



UNIVERSITY OF CRETE
SCHOOL OF SCIENCES AND ENGINEERING
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS

DOCTORAL THESIS

*Polynomials with Special Properties
over Finite Fields*

GIORGOS N. KAPETANAKIS

ADVISOR: THEODOULOS GAREFALAKIS

HERAKLION
2014

*To my family Nikos, Maria and Eri
and to the memory of my uncle
Dimitris*

Committee

PhD advisory committee

- Theodoulos Garefalakis, Associate Professor, Department of Mathematics and Applied Mathematics, University of Crete, Greece (Advisor).
- Aristides Kontogeorgis, Associate Professor, Department of Mathematics, National and Kapodistrian University of Athens, Greece.
- Nikos Tzanakis, Professor, Department of Mathematics and Applied Mathematics, University of Crete, Greece.

Dissertation committee

- Jannis Antoniadis, Professor, Department of Mathematics and Applied Mathematics, University of Crete, Greece.
- Maria Chlouveraki, Assistant Professor, Laboratoire de Mathématiques, Université de Versailles - St. Quentin, France.
- Dimitrios Dais, Associate Professor, Department of Mathematics and Applied Mathematics, University of Crete, Greece.
- Dimitrios Poulakis, Professor, Department of Mathematics, Aristotle University of Thessaloniki, Greece.




Acknowledgments

First of all, I wish to thank my supervisor Prof. Theodoulos Garefalakis, not only for his support, patience, encouragement and the fruitful conversations we had, but also for constantly motivating me and introducing me to the world of finite fields and their wonderful international academic community, to which I am also grateful for many reasons. I also note that the work present in Chapter 3 of this thesis is joint with him.

I also wish to thank Profs. Alexis Kouvidakis and Nikos Tzanakis from the University of Crete and Profs. Evangelos Raptis and Dimitris Varsos from the University of Athens for doing their best in teaching me algebra. Additionally, I would like to thank the academic staff of the (former) Department of Mathematics of the University of Crete for sustaining a great productive academic environment, even in those difficult times. Last but not least, I wish to thank Athanasios Triantis; it was my honor to learn from a so committed mathematician and teacher in my high-school years.

I also wish to thank my parents Nikos and Maria and my sister Eri for their support, encouragement and trust in my abilities and my beloved uncle Dimitris, who passed away in 2012, for making it impossible to count the reasons that I am grateful to him and for being one of the most wonderful persons I ever met. This thesis is naturally dedicated to my family and my uncle Dimitris. Additionally, I wish to thank my girlfriend, Popi, for making this journey far more interesting, challenging and pleasant. I also wish to thank *all* my friends, but especially Thanos Tsouanas, who mentioned me in both his MSc and PhD theses.

Finally, I wish to thank Maria Michael Manassaki Foundation and the University of Crete's Special Research Account (research grand No. 3744) for their support.

EXCLUSIVELY FREE (AS IN FREEDOM) AND OPEN-SOURCE SOFTWARE WAS USED, RUNNING ON LINUX  MACHINES. NON-TRIVIAL (AND SOME TRIVIAL :-)) CALCULATIONS WERE PERFORMED WITH SAGE . TYPESET WAS DONE WITH X_YLA_TE_X, USING THE LINUX LIBERTINE FONT .

Abstract

In this work, we are interested in the existence of polynomials with special properties over finite fields. In Chapter 2 some background material is presented. We present some basic concepts of characters of finite abelian groups and we prove some basic results. Next, we focus on Dirichlet characters and on the characters of the additive and the multiplicative groups of a finite field. We conclude this chapter with an expression of the characteristic function of generators of cyclic R -modules, where R is a Euclidean domain, known as Vinogradov's formula.

In Chapter 3, we consider a special case of the Hansen-Mullen conjecture. In particular, we consider the existence of self-reciprocal monic irreducible polynomials of degree $2n$ over \mathbb{F}_q , where q is odd, with some coefficient prescribed. First, we use Carlitz's characterization of self-reciprocal polynomials over odd finite fields and, with the help of Dirichlet characters, we prove asymptotic conditions for the existence of polynomials with the desired properties. As a conclusion, we restrict ourselves to the first $n/2$ (hence also to the last $n/2$) coefficients, where our results are more efficient, and completely solve the resulting problem.

In Chapter 4 we extend the primitive normal basis theorem and its strong version. Namely, we consider the existence of polynomials whose roots are simultaneously primitive, produce a normal basis and some given Möbius transformation of those roots also produce a normal basis. First, we characterize elements with the desired properties and with the help of characters, we end up with some sufficient conditions, which we furtherly relax using sieving techniques. In the end, we prove our desired results, with roughly the same exceptions as the ones appearing in the strong primitive normal basis theorem.

In Chapter 5, we work in the same pattern as in Chapter 4, only here we demand that the Möbius transformation of the roots of the polynomial is also primitive. We roughly follow the same steps and prove that there exists a polynomial over a finite field such that its roots are simultaneously primitive and produce a normal basis and some given Möbius transformation of its roots also possess both properties, given that the cardinality of the field and the degree of the polynomial are large enough.

Keywords: finite field, primitive element, normal basis, free element, self-reciprocal polynomials, character sums, Hansen-Mullen conjecture

2010 MSC: 11T30, 12E05, 11T06, 11T24, 12E20, 12E10

Contents

Committee	v
Acknowledgments	vii
Abstract	ix
Contents	1
1 Introduction	3
1.1 The Hansen-Mullen conjecture	4
1.2 Extending the (strong) primitive normal basis theorem	4
2 Background material	7
2.1 Characters and character sums	7
2.1.1 Dirichlet characters	8
2.1.2 Additive and multiplicative characters	11
2.2 Vinogradov's formula	13
3 The H-M conjecture for self-reciprocal irreducible polynomials	17
3.1 Preliminaries	17
3.2 Weighted sum	19
3.3 The restriction $k \leq n/2$	22
4 Extending the (strong) primitive normal basis theorem I	25
4.1 Some estimates	25
4.2 The sieve	29
4.3 The case $m = 2$	31
4.4 Evaluations	32
4.5 Completion of the proof	39
5 Extending the (strong) primitive normal basis theorem II	45
5.1 Some estimates	45
5.1.1 Matrices that are neither upper triangular nor anti-diagonal	46

5.1.2	Upper triangular matrices that are not diagonal	48
5.1.3	Anti-diagonal matrices	50
5.1.4	Diagonal matrices	51
5.2	The sieve	52
5.3	Evaluations	55
A	Computer input and output	61
A.1	Computations of Chapter 3	61
A.2	Computations of Chapter 4	63
A.3	Computations of Chapter 5	75
	Bibliography	85
	Index	89

CHAPTER 1

Introduction

In this thesis, some existence results for irreducible polynomials over finite fields, with special properties are shown. These properties include combinations of primitiveness, freeness (i.e. a root of the polynomial form a normal basis) and having some coefficients prescribed. Also, since an irreducible polynomial over a finite field is fully characterized by its roots, we consider the roots of the polynomials, instead of the polynomials themselves, if such a replacement is convenient or natural. In particular, we study the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials and we extend the primitive normal basis theorem and its strong version.

Although the origins of the study of finite fields are found in antiquity, the formal study of finite fields has its roots in beginning of the 19th century and Gauss' book *Disquisitiones Arithmeticae* [29]. The first thought to extensively work on finite fields was, a few years later, Galois in *Sur la théorie des nombres* [22]. This work is a landmark to the subject and, consequently, many authors use the term *Galois field* to denote a finite field. The interested reader is referred to [48, Chapter 1] and the references therein for more detailed coverage of the history of the theory of finite fields.

Throughout this thesis, \mathbb{F}_q will stand for the finite field of q elements, \mathbb{F}_{q^m} for its extension of degree m , where $m \geq 1$ and \mathbb{F}_p as its prime field. It is well-known that p should be a prime number, also known as the *characteristic* of all the mentioned finite fields, and q should power of p . The polynomial ring over a finite field, besides its great theoretical interest, also has numerous important applications, including efficient computation in finite fields, fast Fourier transform, coding theory and cryptography.

The main idea behind our techniques dates back to the 50's and the work of Carlitz [2, 3], yet remains popular among authors in this line of research. Namely, first, we express the characteristic or a characteristic-like function for a polynomial (or its roots) with the desired properties with help of characters and we end up with a sufficient condition for the existence of our desired polynomial. This leads us to asymptotic results, with the the help of characters sum estimates and, if necessary and desirable, we deal with the remaining cases with a case-by-case approach. The interested reader is referred to recent survey articles [10, 36] and the references therein for detailed cov-

erage of this, very active, line of research and the techniques involved.

1.1 The Hansen-Mullen conjecture

Our main work on the Hansen-Mullen conjecture is presented in Chapter 3. Also, we note that this work is joint work with Garefalakis and published in [27, 28].

Hansen and Mullen [32] conjectured that there exists an irreducible polynomial over \mathbb{F}_q with an arbitrary coefficient prescribed, with a couple of obvious exceptions.

Conjecture 1.1 (Hansen-Mullen). Let $a \in \mathbb{F}_q$, let $n \geq 2$ and fix $0 \leq j < n$. Then there exists an irreducible polynomial $P(X) = X^n + \sum_{k=0}^{n-1} P_k X^k$ over \mathbb{F}_q with $P_j = a$ except when $j = a = 0$ or q even, $n = 2$, $j = 1$, and $a = 0$.

By considering primitive polynomials with given trace, Cohen [7] proved that the conjecture is true for $j = n - 1$, while Hansen and Mullen proved their conjecture for $j = 1$. Shortly after, Wan [57] proved that the conjecture holds, for $q > 19$ or $n \geq 36$ and Ham and Mullen [31] proved the remaining cases with the help of computers, completing the proof of the Hansen-Mullen conjecture. Those cases have also been settled theoretically by Cohen and Prešern [14, 15]. Several extensions of this result have also been shown [24, 26, 49]. The interested reader is referred to [48, Section 3.5] and the references therein for a more complete coverage of recent results on prescribing coefficients of irreducible polynomials over finite fields.

Given a polynomial $Q \in \mathbb{F}_q[X]$, its *reciprocal* Q^R is defined as

$$Q^R(X) = X^{\deg(Q)} Q(1/X).$$

One class of polynomials that has been intensively investigated [4, 8, 26, 46, 47, 61] is that of *self-reciprocal irreducible polynomials*, that is, irreducible polynomials that satisfy $Q^R(X) = Q(X)$. Besides the theoretical interest in their existence and density, self-reciprocal irreducible polynomials have been useful in applications, and in particular in the construction of error-correcting codes [34, 45].

It is natural to expect that self-reciprocal monic irreducible polynomials over finite fields, with some coefficient fixed, exist. Here, we restrict ourselves to the case where q is odd and prove that there exists a self-reciprocal irreducible monic polynomial over \mathbb{F}_q , of degree $2n$ with its k -th coefficient prescribed, provided that

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5}k(k+5) + \frac{1}{2}.$$

With this result in mind, we show, see Theorem 3.11, that for odd q and $n \geq 3$, we can prescribe the k -th coefficient of a self-reciprocal irreducible polynomial of degree $2n$, provided that $k \leq \lfloor n/2 \rfloor$, with a small number of genuine exceptions. The proof of the main theorem is based on an estimate of a weighted sum, which is very similar to the one that Wan [57] considers. Our main tools are Weil's bound for character sums, Carlitz's [4] characterization of self-reciprocal irreducible monic polynomials over \mathbb{F}_q and a character sum estimate proved in [26].

1.2 Extending the (strong) primitive normal basis theorem

Our main work on extending the primitive normal basis theorem and its strong version is presented in Chapters 4 and 5. The work in Chapter 4 is published in [41] and

the work in Chapter 5 is published in [40].

A generator of the multiplicative group $\mathbb{F}_{q^m}^*$ is called *primitive*. It is well-known that primitive elements exist for every q and m , see [44, Theorem 2.8]. Besides their theoretical interest, primitive elements of finite fields are widely used in various applications, including cryptographic schemes, such as the Diffie-Hellman key exchange [17], and the construction of Costas arrays [30], used in sonar and radar technology.

An element $x \in \mathbb{F}_{q^m}$ is called *free over \mathbb{F}_q* (or just *free* if such a simplification is not confusing) if the set $\{x, x^q, x^{q^2}, \dots, x^{q^{m-1}}\}$ is an \mathbb{F}_q -basis of \mathbb{F}_{q^m} , once we view the latter as an \mathbb{F}_q -vector space. Such a basis is called *normal*. Hensel [33], in 1888, proved the existence of normal basis for arbitrary finite field extensions. This result is known as the *normal basis theorem* (also see [44, Theorem 2.35]) in modern literature. Hensel also observed their computational advantages for finite field arithmetic. Naturally, a number of software and hardware implementations, used mostly in coding theory and cryptography, make use of normal basis. For further information on normal basis and some of their applications, we refer to [23] and the references therein.

It is not hard to see that both primitiveness and freeness are properties common to either all or none of the roots of some given irreducible polynomial of \mathbb{F}_q of degree m , hence one can define *primitive polynomials* and *free polynomials* naturally, while the existence of primitive or free elements implies the existence of primitive or free polynomials respectively and vice versa. Here, it is worth noting that Hansen and Mullen [32], also conjectured the existence of monic primitive polynomials with prescribed coefficients, with a few exceptions. This has also been shown to be true, see [36, Section 2.4] and the references therein for a detailed account of this result.

As already stated both primitive and free elements exist for every q and m . The existence of elements that are simultaneously primitive and free is also well-known.

Theorem 1.2 (Primitive normal basis theorem). *Let q be a prime power and m a positive integer. There exists some $x \in \mathbb{F}_{q^m}$ that is simultaneously primitive and free over \mathbb{F}_q .*

Lenstra and Schoof [43] were the first to provide a complete proof of the above, completing partial proofs of Carlitz [2, 3] and Davenport [16]. Recently, Cohen and Huczynska [12] provided a computer-free proof, with the help of sieving techniques, previously introduced by Cohen [9]. Also, several generalizations of Theorem 1.2 have been investigated [11, 35, 37, 58]. A family of extensions of the above, that is of special interest for us, is the consideration of primitive and free polynomials with their coefficients prescribed [18, 19, 20, 21]. More recently, an even stronger result was shown.

Theorem 1.3 (Strong primitive normal basis theorem). *Let q be a prime power and m a positive integer. There exists some $x \in \mathbb{F}_{q^m}$ such that x and x^{-1} are both simultaneously primitive and free over \mathbb{F}_q , unless the pair (q, m) is one of $(2, 3)$, $(2, 4)$, $(3, 4)$, $(4, 3)$ or $(5, 4)$.*

Tian and Qi [56] were the first to prove this result for $m \geq 32$, but Cohen and Huczynska [13] were those who extended it to its stated form, once again with the help of their sieving techniques.

We consider an action of $\text{GL}_2(\mathbb{F}_q)$, the group of 2×2 invertible matrices over \mathbb{F}_q , on irreducible polynomials over \mathbb{F}_q of degree at least 2. More specifically, set $\mathbb{I}_n := \{F \in \mathbb{F}_q[X] : F \text{ irreducible of degree } n\}$ and let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$ and $F \in \mathbb{I}_n$, $n \geq 2$. We define

$$A \circ F(X) := (-cX + a)^n F\left(\frac{dX - b}{-cX + a}\right).$$

It is not hard to check that $I \circ F = F$ and that $(AB) \circ F = A \circ (B \circ F)$ for all $A, B \in \text{GL}_2(\mathbb{F}_q)$ and $F \in \mathbb{F}_q[X]$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. It follows that the above rule does indeed define an action of $\text{GL}_2(\mathbb{F}_q)$ on \mathbb{I}_n , $n \geq 2$. The problem of the enumeration of the fixed points of this action has recently gained attention [25, 55].

In this work we are interested in whether there exists a primitive $F \in \mathbb{F}_q[X]$, of degree m such that F and $A \circ F$ are simultaneously free and we are also interested whether there exists an $F \in \mathbb{F}_q[X]$, of degree m such that both F and $A \circ F$ are simultaneously primitive and free. Moreover, for fixed $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$ one easily checks that $x \in \mathbb{F}_{q^m}$ is a root of $F(X) \in \mathbb{I}_m$ if and only if $(ax+b)/(cx+d)$, the Möbius transformation of x that A defines, is a root of $A \circ F$. Further, it turns out to be easier to check the existence of the roots of the polynomials mentioned, than the polynomials themselves. It follows that our problems can be restated as follows.

Problem 1.4. Let q be a prime power, m a positive integer and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$. Does there exist some primitive $x \in \mathbb{F}_{q^m}$ such that both x and $(ax+b)/(cx+d)$ are free over \mathbb{F}_q ?

Problem 1.5. Let q be a prime power, m a positive integer and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$. Does there exist some $x \in \mathbb{F}_{q^m}$ such that both x and $(ax+b)/(cx+d)$ are simultaneously primitive and free over \mathbb{F}_q ?

Here we note, that the two problems are similar, but not identical, i.e. Problem 1.4 has three conditions (x is primitive, x is free over \mathbb{F}_q and $(ax+b)/(cx+d)$ is free over \mathbb{F}_q), while Problem 1.5 has four conditions, the three conditions of Problem 1.4 plus the condition of $(ax+b)/(cx+d)$ to be primitive. Another note is that both problems qualify as extensions to both Theorems 1.2 and 1.3. This is clear for Theorem 1.2. To make it clear for Theorem 1.3, notice that although Theorem 1.3 seems to have four conditions (x is primitive, x is free over \mathbb{F}_q , x^{-1} is primitive and x^{-1} is free over \mathbb{F}_q) it has just three genuine conditions, since the two conditions of x to be primitive and x^{-1} to be primitive overlap.

In Chapter 4 we solve Problem 1.4 completely, see Theorem 4.25. Namely, we prove that the problem can be answered positively, with the exception of an explicit small list of genuine exceptions. In Chapter 5 we partially solve Problem 1.5, see Theorem 5.22. In particular, we show that the problem can be answered positively, when q and m are large enough.

CHAPTER 2

Background material

In this chapter we present some necessary background material. The results presented here are well-known.

2.1 Characters and character sums

Characters and character sums play a crucial role in characterizing polynomials and elements of finite fields with the desired properties and in estimating the number of elements and polynomials who combine all the desired properties. The definition of a character is essential.

Definition 2.1. Let \mathfrak{G} be a finite abelian group. A *character* of \mathfrak{G} is a group homomorphism $\mathfrak{G} \rightarrow \mathbb{C}^*$, where \mathbb{C}^* stands for the multiplicative group of \mathbb{C} . The characters of \mathfrak{G} form a group under multiplication, which is isomorphic to \mathfrak{G} . This group is called the *dual* of \mathfrak{G} and denoted by $\widehat{\mathfrak{G}}$. Furthermore, the character $\chi_0 : \mathfrak{G} \rightarrow \mathbb{C}^*$, where $\chi_0(g) = 1$ for all $g \in \mathfrak{G}$, is called the *trivial character* of \mathfrak{G} . Finally, by $\bar{\chi}$ we denote the inverse of χ .

The interested reader is referred to classic textbooks [38, 44, 52] for an in-depth study of the wonderful world of characters.

A *character* or *exponential sum* is a sum that involves characters. Later, characters will be used to characterize elements with the desired properties and character sums will come up, hence a computation, or at least an estimate, of such sums will be necessary. The simplest, albeit very important, form of character sum is presented in the following lemma.

Lemma 2.2 (Orthogonality relations). *Let χ be a non-trivial character of a group \mathfrak{G} and g a non-trivial element of \mathfrak{G} . Then*

$$\sum_{x \in \mathfrak{G}} \chi(x) = 0 \quad \text{and} \quad \sum_{\chi \in \widehat{\mathfrak{G}}} \chi(g) = 0.$$

Proof. Since χ is non-trivial, there exists some $h \in \mathfrak{G}$ with $\chi(h) \neq 1$. We have that

$$\chi(h) \sum_{x \in \mathfrak{G}} \chi(x) = \sum_{x \in \mathfrak{G}} \chi(hx) = \sum_{x \in \mathfrak{G}} \chi(x),$$

because as x runs through \mathfrak{G} , so does hx . It follows that

$$(\chi(h) - 1) \sum_{x \in \mathfrak{G}} \chi(x) = 0,$$

which implies the first of the two equations in question, since $\chi(h) \neq 1$. For the second part, we observe that the function $\hat{g} : \widehat{\mathfrak{G}} \rightarrow \mathbb{C}^*$, $\chi \mapsto \chi(g)$ is a well-defined non-trivial character of $\widehat{\mathfrak{G}}$. It follows, from what we have already proven, that

$$\sum_{\chi \in \widehat{\mathfrak{G}}} \chi(g) = \sum_{\chi \in \widehat{\mathfrak{G}}} \hat{g}(\chi) = 0. \quad \square$$

Remark 2.3. The orthogonality relations are true for an arbitrary group \mathfrak{G} .

In the proceeding subsections, we present characters and character sums of specific groups.

2.1.1 Dirichlet characters

A useful concept is that of a Dirichlet character modulo F , where $F \in \mathbb{F}_q[X]$. Dirichlet characters are originally defined over \mathbb{Z} , the ring of integers, but one can easily define Dirichlet characters for $\mathbb{F}_q[X]$, the polynomial ring of \mathbb{F}_q .

Definition 2.4. Given some $F \in \mathbb{F}_q[X]$, a *Dirichlet character modulo F* is a function $\chi : \mathbb{F}_q[X] \rightarrow \mathbb{C}^*$, such that

1. $\chi(G + FH) = \chi(G)$,
2. $\chi(GH) = \chi(G)\chi(H)$ and
3. $\chi(G) \neq 0 \iff (G, F) = 1$,

for every $G, H \in \mathbb{F}_q[X]$.

Remark 2.5. Clearly, Dirichlet characters modulo F are essentially the characters of $(\mathbb{F}_q[X]/F\mathbb{F}_q[X])^*$, extended to zero. Also, there is a bijection between Dirichlet characters modulo F and homomorphisms $(\mathbb{F}_q[X]/F\mathbb{F}_q[X])^* \rightarrow \mathbb{C}^*$.

Let $M \in \mathbb{F}_q[X]$ be a polynomial of degree at least 1 and suppose χ is a non-trivial Dirichlet character modulo M . The *Dirichlet L -function* associated with χ is defined to be

$$\mathcal{L}(s, \chi) = \sum_{F \in \mathbb{F}_q[X] \text{ monic}} \frac{\chi(F)}{|F|^s}, \quad s \in \mathbb{C}, \Re(s) > 1,$$

where $|F| = q^{\deg(F)}$ is the *absolute value* of the polynomial F . By using Lemma 2.2, it is not hard to show, see [51, Proposition 4.3], that the above is a polynomial in q^{-s} , of degree $\deg(M) - 1$. By making the substitution $u = q^{-s}$, and noting that the constant term of that polynomial has to be equal to 1, we conclude that

$$\mathcal{L}(s, \chi) = L(u, \chi) = \sum_{n=0}^{\infty} \left(\sum_{\substack{F \text{ monic} \\ \deg(F)=n}} \chi(F) \right) u^n = \prod_{i=1}^{\deg(M)-1} (1 - \pi_i(\chi)u), \quad (2.1)$$

where the π_i 's are the inverses of the roots of $L(u, \chi)$. The following theorem follows from the Riemann hypothesis for function fields and is the function field equivalent of the generalized Riemann hypothesis.

Theorem 2.6 (Weil). $|\pi_i(\chi)| \in \{1, \sqrt{q}\}$.

Weil [60] originally proved this result and gave two proofs, both using algebraic geometric techniques. Later, Bombieri [1] gave an elementary proof of the above. For more information on the Riemann hypothesis for function fields, the interested reader is referred to [39, 51, 54].

Since χ is completely multiplicative, it follows that the power series expression of $L(u, \chi)$ in Eq. (2.1) can be expressed as an Euler product, as

$$L(u, \chi) = \prod_{d=1}^{\infty} \prod_{\substack{P \text{ monic irreducible} \\ \deg(P)=d}} (1 - \chi(P)u^d)^{-1}.$$

Taking the logarithmic derivative of $L(u, \chi)$ and multiplying by u , we obtain a series

$$\sum_{d=1}^{\infty} \sum_{\substack{P \text{ monic irreducible} \\ \deg(P)=d}} d \cdot \frac{\chi(P)u^d}{1 - \chi(P)u^d} = \sum_{d=1}^{\infty} \sum_{\substack{P \text{ monic irreducible} \\ \deg(P)=d}} \sum_{n=1}^{\infty} d(\chi(P)u^d)^n,$$

since $|\chi(P)u| < 1$. The latter can be rewritten as $\sum_{n=1}^{\infty} c_n(\chi)u^n$, with

$$c_n(\chi) = \sum_{d|n} \frac{n}{d} \sum_{\substack{P \text{ monic irreducible} \\ \deg(P)=n/d}} \chi(P)^d.$$

We follow the same steps, i.e. take the logarithmic derivative and multiply by u , in the polynomial expression of $L(u, \chi)$ in (2.1). This leads us to the series

$$\sum_{n=1}^{\infty} \left(\sum_{i=1}^{\deg(M)-1} \pi_i(\chi)^n \right) u^n.$$

The above, combined with Theorem 2.6 imply the following theorem.

Theorem 2.7. *Let χ be a Dirichlet character modulo M . Then*

1. *If $\chi \neq \chi_0$ then*

$$|c_n(\chi)| \leq (\deg(M) - 1)q^{\frac{n}{2}}.$$

2. *If $\chi \neq \chi_0$ and $\chi(\mathbb{F}_q^*) = 1$, then*

$$|1 + c_n(\chi)| \leq (\deg(M) - 2)q^{\frac{n}{2}}.$$

For a detailed account of the above well-known facts, see [51, Chapters 4 and 9]. We will also need the following result of [26].

Theorem 2.8 (Garefalakis). *Let $\psi(P) = (P|X^2 - 4)$ be the Jacobi symbol of P modulo $X^2 - 4$ and χ be a non-trivial Dirichlet character modulo X^{k+1} , where $k \geq 1$. The following bounds hold:*

1. For every $n \in \mathbb{N}$, $n \geq 2$,

$$\left| \sum_{\substack{P \text{ monic irreducible} \\ \psi(P)=-1}} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}.$$

2. For every $n \in \mathbb{N}$, $n \geq 2$, n odd,

$$\left| \sum_{\substack{P \text{ monic irreducible} \\ \psi(P)=1}} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}.$$

For $H \in \mathbb{F}_q[X]$, we define the *von Mangoldt function* as

$$\Lambda(H) = \begin{cases} \deg(P), & \text{if } H \text{ is a power of the irreducible } P, \\ 1, & \text{if } H = 1, \\ 0, & \text{otherwise.} \end{cases}$$

It follows directly from the definition of Λ , that

$$c_n(\chi) = \sum_{\substack{H \text{ monic} \\ \deg(H)=n}} \Lambda(H)\chi(H).$$

We will encounter character sums, which involve a character χ that is trivial on \mathbb{F}_q^* , and where the sums run over polynomials with constant term equal to 1 (not necessarily monic). Estimates for such character sums, follow directly from the estimates of the related sums that run over monic polynomials. Since our focus will be on Dirichlet characters modulo X^{k+1} , we state our proposition accordingly.

Proposition 2.9. *Let $n, k \in \mathbb{N}$, $1 \leq k \leq n$ and let χ be a non-trivial Dirichlet character modulo X^{k+1} , such that $\chi(\mathbb{F}_q^*) = 1$.*

$$\left| \sum_{\substack{\deg(H)=n \\ H_0=1}} \Lambda(H)\chi(H) \right| \leq 1 + kq^{\frac{n}{2}}, \quad \text{for } n \geq 1. \quad (2.2)$$

$$\left| \sum_{\substack{P \text{ irreducible} \\ P_0=1, \psi(P)=\epsilon}} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}, \quad \text{for } n \geq 2, \quad (2.3)$$

where either $\epsilon = -1$, or $\epsilon = 1$ and n is odd.

