4) by using the equivalence of the right-hand sides of (3.6) and (3.7).

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 (5.4).

Of course, (5.3) is recovered from (5.4) by setting $s = 1$. □

Now that we have an expression for $\pi_a(k)$, we wish to obtain an analogous equation for $\pi_{a,c}(k)$ (provided $a \neq 0$).

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

$$\frac{1}{q-1}\sum_{\nu\in\widehat{\mathbb{F}_q^*}} \nu(N_n(\gamma)c^{-1}).$$

Let $\hat{\nu}$ denote the lift of ν to $\widehat{\mathbb{F}_{q^n}^*}$ (so that $\hat{\nu}(\gamma) = \nu(N_n(\gamma))$. By additionally incorporating the characteristic function for elements $\gamma \in \mathbb{F}_{q^n}$ satisfying $N_n(\gamma) = c$ to the expression (5.4), we obtain the following modification of Lemma 5.2.3.

Lemma 5.2.4. *Suppose $a, c \in \mathbb{F}_q^*$ with c a primitive element of $\mathbb{F}_q$, and q is odd. Suppose also that k divides E_n and (k_0, s) is a decomposition of k. Then,*

$$\frac{q^2(q-1)\pi_{a,c}(k)}{\theta(k_0)} = \delta \sum_{d|k_0} \sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*}\\ \alpha,\beta,z\in\mathbb{F}_q}} \bar{\nu}(c)\bar{\chi}(\alpha(z^2-2a)+\beta z)\ S_n(\alpha,\beta;\eta_d\hat{\nu})$$

$$+ \quad \sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right) \sum_{d|k_0} \sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*}\\ \alpha,\beta,z\in\mathbb{F}_q}} \bar{\nu}(c)\bar{\chi}(\alpha(z^2-2a)+\beta z) S_n(\alpha,\beta;\eta_{dp_i}\hat{\nu}). \tag{5.5}$$

In particular, the contribution to the right-hand side of (5.2.4) *attributable to values of $\alpha = \beta = 0$ (the "main term") is $\delta \cdot q(q^n - 1)$.*

At this point it is convenient to split the discussion according to whether the prescribed coefficient a is non-zero (*the non-zero probem*) or zero (*the zero probem*).

5.3 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 5.3.1. *Suppose q is odd and $a \neq 0$. Let $k|q^n-1$ and (k_0, s) be a decomposition of k. Suppose*

$$q^{\frac{n-2}{2}} > 4W(k_0)\Delta_{s,\delta}. \tag{5.6}$$

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

$$q^{\frac{n-2}{2}} > 4W(q^n - 1). \tag{5.7}$$

Proof. Consider the expression (5.4). We aggregate the contributions to the right-hand 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 $\frac{z}{\beta} \in \mathbb{F}_q$. The right-hand side of (5.4) then takes the form

$$\delta \int_{d|k_0} \sum_{\alpha\in\mathbb{F}_q} \sum_{\beta\in\mathbb{F}_q^*} \chi(2a\alpha\beta^2)\bar{\tilde{\eta}}_d(\beta) \sum_{z\in\mathbb{F}_q} \bar{\chi}(\alpha z^2 + z)\ S_n(\alpha, 1; \eta_d),$$

which is the same as

$$\delta \int_{d|k_0} \sum_{\alpha\in\mathbb{F}_q} S_1(2a\alpha, 0; \bar{\tilde{\eta}}_d)\ \overline{S_1(\alpha, 1; \mathbf{1})}\ S_n(\alpha, 1; \eta_d). \tag{5.8}$$

In (5.8), if $\alpha = 0$, then, by Lemma 5.2.2, $S_1(\alpha, 1; \mathbf{1}) = 0$. 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 5.2.2 that (5.8) 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 5.2.2 yields that (5.8) 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 (5.8) 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 (once for A and once for $-A$), replacing $\gamma \in \mathbb{F}_{q^n}$ by $\frac{\gamma}{A}$ and $z \in \mathbb{F}_q$ by $\frac{z}{A} \in \mathbb{F}_q$ in (5.8) gives

$$\begin{aligned} & \frac{1}{2}\,\delta \int_{d|k_0} \sum_{A\in\mathbb{F}_q^*} \chi(2aA^2)\bar{\tilde{\eta}}_d \sum_{z\in\mathbb{F}_q} \chi(z^2)\; S_n(1,0;\eta_d) \\ = \quad & \frac{1}{2}\,\delta \int_{d|k_0} S_1(2a,0;\;\bar{\tilde{\eta}}_d)\;\overline{S_1(1,0;\;\mathbf{1})}\; S_n(1,0;\eta_d). \end{aligned}$$

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

$$\frac{1}{2}\,\delta \int_{d|k_0} S_1(2ac,0;\;\bar{\tilde{\eta}}_d)\;\overline{S_1(c,0;\;\mathbf{1})}\; S_n(c,0;\eta_d).$$

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 (5.4) (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 (5.4) exceeds

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

with $\Delta_{s,\delta}$ as in Section 3.3, since $\sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right) = s-1\;+\delta$. □

The same reasoning, together with taking the $q-1$ characters of $\widehat{\mathbb{F}_q^*}$ into account, yields an analogous criterion for $\pi_{a,c}(E_n)$.

Proposition 5.3.2. *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*

$$q^{\frac{n-4}{2}} > 4\left(1-\frac{1}{q}\right)W(k_0)\Delta_{s,\delta}. \tag{5.9}$$

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

$$q^{\frac{n-4}{2}} > 4\left(1-\frac{1}{q}\right)W(E_n). \tag{5.10}$$

Granted the criteria for existence of primitive polynomials in $\mathbb{F}_q[x]$ depending on divisors of q, we will now split our work in five parts, according to the degree n of the

polynomials ($4 \leq n \leq 8$). As we will see, working becomes much easier and faster as the degree n grows larger.

5.3.1 Quartics

Take $n = 4$. Then the condition (5.6) takes the form

$$q > 4W(k_0)\Delta_{s,\delta}. \tag{5.11}$$

We will 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 4.4.1), 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 5.3.3. *Suppose that $n = 4$, q is 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. We prove this lemma in three steps, taking $\omega_1 \geq 15$ and $\omega_2 \geq 11$, $\omega_1 \leq 14$ and $\omega_2 \geq 11$ and $\omega_1 \geq 15$ or $\omega_2 \leq 10$ respectively in each step.

First suppose $\omega_1 \geq 15$ and $\omega_2 \geq 11$. By $(A.5)$, 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 $(A.17)$, when integer h is a product of primes $l \equiv 1 \pmod 4$ and $\omega(h) \geq 11$, $W(h) < h^{\frac{1}{5}}$. 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 (5.7), 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 three smallest 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 (5.11) 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 (5.6) (equivalent to (5.11) 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 $s = \omega_2 \leq 10$,

$\delta \geq 1 - \sum_{\substack{l \leq 89 \\ l \equiv 1 (\mathrm{mod}\, 4)}} \frac{1}{l} > 0.518$ and $\Delta_{s,\delta} < 19.38$. Now (5.11) is satisfied whenever $q \geq 8636$, which completes the proof since $\omega_1 \geq 15$ implies $q > 10^8$. □

Following Lemma 5.3.3, we can assume $\omega_1 \leq 14$, $\omega_2 \leq 10$. 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

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

where in each sum the prime l_i indicates the i-th prime in the given congruency class mod 4. When working with particular values of q, we can very quickly make the observation that this value of δ yields the notional minimal for the bounded values of ω_1 and ω_2 in the current application: we aim to give a lower bound for δ and the result depends on whether certain primes are considered as divisors of K_1 or K_2. When $p = 5$, for minimal δ it can be supposed that all odd prime divisors of K_1 are $\equiv 3 \pmod 4$. Like in the previous chapter, q_{min} stands for the minimal integral value of q for which (5.11) with the above minimum value of δ holds. The sieving steps are shown 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		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 steps 4 and 5, we have supposed $\omega_2 \leq 3$: although numerically $\omega_2 = 4$ is possible, there are no integers $\frac{q^2+1}{2}$, $q \leq 405$ odd, with this value of ω_2.

Next, for all odd prime powers $q \leq 243$ the computer algebra package Maple is used to check whether (5.11) (with $k_0 = \gcd(6, q)$) holds. This is so, except for those in $\{3, 5, \ldots, 73, 83, 89, 103\}$, which is a set of cardinality 27. The largest composite value in this set is 49. In this case $q^4 - 1 = 2^6 \cdot 3 \cdot 5^2 \cdot 1201$ and $Q_4 = 2^4 \cdot 3$. Half the square-free divisors d of $q^n - 1$ divide Q_4 and for these we can use the bound $2\delta(1 + \frac{1}{7})(q-1)q^{\frac{n}{2}+1}$ in

Proposition 5.3.1 (instead of $4\delta(q-1)q^{\frac{n}{2}+1}$). Hence, for $q = 49$, the condition (5.11) can be replaced by $q > \frac{22}{7}W(k_0)\Delta_{s,\delta}$, which is satisfied with the choice of $k_0 = 2$.

For each of these remaining values the existence of primitive quartics with prescribed coefficient of x^2 was proved directly (with Maple). At this place, we only give the polynomials $f(x)$ in question, for $f(x) \in \mathbb{F}_q[x]$, $q < 10$, as these are the most delicate cases. For the polynomials over larger fields, see Appendix B.

In the first table, $q = 9$ and the field $\mathbb{F}_9$ is defined as $\mathbb{F}_3(\alpha)$ with α a root of the polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$.

a	$f(x)$		a	$f(x)$
1	$x^4 + x^2 + x + \alpha$		$\alpha + 1$	$x^4 + (\alpha+1)x^2 + \alpha x + 2\alpha$
2	$x^4 + 2x^2 + x + (\alpha + 1)$		$\alpha + 2$	$x^4 + (\alpha+2)x^2 + \alpha x + (\alpha+1)$
α	$x^4 + \alpha x^2 + x + \alpha$		$2\alpha + 1$	$x^4 + (2\alpha+1)x^2 + \alpha x + \alpha$
2α	$x^4 + 2\alpha x^2 + (2\alpha+1)x + \alpha$		$2\alpha + 2$	$x^4 + (2\alpha+2)x^2 + x + (2\alpha+2)$

The second table comprises of the primitive polynomials over the fields $\mathbb{F}_7$, $\mathbb{F}_5$ and $\mathbb{F}_3$.

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

This concludes the proof of the existence of primitive polynomials of degree 4 over a field of odd characteristic, with non-zero second coefficient arbitrarily prescribed. In the next subsection, we treat the polynomials of degree 5; as the degree is higher, the condition (5.6) is more generous and the number of cases in which the existence of primitive polynomials has to be proved by finding them explicitly decreases drastically.

5.3.2 Quintics

Take $n = 5$. Then (from (5.6)), the sufficient condition for existence of primitive polynomials over $\mathbb{F}_q$ is

$$q^{\frac{3}{2}} > 4W(k_0)\Delta_{s,\delta}. \tag{5.12}$$

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 $\equiv 1 \pmod{10}$. Write ω_1 for $\omega(K_1)$ and ω_2 for $\omega(K_2)$.

Lemma 5.3.4. *Suppose that $n = 5$, q odd and $\omega_1 \geq 6$ or $\omega_2 \geq 10$. Let a $(\neq 0) \in \mathbb{F}_q$. Then there exists a primitive polynomial of degree 5 over $\mathbb{F}_q$ with the coefficient of x^3 prescribed as a.*

Proof. We consider three distinct cases, like in the proof of the Lemma 5.3.4. First, suppose $\omega_1 \geq 6$ and $\omega_2 \geq 10$. Then, by $(A.1)$, $W(K_1) < q^{\frac{3}{7}}$, and by $(A.26)$, $W(K_2) < (q^4 + q^3 + q^2 + q + 1)^{\frac{1}{6}} < (q^5)^{\frac{1}{6}} = q^{\frac{5}{6}}$. It follows that $W(q^5 - 1) < q^{\frac{53}{42}}$. Consequently, by (5.7) to show existence it suffices that $q^{\frac{3}{2}} > 4q^{\frac{53}{42}}$, so certainly whenever $q \geq 338$. The latter evidently holds since $\omega_1 \geq 6$ implies $q \geq 30030$.

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 (3.5), $\delta \geq 1 - \frac{1}{7} - \frac{1}{11} > 0.766$ and consequently $\Delta_{s,\delta} < 3.31$. By the above reasoning, $W(k_0) < 8q^{\frac{5}{6}}$ and (5.12) 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 $s \leq 9$,

$$\delta \;\geq\; 1 - \sum_{\substack{l \leq 181 \\ l \equiv 1 (\mathrm{mod}\, 10)}} \frac{1}{l} \;>\; 0.792$$

and $\Delta_{s,\delta} < 12.11$, when k_0 is taken to be $k_0 = K_1$. Now (5.12) is satisfied whenever $q \geq 38$, which holds since $\omega_1 \geq 6$ yields $q \geq 30030$. □

After Lemma 5.3.4, we can assume $\omega_1 \leq 5$ and $\omega_2 \leq 9$ and run the sieve. 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 in the following table.

#	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 $k_0 = 2$ and $s = 2$ in each case. Then (5.12) is satisfied : $q > (4W(k_0)\Delta_{s,\delta})^{\frac{2}{3}}$ as shown in the table below.

q	$q^5 - 1$	$\delta >$	$(4W(k_0)\Delta_{s,\delta})^{\frac{2}{3}} <$
13	$2^2 \cdot 3 \cdot 30941$	0.666	$(4 \cdot 2 \cdot 3.51)^{\frac{2}{3}} = 9.23...$
11	$2 \cdot 5^2 \cdot 3221$	0.799	$(4 \cdot 2 \cdot 3.26)^{\frac{2}{3}} = 8.79...$
9	$2^3 \cdot 11^2 \cdot 61$	0.892	$(4 \cdot 2 \cdot 3.13)^{\frac{2}{3}} = 8.55...$

This only leaves $q = 7$, 5 and 3. 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	$x^5 + 6x^3 + 2$	—	—

As predicted, proving that the HMPC holds for polynomials of degree 5 requires much less numerical work as the lower degree 4. Degrees 6 and higher are even easier to deal with. However, at this point we slightly change our tactics and demand that the polynomials satisfy the stricter conditions of Theorem 5.1.3.

5.3.3 Degrees 6, 7 and 8

We will 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 5.3.2. It yields the sufficient conditions

$$q > 4\left(1-\frac{1}{q}\right)W(k_0)\Delta_{s,\delta} \quad \text{when } n=6; \tag{5.13}$$

$$q^{\frac{3}{2}} > 4\left(1-\frac{1}{q}\right)W(k_0)\Delta_{s,\delta} \quad \text{when } n=7; \tag{5.14}$$

$$q^2 > 4\left(1-\frac{1}{q}\right)W(k_0)\Delta_{s,\delta} \quad \text{when } n=8. \tag{5.15}$$

Sextics

First, we consider the polynomials of degree 6. Let K_1 be 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 (as such, K_1 and K_2 are necessarily both odd). Hence the product of distinct primes in E_6 is $K_1 \cdot K_2$. Notice that 3 is never a factor of K_2 and so (by an analogue of Lemma 4.4.1) 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 5.3.5. *Suppose that $n=6$, q is 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 $(A.10)$, $W(K_1) < q^{\frac{5}{18}}$, and, observing that $\frac{q^6-1}{q^2-1} = q^4+q^2+1 < 2q^4$, $W(K_2) < (2q^4)^{\frac{10}{63}}$ by $(A.23)$. Therefore $W(E_6) < 2^{\frac{10}{63}} q^{\frac{115}{126}}$ and, putting $s=1$, criterion (5.13) guarantees existence whenever $q > 4W(E_n)$, i.e., $q > 4 \cdot 2^{\frac{10}{63}} q^{\frac{115}{126}}$, 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 three smallest 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 (5.9) is satisfied whenever $q \geq 4322937$. This suffices since $q > 10^{11}$ as $\omega_2 \geq 24$.

Now suppose $\omega_1 \geq 10$ and $\omega_2 \leq 23$. Setting $k_0 = K_1$ yields $s \leq 23$,

$$\delta \geq 1 - \sum_{\substack{l \leq 223 \\ l \equiv 1 (\mathrm{mod}\, 6)}} \frac{1}{l} > 0.499$$

and $\Delta_{s,\delta} < 48.10$. Hence (5.9) 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 we summarize in the following table.

#	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 point, 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 and 101. The largest four of these satisfy condition (5.13) with $k_0 = 1$, as illustrated below.

q	E_6	s	$\delta >$	$4W(k_0)\Delta_{s,\delta} <$
101	$3 \cdot 7 \cdot 13 \cdot 17 \cdot 37 \cdot 10303$	6	0.360	$4 \cdot 1 \cdot 15.89 = 63.65$
83	$3 \cdot 7 \cdot 19 \cdot 367 \cdot 2269$	5	0.468	$4 \cdot 1 \cdot 10.55 = 42.20$
59	$3 \cdot 5 \cdot 7 \cdot 163 \cdot 3541$	5	0.317	$4 \cdot 1 \cdot 14.62 = 58.48$
41	$3 \cdot 7 \cdot 547 \cdot 1723$	4	0.521	$4 \cdot 1 \cdot 7.76 = 31.04$

We will deal with $q = 29$ later, 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 the step 7 of the seiving process summarized in the table above, $q \leq 63$ implies $\omega_2 \leq 5$, but there are no primes or prime powers of that size with $\omega_2 = 5$. We proceded similarly in the next step, where three such values with $\omega_2 = 4$ exist: $37, 47$ and 49. They all fit into (5.9) 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.

q	E_6	s	$\delta >$	$4W(k_0)\Delta_{s,\delta} <$
49	$5 \cdot 13 \cdot 19 \cdot 43 \cdot 181$	5	0.641	$4 \cdot 1 \cdot 8.25 = 33.00$
47	$3 \cdot 7 \cdot 37 \cdot 61 \cdot 103$	5	0.470	$4 \cdot 1 \cdot 9.52 = 38.08$
37	$7 \cdot 19 \cdot 31 \cdot 43 \cdot 67$	5	0.734	$4 \cdot 1 \cdot 7.45 = 29.80$
31	$7 \cdot 19 \cdot 331$	3	0.801	$4 \cdot 1 \cdot 4.50 = 18.00$
27	$7 \cdot 19 \cdot 37 \cdot 757$	4	0.776	$4 \cdot 1 \cdot 5.87 = 23.48$
25	$7 \cdot 13 \cdot 31 \cdot 601$	4	0.746	$4 \cdot 1 \cdot 6.03 = 24.12$

For illustration, we here give the 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):

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

The rest of the relevant polynomials are listed in the Appendix B.

Septics

Consider the polynomials over $\mathbb{F}_q[x]$ of degree 7, with the (non-zero) coefficient of x^5 arbitrarily prescribed.

Lemma 5.3.6. *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 $\omega(E_7) \geq 6$. Bound $(A.31)$ then provides $W(E_7) < (E_7)^{\frac{1}{6}}$. Certainly $E_7 \leq Q_7$ and we can further estimate the number of square-free divisors of E_7 as $W(E_7) < (Q_7)^{\frac{1}{6}} < (q^7)^{\frac{1}{6}} = q^{\frac{7}{6}}$. Criterion (5.14) 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 $\omega(E_7) \leq 5$. Setting $k_0 = 1$ implies $s \leq 5$. Recall that, by Lemma 4.4.1, every prime divisor of E_7 is $\equiv 1 \pmod{14}$. Therefore $\delta \geq 1 - \frac{1}{29} - \frac{1}{43} - \frac{1}{71} - \frac{1}{113} - \frac{1}{127} > 0.911$ and (5.14) is satisfied for $q \geq 9$. Among the remainding values, $q = 7$ and 5 satisfy (5.14) with $k_0 = 1$, whereas when $q = 3$, the polynomials need to be found explicitly:

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

Octics

Consider the polynomials of degree 8. 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 4.4.1 any prime divisor l of K_2 is $\equiv 1 \pmod 8$, i.e., $l \in L_8$. Let $\omega_1 := \omega(K_1)$ and $\omega_2 := \omega(K_2)$.

Lemma 5.3.7. *Let $n = 8$, 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.*

Proof. Suppose, first, that $\omega_1 \geq 8$ and $\omega_2 \geq 6$. Both conditions yield $q > 470$. Applying the bound $(A.9)$, we can estimate the number of square-free divisors of K_1 to $W(K_1) < \big((q+1)(q^2+1)\big)^{\frac{3}{10}}$. Noting that $(q+1)(q^2+1) < 2q^3$ for $q \geq 2$, we can further estimate $W(K_1) < 2^{\frac{3}{10}} q^{\frac{9}{10}}$. Similarly, $W(K_2) < q^{\frac{68}{100}}$ by $(A.34)$ and thereby $W(E_8) < 2^{\frac{3}{10}} q^{\frac{158}{100}}$. Criterion (5.15) is then certainly sufficient whenever $q^2 > 2^{\frac{3}{10}} q^{\frac{158}{100}}$ or $q \geq 45$, which is the case.

Now assume $\omega_1 \leq 7$ and $\omega_2 \geq 6$. Let (k_0, s) be the decomposition where $k_0 = K_2$. Thus $W(K_2) < q^{\frac{17}{25}}$, $s \leq 7$, $\delta \geq 1 - \frac{1}{3} - \frac{1}{5} - \ldots - \frac{1}{19} > 0.044$ and hence $\Delta_{s,\delta} < 138.37$. Consequently, criterion (5.15) is settled whenever $q^2 > 4 \cdot q^{\frac{17}{25}} \cdot 138.37$, i.e. $q \geq 120$, which is so as we have assumed that $q > 470$.

Let now $\omega_1 \geq 8$ and $\omega_2 \leq 5$ and let (k_0, s) be the decomposition where $k_0 = K_1$. Then $W(K_1) < 2^{\frac{3}{10}} q^{\frac{9}{10}}$, $s \leq 5$, $\delta \geq 1 - \frac{1}{17} - \frac{1}{41} - \frac{1}{73} - \frac{1}{89} - \frac{1}{97} > 0.881$ and $\Delta_{s,\delta} < 6.55$. Criterion (5.15) is satisfied for $q^2 > 2^{\frac{3}{10}} \cdot q^{\frac{9}{10}} \cdot 6.55$, i.e. $q \geq 24$, which is the case.

□

Provided Lemma 5.3.7, we proceed assuming $\omega_1 \leq 7$ and $\omega_2 \leq 5$ and run the sieving process. It takes only two steps to show that the criterion (5.15) is satisfied for values of q larger than 10, and individual checks for $q = 9, 7, 5$ and 3 show that it is satisfied for these values, too. The six steps are presented in detail 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		7	5	105	3	9	0.617	14.97	22
2	≤ 19	4	3	3	1	6	0.469	12.67	11
3	9	2	2	1	0	4	0.711	6.22	5
4	7	1	1	1	0	2	0.799	3.27	4
5	5	2	1	1	0	3	0.586	5.42	5
6	3	1	1	1	0	2	0.775	3.30	3

This concludes our work with primitive polynomials over $\mathbb{F}_q$, where q is odd and the prescribed second coefficient a of the polynomial is non-zero. The following section is about prescribing a zero second coefficient, in particular when the degree of the polynomial is 4 or 5 (the HMPC has in this case already been established for degrees $6 \leq n \leq 8$).

5.4 The odd zero problem

Throughout this section we continue to assume that q is odd but the prescribed coefficient a is now zero. By Lemma 3.3.1, in order to show that there exists a primitive polynomial of desired form over the field $\mathbb{F}_q$, it suffices to prove that $\pi_0(Q_n)$ is positive.

Proposition 5.4.1. *Let $k|Q_n$ and let (k_0, s) be a decomposition of k. Suppose q is odd and*

$$q^{\frac{n-3}{2}} > 2\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{5.16}$$

Then $\pi_0(k)$ is positive.

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

$$q^{\frac{n-3}{2}} > 2\left(1 - \frac{1}{q}\right) W(Q_n). \tag{5.17}$$

Proof. Suppose $k|Q_n$ and consider the expression (5.4). We aggregate the contributions to the right-hand side relating to a specific multiplicative character η_d or η_{dp_i}.

For $d|k_0$, as the contribution of terms with $\beta \neq 0$, we obtain

$$\delta \int_{d|k_0} \sum_{\alpha \in \mathbb{F}_q} S_1(0,0;\bar{\tilde{\eta}}_d)\ \overline{S_1(\alpha,1;\mathbf{1})}\ S_n(\alpha,1;\eta_d). \tag{5.18}$$

We can ignore contributions from terms with $\alpha = 0$ as $S_1(0,1;\mathbf{1}) = 0$ by Lemma 5.2.2, and may therefore suppose that the sum is over $\alpha \in \mathbb{F}_q^*$. Since $\tilde{\eta}_d$ has order 1, then

$S_1(0,0;\bar{\tilde{\eta}}_d) = q-1$, 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 (5.18), 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 the expression (5.4) 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 5.1.1 for $6 \leq n \leq 8$.

5.4.1 Quartics

Take $n=4$. Then, for a decomposition (k_0, s) of $Q_4 = (q+1)(q^2+1)$, (5.16) takes the form

$$q^{\frac{1}{2}} > 2\left(1-\frac{1}{q}\right) W(k_0)\,\Delta_{s,\delta}. \tag{5.19}$$

Let the product of distinct primes in Q_4 be written 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 5.4.2. *Let $n=4$, 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. Suppose $\omega_1 \geq 28$ and $\omega_2 \geq 40$. Then the bounds $(A.6)$ and $(A.18)$ guarantee that $W(Q_4) \leq W(K_1 \cdot K_2) < q^{\frac{1}{5}+\frac{7}{25}} = q^{\frac{12}{25}}$. Consequently, by criterion (5.17), 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 (5.19) is satisfied whenever $q \geq 6.1 \cdot 10^{14}$. Since $\omega_2 \geq 40$, however, then $q > 10^{43}$.

Now 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 $\Delta_{s,\delta} < 102.27$. Thus condition (5.19) is satisfied whenever $q \geq 50418994$. This holds since $\omega_1 \geq 28$ yields $q \geq 10^{42}$. □

As a consequence of Lemma 5.4.2, we can assume $\omega_1 \leq 27$ and $\omega_2 \leq 39$.

We shall consider decompositions (k_0, s) of Q_4, 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

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

The sieving steps are shown in the table below. As usual q_{min} denotes the minimum integer q satisfying condition (5.19) numerically.

#	q	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		27	39	210	4	62	0.159	385.65	152295345
2	≤ 152295343	8	10	30	3	15	0.332	44.17	499454
3	≤ 499453	6	7	6	2	11	0.229	45.67	133488
4	≤ 133487	6	6	6	2	10	0.248	38.30	93881
5	≤ 93879	5	6	6	2	9	0.291	29.50	55696

The first three lines of figures in the above table are 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, 51869, 53129, 67829, 81509, 84629 and 85469 were found with $\omega_1 = 6$. However, they all satisfy criterion (5.19) with k_0 chosen to be 6.

q	Q_4	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
85469	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 37 \cdot 593 \cdot 6159317$	2	6	0.537	11.32	8202
84629	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 31 \cdot 137 \cdot 613 \cdot 42641$	2	7	0.539	13.14	11051
81509	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 797 \cdot 4167953$	2	6	0.578	10.66	7273
67829	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 176952817$	2	6	0.468	12.69	10307
53129	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 53 \cdot 733 \cdot 2137$	2	8	0.443	17.81	20301
51869	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 29 \cdot 46386089$	2	6	0.493	12.15	9448
43889	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 29 \cdot 281 \cdot 118189$	2	7	0.475	14.64	13718
30029	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 450870421$	2	5	0.489	10.18	6633

As indicated, this establishes Theorem 5.1.1 for $q \geq 55696$. We may assume $q \leq 55695$ and continue with step 6 of 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	≤ 55695	5	5	6	2	8	0.316	24.13	37258
7	≤ 62773	6	4	6	2	8	0.299	25.35	41101
8	≤ 55324	4	6	6	2	8	0.344	22.32	31868
9	≤ 37257	5	4	6	2	7	0.343	19.48	24271
10	≤ 37257	4	5	6	2	7	0.368	18.27	24343
11	≤ 41100	6	3	6	2	7	0.334	19.95	25457
12	≤ 31867	3	6	6	2	7	0.435	15.78	15932
13	≤ 24270	4	4	6	2	6	0.396	14.62	13692
14	≤ 24372	5	3	6	2	6	0.377	15.24	14850
15	≤ 24372	3	5	6	2	6	0.459	12.88	10466

There are no integers q with $\omega_1 \geq 5$ or $\omega_2 \geq 5$ that lie outside the scope of the lines $6-10$. 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 condition (5.19) is indeed satisfied in these cases (each time, k_0 is taken to be 6).

q	Q_4	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
24023	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 61 \cdot 269 \cdot 3517$	2	7	0.468	14.83	14076
23873	$2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 23 \cdot 53 \cdot 173 \cdot 181 \cdot 457$	2	7	0.647	11.28	8144
21713	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17^2 \cdot 37 \cdot 47 \cdot 4409$	2	7	0.458	15.11	14612
21419	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 29 \cdot 229 \cdot 2657$	2	7	0.482	14.45	13364
20747	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 29 \cdot 653 \cdot 2273$	2	7	0.491	14.22	12942
19739	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 47 \cdot 53 \cdot 433 \cdot 653$	2	7	0.536	13.20	11152
19469	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 59 \cdot 173 \cdot 4957$	2	7	0.550	12.91	16667
15287	$2^4 \cdot 3 \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 37 \cdot 53 \cdot 701$	2	7	0.474	14.66	13755

More systematically, Maple (with $k_0 = \gcd(6, Q_4)$) was used to check (5.19) 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.

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	$f(x)$
5	$x^4 + x^3 + x + 3$
7	$x^4 + x^3 + x + 3$
13	$x^4 + x^3 + x + 2$
19	$x^4 + 2x + 10$
31	$x^4 + 2x + 17$

The detailed list of the relevant polynomials can be found in Appendix B.

5.4.2 Quintics

Take $n = 5$. Then (5.16) becomes

$$q \ > \ 2\left(1 - \frac{1}{q}\right) \ W(k_0) \ \Delta_{s,\delta}. \tag{5.20}$$

Suppose that a prime l 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 5.4.3. *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 $(A.27)$ it follows that

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

Hence (5.20) 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 5.4.3, we can assume $s = \omega \leq 18$ (or 17). As before, we write q_{min} for the minimal integral value of q that satisfies the condition (5.20) with the displayed value of δ. The outcome is summarised in the following table where the figures focus on the more testing case when $5|Q_5$ until $q < 11$.

#	q	ω	$\delta \geq$	$\Delta_{s,\delta} \leq$	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
6	5	2	0.895	3.12	5
7	3	1	0.876	3.15	3

Note that in the step 7 in the above table, $s = 1$ and the condition (5.20) in this case takes the form $q > 2\left(1 - \frac{1}{q}\right) W(Q_5)$.

In the case of quintics, Theorem 5.1.1 holds without the need for any direct verification. This demonstrates the quality of the theoretical result, as well as emphasizes the delicateness of the case of quartics.

Similar considerations could be applied to degrees $n = 6, 7, 8$ but Theorem 5.1.1 in these cases when $a = 0$ follows, for instance, from [11]. Hence this completes the proof of the HMPC for $m = 2$ and q odd.

5.5 The even problem

Throughout this section, suppose $p = 2$ (so that q is even). Here, the use of 2-adic analysis will be required.

In this context, the identity (5.1) assumes the following shape.

Lemma 5.5.1. *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*

$$2\sigma_2 = s_1^2 - s_2. \tag{5.21}$$

Recall (from Section 2.5) that $s_t = \sum_{j=0}^{\infty} s_{t,j} 2^j,\ s_{t,j} \in \Gamma_1$.

Lemma 5.5.2. *Let f, σ_i and s_i be as in Lemma* 5.5.1. *Then $\sigma_2 \equiv s_{1,1}^2 \pmod 2$.*

Proof. Over $R_{1,2}$, equality (5.21) translates to

$$\begin{aligned} 2\sigma_2 &= (s_{1,0} + 2s_{1,1})^2 - (s_{1,0}^2 + 2s_{1,1}^2) \\ &= 4s_{1,0} + 2s_{1,1}^2 \\ &\equiv 2s_{1,1}^2 \pmod 4. \end{aligned}$$

Hence $\sigma_2 \equiv s_{1,1}^2 \pmod 2$. □

As a consequence of Lemma 5.5.2, for σ_2 to be prescribed modulo 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 5.5.2, 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 5.5.2, 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

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

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

$$\frac{1}{q^2}\sum_{\xi\in R_{1,2}}\chi(\xi(T_n(\gamma)-(z+2A)))\;=\;\frac{1}{q^2}\sum_{\alpha_0,\alpha_1\in\Gamma_{1,1}}\chi_{(n)}((\alpha_0+2\alpha_1)(\gamma))\,\chi(-(\alpha_0+2\alpha_1)z-2\alpha_0 A). \tag{5.22}$$

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

Lemma 5.5.3. *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 5.5.4. *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*

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

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 (5.22)) one obtains

$$\frac{q^2\pi_a(k)}{\theta(k)} \;=\; \int_{d|k}\sum_{\xi\in R_{1,2}}\chi(2\alpha_0 A)\; U_\xi\; S_n(\xi;\eta_d), \tag{5.23}$$

with U_ξ as in Lemma 5.5.3. Since $S_n(0;\eta_d) = 0$ unless $d = 1$, the contribution to (5.23) 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 5.5.3 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 5.1.5), there is an analogous expression for $\dfrac{(q-1)q\pi_{a,c}}{\theta(k_0)}$ to that of Lemma 5.5.4 comparable to the relationship Lemma 5.2.4 bears to Lemma 5.2.3. 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 $\dfrac{q\pi_a}{\theta(k_0)}$ or $\dfrac{(q-1)q\pi_{a,c}}{\theta(k_0)}$, the relevant bounds for $|S_n(\xi;\eta_d)|$ are as follows.

Lemma 5.5.5. *Suppose $\xi \in R^*_{1,2}$. Then $S_n(\xi;\mathbf{1}) = 0$. Further, if d (>1) divides q^n-1, then $|S_n(\xi;\eta_d)| \leq 2q^{\frac{n}{2}}$. Indeed, if $\alpha_1 \in \Gamma_{1,1}$ then $|S_n(2\alpha_1;\eta_d)| \leq q^{\frac{n}{2}}$.*

Proof. This follows from Corollary 6.1 of [23]. 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.

5.6 The even non-zero problem

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

Proposition 5.6.1. *Assume that q is even, $a \in \mathbb{F}_q$ is non-zero, $k|q^n-1$ and that (k_0,s) is a decomposition of k. Suppose also that*

$$q^{\frac{n-1}{2}} > 2\sqrt{2}\ W(k_0)\Delta_{s,\delta}. \tag{5.24}$$

Then $\pi_a(k)$ is positive.

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

$$q^{\frac{n-1}{2}} > 2\sqrt{2}\ W(q^n-1). \tag{5.25}$$

Proof. The sums over $\alpha \in \Gamma^*_{1,1}$ in (5.23) can be written as $\tilde{\eta}_d(a)S_1(1;\bar{\tilde{\eta}}_d)$. Then use Lemma 5.5.5 both for S_n and S_1. (The savings when $\tilde{\eta}_d$ is trivial easily compensate for the -1 in the main term.) □

For the polynomials with prescribed second coefficient and constant term, the additional constraint decreases the power of q on the left-hand side of the inequality, as given in the following proposition. However, as we only need consider the divisors of E_n in this case, the sufficient condition is not too strict.

Proposition 5.6.2. *Assume that q is even, $a \in \mathbb{F}_q$ is non-zero and c is a primitive element of $\mathbb{F}_q$. Assume also that $k|E_n$ and that (k_0,s) is a decomposition of k. Suppose that*

$$q^{\frac{n-3}{2}} > 2\sqrt{2}\left(1-\frac{1}{q}\right)W(k_0)\Delta_{s,\delta}. \tag{5.26}$$

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

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

$$q^{\frac{n-3}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(E_n). \tag{5.27}$$

5.6.1 Quartics

Suppose $n = 4$ and $k|q^n - 1$. Then, for any decomposition of k, condition (5.24) takes the form

$$q^{\frac{3}{2}} > 2\sqrt{2}\ W(k_0)\Delta_{s,\delta}. \tag{5.28}$$

Like in Section 5.3.1, 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 $\omega_i = \omega(K_i),\ i = 1, 2$. In particular, $q^4 - 1$ is odd, $3|K_1$ and all prime divisors of K_2 are $\equiv 1 \pmod 4$.

Lemma 5.6.3. *Suppose that $n = 4$, q even and $\omega_1 \geq 8$ or $\omega_2 \geq 6$. 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 $(A.9)$ and $(A.19)$,

$$\begin{aligned} W(q^4 - 1) &< (q^2 - 1)^{\frac{3}{10}}(q^2 + 1 - 1)^{\frac{1}{4}} \\ &< (q^2 - 1)^{\frac{1}{3}}(q^2 + 1 - 1)^{\frac{1}{4}} \\ &< q^{\frac{2}{3}+\frac{2}{4}} = q^{\frac{7}{6}}. \end{aligned}$$

Consequently, by (5.25), 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 (5.28) 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 (5.28) is satisfied whenever $q \geq 24.46^{\frac{6}{5}} = 46.36\ldots$. Necessarily however $q > 10^4$. □

As a consequence of Lemma 5.6.3 we can assume $\omega_1 \leq 7$ and $\omega_2 \leq 5$.

Take the decomposition with $k_0 = 3$ and apply the criterion (5.28) twice. The two steps are tabulated below; in each step, the resulting q_{min} is the smallest value of q satisfying (5.28).

#	q	$\omega_1 \leq$	$\omega_2 \leq$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		7	5	11	0.216	48.30	43
2	≤ 32	3	2	4	0.489	8.14	13

For $q \leq 8$, criterion (5.28) 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, over $\mathbb{F}_2$, no primitive quartic with coefficient of x^2 equal to 1 exists!

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

5.6.2 Quintics

Take $n = 5$. Then, for any decomposition (k_0, s) of $q^5 - 1$, the condition (5.24) takes the form

$$q^2 > 2\sqrt{2}\, W(k_0)\Delta_{s,\delta}. \tag{5.29}$$

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 $q - 1$. Note that, as q is even, $K_1$and K_2 odd. 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 5.6.4. *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 $(A.7)$, and $(A.25)$,

$$\begin{aligned} W(q^5-1) &< (q^2-1)^{\frac{1}{2}}(\sqrt{q^2+1}-1)^{\frac{1}{2}} \\ &< q\cdot q^{\frac{1}{2}} = q^{\frac{3}{2}}, \end{aligned}$$

provided $q > 8$. Criterion (5.24) 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 (5.29) is satisfied unless $q \leq 8$.

Next, suppose $\omega_1 \geq 3$ (whence $q > 105$) and $\omega_2 \leq 1$. Criterion (5.29) (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 (5.29) holds when $q > 4.6$.

There remain $q = 8, 4$ and 2. For $q = 8$, $q^5 - 1 = 7 \cdot 31 \cdot 151$ and 5.29 (with $s = 1$) holds since $64 > 16\sqrt{2}$. Although (5.29) cannot be satisfied, there does exist a primitive quintic in $\mathbb{F}_4[x]$ with arbitrary coefficient of x^2. For $\mathbb{F}_4$ defined as in the previous subsection, we have

a	$f(x) \in \mathbb{F}_4[x]$
1	$x^5 + x^3 + x + \alpha$
α	$x^5 + \alpha x^3 + (\alpha+1)x + (\alpha+1)$
$\alpha+1$	$x^5 + (\alpha+1)x^3 + \alpha x + \alpha$

Over $\mathbb{F}_2$, any irreducible quintic is primitive: it is enough to quote the example $x^5 + x^3 + 1$. □

5.6.3 Degrees 6, 7 and 8

For q a power of 2, we again consider degrees 6, 7 and 8 and prove a stronger result, namely, the existence of primitive polynomials that, in addition to the second coefficients, also have the constant terms are also prescribed (as a primitive elements of $\mathbb{F}_q$). Proposition 5.6.2 yields the sufficient conditions

$$q^{\frac{3}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta} \quad \text{when } n = 6; \tag{5.30}$$

$$q^{2} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta} \quad \text{when } n = 7; \tag{5.31}$$

$$q^{\frac{5}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta} \quad \text{when } n = 8. \tag{5.32}$$

Sextics

Suppose the degree of the polynomial is 6. Let K_1 be 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 (again, note that K_1 and K_2 are necessarily both odd). Hence the product of distinct primes in E_6 can be written as $K_1 \cdot K_2$. Any prime divisor l of K_2 is $\equiv 1 \pmod 6$ (by an analogue of Lemma 4.4.1 and because 3 is never a factor of K_2) Define $\omega_1 := \omega(K_1)$, $\omega_2 := \omega(K_2)$.

Lemma 5.6.5. *Suppose that $n = 6$, q is even 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.*

Since the condition (5.13) is more demanding than (5.30), the proof of Lemma 5.3.5 suffices here. Consequently, we may assume $\omega_1 \leq 9$ and $\omega_2 \leq 23$. The sieving steps (using the sufficient condition (5.30)) are summarized in the following table (in steps 3 and 4, $E_6 = 7 \cdot 13 \cdot 17 \cdot 241$ and $E_6 = 3 \cdot 19 \cdot 73$ respectively).

#	q	ω_1	ω_2	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		≤ 9	$23 \leq$	105	3	≤ 29	0.364	78.93	148
2	≤ 128	≤ 3	$6 \leq$	3	1	≤ 8	0.354	21.78	25
3	16	1	3	7	1	3	0.860	4.33	9
4	8	1	2	3	1	2	0.933	3.08	7

In $\mathbb{F}_2[x]$, the constant term of the polynomial necessarily equals 1 and the relevant sextic with the non-zero second coefficient is $f(x) = x^6 + x^4 + x^3 + x + 1$. For $\mathbb{F}_4$ defined by $x^2 + x + 1 \in \mathbb{F}_2[x]$ and α a root of the defining polynomial, Maple found the following six polynomials:

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

Septics

Consider the polynomials over $\mathbb{F}_q[x]$ of degree 7, with the (non-zero) coefficient of x^5 arbitrarily prescribed.

Lemma 5.6.6. *Suppose that $n = 7$ and q even. 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. Like for sextics, we can here inherit the relevant result from the Section 5.3.3 (in this case Lemma 5.3.6) and consequently suppose $\omega(E_7) \leq 5$. Then the sufficient condition (5.31) is satisfied for all q in only a few steps, as tabulated below. In steps 2 and 3, $E_7 = 21 \cdot 43$ and $E_7 = 127$ respectively; also, the choice of k_0 in both cases yields $s = 1$ whence the sufficient condition 5.31 takes the form $q^2 > 2\sqrt(2)\left(1 - \frac{1}{q}\right) W(E_7)$.

#	q	$\omega(E_7)$	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		≤ 5	1	0	≤ 5	0.911	6.40	5
2	4	2	43	1	1	–	–	3
3	2	1	7	1	3	–	–	2

This completes the proof. □

Octics

Consider the polynomials of degree 8. As before, 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 $q^4 + 1$. Recall that any prime divisor l of K_2 is $\equiv 1 \pmod 8$, i.e., $l \in L_8$. Define $\omega_1 := \omega(K_1)$ and $\omega_2 := \omega(K_2)$.

Lemma 5.6.7. *Suppose $n = 8$, and q is even, $a\ (\neq 0) \in \mathbb{F}_q$ and c is 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.*

Proof. Reasoning as above (in cases $n = 6$ and 7), we can bring in an already established result, given by Lemma 5.3.7. Hence we proceed assuming $\omega_1 \leq 7$ and $\omega_2 \leq 5$ and begin the sieve using the sufficient condition (5.32). The outcome is summarized in the following table.

#	q	ω_1	ω_2	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
1		≤ 7	≤ 5	15	2	≤ 10	0.474	20.99	9
2	≤ 8	≤ 3	≤ 2	3	1	4	0.573	7.24	4

In $\mathbb{F}_2[x]$, $f(x) = x^8 + x^6 + x^3 + x^2 + 1$ is primitive. This completes the proof. □

With this we conclude the work with primitive polynomials over fields of even characteristic and prescribed non-zero second coefficient. Next, we deal with prescribing a zero second coefficient, in particular when the degree of the polynomial is 4 or 5.

5.7 The even zero problem

Recall that, by Lemma 3.3.1, it suffices to show that $\pi_0(Q_n)$ is positive when the prescribed coefficient $a = 0$. We then have the following condition for $\pi_0(Q_n) > 0$.

Proposition 5.7.1. *Assume that q is even. Let (k_0, s) be a decomposition of Q_n. Suppose that*

$$q^{\frac{n}{2}-1} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{5.33}$$

Then $\pi_0(Q_n)$ is positive.

Proof. This follows from Lemma 5.5.4 as in the proof of Lemma 5.6.1. 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.

5.7.1 Quartics

Suppose $n = 4$. Then, for a decomposition (k_0, s) of Q_4, (5.33) the sufficient condition is

$$q > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{5.34}$$

In particular, when $s = 1$, the condition is

$$q > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(Q_4). \tag{5.35}$$

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 $\omega_1 = \omega(K_1)$ and $\omega_2 = \omega(K_2)$.

Lemma 5.7.2. *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 the bounds $(A.8)$ and $(A.19)$ yield

$$W(Q_4) < (q+1-1)^{\frac{2}{5}}(q^2+1-1)^{\frac{1}{4}} = q^{\frac{9}{10}}.$$

Consequently, the condition (5.35) is satisfied for $q > 2^{15} = 32768$. 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, the condition (5.34) is satisfied whenever $q \geq 1785$. 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 the condition (5.19) is satisfied whenever $q \geq 21$, 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 (5.19) is satisfied when $q \geq 84$. The work with smaller values of q is tabulated below; in each line, q_{min} is, in given circumstances, the smallest integer value satisfying the right-hand side of the condition (5.34) which suffices when $q > q_{min}$.

q	Q_4	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} \leq$	q_{min}
64	$5 \cdot 13 \cdot 17 \cdot 241$	1	3	0.860	4.33	25
32	$3 \cdot 5 \cdot 11 \cdot 41$	1	3	0.684	4.93	28
16	$17 \cdot 257$	0	2	0.937	3.07	9

Examples of primitive polynomials of desired form in $\mathbb{F}_8[x]$ and $\mathbb{F}_4[x]$, (both defined as in the subsection 5.6.1) and in $\mathbb{F}_2[x]$, are as follows:

q	$f(x)$
8	$x^4 + x + \alpha^2$
4	$x^4 + x^3 + x + (\alpha + 1)$
2	$x^4 + x + 1$

5.7.2 Quintics

Take $n = 5$. For a decomposition (k_0, s) of $k|Q_5$ the sufficient condition (5.33) now takes the form

$$q^{\frac{3}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(k_0)\Delta_{s,\delta}. \tag{5.36}$$

Lemma 5.7.3. *Suppose $n = 5$ and q is even Then there exists a primitive polynomial of degree n over $\mathbb{F}_q$ with the coefficient of x^3 prescribed as 0.*

Proof. Suppose $\omega(Q_5) \geq 4$. Then, provided the bound $(A.30)$,

$$W(Q_5) \ < \ \left(\sqrt{Q_5} - 1\right)^{\frac{1}{2}} \ < \ \left(q^{\frac{5}{2}} - 1\right)^{\frac{1}{2}} \ < \ q^{\frac{5}{4}}.$$

To satisfy the condition (5.36) with $s = 1$ we require

$$q^{\frac{3}{2}} > 2\sqrt{2}\left(1 - \frac{1}{q}\right) W(Q_5),$$

i.e. $q^{\frac{1}{4}} > 2\sqrt{2} > 64$. This certainly holds if $\omega(Q_5) \geq 6$ (so that $Q_5 \geq 5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 71$).

Accordingly, assume $\omega(Q_5) \leq 5$. 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 the condition (5.36) is satisfied for $q \geq 9$.

For $q \leq 8$, necessarily $5 \nmid Q_5$ and $\omega(Q_5) \leq 2$. We repeat the last process, taking $k_0 = 1$ so that $s \leq 2$, $\delta \geq 1 - \frac{1}{11} - \frac{1}{31} \geq 0.876$ and $2\sqrt{2}\Delta_{s,\delta} < 8.89$. Thus the condition (5.36) is satisfied when $q > \left(\left(1 - \frac{1}{q}\right) 8.9\right)^{\frac{2}{3}}$, hence the result holds for $q = 8, 4$. When $q = 2$, then $\omega(Q_5) = 1$ and the condition (5.36) with $s = 1$ holds since $2\sqrt{2} > \sqrt{2}$. This completes the proof. □

This concludes our work on second coefficient. The results in this chapter complete the proof of the HMPC for $m = 2$ as well as provide a less computational proof of the previously established results if q is odd and the degree of the polynomial $n \geq 5$. They can be easily extended for higher degrees, where the proof is merely a routine check.

In the following chapter we will complete the proof of the HMPC for $m = 3$.

Chapter 6

The third coefficient

In this chapter, we will prove the HMPC when $m = 3$, that is, when the coefficient of x^{n-3} of a primitive polynomial over any finite field is arbitrarily prescribed and the degree of a polynomial is $n \geq 5$. This will complete the HMPC for $n = 5$ and 6. For $n \geq 7$ we will prove a stronger result, namely that the primitive polynomial may also have its constant term prescribed. This implies further cases of the HMPC and completes the HMPC when $n = 7$.

Dealing with one value of m at the time, we can provide very efficient results. The fields $\mathbb{F}_q$ where $q \not\equiv 0 \pmod 3$ will be considered separately from those with $q \equiv 0 \pmod 3$; when the characteristic of the field is 3, we will require 3-adic analysis for the proofs. The methods used and the fact that we will only focus on certain degrees in particular, enable us to give a compact proof and almost no computation is required.

6.1 Main results

The following theorem asserts the existence of a primitive polynomial of degree $n = 5$ or higher, with arbitrarily prescribed third coefficient.

Theorem 6.1.1. *Suppose $n \geq 5$. Let a be an arbitrary member of the finite field $\mathbb{F}_q$. Then there exists a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n with third coefficient prescribed as a.*

Note that when $n = 5$ and $a = 0$ the conclusion of Theorem 6.1.1 is a consequence of Theorem 1.2 in [13]. A (difficult) case of the HMPC is an immediate consequence of Theorem 6.1.1.

Corollary 6.1.2. *Suppose* $5 \leq n \leq 6$. *Then the HMPC holds.*

Moreover, when the degree $n \geq 7$, we prove a stronger version of Theorem 5.1.1 wherein additionally the constant term of the primitive polynomial is appropriately prescribed as $(-1)^n c \in \mathbb{F}_q$. Recall, from the previous chapter, that c must necessarily be a primitive element of $\mathbb{F}_q$, since this is the norm of a root of the polynomial.

Theorem 6.1.3. *Suppose* $n \geq 7$. *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 third 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 6.1.1 (for $a = 0$) and Theorem 6.1.3 (for $a \neq 0$) imply further cases of the HMPC.

Corollary 6.1.4. *Suppose* $n \geq 7$ *and* $a \in \mathbb{F}_q$. *Then there exists a primitive polynomial of degree* n *over* $\mathbb{F}_q$ *with its coefficient of* x^3 *equal to* a. *In particular, the HMPC is established for* $(n, m) = (7, 4)$ *and* $(8, 5)$.

Granted Theorem 6.1.3, for $a \neq 0$ we need only consider $n = 5$ or 6 in Theorem 6.1.1. Generally, for the numerical aspects we can suppose $5 \leq n \leq 8$, though the calculations could easily be extended to larger values of the degree. Of course, the working becomes easier as n increases.

6.2 The non-ternary problem

Throughout this section we will only consider fields with characteristic *not* 3.

As it stands when $m = 3$, Lemma 3.2.1 is useful only when the characteristic of the field is not 3. Suppose now that $q \not\equiv 0 \pmod 3$ and that $a \in \mathbb{F}_q$ is given.

From (3.4), considering that $2\sigma_2 = s_1^2 - s_2$ and $\sigma_1 = s_1$, we have

$$6\sigma_3 = s_1^3 - 3s_1 s_2 + 2s_3.$$

As we want to assign the value a to the third coefficient, we put $\sigma_3 = -a$. Set $s_1 = 0$. Then we have to put $s_3 = -3a$. The characteristic function for the set of elements $\gamma \in \mathbb{F}_{q^n}$

for which $s_1 = 0$ and $s_3 = -3a$ is

$$\frac{1}{q^2} \sum_{\alpha,\beta \in \mathbb{F}_q} \chi_n(\alpha\gamma^3 + \beta\gamma)\chi(-3\alpha a).$$

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.

Therefore, for $k|q^n - 1$, redefining $\pi_a(k)$ to refer specifically to the number of primitive polynomials with $s_1 = 0$, $s_3 = -a$, we obtain

$$\frac{q^2\pi_a(k)}{\theta(k)} = \int_{d|k} \sum_{\alpha,\beta \in \mathbb{F}_q} \bar{\chi}(\alpha a) S_n(\alpha, \beta; \eta_d), \tag{6.1}$$

where $S_n(\alpha, \beta; \eta) = \sum_{\gamma \in \mathbb{F}_{q^n}} \chi_n(\alpha\gamma^3 + \beta\gamma)\eta(\gamma)$ and, for simplicity, $3a$ has been replaced by a.

More generally, suppose that (k_0, s) is a decomposition of k. Then, by the equivalence of (3.6) and (3.7),

$$\begin{aligned} \frac{q^2\pi_a(k)}{\theta(k)} \;&=\; \delta \int_{d|k_0} \sum_{\alpha,\beta \in \mathbb{F}_q} \bar{\chi}(\alpha a) S_n(\alpha, \beta; \eta_d) \\ &+\; \sum_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \int_{d|k_0} \sum_{\alpha,\beta \in \mathbb{F}_q} \bar{\chi}(\alpha a) S_n(\alpha, \beta; \eta_{dp_i}). \end{aligned} \tag{6.2}$$

Of course, (6.1) is recovered from (6.2) by setting $s = 1$.

Estimates for $S_n(\alpha, \beta; \eta_d)$ are standard as now described (see [2], (1.3)).

Lemma 6.2.1. *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

$$|S_n(\alpha, \beta; \eta_d)| \;\le\; \begin{cases} 3q^{\frac{n}{2}}, & \text{if } \alpha \neq 0, \\ q^{\frac{n}{2}}, & \text{if } \alpha = 0. \end{cases}$$

Define $S_1(\kappa\rho^T, \eta) := \sum_{\rho\in\mathbb{F}_q} \chi(\kappa\rho^T)\eta(\rho)$. The following lemma gives the bounds for $S_1(\kappa\rho^T, \eta)$. It is a version of Lemma 9.5 in [8].

Lemma 6.2.2. *Suppose $p \not| T$ and $T' := \gcd(m, q-1)$. Assume that $\kappa \in \mathbb{F}_q^*$ and $\eta \in \widehat{\mathbb{F}}_q^*$. Then*

$$\begin{aligned} |S_1(\kappa\rho^T, \eta) + 1| &\leq (T'-1)q^{\frac{1}{2}} \quad \textit{if } \eta \textit{ is trivial,} \\ |S_1(\kappa\rho^T, \eta)| &\leq T'q^{\frac{1}{2}} \quad \textit{otherwise.} \end{aligned}$$

Proof. For any $\nu \in \widehat{\mathbb{F}}_q^*$, define the Gaussian sum $G(\nu) := \sum_{z\in\mathbb{F}_q} \psi(z)\nu(z)$. As usual, $G(\nu) = -1$ if ν is trivial and, otherwise, $|G(\nu)| = \sqrt{q}$. Now let ν be a *generator* of $\widehat{\mathbb{F}}_q^*$ and so has order $q-1$. Then $\hat{\chi} = \nu^i$ for some $i \leq q-2$: $i = 0$ if $\hat{\chi}$ is trivial.

Moreover, for $y \in \mathbb{F}_q$,

$$\psi(\kappa y) = \frac{1}{q-1} \sum_{j=0}^{q-2} G(\bar{\nu}^j)\ \nu^j(\kappa y).$$

Hence,

$$\begin{aligned} S_1(\kappa x^T, \hat{\chi}) &= \frac{1}{q-1} \sum_{j=0}^{q-2} G(\bar{\nu}^j) \sum_{c\in\mathbb{F}_q} \nu^j(\kappa c^T)\nu^i(c) \\ &= \frac{1}{q-1} \left(\sum_{j=1}^{q-2} G(\bar{\nu}^j)\nu^j(\kappa) \sum_{c\in\mathbb{F}_q} \nu^{jT+i}(c) \ - \sum_{c\in\mathbb{F}_q} \nu^i(c) \right). \end{aligned}$$

Now, $\sum_{c\in\mathbb{F}_q} \nu^{jT+i}(c) = 0$ unless ν^{jT+i} is trivial (in which case the sum is $q-1$). The latter occurs precisely when $jT + i \equiv 0 \pmod{q-1}$. For this, necessarily $T'|i$, in which case there are T' solutions $j \pmod{q-1}$.

When $i = 0$, there are $T'-1$ such solutions j with $1 \leq j \leq q-2$; otherwise there are T' solutions. □

Lemma 6.2.3. *Suppose that $p \neq 3$ and that $a \in \mathbb{F}_q$ is non-zero and $k|P_{n,3} := \frac{q^n-1}{\gcd(3,q-1)}$. Suppose also that $k = k_0 p_1 \cdots p_s$, $s \geq 1$, $p_1, \ldots, p_s$ prime, with δ positive. Then $\pi_a(k)$ is positive whenever*

$$q^{\frac{n-3}{2}} > \begin{cases} 9W(k_0)\Delta_{s,\delta}, & \textit{when } q \equiv 1 \pmod 3; \\ 3W(k_0)\Delta_{s,\delta}, & \textit{when } q \equiv 2 \pmod 3. \end{cases} \tag{6.3}$$

Specifically, when $s = 1$ and $k = P_{n,3}$, the sufficient condition is

$$q^{\frac{n-3}{2}} > \begin{cases} 9W(q^n-1), & \textit{when } q \equiv 1 \pmod 3; \\ 3W(q^n-1), & \textit{when } q \equiv 2 \pmod 3. \end{cases} \tag{6.4}$$

Proof. In (6.2), 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). Suppose $d|k_0$ and take η_d: similar reasoning applies to each η_{dp_i}. The contribution to the right-hand side of (6.2) attributable to values of $\alpha = \beta = 0$ is $\delta(q^n - 1)$, as $S_n(0,0;\eta_d) = 0$ unless $d = 1$. This yields the main term. It remains to show that for each character η_d for any $d|k$ (with $d > 1$) the sum of terms with α, β not both zero is bounded absolutely by $9\delta q^{\frac{n+3}{2}}$ when $q \equiv 1 \pmod 3$ and by $3\delta q^{\frac{n+3}{2}}$ when $q \equiv 2 \pmod 3$.

Suppose $d \nmid Q_n$. Then the restriction $\tilde{\eta_d}$ (of $\eta_d \in \widehat{\mathbb{F}}_{q^n}$ to $\widehat{\mathbb{F}}_q$) is nontrivial. For the terms with $\beta \neq 0$, we can replace α by $\alpha\beta^3$ and γ by $\frac{\gamma}{\beta}$ to yield $\sum_{\alpha\in\mathbb{F}_q} \bar{S_1}(\alpha a;\tilde{\eta_d}) S_n(\alpha, 1, \eta_d)$, where $S_1(x,\tilde{\eta}) = \sum_{\beta\in\mathbb{F}_q} \chi(x\beta)\tilde{\eta}(\beta)$. Because $q \nmid Q_n$, when $\alpha = 0$, then $S_1(\alpha a;\tilde{\eta_d}) = 0$. On the other hand, when $\alpha \neq 0$, then, as usual, $|S_n(\alpha, 1, \eta_d)| \leq 3q^{\frac{n}{2}}$, whereas $|S_1(\alpha a;\tilde{\eta_d})| \leq m'q^{\frac{1}{2}}$ by Lemma 6.2.2. So the total contribution from terms with $\beta \neq 0$ is bounded absolutely by $9\delta(q-1)q^{\frac{n+1}{2}}$ when $q \equiv 1 \pmod 3$ and by $3\delta(q-1)q^{\frac{n+1}{2}}$ when $q \equiv 2 \pmod 3$.

For the remaining contribution in this case, consider terms with $\beta = 0$ (and hence $\alpha \neq 0$): $\sum_{\alpha\in\mathbb{F}_q} \chi(-\alpha a) S_n(\alpha, 0; \eta_d)$. Here, if $3 \nmid (q-1)$, replace α by α^3 and γ by $\frac{\gamma}{\alpha}$ to obtain $\bar{S_1}(a,\tilde{\eta_d}) S_n(1, 0; \eta_d)$. Again $|S_n| \leq 3q^{\frac{n}{2}}$ and $|S_1| \leq q^{\frac{1}{2}}$ so that the total contribution is $3\delta q^{\frac{n+1}{2}}$. On the other hand, if $3|q-1$, one has to split S_n into three sums (each with weight $\frac{1}{3}$) by replacing α by $g^i\alpha^3$ $(i = 0, 1, 2)$ and γ by $\frac{\gamma}{\alpha}$ for a fixed non-cube in $\mathbb{F}_q$. Each S_3 is bounded as before whereas, now $|S_1| \leq 3q^{\frac{1}{2}}$. Now the total contribution is bounded by $9\delta q^{\frac{n+1}{2}}$.