Proof. For Eq. (2.2), we note that as H runs over the polynomials of degree n with constant term 1, H/H_n runs over the monic polynomials of degree n . Taking into account that $\chi(\mathbb{F}_q^*) = 1$, we have

$$\left| \sum_{\substack{\deg(H)=n \\ H_0=1}} \Lambda(H)\chi(H) \right| = \left| \sum_{\substack{\deg(H)=n \\ H_0=1}} \Lambda(H)\chi\left(\frac{H}{H_n}\right) \right| = \left| \sum_{\substack{\deg(H)=n \\ H \text{ monic}}} \Lambda(H)\chi(H) \right|$$

and the bound follows from Theorem 2.7. For Eq. (2.3) the same observation applies, that is, as P runs over irreducible polynomials with constant term equal to 1, P/P_n runs over monic irreducible polynomials. Further, for any constant $c \in \mathbb{F}_q^*$, $\psi(c) = 1$. The bound in Eq. (2.3) now follows from Theorem 2.8 and the fact that ψ is completely multiplicative. \square

2.1.2 Additive and multiplicative characters

The arbitrary finite field \mathbb{F}_q is associated with two groups: its multiplicative group, which we denote by \mathbb{F}_q^* , and its additive group, which we denote by \mathbb{F}_q . From now on, we will call the characters of \mathbb{F}_q^* *multiplicative characters* and the characters of \mathbb{F}_q *additive characters*. Furthermore, we will denote by χ_0 and ψ_0 the trivial multiplicative and additive character respectively and we will extend the multiplicative characters to zero with the rule

$$\chi(0) := \begin{cases} 0, & \text{if } \chi \in \widehat{\mathbb{F}_q^*} \setminus \{\chi_0\}, \\ 1, & \text{if } \chi = \chi_0. \end{cases}$$

As already mentioned, the group of multiplicative characters is isomorphic to \mathbb{F}_q^* , hence cyclic. We denote a generator of this group by χ_g and call it a *generator character*. It follows that every non-trivial multiplicative character χ satisfies $\chi(x) = \chi_g(x^n)$ for some $1 \leq n \leq q^m - 2$. Another special multiplicative character is the *quadratic character*, denoted by τ , that is $\tau(x) = 1$ if and only if x is a square in \mathbb{F}_q and $\tau(x) = -1$ otherwise.

Similarly, it is not hard to see that the mapping $x \mapsto \exp(2\pi i \text{Tr}(yx)/p)$, where Tr stands for the absolute trace function from \mathbb{F}_q onto \mathbb{F}_p and $y \in \mathbb{F}_q$, is an additive character and, by noting that for different values of y different additive characters arise, we conclude that all additive characters are of that form. The trivial character corresponds to $y = 0$ and the *canonical character*, by definition, corresponds to $y = 1$ and is denoted by ψ_g . It follows that the arbitrary additive character ψ satisfies $\psi(x) = \psi_g(yx)$, for some $y \in \mathbb{F}_q$.

Suppose χ is a multiplicative character, ψ an additive character and $s \in \mathbb{Z}_{\geq 1}$. For $x \in \mathbb{F}_{q^{ms}}$, we define $\chi^{(s)}(x) := \chi(N_{\mathbb{F}_{q^{ms}}/\mathbb{F}_{q^m}}(x))$ and $\psi^{(s)}(x) := \psi(\text{Tr}_{\mathbb{F}_{q^{ms}}/\mathbb{F}_{q^m}}(x))$, where $N_{\mathbb{F}_{q^{ms}}/\mathbb{F}_{q^m}}$ stands for the norm function from $\mathbb{F}_{q^{ms}}$ to \mathbb{F}_{q^m} and $\text{Tr}_{\mathbb{F}_{q^{ms}}/\mathbb{F}_{q^m}}$ stands for the trace function from $\mathbb{F}_{q^{ms}}$ to \mathbb{F}_{q^m} and $\text{Tr}_{\mathbb{F}_{q^{ms}}/\mathbb{F}_{q^m}}$. It follows from the standard properties of norm and trace that $\chi^{(s)}$ and $\psi^{(s)}$ belong to $\widehat{\mathbb{F}_{q^{ms}}^*}$ and $\widehat{\mathbb{F}_{q^{ms}}}$ respectively and are known as the *lifted characters* that χ and ψ define.

We will use additive and multiplicative characters to conveniently express the characteristic functions of the properties we are interested in. As a natural consequence, some character sums of those types will emerge and a computation, or at least an estimation of those will be crucial. The following well-known results provides us with estimations of those sums.

The first two results were originally proved by Weil [59]. Later, Stepanov [53] introduced an elementary method, that was furtherly simplified by Schmidt [52], which is able to prove such results. Detailed description and demonstration of this method, known as the *Stepanov-Schmidt method*, can be found in classic textbooks [44, 52].

Theorem 2.10. *Let χ be a non-trivial multiplicative character of order n , and $F \in \mathbb{F}_{q^m}[X]$ such that $F \neq yH^{q^m-1}$, for any $y \in \mathbb{F}_{q^m}$ and $H \in \mathbb{F}_{q^m}[X]$. If F has l distinct roots (in its*

splitting field), then

$$\left| \sum_{x \in \mathbb{F}_{q^m}} \chi(F(x)) \right| \leq (l-1)q^{m/2}.$$

Rough sketch of the proof. If $l = 1$, the result follows immediately from Lemma 2.2. For $l \geq 2$, first assume that F is monic. Using the Stepanov-Schmidt method, we conclude that

$$\sum_{x \in \mathbb{F}_{q^{ms}}} \chi^{(s)}(F(x)) = -\omega_1^s - \cdots - \omega_{l-1}^s,$$

for all $s \in \mathbb{Z}_{\geq 1}$ and some $\omega_i \in \mathbb{C}^*$. Weil's theorem on the Riemann hypothesis for function fields, yields that for all i , we have that $|\omega_i| = q^{m/2}$ and the result follows, if we consider the case $s = 1$. If F is not monic, we multiply the original sum with $\chi(y^{-1})$, where y is the leading coefficient of F and we end up with a sum which has the same absolute value as the original and the polynomial involved is monic. \square

Lemma 2.11 (Kloosterman sums). *Let ψ be a non-trivial additive character. If $y_1, y_2 \in \mathbb{F}_{q^m}$ are not both zero, then*

$$\left| \sum_{x \in \mathbb{F}_{q^m}^*} \psi(y_1 x + y_2 x^{-1}) \right| \leq 2q^{m/2}.$$

Rough sketch of the proof. If exactly one of y_1, y_2 is zero, then Lemma 2.2 yields that our sum is -1 and the result follows. If both y_1, y_2 are non-zero, using the Stepanov-Schmidt method, we conclude that

$$\sum_{x \in \mathbb{F}_{q^{ms}}^*} \psi^{(s)}(y_1 x + y_2 x^{-1}) = -\omega_1^s - \omega_2^s,$$

for all $s \in \mathbb{Z}_{\geq 1}$ and some $\omega_i \in \mathbb{C}^*$. Weil's theorem on the Riemann hypothesis for function fields, yields that for $i = 1, 2$, we have that $|\omega_i| = q^{m/2}$ and the result follows, if we consider the case $s = 1$. \square

Remark 2.12. In both Theorem 2.10 and Lemma 2.11 one can avoid employing the Riemann hypothesis for function fields and use the estimate $|\omega_i| \leq q^{m/2}$, that can be deduced much easier and still provide enough to prove the desired bounds. Another interesting remark is that the Kloosterman sum is a real number, since

$$\overline{\sum_{x \in \mathbb{F}_{q^m}^*} \psi(y_1 x + y_2 x^{-1})} = \sum_{x \in \mathbb{F}_{q^m}^*} \psi(-y_1 x - y_2 x^{-1}) = \sum_{x \in \mathbb{F}_{q^m}^*} \psi(y_1 x + y_2 x^{-1}).$$

Kloosterman sums were introduced by Kloosterman [42], who achieved an estimate of order $p^{3/4}$ (where the sum run over the prime field \mathbb{F}_p). Weil [59] achieved the bound shown above, which can be shown that is the best possible. For a detailed account on Kloosterman sums, their history and generalizations the reader is referred to [44, p. 252–257]. We will also encounter *hybrid character sums*, that is character sums who involve an additive and a multiplicative character. The following theorem provides us with an estimate for such sums with rational functions as arguments.

Theorem 2.13. *Let χ be a non-trivial multiplicative character of order n and ψ be a non-trivial additive character. Let \mathcal{F}, \mathcal{G} be rational functions in $\mathbb{F}_{q^m}(X)$ such that $\mathcal{F} \neq y\mathcal{H}^n$, for any $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$, and $\mathcal{G} \neq \mathcal{H}^p - \mathcal{H} + y$, for any $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$. Then*

$$\left| \sum_{x \in \mathbb{F}_{q^m} \setminus S} \chi(\mathcal{F}(x)) \psi(\mathcal{G}(x)) \right| \leq (\deg(\mathcal{G})_\infty + l + l' - l'' - 2) q^{m/2},$$

where S is the set of poles of \mathcal{F} and \mathcal{G} , $(\mathcal{G})_\infty$ is the pole divisor of \mathcal{G} , l is the number of distinct zeros and finite poles of \mathcal{F} in $\overline{\mathbb{F}}_q$, l' is the number of distinct poles of \mathcal{G} (including ∞) and l'' is the number of finite poles of \mathcal{F} that are poles or zeros of \mathcal{G} .

A slightly weaker (lacking the term l'') version of the above theorem was initially proved by Perel'muter [50], but Castro and Moreno [5] improved the result to its stated form. Recently, Cochrane and Pinner [6] presented a proof, which utilizes the elementary Stepanov-Schmidt method, instead of concepts from algebraic geometry.

2.2 Vinogradov's formula

In this section, we present a generalization of a characterization of elements with special properties, attributed by modern bibliography, see [48, p. 183], to Vinogradov. Before going further, notice that $\mathbb{F}_{q^m}^*$ can also be seen as a \mathbb{Z} -module under the rule $r \circ x := x^r$, where $r \in \mathbb{Z}$ and $x \in \mathbb{F}_{q^m}^*$ and \mathbb{F}_{q^m} (the additive group), can be seen as an $\mathbb{F}_q[X]$ -module, under the rule $F \circ x := \sum_{i=0}^n F_i x^i$, where $F(X) = \sum_{i=0}^n F_i X^i \in \mathbb{F}_q[X]$ and $x \in \mathbb{F}_{q^m}$. The fact that primitive elements exist for every finite field and the normal basis theorem, imply that both modules are cyclic, while the elements that are interesting for us, i.e. primitive and free elements, are the generators of those modules. It is now clear that we are interested in characterizing generators of cyclic modules over Euclidean domains.

Let R be a Euclidean domain and \mathcal{M} be a cyclic finite R -module, under the rule $r \circ x$, where $r \in R$ and $x \in \mathcal{M}$. Further, let $g \in \mathcal{M}$ be an R -module generator of \mathcal{M} . By definition, \mathcal{M} has also the structure of an abelian group, hence $\widehat{\mathcal{M}}$ is well-defined and can also be seen as an R -module, under the rule $r \circ \chi : x \mapsto \chi(r \circ x)$, for $x \in \mathcal{M}$ and $\chi \in \widehat{\mathcal{M}}$, while it is not hard to show that $\widehat{\mathcal{M}}$ is also cyclic. Also, note that throughout this section we will coincide an element of R with its conjugates that the equivalence relation $r_1 \sim r_2 \iff r_1 = ur_2$, for some $u \in R^*$, defines. In particular, whenever a sum runs through the divisors of some element of R or when a definition applies to all the members of a conjugacy class of R/\sim , just one representative will be considered. This means that in the integer rings we will consider only positive numbers and in the polynomial ring we will consider only monic polynomials.

Let $x \in \mathcal{M}$. It follows from our assumptions that the annihilator of x is an ideal of R and, as such, has a unique generator. This is called the *order* of x and denoted by $\text{ord}(x)$. Set $m := \text{ord}(g)$. It follows that for every $x \in \mathcal{M}$, we have that $\text{ord}(x) \mid m$. The *order* of χ , where $\chi \in \widehat{\mathcal{M}}$, is defined accordingly.

Fix some $r \in R$, with $r \mid m$. We call $x \in \mathcal{M}$ *r-free* if $x = d \circ y$, for some $d \mid r$ and $y \in \mathcal{M}$ implies $d = 1$. Clearly, $x \in \mathcal{M}$ is an R -generator of \mathcal{M} if and only if it is m -free. The purpose of this section is to characterize r -free elements. For $d \in R$, the *Euler function* is defined as

$$\varphi(d) := |(R/dR)^*|.$$

Here note that one can find examples such that $\varphi(d) = \infty$; nonetheless in the cases we are interested in, that is $d \mid m$ where $m = \text{ord}(g)$, we have that $\varphi(d) < |(R/mR)| = |\mathcal{M}| < \infty$, since $\mathcal{M} \cong R/mR$. It is also clear that x has order $d \in R$, where $d \mid m$, if and only if $x = (fm/d) \circ g$ for some $f \in R$, co-prime to r , while for $f_1, f_2 \in R$, co-prime to r , $f_1 = f_2 + kd$ for some $k \in R$ if and only if $(f_1 m/d) \circ g = (f_2 m/d) \circ g$. It follows that for all $d \in R$, $d \mid m$, we have that

$$\sum_{\chi \in \widehat{\mathcal{M}}, \text{ord}(\chi)=d} 1 = \sum_{x \in \mathcal{M}, \text{ord}(x)=d} 1 = \varphi(d). \quad (2.4)$$

The *Möbius function* is defined as

$$\mu(d) := \begin{cases} (-1)^k, & \text{if } d \text{ is a product of } k \text{ distinct irreducible elements of } R, \\ 0, & \text{otherwise} \end{cases}$$

and for $d \mid m$, we define $\theta(d) := \varphi(d)/|(R/dR)|$. The following variation of Lemma 2.2 will prove to be useful.

Lemma 2.14. *Let $x \in \mathcal{M}$ be an r -free element and $d \in R$, with $d \mid r$. We have that*

$$\sum_{\chi \in \widehat{\mathcal{M}}, \text{ord}(\chi) \mid d} \chi(x) = 0.$$

Proof. Set $\mathcal{H} := d \circ \mathcal{M}$. Clearly, \mathcal{H} is an R -submodule of \mathcal{M} and the order of a character of \mathcal{M} divides d if and only if this character is trivial on \mathcal{H} . Further, it is not hard to see that there is a natural bijection between the characters of \mathcal{M}/\mathcal{H} and the characters of \mathcal{M} that are trivial on \mathcal{H} . It follows from Lemma 2.2, that

$$\sum_{\text{ord}(\chi) \mid d} \chi(x) = \sum_{\bar{\chi} \in \widehat{\mathcal{M}/\mathcal{H}}} \bar{\chi}(x + \mathcal{H}) = 0,$$

since $x + \mathcal{H} \neq 0 + \mathcal{H}$, since x is r -free. □

We are now in position to characterize r -free elements

Proposition 2.15. *The characteristic function for r -free elements is*

$$\omega_r : \mathcal{M} \rightarrow \mathbb{C}, \quad x \mapsto \theta(r') \sum_{d \mid r} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \widehat{\mathcal{M}}, \text{ord}(\chi)=d} \chi(x),$$

where r' stands for the square-free part of r .

Proof. First, observe that if d_1, d_2 are co-prime divisors of r' , then for all $x \in \mathcal{M}$, we have that

$$\omega_{d_1}(x) \omega_{d_2}(x) = \omega_{d_1 d_2}(x), \quad (2.5)$$

since

$$\begin{aligned} \omega_{d_1}(x) \omega_{d_2}(x) &= \theta(d_1) \theta(d_2) \left(\sum_{e \mid d_1} \frac{\mu(e)}{\varphi(e)} \sum_{\text{ord}(\chi)=e} \chi(x) \right) \left(\sum_{f \mid d_2} \frac{\mu(f)}{\varphi(f)} \sum_{\text{ord}(\psi)=f} \psi(x) \right) \\ &= \theta(d_1 d_2) \sum_{ef \mid d_1 d_2} \frac{\mu(ef)}{\varphi(ef)} \sum_{\text{ord}(\chi\psi)=ef} (\chi\psi)(x) = \omega_{d_1 d_2}(x). \end{aligned}$$

Also, notice that the Möbius function in the definition of ω_r ensures that r may be replaced by r' . This, along with Eq. (2.5) imply that

$$\omega_r(x) = \theta(r') \prod_{p|r, p \text{ irreducible}} \left(1 - \frac{1}{\varphi(p)} \sum_{\text{ord}(\chi)=p} \chi(x) \right). \quad (2.6)$$

Now, assume that x is not r -free, i.e. there exists some irreducible $p_1 \mid r$ such that $x = p_1 \circ y$ for some $y \in R$. Then for all $\chi \in \widehat{\mathcal{M}}$ of order p_1 we have that $\chi(x) = (p_1 \circ \chi)(y) = 1$ and Eqs. (2.4) and (2.6) imply $\omega_r(x) = 0$.

Finally, assume that x is r -free. It follows from Lemma 2.14 that $\sum_{\text{ord}(\chi)=p} \chi(x) = -1$ for all irreducible $p \mid r$ and Eq. (2.6) gives

$$\omega_r(x) = \prod_{p|r, p \text{ irreducible}} \theta(p) \cdot \frac{\varphi(p) + 1}{\varphi(p)} = \prod_{p|r, p \text{ irreducible}} 1 = 1,$$

since for p irreducible, we have that R/pR is a field, thus $\varphi(p) + 1 = |R/pR|$. \square

Now it is time to return to the finite field case and to the two modules that we are interested in, namely \mathbb{F}_{q^m} and $\mathbb{F}_{q^m}^*$.

From now on, we call *Order* of $x \in \mathbb{F}_{q^m}$ (note the big 'O') its additive order, that is its order of an element of the $\mathbb{F}_q[X]$ -module \mathbb{F}_{q^m} , and denote it by $\text{Ord}(x)$. This means that $\text{Ord}(x) \in \mathbb{F}_q[X]$ and $\text{Ord}(x) \mid X^m - 1$. Further, we can also assume that $\text{Ord}(x)$ is monic for all $x \in \mathbb{F}_{q^m}$. The *Order* of the additive character ψ is defined accordingly. Moreover, for $G \mid X^m - 1$, we call $x \in \mathbb{F}_{q^m}$ *G-free*, if $x = H \circ y$ for some $y \in \mathbb{F}_{q^m}$ and $H \mid G$, implies $H = 1$. According to Proposition 2.15, the characteristic function of G -free elements is

$$\Omega_G : \mathbb{F}_{q^m} \rightarrow \mathbb{C}, \quad x \mapsto \theta(G') \sum_{F|G, F \text{ monic}} \frac{\mu(F)}{\varphi(F)} \sum_{\psi \in \widehat{\mathbb{F}_{q^m}}, \text{Ord}(\psi)=F} \psi(x),$$

where G' is the square-free part of G , and μ , φ and θ are defined appropriately. Here, we also note that elements that generate normal basis are exactly those that have *Order* equal to $X^m - 1$, i.e. those that are $(X^m - 1)$ -free, or F_0 -free, where F_0 is the square-free part of $X^m - 1$, i.e. $F_0 := X^{m_0} - 1$, where m_0 is such that $m = m_0 p^b$ and $(m_0, p) = 1$.

Similarly, *order* of $x \in \mathbb{F}_{q^m}^*$ (note the small 'o') stands for the multiplicative order of x and denoted by $\text{ord}(x)$. This means that $\text{ord}(x) \in \mathbb{Z}_{>0}$ and $\text{ord}(x) \mid q^m - 1$. The *order* of a multiplicative character is defined naturally. Also, for $r \mid q^m - 1$, we call x *r-free*, if $w \mid r$ and $x = y^w$ implies $w = 1$. According to Proposition 2.15 the characteristic function for r -free elements is

$$\omega_r : \mathbb{F}_{q^m} \rightarrow \mathbb{C}, \quad x \mapsto \theta(r') \sum_{d|r} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \widehat{\mathbb{F}_{q^m}^*}, \text{ord}(\chi)=d} \chi(x),$$

where r' is the square-free part of r , and μ , φ and θ are defined appropriately. Further, primitive elements are exactly those that have *order* equal to $q^m - 1$, that is those that are $(q^m - 1)$ -free, or q_0 -free, where q_0 is the square-free part of $q^m - 1$.

CHAPTER 3

The Hansen-Mullen conjecture for self-reciprocal irreducible polynomials

In this chapter we present our results on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials.

3.1 Preliminaries

We denote by \mathbb{I}_n the set of monic irreducible polynomials of degree n and by \mathbb{J}_n the set of irreducible polynomials of degree n and constant term H_0 equal to 1. Further, we set $\mathbb{G}_k = \{H \in \mathbb{F}_q[X] : \deg(H) \leq k \text{ and } H_0 = 1\}$.

It is well-known, see [4], that if Q is a self-reciprocal monic irreducible polynomial over \mathbb{F}_q , then $\deg(Q)$ is even and $Q(X) = X^n P(X + X^{-1})$ for some $P \in \mathbb{I}_n$ such that $\psi(P) = -1$, where $\psi(P) = (P|X^2 - 4)$, the Jacobi symbol of P modulo $X^2 - 4$. Conversely, if $P \in \mathbb{I}_n$, with $\psi(P) = -1$, and $Q = X^n P(X + X^{-1})$, then Q is a self-reciprocal monic irreducible.

We denote $P = \sum_{i=0}^n P_i X^i$ and $Q = \sum_{i=0}^{2n} Q_i X^i$, and we compute

$$\begin{aligned} Q(X) &= X^n P(X + X^{-1}) = \sum_{i=0}^n P_i X^{n-i} (X^2 + 1)^i \\ &= \sum_{i=0}^n P_i X^{n-i} \left(\sum_{j=0}^i \binom{i}{j} X^{2j} \right) = \sum_{i=0}^n \sum_{j=0}^i \binom{i}{j} P_i X^{n-i+2j}. \end{aligned}$$

Since Q is monic and self-reciprocal, $Q_0 = 1$ and $Q_{2n-i} = Q_i$, so we may restrict ourselves to $1 \leq k \leq n$. The last equation implies that

$$Q_k = \sum_{\substack{0 \leq j \leq i \leq n \\ n-i+2j=k}} \binom{i}{j} P_i = \sum_{\substack{n-k \leq i \leq n \\ k-n+i \in 2\mathbb{Z}}} \binom{i}{\frac{k-n+i}{2}} P_i,$$

and by making the variable change $j = n - i$ we have

$$Q_k = \sum_{\substack{0 \leq j \leq k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} P_{n-j}.$$

The coefficient Q_k is expressed in terms of the coefficients of the k largest degree terms of P . In order to express Q_k in terms of the coefficients of low degree terms of a polynomial related to P , we define the polynomial \hat{P} as follows.

Definition 3.1. Let $G \in \mathbb{F}_q[X]$, $\deg(G) = n$. We define $\hat{G} = X^n G(4X^{-1})$.

The following lemma summarizes the properties of the transformation.

Lemma 3.2. Let $P \in \mathbb{J}_n$, $n \geq 2$. Then $\hat{P} \in \mathbb{I}_n$, $\hat{P}_i = 4^{n-i} P_{n-i}$. Further, $\psi(P) = -\epsilon \psi(\hat{P})$, where

$$\epsilon := \begin{cases} -1, & \text{if } n \text{ is even or } q \equiv 1 \pmod{4}. \\ 1, & \text{otherwise.} \end{cases}$$

Proof. Since P is irreducible of degree $n \geq 2$, we see that \hat{P} is of degree n . The irreducibility of \hat{P} follows from the fact that if θ is a root of P , then $4/\theta$ is a root of \hat{P} , and $\mathbb{F}_q(\theta) = \mathbb{F}_q(4/\theta)$. The statement regarding the coefficients of \hat{P} is easily verified and the one regarding $\psi(\hat{P})$ is proven in [26, Lemma 2]. \square

Let $a \in \mathbb{F}_q$ and suppose that there exists an irreducible polynomial $P \in \mathbb{J}_n$, such that $\psi(P) = \epsilon$ and $\sum_{\substack{0 \leq j \leq k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = a$. Then Lemma 3.2 implies that $\hat{P} \in \mathbb{I}_n$ and $\psi(\hat{P}) = -1$. If we let $Q = X^n \hat{P}(X + X^{-1})$, we have

$$Q_k = \sum_{\substack{0 \leq j \leq k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} \hat{P}_{n-j} = \sum_{\substack{0 \leq j \leq k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = a.$$

For convenience, we define

$$\delta_j = \begin{cases} \binom{n-j}{\frac{k-j}{2}} 4^j, & \text{if } k-j \equiv 0 \pmod{2}, \\ 0, & \text{if } k-j \equiv 1 \pmod{2}. \end{cases}$$

We note that $\delta_k = 4^k \neq 0$. If we let $P \equiv H \pmod{X^{k+1}}$, for a polynomial H of degree at most $k-1$, the condition $\sum_{\substack{0 \leq j \leq k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = a$ becomes

$$\sum_{j=0}^k \delta_j H_j = a.$$

This leads us to define the following map.

Definition 3.3. For $n, k \in \mathbb{N}$ with $1 \leq k \leq n$, we define

$$\tau_{n,k} : \mathbb{G}_k \rightarrow \mathbb{F}_q, \quad H \mapsto \sum_{j=0}^k \delta_j H_j.$$

Our observations are summarized in the following proposition.

Proposition 3.4. *Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. Suppose that there exists an irreducible polynomial $P \in \mathbb{J}_n$, such that $\psi(P) = \epsilon$ and $P \equiv H \pmod{X^{k+1}}$ for some $H \in \mathbb{G}_k$ with $\tau_{n,k}(H) = a$. Then there exists a self-reciprocal monic irreducible polynomial Q , of degree $2n$, with $Q_k = a$.*

Later, we will need to correlate the inverse image of $\tau_{n,k}$ with \mathbb{G}_{k-1} . This is achieved in the proposition below.

Proposition 3.5. *Let $a \in \mathbb{F}_q$, $n, k \in \mathbb{N}$, $n \geq 2$ and $1 \leq k \leq n$. Let $F = \sum_{i=0}^k F_i X^i \in \mathbb{F}_q[X]$, with $F_0 = 1$ and $F_i = \delta_{k-i} \delta_k^{-1}$, $1 \leq i \leq k-1$, and $F_k = \delta_k^{-1}(\delta_0 - a)$. Then the map $\sigma_{n,k,a} : \tau_{n,k}^{-1}(a) \rightarrow \mathbb{G}_{k-1}$ defined by $\sigma_{n,k,a}(H) = HF \pmod{X^{k+1}}$ is a bijection.*

Proof. We start by showing that the map is well-defined. The polynomial $\sigma_{n,k,a}(H)$, by its definition, is of degree at most k and has constant term equal to 1. The coefficient of X^k of $\sigma_{n,k,a}(H)$ is $H_k + H_k + \sum_{j=1}^{k-1} H_j F_{k-j}$. Noting that $\tau_{n,k}(H) = a$, we compute

$$\begin{aligned} F_k + H_k + \sum_{j=1}^{k-1} H_j F_{k-j} &= -a\delta_k^{-1} + \delta_0\delta_k^{-1} + H_k\delta_k\delta_k^{-1} + \sum_{j=1}^{k-1} H_j\delta_j\delta_k^{-1} \\ &= -a\delta_k^{-1} + \delta_k^{-1} \left(\sum_{j=0}^k H_j\delta_j \right) = -a\delta_k^{-1} + \delta_k^{-1}\tau_{n,k}(H) = 0. \end{aligned}$$

This shows that $\deg(\sigma_{n,k,a}(H)) \leq k-1$, and the map is well-defined.

To see that the map is one-to-one, assume that there exist some $H_1, H_2 \in \tau_{n,k}^{-1}(a)$ such that $\sigma_{n,k,a}(H_1) = \sigma_{n,k,a}(H_2)$. This implies that

$$H_1 F \equiv H_2 F \pmod{X^{k+1}}.$$

Since F is invertible modulo X^{k+1} , we obtain $H_1 \equiv H_2 \pmod{X^{k+1}}$, which implies $H_1 = H_2$ since $\deg(H_1), \deg(H_2) \leq k$.

It is trivial that $|\mathbb{G}_{k-1}| = q^{k-1}$. The proof will be complete once we show that $|\tau_{n,k}^{-1}(a)| = q^{k-1}$. It is clear that $\tau_{n,k}$ is linear and surjective, therefore, the dimension of its kernel is equal to $k-1$. It follows that the kernel, and therefore the fibers of $\tau_{n,k}$, have cardinality q^{k-1} . \square

Remark 3.6. We easily check that in the above proof we may substitute $\tau_{n,k}$ with an arbitrary \mathbb{F}_q -linear $\tau : \mathbb{G}_k \rightarrow \mathbb{F}_q$, such that $\tau(X^k) \neq 0$, since this is the only property of $\tau_{n,k}$ we actually used.

3.2 Weighted sum

Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$ and $a \in \mathbb{F}_q$. Inspired by Wan's work [57] we introduce the following weighted sum.

$$w_a(n, k) = \sum_{H \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(H)) \sum_{\substack{P \in \mathbb{J}_n, \psi(P) = \epsilon \\ P \equiv H \pmod{X^{k+1}}}} 1. \quad (3.1)$$

It is clear that if $w_a(n, k) > 0$, then there exists some $P \in \mathbb{J}_n$ such that $P \equiv H \pmod{X^{k+1}}$ for some $H \in \mathbb{G}_k$, with $\tau_{n,k}(H) = a$ and $\psi(P) = \epsilon$. Then Proposition 3.4

implies that there exists a self-reciprocal, monic irreducible polynomial Q , of degree n with $Q_k = a$.

Let U be the subgroup of $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ that contains classes of polynomials with constant term equal to 1. Then $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ is the direct sum of U and \mathbb{F}_q^* . The set \mathbb{G}_{k-1} is a set of representatives of U . Further, the group of characters of U consists exactly of those characters of $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ that are trivial on \mathbb{F}_q^* , that is, $\widehat{U} = \{\chi \in (\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^* : \chi(\mathbb{F}_q^*) = 1\}$. Using these observations and with the help of Lemma 2.2, Eq. (3.1) can be rewritten as

$$w_a(n, k) = \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P) = \epsilon}} \chi(P) \sum_{H \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(H)) \bar{\chi}(H).$$

If we denote by G the inverse of F modulo X^{k+1} , where F as defined in Proposition 3.5, and using Proposition 3.5, we obtain

$$\begin{aligned} w_a(n, k) &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P) = \epsilon}} \chi(P) \sum_{H \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(H)) \bar{\chi}(\sigma_{n,k,a}(H)G) \\ &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P) = \epsilon}} \chi(P) \bar{\chi}(G) \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) \bar{\chi}(H). \end{aligned}$$

Separating the term that corresponds to χ_o , we have

$$\left| w_a(n, k) - \frac{\pi_q(n, \epsilon)}{q^k} \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) \right| \leq \frac{1}{q^k} \sum_{\chi \neq \chi_o} \left| \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P) = \epsilon}} \chi(P) \right| \left| \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) \bar{\chi}(H) \right|,$$

where $\pi_q(n, \epsilon) = |\{P \in \mathbb{J}_n : \psi(P) = \epsilon\}|$. It is computed in [4],

$$\pi_q(n, -1) = \begin{cases} \frac{1}{2n}(q^n - 1), & \text{if } n = 2^s, \\ \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{\frac{n}{d}}, & \text{otherwise.} \end{cases}$$

If n is not a power of 2, we have

$$\left| \pi_q(n, -1) - \frac{q^n}{2n} \right| \leq \frac{1}{2n} \frac{q}{q-1} q^{\frac{n}{3}}. \quad (3.2)$$

Note that the bound remains true in the case that n is a power of 2. If n is even, then $\epsilon = -1$. If n is odd then $\pi_q(n, -1) = \frac{1}{2n} \sum_{d|n} \mu(d) q^{\frac{n}{d}} = \frac{1}{2} \pi_q(n)$. Since $\pi_q(n, -1) + \pi_q(n, 1) = \pi_q(n)$, we conclude that $\pi_q(n, 1) = \pi_q(n, -1)$. Thus, in every case, $\pi_q(n, \epsilon) = \pi_q(n, -1)$. Furthermore,

$$\sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) = \sum_{m=0}^{k-1} \sum_{\substack{\deg(H)=m \\ H_0=1}} \Lambda(H) = \sum_{m=0}^{k-1} q^m = \frac{q^k - 1}{q - 1}.$$

Eq. (2.2) of Proposition 2.9 implies that

$$\left| \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) \bar{\chi}(H) \right| \leq 1 + \sum_{m=1}^{k-1} (1 + kq^{\frac{m}{2}}) = k \frac{q^{\frac{k}{2}} - 1}{\sqrt{q} - 1}.$$

Putting everything together, and using Eq. (2.3) we have

$$\left| w_a(n, k) - \frac{q^k - 1}{q^k(q-1)} \pi_q(n, -1) \right| \leq \frac{k(k+5)}{n} \frac{(q^k - 1)(q^{\frac{k}{2}} - 1)q^{\frac{n}{2}}}{q^k(\sqrt{q} - 1)}. \quad (3.3)$$

The following theorem follows directly from this bound.

Theorem 3.7. *Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a monic, self-reciprocal irreducible polynomial $Q \in \mathbb{F}_q[X]$, of degree $2n$ with $Q_k = a$ if the following bound holds.*

$$\pi_q(n, -1) \geq \frac{k(k+5)}{n} (\sqrt{q} + 1) q^{\frac{n+k}{2}}.$$

Proof. From our previous discussion, it suffices to show that $w_a(n, k) > 0$. Eq. (3.3) implies that a sufficient condition is

$$\frac{q^k - 1}{q^k(q-1)} \pi_q(n, -1) > \frac{k(k+5)}{n} \frac{(q^k - 1)(q^{\frac{k}{2}} - 1)q^{\frac{n}{2}}}{q^k(\sqrt{q} - 1)},$$

that is,

$$\pi_q(n, -1) > \frac{k(k+5)}{n} (\sqrt{q} + 1) (q^{\frac{k}{2}} - 1) q^{\frac{n}{2}}. \quad (3.4)$$

The stated condition follows easily. \square

Substituting the bound of Eq. (3.2) in Theorem 3.7, we obtain the following.

Theorem 3.8. *Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a monic, self-reciprocal irreducible polynomial $Q \in \mathbb{F}_q[X]$, of degree $2n$ with $Q_k = a$ if the following bound holds.*

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5} k(k+5) + \frac{1}{2}.$$

Proof. From Theorem 3.7 and Eq. (3.2), we see that a sufficient condition is

$$\frac{q^n}{2n} - \frac{q}{q-1} \frac{q^{\frac{n}{2}}}{2n} \geq \frac{k(k+5)}{n} (\sqrt{q} + 1) q^{\frac{n+k}{2}}.$$

Using the fact that $\frac{q}{q-1} \leq \frac{3}{2}$ and $\sqrt{q} + 1 \leq \frac{16\sqrt{q}}{10}$ for $q \geq 3$, we obtain the sufficient condition

$$q^{\frac{n-k+1}{2}} \geq \frac{16k(k+5)}{5} + \frac{3}{2} q^{-\frac{n}{6} - \frac{k}{2} - \frac{1}{2}}.$$

Since $\frac{3}{2} q^{-\frac{n}{6} - \frac{k}{2} - \frac{1}{2}} \leq \frac{1}{2}$, the condition in the statement follows. \square

Remark 3.9. As pointed out in Remark 3.6 we could obtain more general results by choosing an arbitrary \mathbb{F}_q -linear $\tau : \mathbb{G}_k \rightarrow \mathbb{F}_q$, such that $\tau(X^k) \neq 0$. In this case, if the bounds of Theorems 3.7 or 3.8 hold, then there exists some $P \in \mathbb{I}_n$, with $\psi(P) = -1$ and $\hat{P} \equiv H \pmod{X^{k+1}}$ for some $H \in \tau^{-1}(a)$, for any $a \in \mathbb{F}_q$.

3.3 The restriction $k \leq n/2$

In this section, we content ourselves for $k \leq n/2$ and solve completely the resulting problem. In particular, we use the theory developed previously in this chapter to theoretically prove that the resulting problem can be answered positively for all, but a small, finite number of possible exceptions. Then, with the help of computers, we investigate the remaining cases one-by-one.

For $k \leq n/2$, Eq. (3.4) implies that there exists a monic irreducible self-reciprocal polynomial over \mathbb{F}_q , where q a power of an odd prime, of degree $2n$ with it's k -th coefficient prescribed, if

$$\pi_q(n, -1) > \frac{\lfloor n/2 \rfloor (\lfloor n/2 \rfloor + 5)}{n} (\sqrt{q} + 1) (q^{\lfloor n/2 \rfloor / 2} - 1) q^{n/2}. \quad (3.5)$$

With the help of computers, see Section A.1, we can use Eq. (3.5) to find pairs (q, n) such that if q is a power of an odd prime and n an integer, then there exists some monic irreducible self-reciprocal polynomial over \mathbb{F}_q of degree $2n$ such that any of its $\lfloor n/2 \rfloor$ low degree coefficients is prescribed. Such pairs are illustrated in Table 3.1.

Table 3.1: Pairs (q, n) that satisfy Eq. (3.5).

n	3	4	5	6	7	8	9	10
q	≥ 149	≥ 839	≥ 37	≥ 59	≥ 17	≥ 23	≥ 11	≥ 13
n	11	12	13	14	15	16	17	18
q	≥ 9	≥ 9	≥ 7	≥ 7	≥ 5	≥ 7	≥ 5	≥ 5
n	19	20	21	22	23	24	25	26
q	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 3	≥ 5

Corollary 3.10. *If $n \geq 3$ an integer and q a power of an odd prime, then there exists a monic irreducible self-reciprocal polynomial over \mathbb{F}_q of degree $2n$ such that any of its $\lfloor n/2 \rfloor$ low degree coefficients is prescribed, if either $n \geq 27$ or $q \geq 839$.*

Proof. It is clear that if the bound of Theorem 3.8 holds for some q_0 and $k = n/2$, then it still holds for any $q \geq q_0$ and $1 \leq k \leq n/2$. Also it is not hard to see that

$$3^{\frac{n-\frac{n}{2}-1}{2}} \geq \frac{16n}{10} \left(\frac{n}{2} + 5 \right) + \frac{1}{2}$$

for all $n \geq 27$, since the function

$$g(n) = 3^{\frac{n-2}{4}} - \frac{4n}{5}(n+10) + \frac{1}{2}$$

is increasing for $n \geq 27$ and $g(27) > 0$. Further, from Table 3.1, we see that our statement is true for $q \geq 839$. \square

With the help of computers, we explicitly check the remaining cases, present in Table 3.1. The program that performed this search is illustrated in Section A.1. The results revealed that, under the restriction $k \leq n/2$, we have two (genuine) exceptions. Those results¹, combined with Corollary 3.10 imply the theorem below.

¹Available online at <http://www.math.uoc.gr/~gkapet/hm/hm-results.txt>.

Theorem 3.11. *Let $n \geq 3$ an integer and q a power of an odd prime. If $k \leq n/2$ and $a \in \mathbb{F}_q$, then there exists a monic irreducible self-reciprocal polynomial over \mathbb{F}_q of degree $2n$ such that any of its k -th coefficient is prescribed to a , unless*

1. $q = 3, n = 3, a = 0$ and $k = 1$ or
2. $q = 3, n = 4, a = 0$ and $k = 2$.

Extending the (strong) primitive normal basis theorem I

In this chapter we solve Problem 1.4 completely. Namely, in Theorem 4.25, we prove that the question can be answered positively, with the exception of an explicit small list of genuine exceptions. Also we note that throughout this chapter we assume that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ has at most one zero entry, since the case where there are two zero entries has already been covered in Theorem 1.3.

4.1 Some estimates

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, $q_1 \mid q_0$ and $F_i \mid F_0$, for $i = 1, 2$, where q_0 and F_0 stand for the radicals of $q^m - 1$ and $X^m - 1$ respectively; in particular $F_0 = X^{m_0} - 1$. We denote (q_1, F_1, F_2) by \mathbf{k} and call it a *divisor triple*. Furthermore, we call an element $x \in \mathbb{F}_{q^m}$ \mathbf{k}_A -free, if x is q_1 -free and F_1 -free and $(ax + b)/(cx + d)$ is F_2 -free. Also we denote by $N_A(\mathbf{k})$ the number of $x \in \mathbb{F}_{q^m}$ that are \mathbf{k}_A -free. We write $\mathbf{l} \mid \mathbf{k}$, if $\mathbf{l} = (d_1, G_1, G_2)$ and $d_1 \mid q_1$ and $G_i \mid F_i$ for $i = 1, 2$. Further, \mathbf{w} stands for (q_0, F_0, F_0) and $\mathbf{1}$ stands for $(1, 1, 1)$, while the greatest common divisor and the least common multiple of a set of divisor triples are defined point-wise. A divisor triple \mathbf{p} is called *prime* if it has exactly one entry that is $\neq 1$ and this entry is either a prime number or an irreducible polynomial. Finally, if two divisor triples are co-prime, then their product can be defined naturally.

Example. Let $q = 7$ and $m = 4$. In that case, $q_0 = 30$ (since $q^m - 1 = 2400 = 2^5 \cdot 3 \cdot 5^2$ and $2 \cdot 3 \cdot 5 = 30$) and $F_0 = X^4 - 1 = (X-1)(X+1)(X^2+1) \in \mathbb{F}_7[X]$, since $m = m_0 = 4$. In that case, four distinct divisor triples would be $\mathbf{e}_0 := (3, X^2 - 1, X^3 + X^2 + X + 1)$, $\mathbf{p}_1 := (2, 1, 1)$, $\mathbf{p}_2 := (1, X^2 + 1, 1)$ and $\mathbf{p}_3 := (1, 1, X - 1)$. It is clear that \mathbf{e}_0 , \mathbf{p}_1 , \mathbf{p}_2 and \mathbf{p}_3 are non-trivial, co-prime divisor triples, while \mathbf{e}_0 is non-prime and \mathbf{p}_1 , \mathbf{p}_2 and \mathbf{p}_3 are primes. Also, since they are co-prime, we can define their product, $\mathbf{e} := \mathbf{e}_0 \cdot \mathbf{p}_1 \cdot \mathbf{p}_2 \cdot \mathbf{p}_3 = (6, X^4 - 1, X^4 - 1)$.

For $r \in \mathbb{N}$, set t_r to be the number of prime divisors of r and t_F the number of monic irreducible divisors of $F \in \mathbb{F}_q[X]$ and set $W(r) := 2^{t_r}$ and $W(F) := 2^{t_F}$. It follows that $\sum_{d \mid r} |\mu(d)| = W(r)$ and $\sum_{G \mid F} |\mu(G)| = W(F)$. In the proceeding section as well as in

Chapter 5, an estimation for $W(q_0)$ will be necessary. The lemma below provides us one.

Lemma 4.1. *For any $r \in \mathbb{N}$, $W(r) \leq c_{r,a} r^{1/a}$, where $c_{r,a} = 2^s / (p_1 \cdots p_s)^{1/a}$ and p_1, \dots, p_s are the primes $\leq 2^a$ that divide r . In particular, we are interested in $c_r := c_{r,4}$, $d_r := c_{r,8}$ and $e_r := c_{r,12}$. Moreover, for all $r \in \mathbb{N}$ we have that $c_r < 4.9$, $d_r < 4514.7$ and $e_r < 1.06 \cdot 10^{24}$.*

Proof. It is clear that it suffices to prove the above for r square-free. Assume that $r = p_1 \cdots p_s q_1 \cdots q_t$, where $p_1, \dots, p_s, q_1, \dots, q_t$ are distinct primes and $p_i \leq 2^a$ and $q_j > 2^a$. We have that

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

For the computation of the estimates provided in the statement, see Section A.2. \square

Remark 4.2. The lemma above provides us universal estimates for the numbers c_r , d_r and e_r . Nonetheless, given r , these numbers are easily computable and in some cases better estimates can be employed, for instance $c_r < 2.9$ for odd r . For the computer functions used to compute sharper estimates in special cases, or the exact computation of the above number, see Section A.2. In the proceeding sections, these numbers are freely replaced by the above estimates, by (sharper) estimates or by their exact values, in some cases without special notice.

Moreover, for $\mathbf{k} = (q_1, F_1, F_2)$ we will denote by $f(\mathbf{k})$ the product $f(q_1)f(F_1)f(F_2)$, where f may be θ , φ , μ or W . Before proceeding, we have to study a bit more the behavior of the Order of an additive character.

Lemma 4.3. *Let $\psi \in \widehat{\mathbb{F}_{q^m}}$ be an additive character, then $\psi|_{\mathbb{F}_q}$ is trivial if and only if $\text{Ord}(\psi) \mid X^{m-1} + X^{m-2} + \cdots + 1$.*

Proof. Assume $\psi(\alpha) = 1$ for all $\alpha \in \mathbb{F}_q$. Let $x \in \mathbb{F}_{q^m}$. We have that

$$(X^{m-1} + \cdots + 1) \circ \psi(x) = \psi(x^{q^{m-1}} + x^{q^{m-2}} + \cdots + x) = \psi(\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)) = 1,$$

since $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) \in \mathbb{F}_q$. It follows that $X^{m-1} + \cdots + 1$ lies in the annihilator of ψ , hence divided by $\text{Ord}(\psi)$.

Conversely, assume that $\text{Ord}(\psi) \mid X^{m-1} + \cdots + 1$. Let $\alpha \in \mathbb{F}_q$. Since $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$ is onto, there exist some $x \in \mathbb{F}_{q^m}$ such that $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = \alpha$. Since $\text{Ord}(\psi) \mid X^{m-1} + \cdots + 1$, it follows that $X^{m-1} + \cdots + 1$ lies in the annihilator of ψ , thus

$$(X^{m-1} + \cdots + 1) \circ \psi(x) = 1 \Rightarrow \psi(\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)) = 1 \Rightarrow \psi(\alpha) = 1. \quad \square$$

Lemma 4.4. *If $\text{gcd}(p, m) = 1$, then $\{\psi|_{\mathbb{F}_q} : \psi \in \widehat{\mathbb{F}_{q^m}}, \text{Ord}(\psi) \mid X - 1\} = \widehat{\mathbb{F}_q}$.*

Proof. From Eq. (2.4), it is clear that there are exactly q additive characters, whose Order divides $X - 1$. Therefore, since $\widehat{\mathbb{F}_q}$ also has q elements, it suffices to show that for any two distinct additive characters, whose Order divides $X - 1$, their restrictions on \mathbb{F}_q differ. Let ψ_1, ψ_2 be additive characters whose Order divides $X - 1$ such that $\psi_1|_{\mathbb{F}_q} = \psi_2|_{\mathbb{F}_q}$. It follows that $\psi_1 \bar{\psi}_2$ is trivial on \mathbb{F}_q and Lemma 4.3 yields $\text{Ord}(\psi_1 \bar{\psi}_2) \mid X^{m-1} + \cdots + 1$. It is clear though that $\text{Ord}(\psi_1 \bar{\psi}_2) \mid X - 1$ and it follows that $\text{Ord}(\psi_1 \bar{\psi}_2) = 1$, i.e. $\psi_1 = \psi_2$. \square

Lemma 4.5. *Let $G_1, G_2 \in \mathbb{F}_q[X]$ such that $G_1 G_2 \mid X^m - 1$ and $\gcd(G_1, G_2) = 1$. If $\mathfrak{G}_i := \{\psi \in \widehat{\mathbb{F}_{q^m}} : \text{Ord}(\psi) = G_i\}$ ($i = 1, 2$) and $\mathfrak{G} := \{\psi \in \widehat{\mathbb{F}_{q^m}} : \text{Ord}(\psi) = G_1 G_2\}$, then $\mathfrak{G}_1 \mathfrak{G}_2 = \mathfrak{G}$.*

Proof. It is clear that $|\mathfrak{G}_1 \mathfrak{G}_2| = |\mathfrak{G}|$, thus it suffices to show that $\mathfrak{G}_1 \mathfrak{G}_2 \subseteq \mathfrak{G}$. Let $\psi_1 \in \mathfrak{G}_1$ and $\psi_2 \in \mathfrak{G}_2$. Set $F = \text{Ord}(\psi_1 \psi_2)$. It is clear that $(\psi_1 \psi_2)^{G_1 G_2} = \psi_o$, thus $F \mid G_1 G_2$. It is also clear that $(\psi_1 \psi_2)^F = \psi_o$, that is $\psi_1^F = \bar{\psi}_2^F$. Since $\text{Ord}(\psi_1^F) \mid G_1$ and $\text{Ord}(\bar{\psi}_2^F) \mid G_2$, it follows that $\psi_1^F = \psi_2^F = \psi_o$, consequently $G_1 \mid F$ and $G_2 \mid F$, i.e. $G_1 G_2 \mid F$. \square

Clearly, our purpose is to show that $N_A(\mathbf{w}) > 0$. The proposition below is our first step towards this.

Proposition 4.6. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$ and \mathbf{k} be a divisor triple. If $(q, c) \neq (2, 0)$ and $q^{m/2} \geq 3W(\mathbf{k})$, then $N_A(\mathbf{k}) > 0$.*

Proof. From the fact that ω and Ω are characteristic functions, we have that:

$$N_A(\mathbf{k}) = \sum_x \omega_{q_1}(x) \Omega_{F_1}(x) \Omega_{F_2}((ax + b)/(cx + d)), \quad (4.1)$$

where the sum runs over \mathbb{F}_{q^m} , except $-d/c$ if $c \neq 0$.

First, assume $c \neq 0$. Eq. (4.1) gives

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\substack{\mathbf{l} \mid \mathbf{k} \\ \mathbf{l} = (d_1, G_1, G_2)}} \frac{\mu(\mathbf{l})}{\varphi(\mathbf{l})} \sum_{\substack{\text{ord}(\chi_1) = d_1, \\ \text{Ord}(\psi_1) = G_1, \\ \text{Ord}(\psi_2) = G_2}} \mathcal{X}_A(\chi_1, \psi_1, \psi_2), \quad (4.2)$$

where

$$\begin{aligned} \mathcal{X}_A(\chi_1, \psi_1, \psi_2) &:= \sum_{x \neq -d/c} \chi_1(x) \psi_1(x) \psi_2((ax + b)/(cx + d)) \\ &= \sum_{x \neq -d/c} \chi_g(x^{n_1}) \psi_g(\mathcal{G}(x)), \end{aligned}$$

for $0 \leq n_1 \leq q^m - 2$, $\mathcal{G}(X) := (y_1 X(cX + d) + y_2(aX + b))/(cX + d) \in \mathbb{F}_q(X)$ and $y_i \in \mathbb{F}_{q^m}$. Our first aim is to show that $|\mathcal{X}_A(\chi_1, \psi_1, \psi_2)|$ is bounded by $3q^{m/2}$, unless all three characters are trivial. Theorem 2.13 implies that if $n_1 \neq 0$ and $\mathcal{G} \neq \mathcal{H}^p - \mathcal{H} + y$, for any $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$, then

$$|\mathcal{X}_A(\chi_1, \psi_1, \psi_2)| \leq 3q^{m/2}.$$

If $n_1 = 0$ and at least one of y_1, y_2 is non-zero, then by setting $x' := cx + d$, we have that

$$\begin{aligned} \mathcal{X}_A(\chi_1, \psi_1, \psi_2) &= \sum_{x' \neq 0} \psi_g \left(\frac{y_2 a - y_1 d}{c} + \frac{y_1 x'}{c} + \frac{y_2(bc - ad)}{x'} \right) \\ &= \psi_g \left(\frac{y_2 a - y_1 d}{c} \right) \sum_{x' \neq 0} \psi_g \left(\frac{y_1 x'}{c} + \frac{y_2(bc - ad)}{x'} \right), \end{aligned}$$

which, combined with Lemma 2.11 implies $|\mathcal{X}_A(\chi_1, \psi_1, \psi_2)| \leq 2q^{m/2}$.

Assume $\mathcal{G} = \mathcal{H}^p - \mathcal{H} + y$ for some $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$. Write

$$\mathcal{H} = H_1/H_2,$$

where H_1, H_2 are co-prime polynomials over \mathbb{F}_{q^m} . If $\mathcal{G} \neq 0$, then

$$\mathcal{G} = \mathcal{H}^p - \mathcal{H} + y \Rightarrow \frac{y_1 X(cX + d) + y_2(aX + b)}{cX + d} = \frac{H_1^p - H_1 H_2^{p-1} + y H_2^p}{H_2^p}.$$

It follows immediately from the restrictions on A that $cX + d$ is co-prime to $y_1 X(cX + d) + y_2(aX + b)$ and it is clear that H_2^p is co-prime to $H_1^p - H_1 H_2^{p-1} + y H_2^p$, hence $cX + d = H_2^p$, a contradiction since $c \neq 0$. It follows that $\mathcal{G} = 0$, which clearly implies $y_1 = y_2 = 0$.

We have now shown that $|\mathcal{X}_A(\chi_1, \psi_1, \psi_2)| \leq 3q^{m/2}$, unless all three characters are trivial. This, combined with Eq. (4.2), implies

$$N_A(\mathbf{k}) \geq \theta(\mathbf{k}) \left(q^m - 1 - 3q^{m/2} \sum_{\mathbf{l}|\mathbf{k}, \mathbf{l} \neq \mathbf{1}} \frac{\mu(\mathbf{l})}{\varphi(\mathbf{l})} \sum_{\chi_1, \psi_1, \psi_2} 1 \right),$$

which combined with Eq. (2.4), gives:

$$\begin{aligned} \frac{N_A(\mathbf{k})}{\theta(\mathbf{k})} &\geq q^{m/2} \left(q^{m/2} - \frac{1}{q^{m/2}} - 3 \sum_{\mathbf{l}|\mathbf{k}, \mathbf{l} \neq \mathbf{1}} \mu(\mathbf{l}) \right) \\ &\geq q^{m/2} (q^{m/2} - q^{-m/2} - 3(W(\mathbf{k}) - 1)) \end{aligned}$$

and the desired result follows.