Thus, adding the contributions we obtain the required absolute bound $3\delta \gcd(3, q-1)q^{\frac{n+3}{2}}$.

Now suppose $d|Q_n$. Then $\tilde{\eta_d}$ is trivial. For the terms with $\beta \neq 0$ proceed as before. This time, provided $\alpha \neq 0$, we can conclude that $|S_1(\alpha a;\tilde{\eta_d})| \leq (\gcd(3, q-1) - 1)q^{\frac{1}{2}} + 1$. On the other hand, when $\alpha = 0$, we can only use the trivial bound $|S_1| \leq (q-1)$, though $|S_n(0, 1; \eta_d)| \leq q^{\frac{n}{2}}$ in this case. Hence for these terms (with $\beta \neq 0$) we have a total absolute bound of

$$\begin{aligned} & 3\delta(q-1)((\gcd(3,q-1)-1)q^{\frac{1}{2}}+1)q^{\frac{n}{2}} + \delta(q-1)q^{\frac{n}{2}} \\ = \;& 3\delta(q-1)q^{\frac{n}{2}}((\gcd(3,q-1)-1)q^{\frac{1}{2}} + \frac{4}{3}) \\ \leq \;& 3\delta \gcd(3,q-1)(q-1)q^{\frac{n+1}{2}}. \end{aligned}$$

The contribution from terms with $\beta = 0$ (and so $\alpha \neq 0$) is certainly bounded by

$3\delta \gcd(3, q-1) q^{\frac{n+1}{2}}$ as before. Indeed, the factor $\gcd(3, q-1) q^{\frac{1}{2}}$ could be reduced to $(\gcd(3, q-1) - 1) q^{\frac{1}{2}} + 1$.

The remaining terms on the right side of (6.2) (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 (6.2) exceeds

$$\delta \left(q^n \ - \ 3 \gcd(3, q-1) q^{\frac{n+3}{2}} \Delta_{s,\delta} \right),$$

with $\Delta_{s,\delta}$ as in Section 3.3, since $\sum_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) = s - 1 \ + \delta$. The result follows. □

To prescribe additionally the constant term of the polynomial, use the condition of the following lemma.

Lemma 6.2.4. *Suppose that $a \in \mathbb{F}_q$ is non-zero, c is a primitive element of $\mathbb{F}_q$ and $k|E_n$. Suppose also $k = k_0 p_1 \cdots p_s$,*
$s \geq 1$, $p_1, \ldots, p_s$ prime, with δ positive. Then $\pi_{a,c}(k)$ is positive whenever

$$q^{\frac{n-5}{2}} > \begin{cases} 9W(k_0)\Delta_{s,\delta}, & \text{when } q \equiv 1 \pmod 3; \\ 3W(k_0)\Delta_{s,\delta}, & \text{when } q \equiv 2 \pmod 3. \end{cases} \tag{6.5}$$

Specifically, when $s = 1$, $W(k_0)\Delta_{s,\delta}$ is replaced by $W(E_n)$ in (6.5).

In particular, the norm case of the HM-problem is solved whenever (6.5) *holds with $k = E_n$.*

Proof. The characteristic function for the subset of $\mathbb{F}_{q^n}^*$ comprising elements with $\mathbb{F}_q$-norm c (i.e. $N_n(\gamma) = c$) is $\dfrac{1}{q-1} \displaystyle\sum_{\nu \in \widehat{\mathbb{F}_{q^n}^*}} \nu(N_n(\gamma) c^{-1})$ ($\widehat{\mathbb{F}_{q^n}^*}$ being the group of multiplicative characters of $\mathbb{F}_{q^n}^*$). Redefining $\pi_{a,c}$ to refer to the number of primitive polynomials with $s_1 = 0$, $s_3 = -3a$, we obtain the following modification of the condition (6.2), where $\hat{\nu}$ denotes the lift of ν to $\widehat{\mathbb{F}_{q^n}^*}$ (so that $\hat{\nu}(\gamma) = \nu(N_n(\gamma))$:

$$\begin{aligned} \frac{(q-1)q^2 \pi_{a,c}(k)}{\theta(k)} \ &= \ \delta \int_{d|k_0} \sum_{\alpha,\beta \in \mathbb{F}_q} \sum_{\nu \in \widehat{\mathbb{F}_{q^n}^*}} \bar{\nu}(c) \bar{\chi}(3\alpha a) S_n(\alpha, \beta; \eta_d \hat{\nu}) \\ &+ \ \sum_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \int_{d|k_0} \sum_{\alpha,\beta \in \mathbb{F}_q} \sum_{\nu \in \widehat{\mathbb{F}_{q^n}^*}} \bar{\nu}(c) \bar{\chi}(3\alpha a) S_n(\alpha, \beta; \eta_{dp_i} \hat{\nu}). \end{aligned} \tag{6.6}$$

The result is then obtained by the same methods as (6.3). □

We will distinguish between the cases of $q \equiv 1$ or $2 \pmod 3$ for smaller values of q, when this gives us a useful saving. In general, however, we will use only the condition for $q \equiv 1 \pmod 3$, which applies to all cases.

6.2.1 Quintics

Suppose $n = 5$. 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 6.2.5. *Suppose that $n = 5$, $\omega_1 \geq 13$ or $\omega_2 \geq 26$. Let a $(\neq 0) \in \mathbb{F}_q$. Then there exists a primitive polynomial of degree 5 over $\mathbb{F}_q$ with the coefficient of x^2 prescribed as a.*

Proof. First suppose $\omega_1 \geq 13$ and $\omega_2 \geq 26$. The number of square-free divisors of h, an integer with $\omega(h) \geq 13$, is bounded by $W(h) < h^{\frac{3}{11}}$ (by $(A.4)$). Therefore $W(K_1) < (q-1)^{\frac{3}{11}} < q^{\frac{3}{11}}$. Also, by $(A.29)$, when integer h is a product of primes $l \equiv 1 \pmod{10}$ and $\omega(h) \geq 26$, then $W(h) < h^{\frac{13}{99}}$. That yields $W(K_2) < (Q_5)^{\frac{13}{99}} < (q^5)^{\frac{13}{99}} = q^{\frac{65}{99}}$. It follows that $W(q^5-1) < q^{\frac{92}{99}}$. Consequently, by (6.4), to show existence it suffices that $q > 9q^{\frac{92}{99}}$, i.e. $q \geq 9^{\frac{99}{7}} \approx 3.131 \cdot 10^{13}$, which holds as $\omega_1 \geq 13$ and $\omega_2 \geq 26$ both yield $q > 10^{14}$.

Next, suppose $\omega_1 \leq 12$ and $\omega_2 \geq 26$. Set k_0 to be the product of K_2 and the least three primes in K_1. Thus $s \leq 9$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{37} > 0.440$ and $\Delta_{s,\delta} < 20.19$. By the above, $W(k_0) < 8q^{\frac{65}{99}}$ and (6.3) is satisfied whenever $q \geq 1615716202$. This is the case since $\omega_2 \geq 26$, whence $q > 10^{14}$.

Finally, suppose $\omega_1 \geq 13$ and $\omega_2 \leq 25$. Put $k_0 = K_1$. Then $s \leq 25$,

$$\delta \;\geq\; 1 - \sum_{\substack{l \leq 571 \\ l \equiv 1 (\mathrm{mod}\, 10)}} \frac{1}{l} \;>\; 0.743$$

and $\Delta_{s,\delta} < 34.31$. Now (6.3) is satisfied whenever $q \geq 2651$. This completes the proof since $\omega_1 \geq 13$ implies $q > 10^{14}$. □

Following Lemma 6.2.5, we assume $\omega_1 \leq 12$, $\omega_2 \leq 25$ and run the sieve. The steps are shown in the table below, where q_{min} denotes the minimum integer q satisfying (6.3) numerically.

#	q	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		12	25	30	3	34	0.263	127.48	9179
2	≤ 9178	5	8	6	2	11	0.378	28.46	1025
3	≤ 1024	4	7	6	2	9	0.461	19.36	697
4	≤ 696	4	6	6	2	8	0.469	16.93	610
5	≤ 609	4	5	6	2	7	0.479	14.53	524

In line 5, $q \leq 609$ yields $\omega_2 \leq 6$, but as there are no values of q in this range with $\omega_2 = 6$, we can suppose $\omega_2 \leq 5$. (Similar reductions apply to subsequent tables.)

At this point, it is appropriate to separate the calculations regarding mod 3. Firstly, criterion (6.3) takes a milder form for values of $q \equiv 2 \pmod 3$ and line 5 of the table above gives $q_{min} = 175$. We may then suppose $q \leq 174$, $\omega_1 \leq 3$ and $\omega_2 \leq 5$. Putting $k_0 = 6$ gives $s \leq 6$, $\delta \geq 0.621$, $\Delta_{s,\delta} \leq 10.06$ and $q_{min} = 121$.

Secondly, when $q \equiv 1 \pmod 3$ but $q \not\equiv 1 \pmod 9$, then 3 is not a factor of $P_{n,m}$. In line 5 we obtain $\omega_1 \leq 3$ and $\omega_2 \leq 5$. Putting $k_0 = 2$ yields $s \leq 7$, $\delta \geq 0.479$, $\Delta_{s,\delta} \leq 14.53$ and $q_{min} = 262$. We may then suppose $q \leq 261$, $\omega_1 \leq 3$ and, as there are no values of q in this range with $\omega_2 = 5$, we proceed assuming $\omega_2 \leq 4$. Again we set $k_0 = 2$. Now $\delta \geq 0.493$, $\Delta_{s,\delta} \leq 12.15$ and $q_{min} = 219$.

The remaining prime powers are checked separately. In fact, by individual consideration, all remaining prime powers ≥ 121, other than $q = 163$, satisfy (6.3) with k_0 the least prime factor of $P_{n,m}$. These comprise 361, 343 and 289 ($\equiv 1 \pmod 9$) together with 211, 199, 196, 193, 181, 169, 157, 151, 139 and 127 ($\equiv 1 \pmod 3$). Indeed, lower values of q similarly satisfy (6.3) except for $q = 109, 67, 64, 61, 49, 43, 37, 31, 25, 19, 16, 13, 11, 8, 7, 5, 4$ and 2. For the largest two composite values in this set, $q = 64, 49$ and 25, we can refine the sufficient condition for existence in the same fashion as for $q = 49$ in the Section 5.3.1. For the rest of the values in the above set and for $q = 163$ a primitive polynomial are found explicitly, using Maple (see Appendix B for details).

6.2.2 Sextics: the non-zero problem

Suppose $n = 6$ and $a \neq 0$. Let K_1 be the product of all distinct prime divisors of $q^2 - 1$ and K_2 the product of distinct prime divisors of $\frac{q^6-1}{q^2-1}$ that do not divide $q^2 - 1$. Then product

of distinct primes in q^6-1 can be written as $K_1 \cdot K_2$. Notice that 3 cannot be a factor of K_2 and so (by an analogue of Lemma 4.4.1) any prime divisor l of K_2 is $\equiv 1 \pmod 6$, i.e., $l \in L_6$. Define $\omega_1 := \omega(K_1)$ and $\omega_2 := \omega(K_2)$.

Lemma 6.2.6. *Suppose that $n = 6$, $\omega_1 \geq 13$ or $\omega_2 \geq 15$. Let a $(\neq 0) \in \mathbb{F}_q$. Then there exists a primitive polynomial of degree 6 over $\mathbb{F}_q$ with the coefficient of x^3 prescribed as a.*

Proof. First suppose $\omega_1 \geq 13$ and $\omega_2 \geq 15$. By $(A.4)$, $W(K_1) < (q^2-1)^{\frac{3}{11}} < (q^2-1)^{\frac{2}{7}} < q^{\frac{4}{7}}$. Also, by Lemma $(A.21)$, when integer h is a product of primes $l \equiv 1 \pmod 6$ and $\omega(h) \geq 15$, $W(h) < h^{\frac{5}{28}}$. This yields $W(K_2) < (q^4+q^2+1)^{\frac{5}{28}} < (2q^4)^{\frac{5}{28}} = 2^{\frac{5}{28}} q^{\frac{5}{7}}$. It follows that $W(q^6-1) < 2^{\frac{5}{28}} q^{\frac{9}{7}}$. Consequently, by (5.7), to show existence it suffices that $q^{\frac{3}{2}} > 9 \cdot 2^{\frac{5}{28}} q^{\frac{9}{7}}$, i.e. $q \geq 50582$, which obviously holds as $\omega_1 \geq 13$ and $\omega_2 \geq 15$ both yield $q > 10^6$.

Next, suppose $\omega_1 \leq 12$ and $\omega_2 \geq 15$. Take k_0 to be the product of K_2 and three smallest primes in K_1. Thus $s \leq 9$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{37} > 0.440$ and $\Delta_{s,\delta} < 20.19$. By the above, $W(k_0) < 8 \cdot 2^{\frac{5}{28}} q^{\frac{5}{7}}$ and (5.6) is satisfied whenever $q \geq 12399$. This is the case since $\omega_2 \geq 15$, whence $q > 10^6$.

Finally, we suppose $\omega_1 \geq 13$ and $\omega_2 \leq 14$. Putting $k_0 = K_1$ gives $s \leq 14$,

$$\delta \;\geq\; 1 - \sum_{\substack{l \leq 127 \\ l \equiv 1 (\mathrm{mod}\, 6)}} \frac{1}{l} \;>\; 0.550$$

and $\Delta_{s,\delta} < 25.64$. Now (5.6) is satisfied whenever $q \geq 351$, which completes the proof as $\omega_1 \geq 13$ yields $q > 10^6$. □

Consequently to Lemma 6.2.6, we now assume $\omega_1 \leq 12$ and $\omega_2 \leq 14$. The sieving steps are shown in the following table. As usual, q_{min} denotes the minimal integral value of q for which (6.3) holds with the displayed value of δ.

#	$q \leq$	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		12	14	30	3	24	0.241	93.29	356
2	355	5	7	6	2	11	0.235	44.56	138
3	137	5	6	6	2	9	0.295	29.12	104
4	103	5	5	6	2	8	0.318	24.02	91

Here, in the last line, $\omega_2 \leq 6$ has been reduced to $\omega_2 \leq 5$ for there are no values of q in this range with $\omega_2 = 6$.

We now assume $q \leq 89$ separately treat $q \equiv 1$ and $q \equiv 2 \pmod 3$. When $q \equiv 2 \pmod 3$, $\omega_1, \omega_2 \leq 5$ and setting $k_0 = 6$ results in s, δ and $\Delta_{s,\delta}$ as in row 4 of the table above, and $q_{min} = 44$. Assuming $q \leq 41$ and putting $k_0 = 6$, gives $s \leq 7$, $\delta \geq 0.377$, $\Delta_{s,\delta} \leq 17.92$ and $q_{min} = 36$.

When $q \equiv 1 \pmod 3$ but $q \not\equiv 1 \pmod 9$, then $\omega_1 \leq 4$ and $\omega_2 \leq 5$. We put $k_0 = 2$ and obtain $s \leq 8$, $\delta \geq 0.318$, $\Delta_{s,\delta} \leq 24.04$ and $q_{min} = 58$.

There are two values of $q \equiv 1 \pmod 9$ in between 89 and 36, namely $q = 73$ and $q = 64$, and both satisfy condition (6.3) when we set k_0 to be the smallest divisor of $P_{n,m}$.

Of all the other values of q left out by the sieve procedure, $q = 49$, 43, 32, 31, 29, 25, 23 and 17, satisfy condition (6.3) with $\omega(k_0) = 1$. For $q = 16$, we can refine the sufficient condition for existence in the same fashion as for $q = 49$ in the Section 5.3.1. Primitive polynomials for $q = 37$, 19, 13, 11, 8, 7, 5, 4 and 2 had to be found explicitly, using Maple - see Appendix B.

6.2.3 Sextics: the zero problem

Suppose thet the prescribed coefficient a is zero. By Lemma 3.3.1, it suffices to prove that $\pi_0(Q_n)$ is positive. Now, putting $a = 0$ in (6.2) yields the following proposition. Note that, by comparison with the proof of Lemma 6.2.3 we always have to use the trivial bound $|S_1(0, \bar{\tilde{\eta}}_d)| \leq q - 1$ since $d|Q_n$.

Proposition 6.2.7. *Let $k|Q_n$ and let (k_0, s) be a decomposition of k. Suppose $q \not\equiv 0 \pmod 3$ and*

$$q^{\frac{n-4}{2}} > 9W(k_0)\Delta_{s,\delta}. \tag{6.7}$$

Then $\pi_0(k)$ is positive.

Specifically, when $s = 1$ and $k_0 = Q_n$, the sufficient condition is

$$q^{\frac{n-4}{2}} > 9W(Q_n). \tag{6.8}$$

Now take $n = 6$. Write the product of distinct primes in Q_6 as $K_1 \cdot K_2$, where K_1 is the product of all distinct prime divisors of $q + 1$ and K_2 is the product of distinct prime divisors of $\frac{q^6-1}{q^2-1}$ that do not divide $q^2 - 1$. As in the previous section, any prime divisor l of K_2 is $\equiv 1 \pmod 6$. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2.

Lemma 6.2.8. *Suppose that $n = 6$, $\omega_1 \geq 12$ or $\omega_2 \geq 25$. Then there exists a primitive polynomial of degree 6 over $\mathbb{F}_q$ with the coefficient of x^3 equal to zero.*

Proof. We begin by supposing $\omega_1 \geq 12$ and $\omega_2 \geq 25$. By $(A.3)$, $W(K_1) < (q+1-1)^{\frac{2}{7}} < q^{\frac{2}{7}}$ and by $(A.24)$, $W(K_2) < (q^4+q^2+1)^{\frac{5}{32}} < (2q^4)^{\frac{5}{32}} = 2^{\frac{5}{32}} q^{\frac{5}{8}}$. Hence $W(Q_6) < 2^{\frac{5}{32}} q^{\frac{51}{56}}$. Consequently, by (6.8), to show existence it suffices that $q > 9 \cdot 2^{\frac{5}{32}} q^{\frac{51}{56}}$, i.e. $q \geq 1.6... \cdot 10^{11}$, which holds as the size of ω_1 and ω_2 yields $q > 10^{12}$.

Next, suppose $\omega_1 \leq 11$ and $\omega_2 \geq 25$. Take k_0 to be the product of K_2 and three least primes in K_1. Thus $s \leq 8$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{31} > 0.466$ and $\Delta_{s,\delta} < 17.03$. Now (6.7) is satisfied whenever $q \geq 2.2... \cdot 10^8$. This holds since $\omega_2 \geq 25$, whence $q > 10^{12}$.

At last, we suppose $\omega_1 \geq 12$ and $\omega_2 \leq 24$. Putting $k_0 = K_1$ gives $s \leq 24$,

$$\delta \;\geq\; 1 - \sum_{\substack{l \leq 229 \\ l \equiv 1 (\mathrm{mod}\, 6)}} \frac{1}{l} \;>\; 0.494$$

and $\Delta_{s,\delta} < 48.56$. Now (6.7) is satisfied whenever $q \geq 4975$, which completes the proof as $\omega_1 \geq 12$ yields $q > 10^{12}$. □

Following Lemma 6.2.8, we assume $\omega_1 \leq 11$ and $\omega_2 \leq 24$. The sieving steps are shown in the table below.

#	$q \leq$	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		11	24	30	3	32	0.174	180.17	12973
2	12972	5	10	30	3	12	0.437	27.18	1957
3	1956	4	8	6	2	10	0.322	29.96	1079
4	1078	4	7	6	2	9	0.337	25.74	927
5	926	4	6	6	2	8	0.354	21.78	785
6	784	3	6	6	2	7	0.445	15.49	558
7	557	3	5	6	2	6	0.468	12.69	468

Here there have been reductions to ω_1 and ω_2 in lines $5-7$. When $q \leq 167$, polynomials were found explicitly, using Maple.

6.2.4 Septics

For degrees $n = 7$ and $n = 8$ we prove a stronger result and prove the existence of primitive polynomials over $\mathbb{F}_q$ with prescribed third coefficient *and* constant term (necessarily a

primitive element of $\mathbb{F}_q$). The main tool here is Lemma 6.2.4.

Lemma 6.2.9. *Suppose that $n = 7$ and $\omega(E_7) \geq 20$. Let $a\ (\neq 0) \in \mathbb{F}_q$ and c be a primitive element of $\mathbb{F}_q$. Then there exist a primitive polynomial of degree 7 over $\mathbb{F}_q$ with the coefficient of x^4 and the constant term specified as a and $-c$, respectively.*

Proof. Suppose $\omega(E_7) \geq 20$. Then (by $(A.33)$), $W(E_7) < (E_7)^{\frac{1}{8}} < (q^7)^{\frac{1}{8}} < q^{\frac{7}{8}}$. Then, by (6.5), to show existence it suffices that $q > 9 \cdot q^{\frac{7}{8}}$, or $q > 9^8$, which obviously holds as $\omega(E_7) \geq 20$ yields $q > 10^8$. □

We can now assume $\omega(E_7) \leq 19$ and sieve: the outcome is displayed in the table below.

#	$q \leq$	$\omega(E_7) \leq$	k_0	$\omega(k_0) \leq$	s	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		19	1	0	19	0.874	22.60	204
2	203	7	1	0	7	0.901	8.66	78
3	77	5	1	0	5	0.911	6.40	58

Next, $q = 53$, 49, 47, 43, 41, 37, 32, 31, 29, 23, 17 and 11 all satisfy criterion (6.5) when k_0 is set to be 1. When $q = 25, 16$ and 8, we are able to refine the sufficient condition for existence like we did for $q = 49$ in the Section 5.3.1. For $q = 19$, 13, 7, 5, 4 and 2, we searched for suitable primitive polynomials with Maple.

6.2.5 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 prime divisors of $(q+1)(q^2+1)$ and K_2 is the product of distinct prime divisors of q^4+1 that do not divide q^4-1. By an analogue of Lemma 4.4.1, 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. Note that 2 is never a factor of E_8.

Lemma 6.2.10. *Suppose that $n = 8$, $\omega_1 \geq 16$ or $\omega_2 \geq 13$. 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^5 prescribed as a and constant term c.*

Proof. First suppose $\omega_1 \geq 16$ and $\omega_2 \geq 13$. By $(A.11)$, $W(K_1) < ((q+1)(q^2+1))^{\frac{3}{13}} < (2q^3)^{\frac{3}{13}} = 2^{\frac{3}{13}} q^{\frac{9}{13}}$. Furthermore, the bound $(A.37)$ yields $W(K_2) < (q^4+1-1)^{\frac{2}{13}} < q^{\frac{8}{13}}$. It follows that $W(E_8) < 2^{\frac{3}{13}} q^{\frac{17}{13}}$. Consequently, by (6.5), to show existence it suffices that

$q^{\frac{3}{2}} > 9 \cdot 2^{\frac{3}{13}} q^{\frac{17}{13}}$, i.e. $q \geq 210521$, which obviously holds as the size of ω_1 and ω_2 yields $q > 10^6$.

Next, suppose $\omega_1 \leq 15$ and $\omega_2 \geq 13$. Take k_0 to be the product of K_2 and least two primes in K_1. Then $s \leq 13$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{53} > 0.352$ and $\Delta_{s,\delta} < 36.10$. Hence (6.5) is satisfied whenever $q^{\frac{3}{2}} > 9 \cdot 4 \cdot q^{\frac{8}{13}} \cdot 36.10$, i.e. $q \geq 3311$. This is the case since $\omega_2 \geq 13$, whence $q > 10^6$.

Finally, we suppose $\omega_1 \geq 16$ and $\omega_2 \leq 12$. Take $k_0 = K_1$. Then $s \leq 12$,

$$\delta \ \geq \ 1 - \sum_{\substack{l \leq 281 \\ l \equiv 1 (\mathrm{mod}\, 8)}} \frac{1}{l} \ > \ 0.844$$

and $\Delta_{s,\delta} < 15.04$. Now (6.5) is satisfied whenever $q \geq 531$, which completes the proof as $\omega_1 \geq 16$ yields $q > 10^6$. □

Consequently, we now assume $\omega_1 \leq 15$, $\omega_2 \leq 12$ and run the sieve. The sieving steps are summarized in the following table. (In lines 5 and 6 we can make reductions in ω_1, ω_2 as there are no q with $\omega_1, \omega_2 = 4$ in the given range.)

#	$q \leq$	$\omega_1 \leq$	$\omega_2 \leq$	k_0	$\omega(k_0)$	$s \leq$	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		15	12	15	2	25	0.247	99.17	234
2	233	7	5	3	1	11	0.274	38.50	79
3	78	6	4	3	1	9	0.328	26.40	61
4	60	5	4	3	1	8	0.381	20.38	52
5	51	5	3	3	1	7	0.392	17.31	46
6	45	3	3	3	1	5	0.560	9.15	31

Each prime power q, $29 \geq q \geq 16$ as well as $q = 8$, satisfy (6.5) with k_0 the least prime in E_8. When $q = 13, 11, 7, 5, 4$ or 2, however, the primitive polynomials had to be found explicitly by Maple.

6.3 The ternary problem

Suppose $q \equiv 0 \pmod 3$. Here we apply the p-adic theory, given in Section 2.5, for $p = 3$. In this context Lemma 3.2.1 assumes the following shape.

Lemma 6.3.1. *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*

$$3\sigma_3 = \sigma_2 s_1 - \sigma_1 s_2 + s_3. \tag{6.9}$$

Lemma 6.3.2. *Let f, σ_i and s_i be as in Lemma* 6.3.1. *Then $2\sigma_3 = s_{1,0}^3 - s_{1,0}s_{2,0} + 2s_{1,1}^3 \pmod 3$.*

Proof. Over $R_{1,2}$, equality (6.9) translates to

$$\begin{aligned} 6\sigma_3 &= s_1^3 - 3s_1 s_2 + 2s_3 \\ &= (s_{1,0} + 3s_{1,1})^3 - 3(s_{1,0} + 3s_{1,1})(s_{2,0} + 3s_{2,1}) + 2(s_{1,0}^3 + 3s_{1,1}^3) \end{aligned}$$

which, modulo 9, is congruent to $3s_{1,0}^3 - 3s_{1,0}s_{2,0} + 6s_{1,1}^3$. Hence $2\sigma_3 = s_{1,0}^3 - s_{1,0}s_{2,0} + 2s_{1,1}^3 \pmod 3$. □

We wish to assign the value a to the third coefficient, i.e., set $\sigma_3 = -a$. In characteristic 3, we can write $-a = A^3,\ A \in \mathbb{F}_q$. To achieve this, set $s_{1,0} = 0$ and $s_{1,1} = A$.

The characteristic function for the set of elements $\gamma \in \Gamma_{n,2}$ for which $s_{1,0} = 0$ and $s_{1,1} = A$ is

$$\frac{1}{q^2} \sum_{\xi \in R_{1,2}} \chi(\xi(T_n(\gamma) - 3A)) = \frac{1}{q^2} \sum_{\alpha_0, \alpha_1 \in \Gamma_{1,1}} \chi_{(n)}((\alpha_0 + 3\alpha_1)(\gamma))\chi(-3\alpha_0 A),\ \xi = \alpha_0 + 3\alpha_1$$

It follows that, for k a divisor of $q^n - 1$,

$$\frac{q^2 \pi_a(k)}{\theta(k)} = \int_{d|k} \sum_{\alpha_0, \alpha_1 \in \Gamma_{1,1}} \bar{\chi}(3\alpha_0 A)\ S_n(\xi; \eta_d), \tag{6.10}$$

where $S_n(\xi; \eta) = \sum_{\gamma \in \Gamma_{n,2}} \chi(\xi\gamma)\eta(\gamma)$.

Of course, $S_n(\xi; \eta_d) = 0$ unless $d = 1$. Hence the "main term" (corresponding to $\xi = 0$) is $q^n - 1$.

The next lemma summarises bounds for $S_n(\xi; \eta_d) = 0$ implied by [20] when $\xi \neq 0$.

Lemma 6.3.3. *Suppose $\xi = \alpha_0 + 3\alpha_1 \in R_{1,2}^*$. Then the following hold:*

- $S_n(\xi; \mathbf{1}) = 0$;
- $|S_n(3\alpha_1; \eta_d)| \leq q^{\frac{n}{2}},\ \alpha_1 \neq 0$;

- $|S_n(\alpha_0;\eta_d)| \le q^{\frac{n}{2}},\ \alpha_0 \neq 0$;
- $|S_n(\alpha_0+3\alpha_1;\eta_d)| \le 3q^{\frac{n}{2}},\ \alpha_0\alpha_1 \neq 0$.

We consider the contribution to the right side of (6.10) from terms with $\alpha_0 \neq 0$. Replace α_1 by $\alpha_0\alpha_1$ and γ by $\frac{\gamma}{\alpha_0}$. The contribution is

$$\begin{aligned} & \int_{1<d|k} \sum_{\alpha_1\in\Gamma_{1,1}} \sum_{\alpha_0\in\Gamma_{1,1}} \bar{\chi}(3\alpha_0 A)\bar{\tilde{\eta}}_d(\alpha_0) S_n(1+3\alpha_1;\eta_d) \\ = & \int_{1<d|k} \sum_{\alpha_1\in\Gamma_{1,1}} S_1(3A;\bar{\tilde{\eta}}_d) S_n(1+3\alpha_1;\eta_d). \end{aligned} \tag{6.11}$$

For the terms with $\alpha_0 = 0,\ \alpha_1 \neq 0$, replace γ by $\frac{\gamma}{\alpha_1}$ to yield the contribution

$$\int_{1<d|k} \sum_{\alpha_1\in\Gamma^*_{1,1}} \bar{\tilde{\eta}}_d(\alpha_1) S_n(3;\eta_d). \tag{6.12}$$

Note that in (6.12), the sum over α_1 is zero unless $d|Q_n$ (because $\bar{\tilde{\eta}}_d$ is trivial).

It is time to split the discussion into zero and non-zero cases according to the value of A. The zero case will only be needed when $n = 6$, and is therefore treated in Section 6.3.3. Here we proceed supposing $A \neq 0$. Then by Lemma 6.3.3, the sum $S_1(3A;\bar{\tilde{\eta}}_d)$ in absolute value does not exceed 1 if $d|Q_n$ and does not exceed $\sqrt{q}$ otherwise. Hence, for each character η_d $(1 < d|k)$ with $d \nmid Q_n$, by Lemma 6.3.3, we obtain a total contribution of $3(q-1)q^{\frac{n+1}{2}} = 3(1-\frac{1}{q})q^{\frac{n+3}{2}}$.