Next, assume $c = 0$. Working in a similar way as before, we conclude that Eq. (4.1) gives

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\substack{\mathbf{l}|\mathbf{k} \\ \mathbf{l}=(d_1, G_1, G_2)}} \frac{\mu(\mathbf{l})}{\varphi(\mathbf{l})} \sum_{\substack{\text{ord}(\chi_1)=d_1, \\ \text{Ord}(\psi_1)=G_1, \\ \text{Ord}(\psi_2)=G_2}} \psi_2(b/d) \mathcal{Y}_A(\chi_1, \psi_1, \psi_2), \quad (4.3)$$

where $\mathcal{Y}_A(\chi_1, \psi_1, \psi_2) := \sum_{x \in \mathbb{F}_{q^m}} \chi_1(x) (\psi_1 \psi_2')(x)$, for $\psi_2'(x) := \psi_2(ax/d)$ for all $x \in \mathbb{F}_{q^m}$, an additive character of the same Order as ψ_2 . It follows from Lemma 2.2 and Theorem 2.13, that if at least one of χ_1 or $(\psi_1 \psi_2')$ is non-trivial, then $|\mathcal{Y}_A(\chi_1, \psi_1, \psi_2)| \leq q^{m/2}$. Now, Eq. (4.3) gives:

$$\left| \frac{N_A(\mathbf{k})}{\theta(\mathbf{k})} - q^m \sum_{G|\text{gcd}(F_1, F_2)} \frac{\mu(G)^2}{\psi(G)^2} \sum_{\text{Ord}(\psi_2)=G} \psi_2\left(\frac{b}{a}\right) \right| \leq q^{m/2} W(\mathbf{k}). \quad (4.4)$$

Eq. (4.4) suggests that a lower bound for the coefficient of q^m is desirable. Set $F_3 := \text{gcd}(F_1, F_2)/(X-1)$, if $X-1 \mid \text{gcd}(F_1, F_2)$ and $F_3 := \text{gcd}(F_1, F_2)$ otherwise. Further, set $\gamma := b/a \neq 0$. It follows immediately from Lemma 4.3 that $\psi(\gamma) = 1$ for any additive character ψ whose Order divides F_3 . First, suppose $X-1 \mid \text{gcd}(F_1, F_2)$. With the help

of Lemmata 2.2, 4.4 and 4.5, we evaluate:

$$\begin{aligned}
& \sum_{G|\gcd(F_1, F_2)} \frac{\mu^2(G)}{\varphi^2(G)} \sum_{\text{Ord}(\psi)=G} \psi(\gamma) \\
&= \sum_{G|F_3} \frac{1}{\varphi^2(G)} \sum_{\text{Ord}(\psi)=G} \psi(\gamma) + \sum_{G|F_3} \frac{1}{\varphi^2((X-1)G)} \sum_{\text{Ord}(\psi)=(X-1)G} \psi(\gamma) \\
&= \sum_{G|F_3} \frac{1}{\varphi(G)} + \sum_{G|F_3} \frac{1}{\varphi^2((X-1)G)} \left(\sum_{\text{Ord}(\psi_1)=G} \psi_1(\gamma) \right) \left(\sum_{\text{Ord}(\psi_2)=X-1} \psi_2(\gamma) \right) \\
&= \left(1 - \frac{1}{\varphi(X-1)^2} \right) \sum_{G|F_3} \frac{1}{\varphi(G)} = \frac{q(q-2)}{(q-1)^2} \sum_{G|F_3} \frac{1}{\varphi(G)} \geq \frac{q(q-2)}{(q-1)^2}.
\end{aligned}$$

Similarly, if $X-1 \nmid \gcd(F_1, F_2)$, then

$$\sum_{G|\gcd(F_1, F_2)} \frac{\mu^2(G)}{\varphi^2(G)} \sum_{\text{Ord}(\psi)=G} \psi(\gamma) = \sum_{G|F_3} \frac{1}{\varphi(G)} \geq 1.$$

Summing up, the coefficient of q^m in Eq. (4.4) is, in any case, larger than $q(q-2)/(q-1)^2$. It follows that a sufficient condition for $N_A(\mathbf{k}) > 0$ would be

$$q^{m/2} \frac{q(q-2)}{(q-1)^2} > W(\mathbf{k}),$$

which clearly implies the desired result for $q \neq 2$. \square

Remark 4.7. If $q = 2$, then the left part of the last inequality of the above proof is zero and the inequality is always false. This is a consequence of the fact that, in this case, $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, hence our demand is to exist some free x , such that $x+1$ is also free, which is impossible for odd m . On the other hand for m even, x is free if and only if $x+1$ is free, i.e. the resulting problem is always true from Theorem 1.2.

Remark 4.8. It is clear in the last lines of the proof of the above, that a weaker condition for $N_A(\mathbf{w}) > 0$ could be achieved, if we restricted ourselves to the case $c = 0$.

4.2 The sieve

Following Cohen and Huczynska [12, 13], we introduce a sieve that will help us get improved results. The propositions below are those of Cohen and Huczynska [13], adjusted properly.

Let $\mathbf{k} = (q_1, F_1, F_2)$ be a divisor triple. A set of complementary divisor triples of \mathbf{k} , with common divisor \mathbf{k}_0 is a set $\{\mathbf{k}_1, \dots, \mathbf{k}_r\}$, where the \mathbf{k}_i 's are divisor triples, such that $\mathbf{k}_i \mid \mathbf{k}$ for every i , their least common multiplier is divided by the radical of \mathbf{k} and $(\mathbf{k}_i, \mathbf{k}_j) = \mathbf{k}_0$ for every $i \neq j$. Furthermore, if $\mathbf{k}_1, \dots, \mathbf{k}_r$ are such that $\mathbf{k}_i = \mathbf{k}_0 \mathbf{p}_i$, where $\mathbf{p}_1, \dots, \mathbf{p}_r$ are distinct prime divisor triples, co-prime to \mathbf{k}_0 , then this particular set of complementary divisors is called a (\mathbf{k}_0, r) -decomposition of \mathbf{k} . For a (\mathbf{k}_0, r) -decomposition of \mathbf{k} we define $\delta := 1 - \sum_{i=1}^r 1/|\mathbf{p}_i|$, where $|\mathbf{p}_i|$ stands for the absolute value of the unique entry $\neq 1$ of \mathbf{p}_i , if this entry is a number, and $q^{\deg(F)}$, if this entry is $F \in \mathbb{F}_q[X]$. Finally, we define $\Delta := (r-1)/\delta + 2$. The following continues the example in page 25 and helps us understand the new concepts defined here.

Example. Make all the assumptions of the example in page 25. Further, set $\mathbf{e}_1 := (6, X^2 - 1, X^3 + X^2 + X + 1)$, $\mathbf{e}_2 := (3, X^4 - 1, X^3 + X^2 + X + 1)$ and $\mathbf{e}_3 := (3, X^2 + 1, X^4 - 1)$. Clearly, $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ is a set of complementary divisors of \mathbf{e} with common divisor \mathbf{e}_0 , since $\mathbf{p}_1, \mathbf{p}_2$ and \mathbf{p}_3 are co-prime to \mathbf{e}_0 and $\mathbf{e}_0 \mathbf{p}_i = \mathbf{e}_i$ for $i \in \{1, 2, 3\}$, hence $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ is a $(\mathbf{e}_0, 3)$ -decomposition of \mathbf{e} . For this decomposition, we compute $\delta = 1 - \frac{1}{2} - \frac{1}{7^2} - \frac{1}{7} = \frac{33}{98}$ and $\Delta = 6$.

Proposition 4.9 (Sieving inequality). *Let $A \in \text{GL}_2(\mathbb{F}_q)$, \mathbf{k} be a divisor triple and $\{\mathbf{k}_1, \dots, \mathbf{k}_r\}$ be a set of complementary divisors of \mathbf{k} with common divisor \mathbf{k}_0 . Then*

$$N_A(\mathbf{k}) \geq \sum_{i=1}^r N_A(\mathbf{k}_i) - (r-1)N_A(\mathbf{k}_0).$$

Proof. The result is trivial for $r = 1$. For $r = 2$, denote by $\mathbb{S}(\mathbf{k})$ the set of elements that are \mathbf{k}_A -free over \mathbb{F}_q , and with $\mathbb{S}(\mathbf{k}_i)$ the set of elements that are $(\mathbf{k}_i)_A$ -free over \mathbb{F}_q , where $i = 0, 1, 2$. Then $\mathbb{S}(\mathbf{k}_1) \cup \mathbb{S}(\mathbf{k}_2) \subseteq \mathbb{S}(\mathbf{k}_0)$ and $\mathbb{S}(\mathbf{k}_1) \cap \mathbb{S}(\mathbf{k}_2) = \mathbb{S}(\mathbf{k})$. The desired inequality follows after consideration of cardinalities. Suppose the result holds for $r = k \geq 1$. For $r = k + 1$, if we denote by \mathbf{k}' the least common multiplier of $\mathbf{k}_2, \dots, \mathbf{k}_{k+1}$, then it is clear that $\{\mathbf{k}', \mathbf{k}_1\}$ is a set of complementary divisor triples of \mathbf{k} with common divisor \mathbf{k}_0 . The desired result follows immediately from the induction hypothesis. \square

Proposition 4.10. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, \mathbf{k} be a divisor triple with a (\mathbf{k}_0, r) -decomposition, such that $\delta > 0$ and $\mathbf{k}_0 = (q_1, F_1, F_1)$. If $(q, c) \neq (2, 0)$ and $q^{m/2} > 3W(\mathbf{k}_0)\Delta$, then $N_A(\mathbf{k}) > 0$.*

Proof. Let $\mathbf{p}_1, \dots, \mathbf{p}_r$ be the primes of the (\mathbf{k}_0, r) -decomposition. Proposition 4.9 implies

$$N_A(\mathbf{k}) \geq \delta N_A(\mathbf{k}_0) + \sum_{i=1}^r \left(N_A(\mathbf{k}_0 \mathbf{p}_i) - \left(1 - \frac{1}{|\mathbf{p}_i|}\right) N_A(\mathbf{k}_0) \right). \quad (4.5)$$

Suppose $c \neq 0$. Taking into account the analysis done in the corresponding part of the proof of Proposition 4.6, Eq. (4.5) implies

$$\frac{N_A(\mathbf{k})}{\theta(\mathbf{k}_0)} \geq \delta \left(q^m - 1 + \sum_{\mathbf{l}|\mathbf{k}_0, \mathbf{l} \neq \mathbf{1}} U(\mathbf{l}) \right) + \sum_{i=1}^r \left(1 - \frac{1}{|\mathbf{p}_i|}\right) \sum_{\mathbf{l}|\mathbf{k}_0} U(\mathbf{l} \mathbf{p}_i),$$

where the absolute values of the expressions U does not exceed $3q^{m/2}$. Since $\delta > 0$, we conclude that $N_A(\mathbf{k}) > 0$, if

$$\delta q^{m/2} \geq 3W(\mathbf{k}_0) \left(\delta + \sum_{i=1}^r \left(1 - \frac{1}{|\mathbf{p}_i|}\right) \right),$$

and the result follows, since $\sum_{i=1}^r (1 - 1/|\mathbf{p}_i|) = r - 1 + \delta$. Next, assume $c = 0$ and $q \neq 2$. Taking into account the analysis performed in the corresponding part of the proof of Proposition 4.6, Eq. (4.5) implies

$$\frac{N_A(\mathbf{k})}{\theta(\mathbf{k}_0)} \geq \delta \left(\kappa q^m + \sum_{\mathbf{l}|\mathbf{k}_0, \mathbf{l} \neq \mathbf{1}} U(\mathbf{l}) \right) + \sum_{i=1}^r \left(1 - \frac{1}{|\mathbf{p}_i|}\right) \sum_{\mathbf{l}|\mathbf{k}_0} U(\mathbf{l} \mathbf{p}_i),$$

where $\kappa \geq q(q-2)/(q-1)^2$ and the absolute values of the expressions U is smaller than $q^{m/2}$. As before, it follows that $N_A(\mathbf{k}_0) > 0$, if $q^{m/2} > \kappa^{-1} W(\mathbf{k}_0) \Delta$, which clearly implies the desired result, since $\kappa \geq 3/4$ for $q \geq 3$. \square

It is well-known, that $F_0 = \prod_{d|m_0} Q_d$, where Q_d is the d -th cyclotomic polynomial. The d -th cyclotomic polynomial splits into $\varphi(d)/s_d$ distinct monic irreducible polynomials of degree s_d , where s_d is minimal such that $d \mid q^{s_d} - 1$. For a detailed account of the above, the reader is referred to [44, §2.4]. It follows that F_0 splits into $\varphi(m_0)/s$ monic irreducible polynomials of degree $s := s_{m_0}$ and some other polynomials of degree dividing s . We denote the product of those with degree s by G_0 . The proposition below will prove to be useful.

Proposition 4.11. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, $(q, c) \neq (2, 0)$, $\{l_1, \dots, l_t\}$ be a set of distinct primes (this set may be \emptyset , in which case $t = 0$) dividing q_0 and $r_0 := \deg(F_0/G_0)$. If*

$$q^{m/2} > \frac{3}{2^t} W(q_0) W^2(F_0/G_0) \left(\frac{q^s(2(m_0 - r_0) + s(t-1))}{sq^s(1 - \sum_{i=1}^t 1/l_i) - 2(m_0 - r_0)} + 2 \right),$$

then $N_A(\mathbf{w}) > 0$, provided that the above denominator is positive.

Proof. Let $G_0 = \prod_{i=1}^{r_1} G_i$ be the factorization of G_0 into monic irreducible polynomials. Consider the $(\mathbf{k}_0, 2r_1 + t)$ -decomposition of \mathbf{w} , where

$$\mathbf{k}_0 = \left(q_0 / \prod_{i=1}^t l_i, F_0/G_0, F_0/G_0 \right).$$

Clearly, the prime divisor triples of this decomposition are exactly those who have exactly one $\neq 1$ entry and this entry is either l_i , for some $i = 1, \dots, t$, or G_i , for some $i = 1, \dots, r_1$. Proposition 4.10 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > \frac{3}{2^t} W(q_0) W^2(F_0/G_0) \left(\frac{2r_1 + t - 1}{1 - \sum_{i=1}^t 1/l_i - 2 \sum_{i=1}^{r_1} 1/q^s} + 2 \right),$$

that is

$$q^{m/2} > \frac{3}{2^t} W(q_0) W^2(F_0/G_0) \left(\frac{q^s(2sr_1 + s(t-1))}{sq^s(1 - \sum_{i=1}^t 1/l_i) - 2sr_1} + 2 \right).$$

The desired result follows immediately, since $sr_1 = m_0 - r_0$. \square

We will call the primes used above *sieving primes*.

4.3 The case $m = 2$

Before continuing further, we focus on the delicate case $m = 2$. Although Proposition 4.11 holds in that case as well, much weaker conditions for $N_A(\mathbf{w}) > 0$ can be established. Moreover, the fact that this case is absent in related previous works [12, 13] makes this case more interesting. First of all we note that, granted that $x \in \mathbb{F}_{q^2}$ is primitive, then x is free and $(ax + b)/(cx + d)$ is $(X + 1)$ -free. It follows that $N_A(\mathbf{w}) = N_A(q_0, X - 1)$, where

$$N_A(q_1, F_1) := \sum_x \omega_{q_1}(x) \Omega_{F_1}((ax + b)/(cx + d)), \quad (4.6)$$

where $q_1 \mid q_0$, $F_1 \mid X - 1$ and the sum runs over \mathbb{F}_{q^2} , except $-d/c$ if $c \neq 0$. The proposition below provides us with a sufficient condition for $N_A(q_1, F_1) > 0$.

Proposition 4.12. *Suppose $m = 2$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, $q_1 \mid q_0$ and $F_1 \mid X - 1$. If $(q, c) \neq (2, 0)$ and $q \geq W(q_1)W(F_1)$, then $N_A(q_1, F_1) > 0$.*

Proof. As in Proposition 4.6, first assume that $c \neq 0$. Eq. (4.6) implies

$$N_A(q_1, F_1) = \theta(q_1)\theta(F_1) \sum_{\substack{d_1 \mid q_1 \\ G_1 \mid F_1}} \frac{\mu(d_1)\mu(F_1)}{\varphi(d_1)\varphi(F_1)} \sum_{\substack{\text{ord}(\chi_1)=d_1 \\ \text{Ord}(\psi_1)=G_1}} \mathcal{Z}_A(\chi_1, \psi_1),$$

where $\mathcal{Z}_A(\chi_1, \psi_1) := \sum_{x \neq -d/c} \chi_1(x) \psi_1((ax + b)/(cx + d))$. As in the proof of Proposition 4.6, we use Theorem 2.13 to show that $|\mathcal{Z}_A(\chi_1, \psi_1)| \leq q$, unless both χ_1 and ψ_1 are trivial. It follows that

$$\frac{N_A(q_1, F_1)}{\theta(q_1)\theta(F_1)} \geq q^2 - 1 - q(W(q_1)W(F_1) - 1),$$

which implies the desired result. Next, assume $c = 0$. As before, Eq. (4.6) yields

$$N_A(q_1, F_1) = \theta(q_1)\theta(F_1) \sum_{\substack{d_1 \mid q_1 \\ G_1 \mid F_1}} \frac{\mu(d_1)\mu(F_1)}{\varphi(d_1)\varphi(F_1)} \sum_{\substack{\text{ord}(\chi_1)=d_1 \\ \text{Ord}(\psi_1)=G_1}} \psi_1(b/d) \mathcal{W}_A(\chi_1, \psi_1),$$

where $\mathcal{W}_A(\chi_1, \psi_1) := \sum_{x \in \mathbb{F}_{q^2}} \chi_1(x) \psi_1(ax/d)$. Again, Lemma 2.2 and Theorem 2.13 imply $|\mathcal{W}_A(\chi_1, \psi_1)| \leq q$, unless both χ_1 and ψ_1 are trivial. It follows that

$$\frac{N_A(q_1, F_1)}{\theta(q_1)\theta(F_1)} \geq q^2 - q(W(q_1)W(F_1) - 1),$$

which implies the desired result. \square

The above is enough to give us results, but, as in the general case, sieving can be used to give us improved results. The proofs of the analogues of Propositions 4.9, 4.10 and 4.11 in this case are straightforward. We state the analogue of Proposition 4.11.

Proposition 4.13. *Suppose $m = 2$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, $(q, c) \neq (2, 0)$, $\{l_1, \dots, l_t\}$ be a set of distinct primes (this set may be \emptyset , in which case $t = 0$) dividing q_0 . If*

$$q > \frac{W(q_0)}{2^t} \left(\frac{t}{1 - \sum_{i=1}^t 1/l_i - 1/q} + 2 \right),$$

then $N_A(\mathfrak{w}) > 0$, provided that the above denominator is positive.

4.4 Evaluations

Proposition 4.11 implies that some knowledge regarding the factorization of F_0 can improve our results. In this section we, at least to some point, describe the factorization of F_0 and then use the theory presented earlier, in order to prove our results. All non-trivial calculations described in the proofs of this section were performed with Sage and the commands used are present in Section A.2. Moreover, in this section we assume that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$ and $(q, c) \neq (2, 0)$. The lemma below (analogue to [13, Lemma 2.5]) will prove to be useful.

Lemma 4.14. *If $m = 3$ or 4 and $q \equiv m - 1 \pmod{m}$, then*

$$N_A(\mathbf{w}) = N_A(q_0, X^{m-2} - 1, X^{m-2} - 1).$$

Proof. Assume $m = 4$. It suffices to show that if some $x \in \mathbb{F}_{q^4}$ is $(q_0, X^2 - 1, X^2 - 1)_A$ -free, then x is \mathbf{w}_A -free. Let x be $(q_0, X^2 - 1, X^2 - 1)_A$ -free. Clearly, $X^2 + 1$ is irreducible over \mathbb{F}_q and if x is not $(X^4 - 1)$ -free, then there exists some $y \in \mathbb{F}_{q^4}$, such that $x = y^2 + y$, i.e. $x = x^2$, impossible since $x \notin \mathbb{F}_{q^2}$. The same argument applies to $(ax + b)/(cx + d)$ and the result follows. The proof for the case $m = 3$ is almost identical. \square

Proposition 4.15. *Suppose that (q, m) is such that $m > 2$ and $m_0 \leq 4$. Moreover, suppose that if $m = 3$ or $m = 4$, then $q \not\equiv 1 \pmod{m}$. Then $N_A(\mathbf{w}) > 0$ for all pairs (q, m) not listed in Table 4.1.*

Proof. It follows from Proposition 4.6 and Lemma 4.1, that $N_A(\mathbf{w}) > 0$, if

$$q^{m/4} > 3c_{q_0}4^{m_0}. \quad (4.7)$$

The above holds for $q \geq 17$ and $m \geq 12$, since $c_{q_0} < 4.9$.

For $q = 16$, we have that $c_{q_0} < 2.9$ and $m_0 \leq 3$, hence Eq. (4.7) is satisfied for $m \geq 10$. For $q = 13$, we have $c_{q_0} < 4.7$ and Eq. (4.7) holds for $m \geq 13$. If $q = 11$, then $c_{q_0} < 4.5$ and Eq. (4.7) is true for $m \geq 14$. If $q = 9$, then $c_{q_0} < 3.2$ and Eq. (4.7) is satisfied for $m \geq 15$. For $q = 8$, we have that $c_{q_0} < 2.9$ and $m_0 \leq 3$, i.e. Eq. (4.7) holds for $m \geq 13$. If $q = 7$, then Eq. (4.7) is true for $m \geq 17$, since $c_{q_0} < 4$. For $q = 5$, we see that Eq. (4.7) holds for $m \geq 20$ and $c_{q_0} < 3.7$. For $q = 4$, we can assume that $m_0 \leq 3$ and $c_{q_0} < 2.9$ and it follows that Eq. (4.7) is satisfied for $m \geq 19$. If $q = 3$, then $c_{q_0} < 2.9$ and Eq. (4.7) holds for $m \geq 29$. Finally, of $q = 2$, then $c_{q_0} < 2.9$ and $m_0 \leq 3$ and Eq. (4.7) holds for $m \geq 37$.

For $m = 11$, we have $m_0 = 1$ and $c_{q_0} < 4.5$, i.e. Eq. (4.7) holds for $q \geq 5$. If $m = 10$, then $m_0 = 2$ and $c_{q_0} < 3.7$ and Eq. (4.7) holds for $q \geq 8$. For $m = 9, 8$, or 7 , $m_0 = 1$ and $c_{q_0} < 3.2, 2.9$ and 4 respectively, thus Eq. (4.7) is true for $q \geq 6$, if $m = 9$ or 8 , and for $q \geq 10$, if $m = 7$. If $m = 6$, then m_0 may be 2 , in which case $c_{q_0} < 3.2$ and Eq. (4.7) holds for $q \geq 29$, or 3 , in which case $c_{q_0} < 2.9$ and Eq. (4.7) holds for $q \geq 68$. If $m = 5$, then $m_0 = 1$, $c_{q_0} < 3.7$ and Eq. (4.7) is satisfied for $q \geq 21$. If $m = 4$, then m_0 may be 1 , in which case $c_{q_0} < 2.9$ and Eq. (4.7) holds for $q \geq 35$, or 4 , in which case, accounting Lemma 4.14, we may assume that $m_0 = 2$ and $c_{q_0} < 4.9$, i.e. Eq. (4.7) is satisfied for $q \geq 235$. Finally, if $m = 3$, thanks to Lemma 4.14 we can assume that $m_0 = 1$ and $c_{q_0} < 3.2$, hence Eq. (4.7) holds for $q \geq 130$.

A careful reading of the above reveals that there is a total of 86 possible exceptions (q, m) , namely

(16, 6), (16, 4), (9, 12), (9, 6), (8, 12), (8, 6), (7, 14), (7, 7), (5, 15), (5, 10), (5, 5),
(4, 16), (4, 12), (4, 8), (4, 6), (3, 27), (3, 18), (3, 12), (3, 9), (3, 6), (2, 32), (2, 24),
(2, 16), (2, 12), (2, 8), (2, 6), (64, 6), (12, 6), (27, 6), (2, 4), (4, 4), (8, 4), (16, 4), (32, 4),
(3, 4), (7, 4), (11, 4), (19, 4), (23, 4), (27, 4), (31, 4), (43, 4), (47, 4), (59, 4), (67, 4),
(71, 4), (79, 4), (83, 4), (103, 4), (107, 4), (127, 4), (131, 4), (139, 4), (151, 4), (163, 4),
(167, 4), (179, 4), (191, 4), (199, 4), (211, 4), (223, 4), (227, 4), (2, 3), (3, 3), (5, 3),
(8, 3), (9, 3), (11, 3), (17, 3), (23, 3), (27, 3), (29, 3), (32, 3), (41, 3), (47, 3), (53, 3),
(59, 3), (71, 3), (81, 3), (83, 3), (89, 3), (101, 3), (107, 3), (113, 3), (125, 3) and (128, 3).

According to Proposition 4.10, for our purposes, it also suffices to show that

$$q^{m/2} > \frac{3W(q_0)4^{m_0}}{2^t} \cdot \left(\frac{t-1}{\delta} + 2 \right),$$

where $\{l_1, \dots, l_t\}$ are distinct primes dividing q_0 and $\delta := 1 - \sum_{i=1}^t 1/l_i$ should be > 0 . This is satisfied for 53 pairs (q, m) . In particular, the pairs

$$\begin{aligned} & (16, 4), (9, 12), (8, 12), (7, 14), (7, 7), (5, 15), (5, 10), (4, 16), (4, 8), (3, 27), (3, 18), \\ & (3, 9), (2, 32), (2, 16), (64, 6), (27, 6), (16, 4), (32, 4), (59, 4), (67, 4), (71, 4), (79, 4), \\ & (83, 4), (103, 4), (107, 4), (127, 4), (131, 4), (139, 4), (151, 4), (163, 4), (167, 4), \\ & (179, 4), (191, 4), (199, 4), (211, 4), (223, 4), (227, 4), (17, 3), (27, 3), (32, 3), (41, 3), \\ & (47, 3), (53, 3), (59, 3), (71, 3), (81, 3), (83, 3), (89, 3), (101, 3), (107, 3), (113, 3), \\ & (125, 3), (128, 3) \end{aligned}$$

were settled with \emptyset as the described set of primes, i.e. no multiplicative sieving was necessary. For the pairs $(16, 6)$, $(4, 12)$ and $(2, 24)$ the set $\{241, 17, 13, 7, 5\}$ was our set of sieving primes. For the pairs $(9, 6)$ and $(27, 4)$ this set was $\{73, 13, 7, 5\}$. For the pair $(12, 6)$, this set was $\{157, 19, 13, 11, 7\}$; for $(31, 4)$ it was $\{37, 13, 5\}$; for $(43, 4)$ it was $\{37, 11, 7\}$; for $(47, 4)$ it was $\{23, 17, 13\}$ and for $(29, 3)$ it was $\{67, 13\}$. The remaining pairs are listed in Table 4.1. \square

The following two propositions deal with the special case $m_0 \mid q - 1$.

Proposition 4.16. *If $m_0 = q - 1$ and $m > 2$, then $N_A(\mathbf{w}) > 0$ for all (q, m) not listed in Table 4.1.*

Proof. Here, F_0 splits into $q - 1$ linear factors. We choose a (\mathbf{k}_0, r) -decomposition of \mathbf{w} , where $\mathbf{k}_0 = (q_0, G, G)$, for $G \mid F_0$ with $1 \leq \deg(G) \leq q - 1$. In that case all the $2(q - 1 - \deg(G))$ primes of the decomposition have absolute value q .

For q odd choose $\deg(G) = (q - 1)/2$. In that case $\delta = 1/q$, $\Delta = (q - 1)^2 + 1$ and $W(G) = 2^{(q-1)/2}$ and Proposition 4.10 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 3 \cdot 2^{q-1}((q - 1)^2 + 1)W(q_0). \quad (4.8)$$

For q even choose $\deg(G) = q/2$. Now, $\delta = 2/q$, $\Delta = (q^2 - 3q_4)/2$, $W(G) = 2^{q/2}$ and Proposition 4.10 yields that if Eq. (4.8) holds, then $N_A(\mathbf{w}) > 0$, in that case as well. With the help of Lemma 4.1, Eq. (4.8) may be replaced by

$$q^{m/4} > 3 \cdot 4.9 \cdot 2^{q-1}((q - 1)^2 + 1). \quad (4.9)$$

First of all we can restrict ourselves to pairs (q, m) with $q > 3$, since those cases have already been investigated in Proposition 4.15. After keeping in mind that $m_0 = q - 1$, we easily check that Eq. (4.9) holds for $q \geq 43$ and $m \geq m_0$. If $m \geq 2m_0$ then Eq. (4.9) is satisfied for any $q \geq 14$. If $m \geq 3m_0$, then Eq. (4.9) is satisfied for $q \geq 9$. If $m \geq 4m_0$, then Eq. (4.9) holds for $q \geq 7$. For $m \geq 5m_0$, Eq. (4.9) is true for $q \geq 6$ and if $m \geq 7m_0$, then Eq. (4.9) holds for any $q \geq 4$.