On the other hand, for each character η_d $(1 < d|k)$ with $d|Q_n$, we obtain a bound $3(q-1)q^{\frac{n}{2}}$ from contributions with $\alpha_0 \neq 0$ (governed by (6.11)) and $(q-1)q^{\frac{n}{2}}$ from contributions with $\alpha_0 = 0$, $\alpha_1 \neq 0$ (governed by (6.12)), a total of $4(1-\frac{1}{q})q^{\frac{n}{2}+1}$. Since this is less than $3(1-\frac{1}{q})q^{\frac{n+3}{2}}$, for simplicity we use the latter as a bound for the contribution for every $\eta_d,\ d > 1$.

Thus the right hand side of (6.10) is bounded by $3W(k)\left(1-\frac{1}{q}\right)q^{\frac{n+3}{2}}$. This yields a sufficient condition (in the non-sieve case) of

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

More generally:

Proposition 6.3.4. *Assume that $q \equiv 0 \pmod 3$ and $a \in \mathbb{F}$ is non-zero. Assume also that $k|q^n-1$ and that (k_0,s) is a decomposition of k. Suppose also that*

$$q^{\frac{n-3}{2}} > 3\left(1-\frac{1}{q}\right)W(k_0)\Delta_{s,\delta}. \tag{6.13}$$

Then $\pi_a(k)$ is positive. In particular, when $s = 1$, the sufficient condition is

$$q^{\frac{n-3}{2}} > 3\left(1 - \frac{1}{q}\right) W(q^n - 1). \tag{6.14}$$

Multiplicatively, $\mathbb{F}_{q^n}^* \cong \Gamma_{n,3}^*$. 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 5.1.5), there is an analogous expression for $\dfrac{(q-1)q\pi_{a,c}}{\theta(k_0)}$ to (6.10) comparable to the relationship Lemma 6.2.4 bears to Lemma 6.2.3. 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 $\Gamma_{n,2}^*$.

Proposition 6.3.5. *Assume that $q \equiv 0 \pmod 3$, $a \in \mathbb{F}$ is non-zero and c is a primitive element of $\mathbb{F}$. Assume also that $k|E_n$ and that (k_0, s) is a decomposition of k. Suppose also that*

$$q^{\frac{n-5}{2}} > 3\left(1 - \frac{1}{q}\right)^2 W(k_0)\Delta_{s,\delta}. \tag{6.15}$$

Then $\pi_{a,c}(k)$ is positive. In particular, when $s = 1$, the condition takes the form

$$q^{\frac{n-5}{2}} > 3\left(1 - \frac{1}{q}\right)^2 W(E_n). \tag{6.16}$$

6.3.1 Quintics

Suppose $n = 5$. Express the product of distinct primes in $q^5 - 1$ as $K_1 \cdot K_2$ and define ω_1, ω_2 as in Section 6.2.1 and note again that all prime divisors of K_2 are $\equiv 1 \pmod{10}$. Observe that, throughout Section 6.3, 3 is not a factor of $q^n - 1$.

Lemma 6.3.6. *Suppose that $n = 5$, $q \equiv 0 \pmod 3$ and $\omega_1 \geq 11$ or $\omega_2 \geq 22$. Let a ($\neq 0$) $\in \mathbb{F}_q$. Then there exists a primitive polynomial of degree 5 over $\mathbb{F}_q$ with the coefficient of x^2 prescribed as a.*

Proof. First suppose $\omega_1 \geq 11$ and $\omega_2 \geq 22$. By (*A*.14), the number of square-free divisors of h, an integer such that $\omega(h) \geq 11$ and $h \not\equiv 0 \pmod 3$, is bounded by $W(h) < h^{\frac{7}{26}}$. Therefore $W(K_1) < (q-1)^{\frac{7}{26}} < q^{\frac{7}{26}}$. Also, by (*A*.28), $W(h) < h^{\frac{3}{22}}$. That yields $W(K_2) < (Q_5)^{\frac{3}{22}} < (q^5)^{\frac{3}{22}} = q^{\frac{15}{22}}$. It follows that $W(q^5 - 1) < q^{\frac{136}{143}}$. Consequently, by (6.14), to show existence it suffices that $q > 3q^{\frac{136}{143}}$, i.e. $q \geq 3^{\frac{143}{7}} = 5583488579$, which obviously holds as $\omega_1 \geq 11$ and $\omega_2 \geq 22$ both yield $q > 10^{12}$.

Next, suppose $\omega_1 \leq 10$ and $\omega_2 \geq 22$. Set k_0 to be the product of K_2 and three smallest primes in K_1. Thus $s \leq 7$, $\delta \geq 1 - \frac{1}{11} - \ldots - \frac{1}{31} > 0.610$ and $\Delta_{s,\delta} < 11.84$. By the above, $W(k_0) < 8q^{\frac{15}{22}}$ and (6.13) is satisfied whenever $q \geq 51427786$. This is the case since $\omega_2 \geq 22$, whence $q > 10^{12}$.

At last, suppose $\omega_1 \geq 11$ and $\omega_2 \leq 21$. Put $k_0 = K_1$. Then $s \leq 21$,

$$\delta \;\geq\; 1 - \sum_{\substack{l \leq 461 \\ l \equiv 1 (\mathrm{mod}\, 10)}} \frac{1}{l} \;>\; 0.751$$

and $\Delta_{s,\delta} < 28.64$. Now (6.13) is satisfied whenever $q \geq 444$, which completes the proof since $\omega_1 \geq 11$ implies $q > 10^{12}$. □

Following Lemma 6.3.6, we assume $\omega_1 \leq 10$, $\omega_2 \leq 21$ and obtain the following results.

#	q	ω_1	ω_2	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		≤ 10	≤ 21	10	2	≤ 29	0.291	98.22	1179
2	≤ 729	≤ 3	≤ 6	2	1	≤ 8	0.469	16.93	102
3	81	2	3	2	1	4	0.691	6.35	38
4	27	2	2	2	1	3	0.831	4.41	26

When $q = 9$ or 3, primitive quintics with third coefficient prescribed have to be found explicitly. Here $\mathbb{F}_9$ is defined as $\mathbb{F}_3(\alpha)$, where α is a root of $x^2 + x + 2 \in \mathbb{F}_3$.

a	$q = 3$	$q = 9$
1	$x^5 + x^4 + x^2 + 1$	$x^5 + x^2 + \alpha$
2	$x^5 + 2x^2 + x + 1$	$x^5 + 2x^2 + \alpha + 2$
α	—	$x^5 + \alpha x^2 + \alpha$
$\alpha + 1$	—	$x^5 + (\alpha + 1)x^2 + \alpha$
$2\alpha + 1$	—	$x^5 + (2\alpha + 1)x^2 + 2\alpha + 1$
$2\alpha + 2$	—	$x^5 + (2\alpha + 2)x^2 + 2\alpha + 1$
$\alpha + 2$	—	$x^5 + (\alpha + 2)x^2 + 2\alpha + 1$
2α	—	$x^5 + 2\alpha x^2 + \alpha$

6.3.2 Sextics: the non-zero problem

Express the product of distinct primes in $q^6 - 1$ as $K_1 \cdot K_2$ and define ω_1, ω_2 as in Section 6.2.2.

Lemma 6.3.7. *Suppose that* $n = 6$, $q \equiv 0 \pmod 3$ *and* $\omega_1 \geq 9$ *or* $\omega_2 \geq 12$. *Let* $a\ (\neq 0) \in \mathbb{F}_q$. *Then there exists a primitive polynomial of degree* 6 *over* $\mathbb{F}_q$ *with the coefficient of* x^3 *prescribed as* a.

Proof. First suppose $\omega_1 \geq 9$ and $\omega_2 \geq 12$. By $(A.12)$, the number of square-free divisors of an integer $h \not\equiv 0 \pmod 3$, with $\omega(h) \geq 9$, is bounded by $W(h) < h^{\frac{3}{10}}$. Hence $W(K_1) < (q^2-1)^{\frac{3}{10}} < q^{\frac{3}{5}}$. Also, by the bound $(A.20)$, $W(h) < h^{\frac{3}{16}}$. That yields $W(K_2) < (q^4 + q^2 + 1)^{\frac{3}{16}} < (2q^4)^{\frac{3}{16}} = 2^{\frac{3}{16}} q^{\frac{3}{4}}$. It follows that $W(q^6-1) < 2^{\frac{3}{16}} q^{\frac{27}{20}}$. Consequently, by (6.14), to show existence it suffices that $q^{\frac{3}{2}} > 3 \cdot 2^{\frac{3}{16}} q^{\frac{27}{20}}$, i.e. $q \geq 3607$, which obviously holds as $\omega_1 \geq 9$ and $\omega_2 \geq 12$ both yield $q > 10^4$.

Next, suppose $\omega_1 \leq 8$ and $\omega_2 \geq 12$. Take k_0 to be the product of K_2 and two smallest primes in K_1. Thus $s \leq 6$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{23} > 0.534$ and $\Delta_{s,\delta} < 11.37$. By the above, $W(k_0) < 4 \cdot 2^{\frac{3}{16}} q^{\frac{3}{4}}$ and (6.13) is satisfied whenever $q \geq 836$. This is the case since $\omega_2 \geq 12$, whence $q > 10^4$.

Finally, we suppose $\omega_1 \geq 9$ and $\omega_2 \leq 11$. Putting $k_0 = K_1$ gives $s \leq 11$,

$$\delta \ \geq \ 1 - \sum_{\substack{l \leq 97 \\ l \equiv 1 \pmod 6}} \frac{1}{l} \ > \ 0.571$$

and $\Delta_{s,\delta} < 19.52$. Now (6.13) is satisfied whenever $q \geq 93$, which completes the proof as $\omega_1 \geq 9$ yields $q > 10^4$. □

Consequently to the above Lemma, we now assume $\omega_1 \leq 8$, $\omega_2 \leq 11$ and run the sieve: the two steps are shown in the following table.

#	q	ω_1	ω_2	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		≤ 8	≤ 11	10	2	≤ 17	0.298	55.70	77
2	≤ 27	≤ 3	≤ 4	2	1	≤ 6	0.404	14.38	20

The relevant polynomials in $\mathbb{F}_9$ (defined as in the previous section) and $\mathbb{F}_3$ are given

below.

a	$q=3$	$q=9$
1	x^6+x^3+x+2	$x^6+x^3+x^2+x+\alpha$
2	x^6+2x^3+2x+2	$x^6+2x^3+x^2+2x+\alpha$
α	—	$x^6+\alpha x^3+x^2+2\alpha+2$
$\alpha+1$	—	$x^6+(\alpha+1)x^3+x^2+\alpha$
$2\alpha+1$	—	$x^6+(2\alpha+1)x^3+x^2+(\alpha+2)x+\alpha+1$
$2\alpha+2$	—	$x^6+(2\alpha+2)x^3+x^2+\alpha$
$\alpha+2$	—	$x^6+(\alpha+2)x^3+x^2+(2\alpha+1)x+\alpha+1$
2α	—	$x^6+2\alpha x^3+x^2+2\alpha+2$

6.3.3 Sextics: the zero problem

An isolated case of the ternary problem where considering the possibility of the third coefficient being prescribed zero is needed, is when $n=6$. Therefore we treat it in this separate subsection, complete with the estimates necessary to establish the criterion for the existence of desired primitive polynomials.

Now, wishing to fix the third coefficient as zero, following Lemma 6.3.2 we suppose $A=0$. We may therefore assume also that $k|Q_n$. Suppose $1<d|Q_n$. In this case, the sum $S_1(3A;\tilde{\bar{\eta}}_d)$ is trivially $q-1$ and we obtain a contribution for each η_d bounded by the sum $3(q-1)q^{\frac{n}{2}+1}$ (from (6.11)) and $(q-1)q^{\frac{n}{2}}$ (from (6.12)). In total this is less than $3\left(1-\frac{2}{3q}\right)q^{\frac{n+4}{2}}$. Thus the right hand side of (6.10) is bounded by $3W(k)\left(1-\frac{2}{3q}\right)q^{\frac{n+4}{2}}$. This yields a sufficient condition of

$$q^{\frac{n-4}{2}} > 3\left(1-\frac{2}{3q}\right)W(k_0)\Delta_{s,\delta} \tag{6.17}$$

and, if $s=1$,

$$q^{\frac{n-4}{2}} > 3\left(1-\frac{2}{3q}\right)W(Q_n). \tag{6.18}$$

As always, when the coefficient is prescribed to be zero, we only need to consider $W(Q_n)$. Therefore we express the product of distinct primes in Q_6 as $K_1\cdot K_2$ and define ω_1, ω_2 as in Section 6.2.3.

Lemma 6.3.8. *Suppose that $n=6$, $q\equiv 0 \pmod 3$ and $\omega_1\geq 10$ or $\omega_2\geq 23$. Then there exists a primitive polynomial of degree 6 over $\mathbb{F}_q$ with the coefficient of x^3 prescribed as zero.*

Proof. We begin by supposing $\omega_1 \geq 10$ and $\omega_2 \geq 23$. By $(A.13)$, $W(K_1) < (q+1-1)^{\frac{7}{25}} < q^{\frac{7}{25}}$ and by $(A.22)$, $W(K_2) < (q^4+q^2+1)^{\frac{4}{25}} < (2q^4)^{\frac{4}{25}} = 2^{\frac{4}{25}} q^{\frac{16}{25}}$. Hence $W(Q_6) < 2^{\frac{4}{25}} q^{\frac{23}{25}}$. Consequently, by (6.18), to show existence it suffices that $q > 3 \cdot 2^{\frac{4}{25}} q^{\frac{23}{25}}$, i.e. $q \geq 3681932$, which holds as $\omega_1 \geq 10$ and $\omega_2 \geq 23$ both yield $q > 10^{10}$.

Next, suppose $\omega_1 \leq 9$ and $\omega_2 \geq 23$. Take k_0 to be the product of K_2 and two smallest primes in K_1. Thus $s \leq 7$, $\delta \geq 1 - \frac{1}{7} - \ldots - \frac{1}{29} > 0.499$ and $\Delta_{s,\delta} < 14.03$. By the above reasoning, $W(k_0) < 4 \cdot 2^{\frac{4}{25}} q^{\frac{16}{25}}$ and (6.17) is satisfied whenever $q \geq 2078683$. This holds since $\omega_2 \geq 23$, whence $q > 10^{10}$.

At last, we suppose $\omega_1 \geq 10$ and $\omega_2 \leq 22$. Putting $k_0 = K_1$ gives $s \leq 22$,

$$\delta \;\geq\; 1 - \sum_{\substack{l \leq 211 \\ l \equiv 1 \pmod 6}} \frac{1}{l} \;>\; 0.503$$

and $\Delta_{s,\delta} < 43.75$. Now (6.17) is satisfied whenever $q \geq 875$, which completes the proof as $\omega_1 \geq 10$ yields $q > 10^{10}$. □

Assume now that $\omega_1 \leq 9$ and $\omega_2 \leq 22$. Here is the sieving table.

#	q	ω_1	ω_2	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		≤ 9	≤ 22	70	3	≤ 28	0.368	75.37	1809
2	≤ 729	≤ 3	≤ 7	2	1	≤ 9	0.337	25.74	155
3	81	2	4	2	1	5	0.741	7.40	45

The relevant polynomials for the remaining values $q = 27$, 9 and 3 are listed below. (Here $\mathbb{F}_{27}$ is defined as $\mathbb{F}_3(\alpha)$, where α is a root of $x^3 + 2x + 1 \in \mathbb{F}_3[x]$, and $\mathbb{F}_9$ is defined as before.)

q	$f(x)$
27	$x^6 + x + \alpha$
9	$x^6 + x^2 + \alpha x + \alpha$
3	$x^6 + x + 2$

6.3.4 Septics

Lemma 6.3.9. *Suppose that $n = 7$ and $q \equiv 0 \pmod 3$. 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^4 and the constant term specified as a and $-c$, respectively.*

Proof. Suppose $\omega(E_7) \geq 16$. Then, by $(A.32)$, when integer h is a product of primes $l \equiv 1 \pmod{14}$ and $\omega(h) \geq 16$, the number of square-free divisors of h is bounded by $W(h) < h^{\frac{13}{100}}$. Hence $W(E_7) < (E_7)^{\frac{13}{100}} < (q^7)^{\frac{13}{100}} < q^{\frac{91}{100}}$. Then, by (6.16), to show existence it suffices that $q > 3 \cdot q^{\frac{91}{100}}$, or $q \geq 200147$, which obviously holds as $\omega(E_7) \geq 16$ yields $q > 10^7$.

Assume $\omega(E_7) \leq 15$. The sieving steps are shown in the table below.

#	q	$\omega(E_7)$	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		≤ 15	1	0	≤ 15	0.879	17.93	54
2	≤ 27	≤ 4	1	0	≤ 4	0.919	5.27	16
3	9	2	1	0	3	0.997	3.01	8

The two remaining polynomials in $\mathbb{F}_3[x]$ are $x^7 + x^6 + x^3 + 2x^2 + x + 1$ and $x^7 + x^6 + 2x^3 + x^2 + 2x + 1$ (note that the constant must necessarily equal 1.) This completes the proof. □

6.3.5 Octics

Express the product of distinct primes in E_8 as $K_1 \cdot K_2$ and define ω_1, ω_2 as in Section 6.2.5.

Lemma 6.3.10. *Suppose that $n = 8$, $q \equiv 0 \pmod{3}$ and $\omega_1 \geq 11$ or $\omega_2 \geq 10$. 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^5 and the constant term specified as a and c, respectively.*

Proof. First suppose $\omega_1 \geq 11$ and $\omega_2 \geq 10$. By $(A.15)$, $W(K_1) < ((q+1)(q^2+1))^{\frac{1}{4}} < (2q^3)^{\frac{1}{4}} = 2^{\frac{1}{4}} q^{\frac{3}{4}}$. Furthermore, $(A.36)$ yields $W(K_2) < (q^4 + 1 - 1)^{\frac{2}{13}} < q^{\frac{8}{13}}$. It follows that $W(E_8) < 2^{\frac{1}{4}} q^{\frac{71}{52}}$. Consequently, by (6.16), to show existence it suffices that $q^{\frac{3}{2}} > 3 \cdot 2^{\frac{1}{4}} q^{\frac{71}{52}}$, i.e. $q \geq 12688$, which obviously holds as $\omega_1 \geq 11$ and $\omega_2 \geq 10$ both yield $q > 3 \cdot 10^4$.

Next, suppose $\omega_1 \leq 10$ and $\omega_2 \geq 10$. Take $k_0 = K_2$. Then $s \leq 10$, $\delta \geq 1 - \frac{1}{5} - \ldots - \frac{1}{37} > 0.240$ and $\Delta_{s,\delta} < 39.51$. Hence (6.15) is satisfied whenever $q^{\frac{3}{2}} > 3 \cdot q^{\frac{8}{13}} \cdot 39.51$, i.e. $q \geq 221$. This is the case since $\omega_2 \geq 10$, whence $q > 10^4$.

Finally, we suppose $\omega_1 \geq 11$ and $\omega_2 \leq 9$. Take $k_0 = K_1$. Then $s \leq 9$,

$$\delta \;\geq\; 1 - \sum_{\substack{l \leq 233 \\ l \equiv 1 (\mathrm{mod}\, 8)}} \frac{1}{l} \;>\; 0.855$$

and $\Delta_{s,\delta} < 11.36$. Now (6.15) is satisfied whenever $q \geq 140$, which completes the proof as $\omega_1 \geq 11$ yields $q > 10^4$. □

Consequently to Lemma 6.3.10, we now assume $\omega_1 \leq 10$, $\omega_2 \leq 9$ and sieve:

#	q	ω_1	ω_2	k_0	$\omega(k_0)$	s	$\delta \geq$	$\Delta_{s,\delta} <$	q_{min}
1		≤ 10	≤ 9	5	1	≤ 18	0.331	53.36	47
2	≤ 27	≤ 4	≤ 3	1	0	≤ 7	0.392	17.31	14
3	≤ 9	≤ 3	≤ 2	1	0	≤ 5	0.483	10.29	9
4	3	1	1	1	0	2	0.775	3.30	3

This completes the chapter as well as the HMPC for $n = 5, 6$ and 7. The only remaining case of the HMPC is now $m = 4$, $n = 8$ and is the subject of the following chapter.

Chapter 7

The fourth coefficient

This chapter is dedicated to the HMPC with $m = 4$. It achieves the final goal of settling the existence of primitive polynomials with $(n, m) = (8, 4)$, thereby completing the proof of the Hansen-Mullen conjecture. We separately consider the fields of characteristic 2, where p-adic is required, (the *even* problem) and those with odd characteristic (the *odd* problem). The methods used are very efficient and the amount of computation required is next to none.

7.1 Main results

The following theorem asserts the existence of a primitive polynomial of degree $n \geq 8$, with arbitrarily prescribed fourth coefficient.

Theorem 7.1.1. *Suppose $n \geq 8$. Let a be an arbitrary member of the finite field $\mathbb{F}_q$. Then there exists a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n with fourth coefficient prescribed as a.*

Corollary 7.1.2. *Suppose $n = 8$ and $m = 4$. Then the HMPC holds.*

7.2 The odd problem

Throughout this section $\mathbb{F}_q$ is a field of characteristic *not* 2. Putting $m = 4$ in Lemma 3.2.1 and setting $s_1 = 0$ (already) yields

$$4\sigma_4 = -\sigma_2 s_2 - s_4. \tag{7.1}$$

(We would like to signify that working in this order avoids any difficulties in characteristic 3.)

Condition (7.1) can be further expressed as

$$8\sigma_4 = s_2^2 - 2s_4.$$

For $a \in \mathbb{F}_q$ and for any $z \in \mathbb{F}_q$, setting $s_2 = z$ and $2s_4 = z^2 - 8a$ fixes the fourth coefficient of the polynomial as a. Now, using the characteristic functions defined in Section 3.3, we can deduce a basic formula for $\pi_a(k)$.

Lemma 7.2.1. *Suppose q is odd, $a \in \mathbb{F}_q$ is given and $k|q^n - 1$. Then*

$$q^3\pi_a(k) \;=\; \theta(k) \int\limits_{d|k} \sum_{\alpha,\beta,z\in\mathbb{F}_q} \bar{\chi}(\alpha(z^2-8a)+\beta z)\; S_n(2\alpha,\beta;\eta_d), \tag{7.2}$$

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

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

$$\begin{aligned}\frac{q^3\pi_a(k)}{\theta(k_0)} \;&=\; \delta \int\limits_{d|k_0} \sum_{\alpha,\beta,z\in\mathbb{F}_q} \bar{\chi}(\alpha(z^2-8a)+\beta z)\; S_n(2\alpha,\beta;\eta_d) \\ &+\; \sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right) \int\limits_{d|k_0} \sum_{\alpha,\beta,z\in\mathbb{F}_q} \bar{\chi}(\alpha(z^2-8a)+\beta z) S_n(2\alpha,\beta;\eta_{dp_i}).\end{aligned} \tag{7.3}$$

In particular, the contribution to the right side of (7.3) *attributable to values of $\alpha = \beta = 0$ (the "main term") is $\delta q(q^n - 1)$.*

Proof. For (7.3) use the equivalence of the right sides of (3.6) and (3.7).

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 (7.3).

Of course, (7.2) is recovered from (7.3) by setting $s = 1$. □

Estimates for $S_n(\alpha,\beta;\eta_d)$ are standard (see [2], (1.3)):

Lemma 7.2.2. *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

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

Of course, now $S_1(\alpha, \beta; \eta_d)$ is not the same function as $S_1(\kappa\beta^T, \eta)$ in Chapter 6.

At this point it is convenient to split the discussion in two parts: the zero and the non-zero problem. First consider the case when the prescribed coefficient a is *non-zero*.

The odd non-zero problem

Proposition 7.2.3. *Suppose q is odd and $a \neq 0$. Let $k|q^n-1$ and (k_0, s) be a decomposition of k. Suppose*

$$q^{\frac{n-4}{2}} > 4W(k_0)\Delta_{s,\delta}. \tag{7.4}$$

Then $\pi_a(k)$ is positive.

Proof. Consider the expression (7.3). 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 $\frac{d}{\gcd(d,Q_n)}$.

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

$$\delta \sum_{\alpha\in\mathbb{F}_q} \sum_{\beta\in\mathbb{F}_q^*} \chi(8a\alpha\beta^2)\bar{\tilde{\eta}}_d(\beta) \sum_{z\in\mathbb{F}_q} \bar{\chi}(\alpha z^2 + z)\ S_n(2\alpha, 1; \eta_d),$$

which is the same as

$$\delta \sum_{\alpha\in\mathbb{F}_q} S_1(8a\alpha, 0; \bar{\tilde{\eta}}_d)\ \overline{S_1(\alpha, 1; \mathbf{1})}\ S_n(2\alpha, 1; \eta_d). \tag{7.5}$$

The expression (7.5) is essentially the same as in the proof of Proposition 4.1 in [13]. Similarly, we obtain an analogous expression when considering the contribution from terms with $\beta = 0$. We therefore do not give a detailed discussion here; summarising, we obtain an absolute bound of $4\delta q^{\frac{n}{2}+3}$ for the (non-weighted) contribution of all terms corresponding to a character η_d.

The remaining terms on the right side of (7.3) (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 (7.3) exceeds

$$\delta\left(q^{n+1} \ - \ 4q^{\frac{n}{2}+3}\Delta_{s,\delta}\right),$$

with $\Delta_{s,\delta}$ as in Section 3.3, since $\sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right) = s-1 \ +\delta$.

□

Now consider $n = 8$. Criterion (7.4) then takes form

$$q^2 > 4W(k_0)\Delta_{s,\delta}. \tag{7.6}$$

Express the product of distinct primes in q^8-1 as $K_1 \cdot K_2$ where K_1 is the product of all distinct prime divisors of $(q^2+1)(q^2+1)$ and K_2 is the product of distinct prime divisors of q^4+1 that do not divide q^4-1. Remember that any prime divisor l of K_2 is an element of L_8. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2. Note that $16|q^4-1$ and therefore $\omega_1 = \omega(\frac{q^4-1}{8})$.

Lemma 7.2.4. *Suppose that $n = 8$, a $(\neq 0) \in \mathbb{F}_q$, q odd and $\omega_1 \geq 13$ or $\omega_2 \geq 7$. Then there exists a primitive polynomial of degree 8 over $\mathbb{F}_q$ with the coefficient of x^5 specified as a.*

Though the characteristic of the field is now different, the proof of this lemma parallels those of analogous lemmas in Chapter 6 and is omitted. Also the proofs of Lemmas 7.2.6, 7.3.7 and 7.3.8 will be omitted.

Now suppose $\omega_1 \leq 12$ or $\omega_2 \leq 6$. Employing the sieve, the existence of primitive octics with forth coefficient prescribed as $a \neq 0$ is proved in just two steps for $q \geq 17$. First, taking k_0 to be the product of three least primes in K_1 yields $s \leq 14$, $\delta > 0.371$, $\Delta_{s,\delta} < 37.05$ and condition (7.6) holds for $q \geq 35$. Now take k_0 to be the product of two least primes in K_1. Hence $s \leq 7$, $\delta > 0.393$, $\Delta_{s,\delta} < 17.31$ and (7.6) is satisfied when $q \geq 17$. Applying (7.6) to $q = 13$ and 11 with $k_0 = 6$ also proves existence for these two values. Only $q = 7$, 5 and 3 need direct verification with Maple.

a	$q=3$	$q=5$	$q=7$
1	$x^8+x^5+x^4+2x^2+2$	$x^8+x^5+x^4+3x+3$	$x^8+x^5+x^4+x+5$
2	$x^8+2x^5+x^4+2x^2+2$	$x^8+2x^5+x^4+x+3$	$x^8+2x^5+x^4+2x+5$
3	—	$x^8+3x^5+x^4+4x+3$	$x^8+3x^5+x^4+5$
4	—	$x^8+4x^5+x^4+2x+3$	$x^8+4x^5+x^4+5$
5	—	—	$x^8+5x^5+x^4+5x+5$
6	—	—	$x^8+6x^5+x^4+6x+5$

The odd zero problem

When the prescribed coefficient is zero, it suffices to prove that $\pi_0(Q_n)$ is positive. Considering expression (7.5) with $a = 0$ and proceeding as before, the following proposition is derived.

Proposition 7.2.5. *Suppose q is odd, $a = 0$ and $n = 8$. Let $k|Q_8$ and (k_0, s) be a decomposition of k. Suppose*

$$q^{\frac{3}{2}} > 4W(k_0)\Delta_{s,\delta}. \tag{7.7}$$

Then $\pi_0(k)$ is positive.

Express the product of distinct primes in Q_8 as $K_1 \cdot K_2$, where K_1 is the product of all distinct prime divisors of $(q+1)(q^2+1)$ (and so even) and K_2 is the product of distinct odd prime divisors of q^4+1. By an analogue of Lemma 4.4.1 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 7.2.6. *Suppose that $n = 8$, $a = 0$, q odd and $\omega_1 \geq 16$ or $\omega_2 \geq 12$. Then there exists a primitive polynomial of degree 8 over $\mathbb{F}_q$ with the coefficient of x^5 specified as 0.*

Now assume $\omega_1 \leq 15$ and $\omega_2 \leq 11$ and begin the sieve. In the first step, take k_0 to be the product of three least primes in K_1. Then $s \leq 23$, $\delta > 0.279$, $\Delta_{s,\delta} < 80.86$ and criterion (7.7) holds for $q \geq 99$. Now, taking k_0 to be the product of two least primes in K_1 yields $s \leq 8$, $\delta > 0.381$, $\Delta_{s,\delta} < 20.38$ and (7.7) is satisfied for $q \geq 48$. It also holds for $q = 47$, 43, 41, 37, 31, 29, 27, 25, 23 and 19, but smaller values (17, 13, 11, 9, 7, 5, 3) need direct verification with Maple.

q	$f(x)$
3	$x^8 + x^3 + 2$
5	$x^8 + x^3 + 2x^2 + 2$
7	$x^8 + x^3 + 3x^2 + 3$
9	$x^8 + (2\alpha + 2)x^4 + (\alpha + 2)x + 2\alpha + 2$
11	$x^8 + 2x^3 + x^2 + 2$
13	$x^8 + x^3 + x^2 + 2$
17	$x^8 + 2x^3 + x^2 + 3$

7.3 The even problem

Suppose that q is even. In this section, we again require the use of p-adic analysis.

Lemma 7.3.1. *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*

$$4\sigma_4 = \sigma_3 s_1 - \sigma_2 s_2 + \sigma_1 s_3 - s_4. \tag{7.8}$$

Lemma 7.3.2. *Let f, σ_i and s_i be as in Lemma* 7.3.1. *Suppose $s_{1,0} = 0$. Then $\sigma_4 \equiv s_{1,2}^4 \pmod 2$.*

Proof. Over $R_{1,3}$, s_i $i = 1, ..., 4$ expand to $s_1 = s_{1,0} + 2s_{1,1} + 4s_{1,2}$, $s_2 = s_{1,0}^2 + 2s_{1,1}^2 + 4s_{1,2}^2$, $s_3 = s_{3,0} + 2s_{3,1} + 4s_{3,2}$ and $s_4 = s_{1,0}^4 + 2s_{1,1}^4 + 4s_{1,2}^4$. Accordingly, (7.8) translates to

$$\begin{aligned} 4\sigma_4 &\equiv 4s_{1,0}^4 + 4s_{1,0}(s_{3,0} + 2s_{3,1} + 4s_{3,2}) + 4s_{1,2}^4 \pmod 8 \\ \sigma_4 &\equiv s_{1,0}^4 + s_{1,0}(s_{3,0} + 2s_{3,1} + 4s_{3,2}) + s_{1,2}^4. \pmod 2 \end{aligned} \tag{7.9}$$

Setting $s_{1,0} = 0$ in (7.9) yields $\sigma_4 \equiv s_{1,2}^4 \pmod 2$. □

As a consequence of Lemma 7.3.2, for σ_4 to be prescribed modulo 2, it suffices to prescribe $s_{1,0} = 0$ and $s_{1,2} \in \Gamma_1$ appropriately. The value of $s_{1,1}$ appears to be irrelevant. Nevertheless, in practice we cannot prescribe $s_{1,2}$ without assigning a value (say $z \in \Gamma_{1,1}$) to $s_{1,1}$. In view of Lemma 7.3.2, given $a \in \mathbb{F}_q \cong \Gamma_{1,1}$, write $a = A^4, A \in \mathbb{F}_q$. We wish to prescribe $s_1 = s_{1,0} + 2s_{1,1} + 4s_{1,2} \in R_{1,2}$ as $2z + 4A$.

In order to apply Lemma 7.3.2, we require to work with the multiplicative characters of $\Gamma_{n,3}^*$, a cyclic group of order $q^n - 1$, and the additive characters of $R_{n,3}$. So now, for any divisor d of $q^n - 1$, η_d is a character of order d. It is extended to $\Gamma_{n,3}$ 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 $R_{n,3}$: thus

$$\chi_{(n)}(\gamma) = \exp\left(\frac{2\pi i T_{nu}(\gamma)}{8}\right), \quad q = 2^u, \quad \gamma \in R_{n,3}.$$

Here $T_{nu}(\gamma)$ yields the *absolute trace* of γ. In particular, set $\chi_{(1)} = \chi$. The characteristic function for the set of elements $\gamma \in \Gamma_{n,3}$ for which $s_1 (= s_{1,0} + 2s_{1,1} + 4s_{1,2}) = 2z + 4A$ is

$$\frac{1}{q^3} \sum_{\xi \in R_{1,3}} \chi(\xi(T_n(\gamma) - (2z + 4A))) \tag{7.10}$$

which equals

$$\frac{1}{q^3}\sum_{\alpha_0,\alpha_1,\alpha_2\in\Gamma_{1,1}}\chi_{(n)}((\alpha_0+2\alpha_1+4\alpha_2)(\gamma))\ \chi(-2(\alpha_0+2\alpha_1)z-4\alpha_0 A).$$

For the next lemma, note that, if $\xi=\alpha_0+2\alpha_1+4\alpha_2\in R_{1,3}$ with $\alpha_0,\alpha_1,\alpha_2\in\Gamma_{1,1}$, then $2\xi=2\hat{\xi}$, where $\hat{\xi}=\alpha_0+2\alpha_1\in R_{1,2}$.

Lemma 7.3.3. *Write $\xi\in R_{1,3}^*$ as $\hat{\xi}+4\alpha_2$, where $\hat{\xi}\in R_{1,2}$ and $\alpha_2\in\Gamma_{1,1}$. Set*

$$U_\xi=\sum_{z\in\Gamma_{1,1}}\chi(2\xi z).$$

Then $U_\xi=0$ unless $\hat{\xi}=0$ (and $\alpha_2\neq 0$) in which case $U_\xi=q$, or $\hat{\xi}=\pm\alpha_0$ $(\neq 0)$, in which case $U_\xi=\frac{1\pm i}{2}\cdot q$, respectively.

Proof. If $\hat{\xi}=0$ (and $\alpha_2\neq 0$) the result is obvious. Otherwise $U_\xi=\sum_{z\in\Gamma_{1,1}}\chi(\hat{\xi}z)$ and the conclusion follows from Lemma 6.3 of [13].

□

For $k|q^n-1$ and $a\neq 0\in\mathbb{F}_q$, write $\pi_a(k)$ for the number of k-free elements of $\mathbb{F}_{q^n}$ whose characteristic polynomial has first coefficient zero and fourth coefficient $a=A^4\in\mathbb{F}_q$.

Lemma 7.3.4. *Assume q is even and $a=A^4\in\mathbb{F}_q\cong\Gamma_{1,1}^*$. Let $k|q^n-1$ and (k_0,s) be a decomposition of k. Then*

$$\begin{aligned}
&\frac{q^2\pi_a(k)}{\theta(k_0)}\\
=\ &\delta\Big(q^n-1+\int_{d|k_0}\sum_{\alpha\in\Gamma_{1,1}^*}\bar{\tilde{\eta}}_d(\alpha)S_n(4,\eta_d)\\
+\ &\frac{1}{2}\int_{d|k_0}\sum_{\beta\in\Gamma_{1,1}}\sum_{\alpha\in\Gamma_{1,1}^*}\bar{\chi}(4\alpha A)\bar{\tilde{\eta}}_d(\alpha)\Big\{(1-i)S_n(1+4\beta;\eta_d)+(1+i)S_n(-(1+4\beta);\eta_d)\Big\}\Big)\\
+\ &\sum_{i=1}^{s}\left(1-\frac{1}{p_i}\right)\Big(\sum_{\alpha\in\Gamma_{1,1}^*}\bar{\tilde{\eta}}_d(\alpha)S_n(4,\eta_{dp_i})\\
&\frac{1}{2}\int_{d|k_0}\sum_{\beta\in\Gamma_{1,1}}\sum_{\alpha\in\Gamma_{1,1}^*}\bar{\chi}(4\alpha A)\bar{\tilde{\eta}}_{dp_i}(\alpha)\Big\{(1-i)S_n(1+4\beta;\eta_{dp_i})\Big\}\Big)\\
+\ &\frac{1}{2}\int_{d|k_0}\sum_{\beta\in\Gamma_{1,1}}\sum_{\alpha\in\Gamma_{1,1}^*}\bar{\chi}(4\alpha A)\bar{\tilde{\eta}}_{dp_i}(\alpha)\Big\{(1+i)S_n(-(1+4\beta);\eta_{dp_i})\Big\}\Big),
\end{aligned}$$

where, for $\xi\in R_{1,3}$, $S_n(\xi;\eta_d):=\sum_{\gamma\in\Gamma_{n,3}}\chi_{(n)}(\xi\gamma)\eta_d(\gamma)$ and $\tilde{\eta}_d$ is the restriction of η_d to $\Gamma_{1,1}$.

Proof. For notational simplicity consider only the trivial decomposition of k with $s = 1$. Write $\xi = \alpha_0 + 2\alpha_1 + 4\alpha_2 = \hat{\xi} + 4\alpha_2$ for a typical element of $R_{1,3}$.

From the characteristic functions (in particular (7.10)) one obtains

$$\frac{q^3\pi_a(k)}{\theta(k)} = \int_{d|k} \sum_{\xi \in R_{1,3}} \chi(4\alpha_0 A)\ U_\xi\ S_n(\xi;\eta_d), \tag{7.11}$$

with U_ξ as in Lemma 7.3.3. Since $S_n(0;\eta_d) = 0$ unless $d = 1$, the contribution to (7.11) from $\xi = 0$ (the "main term") is $q(q^n - 1)$.

From Lemma 7.3.3, $U_\xi = 0$ unless $\hat{\xi} = 0$ (i.e., $\xi = 4\alpha_2 \neq 0$), or $\xi = \pm\alpha_0$. Note that, when U_ξ is non-zero, its value can be expressed as cq and, ultimately, a factor of q is cancelled from (7.11). We consider the contributions from these excepted ξ.

First suppose $\hat{\xi} = 0$, i.e., $\alpha_0 = \alpha_1 = 0$ but $\alpha_d \neq 0$. Then $U_\xi = q$. Replacing γ by $\frac{\gamma}{\alpha_2}$ in the expression for $S_n(4\alpha_2;\eta_d)$, we obtain the sum $q \sum_{\alpha_2 \in \Gamma_{1,1}^*} \bar{\bar{\eta}}_d(\alpha_2) S_n(4;\eta_d)$, which is equivalent to the expression shown

Now consider the contribution from $\hat{\xi} = \pm\alpha_0 \neq 0$, i.e., $\alpha_0 \neq 0,\ \alpha_1 = 0,\ \alpha_2$ arbitrary. Replace $\gamma \in \Gamma_{n,3}$ by $\frac{\gamma}{\alpha_0} \in \Gamma_{n,3}$ and $\alpha_2 \in \Gamma_{1,1}$ by $\alpha_0\beta \in \Gamma_{1,1}$ to obtain the remainder of the displayed identity. □

The relevant bounds for $|S_n(\xi;\eta_d)|$ are as follows.

Lemma 7.3.5. *Suppose $\xi \in R_{1,3}^*$. Then $S_n(\xi;\mathbf{1}) = 0$. Further, if d (> 1) divides $q^n - 1$, then $|S_n(\xi;\eta_d)| \leq 4q^{\frac{n}{2}}$. Indeed, if $\beta \in \Gamma_{1,1}$ then $|S_n(4;\eta_d)| \leq q^{\frac{n}{2}}$.*

Proof. This follows from Corollary 6.1 of [23]. The significant point is that the polynomial $(\alpha_0 + 2\alpha_1 + 4\alpha_2)x \in R_{1,3}^*[x]$ has *weighted degree* 4 (if $\alpha_0 \neq 0$) or 1 (if $\alpha_0 = \alpha_1 = 0$). □

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

7.3.1 The even non-zero problem

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

Proposition 7.3.6. *Assume that q is even and $a \in \mathbb{F}$ is non-zero. Assume also that $k|q^n - 1$ and that (k_0, s) is a decomposition of k.Suppose also that*

$$q^{\frac{n-3}{2}} > 4\sqrt{2}\ W(k_0)\Delta_{s,\delta}. \tag{7.12}$$

Then $\pi_a(k)$ is positive.

Proof. Again for notational simplicity focus on the situation when the decomposition of k is trivial, i.e., $k_0 = k$ and only the first two lines of the identity of Lemma 7.3.4 are relevant. Indeed, apart from the main term $q^n - 1$, for any divisor d of k the balance of the contributions relating to multiplicative characters η_d arise from the first line and the second line is different, according to the value of d.

Specifically, suppose $d|Q_n$. Then $\bar{\bar{\eta}}_d$ is trivial and so $\sum_{\alpha\in\Gamma^*_{1,1}} \bar{\bar{\eta}}_d(\alpha) = q - 1$. Hence, by Lemma 7.3.5, the characters of order d contribute $(q-1)q^{\frac{n}{2}}$ from the first line. On the other hand, from the second line $\sum_{\alpha\in\Gamma^*_{1,1}} \bar{\chi}(4\alpha A)\bar{\bar{\eta}}_d(\alpha) = \sum_{\alpha\in\mathbb{F}^*_q} \bar{\chi_0}(\alpha A)$, where χ_0 is the canonical additive character on $\mathbb{F}_q$, and this is ≤ 1 in absolute value. Hence, by Lemma 7.3.5, the contributions from the second line of multiplicative characters of order d do not exceed $q^{\frac{n+1}{2}}$. Accordingly, the total contributions from characters or order d is certainly bounded by $2q^{\frac{n}{2}+1}$.

Finally, suppose, $d \nmid Q_0$. Then, in the first line, $\sum_{\alpha\in\Gamma^*_{1,1}} \bar{\bar{\eta}}_d(\alpha) = 0$. By the same lemma (with $n = 1$), in the second line $\displaystyle\sum_{\alpha\in\Gamma^*_{1,1}} \bar{\chi}(4\alpha A)\bar{\bar{\eta}}_d(\alpha) \leq q^{\frac{1}{2}}$ and, of course $|S_n(\pm(1 + 4\beta); \eta_d)| \leq 4q^{\frac{n}{2}}$. Accordingly, the contribution of characters of order d is bounded by $4\sqrt{2}q^{\frac{n+3}{2}}$. Since this easily exceeds the contribution for a divisor d of Q_n, we can use this as a global bound for any $d|k$ and the result follows.

□

Express the product of distinct primes in $q^8 - 1$ as $K_1 \cdot K_2$, where K_1 is the product of all distinct odd prime divisors of $q^4 - 1$ and K_2 is the product of distinct odd prime divisors of q^4+1. By an analogue of Lemma 4.4.1 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 7.3.7. *Suppose that $n = 8$, q odd, $\omega_1 \geq 8$ or $\omega_2 \geq 5$. Let a $(\neq 0) \in \mathbb{F}_q$. Then there exists a primitive polynomial of degree 8 over $\mathbb{F}_q$ with the coefficient of x^4 prescribed as a.*

After Lemma 7.3.7 we can assume $\omega_1 \leq 7$ and $\omega_2 \leq 4$ and start the sieving process. It turns out, however, that one sieving step is enough. Taking $k_0 = 3 \cdot 5$ yields $s \leq 9$, $\delta \geq 0.285$ and $\Delta_{s,\delta} < 18,50$ whence (7.12) is satisfied for $q \geq 12$. Next, putting $k_0 = 3$, $q = 8$ satisfies (7.12), but the appropriate primitive polynomials over fields $\mathbb{F}_4$ and $\mathbb{F}_2$ have to be found explicitly.

a	$q = 2$	$q = 4$
1	$x^8 + x^5 + x^3 + x^2 + x + 1$	$x^8 + x^5 + x^2 + x + \alpha$
α	—	$x^8 + \alpha x^5 + (\alpha + 1)x^2 + \alpha$
$\alpha + 1$	—	$x^8 + (\alpha + 1)x^5 + \alpha x^2 + \alpha$

7.3.2 The even zero problem

To fix the fourth coefficient as zero, following Lemma 7.3.2 we suppose $A = 0$. We may therefore assume also that $k|Q_n$. Suppose $1 < d|Q_n$ and take $n = 8$. A sufficient condition is then

$$q^2 > 4\sqrt{2}\, W(k_0)\Delta_{s,\delta}. \tag{7.13}$$

Define K_1, K_2 as in Section 7.2 and note that both, K_1 and K_2, are odd. Denote $\omega(K_1)$ by ω_1 and $\omega(K_2)$ by ω_2.

Lemma 7.3.8. *Suppose that $n = 8$, q odd, $\omega_1 \geq 10$ or $\omega_2 \geq 8$. Then there exists a primitive polynomial of degree 8 over $\mathbb{F}_q$ with the coefficient of x^4 prescribed as 0.*

Consequently to Lemma 7.3.8, assume $\omega_1 \leq 9$ and $\omega_2 \leq 7$ and begin the sieve. Taking k_0 to be the product of least three primes in K_1 yields $s \leq 13$, $\delta > 0.450$, $\Delta_{s,\delta} < 28,67$ and condition (7.13) holds for $q \geq 37$. Hence assume $\omega_1 \leq 5$, $\omega_2 \leq 3$ and set $k_0 = 3$. Then $s \leq 7$, $\delta > 0.392$, $\Delta_{s,\delta} < 17,31$ and condition (7.13) holds for $q \geq 14$. For the three remaining values of q, primitive polynomials in $\mathbb{F}_8[x]$, $\mathbb{F}_4[x]$ and $\mathbb{F}_2[x]$ have to be explicitly found. The field $\mathbb{F}_4$ is defined as $\mathbb{F}_2(\alpha)$ and $\mathbb{F}_8$ is defined as $\mathbb{F}_2(\alpha)$, where α is the root of $x^2 + x + 1 \in \mathbb{F}_2$ and $x^3 + x^2 + 1 \in \mathbb{F}_2$, respectively.

q	$f(x)$
2	$x^8 + x^7 + x^2 + x + 1$
4	$x^8 + x^7 + x^2 + x + \alpha$
8	$x^8 + (\alpha^2 + \alpha)x^6 + (\alpha^2 + \alpha + 1)x^4 + (\alpha^2 + \alpha)x^3 + \alpha^2 x^2 + \alpha x + \alpha$

This concludes this chapter and completes the proof of the Hansen-Mullen primitivity conjecture.

Chapter 8

Conclusions and further research

In the preceding chapters, we have proved the most delicate, previously unestablished cases of the Hansen-Mullen primitivity conjecture by developing efficient methods involving the use of character sums and sieving techniques. By extending these methods we have additionally provided a self-contained proof for some of the previously established cases of HMPC; due to the quality of our results, only little computation was required.

We believe similar powerful methods, perhaps involving Kloosterman and other types of character sums, can be developed to prove existence of primitive polynomials with prescribed several coefficients. A conjecture that a primitive polynomial in $\mathbb{F}_q[x]$ of any degree n, with first m_1 and last m_2 coefficients arbitrarily prescribed exists for any choice of q (with some natural exceptions), seems feasible to prove for $m_1 + m_2 < \frac{n}{2}$.

Appendix A

Bounds for the number of square-free divisors

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

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

$$W(h) < h^{\frac{3}{7}}, \quad \text{when } r = 6; \tag{A.1}$$

$$W(h) < h^{\frac{1}{3}}, \quad \text{when } r = 9; \tag{A.2}$$

$$W(h) < h^{\frac{2}{7}}, \quad \text{when } r = 12; \tag{A.3}$$

$$W(h) < h^{\frac{3}{11}}, \quad \text{when } r = 13; \tag{A.4}$$

$$W(h) < h^{\frac{13}{50}}, \quad \text{when } r = 15; \tag{A.5}$$

$$W(h) < (h-1)^{\frac{1}{5}}, \quad \text{when } r = 28. \tag{A.6}$$

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

$$W(h) < h^{\frac{1}{2}}, \quad \text{when } r = 3; \tag{A.7}$$

$$W(h) < (h-1)^{\frac{2}{5}}, \quad \text{when } r = 5; \tag{A.8}$$

$$W(h) < h^{\frac{3}{10}}, \quad \text{when } r = 8; \tag{A.9}$$

$$W(h) < (h-1)^{\frac{5}{18}}, \quad \text{when } r = 10; \tag{A.10}$$

$$W(h) < h^{\frac{3}{13}}, \quad \text{when } r = 16. \tag{A.11}$$

Let the integer h be such that $h \not\equiv 0 \pmod 3$ and $\omega(h) \geq r$. Then the following

statements hold:

$$W(h) < h^{\frac{3}{10}}, \quad \text{when } r = 9; \tag{A.12}$$

$$W(h) < (h-1)^{\frac{7}{25}}, \quad \text{when } r = 10; \tag{A.13}$$

$$W(h) < h^{\frac{7}{26}}, \quad \text{when } r = 11. \tag{A.14}$$

Furthermore, for an odd integer h, $h \not\equiv 0 \pmod 3$ with $\omega(h) \geq 11$,

$$W(h) < h^{\frac{1}{4}}. \tag{A.15}$$

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

$$W(h) < (h^{\frac{1}{2}} - 1)^{\frac{1}{2}}, \quad \text{when } r = 2; \tag{A.16}$$

$$W(h) < h^{\frac{1}{5}}, \quad \text{when } r = 11; \tag{A.17}$$

$$W(h) < (h-1)^{\frac{7}{50}}, \quad \text{when } r = 40. \tag{A.18}$$

Furthermore, for an odd integer h, a product of primes $l \equiv 1 \pmod 4$ with $\omega(h) \geq 6$,

$$W(h) < (h-1)^{\frac{1}{4}}. \tag{A.19}$$

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

$$W(h) < h^{\frac{3}{16}}, \quad \text{when } r = 12; \tag{A.20}$$

$$W(h) < h^{\frac{9}{50}}, \quad \text{when } r = 15; \tag{A.21}$$

$$W(h) < h^{\frac{4}{25}}, \quad \text{when } r = 23; \tag{A.22}$$

$$W(h) < (h-1)^{\frac{10}{63}}, \quad \text{when } r = 24; \tag{A.23}$$

$$W(h) < (h-1)^{\frac{5}{32}}, \quad \text{when } r = 25. \tag{A.24}$$

Suppose that the integer h is product of primes $l \equiv 1 \pmod{10}$ and $\omega(h) \geq r$. Then

the statements below holds:

$$W(h) < (h^{\frac{1}{2}} - 1)^{\frac{1}{2}}, \quad \text{when } r = 2; \tag{A.25}$$

$$W(h) < h^{\frac{1}{6}}, \quad \text{when } r = 10; \tag{A.26}$$

$$W(h) < (h^{\frac{1}{2}} - 1)^{\frac{23}{80}}, \quad \text{when } r = 17; \tag{A.27}$$

$$W(h) < h^{\frac{3}{22}}, \quad \text{when } r = 22; \tag{A.28}$$

$$W(h) < h^{\frac{13}{99}}, \quad \text{when } r = 26. \tag{A.29}$$

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

$$W(h) < (h^{\frac{1}{2}} - 1)^{\frac{1}{2}}. \tag{A.30}$$

Suppose that the integer h is product of primes $l \equiv 1 \pmod{14}$ and $\omega(h) \geq r$. Then

$$W(h) < (h-1)^{\frac{1}{6}}, \quad \text{when } r = 6; \tag{A.31}$$

$$W(h) < h^{\frac{13}{100}}, \quad \text{when } r = 16; \tag{A.32}$$

$$W(h) < h^{\frac{1}{8}}, \quad \text{when } r = 20. \tag{A.33}$$

Suppose that the integer h is product of primes $l \equiv 1 \pmod{8}$ and $\omega(h) \geq r$. Then

$$W(h) < (h-1)^{\frac{17}{100}}, \quad \text{when } r = 6; \tag{A.34}$$

$$W(h) < (h-1)^{\frac{1}{6}}, \quad \text{when } r = 7; \tag{A.35}$$

$$W(h) < (h-1)^{\frac{2}{13}}, \quad \text{when } r = 10; \tag{A.36}$$

$$W(h) < (h-1)^{\frac{2}{13}}, \quad \text{when } r = 13. \tag{A.37}$$

Appendix B

Tables of primitive polynomials

In Chapters 5 - 7, we were sometimes not able to theoretically prove existence of a primitive polynomial over a finite field $\mathbb{F}_q$. This occured for highly composite q^n-1 with many small prime factors. We should point out that, because of the quality of the results, the amount of computation needed is very little. The vast majority of cases where the primitive polynomial had to be found explicitly, arised when prescribing the second coefficient of a polynomial of degree 4. In the other cases, only a handful of polynomials, if any, required direct verification.

The computation was carried out with Maple, a mathematics software package. The programs were carefully written to minimize the computing time. For prime fields, the results were virtually instantaneous and only composite fields posed a stiffer task. While, even for small values of q, there often exist several polynomials of the desired form, we here only give one as this suffices as a proof of existence.

B.1 Primitive polynomials with m-th coefficient prescribed

We first provide the list of relevant primitive polynomials with prescribed only the m-th coefficient over a finite field $\mathbb{F}_q$ (polynomials with additionally prescribed constant term are listed in the following section). For composite q, the fields were defined as follows:

$\mathbb{F}_4$ is defined as $\mathbb{F}_2(\alpha)$ with α a root of the polynomial $x^2+x+1 \in \mathbb{F}_2[x]$,

$\mathbb{F}_8$ is defined as $\mathbb{F}_2(\alpha)$ with α a root of the polynomial $x^3+x^2+1 \in \mathbb{F}_2[x]$,

$\mathbb{F}_9$ is defined as $\mathbb{F}_3(\alpha)$ with α a root of the polynomial $x^2+x+2 \in \mathbb{F}_3[x]$,

$\mathbb{F}_{16}$ is defined as $\mathbb{F}_2(\alpha)$ with α a root of the polynomial $x^4+x^3+1 \in \mathbb{F}_2[x]$,

$\mathbb{F}_{25}$ is defined as $\mathbb{F}_5(\alpha)$ with α a root of the polynomial $x^2 + x + 2 \in \mathbb{F}_5[x]$ and $\mathbb{F}_{27}$ is defined as $\mathbb{F}_3(\alpha)$ with α a root of the polynomial $x^3 + 2x + 1 \in \mathbb{F}_3[x]$.

The polynomials are ordered by the size of q (and m, where applicable), starting with the largest value, 11003.

q = 11003, $m = 2$, $a = 0$: $f(x) = x^4 + x + 23$;
q = 7853, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 7727, $m = 2$, $a = 0$: $f(x) = x^4 + x + 35$;
q = 6323, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 6269, $m = 2$, $a = 0$: $f(x) = x^4 + x + 39$;
q = 6089, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$
q = 5813, $m = 2$, $a = 0$: $f(x) = x^4 + x + 42$;
q = 5147, $m = 2$, $a = 0$: $f(x) = x^4 + x + 34$
q = 5039, $m = 2$, $a = 0$: $f(x) = x^4 + x + 39$;
q = 4493, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$
q = 4283, $m = 2$, $a = 0$: $f(x) = x^4 + x + 8$;
q = 4217, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$
q = 4157, $m = 2$, $a = 0$: $f(x) = x^4 + x + 29$;
q = 4073, $m = 2$, $a = 0$: $f(x) = x^4 + x + 27$
q = 3947, $m = 2$, $a = 0$: $f(x) = x^4 + x + 50$;
q = 3863, $m = 2$, $a = 0$: $f(x) = x^4 + x + 15$
q = 3617, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 3557, $m = 2$, $a = 0$: $f(x) = x^4 + x + 31$
q = 3359, $m = 2$, $a = 0$: $f(x) = x^4 + x + 37$;
q = 3323, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 3203, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$;
q = 2969, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$
q = 2939, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 2903, $m = 2$, $a = 0$: $f(x) = x^4 + x + 20$
q = 2897, $m = 2$, $a = 0$: $f(x) = x^4 + x + 59$;
q = 2843, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 2777, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 2729, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 2699, $m = 2$, $a = 0$: $f(x) = x^4 + x + 18$;
q = 2633, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 2621, $m = 2$, $a = 0$: $f(x) = x^4 + x + 37$;
q = 2579, $m = 2$, $a = 0$: $f(x) = x^4 + x + 8$
q = 2477, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$;
q = 2423, $m = 2$, $a = 0$: $f(x) = x^4 + x + 28$
q = 2417, $m = 2$, $a = 0$: $f(x) = x^4 + x + 29$;
q = 2393, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 2339, $m = 2$, $a = 0$: $f(x) = x^4 + x + 22$;
q = 2333, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$
q = 2309, $m = 2$, $a = 0$: $f(x) = x^4 + x + 17$;
q = 2267, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$
q = 2243, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$;
q = 2213, $m = 2$, $a = 0$: $f(x) = x^4 + x + 17$
q = 2207, $m = 2$, $a = 0$: $f(x) = x^4 + x + 53$;
q = 2153, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$
q = 2141, $m = 2$, $a = 0$: $f(x) = x^4 + x + 11$;
q = 2129, $m = 2$, $a = 0$: $f(x) = x^4 + x + 27$
q = 2099, $m = 2$, $a = 0$: $f(x) = x^4 + x + 57$;
q = 2087, $m = 2$, $a = 0$: $f(x) = x^4 + x + 14$
q = 2069, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$;
q = 2063, $m = 2$, $a = 0$: $f(x) = x^4 + x + 41$
q = 2039, $m = 2$, $a = 0$: $f(x) = x^4 + x + 28$;
q = 2027, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$
q = 1997, $m = 2$, $a = 0$: $f(x) = x^4 + x + 11$;
q = 1979, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$
q = 1973, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$;
q = 1931, $m = 2$, $a = 0$: $f(x) = x^4 + x + 8$
q = 1913, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 1889, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$

q = 1877, $m = 2$, $a = 0$: $f(x) = x^4 + x + 11$;
q = 1847, $m = 2$, $a = 0$: $f(x) = x^4 + x + 20$
q = 1823, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$;
q = 1787, $m = 2$, $a = 0$: $f(x) = x^4 + x + 19$
q = 1747, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$;
q = 1733, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$
q = 1721, $m = 2$, $a = 0$: $f(x) = x^4 + x + 24$;
q = 1697, $m = 2$, $a = 0$: $f(x) = x^4 + x + 20$
q = 1637, $m = 2$, $a = 0$: $f(x) = x^4 + x + 30$;
q = 1613, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 1607, $m = 2$, $a = 0$: $f(x) = x^4 + x + 29$;
q = 1583, $m = 2$, $a = 0$: $f(x) = x^4 + x + 47$
q = 1559, $m = 2$, $a = 0$: $f(x) = x^4 + x + 103$;
q = 1553, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$
q = 1523, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 1493, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$
q = 1487, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$;
q = 1481, $m = 2$, $a = 0$: $f(x) = x^4 + x + 55$
q = 1433, $m = 2$, $a = 0$: $f(x) = x^4 + x + 47$;
q = 1427, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$
q = 1409, $m = 2$, $a = 0$: $f(x) = x^4 + x + 52$;
q = 1373, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 1367, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 1319, $m = 2$, $a = 0$: $f(x) = x^4 + x + 39$
q = 1307, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$;
q = 1301, $m = 2$, $a = 0$: $f(x) = x^4 + x + 35$
q = 1289, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$;
q = 1283, $m = 2$, $a = 0$: $f(x) = x^4 + x + 45$
q = 1277, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 1259, $m = 2$, $a = 0$: $f(x) = x^4 + x + 14$
q = 1229, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$;
q = 1223, $m = 2$, $a = 0$: $f(x) = x^4 + x + 15$
q = 1217, $m = 2$, $a = 0$: $f(x) = x^4 + x + 23$;
q = 1193, $m = 2$, $a = 0$: $f(x) = x^4 + x + 40$
q = 1187, $m = 2$, $a = 0$: $f(x) = x^4 + x + 18$;
q = 1163, $m = 2$, $a = 0$: $f(x) = x^4 + x + 18$
q = 1109, $m = 2$, $a = 0$: $f(x) = x^4 + x + 22$;
q = 1103, $m = 2$, $a = 0$: $f(x) = x^4 + x + 21$
q = 1097, $m = 2$, $a = 0$: $f(x) = x^4 + x + 20$;
q = 1091, $m = 2$, $a = 0$: $f(x) = x^4 + x + 17$
q = 1061, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$;
q = 1049, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 1033, $m = 2$, $a = 0$: $f(x) = x^4 + x + 29$;
q = 1019, $m = 2$, $a = 0$: $f(x) = x^4 + x + 21$
q = 1013, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 983, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 977, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$;
q = 953, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$
q = 947, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 941, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$
q = 929, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 919, $m = 2$, $a = 0$: $f(x) = x^4 + x + 30$
q = 911, $m = 2$, $a = 0$: $f(x) = x^4 + x + 33$;
q = 887, $m = 2$, $a = 0$: $f(x) = x^4 + x + 30$
q = 863, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$;
q = 857, $m = 2$, $a = 0$: $f(x) = x^4 + x + 89$
q = 853, $m = 2$, $a = 0$: $f(x) = x^4 + x + 29$;
q = 839, $m = 2$, $a = 0$: $f(x) = x^4 + x + 66$
q = 829, $m = 2$, $a = 0$: $f(x) = x^4 + x + 82$;
q = 827, $m = 2$, $a = 0$: $f(x) = x^4 + x + 37$
q = 811, $m = 2$, $a = 0$: $f(x) = x^4 + x + 86$;
q = 809, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$
q = 797, $m = 2$, $a = 0$: $f(x) = x^4 + x + 26$;
q = 773, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 769, $m = 2$, $a = 0$: $f(x) = x^4 + x + 23$;
q = 761, $m = 2$, $a = 0$: $f(x) = x^4 + x + 31$
q = 743, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$;
q = 727, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$
q = 719, $m = 2$, $a = 0$: $f(x) = x^4 + x + 22$;
q = 701, $m = 2$, $a = 0$: $f(x) = x^4 + x + 67$
q = 683, $m = 2$, $a = 0$: $f(x) = x^4 + x + 15$;
q = 677, $m = 2$, $a = 0$: $f(x) = x^4 + x + 18$
q = 659, $m = 2$, $a = 0$: $f(x) = x^4 + x + 32$;
q = 653, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$