A careful interpretation of the above shows that the 20 pairs

$$\begin{aligned} & (41, 40), (37, 36), (32, 31), (31, 30), (29, 28), (27, 26), (25, 24), (23, 22), (19, 18), \\ & (17, 16), (16, 15), (13, 12), (11, 10), (9, 8), (8, 7), (7, 6), (5, 4), (4, 3), (8, 14) \text{ and } (5, 20) \end{aligned}$$

have not not been shown to satisfy Eq. (4.9) yet, after we exclude those that have been investigated in Proposition 4.15. A quick computation reveals that 12 of them satisfy Eq. (4.8), if each appearing quantity is computed explicitly. The remaining 8 pairs are listed in Table 4.1. \square

Proposition 4.17. *If $m_0 \mid q - 1$, $m_0 \neq q - 1$ and $m > 2$, then $N_A(\mathbf{w}) > 0$ for all (q, m) not listed in Table 4.1.*

Proof. In our case, $G_0 = F_0$ and $s = 1$ and it is clear that the denominator of the inequality in Proposition 4.11 is positive, since $m_0 \leq (q - 1)/2$. It follows that $N_A(\mathbf{w}) > 0$ if

$$q^{m/2} > 3W(q_0) \left(\frac{q(2m_0 - 1)}{q - 2m_0} + 2 \right). \quad (4.10)$$

Lemma 4.1 implies that another sufficient condition for our purposes would be

$$q^{m/4} > 3 \cdot 4.9 \left(\frac{q(2m_0 - 1)}{q - 2m_0} + 2 \right). \quad (4.11)$$

The above equation is always true for $m_0 \geq 12$, provided that $m_0 \leq m$ and $q \geq 2m_0 + 1$. If $m_0 = m = 11$, then Eq. (4.11) is satisfied for $q \geq 24$, while it is always true if $m > m_0 = 11$. The same holds for $m_0 = 10$, and $q \geq 23$, for $m_0 = 10$ and $q \geq 23$, for $m_0 = 9$ and $q \geq 24$, for $m_0 = 8$ and $q \geq 26$, for $m_0 = 7$ and $q \geq 31$ and for $m_0 = 6$ and $q \geq 41$. If $m = m_0 = 5$, then Eq. (4.11) is true for $q \geq 66$. If $m = 2m_0$ and $m_0 = 5$, then Eq. (4.11) is true for $q \geq 13$, while it is always true for $m \geq 3m_0$ and $m_0 = 5$. If $m_0 = m = 3$ or 4 , then Eq. (4.11) is satisfied when $q \geq 139$ or 488 respectively, while the cases when $m_0 = 3$ or 4 , but $m > m_0$ have already been investigated in Proposition 4.15.

Summing up, we end up with a set of 89 pairs (q, m) , in particular

(23, 11), (19, 9), (17, 8), (25, 8), (29, 7), (13, 6), (19, 6), (25, 6), (31, 6), (37, 6), (11, 5), (16, 5), (31, 5), (41, 5), (61, 5), (9, 4), (13, 4), (17, 4), (25, 4), (29, 4), (37, 4), (41, 4), (49, 4), (53, 4), (61, 4), (73, 4), (81, 4), (89, 4), (97, 4), (101, 4), (109, 4), (113, 4), (121, 4), (125, 4), (137, 4), (7, 3), (13, 3), (16, 3), (19, 3), (25, 3), (31, 3), (37, 3), (43, 3), (49, 3), (61, 3), (64, 3), (67, 3), (73, 3), (79, 3), (97, 3), (103, 3), (109, 3), (121, 3), (127, 3), (139, 3), (151, 3), (157, 3), (163, 3), (169, 3), (181, 3), (193, 3), (199, 3), (211, 3), (223, 3), (229, 3), (241, 3), (256, 3), (271, 3), (277, 3), (283, 3), (289, 3), (307, 3), (313, 3), (331, 3), (337, 3), (343, 3), (349, 3), (361, 3), (367, 3), (373, 3), (379, 3), (397, 3), (409, 3), (421, 3), (433, 3), (439, 3), (457, 3), (463, 3) and (487, 3)

not yet shown to satisfy Eq. (4.11). Nonetheless, an exact computation reveals that only 20 of them fail to satisfy Eq. (4.10). Moreover, the pair (121, 3) satisfies the demands of Proposition 4.11, where {37} is the mentioned set. The same holds for (79, 3) and {43}, for (67, 3) and {31}, for (61, 3) and {97}, for (49, 3) and {43}, for (43, 3) and {631}, for (37, 3) and {67}, for (31, 3) and {331, 5}, for (29, 4) and {421} and, finally, for (16, 5) and {41, 31}. The remaining 10 pairs (q, m) are listed in Table 4.1. \square

Next, we focus on the case $m_0 > 4$ and $s \neq 1$. Following Cohen and Huczynska [12, 13], we define $\rho := t_{F_0/G_0}/m_0$, where t_{F_0/G_0} stands for the number of monic irreducible factors of F_0/G_0 . Furthermore, Proposition 4.11 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 3 \cdot 4^{\rho m_0} W(q_0) \left(\frac{2q^s(1 - \rho)m_0 - sq^s}{sq^s - 2(1 - \rho)m_0} + 2 \right), \quad (4.12)$$

since $t_{F_0/G_0} \leq r_0$ and $\rho m_0 = t_{F_0/G_0}$. The lemma below, proven in [12], provides us an estimation of ρ , for $q > 4$.

Lemma 4.18. *Assume $m_0 > 4$ and $q > 4$.*

1. *If $m_0 = 2 \gcd(m, q - 1)$ with q odd, then $s = 2$ and $\rho = 1/2$.*
2. *If $m_0 = 4 \gcd(m, q - 1)$ with $q \equiv 1 \pmod{4}$, then $s = 4$ and $\rho = 3/8$.*
3. *If $m_0 = 6 \gcd(m, q - 1)$ with $q \equiv 1 \pmod{6}$, then $s = 6$ and $\rho = 13/36$.*
4. *Otherwise $\rho \leq 1/3$.*

Proposition 4.19. *If $m_0 > 4$, $q > 4$, $s \neq 1$ and $\rho > 1/3$, then $N_A(\mathbf{w}) > 0$, unless (q, m) is listed in Table 4.1.*

Proof. According to Lemma 4.18, ρ may be $1/2$, $3/8$ or $13/36$. First, assume $\rho = 1/2$. A careful view of Lemma 4.18 implies that in that case $4 \mid m_0$, i.e. since $m_0 > 4$ we can assume that $m_0 \geq 8$. With the help of Lemma 4.18, Eq. (4.12) yields another condition for $N_A(\mathbf{w}) > 0$, namely

$$q^{m/2} > 3 \cdot 2^{m_0} W(q_0) \left(\frac{q^2(q-2)}{q^2 - q + 1} + 2 \right).$$

This inequality is satisfied for all $q > 4$ and $m_0 \geq 8$, if $m > m_0$, where we assume that $W(q_0) < 4.9q^{m/4}$, from Lemma 4.1. If $m = m_0$, it is satisfied for $m \geq 8$ and $q \geq 1863$ and for $m \geq 33$ and $q \geq m_0/2 + 1$, where $W(q_0) < 4514.7q^{m/8}$. Since $m_0 \leq 2(q-1)$, it follows that for our exception pairs (q, m) , if any, $8 \leq m \leq 32$ and $5 \leq q \leq 1861$. In this region there are 310 pairs, such that $m = m_0 = 2 \gcd(m, q-1)$. Among those pairs only 22 fail to satisfy

$$q^{m/2} > 3 W(q_0) 2^m \left(\frac{q^2(m-2)}{2q^2 - m} + 2 \right),$$

another condition deriving from Lemma 4.18 and Eq. (4.12), for $W(q_0) \leq 4.9q^{m/4}$. Those pairs are

$$(5, 8), (13, 8), (29, 8), (37, 8), (53, 8), (61, 8), (101, 8), (109, 8), (125, 8), (7, 12), \\ (19, 12), (31, 12), (43, 12), (67, 12), (9, 16), (25, 16), (41, 16), (11, 20), (31, 20), \\ (13, 24), (37, 24) \text{ and } (17, 32)$$

Among those, $(5, 8)$, $(7, 12)$, $(9, 16)$ and $(13, 8)$ are the only pairs that fail, if $W(q_0)$ is computed explicitly, but $(9, 16)$ satisfies the resulting inequality, if we apply multiplicative sieving as well, with $\{21523361, 193\}$ as our set of sieving primes.

Next, assume $\rho = 3/8$. With the help of Lemmas 4.1 and 4.18, Eq. (4.12) gives another condition for $N_A(\mathbf{w}) > 0$, namely

$$q^{3m/8} > 3 \cdot 2^{3m_0/4} \cdot 4514.7 \cdot \left(\frac{5q^5 - q^4 - 10q + 10}{4q^4 - 5q + 5} \right).$$

This inequality is always true for $m > m_0$. If $m = m_0$, then this inequality holds, for $m \geq 16$ and $q \geq 37$, $m \geq 32$ and $q \geq 11$, $m \geq 48$ and $q \geq 8$ and for $m \geq 144$ and $q \geq 5$. After taking into account the implied restrictions from Lemma 4.18, it follows that the possible exception pairs are $(5, 16)$, $(13, 16)$, $(29, 16)$ and $(9, 32)$, but only $(5, 16)$ fails to satisfy

$$q^{m/2} > 3 W(q_0) 2^{3m/4} \left(\frac{q^4(5m-16)}{16q^4 - 5m} + 2 \right),$$

another condition deriving from Lemma 4.18 and Eq. (4.12).

Finally, assume $\rho = 13/36$. With the help of Lemma 4.18, Eq. (4.12) gives another condition for $N_A(\mathbf{w}) > 0$, namely

$$q^{m/2} > 3W(q_0)2^{13m_0/18} \left(\frac{23q^6(q-1) - 18q^6}{18q^6 - 23(q-1)} + 2 \right).$$

This inequality is always true, if $m > m_0$ and $W(q_0) < 4514.7q^{m/8}$. It is also true for $m = m_0 \geq 36$ and $q \geq 10$ and for $m = m_0 \geq 72$ and $q \geq 7$, for $W(q_0) < 4514.7q^{m/8}$. It follows from Lemmas 4.1 and 4.18, that the only possible exception pair is $(7, 36)$, which satisfies the above inequality, if $W(q_0)$ is exactly computed. \square

Proposition 4.20. *If $m_0 > 4$, $q > 4$, $s \neq 1$ and $\rho \leq 1/3$, then $N_A(\mathbf{w}) > 0$, unless (q, m) is listed in Table 4.1.*

Proof. We begin with the case $m_0 \geq 8$. In that case, see [13, Lemma 6.5], the function

$$f(\rho) := 4^{\rho m_0} \frac{2q^s(1-\rho)m_0 - sq^s}{sq^s - 2(1-\rho)m_0}$$

is increasing (for ρ), when $0 \leq \rho \leq 1/3$. It follows that it suffices to prove Eq. (4.12) when $\rho = 1/3$. Moreover, since $m_0 \leq q^s$, and $s \geq 2$, it follows that

$$\frac{2q^s(1-\rho)m_0 - sq^s}{sq^s - 2(1-\rho)m_0} + 2 \leq 2m_0 - 1,$$

that is Eq. (4.12) implies that if

$$q^{m/2} > 3W(q_0)4^{m_0/3}(2m_0 - 1), \quad (4.13)$$

then $N_A(\mathbf{w}) > 0$. With the help of Lemma 4.1, we see that this inequality is true for $m \geq 8$, $q \geq 95$ and $W(q_0) < 4.9q^{m/4}$, and $m \geq 106$, $q \geq 5$ and $W(q_0) < 4514.7q^{m/8}$. In the remaining region, there are exactly 2675 pairs (q, m) , who not fall in some case examined so far, but only 430 do not satisfy Eq. (4.13), for $W(q_0) < 4.9q^{m/4}$ and just 31 who fail to satisfy Eq. (4.13), if we compute $W(q_0)$ explicitly. A computation reveals that all of, except $(5, 9)$, $(5, 12)$, $(7, 8)$ and $(7, 9)$ them satisfy Eq. (4.12), if all mentioned quantities (i.e. ρ , s and $W(q_0)$) are replaced by their exact values.

Next, we focus on the case $5 \leq m_0 \leq 7$. Since $\rho \leq 1/3$ and $s \geq 2$, it is clear that $W(F_0) \leq 2^{2m_0/3}$, hence Proposition 4.6 and Lemma 4.1, yield that $N_A(\mathbf{w}) > 0$, if

$$q^{m/4} > 3 \cdot 4.9 \cdot 4^{2m_0/3}.$$

This condition is satisfied when $m \geq 5$ and $q \geq 347$ and for all $q \geq 5$ and $m \geq 5$, if $m \geq 4m_0$. It follows that there are exactly 184 pairs (q, m) in that region fulfilling all restrictions. Among these pairs only $(5, 6)$, $(7, 5)$, $(8, 5)$, $(9, 5)$, $(11, 6)$, $(17, 6)$, $(23, 6)$ and $(29, 6)$ fail to satisfy Eq. (4.12), with all appearing quantities computed explicitly.

Finally, we can successfully apply multiplicative sieving as well for most of the 12 remaining pairs. Namely, for $(5, 9)$ our set of sieving primes was $\{829, 31\}$, for $(7, 8)$ was $\{1201, 5\}$, for $(7, 9)$ $\{1063, 37, 19, 3\}$, for $(8, 5)$ $\{151, 31\}$, for $(9, 5)$ $\{61, 11\}$, for $(17, 6)$ $\{307\}$, for $(23, 6)$ $\{79\}$ and for $(29, 6)$ $\{271\}$. The remaining pairs are listed in Table 4.1. \square

Our next aim is to prove our result when $2 \leq q \leq 4$ and $m_0 \geq 4$. The lemma below, proven in [12], is very useful towards that proof.

Lemma 4.21. *Suppose $m_0 \geq 4$. If $q = 4$ and $m \notin \{9, 45\}$, then $\rho \leq 1/5$. If $q = 3$ and $m \neq 16$, then $\rho \leq 1/4$. If $q = 2$ and $m \notin \{5, 9, 21\}$, then $\rho \leq 1/6$.*

Proposition 4.22. *If $m_0 > 4$, $s \neq 1$ and $q < 5$, then $N_A(\mathbf{w}) > 0$, unless (q, m) is listed in Table 4.1.*

Proof. First, assume $q = 4$. Lemma 4.21 implies that if $m \neq 9, 45$, then $\rho \leq 1/5$. Moreover, Proposition 4.6 and Lemma 4.1 imply that $N_A(\mathbf{w}) > 0$, if $q^{m/4} > 3 \cdot 2.9 \cdot 4^{3m_0/5}$, since here $W(F_0) < 4^{3m_0/5}$. This condition is satisfied for all $m_0 \geq 4$, if $m \geq 4m_0$. Working as in the proof of Proposition 4.20, we end up for another condition for $N_A(\mathbf{w}) > 0$, for $m \neq 9, 45$, namely

$$q^{3m/8} > 3 \cdot 2461.7 \cdot 4^{m_0/5}(4m - 3).$$

This is true for $m \geq 60$ if $m = m_0$ and for $m \geq 35$ if $m = 2m_0$. We end up with 28 pairs $(4, m)$ left to consider. Among those pairs, only $(4, 5)$, $(4, 7)$, $(4, 9)$ and $(4, 15)$ fail to satisfy Eq. (4.12), if all appearing quantities (i.e. ρ , $W(q_0)$, s and m_0) are replaced by their exact values.

Next, assume $q = 3$. If $m \neq 16$, then $N_A(\mathbf{w}) > 0$, if $q^{m/4} > 3 \cdot 3.2 \cdot 4^{5m_0/8}$, as before. This is satisfied for all $m_0 > 4$, if $m \geq 9m_0$, hence we can focus on the cases and $m_0 \leq m \leq 3m_0$. As in the previous case, we have that $N_A(\mathbf{w}) > 0$, if $m \neq 16$ and

$$q^{3m/8} > 3d_r 4^{m_0/4}(3m_0 - 2),$$

where d_r is as defined in Lemma 4.1, while here, $d_r < 2589.6$. This is true for $m_0 \geq 238$, if $m = m_0$ and $m_0 \geq 43$, if $m = 3m_0$. A quick computation reveals that there exist 155 pairs $(3, m)$ not settled yet. This number is further reduced to 78, if d_r is explicitly computed for each pair. Eventually, from those 78 pairs, only $(3, 5)$, $(3, 7)$, $(3, 8)$, $(3, 10)$, $(3, 11)$, $(3, 16)$ and $(3, 20)$ fail to satisfy Eq. (4.12), if all appearing quantities are computed explicitly.

Finally, assume $q = 2$. If $m \neq 5, 9, 21$, then $N_A(\mathbf{w}) > 0$, if $q^{m/4} > 3 \cdot 2.9 \cdot 4^{7m_0/12}$, as before. This is satisfied for all $m_0 > 4$, if $m \geq 8m_0$, hence we can focus on the cases $m \neq 5, 9, 21$ and $m_0 \leq m \leq 4m_0$. As in the previous cases, we have that $N_A(\mathbf{w}) > 0$, if

$$q^{3m/8} > 3d_r 4^{m_0/6}(5m_0 - 4),$$

where $d_r < 2461.7$. This inequality holds for $m_0 \geq 585$ if $m = m_0$, for $m_0 \geq 100$ if $m = 2m_0$ and for $m_0 \geq 66$ if $m = 4m_0$. Another computation reveals that there are 290 pairs $(2, m)$ not settled yet, but this number is reduced to 148, if d_r is replaced by its exact value. This number is additionally reduced to 17, if we consider Eq. (4.12), with $\rho < 1/6$ and eventually to 6, namely $(2, 5)$, $(2, 7)$, $(2, 9)$, $(2, 11)$, $(2, 15)$ and $(2, 21)$ if ρ is computed explicitly.

We end up with a list of 17 pairs (q, m) of possible exceptions, but we can exclude $(3, 11)$ and $(3, 20)$, since we can successfully apply multiplicative sieving on those pairs with $\{3851\}$ and $\{1181\}$ as our set of sieving primes respectively. The other pairs are listed in Table 4.1 \square

We conclude this section with the delicate case $m = 2$.

Proposition 4.23. *Suppose $m = 2$. If (q, m) is not listed in Table 4.1, then $N_A(\mathbf{w}) > 0$.*

Proof. Proposition 4.13 implies that $N_A(\mathbf{w}) > 0$, if $q > 2W(q_0)$. This is true for $q \geq 97$, for $W(q_0) < 4.9q^{m/4}$, from Lemma 4.1. From the 34 remaining pairs, only 10 fail to

Table 4.1: Possible exceptions (q, m) from Section 4.4.

Proposition	Possible exception pairs (q, m)	#
4.15	$(8, 6), (5, 5), (4, 6), (3, 12), (3, 6), (2, 12), (2, 8), (2, 6), (2, 4), (4, 4), (8, 4), (3, 4), (7, 4), (11, 4), (19, 4), (23, 4), (2, 3), (3, 3), (5, 3), (8, 3), (9, 3), (11, 3), (23, 3)$	23
4.16	$(4, 3), (5, 4), (7, 6), (8, 7), (9, 8), (11, 10), (13, 12), (16, 15)$	8
4.17	$(7, 3), (9, 4), (11, 5), (13, 3), (13, 4), (13, 6), (16, 3), (17, 4), (19, 3), (25, 3)$	10
4.19	$(5, 8), (7, 12), (13, 8), (5, 16)$	4
4.20	$(5, 6), (5, 12), (7, 5), (11, 6)$	4
4.22	$(4, 5), (4, 7), (4, 9), (4, 15), (3, 5), (3, 7), (3, 8), (3, 10), (3, 16), (2, 5), (2, 7), (2, 9), (2, 11), (2, 15), (2, 21)$	15
4.23	$(2, 2), (3, 2), (4, 2), (5, 2), (7, 2), (11, 2)$	6
Total:		70

satisfy the latter inequality, if we compute $W(q_0)$ separately for each pair. Among those pairs, we find $(29, 2)$, which manages to satisfy the resulting inequality, if we apply multiplicative sieving as well, for $\{7\}$ as the set of sieving primes. The same holds for $(16, 2)$ and $\{17\}$, for $(13, 2)$ and $\{7, 3\}$ and for $(8, 2)$ and $\{7\}$. The remaining pairs are listed in Table 4.1. \square

Summing up, in this section we proved the following.

Theorem 4.24. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$. If $q \neq 2$ or $A \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, there exist some primitive $x \in \mathbb{F}_{q^m}$, such that both x and $(ax + b)/(cx + d)$ produce a normal \mathbb{F}_q -basis of \mathbb{F}_{q^m} , unless (q, m) is one of the 70 pairs listed in Table 4.1.*

4.5 Completion of the proof

In this section we examine the remaining cases one-by-one and identify the true exceptions to our problem. In order to perform all the necessary tests, a computer program was written in Sage. The code of this program is illustrated in Section A.2. All pairs (q, m) appearing in Table 4.1 were dealt with fairly quickly. In this section, $A \circ x$ stands for $(ax + b)/(cx + d)$, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ and $x \in \mathbb{F}_{q^m}$.

Our first and simplest case is $q = 2$, see Table 4.2. Here, only three matrices had to be investigated, namely $A_0 := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $A_1 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $A_2 := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. In Table 4.2, $f \in \mathbb{F}_2[X]$ is an irreducible polynomial of degree m , and β is a root of f , such that $\mathbb{F}_{2^m} = \mathbb{F}_2[\beta]$. From Table 4.2, we see that when $q = 2$, the only exceptions are $m = 3$ and $m = 4$, the exceptions already present in Theorem 1.3.

Next, in Tables 4.3 and 4.4, we present the results, when q is an odd prime. Before continuing, we note a few things regarding the matrices. First of all, as already noted, we do not need to check diagonal and anti-diagonal matrices, since those cases have already been settled by Theorems 1.2 and 1.3 respectively. Moreover, it is clear, that if $A, B \in \mathrm{GL}_2(\mathbb{F}_q)$ and $B = \alpha A$, for some $\alpha \in \mathbb{F}_q^*$, then $A \circ x = B \circ x$. Furthermore, $x \in \mathbb{F}_{q^m}$ is free if and only if αx is free, for all $\alpha \in \mathbb{F}_q^*$. It follows that, for our purposes, it suffices to check the matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, where either $d = b = 1$ and

Table 4.2: $q = 2$.

m	$f \in \mathbb{F}_2[X]$ irreducible	$x \in \mathbb{F}_{2^m}$ primitive, such that x and $A_i \circ x$ free
2	$X^2 + X + 1$	β for $i = 0, 1, 2$
3	$X^3 + X + 1$	$\beta + 1$ for $i = 0, 2$; None for $i = 1$
4	$X^4 + X + 1$	None for $i = 0$; $\beta^3 + 1$ for $i = 1, 2$
5	$X^5 + X^2 + 1$	β^3 for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^2 + \beta + 1$ for $i = 2$
6	$X^6 + X^4 + X^3 + X + 1$	$\beta^3 + 1$ for $i = 0$; $\beta^3 + \beta + 1$ for $i = 1, 2$
7	$X^7 + X + 1$	$\beta^3 + \beta + 1$ for $i = 0$; $\beta^3 + \beta^2 + 1$ for $i = 1$; $\beta^3 + 1$ for $i = 2$
8	$X^8 + X^4 + X^3 + X^2 + 1$	$\beta^5 + \beta$ for $i = 0$; $\beta^5 + \beta + 1$ for $i = 1, 2$
9	$X^9 + X^4 + 1$	$\beta^4 + \beta + 1$ for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^2 + \beta + 1$ for $i = 2$
11	$X^{11} + X^2 + 1$	$\beta^3 + 1$ for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^2 + \beta + 1$ for $i = 2$
12	$X^{12} + X^7 + X^6 + X^5 + X^3 + X + 1$	$\beta^5 + 1$ for $i = 0, 1, 2$
15	$X^{15} + X^5 + X^4 + X^2 + 1$	$\beta^3 + 1$ for $i = 0$; $\beta + 1$ for $i = 1$; $\beta^4 + \beta^3 + \beta^2 + \beta + 1$ for $i = 2$
21	$X^{21} + X^6 + X^5 + X^2 + 1$	$\beta^5 + \beta^2 + \beta + 1$ for $i = 0$; $\beta^3 + \beta + 1$ for $i = 1$; $\beta^4 + \beta^3 + \beta + 1$ for $i = 2$

$c, a \neq 0, d = 0 \neq a$ and $b = c = 1, a = d = 1$ and $b = 0 \neq c, d = b = 1$ and $c = 0 \neq a$ and, finally, $d = b = 1$ and $c \neq 0 = a$, i.e. $(q - 1)(q + 2)$ matrices.

As before, $f \in \mathbb{F}_q[X]$ is an irreducible polynomial of degree m , and β is a root of f , such that $\mathbb{F}_{q^m} = \mathbb{F}_q[\beta]$. Moreover, in the last column, we list elements $x \in \mathbb{F}_{q^m}$ that are primitive and free and inside the following parenthesis the number of matrices $A \in \text{GL}_2(\mathbb{F}_q)$ we investigated and found $A \circ x$ to be free. An interesting notice in Table 4.3 is that, not only we have no new exceptions, than those of Theorem 1.3, but also the pair (3, 4) is not an exception for any of the matrices we investigated, i.e. it is an exception only when A is anti-diagonal. On the other hand, the pair (5, 4) yields new exceptions for 4 matrices, the matrices $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$, where $a \neq 0$. It follows that (5, 4) is an exception for all $A = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \in \text{GL}_2(\mathbb{F}_5)$.

Finally, in Table 4.5, we present the results, when q is composite. All the previous arguments about the matrices hold here as well. Moreover, $h \in \mathbb{F}_p[X]$ is irreducible and α is a root of h , such that $\mathbb{F}_q = \mathbb{F}_p[\alpha]$. Also, we respect all previous conventions. We notice that only the pair (4, 3), which also appears in Theorem 1.3, yields exceptions, for the 3 matrices $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$, where $a \neq 0$, hence (4, 3) is an exception for all $A = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \in \text{GL}_2(\mathbb{F}_4)$.

We have now completed the proof of the main theorem of this chapter.

Theorem 4.25. *Let q be a prime power, $m \geq 2$ an integer and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, where $A \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ if $q = 2$ and m is odd. There exists some primitive $x \in \mathbb{F}_{q^m}$, such that both x and $(ax + b)/(cx + d)$ produce a normal basis of \mathbb{F}_{q^m} over \mathbb{F}_q , unless one of the following hold:*

1. $q = 2, m = 3$ and $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$,
2. $q = 3, m = 4$ and A is anti-diagonal or
3. (q, m) is (2, 4), (4, 3) or (5, 4) and $d = 0$.

Remark 4.26. It is interesting to notice that, not only we have no new exceptions

Table 4.3: $q \in \{3, 5\}$.

q	m	$f \in \mathbb{F}_q[X]$ irreducible	$x \in \mathbb{F}_{q^m}$ primitive, such that x and $A \circ x$ free
3	2	$X^2 + 2X + 2$	$\beta + 2$ (4); β (6)
	3	$X^3 + 2X + 1$	$2\beta^2 + 1$ (3); $\beta^2 + 1$ (7)
	4	$X^4 + 2X^3 + 2$	β (7); 2β (3)
	5	$X^5 + 2X + 1$	$\beta + 1$ (6); $\beta + 2$ (3); $\beta + 2$ (1)
	6	$X^6 + 2X^4 + X^2 + 2X + 2$	$\beta^2 + 1$ (5); $\beta^2 + \beta + 2$ (3); $\beta^4 + 2\beta^2$ (2)
	7	$X^7 + 2X^2 + 1$	$\beta^2 + 1$ (2); $2\beta + 2$ (2); $\beta + 2$ (6)
	8	$X^8 + 2X^5 + X^4 + 2X^2 + 2X + 2$	$\beta^4 + \beta + 1$ (4); $\beta^4 + \beta^2 + 2\beta + 1$ (3); $\beta^4 + \beta^3 + 1$ (1); $\beta^4 + 2\beta$ (2)
	10	$X^{10} + 2X^6 + 2X^5 + 2X^4 + X + 2$	$\beta^3 + 2\beta + 1$ (7); $\beta^3 + 2\beta^2 + 1$ (1); $2\beta^3 + \beta + 2$ (2)
	12	$X^{12} + X^6 + X^3 + X^4 + X^2 + 2$	$\beta^7 + 2\beta + 2$ (5); $\beta^7 + \beta^2 + \beta$ (3); $\beta^7 + \beta^2 + \beta + 2$ (2)
16	$X^{16} + 2X^7 + 2X^6 + 2X^4 + 2X^3 + 2X^2 + X + 2$	$\beta + 2$ (3); $2\beta + 1$ (3); $\beta^2 + 2$ (1); $2\beta^2 + 1$ (1); $2\beta^3 + \beta^2 + 1$ (1); $\beta^3 + 2\beta^2 + 2$ (1)	
5	2	$X^2 + 4X + 2$	β (22); $\beta + 4$ (6)
	3	$X^3 + 3X + 3$	$\beta + 3$ (23); $2\beta + 4$ (1); $\beta + 4$ (4)
	4	$X^4 + 4X^2 + 4X + 2$	$\beta^2 + \beta + 1$ (15); $\beta^2 + 3\beta + 3$ (5); $\beta^2 + 3\beta + 4$ (1); None (4); $\beta^2 + 4\beta$ (1); $2\beta^2 + \beta + 1$ (1); $2\beta^2 + 3\beta$ (1)
	5	$X^5 + 4X + 3$	$\beta^4 + 1$ (23); $\beta^4 + 2$ (5)
	6	$X^6 + X^4 + 4X^3 + X^2 + 2$	$\beta^2 + 1$ (11); $2\beta^2 + 4\beta + 3$ (4); $\beta^2 + 2\beta + 4$ (5); $\beta^2 + \beta$ (6); $2\beta^2 + 2\beta$ (1); $3\beta^2 + 3$ (1)
	8	$X^8 + X^4 + 3X^2 + 4X + 2$	$\beta^3 + 2\beta + 2$ (9); $\beta^3 + 3\beta + 2$ (5); $\beta^3 + 2\beta + 1$ (10); $\beta^3 + 4\beta + 3$ (2); $\beta^3 + 3\beta + 4$ (1); $\beta^3 + 4\beta + 4$ (1)
	12	$X^{12} + X^7 + X^6 + 4X^4 + 4X^3 + 3X^2 + 2X + 2$	$\beta + 4$ (14); $3\beta + 2$ (5); $2\beta + 3$ (7); $4\beta + 1$ (2)
	16	$X^{16} + X^8 + 4X^7 + 4X^6 + 4X^5 + 2X^4 + 4X^3 + 4X^2 + X + 2$	$2\beta^2 + 4\beta + 1$ (1); $\beta^2 + 2\beta + 3$ (7); $\beta^2 + 2$ (10); $\beta^2 + 4\beta + 3$ (8); $3\beta^2 + 2\beta + 4$ (1); $2\beta^2 + 4$ (1)

Table 4.4: q is a prime ≥ 7 .

q	m	$f \in \mathbb{F}_q[X]$ irreducible	$x \in \mathbb{F}_{q^m}$ primitive, such that x and $A \circ x$ free
7	2	$X^2 + 6X + 3$	β (46); $\beta + 1$ (8)
	3	$X^3 + 6X^2 + 4$	$\beta + 1$ (16); $\beta + 6$ (3); β (35)
	4	$X^4 + 5X^2 + 4X + 3$	$\beta + 1$ (46); $\beta + 3$ (8)
	5	$X^5 + X + 4$	$\beta + 1$ (46); $3\beta + 4$ (8)
	6	$X^6 + X^4 + 5X^3 + 4X^2 + 6X + 3$	$\beta^2 + 5\beta$ (8); $\beta^2 + 4\beta$ (9); $\beta^2 + 4\beta + 2$ (12); $\beta^2 + 5\beta + 4$ (6); $\beta^2 + 3\beta + 6$ (16); $2\beta^2 + \beta$ (1); $\beta^2 + 6\beta + 6$ (1); $\beta^2 + 6\beta + 1$ (1)
12	$X^{12} + 2X^8 + 5X^7 + 3X^6 + 2X^5 + 4X^4 + 5X^2 + 3$	$\beta^2 + 4\beta + 1$ (15); $3\beta^2 + 3\beta + 4$ (1); $2\beta^2 + \beta + 2$ (1); $\beta^2 + \beta + 6$ (29); $\beta^2 + 5\beta + 4$ (5); $2\beta^2 + 3\beta + 1$ (1); $\beta^2 + 5\beta + 3$ (2)	
11	2	$X^2 + 7X + 2$	β (118); $\beta + 7$ (12)
	3	$X^3 + 2X + 9$	$\beta + 7$ (12); $\beta + 4$ (118)
	4	$X^4 + 8X^2 + 10X + 2$	$\beta + 2$ (118); $\beta + 5$ (10); $\beta + 6$ (2)
	5	$X^5 + 10X^2 + 9$	$\beta + 7$ (6); $\beta + 4$ (78); $\beta + 5$ (35); $\beta + 10$ (1); $\beta + 9$ (10)
	6	$X^6 + 3X^4 + 4X^3 + 6X^2 + 7X + 2$	$\beta + 3$ (118); $\beta + 8$ (10); $2\beta + 5$ (2)
	10	$X^{10} + 7X^5 + 8X^4 + 10X^3 + 6X^2 + 6X + 2$	$\beta + 10$ (22); $\beta + 4$ (59); $\beta + 7$ (33); $2\beta + 3$ (13); $2\beta + 9$ (2); $2\beta + 8$ (1)
13	3	$X^3 + 2X + 11$	$\beta + 5$ (142); $2\beta + 6$ (15); $2\beta + 3$ (21); $2\beta + 8$ (1); $2\beta + 9$ (1)
	4	$X^4 + 3X^2 + 12X + 2$	$\beta + 2$ (142); $\beta + 4$ (32); $\beta + 11$ (6)
	6	$X^6 + 10X^3 + 11X^2 + 11X + 2$	$\beta^3 + \beta + 9$ (3); $\beta^3 + \beta + 3$ (31); $\beta^3 + \beta$ (118); $\beta^3 + \beta + 7$ (28)
	8	$X^8 + 8X^4 + 12X^3 + 2X^2 + 3X + 2$	$\beta + 1$ (131); $\beta + 3$ (42); $\beta + 5$ (6); $\beta + 11$ (1)
	12	$X^{12} + X^8 + 5X^7 + 8X^6 + 11X^5 + 3X^4 + X^3 + X^2 + 4X + 2$	$\beta + 11$ (37); $\beta + 3$ (59); $2\beta + 1$ (13); $\beta + 7$ (37); $\beta + 6$ (15); $3\beta + 5$ (1); $2\beta + 5$ (2); $\beta + 9$ (13); $2\beta + 9$ (2); $3\beta + 7$ (1)
17	4	$X^4 + 7X^2 + 10X + 3$	$\beta + 9$ (222); $\beta + 10$ (58); $\beta + 13$ (21); $2\beta + 3$ (1); $2\beta + 3$ (2)
19	3	$X^3 + 4X + 17$	$\beta + 3$ (322); $\beta + 5$ (52); $\beta + 6$ (4)
	4	$X^4 + 2X^2 + 11X + 2$	$\beta + 1$ (322); $\beta + 5$ (50); $\beta + 8$ (5); $\beta + 9$ (1)
23	3	$X^3 + 2X + 18$	$\beta + 9$ (526); $\beta + 3$ (24)
	4	$X^4 + 3X^2 + 19X + 5$	$\beta + 7$ (526); $\beta + 9$ (23); $\beta + 11$ (1)

Table 4.5: q is composite.

q	$h \in \mathbb{F}_p[X]$	m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_{q^m}$
4	$X^2 + X + 1$	2	$X^2 + X + \alpha$	$\alpha\beta + \alpha + 1$ (18)
		3	$X^3 + \alpha X^2 + (\alpha + 1)X + \alpha$	$\alpha\beta^2 + (\alpha + 1)\beta + \alpha + 1$ (3); $\alpha\beta^2 + \alpha\beta$ (8); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (3); None (3); $\alpha\beta^2 + (\alpha + 1)\beta + 1$ (1)
		4	$X^4 + X^2 + (\alpha + 1)X + \alpha$	$\alpha\beta^3$ (15); $\alpha\beta^3 + \alpha$ (3)
		5	$X^5 + (\alpha + 1)X^4 + X + \alpha$	$\alpha\beta + \alpha$ (14); $(\alpha + 1)\beta$ (4)
		6	$X^6 + (\alpha + 1)X^5 + (\alpha + 1)X^4 + X^3 + X + \alpha + 1$	$\alpha\beta^3 + \alpha\beta$ (11); $\alpha\beta^3 + \alpha$ (7)
		7	$X^7 + \alpha X^6 + X^5 + (\alpha + 1)X^3 + X^2 + \alpha X + 1$	$\alpha\beta$ (13); $\alpha\beta + 1$ (5)
		9	$X^9 + (\alpha + 1)X^8 + \alpha X^7 + X^6 + (\alpha + 1)X^5 + \alpha X^4 + X^3 + (\alpha + 1)X + 1$	$\alpha\beta^2 + \alpha\beta$ (8); $\alpha\beta^2 + \alpha\beta + 1$ (2); $(\alpha + 1)\beta^2 + \alpha\beta + 1$ (1); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (6); $\alpha\beta^2 + \beta + \alpha + 1$ (1)
		15	$X^{15} + \alpha X^{14} + (\alpha + 1)X^{13} + X^{12} + \alpha X^{11} + \alpha X^{10} + X^8 + X^7 + X^6 + X^4 + (\alpha + 1)X^3 + \alpha X + 1$	$(\alpha + 1)\beta^2 + \alpha\beta + \alpha$ (4); $\alpha\beta^2 + \alpha\beta + 1$ (8); $\alpha\beta^2 + (\alpha + 1)\beta + 1$ (1); $\beta^2 + \beta + \alpha + 1$ (1); $\alpha\beta^2 + \beta + 1$ (2); $\beta^2 + \alpha\beta + \alpha + 1$ (1); $(\alpha + 1)\beta^2 + (\alpha + 1)\beta + \alpha$ (1)
		8	$X^3 + X + 1$	3
4	$X^4 + (\alpha^2 + 1)X^3 + (\alpha^2 + \alpha)X^2 + (\alpha^2 + \alpha)X + \alpha^2 + 1$			$\alpha\beta$ (62); $\alpha\beta + \alpha + 1$ (8)
6	$X^6 + (\alpha^2 + \alpha + 1)X^5 + (\alpha^2 + \alpha + 1)X^3 + X^2 + (\alpha^2 + \alpha + 1)X + 1$			$\alpha\beta$ (70)
7	$X^7 + (\alpha^2 + \alpha + 1)X^6 + (\alpha + 1)X^5 + (\alpha^2 + 1)X^4 + \alpha^2 X^3 + (\alpha + 1)X^2 + (\alpha + 1)X + \alpha^2 + 1$			$\alpha\beta^2 + \alpha\beta + \alpha^2 + \alpha$ (9); $\alpha\beta^2 + \alpha\beta + \alpha^2$ (8); $\alpha\beta^2 + \alpha\beta + \alpha$ (22); $\alpha\beta^2 + \alpha\beta$ (27); $\alpha\beta^2 + \alpha\beta + \alpha^2 + 1$ (2); $\alpha\beta^2 + \alpha\beta + \alpha^2 + \alpha + 1$ (2)
9	$X^2 + 2X + 2$	3	$X^3 + X^2 + \alpha + 1$	$\alpha\beta$ (80); $\alpha\beta + \alpha$ (8)
		4	$X^4 + (\alpha + 2)X^3 + 2X^2 + (\alpha + 1)X + 2\alpha + 1$	$\alpha\beta + \alpha + 1$ (63); $\alpha\beta + \alpha + 2$ (15); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (7); $(\alpha + 1)\beta + 2\alpha + 1$ (1); $\alpha\beta^2 + (\alpha + 2)\beta + 2$ (1); $(\alpha + 1)\beta + 1$ (1)
		8	$X^8 + (2\alpha + 2)X^7 + 2\alpha X^5 + 2\alpha X^4 + 2X^3 + (2\alpha + 1)X^2 + (2\alpha + 2)X + \alpha + 2$	$\alpha\beta^2 + \alpha\beta + 2\alpha + 1$ (47); $\alpha\beta^2 + \alpha\beta + \alpha + 2$ (19); $\alpha\beta^2 + (2\alpha + 1)\beta + 1$ (8); $\alpha\beta^2 + \alpha\beta + 2\alpha + 2$ (11); $\alpha\beta^2 + (2\alpha + 1)\beta$ (2); $\alpha\beta^2 + 2\beta + 2\alpha + 1$ (1)
16	$X^4 + X + 1$	3	$X^3 + (\alpha + 1)X + \alpha^2$	$\alpha\beta + \alpha$ (223); $\alpha\beta + \alpha + 1$ (41); $\alpha\beta + \alpha^2 + \alpha + 1$ (6)
		15	$X^{15} + (\alpha^3 + 1)X^{14} + (\alpha^3 + \alpha^2 + \alpha + 1)X^{13} + \alpha^3 X^{12} + \alpha X^{11} + (\alpha^2 + \alpha + 1)X^{10} + (\alpha^3 + \alpha^2)X^9 + \alpha X^8 + (\alpha^2 + \alpha)X^7 + (\alpha^2 + 1)X^6 + (\alpha^3 + \alpha)X^5 + (\alpha^2 + \alpha + 1)X^4 + \alpha^2 X^3 + (\alpha^3 + \alpha^2)X^2 + (\alpha^2 + \alpha)X + \alpha^3 + \alpha$	$\alpha\beta + \alpha^3$ (93); $\alpha\beta + \alpha + 1$ (21); $\alpha\beta + \alpha$ (133); $\alpha\beta + \alpha^2 + 1$ (17); $\alpha\beta + \alpha^3 + \alpha + 1$ (4); $\alpha\beta + \alpha^3 + \alpha$ (2)
25	$X^2 + 4X + 2$	3	$X^3 + (3\alpha + 3)X^2 + 2\alpha X + 2\alpha + 2$	$\alpha\beta$ (575); $\alpha\beta + \alpha$ (67); $\alpha\beta + 2\alpha + 2$ (5); $\alpha\beta + 2\alpha + 1$ (1)

than those appearing in Theorem 1.3, but we have no exceptions at all if all of the entries of A are non-zero. This is somehow surprising, if we consider the vast number of different transformations that the various A 's define. Also, note that the (infinite) family $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $q = 2$ and m odd consists solely of genuine exceptions. See the remark following Proposition 4.6 for a more detailed account of this delicate case.

CHAPTER 5

Extending the (strong) primitive normal basis theorem II

In this chapter, we consider Problem 1.5. Our approach is similar to the one of the previous chapter, but since now we have four conditions (instead of three), more effort is required in order to achieve sufficient conditions for Problem 1.5 to be answered positively, and even then end up with stronger conditions, harder to satisfy. As a result, we prove that this question can be answered positively, when $q \geq 23$ and $m \geq 17$, and leave the remaining cases unresolved. Nonetheless, we try to prove all results in their full generality.

5.1 Some estimates

The purpose of this section is to prove Proposition 5.1, which provides us with a condition for the existence of elements with the desired properties. Towards that, we express the number of elements with the desired properties with the help of the functions presented earlier, leading us to character sums. After that, utilizing the results of the previous section, we prove Proposition 5.1. Also, note that due to the complexity of the character sums it is necessary to distinguish four cases depending on the form of A , A is neither upper triangular nor anti-diagonal, A is upper triangular, but not diagonal, A is anti-diagonal and A is diagonal, resulting four subsections.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, $q_i \mid q_0$ and $F_i \mid F_0$, for $i = 1, 2$, where q_0 and F_0 stand for the radicals of $q^m - 1$ and $X^m - 1$ respectively; in particular $F_0 = X^{m_0} - 1$. We denote by \mathbf{k} the quadruple (q_1, q_2, F_1, F_2) and call it a *divisor quadruple*. Furthermore, we call an element $x \in \mathbb{F}_{q^m}$ \mathbf{k}_A -free over \mathbb{F}_q , if x is q_1 -free and F_1 -free over \mathbb{F}_q and $(ax + b)/(cx + d)$ is q_2 -free and F_2 -free over \mathbb{F}_q . Also we denote by $N_A(\mathbf{k})$ the number of $x \in \mathbb{F}_{q^m}$ that are \mathbf{k}_A -free over \mathbb{F}_q . We write $\mathbf{l} \mid \mathbf{k}$, if $\mathbf{l} = (d_1, d_2, G_1, G_2)$ and $d_i \mid q_i$ and $G_i \mid F_i$ for $i = 1, 2$. Further, \mathbf{w} stands for (q_0, q_0, F_0, F_0) and $\mathbf{1}$ stands for $(1, 1, 1, 1)$, while the greatest common divisor and the least common multiple of a set of divisor quadruples are defined point-wise. A divisor quadruple \mathbf{p} is called *prime* if it has exactly one entry that is $\neq 1$ and this entry is either a prime number or an irreducible polynomial. Finally, if two or more divisor quadruples are co-prime, i.e. their greatest common divisor is 1, then their product can be defined naturally.

Example. If $q = 5$ and $m = 4$, then $q_0 = 78$ (since $q^m - 1 = 624 = 2^4 \cdot 3 \cdot 13$ and $2 \cdot 3 \cdot 13 = 78$) and $F_0 = X^4 - 1 = (X - 1)(X - 2)(X - 3)(X - 4) \in \mathbb{F}_5[X]$, since $m = m_0 = 4$. In that case, four distinct divisor quadruples would be $\mathbf{e}_0 := (2, 6, X^2 - 1, 1)$, $\mathbf{p}_1 := (1, 1, 1, X - 1)$, $\mathbf{p}_2 := (3, 1, 1, 1)$ and $\mathbf{p}_3 := (1, 1, 1, X + 1)$. It is clear that \mathbf{e}_0 , \mathbf{p}_1 , \mathbf{p}_2 and \mathbf{p}_3 are non-trivial, co-prime divisor quadruples, while \mathbf{e}_0 is non-prime and \mathbf{p}_1 , \mathbf{p}_2 and \mathbf{p}_3 are primes. Also, since they are co-prime, we can define $\mathbf{e} := \mathbf{e}_0 \cdot \mathbf{p}_1 \cdot \mathbf{p}_2 \cdot \mathbf{p}_3 = (6, 6, X^2 - 1, X^2 - 1)$.

It is clear that for our purposes it suffices to show that $N_A(\mathbf{w}) > 0$. In the next subsections we are going to express $N_A(\mathbf{k})$ in terms of character sums and export some useful expressions. From the fact that ω and Ω are characteristic functions we have that:

$$N_A(\mathbf{k}) = \sum_x \omega_{q_1}(x) \Omega_{F_1}(x) \omega_{q_2} \left(\frac{ax + b}{cx + d} \right) \Omega_{F_2} \left(\frac{ax + b}{cx + d} \right), \quad (5.1)$$

where the sum runs over \mathbb{F}_{q^m} , except $-d/c$ if $c \neq 0$.

Let $\mathbf{k} = (q_1, q_2, F_1, F_2)$ be a divisor quadruple, from now on we will denote by $f(\mathbf{k})$ the product $f(q_1)f(q_2)f(F_1)f(F_2)$, where f may be θ , φ , μ or W^1 . The purpose of the rest of this section is to prove the following.

Proposition 5.1. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$ and \mathbf{k} be a divisor quadruple. If $q^{m/2} > 4W(\mathbf{k})$, then $N_A(\mathbf{k})$ is positive, provided that $q \neq 2$ and if A has exactly two non-zero entries and γ is their quotient, then $\tau(\gamma) = 1$, where τ is the quadratic character.*

Remark 5.2. In the following subsections we will prove the above proposition for all possible forms of A . Also, it will become clear why the restriction $q \neq 2$ as well as the restriction regarding the entries are indeed necessary.

5.1.1 Matrices that are neither upper triangular nor anti-diagonal

In this subsection we assume that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, where $c \neq 0$ and at most one of the other entries is zero. A more convenient expression of $N_A(\mathbf{k})$ is desirable, i.e. Eq. (5.1) can be rewritten as:

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}|\mathbf{k}} \frac{\mu(\mathbf{l})}{\varphi(\mathbf{l})} \sum_{\chi_i, \psi_i} \mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2), \quad (5.2)$$

where

$$\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2) := \sum_{x \neq -d/c} \chi_1(x) \chi_2 \left(\frac{ax + b}{cx + d} \right) \psi_1(x) \psi_2 \left(\frac{ax + b}{cx + d} \right).$$

Proposition 5.3. *Let χ_1, χ_2 be multiplicative characters and ψ_1, ψ_2 be additive characters such that $(\chi_1, \chi_2, \psi_1, \psi_2) \neq (\chi_o, \chi_o, \psi_o, \psi_o)$, then*

$$|\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2)| \leq 4q^{m/2}.$$

Proof. There exist some $n_i \in \{0, 1, \dots, q^m - 2\}$ such that $\chi_i(x) = \chi_g(x^{n_i})$ and some $y_i \in \mathbb{F}_{q^m}$ such that $\psi_i(x) = \psi_g(y_i x)$, for $i = 1, 2$. It follows that

$$\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2) = \sum_{x \neq -d/c} \chi_g(\mathcal{F}(x)) \psi_g(\mathcal{G}(x)), \quad (5.3)$$

¹For the explicit definitions of these functions see the previous chapter.

where $\mathcal{F}(X) := (X^{n_1}(aX + b)^{n_2})/(cX + d)^{n_2} \in \mathbb{F}_q(X)$ and $\mathcal{G}(X) := (y_1X(cX + d) + y_2(aX + b))/(cX + d) \in \mathbb{F}_q(X)$. We prove the desired result for all possible forms of \mathcal{F} and \mathcal{G} .

From Eq. (5.3), Theorem 2.13 implies that if $\mathcal{F} \neq y\mathcal{H}^{q^m-1}$, for any $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$, and $\mathcal{G} \neq \mathcal{H}^p - \mathcal{H} + y$, for any $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$, then

$$|\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2)| \leq 4q^{m/2}.$$

Assume $\mathcal{F} = y\mathcal{H}^{q^m-1}$ for some $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$. In that case $n_1 = n_2 = 0$. To see this, write $\mathcal{H} = H_1/H_2$, where H_1, H_2 are co-prime polynomials over \mathbb{F}_{q^m} . It follows that

$$X^{n_1}(aX + b)^{n_2}H_2^{q^m-1} = y(cX + d)^{n_2}H_1^{q^m-1}.$$

Since H_1 and H_2 are co-prime, the above equation implies $H_2^{q^m-1} \mid (cX + d)^{n_2}$, that is H_2 is constant, since $n_2 < q^m - 1$. By considering degrees, we conclude that H_1 is also constant and that $n_1 = 0$. It follows that $(aX + b)^{n_2} = y'(cX + d)^{n_2}$, where $y' := yH_1^{q^m-1}H_2^{1-q^m} \in \mathbb{F}_{q^m}$, impossible for $A \in \text{GL}_2(\mathbb{F}_q)$, unless $n_2 = 0$. Additionally, if $y_1 = 0$ and $y_2 \neq 0$, then, from Eq. (5.3), we have that

$$\begin{aligned} |\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2)| &= \left| \sum_{x \neq -d/c} \psi \left(\frac{y_2(ax + b)}{cx + d} \right) \right| = \left| \sum_{y \neq 0} \psi \left(\frac{y_2a}{c} + \frac{y_2(bc - da)}{cy} \right) \right| \\ &= \left| \psi(y_2a/c) \sum_{y \neq 0} \psi(y) \right| = \left| -1 + \sum_{y \in \mathbb{F}_{q^m}} \psi(y) \right| = 1, \end{aligned}$$

according to Lemma 2.2. Similarly, if $y_1 \neq 0$ and $y_2 = 0$, then

$$\begin{aligned} |\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2)| &= \left| \sum_{x \neq -d/c} \psi_g(y_1x) \right| = \left| -\psi_g(-y_1d/c) + \sum_{x \in \mathbb{F}_{q^m}} \psi_1(x) \right| \\ &= |-\psi_g(-y_1d/c)| = 1. \end{aligned}$$

Finally, if $y_1, y_2 \neq 0$, then Eq. (5.3) yields

$$\begin{aligned} |\mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2)| &= \left| \sum_{x \neq -d/c} \psi_g((y_1x(cx + d) + y_2(ax + b))/(cx + d)) \right| \\ &= \left| \sum_{y \neq 0} \psi_g(y y_1/c + y^{-1} y_2(-da + bc)/c + (y_2a - y_1d)/c) \right| \\ &= \left| \psi_g(z_0) \sum_{y \neq 0} \psi_g(z_1y + z_2y^{-1}) \right| = \left| \sum_{y \neq 0} \psi_g(z_1y + z_2y^{-1}) \right|, \end{aligned}$$

where $z_0 := (y_2a - y_1d)/c$, $z_1 := y_1/c$ and $z_2 := y_2(-da + bc)/c$. It follows that, since both z_1 and z_2 are non-zero, the last sum is bounded by $2q^{m/2}$, from Lemma 2.11.

Assume $\mathcal{G} = \mathcal{H}^p - \mathcal{H} + y$ for some $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$. Write $\mathcal{H} = H_1/H_2$, where H_1, H_2 are co-prime polynomials over \mathbb{F}_{q^m} . If $\mathcal{G} \neq 0$, then

$$\mathcal{G} = \mathcal{H}^p - \mathcal{H} + y \Rightarrow \frac{y_1X(cX + d) + y_2(aX + b)}{cX + d} = \frac{H_1^p - H_1H_2^{p-1} + yH_2^p}{H_2^p}.$$

It follows immediately from the restrictions on A that $cX + d$ is co-prime to $y_1X(cX + d) + y_2(aX + b)$ and it is clear that H_2^p is co-prime to $H_1^p - H_1H_2^{p-1} + yH_2^p$, hence $cX + d = H_2^p$, a contradiction since $c \neq 0$. It follows that $\mathcal{G} = 0$, that is $y_1 = y_2 = 0$. Additionally, if at least one of n_1, n_2 is non-zero it follows that the polynomial $X^{n_1}(aX + b)^{n_2}(cX + d)^{q^m-1-n_2}$ has at most three distinct roots and is not of the form yH^{q^m-1} , for $y \in \mathbb{F}_{q^m}, H \in \mathbb{F}_{q^m}[X]$. Now, from Eq. (5.3), we have

$$\begin{aligned} \mathcal{X}_A(\chi_1, \chi_2, \psi_1, \psi_2) &= \sum_{x \neq -d/c} \chi_g(x^{n_1}(ax + b)^{n_2}(cx + d)^{-n_2}) \\ &= \sum_{x \in \mathbb{F}_{q^m}} \chi_g(x^{n_1}(ax + b)^{n_2}(cx + d)^{q^m-1-n_2}), \end{aligned}$$

but the last sum is bounded by $2q^{m/2}$, from Theorem 2.10. \square

Proposition 5.3 and Eq. (5.2) imply

$$N_A(\mathbf{k}) \geq \theta(\mathbf{k}) \left(q^m - 1 - 4q^{m/2} \sum_{\mathbf{l}|\mathbf{k}, \mathbf{l} \neq \mathbf{1}} \frac{\mu(\mathbf{l})}{\varphi(\mathbf{l})} \sum_{\chi_1, \chi_2, \psi_1, \psi_2} 1 \right).$$

The above, combined with Eq. (2.4), is rewritten as

$$\begin{aligned} N_A(\mathbf{k}) &\geq \theta(\mathbf{k}) q^{m/2} \left(q^{m/2} - \frac{1}{q^{m/2}} - 4 \sum_{\mathbf{l}|\mathbf{k}, \mathbf{l} \neq \mathbf{1}} \mu(\mathbf{l}) \right) \\ \Rightarrow N_A(\mathbf{k}) &\geq \theta(\mathbf{k}) q^{m/2} (q^{m/2} - q^{-m/2} - 4(2^{t_{q_1} + t_{q_2} + t_{r_1} + t_{r_2}} - 1)). \end{aligned}$$

Summing up, we have proved the following, which clearly implies Proposition 5.1, provided A is of the described form.

Proposition 5.4. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, where $c \neq 0$ and at most one of the other entries is zero. Let \mathbf{k} be a divisor quadruple. If $q^{m/2} > 4W(\mathbf{k}) - \frac{7}{2}$, then $N_A(\mathbf{k})$ is positive.*

5.1.2 Upper triangular matrices that are not diagonal

In this section we focus on matrices of the form $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, with $b \neq 0$.