q = 647, $m = 2$, $a = 0$: $f(x) = x^4 + x + 33$;
q = 643, $m = 2$, $a = 0$: $f(x) = x^4 + x + 11$
q = 619, $m = 2$, $a = 0$: $f(x) = x^4 + x + 18$;
q = 617, $m = 2$, $a = 0$: $f(x) = x^4 + x + 17$
q = 599, $m = 2$, $a = 0$: $f(x) = x^4 + x + 14$;
q = 593, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$
q = 587, $m = 2$, $a = 0$: $f(x) = x^4 + x + 18$;
q = 577, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 569, $m = 2$, $a = 0$: $f(x) = x^4 + x + 22$;
q = 563, $m = 2$, $a = 0$: $f(x) = x^4 + x + 14$
q = 557, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$;
q = 523, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$
q = 531, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$;
q = 509, $m = 2$, $a = 0$: $f(x) = x^4 + x + 22$
q = 503, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 499, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 491, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$;
q = 487, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$
q = 479, $m = 2$, $a = 0$: $f(x) = x^4 + x + 39$;
q = 467, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 463, $m = 2$, $a = 0$: $f(x) = x^4 + x + 11$;
q = 461, $m = 2$, $a = 0$: $f(x) = x^4 + x + 50$
q = 449, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 443, $m = 2$, $a = 0$: $f(x) = x^4 + x + 21$
q = 439, $m = 2$, $a = 0$: $f(x) = x^4 + x + 46$;
q = 433, $m = 2$, $a = 0$: $f(x) = x^4 + x + 40$
q = 431, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$;
q = 421, $m = 2$, $a = 0$: $f(x) = x^4 + x + 14$
q = 419, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 401, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$
q = 389, $m = 2$, $a = 0$: $f(x) = x^4 + x + 31$;
q = 383, $m = 2$, $a = 0$: $f(x) = x^4 + x + 78$
q = 373, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 359, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$
q = 353, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$;
q = 349, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$
q = 347, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 337, $m = 2$, $a = 0$: $f(x) = x^4 + x + 61$
q = 317, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$;
q = 313, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$
q = 311, $m = 2$, $a = 0$: $f(x) = x^4 + x + 43$;
q = 307, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 293, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$;
q = 283, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$
q = 281, $m = 2$, $a = 0$: $f(x) = x^4 + x + 15$;
q = 277, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 269, $m = 2$, $a = 0$: $f(x) = x^4 + x + 8$;
q = 263, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 257, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$;
q = 251, $m = 2$, $a = 0$: $f(x) = x^4 + x + 14$
q = 241, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$;
q = 239, $m = 2$, $a = 0$: $f(x) = x^4 + x + 13$
q = 233, $m = 2$, $a = 0$: $f(x) = x^4 + x + 10$;
q = 229, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 227, $m = 2$, $a = 0$: $f(x) = x^4 + x + 38$;
q = 223, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$
q = 211, $m = 2$, $a = 0$: $f(x) = x^4 + x + 17$;
q = 197, $m = 2$, $a = 0$: $f(x) = x^4 + x + 18$
q = 193, $m = 2$, $a = 0$: $f(x) = x^4 + x + 19$;
q = 191, $m = 2$, $a = 0$: $f(x) = x^4 + x + 28$
q = 181, $m = 2$, $a = 0$: $f(x) = x^4 + x + 54$;
q = 179, $m = 2$, $a = 0$: $f(x) = x^4 + x + 7$
q = 173, $m = 2$, $a = 0$: $f(x) = x^4 + x + 26$;
q = 167, $m = 2$, $a = 0$: $f(x) = x^4 + x + 60$
q = 167, $m = 3$, $a = 0$: $f(x) = x^6 + 18x^2 + 5$;
q = 163, $m = 2$, $a = 0$: $f(x) = x^4 + x + 42$
q = 163, $m = 3$, $a = 0$: $f(x) = x^6 + x + 2$

q = 163, $m = 3$: the following table gives 162 primitive polynomials $f(x) \in \mathbb{F}_{163}[x]$ of the form $f(x) = x^5 + ax^2 + c$, $a \neq 0$; each polynomial is represented by a pair (a, c), except for $a = 36, 61, 64, 115, 126, 132, 136, 150$ and 158 when the polynomial is of the form $f(x) = x^5 + ax^2 + x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	14		2	15		3	14		4	4		5	16		6	9		7	10
8	9		9	15		10	15		11	15		12	10		13	43		14	15
15	35		16	4		17	9		18	24		19	10		20	4		21	9
22	16		23	24		24	4		25	10		26	47		27	26		28	10
29	4		30	9		31	9		32	39		33	10		34	35		35	14
36	33		37	15		38	81		39	9		40	15		41	83		42	14
43	4		44	24		45	9		46	4		47	43		48	14		49	14
50	14		51	9		52	10		53	4		54	4		55	9		56	16
57	35		58	24		59	10		60	10		61	4		62	16		63	9
64	14		65	35		66	4		67	9		68	16		69	14		70	46
71	39		72	9		73	9		74	26		75	9		76	4		77	10
78	14		79	14		80	9		81	9		82	35		83	9		84	10
85	39		86	39		87	4		88	14		89	15		90	43		91	9
92	4		93	10		94	15		95	10		96	24		97	14		98	9
99	10		100	4		101	4		102	4		103	9		104	4		105	4
106	16		107	26		108	15		109	4		110	15		111	26		112	4
113	10		114	9		115	4		116	9		117	24		118	4		119	9
120	14		121	9		122	4		123	4		124	24		125	4		126	10
127	24		128	14		129	43		130	4		131	24		132	10		133	43
134	16		135	46		136	26		137	15		138	4		139	14		140	14
141	26		142	16		143	10		144	4		145	4		146	35		147	4
148	9		149	4		150	56		151	10		152	24		153	4		154	15
155	26		156	14		157	10		158	33		159	10		160	10		161	14
162	15																		

q = 157, $m = 2$, $a = 0$: $f(x) = x^4 + x + 15$;
q = 151, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 149, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$;
q = 139, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$;
q = 137, $m = 2$, $a = 0$: $f(x) = x^4 + x + 26$;
q = 131, $m = 2$, $a = 0$: $f(x) = x^4 + x + 6$;
q = 127, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$;
q = 113, $m = 2$, $a = 0$: $f(x) = x^4 + x + 5$;
q = 109, $m = 2$, $a = 0$: $f(x) = x^4 + x + 30$;

q = 157, $m = 3$, $a = 0$: $f(x) = x^6 + 2x^2 + x + 5$
q = 151, $m = 3$, $a = 0$: $f(x) = x^6 + x + 6$
q = 149, $m = 3$, $a = 0$: $f(x) = x^6 + 13x^2 + x + 2$
q = 139, $m = 3$, $a = 0$: $f(x) = x^6 + x^2 + x + 2$
q = 137, $m = 3$, $a = 0$: $f(x) = x^6 + 12x^2 + x + 3$
q = 131, $m = 3$, $a = 0$: $f(x) = x^6 + 6x^2 + x + 2$
q = 127, $m = 3$, $a = 0$: $f(x) = x^6 + x^2 + x + 3$
q = 113, $m = 3$, $a = 0$: $f(x) = x^6 + x^2 + x + 3$
q = 109, $m = 3$, $a = 0$: $f(x) = x^6 + 5x^2 + x + 6$

q = 109, $m = 3$: the following table gives 108 primitive polynomials $f(x) \in \mathbb{F}_{109}[x]$ of the form $f(x) = x^5 + ax^2 + c$, $a \neq 0$; each polynomial is represented by a pair (a, c), except for $a = 15, 21, 36, 73, 88$ and 94 when the polynomial is of the form $f(x) = x^5 + ax^2 + x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	62		2	6		3	6		4	24		5	10		6	18		7	6
8	11		9	67		10	10		11	11		12	11		13	6		14	6
15	52		16	18		17	10		18	13		19	10		20	10		21	10
22	11		23	53		24	13		25	13		26	6		27	24		28	6
29	6		30	6		31	18		32	6		33	18		34	13		35	24
36	42		37	10		38	6		39	62		40	13		41	11		42	11
43	11		44	13		45	11		46	30		47	24		48	10		49	57
50	30		51	30		52	11		53	10		54	10		55	24		56	10
57	11		58	30		59	67		60	6		61	11		62	6		63	67
64	50		65	6		66	13		67	13		68	50		69	13		70	18
71	57		72	18		73	50		74	10		75	53		76	30		77	57
78	62		79	18		80	6		81	18		82	10		83	10		84	53
85	13		86	13		87	50		88	24		89	6		90	24		91	10
92	6		93	6		94	40		95	6		96	6		97	6		98	50
99	10		100	30		101	50		102	11		103	18		104	11		105	10
106	13		107	53		108	18												

q = 107, $m = 2$, $a = 0$: $f(x) = x^4 + x + 2$; **q = 107**, $m = 3$, $a = 0$: $f(x) = x^6 + 7x^2 + x + 2$

q = 103, $m = 2$: the following table gives 103 primitive polynomials $f(x) \in \mathbb{F}_{103}[x]$ of the form $f(x) = x^4 + ax^2 + x + c$; each polynomial is represented by a pair (a, c) .

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	21		2	12		3	51		4	40		5	12		6	75		7	12		8	43
9	5		10	5		11	5		12	11		13	43		14	20		15	5		16	43
17	5		18	12		19	5		20	20		21	40		22	5		23	48		24	40
25	12		26	6		27	51		28	11		29	44		30	12		31	6		32	35
33	51		34	21		35	5		36	21		37	6		38	6		39	11		40	6
41	5		42	12		43	12		44	20		45	96		46	5		47	45		48	20
49	5		50	12		51	20		52	12		53	6		54	12		55	11		56	5
57	53		58	6		59	12		60	35		61	6		62	6		63	54		64	44
65	5		66	6		67	21		68	11		69	20		70	20		71	40		72	6
73	5		74	45		75	11		76	5		77	12		78	35		79	48		80	43
81	21		82	35		83	51		84	70		85	5		86	5		87	40		88	35
89	5		90	5		91	11		92	6		93	62		94	6		95	21		96	6
97	43		98	35		99	5		100	11		101	35		102	11		0	5			

q = 103, $m = 3$, $a = 0$: $f(x) = x^6 + x + 5$;
q = 101, $m = 3$, $a = 0$: $f(x) = x^6 + 6x^5 + 2$;
q = 97, $m = 3$, $a = 0$: $f(x) = x^6 + 10x^5 + 5$;
q = 101, $m = 2$, $a = 0$: $f(x) = x^4 + x + 12$
q = 97, $m = 2$, $a = 0$: $f(x) = x^4 + x + 23$
q = 89, $m = 3$, $a = 0$: $f(x) = x^6 + 6x^5 + 3$

q = 89, $m = 2$: the following table contains 89 polynomials $f(x) \in \mathbb{F}_{89}[x]$; each pair (a, c) represents a polynomial of the form $f(x) = x^4 + ax^2 + x + c$, except for $a = 64$ when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	7		2	7		3	6		4	14		5	6		6	43		7	15		8	19
9	6		10	19		11	43		12	7		13	26		14	14		15	14		16	15
17	35		18	29		19	3		20	13		21	26		22	23		23	15		24	6
25	7		26	19		27	23		28	24		29	13		30	5		31	6		32	3
33	24		34	48		35	23		36	14		37	14		38	6		39	3		40	19
41	23		42	29		43	3		44	7		45	26		46	61		47	3		48	7
49	7		50	59		51	14		52	7		53	30		54	23		55	25		56	13
57	23		58	6		59	19		60	38		61	3		62	28		63	14		64	3
65	26		66	30		67	13		68	7		69	29		70	3		71	48		72	6
73	24		74	70		75	13		76	15		77	15		78	54		79	13		80	23
81	24		82	15		83	31		84	27		85	3		86	13		87	15		88	3
0	27																					

q = 83, $m = 2$: the table below gives a pair (a, c) for each polynomial $f(x) = x^4 + ax^2 + x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
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		0	22															

q = 83, $m = 3$, $a = 0$: $f(x) = x^6 + 8x^2 + x + 2$

q = 79, $m = 2$, $a = 0$: $f(x) = x^4 + x + 3$

q = 79, $m = 3$, $a = 0$: $f(x) = x^6 + 4x^2 + x + 3$

q = 73, $m = 3$, $a = 0$: $f(x) = x^6 + x + 5$

q = 73, $m = 2$: the following table gives a pair (a, c) for each polynomial of the form $f(x) = x^4 + ax^2 + x + c$, except for $a = 5, 28, 40$ when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	15		2	34		3	44		4	13		5	15		6	11		7	15		8	11
9	15		10	14		11	14		12	5		13	14		14	20		15	20		16	45
17	5		18	5		19	5		20	11		21	29		22	14		23	5		24	34
25	40		26	5		27	14		28	5		29	13		30	13		31	5		32	5
33	29		34	15		35	33		36	14		37	11		38	28		39	15		40	11
41	5		42	5		43	5		44	11		45	13		46	59		47	33		48	40
49	34		50	26		51	39		52	20		53	5		54	5		55	33		56	11
57	13		58	14		59	28		60	14		61	44		62	13		63	11		64	5
65	34		66	11		67	28		68	13		69	11		70	20		71	28		72	11
0	13																					

q = 71, $m = 2$: we give a pair (a, c) for each polynomial $f(x) = x^4 + ax^2 + x + c$, except for $a = 55$ when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	7		2	61		3	11		4	21		5	22		6	22		7	21		8	7
9	13		10	74		11	55		12	22		13	7		14	22		15	11		16	7
17	11		18	11		19	22		20	7		21	47		22	31		23	28		24	11
25	31		26	11		27	13		28	7		29	33		30	42		31	22		32	33
33	52		34	7		35	7		36	11		37	69		38	56		39	11		40	7
41	22		42	22		43	7		44	7		45	7		46	7		47	21		48	13
49	11		50	44		51	44		52	7		53	47		54	13		55	28		56	11
57	33		58	28		59	21		60	22		61	53		62	11		63	13		64	13
65	11		66	7		67	13		68	22		69	42		70	31		0	11			

q = 71, $m = 3$, $a = 0$: $f(x) = x^6 + 2x^2 + x + 7$

q = 67, $m = 3$, $a = 0$: $f(x) = x^6 + 2x^2 + x + 2$

q = 67, $m = 2$: the following table contains a pair (a, c) for each polynomial $f(x) = x^4+ax^2+x+c$, except for $a = 26$ when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	28		2	7		3	12		4	32		5	2		6	31		7	2		8	34
9	12		10	18		11	2		12	11		13	31		14	20		15	11		16	7
17	13		18	18		19	7		20	11		21	11		22	13		23	46		24	11
25	50		26	12		27	11		28	12		29	2		30	28		31	13		32	2
33	2		34	28		35	12		36	12		37	7		38	7		39	18		40	11
41	1		42	20		43	51		44	13		45	12		46	11		47	7		48	2
49	32		50	11		51	7		52	7		53	41		54	63		55	18		56	2
57	7		58	12		59	13		60	20		61	12		62	18		63	20		64	2
65	11		66	2		0	2															

q = 67, $m = 3$: the following table contains a pair (a, c) for each polynomial $f(x) = x^5 + ax^2 + c$, $a \neq 0$, except for $a = 20$ and 48 when the polynomial is of the form $f(x) = x^5 + ax^2 + x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	17		2	6		3	6		4	4		5	4		6	4		7	19		8	4
9	6		10	17		11	16		12	6		13	16		14	4		15	4		16	54
17	17		18	10		19	6		20	10		21	4		22	6		23	6		24	4
25	16		26	17		27	6		28	36		29	10		30	17		31	23		32	4
33	6		34	36		35	6		36	19		37	10		38	60		39	4		40	10
41	10		42	6		43	10		44	54		45	4		46	17		47	10		48	6
49	16		50	4		51	60		52	19		53	16		54	36		55	60		56	17
57	19		58	19		59	4		60	16		61	23		62	17		63	54		64	6
65	23		66	19																		

q = 61, $m = 2$: each pair (a, c) in the following table represents a polynomial $f(x) = x^4 + ax^2 + x + c$, except when $a = 41$ and the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	6		2	6		3	2		4	10		5	7		6	54		7	6		8	2
9	10		10	26		11	2		12	6		13	7		14	44		15	6		16	2
17	10		18	7		19	17		20	6		21	6		22	26		23	31		24	6
25	10		26	6		27	2		28	18		29	2		30	17		31	10		32	10
33	17		34	6		35	31		36	2		37	18		38	31		39	2		40	43
41	10		42	2		43	2		44	7		45	10		46	2		47	2		48	35
49	2		50	2		51	31		52	30		53	30		54	2		55	30		56	7
57	18		58	43		59	35		60	10		0	2									

q = 61, $m = 3$: each pair (a, c) in the following table represents a polynomial $f(x) = x^5 + ax^2 + c$, except when $a = 8, 11, 23, 24, 28, 33, 37, 38, 50$ and 53 and the polynomial is of the form $f(x) = x^5 + ax^2 + x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	6		2	2		3	31		4	18		5	2		6	2		7	2		8	10
9	6		10	44		11	2		12	10		13	10		14	18		15	10		16	10
17	44		18	2		19	18		20	6		21	2		22	10		23	6		24	54
25	10		26	6		27	31		28	10		29	44		30	6		31	44		32	6
33	44		34	6		35	44		36	18		37	7		38	31		39	2		40	2
41	31		42	10		43	2		44	6		45	2		46	2		47	10		48	2
49	18		50	7		51	6		52	31		53	51		54	2		55	2		56	10
57	10		58	6		59	2		60	31												

q = 61, $m = 3$, $a = 0$: $f(x) = x^6 + 2x^2 + x + 2$

q = 59, $m = 3$, $a = 0$: $f(x) = x^6 + 3x^2 + x + 2$

q = 59, $m = 2$: the table below gives a pair (a, c) for each polynomial $f(x) = x^4 + ax^2 + x + c$, except when $a = 33$ or 42 and the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	2		2	6		3	10		4	24		5	13		6	14		7	6		8	2
9	8		10	14		11	14		12	18		13	14		14	50		15	11		16	6
17	8		18	18		19	47		20	2		21	10		22	39		23	2		24	11
25	8		26	37		27	2		28	2		29	34		30	32		31	32		32	8
33	18		34	6		35	8		36	40		37	8		38	31		39	10		40	8
41	32		42	13		43	2		44	18		45	6		46	8		47	11		48	8
49	11		50	30		51	32		52	6		53	8		54	13		55	13		56	6
57	24		58	10		0	14															

q = 53, $m = 2$: the table below contains 53 pairs (a, c), one for each polynomial $f(x) = x^4 + ax^2 + x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	2		2	3		3	35		4	48		5	20		6	2		7	3		8	27
9	5		10	20		11	3		12	12		13	2		14	41		15	5		16	5
17	50		18	2		19	5		20	20		21	31		22	8		23	22		24	3
25	5		26	14		27	2		28	18		29	8		30	33		31	12		32	3
33	12		34	31		35	26		36	18		37	34		38	3		39	3		40	3
41	22		42	27		43	2		44	21		45	33		46	48		47	19		48	33
49	31		50	5		51	8		52	8		0	18									

q = 53, $m = 3$, $a = 0$: $f(x) = x^6 + 6x^2 + x + 2$

q = 47, $m = 3$, $a = 0$: $f(x) = x^6 + x + 5$

q = 47, $m = 2$: each pair (a, c) in the following table represents a polynomial $f(x) = x^4 + ax^2 + x + c$, except for $a = 7, 10$ when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	30		2	23		3	15		4	30		5	10		6	26		7	10		8	40
9	15		10	29		11	10		12	40		13	33		14	30		15	10		16	5
17	35		18	5		19	15		20	23		21	33		22	13		23	10		24	20
25	10		26	39		27	22		28	29		29	5		30	31		31	30		32	22
33	20		34	10		35	20		36	33		37	5		38	11		39	10		40	20
41	5		42	19		43	40		44	15		45	5		46	10		0	39			

q = 43, $m = 2$: again, we give a pair (a, c) for each polynomial $f(x) = x^4 + ax^2 + x + c$, with the exception when $a = 10, 23, 25, 27$ or 30 and the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	5		2	3		3	3		4	3		5	3		6	19		7	28		8	18
9	28		10	3		11	19		12	19		13	3		14	18		15	5		16	19
17	28		18	20		19	20		20	12		21	30		22	12		23	20		24	3
25	5		26	5		27	20		28	26		29	18		30	29		31	3		32	5
33	30		34	19		35	3		36	12		37	20		38	18		39	5		40	5
41	3		42	19		0	20															

q = 43, $m = 3$: each pair (a, c) represents a polynomial of the form $f(x) = x^5 + ax^2 + c$, with the exception when $a = 6, 10, 24, 31, 32, 38$ or 40 and the polynomial is of the form $f(x) = x^5 + ax^2 + x + c$ or $a = 23$ and the polynomial is of the form $f(x) = x^5 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	10		2	9		3	13		4	9		5	9		6	14		7	10		8	25
9	10		10	9		11	9		12	10		13	13		14	15		15	13		16	14
17	10		18	10		19	14		20	9		21	15		22	10		23	9		24	9
25	9		26	13		27	13		28	9		29	9		30	15		31	23		32	23
33	14		34	13		35	10		36	9		37	25		38	13		39	15		40	13
41	13		42	14																		

q = 43, $m = 3$, $a = 0$: $f(x) = x^6 + 14x^2 + x + 3$

q = 41, $m = 3$, $a = 0$: $f(x) = x^6 + 9x^2 + x + 6$

q = 41, $m = 2$: every pair (a, c) in the following table stands for a polynomial $f(x) = x^4 + ax^2 + x + c$, except for $a = 5, 30$ and 40, when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	22		2	6		3	30		4	19		5	26		6	15		7	7		8	6
9	7		10	15		11	12		12	12		13	7		14	7		15	6		16	19
17	28		18	22		19	7		20	7		21	22		22	22		23	26		24	11
25	29		26	7		27	19		28	17		29	11		30	13		31	11		32	13
33	19		34	29		35	28		36	12		37	19		38	12		39	11		40	15
0	17																					

q = 37, $m = 2$: every pair (a, c) below represents a polynomial of the form $f(x) = x^4 + ax^2 + x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	5		2	5		3	5		4	2		5	2		6	15		7	2		8	2
9	13		10	19		11	5		12	19		13	15		14	22		15	13		16	5
17	5		18	2		19	2		20	19		21	5		22	19		23	20		24	20
25	2		26	13		27	5		28	13		29	17		30	13		31	35		32	15
33	5		34	13		35	13		36	13		0	2									

q = 37, $m = 3$: each pair (a, c) represents a polynomial of the form $f(x) = x^5 + ax^2 + x + c$, with the exception when $a = 9$ or 28 and the polynomial is of the form $f(x) = x^5 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	18		2	5		3	5		4	17		5	18		6	19		7	15		8	19
9	19		10	13		11	19		12	5		13	15		14	20		15	2		16	35
17	17		18	24		19	13		20	17		21	2		22	15		23	17		24	2
25	5		26	18		27	22		28	2		29	15		30	20		31	2		32	15
33	17		34	32		35	2		36	2												

q = 37, $m = 3$: each pair (a, c) represents a polynomial of the form $f(x) = x^6 + ax^3 + 10x + c$, except for $a = 4, 6, 8, 15, 20, 26$ and 27 when the polynomial is of the form $f(x) = x^6 + ax^3 + 11x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	2		2	15		3	15		4	19		5	19		6	2		7	5		8	5
9	15		10	5		11	19		12	20		13	35		14	15		15	24		16	13
17	15		18	35		19	24		20	15		21	2		22	24		23	13		24	17
25	2		26	19		27	5		28	17		29	5		30	32		31	2		32	13
33	19		34	20		35	32		36	2		0	20									

p = 31, $m = 2$: we give a pair (a, c) for each polynomial $f(x) = x^4 + ax^2 + x + c$, except for $a = 0, 2, 8, 9$ and 14 when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	21		2	24		3	3		4	3		5	3		6	3		7	13		8	12
9	3		10	17		11	11		12	3		13	17		14	3		15	13		16	17
17	24		18	12		19	22		20	3		21	13		22	11		23	3		24	17
25	12		26	12		27	11		28	12		29	3		30	3		0	17			

p = 31, $m = 3$: each pair (a, c) represents a polynomial of the form $f(x) = x^5 + ax^2 + x + c$, with the exception of $a = 7, 9, 16, 20$ and 22 when the polynomial is of the form $f(x) = x^5 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	14		2	9		3	7		4	19		5	9		6	18		7	9		8	14
9	7		10	7		11	9		12	28		13	10		14	14		15	9		16	19
17	14		18	7		19	7		20	9		21	9		22	9		23	14		24	7
25	9		26	18		27	9		28	20		29	7		30	10						

q = 31, $m = 3$, $a = 0$: $f(x) = x^6 + 2x^2 + x + 3$

q = 29, $m = 3$, $a = 0$: $f(x) = x^6 + 2x^2 + x + 2$

q = 29, $m = 2$: each pair (a, c) in the following table represents a polynomial $f(x) = x^4 + ax^2 + x + c$, except when $a = 2, 10$ or 1 and the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	3		2	19		3	10		4	18		5	2		6	27		7	8		8	15
9	11		10	10		11	21		12	2		13	18		14	8		15	21		16	2
17	2		18	8		19	2		20	15		21	2		22	15		23	14		24	10
25	11		26	10		27	11		28	2		0	19									

q = 27, $m = 3$, $a = 0$: $f(x) = x^6 + x + \alpha$

q = 27, $m = 2$: each pair (a, c) in the following table represents a polynomial $f(x) = x^4 + ax^2 + x + c$, except for $a = 1$ and the polynomial is of the form $f(x) = x^4 + ax^2 + (\alpha^2 + 2\alpha + 2)x + c$.

a	c		a	c		a	c
1	$\alpha^2 + \alpha + 2$		$\alpha^2 + 1$	$2\alpha^2 + 2\alpha + 2$		$\alpha^2 + \alpha + 1$	$\alpha + 1$
2	$2\alpha^2 + \alpha + 2$		$\alpha^2 + 2$	$2\alpha^2 + \alpha + 2$		$\alpha^2 + \alpha + 2$	$2\alpha^2 + \alpha + 2$
α	$\alpha^2 + \alpha + 2$		$\alpha^2 + \alpha$	$\alpha^2 + 2\alpha + 2$		$\alpha^2 + 2\alpha + 1$	α
$\alpha + 1$	$2\alpha^2 + \alpha + 2$		$\alpha^2 + 2\alpha$	$2\alpha^2 + 2\alpha + 2$		$\alpha^2 + 2\alpha + 2$	$2\alpha^2$
$\alpha + 2$	$\alpha^2 + 2\alpha + 2$		$2\alpha^2$	$\alpha^2 + 2\alpha + 2$		$2\alpha^2 + \alpha + 1$	$2\alpha^2 + 2\alpha + 2$
2α	$\alpha^2 + 2\alpha + 2$		$2\alpha^2 + 1$	$2\alpha^2 + \alpha + 2$		$2\alpha^2 + \alpha + 2$	$2\alpha^2 + \alpha + 2$
$2\alpha + 1$	$\alpha + 1$		$2\alpha^2 + 2$	$2\alpha^2 + \alpha + 2$		$2\alpha^2 + 2\alpha + 1$	$2\alpha^2$
$2\alpha + 2$	α		$2\alpha^2 + \alpha$	$\alpha^2 + 2\alpha + 2$		$2\alpha^2 + 2\alpha + 2$	$2\alpha^2 + 2\alpha + 2$
α^2	$\alpha^2 + 2\alpha + 2$		$2\alpha^2 + 2\alpha$	$\alpha^2 + \alpha + 2$		0	α

q = 25, $m = 2$: the table below gives a pair (a, c) for a polynomial of the form $f(x) = x^4 + ax^2 + x + c$, except when $a = \alpha + 4$ or $4\alpha + 3$ and the polynomial has the form $x^4 + x^3 + ax^2 + c$.