As in Subsection 5.1.1, we have

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}|\mathbf{k}} \frac{\mu(\mathbf{l})}{\varphi(\mathbf{l})} \sum_{\chi_i, \psi_i} \psi_2(b/d) \mathcal{Y}_A(\chi_1, \chi_2, \psi_1, \psi_2), \quad (5.4)$$

where

$$\begin{aligned} \mathcal{Y}_A(\chi_1, \chi_2, \psi_1, \psi_2) &:= \sum_{x \in \mathbb{F}_{q^m}} \chi_1(x) \chi_2 \left(\frac{ax + b}{d} \right) (\psi_1 \psi_2')(x) \\ &= \sum_{x \in \mathbb{F}_{q^m}} \chi \left(x^{n_1} \left(\frac{ax + b}{d} \right)^{n_2} \right) (\psi_1 \psi_2')(x), \end{aligned}$$

where $\psi_2'(x) := \psi_2(ax/d)$ for $x \in \mathbb{F}_{q^m}$, an additive character with the same Order as ψ_2 and $\psi_1 \psi_2'$ is the product of ψ_1 and ψ_2' , i.e. another additive character. If all

$\chi_1, \chi_2, (\psi_1 \psi_2')$ are non-trivial, then $|\mathcal{Y}_A(\chi_1, \chi_2, \psi_1, \psi_2)| \leq 2q^{m/2}$, from Theorem 2.13. If exactly two of $\chi_1, \chi_2, (\psi_1 \psi_2')$ are non-trivial, then Theorems 2.10 and 2.13 imply $|\mathcal{Y}_A(\chi_1, \chi_2, \psi_1, \psi_2)| \leq q^{m/2}$. If exactly one of $\chi_1, \chi_2, \psi_1 \psi_2'$ is non-trivial, Lemma 2.2 implies $\mathcal{Y}_A(\chi_1, \chi_2, \psi_1, \psi_2) = 0$. Now, as in section 5.1.1, we get

$$\left| \frac{N_A(\mathbf{k})}{\theta(\mathbf{k})} - q^m \sum_{G|\gcd(F_1, F_2)} \frac{\mu(G)^2}{\varphi(G)^2} \sum_{\text{Ord}(\psi_2)=G} \psi_2\left(\frac{b}{d}\right) \right| \leq 2q^{m/2}(W(\mathbf{k}) - 4). \quad (5.5)$$

Eq. (5.5) suggests that a lower bound for the coefficient of q^m is desirable. Set $F_3 := \gcd(F_1, F_2)/(X-1)$, if $X-1 \mid \gcd(F_1, F_2)$ and $F_3 := \gcd(F_1, F_2)$ otherwise. Further, set $\gamma := b/d \neq 0$. It follows immediately from Lemma 4.3 that $\psi(\gamma) = 1$ for any additive character ψ whose Order divides F_3 . First, suppose $X-1 \mid \gcd(F_1, F_2)$. With the help of Lemmata 2.2, 4.4 and 4.5, we evaluate:

$$\begin{aligned} & \sum_{G|\gcd(F_1, F_2)} \frac{\mu^2(G)}{\varphi^2(G)} \sum_{\text{Ord}(\psi)=G} \psi(\gamma) \\ &= \sum_{G|F_3} \frac{1}{\varphi^2(G)} \sum_{\text{Ord}(\psi)=G} \psi(\gamma) + \sum_{G|F_3} \frac{1}{\varphi^2((X-1)G)} \sum_{\text{Ord}(\psi)=(X-1)G} \psi(\gamma) \\ &= \sum_{G|F_3} \frac{1}{\varphi(G)} + \sum_{G|F_3} \frac{1}{\varphi^2((X-1)G)} \left(\sum_{\text{Ord}(\psi_1)=G} \psi_1(\gamma) \right) \left(\sum_{\text{Ord}(\psi_2)=X-1} \psi_2(\gamma) \right) \\ &= \left(1 - \frac{1}{\varphi(X-1)^2} \right) \sum_{G|F_3} \frac{1}{\varphi(G)} = \frac{q(q-2)}{(q-1)^2} \sum_{G|F_3} \frac{1}{\varphi(G)} \geq \frac{q(q-2)}{(q-1)^2}. \end{aligned}$$

Similarly, if $X-1 \nmid \gcd(F_1, F_2)$, then

$$\sum_{G|\gcd(F_1, F_2)} \frac{\mu^2(G)}{\varphi^2(G)} \sum_{\text{Ord}(\psi)=G} \psi(\gamma) = \sum_{G|F_3} \frac{1}{\varphi(G)} \geq 1.$$

Summing up, Eqs. (5.4) and (5.5) give

$$N_A(\mathbf{k}) \geq \theta(\mathbf{k})q^{m/2} \left(q^{m/2} \frac{q(q-2)}{(q-1)^2} + 4 - 2W(\mathbf{k}) \right),$$

which implies the following.

Proposition 5.5. *Let $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, where $b \neq 0$ and \mathbf{k} be a divisor quadruple. If*

$$q^{m/2} \frac{q(q-2)}{(q-1)^2} > 2W(\mathbf{k}) - 4,$$

then $N_A(\mathbf{k})$ is positive.

Remark 5.6. If $q = 2$, then the left part of the latter is zero and the inequality holds only for $\mathbf{k} = 1$. This is not a surprise, since one easily checks that in this case $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and, therefore, Problem 1.5 holds if there exists some $x \in \mathbb{F}_{2^m}$ such that x and $x+1$ are both free over \mathbb{F}_2 , impossible from the definition of free elements for m odd. On the other hand, Proposition 5.1 is clearly implied, provided that A is of the described form.

5.1.3 Anti-diagonal matrices

In this subsection we assume that $A = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, $\gamma := b/c$ and $\tau(\gamma) = 1$, where τ is the quadratic character. The following lemma will prove to be useful.

Lemma 5.7. *Let α, β be integers such that β/α is an odd integer and β is square-free. Then*

$$\frac{\beta}{\varphi(\beta)} \prod_{\substack{p|\frac{\beta}{\alpha} \\ p \text{ prime}}} \frac{p-2}{p-1} > \frac{1}{2}.$$

Proof. Write $\beta/\alpha = p_1 \cdots p_k$, where p_i are primes such that $p_i < p_j$, for $i < j$. Clearly, our statement is true for $k \in \{0, 1\}$. Suppose $k \geq 2$, then it follows that

$$B := \frac{\beta}{\varphi(\beta)} \prod_{\substack{p|\frac{\beta}{\alpha} \\ p \text{ prime}}} \frac{p-2}{p-1} = \frac{p_1-2}{p_1-1} \cdot \frac{\beta}{\varphi(\beta)} \prod_{i=2}^k \frac{p_i-2}{p_i-1}.$$

Since the function $f(x) = (x-2)/(x-1)$ is increasing for $x > 1$, we deduce

$$B \geq \frac{p_1-2}{p_1-1} \cdot \frac{\beta}{\varphi(\beta)} \prod_{i=1}^{k-1} \frac{p_i-1}{p_i} = \frac{p_1-2}{p_1-1} \cdot \frac{\beta}{\varphi(\beta)} \cdot \frac{\varphi(\beta/p_k\alpha)}{\beta/p_k\alpha} = \frac{p_1-2}{p_1-1} \cdot \frac{\alpha p_k}{\varphi(\alpha p_k)}.$$

The result follows, since $p_1 \geq 3$. \square \square

As in Subsection 5.1.1, we conclude

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}|\mathbf{k}} \frac{\mu(\mathbf{l})}{\varphi(\mathbf{l})} \sum_{\chi, \psi_i} \chi_2(\gamma) \mathcal{Z}_A(\chi_1, \chi_2, \psi_1, \psi_2), \quad (5.6)$$

where

$$\mathcal{Z}_A(\chi_1, \chi_2, \psi_1, \psi_2) := \sum_{x \neq 0} (\chi_1 \bar{\chi}_2)(x) \psi_1(x) \psi_2(\gamma x^{-1}).$$

If at least two of ψ_1, ψ_2 and $(\chi_1 \bar{\chi}_2)$ (where $(\chi_1 \bar{\chi}_2)$ is the product of χ_1 and $\bar{\chi}_2$, another multiplicative character), are non-trivial, then $|\mathcal{Z}_A(\chi_1, \chi_2, \psi_1, \psi_2)|$ is bounded by $2q^{m/2}$, from Lemma 2.11. If exactly one of ψ_1, ψ_2 and $(\chi_1 \bar{\chi}_2)$ is non-trivial, from Lemma 2.2, then $|\mathcal{Z}_A(\chi_1, \chi_2, \psi_1, \psi_2)| = 0$. We eventually get

$$\left| \frac{N_A(\mathbf{k})}{\theta(\mathbf{k})} - (q^m - 1) \sum_{d|\mathrm{gcd}(q_1, q_2)} \frac{\mu^2(d)}{\varphi^2(d)} \sum_{\mathrm{ord}(\chi_2)=d} \chi_2(\gamma) \right| \leq 2q^{m/2}(W(\mathbf{k}) - 4). \quad (5.7)$$

Eq. (5.7) implies that a lower bound for the coefficient of q^m is desirable. Set $q_3 := \mathrm{gcd}(q_1, q_2)$. Furthermore, we observe that the function

$$f(x) = \sum_{d|x} \frac{\mu^2(d)}{\varphi^2(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(\gamma)$$

is multiplicative. Consequently, if we write $q_3 = p_1^{n_1} \cdots p_l^{n_l}$, where the p_i 's are distinct primes, then the coefficient of q^m in Eq. (5.7) can be rewritten as

$$\prod_{i=1}^l \sum_{d|p_i^{n_i}} \frac{\mu^2(d)}{\varphi^2(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(\gamma) = \prod_{\substack{p|q_3 \\ p \text{ prime}}} \left(1 + \frac{1}{(p-1)^2} \sum_{\mathrm{ord}(\chi)=p} \chi(\gamma) \right).$$

It is clear that if a prime p divides q_3 , then $\sum_{\text{ord}(\chi)=p} \chi(\gamma)$ is $p-1$, if $\chi(\gamma) = 1$ for all multiplicative characters χ of order p , and -1 if there exists some multiplicative character χ of order p such that $\chi(\gamma) \neq 1$. Furthermore, set

$$q_4 := \prod_{\substack{p \text{ prime, } p|q_3 \\ \chi(\gamma)=1 \text{ if } \text{ord}(\chi)=p}} p.$$

With the help of these observations, the coefficient of q^m in Eq. (5.7) can be rewritten as

$$\begin{aligned} & \prod_{p \text{ prime, } p|q_4} \left(1 + \frac{1}{p-1}\right) \prod_{p \text{ prime, } p|q_3, p \nmid q_4} \left(1 - \frac{1}{(p-1)^2}\right) \\ &= \prod_{p|q_3, p \text{ prime}} \frac{p}{p-1} \prod_{p \text{ prime, } p|q_3, p \nmid q_4} \frac{p-2}{p-1} = \frac{q_3^*}{\varphi(q_3^*)} \prod_{p|\frac{q_3^*}{q_4}, p \text{ prime}} \frac{p-2}{p-1}, \end{aligned}$$

where q_3^* is the radical of q_3 . Here we note that q_3^*/q_4 is always odd. This is immediate if q_3^* is odd, i.e. q is even. If q_3^* is even, i.e. q is odd, then q_4 is also even since $\chi(\gamma) = 1$, when χ has order 2, i.e. $\chi = \tau$.

It follows immediately from Lemma 5.7 that the last expression of the coefficient of q^m in Eq. (5.7) is larger than $1/2$. Now, Eqs. (5.6) and (5.7) give:

$$N_A(\mathbf{k}) > \theta(\mathbf{k}) q^{m/2} \left(\frac{q^{m/2}}{2} - \frac{1}{2q^{m/2}} + 8 - 2W(\mathbf{k}) \right),$$

which implies the following.

Proposition 5.8. *Let $A = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, where $\tau(b/c) = 1$, where τ is the quadratic character, and \mathbf{k} be a divisor quadruple. If $q^{m/2} \geq 4W(\mathbf{k}) - 15$, then $N_A(\mathbf{k})$ is positive.*

Remark 5.9. The restriction for $\tau(b/c) = 1$ may look unnecessary, but is not. For instance, if $x \in \mathbb{F}_{q^m}$ is primitive and $y \in \mathbb{F}_{q^m}$ is not a square, i.e. $\tau(y) = -1$, then one easily checks that $(yx)^{(q^m-1)/2} = 1$, i.e. yx is not primitive. Additionally, it is clear that Proposition 5.8 implies Proposition 5.1, provided that A is of the described form.

5.1.4 Diagonal matrices

In this subsection we prove Proposition 5.1, when A is diagonal. Suppose $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, $\gamma := a/d$ and $\tau(\gamma) = 1$, where τ is the quadratic character; Eq. (5.1) becomes:

$$N_A(\mathbf{k}) = \sum_{x \in \mathbb{F}_{q^m}} \omega_{q_1}(x) \Omega_{F_1}(x) \omega_{q_2}(\gamma x) \Omega_{F_2}(\gamma x).$$

It is clear from the definition of an F_2 -free element, that since $\gamma \in \mathbb{F}_q^*$, x is F_2 -free if and only if γx is F_2 -free, i.e. $\Omega_{F_2}(\gamma x) = \Omega_{F_2}(x)$. Furthermore, $\Omega_{F_1}(x) \Omega_{F_2}(x)$ is 1, if x is simultaneously F_1 -free and F_2 -free, and 0 otherwise, but x is simultaneously F_1 -free and F_2 -free if and only if it is F_3 -free, where $F_3 := \text{lcm}(F_1, F_2)$, hence $\Omega_{F_1}(x) \Omega_{F_2}(x) = \Omega_{F_3}(x)$. It follows that

$$N_A(\mathbf{k}) = \sum_{x \in \mathbb{F}_{q^m}} \omega_{q_1}(x) \omega_{q_2}(\gamma x) \Omega_{F_3}(\gamma x).$$

Now, as in Subsection 5.1.1, we get

$$N_A(\mathbf{k}) = \theta(q_1)\theta(q_2)\theta(F_3) \sum_{d_1, d_2, G} \frac{\mu(d_1)\mu(d_2)\mu(G)}{\varphi(d_1)\varphi(d_2)\varphi(G)} \sum_{\chi_1, \psi} \chi_2(\gamma) \mathcal{W}(\chi_1, \chi_2, \psi),$$

where

$$\mathcal{W}(\chi_1, \chi_2, \psi) := \sum_{x \in \mathbb{F}_{q^m}} (\chi_1 \chi_2)(x) \psi(x).$$

Lemma 2.2 implies that $\mathcal{W}(\chi_1, \chi_2, \psi) = 0$, provided that exactly one of $(\chi_1 \chi_2)$ or ψ is non-trivial, where $(\chi_1 \chi_2)$ is the product of χ_1 and χ_2 , a multiplicative character. If both $\chi_1 \chi_2$ and ψ are non-trivial, then Theorem 2.13 implies that $|\mathcal{W}(\chi_1, \chi_2, \psi)| \leq q^{m/2}$. Now, as in previous subsections, we get

$$\left| \frac{N_A(\mathbf{k})}{\theta(q_1)\theta(q_2)\theta(F_3)} - q^m \sum_{d | \gcd(q_1, q_2)} \frac{\mu^2(d)}{\varphi^2(d)} \sum_{\text{ord}(\chi_2)=d} \chi_2(\gamma) \right| \leq q^{m/2} (W(q_1)W(q_2)W(F_3) - 3).$$

The coefficient of q^m in the above equation was proved to be larger than $1/2$ in Subsection 5.1.3, hence we get

$$N_A(\mathbf{k}) > \theta(q_1)\theta(q_2)\theta(F_3) q^{m/2} \left(\frac{q^{m/2}}{2} + 6 - W(q_1)W(q_2)W(F_3) \right),$$

which clearly implies the following.

Proposition 5.10. *Let $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, where $\tau(a/d) = 1$, where τ is the quadratic character, and \mathbf{k} be a divisor quadruple. If $q^{m/2} \geq 2W(\mathbf{k}) - 12$, then $N_A(\mathbf{k})$ is positive.*

Remark 5.11. Clearly, the bound of the above proposition is far from optimal, since the much weaker condition $q^{m/2} \geq 2W(q_1)W(q_2)W(F_3) - 12$ could be used instead. Despite being non-optimal, Proposition 5.10 fits our purposes and is consistent with the rest of this paper. Nonetheless, it is clear that if we restricted ourselves to diagonal matrices, then we could get significantly better results. Moreover, one easily checks that the comments of Remark 5.9 apply in this case as well.

5.2 The sieve

Following Cohen and Huczynska [12, 13], like we did in Section 4.2, we introduce a sieve that will help us relax the condition proved in the previous section. The propositions included in this section are those of Cohen and Huczynska [13], adjusted properly. Moreover, from now on we assume that if A has exactly two non-zero entries and γ is their quotient, then $\tau(\gamma) = 1$, where τ stands for the quadratic character. In particular, A may have two, three or four non-zero entries with the above further condition in the case it has exactly two non-zero entries.

Let $\mathbf{k} = (q_1, q_2, F_1, F_2)$ be a divisor quadruple. A set of complementary divisor quadruples of \mathbf{k} , with common divisor \mathbf{k}_0 is a set $\{\mathbf{k}_1, \dots, \mathbf{k}_r\}$, where the \mathbf{k}_i 's are divisor quadruples such that $\mathbf{k}_i | \mathbf{k}$ for every i , their least common multiplier is divided

by the radical of \mathbf{k} and $(\mathbf{k}_i, \mathbf{k}_j) = \mathbf{k}_0$ for every $i \neq j$. Furthermore, if $\mathbf{k}_1, \dots, \mathbf{k}_r$ are such that $\mathbf{k}_i = \mathbf{k}_0 \mathbf{p}_i$, where $\mathbf{p}_1, \dots, \mathbf{p}_r$ are distinct prime divisor quadruples, co-prime to \mathbf{k}_0 , then this particular set of complementary divisors is called a (\mathbf{k}_0, r) -decomposition of \mathbf{k} . For a (\mathbf{k}_0, r) -decomposition of \mathbf{k} we define $\delta := 1 - \sum_{i=1}^r 1/|\mathbf{p}_i|$, where $|\mathbf{p}_i|$ stands for the absolute value of the unique entry $\neq 1$ of \mathbf{p}_i , if this entry is a number, and $q^{\deg(F)}$, if this entry is $F \in \mathbb{F}_q[X]$. Finally, we define $\Delta := (r-1)/\delta + 2$. The following is a supplement to the example of page 46 and helps us understand the new concepts defined here.

Example. Make all the assumptions of the example in page 46. Further, set $\mathbf{e}_1 := (2, 6, X^2 - 1, X - 1)$, $\mathbf{e}_2 := (6, 6, X^2 - 1, 1)$ and $\mathbf{e}_3 := (2, 6, X^2 - 1, X + 1)$. Clearly, $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ is a set of complementary divisors of \mathbf{e} with common divisor \mathbf{e}_0 . In particular, observe that $\mathbf{p}_1, \mathbf{p}_2$ and \mathbf{p}_3 are all co-prime to \mathbf{e}_0 and $\mathbf{e}_0 \mathbf{p}_i = \mathbf{e}_i$ for $i \in \{1, 2, 3\}$, hence $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ is also a $(\mathbf{e}_0, 3)$ -decomposition of \mathbf{e} . For this decomposition, we compute $\delta = 1 - \frac{1}{3} - \frac{1}{5} - \frac{1}{5} = \frac{4}{15}$ and $\Delta = 19/2$

Proposition 5.12 (Sieving inequality). *Let $A \in \text{GL}_2(\mathbb{F}_q)$, \mathbf{k} be a divisor quadruple and $\{\mathbf{k}_1, \dots, \mathbf{k}_r\}$ be a set of complementary divisors of \mathbf{k} with common divisor \mathbf{k}_0 . Then*

$$N_A(\mathbf{k}) \geq \sum_{i=1}^r N_A(\mathbf{k}_i) - (r-1)N_A(\mathbf{k}_0).$$

Proof. The proof is identical to the proof of Proposition 4.9, where the word ‘triple’ is replaced by the word ‘quadruple’. \square

Proposition 5.13. *Let \mathbf{k} be a divisor quadruple with a (\mathbf{k}_0, r) -decomposition, such that $\delta > 0$ and $\mathbf{k}_0 = (q_1, q_1, F_1, F_1)$ for some $q_1 \mid q_0$ and $F_1 \mid F_0$. If $A \in \text{GL}_2(\mathbb{F}_q)$, $q > 2$ and $q^{m/2} > 4W(\mathbf{k}_0)\Delta$, then $N_A(\mathbf{k}) > 0$.*

Proof. Let $\mathbf{p}_1, \dots, \mathbf{p}_r$ be the primes of the (\mathbf{k}_0, r) -decomposition. Proposition 5.12 implies

$$N_A(\mathbf{k}) \geq \delta N_A(\mathbf{k}_0) + \sum_{i=1}^r \left(N_A(\mathbf{k}_0 \mathbf{p}_i) - \left(1 - \frac{1}{|\mathbf{p}_i|}\right) N_A(\mathbf{k}_0) \right). \quad (5.8)$$

Suppose A is of the form described in Subsection 5.1.1. In that case, taking into account the analysis done in subsection 5.1.1, Eq. (5.8) implies

$$N_A(\mathbf{k}) \geq \delta \theta(\mathbf{k}_0) \left(q^m - 1 + \sum_{\substack{\mathbf{l} \mid \mathbf{k}_0 \\ \mathbf{l} \neq \mathbf{1}}} U(\mathbf{l}) \right) + \theta(\mathbf{k}_0) \sum_{i=1}^r \left(1 - \frac{1}{|\mathbf{p}_i|}\right) \sum_{\substack{\mathbf{l} \mid \mathbf{k}_0 \mathbf{p}_i \\ \mathbf{l} \nmid \mathbf{k}_0}} U_i(\mathbf{l}),$$

where the absolute values of the expressions $U(\mathbf{l})$ and $U_i(\mathbf{l})$ does not exceed $4q^{m/2}$. Since $\delta > 0$ it follows that $N_A(\mathbf{k}) > 0$ if

$$\delta q^{m/2} > 4\delta W(\mathbf{k}_0) + 4 \sum_{i=1}^r (W(\mathbf{k}_0 \mathbf{p}_i) - W(\mathbf{k}_0)) \left(1 - \frac{1}{|\mathbf{p}_i|}\right).$$

The result follows, since $W(\mathbf{k}_0 \mathbf{p}_i) - W(\mathbf{k}_0) = W(\mathbf{k}_0)$ and $\sum_{i=1}^r \left(1 - \frac{1}{|\mathbf{p}_i|}\right) = r - 1 + \delta$.

Suppose A falls in the categories examined in subsections 5.1.2 and 5.1.3. With the help of the analysis of those subsections and Eq. (5.8), we conclude that

$$N_A(\mathbf{k}) \geq \delta\theta(\mathbf{k}_0) \left(\kappa q^m + \lambda_A + \sum_{\substack{\mathbf{l}|\mathbf{k}_0 \\ \mathbf{l} \neq \mathbf{1}}} U(\mathbf{l}) \right) + \theta(\mathbf{k}_0) \sum_{i=1}^r \left(1 - \frac{1}{|\mathbf{p}_i|} \right) \sum_{\substack{\mathbf{l}|\mathbf{k}_0 \mathbf{p}_i \\ \mathbf{l} \nmid \mathbf{k}_0}} U_i(\mathbf{l}),$$

where $\kappa \geq 1/2$, λ_A is -1 if A is anti-diagonal and 0 otherwise and the absolute values of the expressions $U(\mathbf{l})$ and $U_i(\mathbf{l})$ does not exceed $2q^{m/2}$. The result follows as above.

Finally, suppose A is diagonal. We recall the facts proven in subsection 5.1.4. Eq. (5.8) gives

$$\begin{aligned} N_A(\mathbf{k}) \geq & \delta\theta^2(q_1)\theta(F_1) \left(\kappa q^m + \sum_{\substack{d_1|q_1, d_2|q_1, G|F_1 \\ \text{not all } =1}} U(d_1, d_2, G) \right) \\ & + \theta^2(q_1)\theta(F_1) \sum_{i=1}^{r'} \left(1 - \frac{1}{|\mathbf{p}_i|} \right) \sum_{\substack{d_1|q_{i,1}, d_2|q_{i,2} \text{ and } G|F_{i,1} \\ d_1 \nmid q_1, d_2 \nmid q_2 \text{ or } G \nmid F_1}} U_i(d_1, d_2, G), \end{aligned}$$

where $\mathbf{p}_1, \dots, \mathbf{p}_{r'}$ are exactly those prime divisor quadruples, appearing in the (\mathbf{k}_0, r) -decomposition of \mathbf{k} , whose fourth entry is 1 , $(q_{i,1}, q_{i,2}, F_{i,1}, F_{i,2}) = \mathbf{k}_0 \mathbf{p}_i$, the absolute values of the expressions $U(d_1, d_2, G)$ and $U_i(d_1, d_2, G)$ does not exceed $q^{m/2}$ and $\kappa \geq 1/2$. The result follows as above. \square

Recall the arguments prior to Proposition 4.11 regarding the factorization of F_0 . As then, from now on, s will stand for the minimal natural number, such that $m_0 \mid q^s - 1$ and G_0 will stand for the product of the irreducible factors of F_0 of degree s .

Proposition 5.14. *Let $\{l_1, \dots, l_t\}$ be a set of distinct primes (this set may be \emptyset , in which case $t = 0$) dividing q_0 and $r_0 := \deg(F_0/G_0)$. If*

$$q^{m/2} > 4^{1-t} W^2(q_0) W^2(F_0/G_0) \left(\frac{q^s(2(m_0 - r_0) + s(2t - 1))}{sq^s(1 - 2 \sum_{i=1}^t 1/l_i) - 2(m_0 - r_0)} + 2 \right),$$

then $N_A(\mathbf{w}) > 0$, provided that the denominator of the inequality is positive.

Proof. Let $G_0 = \prod_{i=1}^{r_1} G_i$ be the factorization of G_0 into monic irreducible polynomials. Consider a $(\mathbf{k}_0, 2(r_1 + t))$ -decomposition of \mathbf{w} , where

$$\mathbf{k}_0 = \left(\frac{q_0}{\prod_{i=1}^t l_i}, \frac{q_0}{\prod_{i=1}^t l_i}, \frac{F_0}{G_0}, \frac{F_0}{G_0} \right).$$

Clearly, the prime divisor quadruples of this decomposition are exactly those who have exactly one $\neq 1$ entry and this entry is either l_i , for some $i = 1, \dots, t$, or G_i , for some $i = 1, \dots, r_1$. Proposition 5.13 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 4^{1-t} W^2(q_0) W^2(F_0/G_0) \left(\frac{2(r_1 + t) - 1}{1 - 2 \sum_{i=1}^t 1/l_i - 2 \sum_{i=1}^{r_1} 1/q^s} + 2 \right),$$

that is

$$q^{m/2} > 4^{1-t} W^2(q_0) W^2(F_0/G_0) \left(\frac{q^s(2sr_1 + s(2t-1))}{sq^s(1 - 2\sum_{i=1}^t 1/l_i) - 2sr_1} + 2 \right).$$

The desired result follows immediately, since $sr_1 = m_0 - r_0$. \square

5.3 Evaluations

From Proposition 5.14 it is clear that some knowledge regarding the factorization of F_0 can be used in order to effectively use the results of the previous section. In this section we, at least to some point, describe the factorization of F_0 and then prove our result. For the proof of Proposition 5.15 sieving is unnecessary, but is essential for all the rest.