a	c		a	c		a	c		a	c		a	c
1	α		$\alpha + 1$	$2\alpha + 2$		$2\alpha + 1$	$3\alpha + 3$		$3\alpha + 1$	α		$4\alpha + 1$	$3\alpha + 3$
2	$3\alpha + 3$		$\alpha + 2$	2α		$2\alpha + 2$	α		$3\alpha + 2$	2α		$4\alpha + 2$	α
3	$2\alpha + 4$		$\alpha + 3$	$4\alpha + 4$		$2\alpha + 3$	$4\alpha + 4$		$3\alpha + 3$	$4\alpha + 4$		$4\alpha + 3$	$\alpha + 4$
4	$2\alpha + 2$		$\alpha + 4$	$2\alpha + 3$		$2\alpha + 4$	$3\alpha + 3$		$3\alpha + 4$	2α		$4\alpha + 4$	$4\alpha + 4$
α	α		2α	α		3α	$4\alpha + 4$		4α	3α		0	$4\alpha + 1$

q = 23, $m = 2$: each pair (a, c) in the following table represents a polynomial $f(x) = x^4 + ax^2 + x + c$, except for $a = 1, 12, 15, 16$ when the polynomial is of the form $f(x) = x^4 + ax^2 + 2x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	11		2	5		3	15		4	7		5	11		6	7		7	7		8	10
9	21		10	20		11	5		12	7		13	17		14	5		15	5		16	15
17	21		18	10		19	14		20	15		21	21		22	14		0	11			

q = 23, $m = 3$, $a = 0$: $f(x) = x^6 + 9x^2 + x + 5$

p = 19, $m = 3$: each pair (a, c) represents a polynomial of the form $f(x) = x^5 + ax^2 + x + c$, with the exception of $a = 8$ when the polynomial is of the form $f(x) = x^5 + ax^2 + 2x + c$ and $a = 7$ and 17 when the polynomial is of the form $f(x) = x^5 + ax^2 + 4x + c$.

a	c		a	c		a	c		a	c		a	c		a	c		a	c		a	c
1	17		2	5		3	5		4	4		5	5		6	5		7	9		8	16
9	5		10	17		11	4		12	6		13	16		14	4		15	4		16	6
17	9		18	5																		

p = 19, $m = 3$: every triple (a, b, c) in the following table represents a polynomial of the form $f(x) = x^6 + ax^3 + bx + c$.

a	b	c		a	b	c		a	b	c		a	b	c		a	b	c		a	b	c
1	4	14		2	1	10		3	1	10		4	2	2		5	2	2		6	8	14
7	1	2		8	2	3		9	10	3		10	4	3		11	1	14		12	5	10
13	1	14		14	2	3		15	5	2		16	1	13		17	1	2		18	1	13
0	1	3																				

q = 19, 17, 13 and **11**, $m = 2$:

a	$q = 19$	$q = 17$	$q = 13$	$q = 11$
0	$x^4 + 2x + 10$	$x^4 + x + 11$	$x^4 + x^3 + x + 2$	$x^4 + x + 2$
1	$x^4 + x^2 + x + 3$	$x^4 + x^2 + x + 7$	$x^4 + x^2 + x + 2$	$x^4 + x^2 + 2x + 2$
2	$x^4 + 2x^2 + 3x + 2$	$x^4 + 2x^2 + x + 11$	$x^4 + 2x^2 + 2x + 2$	$x^4 + 2x^2 + 2x + 7$
3	$x^4 + 3x^2 + 3x + 2$	$x^4 + 3x^2 + 4x + 10$	$x^4 + 3x^2 + x + 2$	$x^4 + 3x^2 + x + 2$
4	$x^4 + 4x^2 + x + 14$	$x^4 + 4x^2 + x + 3$	$x^4 + 4x^2 + x + 2$	$x^4 + 4x^2 + x + 2$
5	$x^4 + 5x^2 + x + 13$	$x^4 + 5x^2 + x + 5$	$x^4 + 5x^2 + 2x + 2$	$x^4 + 5x^2 + x + 7$
6	$x^4 + 6x^2 + x + 3$	$x^4 + 6x^2 + x + 6$	$x^4 + 6x^2 + 2x + 6$	$x^4 + 6x^2 + x + 8$
7	$x^4 + 7x^2 + x + 14$	$x^4 + 7x^2 + 2x + 12$	$x^4 + 7x^2 + 2x + 6$	$x^4 + 7x^2 + x + 6$
8	$x^4 + 8x^2 + x + 10$	$x^4 + 8x^2 + 2x + 3$	$x^4 + 8x^2 + 2x + 7$	$x^4 + 8x^2 + x + 2$
9	$x^4 + 9x^2 + x + 2$	$x^4 + 9x^2 + x + 10$	$x^4 + 9x^2 + x + 6$	$x^4 + 9x^2 + x + 8$
10	$x^4 + 10x^2 + x + 2$	$x^4 + 10x^2 + 2x + 7$	$x^4 + 10x^2 + x + 6$	$x^4 + 10x^2 + 5x + 7$
11	$x^4 + 11x^2 + x + 2$	$x^4 + 11x^2 + x + 5$	$x^4 + 11x^2 + 2x + 11$	—
12	$x^4 + 12x^2 + x + 3$	$x^4 + 12x^2 + 2x + 5$	$x^4 + 12x^2 + 2x + 7$	—
13	$x^4 + 13x^2 + x + 2$	$x^4 + 13x^2 + x + 5$	—	—
14	$x^4 + 14x^2 + 3x + 3$	$x^4 + 14x^2 + x + 10$	—	—
15	$x^4 + 15x^2 + x + 3$	$x^4 + 15x^2 + x + 3$	—	—
16	$x^4 + 16x^2 + x + 10$	$x^4 + 16x^2 + 2x + 11$	—	—
17	$x^4 + 17x^2 + x + 15$	—	—	—
18	$x^4 + 18x^2 + x + 2$	—	—	—

q = 17, $m = 3$, $a = 0$: $f(x) = x^6 + 13x^2 + x + 3$

q = 17, $m = 4$, $a = 0$, $n = 8$: $x^8 + 2x^3 + x^2 + 3$

q = 16 , $m = 3$:

a	$f(x)$
1	$x^5 + x^2 + x + \alpha^3 + 1$
α	$x^5 + \alpha x^2 + x + \alpha^2$
$\alpha + 1$	$x^5 + (\alpha + 1)x^2 + (\alpha^3 + \alpha^2 + \alpha + 1)x + \alpha^2$
α^2	$x^5 + \alpha^2 x^2 + \alpha^3 x + \alpha^2$
$\alpha^2 + 1$	$x^5 + (\alpha^2 + 1)x^2 + (\alpha^3 + \alpha)x + \alpha^2$
$\alpha^2 + \alpha$	$x^5 + (\alpha^2 + \alpha)x^2 + (\alpha^3 + \alpha^2 + \alpha + 1)x + \alpha^2$
$\alpha^2 + \alpha + 1$	$x^5 + (\alpha^2 + \alpha + 1)x^2 + (\alpha^3 + \alpha^2 + \alpha + 1)x + \alpha^2$
α^3	$x^5 + \alpha^3 x^2 + (\alpha^2 + \alpha + 1)x + \alpha^2$
$\alpha^3 + 1$	$x^5 + (\alpha^3 + 1)x^2 + (\alpha^3 + \alpha^2 + \alpha + 1)x + \alpha^3 + 1$
$\alpha^3 + \alpha$	$x^5 + (\alpha^3 + \alpha)x^2 + x + \alpha^2$
$\alpha^3 + \alpha + 1$	$x^5 + (\alpha^3 + \alpha + 1)x^2 + (\alpha + 1)x + \alpha^2$
$\alpha^3 + \alpha^2$	$x^5 + (\alpha^3 + \alpha^2)x^2 + (\alpha^2 + 1)x + \alpha^2$
$\alpha^3 + \alpha^2 + 1$	$x^5 + (\alpha^3 + \alpha^2 + 1)x^2 + x + \alpha^2$
$\alpha^3 + \alpha^2 + \alpha$	$x^5 + (\alpha^3 + \alpha^2 + \alpha)x^2 + (\alpha^3 + \alpha^2 + \alpha + 1)x + \alpha^2$
$\alpha^3 + \alpha^2 + \alpha + 1$	$x^5 + (\alpha^3 + \alpha^2 + \alpha + 1)x^2 + \alpha^3 x + \alpha^2$

q = 13, 11, 7 and **5**, $m = 3$, $n = 5$:

a	$q = 13$	$q = 11$	$q = 7$	$q = 5$
1	$x^5 + x^2 + x + 6$	$x^5 + x^2 + x + 4$	$x^5 + x^3 + x^2 + 3x + 2$	$x^5 + x^2 + 2$
2	$x^5 + 2x^2 + x + 2$	$x^5 + 2x^2 + 9$	$x^5 + 2x^2 + 2x + 4$	$x^5 + 2x^2 + x + 2$
3	$x^5 + 3x^2 + 2$	$x^5 + 3x^2 + x + 3$	$x^5 + 3x^2 + 2$	$x^5 + 3x^2 + x + 3$
4	$x^5 + 4x^2 + 2$	$x^5 + 4x^2 + x + 3$	$x^5 + 4x^2 + x + 2$	$x^5 + 4x^2 + 3$
5	$x^5 + 5x^2 + 2$	$x^5 + 5x^2 + x + 9$	$x^5 + 5x^2 + 3x + 2$	—
6	$x^5 + 6x^2 + x + 6$	$x^5 + 6x^2 + 9$	$x^5 + 6x^2 + x + 2$	—
7	$x^5 + 7x^2 + x + 2$	$x^5 + 7x^2 + 9$	—	—
8	$x^5 + 8x^2 + 7$	$x^5 + 8x^2 + 9$	—	—
9	$x^5 + 9x^2 + 7$	$x^5 + 9x^2 + 2x + 4$	—	—
10	$x^5 + 10x^2 + 7$	$x^5 + 10x^2 + 9$	—	—
11	$x^5 + 11x^2 + x + 11$	—	—	—
12	$x^5 + 12x^2 + x + 7$	—	—	—

q = 13, $m = 4$, $a = 0$, $n = 8$: $x^8 + x^3 + x^2 + 2$

q = 13, 11, 7 and **5**, $m = 3$, $n = 6$:

a	$q = 13$	$q = 11$	$q = 7$	$q = 5$
0	$x^6 + x^5 + 2x + 6$	$x^6 + x^5 + x + 7$	$x^6 + x^5 + 5x + 3$	$x^6 + x + 2$
1	$x^6 + x^3 + x + 6$	$x^6 + x^3 + 2x + 6$	$x^6 + x^3 + x + 5$	$x^6 + x^3 + x^2 + 3$
2	$x^6 + 2x^3 + x + 11$	$x^6 + 2x^3 + 4x + 2$	$x^6 + 2x^3 + 3x + 3$	$x^6 + 2x^3 + x^2 + 2$
3	$x^6 + 3x^3 + x + 2$	$x^6 + 3x^3 + 2x + 2$	$x^6 + x^5 + 3x^3 + 5$	$x^6 + 3x^3 + x^2 + 2$
4	$x^6 + 4x^3 + 7x + 2$	$x^6 + 4x^3 + 2x + 6$	$x^6 + x^5 + 4x^3 + 3$	$x^6 + 4x^3 + x^2 + 3$
5	$x^6 + 5x^3 + 2x + 11$	$x^6 + 5x^3 + 2x + 7$	$x^6 + 5x^3 + x + 3$	—
6	$x^6 + 6x^3 + x + 7$	$x^6 + 6x^3 + 4x + 7$	$x^6 + 6x^3 + 3x + 5$	—
7	$x^6 + 7x^3 + 4x + 7$	$x^6 + 7x^3 + 4x + 6$	—	—
8	$x^6 + 8x^3 + x + 11$	$x^6 + 8x^3 + 4x + 2$	—	—
9	$x^6 + 9x^3 + 2x + 2$	$x^6 + 9x^3 + 2x + 2$	—	—
10	$x^6 + 10x^3 + x + 2$	$x^6 + 10x^3 + 4x + 6$	—	—
11	$x^6 + 11x^3 + x + 7$	—	—	—
12	$x^6 + 12x^3 + x + 2$	—	—	—

q = 11, $m = 4$, $a = 0$, $n = 8$: $x^8 + 2x^3 + x^2 + 2$

q = 9 and **3**, $m = 3$

n	a	$q = 3$	$q = 9$
5	1	$x^5 + x^4 + x^2 + 1$	$x^5 + x^2 + \alpha$
	2	$x^5 + 2x^2 + x + 1$	$x^5 + 2x^2 + \alpha + 2$
	α	—	$x^5 + \alpha x^2 + \alpha$
	$\alpha + 1$	—	$x^5 + (\alpha + 1)x^2 + \alpha$
	$2\alpha + 1$	—	$x^5 + (2\alpha + 1)x^2 + 2\alpha + 1$
	$2\alpha + 2$	—	$x^5 + (2\alpha + 2)x^2 + 2\alpha + 1$
	$\alpha + 2$	—	$x^5 + (\alpha + 2)x^2 + 2\alpha + 1$
	2α	—	$x^5 + 2\alpha x^2 + \alpha$
6	1	$x^6 + x^3 + x + 2$	$x^6 + x^3 + x^2 + x + \alpha$
	2	$x^6 + 2x^3 + 2x + 2$	$x^6 + 2x^3 + x^2 + 2x + \alpha$
	α	—	$x^6 + \alpha x^3 + x^2 + 2\alpha + 2$
	$\alpha + 1$	—	$x^6 + (\alpha + 1)x^3 + x^2 + \alpha$
	$2\alpha + 1$	—	$x^6 + (2\alpha + 1)x^3 + x^2 + (\alpha + 2)x + \alpha + 1$
	$2\alpha + 2$	—	$x^6 + (2\alpha + 2)x^3 + x^2 + \alpha$
	$\alpha + 2$	—	$x^6 + (\alpha + 2)x^3 + x^2 + (2\alpha + 1)x + \alpha + 1$
	2α	—	$x^6 + 2\alpha x^3 + x^2 + 2\alpha + 2$
	0	$x^6 + x + 2$	$x^6 + x^2 + \alpha x + \alpha$

q = 9, $m = 4$, $a = 0$, $n = 8$: $f(x) = x^8 + (2\alpha+2)x^4 + (\alpha+2)x + 2\alpha + 2$

q = 9, $m = 2$:

a	$f(x)$		a	$f(x)$
1	$x^4 + x^2 + x + \alpha$		$\alpha+1$	$x^4 + (\alpha+1)x^2 + \alpha x + 2\alpha$
2	$x^4 + 2x^2 + x + (\alpha+1)$		$\alpha+2$	$x^4 + (\alpha+2)x^2 + \alpha x + (\alpha+1)$
α	$x^4 + \alpha x^2 + x + \alpha$		$2\alpha+1$	$x^4 + (2\alpha+1)x^2 + \alpha x + \alpha$
2α	$x^4 + 2\alpha x^2 + (2\alpha+1)x + \alpha$		$2\alpha+2$	$x^4 + (2\alpha+2)x^2 + x + (2\alpha+2)$
0	$x^4 + x + (2\alpha+2)$			

q = 8 and **4**, $m = 3$, $n = 5$:

a	$q = 8$	$q = 4$
1	$x^5 + x^2 + x + \alpha$	$x^5 + (\alpha+1)x^3 + x^2 + x + \alpha + 1$
α	$x^5 + \alpha x^2 + (\alpha+1)x + \alpha$	$x^5 + x^3 + \alpha x^2 + (\alpha+1)x + \alpha + 1$
$\alpha+1$	$x^5 + (\alpha+1)x^2 + \alpha^2 x + \alpha$	$x^5 + x^3 + (\alpha+1)x^2 + x + \alpha + 1$
α^2	$x^5 + \alpha^2 x^2 + x + \alpha$	—
α^2+1	$x^5 + (\alpha^2+1)x^2 + \alpha^2 x + \alpha$	—
$\alpha^2+\alpha$	$x^5 + (\alpha^2+\alpha)x^2 + x + \alpha$	—
$\alpha^2+\alpha+1$	$x^5 + (\alpha^2+\alpha+1)x^2 + (\alpha^2+\alpha)x + \alpha$	—

q = 8 and **4**, $m = 3$, $n = 6$:

a	$q = 8$	$q = 4$
0	$x^6 + x + \alpha^2 + 1$	$x^6 + x^2 + x + \alpha + 1$
1	$x^6 + x^3 + x + \alpha^2$	$x^6 + x^5 + x^3 + (\alpha+1)x^2 + x + \alpha$
α	$x^6 + \alpha x^3 + x + \alpha^2 + 1$	$x^6 + \alpha x^3 + x^2 + \alpha + 1$
$\alpha+1$	$x^6 + (\alpha+1)x^3 + x + \alpha^2 + 1$	$x^6 + (\alpha+1)x^3 + x^2 + \alpha$
α^2	$x^6 + \alpha^2 x^3 + x + \alpha^2 + \alpha$	—
α^2+1	$x^6 + (\alpha^2+1)x^3 + x + \alpha^2 + \alpha$	—
$\alpha^2+\alpha$	$x^6 + (\alpha^2+\alpha)x^3 + x + \alpha + 1$	—
$\alpha^2+\alpha+1$	$x^6 + (\alpha^2+\alpha+1)x^3 + x + \alpha + 1$	—

q = 8, $m = 2$, $a = 0$: $f(x) = x^4 + x + \alpha^2$

q = 8, $m = 4$, $a = 0$, $n = 8$: $x^8 + (\alpha^2+\alpha)x^6 + (\alpha^2+\alpha+1)x^4 + (\alpha^2+\alpha)x^3 + \alpha^2 x^2 + \alpha x + \alpha$

q = 7, 5 and **3**, $m = 2$, $n = 4$:

a	$q = 7$	$q = 5$	$q = 3$
0	$x^4 + x^3 + x + 3$	$x^4 + x^3 + x + 3$	$x^4 + x + 2$
1	$x^4 + x^3 + x^2 + 3$	$x^4 + x^2 + 2x + 2$	$x^4 + 2x^3 + x^2 + x + 2$
2	$x^4 + 2x^3 + 2x^2 + 3$	$x^4 + x^3 + x^2 + 2x + 2$	$x^4 + 2x^3 + 2x^2 + x + 2$
3	$x^4 + 2x^3 + 3x^2 + 3$	$x^4 + 2x^3 + 3x^2 + 2$	—
4	$x^4 + 2x^3 + 4x^2 + 3$	$x^4 + 4x^2 + x + 2$	—
5	$x^4 + 5x^2 + 3x + 3$	—	—
6	$x^4 + 6x^2 + x + 3$	—	—

q = 7, 5 and **3**, $m = 2$, $n = 5$:

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	$x^5 + 6x^3 + 2$	—	—

q = 7, 5 and **3**, $m = 2$, $n = 4$:

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

q = 7, 5 and **3** $m = 4$:

a	$q = 3$	$q = 5$	$q = 7$
0	$x^8 + x^3 + 2$	$x^8 + x^3 + 2x^2 + 2$	$x^8 + x^3 + 3x^2 + 3$
1	$x^8 + x^5 + x^4 + 2x^2 + 2$	$x^8 + x^5 + x^4 + 3x + 3$	$x^8 + x^5 + x^4 + x + 5$
2	$x^8 + 2x^5 + x^4 + 2x^2 + 2$	$x^8 + 2x^5 + x^4 + x + 3$	$x^8 + 2x^5 + x^4 + 2x + 5$
3	—	$x^8 + 3x^5 + x^4 + 4x + 3$	$x^8 + 3x^5 + x^4 + 5$
4	—	$x^8 + 4x^5 + x^4 + 2x + 3$	$x^8 + 4x^5 + x^4 + 5$
5	—	—	$x^8 + 5x^5 + x^4 + 5x + 5$
6	—	—	$x^8 + 6x^5 + x^4 + 6x + 5$

q = 4, $m = 2$, $a = 0$, $n = 4$: $f(x) = x^4 + x^3 + x + (\alpha + 1)$

q = 4, $m = 2$, $n = 5$:

a	$f(x)$
1	$x^5 + x^3 + x + \alpha$
α	$x^5 + \alpha x^3 + (\alpha + 1)x + (\alpha + 1)$
$\alpha + 1$	$x^5 + (\alpha + 1)x^3 + \alpha x + \alpha$

q = 4 and **2**, $m = 4$:

a	$q = 2$	$q = 4$
1	$x^8 + x^5 + x^3 + x^2 + x + 1$	$x^8 + x^5 + x^2 + x + \alpha$
α	—	$x^8 + \alpha x^5 + (\alpha + 1)x^2 + \alpha$
$\alpha + 1$	—	$x^8 + (\alpha + 1)x^5 + \alpha x^2 + \alpha$

q = 2, $m = 2$, $a = 1$, $n = 5$: $f(x) = x^5 + x^3 + 1$

q = 2, $m = 2$, $a = 0$, $n = 4$: $f(x) = x^4 + x + 1$

q = 2, $m = 3$, $a = 1$, $n = 5$: $f(x) = x^5 + x^2 + 1$

q = 2, $m = 3$, $a = 0$, $n = 6$: $f(x) = x^6 + x + 1$

q = 2, $m = 3$, $a = 1$, $n = 6$: $f(x) = x^6 + x^5 + x^3 + x^2 + 1$

For composite q, it takes Maple significantly longer to verify if a polynomial in $\mathbb{F}_q[x]$ is primitive. From the above list, 18 primitive polynomials over composite fields with $q \geq 16$ elements were left out: 10 primitive quartics with zero second coefficient and 8 primitive sextics with zero third coefficient. We will here prove their existence, but the primitive polynomials themselves are not given, due to the time they take to compute.

In what follows, the fields $\mathbb{F}_{q^4}$ and $\mathbb{F}_{q^6}$ are defined as $\mathbb{F}_p(\alpha)$ where $f_q(x)$ is the minimal polynomial of α. Then γ is a primitive element of $\mathbb{F}_{q^4}$ (or $\mathbb{F}_{q^6}$) (in terms of α) with minimal polynomial of γ over $\mathbb{F}_q$ having second (or third, as appropriate) coefficient a. There were no special preferences when choosing α and γ; the choice was random.

q = 4913 $= 17^3$, $m = 2$, $n = 4$:
$f_q(x) = x^{12} + 16x^{11} + 9x^9 + 5x^8 + 14x^7 + 13x^6 + 8x^5 + 3x^4 + 3x^3 + 11x^2 + 12x + 6,$
$\gamma = 10\alpha^{11} + 11\alpha^{10} + 12\alpha^9 + 14\alpha^8 + 14\alpha^7 + \alpha^6 + 2\alpha^5 + 11\alpha^4 + \alpha^3 + 11\alpha^2 + 13$

q = 1331 $= 11^3$, $m = 2$, $n = 4$:
$f_q(x) = x^{12} + 5x^{11} + 4x^{10} + 10x^9 + 10x^8 + 8x^7 + x^6 + 2x^5 + 5x^4 + 6x^2 + 1,$
$\gamma = 7\alpha^{11} + 5\alpha^{10} + \alpha^9 + 2\alpha^8 + 10\alpha^7 + 9\alpha^5 + 6\alpha^4 + 10\alpha + 4$

q = 343 $= 7^3$, $m = 2$, $n = 4$:
$f_q(x) = x^{12} + 4x^{11} + 3x^{10} + 3x^9 + 3x^8 + x^7 + 3x^6 + 4x^4 + 4x^3 + 5x + 4,$
$\gamma = 4\alpha^{11} + 3\alpha^{10} + 2\alpha^9 + 6\alpha^8 + \alpha^7 + 3\alpha^6 + 4\alpha^5 + 6\alpha^4 + 6\alpha^3 + 4\alpha + 5$

q = 289 $= 17^2$, $m = 2$, $n = 4$:
$f_q(x) = x^8 + 10x^7 + 11x^6 + 8x^5 + 5x^4 + 8x^3 + 12x^2 + 3x + 5,$
$\gamma = 4\alpha^7 + 2\alpha^4 + 2\alpha^2 + 4$

q = 243 $= 3^5$, $m = 2$, $n = 4$:
$f_q(x) = x^{20} + 2x^{17} + 2x^{15} + x^{14} + x^{12} + 2x^{11} + 2x^{10} + x^7 + 2x^6 + x^5 + x^4 + x^3 + 2x + 1,$
$\gamma = 2\alpha^{19} + 2\alpha^{18} + \alpha^{17} + 2\alpha^{16} + 2\alpha^{15} + \alpha^{14} + \alpha^{13} + \alpha^{12} + 2\alpha^7 + 2\alpha^6 + \alpha^5 + 2\alpha^2 + 2\alpha + 2$

q = 169 $= 13^2$, $m = 2$, $n = 4$:
$f_q(x) = x^8 + 10x^7 + x^6 + 10x^5 + 9x^3 + 9x^2 + 6x + 5,$
$\gamma = 10\alpha^7 + 4\alpha^6 + 10\alpha^5 + 9\alpha^4 + 2\alpha^3 + 9\alpha^2 + 11\alpha + 11$

q = 128 $= 2^7$, $m = 3$, $n = 6$:
$f_q(x) = x^{42} + x^{39} + x^{37} + x^{36} + x^{28} + x^{27} + x^{22} + x^{20} + x^{18} + x^{12} + x^8 + x^7 + x^6 + x^4 + 1,$
$\gamma = \alpha^{41} + \alpha^{39} + \alpha^{37} + \alpha^{32} + \alpha^{26} + \alpha^{24} + \alpha^{21} + \alpha^{18} + \alpha^{15} + \alpha^{13} + \alpha^{10} + \alpha^9 + \alpha^8 + \alpha^3$

q = 125 $= 5^3$, $m = 2$, $n = 4$:
$f_q(x) = x^{12} + 2x^{11} + 2x^{10} + 3x^9 + x^8 + 2x^7 + 2x^6 + x^5 + 3x + 2$
$\gamma = 4\alpha^{10} + 3\alpha^9 + \alpha^8 + 3\alpha^6 + 3\alpha^5 + 4\alpha^3 + 2\alpha^2 + 3\alpha + 3$

q = 125 $= 5^3$, $m = 3$, $n = 6$:
$f_q(x) = x^{18} + 2x^{17} + 2x^{15} + x^{14} + x^9 + 4x^8 + 4x^7 + 3x^6 + 2x^5 + x^4 + 3x^3 + 2x^2 + 3x + 3$
$\gamma = \alpha^{17} + \alpha^{15} + \alpha^{14} + 3\alpha^{13} + \alpha^{11} + 4\alpha^{10} + 3\alpha^9 + 2\alpha^7 + 2\alpha^6 + 4\alpha^5 + 2\alpha^3 + \alpha^2 + 2\alpha$

q = 121 $= 11^2$, $m = 2$, $n = 4$:

$f_q(x) = x^8 + 10x^7 + 10x^6 + 5x^5 + 4x^4 + 7x^3 + 5x^2 + 5x + 2,$

$\gamma = 8\alpha^7 + 6\alpha^5 + 8\alpha^4 + 5\alpha^3 + 7\alpha^2 + 3\alpha + 6$

q = 121 $= 11^2$, $m = 3$, $n = 6$:

$f_q(x) = x^{12} + 10x^{11} + 4x^9 + 7x^8 + 6x^7 + 9x^6 + x^5 + 7x^4 + 10x^3 + 6x^2 + 8x + 4,$

$\gamma = 5\alpha^{11} + 8\alpha^{10} + 7\alpha^9 + \alpha^8 + 8\alpha^7 + 4\alpha^6 + 5\alpha^5 + 7\alpha^4 + 5\alpha^3 + 2\alpha^2 + 7\alpha$

q = 81 $= 3^4$, $m = 2$, $n = 4$:

$f_q(x) = x^{16} + 2x^{15} + 2x^{14} + 2x^{11} + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2,$

$\gamma = \alpha^{15} + \alpha^{13} + \alpha^{12} + 2\alpha^{10} + \alpha^8 + \alpha^7 + 2\alpha^6 + 2\alpha^5 + 2\alpha^4 + 2\alpha^3 + \alpha^2 + \alpha + 2$

q = 64 $= 2^6$, $m = 3$, $n = 6$:

$f_q(x) = x^{36} + x^{35} + x^{33} + x^{27} + x^{26} + x^{17} + x^{15} + x^{12} + x^6 + x^3 + x^2 + x + 1,$

$\gamma = \alpha^{35} + \alpha^{33} + \alpha^{28} + \alpha^{23} + \alpha^{22} + \alpha^{19} + \alpha^{17} + \alpha^{15} + \alpha^{13} + \alpha^{12} + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$

q = 49 $= 7^2$, $m = 2$, $n = 4$:

$f_q(x) = x^8 + x^7 + x^6 + 5x^5 + 4x^3 + 4x^2 + 3,$

$\gamma = \alpha^7 + \alpha^6 + 5\alpha^5 + 6\alpha^4 + 5\alpha^2 + 6\alpha$

q = 49 $= 7^2$, $m = 3$, $n = 6$:

$f_q(x) = x^{12} + 4x^{11} + 2x^{10} + 3x^9 + 6x^8 + 6x^7 + 3x^6 + x^4 + 6x^3 + 2x^2 + 6x + 4,$

$\gamma = \alpha^{11} + 4\alpha^9 + 4\alpha^7 + 6\alpha^6 + 4\alpha^5 + \alpha^3 + 5\alpha^2 + 4\alpha + 6$

q = 32 $= 2^5$, $m = 3$, $n = 6$:

$f_q(x) = x^{30} + x^{29} + x^{28} + x^{25} + x^{22} + x^{19} + x^{16} + x^{14} + x^{12} + x^{11} + x^7 + x^3 + x^2 + x + 1,$

$\gamma = \alpha^{29} + \alpha^{27} + \alpha^{24} + \alpha^{23} + \alpha^{22} + \alpha^{21} + \alpha^{20} + \alpha^{17} + \alpha^{15} + \alpha^{12} + \alpha^{10} + \alpha^8 + \alpha^7 + \alpha^3 + \alpha^2 + \alpha$

q = 25 $= 5^2$, $m = 3$, $n = 6$:

$f_q(x) = x^{12} + 4x^{11} + x^{10} + 3x^9 + 2x^8 + 4x^7 + 4x^5 + 3x^4 + 4x^2 + 2x + 4,$

$\gamma = 3\alpha^{11} + 2\alpha^{10} + 4\alpha^8 + 4\alpha^6 + 4\alpha^5 + 4\alpha^3 + 4\alpha^2 + 3\alpha + 3$

q = 16 $= 2^4$, $m = 3$, $n = 6$:

$f_q(x) = x^{24} + x^{23} + x^{22} + x^{19} + x^{17} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^3 + x^2 + 1,$

$\gamma = \alpha^{23} + \alpha^{21} + \alpha^{20} + \alpha^{19} + \alpha^{17} + \alpha^{14} + \alpha^{13} + \alpha^{11} + \alpha^8 + \alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$

B.2 Primitive polynomials with m-th coefficient and constant term prescribed

q = 29, $m = 2$: for each pair (a, c) we give a corresponding pair (b, d) to represent a primitive polynomial of the form $x^6 + ax^4 + bx^2 + dx + c$.

$a\backslash c$	2	3	8	10	11	14	15	18	19	21	26	27
1	(0, 7)	(0, 12)	(1, 9)	(0, 10)	(0, 8)	(0, 10)	(1, 7)	(0, 7)	(0, 3)	(1, 6)	(0, 4)	(0, 1)
2	(1, 2)	(0, 1)	(0, 5)	(0, 3)	(0, 5)	(0, 1)	(0, 8)	(0, 5)	(1, 10)	(1, 1)	(0, 1)	(2, 2)
3	(1, 9)	(0, 3)	(0, 6)	(0, 8)	(0, 9)	(2, 3)	(1, 5)	(0, 14)	(0, 13)	(0, 9)	(0, 3)	(0, 13)
4	(0, 1)	(2, 8)	(0, 2)	(1, 3)	(0, 12)	(0, 6)	(0, 10)	(0, 7)	(1, 6)	(0, 5)	(0, 1)	(0, 1)
5	(0, 2)	(0, 5)	(0, 3)	(0, 5)	(0, 4)	(1, 2)	(1, 10)	(0, 4)	(2, 3)	(0, 1)	(0, 5)	(0, 6)
6	(0, 13)	(0, 1)	(0, 1)	(0, 5)	(0, 4)	(0, 1)	(0, 3)	(0, 3)	(0, 8)	(1, 2)	(0, 13)	(0, 11)
7	(0, 5)	(0, 3)	(0, 2)	(0, 2)	(3, 1)	(0, 10)	(0, 13)	(1, 1)	(0, 1)	(0, 6)	(0, 1)	(0, 1)
8	(0, 9)	(0, 5)	(0, 5)	(2, 1)	(0, 2)	(0, 1)	(0, 1)	(0, 3)	(0, 14)	(0, 7)	(0, 3)	(3, 3)
9	(1, 6)	(2, 5)	(0, 1)	(0, 2)	(0, 6)	(0, 1)	(0, 1)	(0, 2)	(0, 7)	(0, 1)	(2, 1)	(0, 6)
10	(0, 10)	(0, 2)	(0, 5)	(0, 7)	(1, 14)	(0, 12)	(1, 5)	(1, 4)	(0, 4)	(0, 5)	(1, 8)	(0, 7)
11	(0, 2)	(1, 3)	(1, 4)	(0, 14)	(1, 4)	(0, 7)	(0, 7)	(0, 6)	(0, 7)	(1, 7)	(0, 7)	(0, 12)
12	(0, 5)	(2, 7)	(0, 1)	(0, 1)	(0, 9)	(0, 1)	(2, 8)	(0, 9)	(0, 2)	(0, 13)	(2, 4)	(0, 10)
13	(1, 1)	(0, 2)	(0, 9)	(0, 6)	(2, 1)	(0, 4)	(0, 2)	(0, 4)	(0, 2)	(0, 3)	(0, 10)	(2, 11)
14	(0, 9)	(0, 3)	(0, 2)	(1, 8)	(1, 7)	(0, 2)	(0, 4)	(0, 9)	(1, 1)	(1, 1)	(0, 9)	(0, 11)
15	(0, 13)	(0, 4)	(1, 5)	(1, 11)	(0, 8)	(0, 3)	(0, 5)	(1, 3)	(1, 9)	(0, 1)	(0, 7)	(0, 8)
16	(2, 13)	(0, 1)	(0, 7)	(0, 5)	(0, 3)	(0, 5)	(0, 9)	(2, 10)	(0, 6)	(0, 8)	(0, 5)	(1, 3)
17	(0, 4)	(2, 4)	(0, 11)	(0, 5)	(0, 4)	(2, 4)	(0, 9)	(0, 8)	(0, 4)	(0, 3)	(2, 3)	(2, 2)
18	(0, 1)	(0, 3)	(1, 3)	(0, 3)	(0, 4)	(0, 3)	(0, 1)	(1, 8)	(0, 6)	(1, 10)	(1, 7)	(0, 5)
19	(0, 1)	(1, 9)	(0, 2)	(0, 10)	(1, 6)	(1, 2)	(0, 1)	(1, 6)	(0, 3)	(0, 1)	(0, 3)	(0, 4)
20	(0, 8)	(2, 4)	(0, 8)	(0, 3)	(0, 5)	(0, 1)	(0, 4)	(0, 8)	(0, 5)	(0, 4)	(2, 2)	(1, 14)
21	(3, 7)	(0, 7)	(0, 3)	(0, 6)	(0, 6)	(0, 6)	(0, 12)	(0, 5)	(2, 11)	(0, 2)	(0, 2)	(0, 1)
22	(0, 9)	(0, 7)	(0, 1)	(0, 7)	(1, 12)	(0, 11)	(0, 4)	(3, 7)	(0, 5)	(0, 5)	(0, 3)	(0, 2)
23	(0, 11)	(0, 6)	(1, 2)	(0, 9)	(0, 1)	(0, 7)	(0, 8)	(0, 6)	(0, 2)	(0, 8)	(0, 5)	(0, 6)
24	(0, 14)	(0, 2)	(0, 12)	(2, 3)	(0, 10)	(1, 4)	(1, 5)	(0, 3)	(0, 2)	(0, 7)	(0, 2)	(0, 5)
25	(0, 4)	(0, 11)	(0, 2)	(1, 4)	(0, 3)	(0, 4)	(0, 9)	(0, 1)	(1, 7)	(0, 2)	(2, 9)	(0, 11)
26	(0, 11)	(0, 7)	(0, 4)	(0, 6)	(0, 6)	(1, 2)	(2, 4)	(0, 1)	(0, 9)	(0, 8)	(0, 7)	(1, 8)
27	(2, 1)	(0, 8)	(1, 12)	(1, 1)	(0, 1)	(0, 9)	(0, 6)	(0, 2)	(0, 6)	(0, 2)	(0, 2)	(1, 5)
28	(0, 6)	(0, 10)	(1, 3)	(0, 4)	(0, 3)	(1, 3)	(0, 4)	(0, 8)	(0, 4)	(1, 4)	(0, 1)	(0, 3)

q = 23, $m = 2$: for each pair (a, c) we give a corresponding pair (b, d) to represent a primitive polynomial of the form $x^6 + ax^4 + bx^2 + dx + c$.

$a\backslash c$	5	7	10	11	14	15	17	19	20	21
1	(4, 3)	(0, 2)	(1, 3)	(0, 2)	(1, 2)	(2, 1)	(1, 9)	(0, 7)	(0, 3)	(0, 10)
2	(1, 7)	(0, 7)	(0, 6)	(2, 9)	(0, 2)	(1, 7)	(3, 4)	(0, 6)	(2, 5)	(2, 4)
3	(0, 11)	(0, 4)	(1, 4)	(0, 5)	(1, 9)	(0, 9)	(1, 5)	(1, 3)	(1, 7)	(0, 11)
4	(2, 9)	(1, 9)	(0, 2)	(0, 5)	(0, 5)	(0, 4)	(1, 1)	(1, 4)	(0, 6)	(1, 2)
5	(0, 1)	(0, 9)	(0, 4)	(1, 7)	(0, 6)	(0, 9)	(0, 6)	(0, 3)	(0, 2)	(0, 3)
6	(0, 4)	(0, 10)	(0, 11)	(2, 11)	(1, 2)	(1, 2)	(0, 10)	(0, 8)	(1, 1)	(1, 5)
7	(0, 8)	(4, 3)	(0, 2)	(0, 7)	(0, 7)	(0, 7)	(0, 1)	(0, 7)	(0, 1)	(0, 3)
8	(0, 11)	(1, 3)	(2, 6)	(0, 6)	(1, 3)	(1, 5)	(1, 7)	(0, 8)	(0, 8)	(2, 1)
9	(0, 1)	(1, 1)	(1, 10)	(2, 7)	(0, 8)	(0, 3)	(1, 3)	(1, 6)	(0, 3)	(0, 7)
10	(0, 4)	(0, 9)	(0, 4)	(0, 11)	(0, 5)	(0, 2)	(0, 3)	(1, 2)	(0, 5)	(0, 5)
11	(0, 3)	(0, 7)	(0, 11)	(0, 3)	(0, 7)	(0, 2)	(0, 1)	(0, 10)	(0, 2)	(0, 3)
12	(3, 3)	(1, 4)	(0, 7)	(0, 10)	(0, 1)	(1, 1)	(0, 11)	(1, 7)	(1, 3)	(0, 7)
13	(3, 10)	(3, 9)	(0, 6)	(1, 2)	(3, 5)	(0, 4)	(0, 4)	(1, 3)	(11, 8)	(0, 9)
14	(0, 2)	(0, 9)	(2, 2)	(0, 1)	(0, 2)	(0, 8)	(0, 1)	(0, 2)	(0, 2)	(0, 3)
15	(0, 8)	(0, 1)	(0, 10)	(0, 10)	(0, 8)	(0, 5)	(0, 1)	(0, 3)	(0, 6)	(1, 1)
16	(1, 1)	(1, 5)	(2, 1)	(2, 9)	(0, 1)	(0, 8)	(0, 10)	(0, 5)	(1, 6)	(1, 2)
17	(0, 1)	(0, 4)	(0, 1)	(0, 11)	(0, 7)	(0, 1)	(0, 1)	(0, 10)	(2, 1)	(0, 10)
18	(0, 9)	(0, 2)	(2, 7)	(3, 11)	(1, 6)	(1, 2)	(0, 3)	(3, 1)	(0, 1)	(1, 4)
19	(0, 8)	(0, 11)	(0, 4)	(0, 1)	(0, 2)	(0, 5)	(1, 4)	(0, 5)	(0, 11)	(0, 6)
20	(0, 6)	(0, 8)	(0, 4)	(0, 11)	(1, 4)	(0, 5)	(0, 11)	(0, 10)	(0, 1)	(0, 9)
21	(2, 1)	(0, 4)	(0, 3)	(0, 6)	(0, 4)	(0, 5)	(0, 2)	(0, 7)	(0, 2)	(0, 4)
22	(0, 4)	(0, 1)	(0, 2)	(0, 10)	(0, 7)	(3, 1)	(0, 9)	(0, 9)	(0, 2)	(0, 3)

q = 19, $m = 2$: for each pair (a, c) we give a corresponding pair (b, d) to represent a primitive polynomial of the form $x^6 + ax^4 + bx^2 + dx + c$.

$a\backslash c$	2	3	10	13	14	15
1	(0, 2)	(2, 1)	(0, 4)	(2, 1)	(1, 9)	(2, 9)
2	(1, 8)	(0, 4)	(1, 4)	(0, 6)	(0, 9)	(0, 6)
3	(1, 6)	(0, 6)	(1, 5)	(0, 7)	(0, 4)	(0, 9)
4	(2, 4)	(1, 3)	(1, 2)	(0, 5)	(0, 4)	(1, 8)
5	(1, 3)	(0, 2)	(1, 4)	(1, 2)	(1, 3)	(0, 4)
6	(1, 2)	(2, 4)	(1, 2)	(0, 2)	(0, 1)	(1, 2)
7	(0, 5)	(1, 2)	(0, 3)	(2, 2)	(3, 9)	(1, 2)
8	(0, 5)	(0, 3)	(0, 2)	(1, 5)	(1, 1)	(0, 2)
9	(1, 9)	(1, 2)	(1, 9)	(0, 1)	(0, 8)	(1, 3)
10	(0, 8)	(1, 9)	(0, 1)	(0, 1)	(0, 7)	(1, 1)
11	(0, 1)	(1, 4)	(0, 2)	(1, 4)	(1, 5)	(1, 7)
12	(0, 2)	(0, 5)	(0, 3)	(1, 4)	(1, 3)	(0, 3)
13	(0, 1)	(2, 9)	(0, 3)	(0, 7)	(0, 8)	(2, 4)
14	(1, 6)	(0, 9)	(1, 5)	(0, 1)	(0, 6)	(0, 4)
15	(0, 7)	(1, 5)	(0, 2)	(0, 8)	(0, 1)	(1, 2)
16	(1, 6)	(0, 4)	(4, 1)	(1, 1)	(1, 3)	(0, 8)
17	(2, 4)	(0, 3)	(2, 5)	(1, 3)	(1, 3)	(0, 1)
18	(0, 3)	(0, 2)	(0, 5)	(1, 9)	(1, 3)	(0, 5)

q = 19, $m = 3$: for each pair (a, c) we give a corresponding pair (b, d) to represent a primitive polynomial of the form $x^7 + ax^4 + bx^2 + dx + c$.

$a\backslash c$	4	5	6	9	16	17
1	(0, 10)	(0, 4)	(0, 10)	(0, 10)	(0, 4)	(0, 4)
2	(0, 0)	(0, 10)	(0, 0)	(0, 0)	(0, 10)	(0, 10)
3	(0, 3)	(0, 3)	(0, 3)	(0, 3)	(0, 3)	(0, 3)
4	(0, 6)	(0, 3)	(0, 6)	(0, 6)	(0, 3)	(0, 3)
5	(0, 1)	(0, 4)	(0, 1)	(0, 1)	(0, 4)	(0, 4)
6	(0, 2)	(0, 1)	(0, 2)	(0, 2)	(0, 1)	(0, 1)
7	(0, 0)	(0, 2)	(0, 0)	(0, 0)	(0, 2)	(0, 2)
8	(0, 9)	(0, 9)	(0, 9)	(0, 9)	(0, 9)	(0, 9)
9	(0, 4)	(0, 2)	(0, 4)	(0, 4)	(0, 2)	(0, 2)
10	(0, 8)	(0, 2)	(0, 8)	(0, 8)	(0, 2)	(0, 2)
11	(0, 9)	(0, 0)	(0, 9)	(0, 9)	(0, 0)	(0, 0)
12	(0, 3)	(0, 0)	(0, 3)	(0, 3)	(0, 0)	(0, 0)
13	(0, 3)	(0, 2)	(0, 3)	(0, 3)	(0, 2)	(0, 2)
14	(0, 2)	(0, 0)	(0, 2)	(0, 2)	(0, 0)	(0, 0)
15	(0, 9)	(0, 14)	(0, 9)	(0, 9)	(0, 14)	(0, 14)
16	(1, 2)	(0, 7)	(1, 0)	(1, 9)	(0, 7)	(0, 7)
17	(0, 9)	(1, 11)	(0, 9)	(0, 9)	(1, 0)	(1, 3)
18	(0, 0)	(0, 4)	(0, 0)	(0, 0)	(0, 4)	(0, 4)

q = 17, $m = 2$: for each pair (a, c) we give a corresponding pair (b, d) to represent a primitive polynomial of the form $x^6 + ax^4 + bx^2 + dx + c$.

$a\backslash c$	3	5	6	7	10	11	12	14
1	(2, 1)	(0, 2)	(0, 2)	(0, 5)	(0, 3)	(3, 3)	(0, 1)	(0, 2)
2	(5, 5)	(0, 1)	(0, 3)	(1, 3)	(0, 3)	(0, 7)	(0, 4)	(0, 1)
3	(0, 4)	(0, 4)	(0, 4)	(1, 3)	(2, 4)	(0, 6)	(0, 7)	(2, 7)
4	(0, 2)	(1, 3)	(0, 7)	(1, 8)	(0, 4)	(0, 6)	(0, 1)	(0, 4)
5	(0, 2)	(2, 1)	(1, 3)	(0, 2)	(0, 3)	(2, 3)	(0, 2)	(0, 5)
6	(0, 8)	(2, 6)	(0, 6)	(0, 6)	(1, 3)	(0, 2)	(1, 8)	(0, 6)
7	(0, 7)	(0, 1)	(0, 1)	(0, 4)	(0, 5)	(1, 5)	(0, 5)	(5, 5)
8	(0, 8)	(2, 4)	(1, 6)	(0, 3)	(0, 6)	(0, 6)	(0, 2)	(0, 2)
9	(0, 8)	(0, 3)	(0, 6)	(0, 7)	(0, 5)	(1, 7)	(2, 1)	(0, 2)
10	(5, 3)	(0, 3)	(1, 3)	(0, 3)	(0, 1)	(0, 3)	(0, 4)	(1, 6)
11	(0, 7)	(1, 2)	(0, 8)	(1, 5)	(0, 2)	(0, 7)	(2, 7)	(0, 2)
12	(0, 3)	(0, 5)	(2, 5)	(0, 5)	(0, 8)	(1, 5)	(2, 4)	(0, 8)
13	(0, 1)	(0, 1)	(0, 7)	(0, 1)	(1, 2)	(0, 6)	(1, 5)	(0, 8)
14	(2, 6)	(0, 6)	(0, 7)	(2, 1)	(1, 5)	(0, 1)	(0, 1)	(0, 1)
15	(0, 4)	(0, 1)	(0, 6)	(0, 3)	(1, 1)	(0, 5)	(0, 4)	(5, 3)
16	(0, 2)	(0, 4)	(3, 5)	(0, 5)	(0, 3)	(0, 1)	(0, 8)	(2, 4)

q = 13, $m = 2$: for each pair (a, c) we give a corresponding value b to represent a primitive polynomial of the form $x^6 + ax^4 + bx + c$.

$a\backslash c$	2	6	7	11		$a\backslash c$	2	6	7	11		$a\backslash c$	2	6	7	11
1	5	3	3	6		5	3	5	5	5		9	6	1	1	2
2	4	2	2	2		6	1	6	2	6		10	1	1	1	3
3	2	4	4	5		7	4	3	4	5		11	3	1	3	6
4	3	3	3	4		8	1	1	1	2		12	4	2	2	1

q = 13, $m = 3$, $n = 7$: for every pair (a, c) we give a corresponding value b to represent a primitive polynomial of the form $x^7 + ax^4 + bx + c$.

$a\backslash c$	2	6	7	11		$a\backslash c$	2	6	7	11		$a\backslash c$	2	6	7	11
1	0	0	1	1		5	7	7	4	4		9	2	2	0	0
2	11	11	10	10		6	3	3	4	4		10	5	5	1	1
3	1	1	5	5		7	4	4	3	3		11	10	10	1	1
4	0	0	2	2		8	4	4	7	7		12	1	1	0	0

q = 13, $m = 3$, $n = 8$: for every value a and c in the table below the pair (b, d) corresponds to a primitive polynomial of the form $x^8 + ax^5 + bx^2 + dx + c$.

$a\backslash c$	2	6	7	11		$a\backslash c$	2	6	7	11
1	$(2,8)$	$(2,7)$	$(1,12)$	$(1,10)$		7	$(0,2)$	$(0,5)$	$(1,4)$	$(1,2)$
2	$(1,3)$	$(1,1)$	$(0,5)$	$(0,1)$		8	$(2,9)$	$(2,3)$	$(1,0)$	$(1,0)$
3	$(2,4)$	$(2,10)$	$(0,1)$	$(0,3)$		9	$(0,10)$	$(0,12)$	$(1,6)$	$(1,5)$
4	$(0,3)$	$(0,1)$	$(1,1)$	$(1,3)$		10	$(2,9)$	$(2,3)$	$(0,6)$	$(0,5)$
5	$(2,4)$	$(2,10)$	$(1,0)$	$(1,0)$		11	$(1,10)$	$(1,12)$	$(0,4)$	$(0,11)$
6	$(0,11)$	$(0,8)$	$(1,8)$	$(1,1)$		12	$(2,5)$	$(2,6)$	$(1,1)$	$(3,1)$

q = 11, $m = 2$, $n = 6$: for each pair (a, c) we give a corresponding pair (b, d) to represent a primitive polynomial of the form $x^6 + ax^4 + bx^2 + dx + c$.

$a\backslash c$	2	6	7	8		$a\backslash c$	2	6	7	8
1	$(2,3)$	$(1,3)$	$(3,3)$	$(0,2)$		6	$(2,4)$	$(0,1)$	$(1,1)$	$(2,2)$
2	$(0,4)$	$(2,2)$	$(1,1)$	$(3,5)$		7	$(1,5)$	$(0,4)$	$(5,1)$	$(0,1)$
3	$(1,2)$	$(0,3)$	$(0,2)$	$(1,3)$		8	$(0,1)$	$(1,1)$	$(0,4)$	$(4,5)$
4	$(0,3)$	$(0,2)$	$(1,5)$	$(3,2)$		9	$(0,2)$	$(2,3)$	$(1,1)$	$(0,3)$
5	$(1,3)$	$(4,2)$	$(0,3)$	$(4,1)$		10	$(1,1)$	$(1,2)$	$(0,1)$	$(0,4)$

q = 11, $m = 3$, $n = 8$: for every pair (a, c) we give a corresponding value b to represent a primitive polynomial of the form $x^8 + ax^5 + bx + c$.

$a\backslash c$	2	6	7	8		$a\backslash c$	2	6	7	8
1	6	8	5	3		6	9	7	6	5
2	2	7	3	5		7	3	3	6	4
3	1	2	7	3		8	10	9	1	6
4	2	4	1	7		9	1	4	8	3
5	1	3	5	2		10	5	1	1	8

q = 9, $m = 2$, $n = 6$:

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

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

q = 7, $m = 2$, $n = 6$:

a	$c = 3$	$c = 5$
1	$x^6 + x^4 + 2x^2 + 2x + 3$	$x^6 + x^4 + 2x + 5$
2	$x^6 + 2x^4 + x^2 + 3x + 3$	$x^6 + 2x^4 + 3x + 5$
3	$x^6 + 3x^4 + x^2 + 2x + 3$	$x^6 + 3x^4 + 3x + 5$
4	$x^6 + 4x^4 + 3x^2 + x + 3$	$x^6 + 4x^4 + x + 5$
5	$x^6 + 5x^4 + x^2 + x + 3$	$x^6 + 5x^4 + 2x + 5$
6	$x^6 + 6x^4 + x^2 + 2x + 3$	$x^6 + 6x^4 + x + 5$

q = 7, $m = 3$, $n = 7$:

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

q = 7, $m = 3$, $n = 8$:

a	$c = 3$	$c = 5$
1	$x^8 + x^5 + x^2 + 6x + 3$	$x^8 + x^5 + x^2 + 5x + 5$
2	$x^8 + 2x^5 + 5x + 3$	$x^8 + 2x^5 + 3x + 5$
3	$x^8 + 3x^5 + 2x + 3$	$x^8 + 3x^5 + 4x + 5$
4	$x^8 + 4x^5 + 5x + 3$	$x^8 + 4x^5 + 3x + 5$
5	$x^8 + 5x^5 + x + 3$	$x^8 + 5x^5 + 2x + 5$
6	$x^8 + 6x^5 + x^2 + x + 3$	$x^8 + 6x^5 + x^2 + 2x + 5$

q = 5, $m = 2$, $n = 6$:

a	$c = 2$	$c = 3$
1	$x^6 + x^4 + 2x + 2$	$x^6 + x^4 + 3x^2 + x + 3$
2	$x^6 + 2x^4 + 2x + 2$	$x^6 + 2x^4 + x^3 + x + 3$
3	$x^6 + 3x^4 + x^3 + x^2 + 4x + 2$	$x^6 + 3x^4 + x + 3$
4	$x^6 + 4x^4 + 3x^2 + 2x + 2$	$x^6 + 4x^4 + x + 3$

q = 5, $m = 3$, $n = 7$:

a	$c = 2$	$c = 3$
1	$x^7 + x^4 + 3x + 2$	$x^7 + x^4 + 2x^2 + x + 3$
2	$x^7 + 2x^4 + x + 2$	$x^7 + 2x^4 + 3$
3	$x^7 + 3x^4 + 2$	$x^7 + 3x^4 + x + 3$
4	$x^7 + 4x^4 + x^2 + 3x + 2$	$x^7 + 4x^4 + 3x + 3$

q = 5, $m = 3$, $n = 8$:

a	$c = 2$	$c = 3$
1	$x^8 + x^5 + 2x^2 + 2$	$x^8 + x^5 + 3x^2 + 3x + 3$
2	$x^8 + 2x^5 + 2x^2 + 4x + 2$	$x^8 + 2x^5 + x^2 + x + 3$
3	$x^8 + 3x^5 + 2x^2 + x + 2$	$x^8 + 3x^5 + +x^2 + 4x + 3$
4	$x^8 + 4x^5 + 2x^2 + 2$	$x^8 + 4x^5 + 3x^2 + x + 3$

q = 4, $m = 2$, $n = 6$:

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

q = 4, $m = 3$, $n = 7$:

a	$c = \alpha$	$c = \alpha + 1$
1	$x^7 + x^4 + x^2 + \alpha x + \alpha$	$x^7 + x^4 + x^2 + (\alpha + 1)x + (\alpha + 1)$
α	$x^7 + \alpha x^4 + (\alpha + 1)x^2 + \alpha$	$x^7 + \alpha x^4 + \alpha x^2 + (\alpha + 1)$
$\alpha + 1$	$x^7 + (\alpha + 1)x^4 + (\alpha + 1)x^2 + \alpha$	$x^7 + (\alpha + 1)x^4 + \alpha x^2 + (\alpha + 1)$

q = 4, $m = 3$, $n = 8$:

a	$c = \alpha$	$c = \alpha + 1$
1	$x^8 + x^5 + x^2 + x + \alpha$	$x^8 + x^5 + x^2 + x + (\alpha + 1)$
α	$x^8 + \alpha x^5 + (\alpha + 1)x^2 + \alpha$	$x^8 + \alpha x^5 + (\alpha + 1)x^2 + (\alpha + 1)$
$\alpha + 1$	$x^8 + (\alpha + 1)x^5 + \alpha x^2 + \alpha$	$x^8 + (\alpha + 1)x^5 + \alpha x^2 + (\alpha + 1)$

q = 3, $m = 2$, $n = 6$:

a	$c = 2$
1	$x^6 + x^4 + 2x^2 + x + 2$
2	$x^6 + 2x^4 + x^2 + x + 2$

q = 3, $m = 2$, $n = 7$: $a = 1:\ x^7 + x^5 + x + 1, \qquad a = 2:\ x^7 + 2x^5 + 1.$

q = 3, $m = 3$, $n = 7$: $a = 1:\ x^7 + x^6 + x^3 + 2x^2 + x + 1, \qquad a = 2:\ x^7 + x^6 + 2x^3 + x^2 + 2x + 1.$

q = 2, $m = 2$, $n = 8$: $f(x) = x^8 + x^6 + x^3 + x^2 + 1$

q = 2, $m = 2$, $n = 6$: $f(x) = x^6 + x^4 + x^3 + x + 1$

q = 2, $m = 3$, $n = 7$: $f(x) = x^7 + x^4 + 1$

q = 2, $m = 3$, $n = 8$: $f(x) = x^8 + x^5 + x^3 + x + 1$

References

[1] Gilberto Bini and Flaminio Flamini. *Finite commutative rings and their applications*. The Kluwer International Series in Engineering and Computer Science, 680. Kluwer Academic Publishers, Boston, MA, 2002. With a foreword by Dieter Jungnickel.

[2] Todd Cochrane and Christopher Pinner. Using Stepanov's method for exponential sums involving rational functions. *J. Number Theory*, 116(2):270–292, 2006.

[3] Stephen D. Cohen. Primitive roots in the quadratic extension of a finite field. *J. London Math. Soc. (2)*, 27(2):221–228, 1983.

[4] Stephen D. Cohen. Generators in cyclic difference sets. *J. Combin. Theory Ser. A*, 51(2):227–236, 1989.

[5] Stephen D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.

[6] Stephen D. Cohen. Gauss sums and a sieve for generators of Galois fields. *Publ. Math. Debrecen*, 56(3-4):293–312, 2000. Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday.

[7] Stephen D. Cohen. Primitive polynomials over small fields. In *Finite fields and applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 197–214. Springer, Berlin, 2004.

[8] Stephen D. Cohen. Primitive polynomials with a prescribed coefficient. *Finite Fields Appl.*, 12(3):425–491, 2006.

[9] Stephen D. Cohen and Sophie Huczynska. Primitive free quartics with specified norm and trace. *Acta Arith.*, 109(4):359–385, 2003.

[10] Stephen D. Cohen and Charles King. The three fixed coefficient primitive polynomial theorem. *JP J. Algebra Number Theory Appl.*, 4(1):79–87, 2004.

[11] Stephen D. Cohen and Donald Mills. Primitive polynomials with first and second coefficients prescribed. *Finite Fields Appl.*, 9(3):334–350, 2003.

[12] Stephen D. Cohen and Mateja Prešern. Primitive finite field elements with prescribed trace. *Southeast Asian Bull. Math.*, 29(2):283–300, 2005.

[13] Stephen D. Cohen and Mateja Prešern. Primitive polynomials with prescribed second coefficient. *Glasg. Math. J.*, 48(2):281–307, 2006.

[14] Stephen D. Cohen and Mateja Prešern. The Hansen–Mullen primitivity conjecture: completion of proof. In *Number theory and polynomials.* Editors James McKee and Chris Smyth, LMS Lecture notes (No. 352). To appear in February 2008.

[15] Shuqin Fan and Wenbao Han. Character sums over Galois rings and primitive polynomials over finite fields. *Finite Fields Appl.*, 10(1):36–52, 2004.

[16] Shuqin Fan and Wenbao Han. Primitive polynomial with three coefficients prescribed. *Finite Fields Appl.*, 10(4):506–521, 2004.

[17] Reinaldo E. Giudici and Claudio Margaglio. A geometric characterization of the generators in a quadratic extension of a finite field. *Rend. Sem. Mat. Univ. Padova*, 62:103–114, 1980.

[18] Wen Bao Han. The coefficients of primitive polynomials over finite fields. *Math. Comp.*, 65(213):331–340, 1996.

[19] Tom Hansen and Gary L. Mullen. Primitive polynomials over finite fields. *Math. Comp.*, 59(200):639–643, S47–S50, 1992.

[20] Sophie Huczynska and Stephen D. Cohen. Primitive free cubics with specified norm and trace. *Trans. Amer. Math. Soc.*, 355(8):3099–3116 (electronic), 2003.

[21] Dieter Jungnickel and Scott A. Vanstone. On primitive polynomials over finite fields. *J. Algebra*, 124(2):337–353, 1989.

[22] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[23] Wen-Ching Winnie Li. Character sums over p-adic fields. *J. Number Theory*, 74(2):181–229, 1999.

[24] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[25] Donald Mills. Existence of primitive polynomials with three coefficients prescribed. *JP J. Algebra Number Theory Appl.*, 4(1):1–22, 2004.

[26] M. Ram Murty. *Introduction to p-adic analytic number theory*, volume 27 of *AMS/IP Studies in Advanced Mathematics*. American Mathematical Society, Providence, RI, 2002.

[27] Fan Shuqin and Han Wenbao. Primitive polynomials over finite fields of characteristic two. *Appl. Algebra Engrg. Comm. Comput.*, 14(5):381–395, 2004.

[28] Zhe-Xian Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Co. Inc., River Edge, NJ, 2003.