Proposition 5.15. *Let q and m be such that $m_0 \leq 4$. If $q \geq 23$ and $m \geq 17$, then $N_A(\mathbf{w}) > 0$.*

Proof. From Proposition 5.1 and Lemma 4.1, since $W(F_0) \leq 2^4$, it suffices to show that

$$q^{m/4} > 4^5 d_{q_0}^2, \quad (5.9)$$

where $d_{q_0} < 4514.7$. This inequality is satisfied for $q \geq 23$ and $m \geq 31$ and for $q \geq 268$ and $m \geq 17$. In the remaining region there are exactly 20 pairs (q, m) satisfying $m_0 \leq 4$. Those pairs are

$$(23, 23), (25, 20), (25, 25), (27, 18), (27, 27), (29, 29), (32, 24), (49, 21), (49, 28), \\ (64, 24), (81, 18), (81, 27), (121, 22), (125, 20), (125, 25), (128, 24), (169, 26), (243, 18), \\ (243, 27) \text{ and } (256, 24)$$

A quick calculation reveals that all of them satisfy $q^{m/2} > 4W(\mathbf{k})$ and the result follows from Proposition 5.1. \square

In the two following propositions we deal with the case when F_0 splits into linear factors, which occurs when $m_0 \mid q - 1$.

Proposition 5.16. *Let q and m be such that $m_0 = q - 1$. If $q \geq 23$, then $N_A(\mathbf{w}) > 0$.*

Proof. We have that $\mathbf{w} = (q_0, q_0, F_0, F_0)$, where $F_0 = X^{q-1} - 1 = \prod_{x \in \mathbb{F}_q^*} (X - x)$. Therefore, it is clear that, for $0 \leq r \leq 2(q-1)$, we can choose a (\mathbf{k}_0, r) -decomposition of \mathbf{w} , where $\mathbf{k}_0 = (q_0, q_0, G, G)$, where some $G \mid F_0$ with $1 \leq \deg(G) \leq q-1$. In that case all the $2(q-1 - \deg(G))$ primes of the decomposition have absolute value q .

For q odd choose G , such that $\deg(G) = (q-1)/2$. In that case $\delta = 1/q$, $\Delta = (q-1)^2 + 1$ and $W(G) = 2^{(q-1)/2}$. It follows from Proposition 5.13 that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 2^{q+1}((q-1)^2 + 1)W^2(q_0). \quad (5.10)$$

For q even choose G such that $\deg(G) = q/2$. In that case $\delta = 2/q$, $\Delta = \frac{q(q-3)}{2} + 2$, $W(G) = 2^{q/2}$ and Proposition 5.13 yields that if Eq. (5.10) holds, then $N_A(\mathbf{w}) > 0$, hence if Eq. (5.10) holds, then $N_A(\mathbf{w}) > 0$ in any case. With the help of Lemma 4.1, Eq. (5.10) may be replaced with

$$q^{m/4} > 2^{q+1}((q-1)^2 + 1)d_{q_0}^2. \quad (5.11)$$

Eq. (5.11) is easily verified for $q > 72$, since $m \geq q - 1$ and $d_{q_0} \leq 4514.7$. Similarly, if $m \neq q - 1$, then for $m \geq 2(q - 1)$ Eq. (5.11) is verified for $q \geq 27$ and for $m \geq 3(q - 1)$ it holds for all $q \geq 23$.

The remaining cases are those when $m = q - 1$ and $23 \leq q \leq 71$. For those values, we verify that Eq. (5.11) holds for all q in question unless q is 23, 25, 27, 29, 31, 32, 37, 41 or 43, where we compute d_{q_0} explicitly for each q . For those values of q , we verify directly that Eq. (5.10) holds with the sole exception of $q = 25$.

For $q = 25$, we compute

$$q_0 = 2 \cdot 3 \cdot 13 \cdot 17 \cdot 31 \cdot 313 \cdot 601 \cdot 11489 \cdot 390001 \cdot 152587500001$$

and set $q_1 = 2 \cdot 3 \cdot 13 \cdot 17 \cdot 31$. We choose a $(\mathbf{k}_0, 34)$ -decomposition of \mathbf{w} , where $\mathbf{k}_0 = (q_1, q_1, G, G)$, where G is defined as before. It follows that $\delta = \frac{1}{25} - \frac{2}{152587500001} - \frac{2}{390001} - \frac{2}{11489} - \frac{2}{601} - \frac{2}{313}$ and $\Delta = 33/\delta + 2$. It can be computationally confirmed that the conditions of Proposition 5.13 are satisfied, i.e. $N_A(\mathbf{w}) > 0$. \square

Proposition 5.17. *Let m and q be such that $m_0 \mid q - 1$ and $m_0 \neq q - 1$. If $q \geq 23$ and $m \geq 17$, then $N_A(\mathbf{w}) > 0$.*

Proof. We use Proposition 5.14, with \emptyset as the mentioned set of primes. It is clear that, in that case $G_0 = F_0$ and $s = 1$. It is also clear that the denominator of the inequality of Proposition 5.14 is positive, since $m_0 \leq (q - 1)/2$. It follows that $N_A(\mathbf{w}) > 0$ if

$$q^{m/2} > 4W^2(q_0) \left(\frac{q(2m_0 - 1)}{q - 2m_0} + 2 \right). \quad (5.12)$$

Assume $m_0 = (q - 1)/2$. With the help of Lemma 4.1, Eq. (5.12) can be replaced by $q^{m/4} > 4d_{q_0}^2((q - 1)^2 + 1)$, where $d_{q_0} < 4514.7$. This inequality is satisfied for $q \geq 23$ and $m \geq 32$. Further, $m \geq m_0 = (q - 1)/2$, i.e. another sufficient condition is $q^{(q-1)/8} > 4d_{q_0}^2((q - 1)^2 + 1)$. This is satisfied for $q \geq 54$. For the remaining pairs (q, m) , q is an odd prime power $23 \leq q < 54$ and $17 \leq m < 32$. A computation shows that in the remaining region only six pairs, namely $(37, 18)$, $(41, 20)$, $(43, 21)$, $(47, 23)$, $(49, 24)$ and $(53, 26)$, satisfy $m_0 = (q - 1)/2$. For all six pairs Eq. (5.12) can be verified directly.

Next, assume $m_0 = (q - 1)/3$. As above, it turns out that $N_A(\mathbf{w}) > 0$, if $q^{m/4} > 4d_{q_0}^2 \frac{2q^2 - 3q + 4}{q + 2}$, where $d_{q_0} < 4514.7$. This condition is satisfied for $q \geq 23$ and $m \geq 28$. Furthermore, since $m \geq m_0 = (q - 1)/3$ another sufficient condition is $q^{(q-1)/12} > 4d_{q_0}^2 \frac{2q^2 - 3q + 4}{q + 2}$, which holds for $q \geq 67$. A quick computation shows that, in the remaining region, only two pairs, namely $(61, 20)$ and $(64, 21)$, satisfy $m_0 = (q - 1)/3$, but both of them satisfy Eq. (5.12) can be verified directly with all quantities computed explicitly.

Finally, assume $m_0 \leq (q - 1)/4$. If $t_{q_0} \leq 17$, it follows that $W^2(q_0) \leq (2^{17})^2$, hence Eq. (5.12) implies that $N_A(\mathbf{w}) > 0$, if $q^{m/2} > 4^{18} \cdot \frac{q^2 - q + 2}{q + 1}$, which holds for $q \geq 23$ and $m \geq 17$, except when $m = 17$ and $23 \leq q < 28$, but in those cases $m_0 \nmid q - 1$. For $t_{q_0} > 17$ we use Proposition 5.14 with $\{l_1, l_2, l_3\}$ as our set of primes, where $l_1 \geq 53$, $l_2 \geq 59$ and $l_3 \geq 61$, primes dividing q_0 . As before, Proposition 5.14 and Lemma 4.1 imply that $N_A(\mathbf{w})$ is positive, granted that

$$4^2 q^{m/4} > d_{q_0}^2 \frac{q^2 - (4\alpha + 7)q + 2}{(2\alpha - 1)q + 1}, \quad (5.13)$$

where $\alpha := 1 - 2/l_1 - 2/l_2 - 2/l_3$. Since $\alpha \geq 1 - 2/53 - 2/59 - 2/61$ and $d_{q_0} < 4514.7$, Eq. (5.13) holds for $q \geq 23$ and $m \geq 22$ and for $q \geq 78$ and $m \geq 17$. For the remaining pairs, i.e. $17 \leq m < 21$ and prime powers $29 \leq q < 78$ we have that Eq. (5.13) is satisfied, if d_{q_0} is replaced by its exact value. \square

In the rest of this section we focus on the remaining cases, i.e. when $m_0 > 4$ and $s \neq 1$. As we did in Section 4.4, we define $\rho := t_{F_0/G_0}/m_0$, where t_{F_0/G_0} stands for the number of monic irreducible factors of F_0/G_0 . The following four propositions deal with the various values of ρ , as described in Lemma 4.18. Also, the demand $m_0 > 4$ is not a restriction at all, since in Proposition 5.15 the cases where $m_0 \leq 4$ have already been settled. Furthermore, Proposition 5.14 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 4^{\rho m_0 + 1} W^2(q_0) \left(\frac{2q^s(1-\rho)m_0 - sq^s}{sq^s - 2(1-\rho)m_0} + 2 \right), \quad (5.14)$$

since $t_{F_0/G_0} \leq r_0$ and $\rho m_0 = t_{F_0/G_0}$, for $m_0 < sq^s/(2-2\rho)$.

Proposition 5.18. *If $q \geq 27$, $m \geq 17$, $m_0 > 4$ and $\rho = 1/2$, then $N_A(\mathbf{w}) > 0$.*

Proof. Under the given restrictions, Lemma 4.18 implies $s = 2$, q is even and $m \equiv 0 \pmod{4}$, i.e. it suffices to only examine $m \geq 20$. Furthermore, $m_0 \leq 2(q-1) < 2q^2$, that is we can use Eq. (5.14) as a sufficient condition for $N_A(\mathbf{w}) > 0$. It follows from Lemma 4.1 that if

$$\left(\frac{\sqrt[4]{q}}{2} \right)^m > 4d_{q_0}^2 \left(\frac{q^2(q-2)}{q^2 - q + 1} + 2 \right),$$

then $N_A(\mathbf{w}) > 0$, since the substitution of m_0 with $2(q-1)$ ensures that the denominator of the above fraction remains positive. This inequality holds for $d_{q_0} < 4514.7$, $q \geq 23$ and $m \geq 236$. For $m < 236$ the denominator of the fraction of Eq. (5.14) remains positive for $q \geq 23$, even if we substitute m_0 with m . It follows that a sufficient condition is

$$\left(\frac{\sqrt[4]{q}}{2} \right)^m > 4d_{q_0}^2 \left(\frac{q^2(m-2)}{2q^2 - m} + 2 \right).$$

This inequality holds for $d_{q_0} < 4514.7$, $q \geq 988$ and $20 \leq m < 236$.

There are 310 pairs (q, m) , where $23 \leq q < 988$ is an odd prime power, $20 \leq m < 236$, and $m_0 = 2 \gcd(m, q-1)$. All those pairs satisfy Eq. (5.14), if we replace $W(q_0)$ by $d_{q_0} q^{m/4}$ and compute d_{q_0} explicitly for each pair. The result follows. \square

Proposition 5.19. *If $q \geq 27$, $m \geq 17$, $m_0 > 4$ and $\rho = 3/8$, then $N_A(\mathbf{w}) > 0$.*

Proof. Since $\rho = 3/8$, Lemma 4.18 implies $q \equiv 1 \pmod{4}$, $16 \mid m$ and $s = 4$, i.e. it is safe to show the desired result for $q \geq 25$ and $m \geq 32$. Furthermore, $m_0 \leq 4(q-1) < sq^s/2(1-\rho)$, which means we can use Eq. (5.14) as a sufficient condition for $N_A(\mathbf{w}) > 0$. It follows from Lemma 4.1 that if

$$(q/8)^{m/4} > 4d_{q_0}^2 \left(\frac{5q-9}{4-5(q-1)/q^4} + 2 \right),$$

then $N_A(\mathbf{w}) > 0$, since the substitution of m_0 with $4(q-1)$ ensures that the denominator of the above fraction remains positive. This inequality holds for $d_{q_0} < 4514.7$, $q \geq 25$ and $m \geq 77$.

For $m < 77$ the denominator appearing in Eq. (5.14) remains positive, even if we substitute m_0 with m . It follows that $N_A(\mathbf{w}) > 0$ if

$$(q/8)^{m/4} > 4d_{q_0}^2 \left(\frac{q^4(5m-16)}{16q^4-5m} + 2 \right).$$

This condition is satisfied for $q \geq 106$, $32 \leq m < 77$ and $d_{q_0} < 4514.7$. We end up with 8 pairs (q, m) , namely $(25, 32)$, $(41, 32)$, $(73, 32)$, $(89, 32)$, $(37, 48)$, $(61, 48)$, $(49, 64)$ and $(81, 64)$, $25 \leq q < 106$, $32 \leq m < 77$ and $m_0 = 4 \gcd(m, q-1)$. For those pairs, we compute d_{q_0} explicitly and check that the above condition is satisfied. \square

Proposition 5.20. *If $q \geq 23$, $m \geq 17$, $m_0 > 4$ and $\rho = 13/36$, then $N_A(\mathbf{w}) > 0$.*

Proof. Since $\rho = 13/36$, Lemma 4.18 implies $q \equiv 1 \pmod{6}$, $36 \mid m$ and $s = 6$, that is we can only show the desired result for $q \geq 25$ and $m \geq 36$. Furthermore, $m_0 \leq 6(q-1) < sq^s/2(1-\rho)$, which means we can use Eq. (5.14) as a sufficient condition for $N_A(\mathbf{w}) > 0$. It follows, from Lemma 4.1. that if

$$(q/4^{13/9})^{m/4} > 4d_{q_0}^2 \left(\frac{46q-82}{36-46(q-1)/q^6} + 2 \right),$$

then $N_A(\mathbf{w}) > 0$, since the substitution of m_0 with $6(q-1)$ ensures that the denominator of the above fraction remains positive. This inequality holds for $d_{q_0} < 4514.7$, $q \geq 25$ and $m \geq 72$, therefore from now on we can focus on the case $m = 36$. It follows that $N_A(\mathbf{w}) > 0$ if

$$(q/4^{13/9})^{m/4} > 4d_{q_0}^2 \left(\frac{q^6(23m-108)}{108q^6-23m} + 2 \right).$$

This condition is satisfied for $q \geq 72$, $m = 36$ and $d_{q_0} < 4514.7$. For the remaining pairs, i.e. $25 \leq q < 72$, a prime power with $q \equiv 1 \pmod{6}$, and $m = 36$, we check than only 3 pairs (q, m) , namely $(31, 36)$, $(43, 36)$ and $(67, 36)$ satisfy $m_0 = 6 \gcd(m, q-1)$, but all three of them satisfy the latter inequality if we replace d_{q_0} by its exact value. \square

Proposition 5.21. *Suppose $q \geq 23$, $m \geq 17$, $m_0 > 4$, $m_0 \nmid q-1$ and $\rho \leq 1/3$. Then $N_A(\mathbf{w}) > 0$.*

Proof. We begin with $q \geq 27$. From the definition of ρ , it is clear that $W(F_0) \leq 2^{(1+(s-1)\rho)m_0/s}$. Since $s \geq 2$ and $\rho \leq 1/3$, it follows that $W(F_0) \leq 2^{2m_0/3}$. It follows from Proposition 5.1 and Lemma 4.1 that $N_A(\mathbf{w}) > 0$, if $(q/16)^{m/3} > 4e_{q_0}^2$, where $e_{q_0} < 1.06 \cdot 10^{24}$. This inequality is satisfied for $q \geq 27$ and $m > 642$.

For $m \leq 642$ we have that $m_0 \leq m < 729 \leq \frac{sq^s}{2(1-\rho)}$, since $\rho \leq 1/3$, $q \geq 27$ and $s \geq 2$, i.e. we can use Eq. (5.14) for the remaining cases. This means that if

$$(\sqrt[3]{q}/\sqrt[3]{4})^m > 4d_{q_0}^2 \left(\frac{q^2(2m-3)}{3q^2-2m} + 2 \right), \quad (5.15)$$

from Lemma 4.1, then $N_A(\mathbf{w}) > 0$. This condition is satisfied for $q \geq 27$ and $61 \leq m \leq 642$ and for $q \geq 834$ and $17 \leq m \leq 642$, provided that $d_{q_0} < 4514.7$. In the remaining region, we compute d_{q_0} , for each pair (q, m) , and it follows that Eq. (5.15) is satisfied for all but 26 pairs. Moreover, Eq. (5.14) implies that if

$$(\sqrt{q}/\sqrt[3]{4})^m > 4W^2(q_0) \left(\frac{q^2(2m-3)}{3q^2-2m} + 2 \right), \quad (5.16)$$

then $N_A(\mathbf{w}) > 0$. We end up with 26 pairs (q, m) , not yet settled. Those pairs are

(31, 17), (27, 18), (29, 18), (31, 18), (32, 18), (37, 18), (41, 18), (43, 18), (47, 18),
 (49, 18), (61, 18), (27, 20), (29, 20), (31, 20), (32, 20), (37, 20), (41, 20), (43, 20),
 (47, 20), (29, 22), (27, 24), (29, 24), (31, 24), (32, 24), (37, 24) and (43, 24).

We explicitly compute $W(q_0)$ for those pairs and check that they satisfy the latter inequality.

Next we focus on the case when $q = 23$ or 25 . In that case, since 23 or 5 does not divide q_0 , it follows that $d_{q_0} < 3340.6$ or $d_{q_0} < 2760.4$ respectively. Assume $s = 2$. In that case $m_0 \mid q^2 - 1$, that is $m_0 \leq 624$, i.e. $W(F_0) \leq 2^{2 \cdot 624/3}$. It follows from Proposition 5.1 and Lemma 4.1 that $N_A(\mathbf{w}) > 0$ if $q^{m/4} > 4^{1+2 \cdot 624/3} d_{q_0}^2$. This condition is satisfied for $q = 23$, $m \geq 759$ and $d_{q_0} < 3340.6$ and for $q = 25$, $m \geq 739$ and $d_{q_0} < 2760.4$. For now, we consider only the pairs (q, m) where $m \geq 530$ and a quick computation reveals that in the remaining region only 3 pairs, namely (23, 552), (25, 624) and (25, 650) fail to satisfy $q^{m/4} > 4^{1+2 \cdot 624/3} d_{q_0}^2$, if we compute d_{q_0} explicitly and demand $s = 2$. Finally, we verify that all 3 pairs satisfy $q^{m/4} > 4W(F_0)^2 d_{q_0}^2$, where $W(F_0)$ and d_{q_0} are computed explicitly for each pair.

For $m \leq 529$, we have that $m_0 \leq m < 530 \leq \frac{sq^s}{2(1-\rho)}$, which means we can use Eq. (5.14) for the remaining cases, i.e. if Eq. (5.15) is satisfied, then $N_A(\mathbf{w}) > 0$. This condition is satisfied for $q \geq 23$, $67 \leq m < 759$ and $d_{q_0} < 3340.6$. For the remaining cases, namely $q \in \{23, 25\}$ and $17 \leq m < 67$, we compute d_{q_0} for each pair and check that Eq. (5.15) is satisfied for all but 16 pairs (q, m) , namely

(23, 17), (25, 17), (23, 18), (25, 18), (23, 20), (25, 20), (23, 21), (25, 21), (23, 22),
 (25, 22), (23, 24), (25, 24), (23, 28), (23, 30), (25, 30) and (23, 36).

We explicitly check those pairs and find that only (23, 24) satisfies $s = 2$, but that pair satisfies Eq. (5.16), where $W(q_0)$ is replaced by its exact value.

Finally, assume $q = 23$ or 25 and $s \geq 3$. It follows from Proposition 5.1 and Lemma 4.1 that, for our purposes, a sufficient condition would be $q^{m/4} > 4^{1+5m/9} d_{q_0}^2$. This condition holds for $q \geq 23$, $m \geq 1285$ and $d_{q_0} < 3340.6$. For the remaining cases we can use Eq. (5.14) as a sufficient condition, since $m_0 \leq m < 18250.5 \leq \frac{sq^s}{2(1-\rho)}$. It follows that $N_A(\mathbf{w}) > 0$, if

$$q^{m/4} > 4^{\frac{m}{3}+1} d_{q_0}^2 \left(\frac{q^3(4m-9)}{9q^3-4m} + 2 \right),$$

which holds for $q \geq 23$, $66 \leq m < 1285$ and $d_{q_0} < 3340.6$. From the remaining pairs, i.e. (q, m) where $q \in \{23, 25\}$ and $17 \leq m < 66$, we exclude those who satisfy the latter inequality (where d_{q_0} is explicitly computed for each pair) and those for who $s \leq 2$ or $m_0 \leq 4$. We are now left with only 11 possible exception pairs, namely (23, 17), (23, 18), (23, 20), (23, 21), (23, 28), (23, 30), (23, 36), (25, 17), (25, 18), (25, 21) and (25, 22). Moreover, a computation reveals that all of them satisfy

$$q^{m/2} > 4W^2(q_0) \left(\frac{q^3(4m-9)}{9q^3-4m} + 2 \right),$$

which is a sufficient condition for our purposes. In that computation, $W(q_0)$ is computed explicitly for each pair (q, m) . \square

Summing up, in this section we proved the following.

Theorem 5.22. *Let $q \geq 23$ be a prime power, $m \geq 17$ an integer and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_q)$, such that if A has exactly two non-zero entries and q is odd, then the quotient of these entries is a square in \mathbb{F}_{q^m} (thus A may have two, three or four non-zero entries). There exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(ax + b)/(cx + d)$ are simultaneously primitive and free over \mathbb{F}_q .*

Example. As a demonstration of the above, assume $q = 23$, $m = 18$ and $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$. In that case, our aim is to find some $x \in \mathbb{F}_{23^{18}}$, such that both x and $(2x + 1)/(x + 1)$ are simultaneously primitive and free over \mathbb{F}_{23} . We represent $\mathbb{F}_{23^{18}}$ as $\mathbb{Z}_{29}(\alpha)$, where α is a root of $X^{18} + X^{12} + 18X^{11} + 2X^{10} + X^9 + 18X^8 + 3X^7 + 16X^6 + 21X^5 + 11X^3 + 3X^2 + 19X + 5$. A quick computation reveals that the set of elements satisfying these conditions include $\alpha + 1$, $2\alpha + 5$ and $3\alpha + 3$ among others.

APPENDIX A

Computer input and output

Here, in the appendix, we present all the raw computer input and output described throughout the text. Throughout this work, the program *Sage*¹ was exclusively used.

A.1 Computations of Chapter 3

These are the commands used to generate Table 3.1.

```
def mypi(q,n):
    if prime_divisors(n) == [2]:
        return (1/(2^n))*(q^n-1)
    else:
        result=0
        for d in divisors(n):
            if is_odd(d):
                result=result+(1/(2^n))*moebius(d)*q^(n/d)
        return result
A=[]
for n in range(3,27):
    q=3
    while mypi(q,n) <= (floor(n/2)*(floor(n/2)+5)/n)*(q^(1/2)+1)*(q^(floor(n/2)/2)-1)*q^(n/2):
        q=q+1
    A.append([n,q])
A
```

```
[[3, 142], [4, 838], [5, 32], [6, 55], [7, 16], [8, 20], [9, 10], [10, 12], [11, 8], [12, 8], [13, 6], [14, 7], [15, 5], [16, 6], [17, 5], [18, 5], [19, 4], [20, 4], [21, 4], [22, 4], [23, 4], [24, 4], [25, 3], [26, 4]]
```

These are the commands used in order to deal with the remaining cases of Table 3.1. The output of the below program, combined with Table 3.1 and Corollary 3.10, proved Theorem 3.11.

```
"""
Here we create a dictionary (exc) with all possible exceptions,
according to Table 3.1.
"""
exc={}
for q in range(3,839):
    if is_prime_power(q) and is_odd(q):
        exc.update({q:[]})
```

¹<http://www.sagemath.org/>

```

for alpha in A:
    for q in range(3,alpha[1]):
        if is_prime_power(q) and is_odd(q):
            exc[q].append(alpha[0])
"""
Our dictionary, 'exc', is now complete, according to Table 3.1.
numtopoly takes as input a degree (n), an integer (i), which is assumed
to be between 0 and  $q^{(n-1)}-1$ , a finite field (F) and the degree and the
value of the prescribed coefficient. It returns a self-reciprocal
polynomial of degree  $2^n$ , distinct for each i within range.
"""
def numtopoly(n,i,F,fixed_coef,fixed_deg):
    q=order(F); P.<x>=PolynomialRing(F)
    f=x^(2^n)+1+fixed_coef*(x^(fixed_deg)+x^(2^n-fixed_deg)); j=1
    while i!=0 and j!=n:
        if j<fixed_deg:
            f=f+list(F)[i%q]*(x^j+x^(2^n-j))
        else:
            f=f+list(F)[i%q]*(x^(j+1)+x^(2^n-j-1))
            i=floor(i/q); j=j+1
    f=f+list(F)[i%q]*x^n
    return f

"""
checkirr takes as input the degree of the polynomial, the degree and the
value of the prescribed coefficient and the finite field and checks the
irreducibility of all possible self-reciprocal polynomials with this
prescribed coefficient. It stops at the first valid polynomial it finds. If
the search is successful it returns "True" and the polynomial, otherwise,
it returns "False"
"""
def checkirr(n,fixed_coef,fixed_deg,F):
    for i in xrange (1,order(F)^(n-1)):
        f=numtopoly(n,i,F,fixed_coef,fixed_deg)
        if f.is_irreducible():
            return True,f
    return False

"""
Here we perform the actual calculations...
"""
f=open('sage_output.txt','w')
f.write(' ----- Start of file -----\n')
f.close()
for q in exc:
    f=open('sage_output.txt','a')
    f.write('\n\n-----')
    f.write('\n ----- Checking q='+str(q)+' -----')
    f.write('\n-----')
    if is_prime(q):
        F=GF(q)
        f.write('\nF_'+str(q)+'=Z_'+str(q))
    else:
        F=GF(q,'b')
        f.write('\nF_'+str(q)+'=Z_'+str(divisors(q)[1])+'[x]'+str(F.modulus()))
    f.close()
    for n in exc[q]:
        f=open('sage_output.txt','a')
        f.write('\n ----- Checking n='+str(n)+' -----')
        f.close()
        for k in range(1,floor(n/2)+1):
            for a in F:
                f=open('sage_output.txt','a')
                f.write('\na='+str(a)+' k='+str(k)+' '+str(checkirr(n,a,k,F)))
                f.close()

"""
The file sage_output.txt includes our results.
"""

```

The resulting file, `sage_output.txt`, is too large² to be included in this document. The interested reader can find it online³, while its format is self-explained.

²Although it is a text file, it is larger than 7.5mb!

³<http://www.math.uoc.gr/~gkapet/hm/hm-results.txt>

A.2 Computations of Chapter 4

These are the commands used to complete the proof of Lemma 4.1.

```
def c(a,known_non_divisors):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if p not in known_non_divisors:
            gin=gin*p; s=s+1
            p=Primes().next(p)
    return 2^s/gin.nth_root(a)
c(4,[1]),c(8,[1]),c(12,[1]),c(4,[2]),c(4,[3]),c(4,[5]),c(4,[7]),c(4,[11]),c(8,[3]),c(8,[2]),
    c(8,[5]),c(8,[23])

(4.86173341033942, 4514.62651178517, 1.05730734177260e24, 2.89080398141104, 3.19920049962530, 3.63499356488677,
 3.95399080724057, 4.42699790605150, 2589.59584032557, 2461.61756059865, 2760.34320131056, 3340.47181248841)
```

These are the commands used to prove Proposition 4.15.

```
"""
Here we use Eq.(4.7) as described in the first two paragraphs of the proof,
in order to deal with the vast majority of pairs and remain with just a finite
set of possible exceptions.
"""
list=[[17,4,9,4],[16,2,9,3],[13,4,7,4],[11,4,5,4],[9,3,2,4],[8,2,9,3],[7,4,4],
[5,3,7,4],[4,2,9,3],[3,3,2,4],[2,2,9,3]]
for alpha in list:
    m=0
    while alpha[0]^(m/4) <= 3*4^alpha[2]*alpha[1]:
        m=m+1
    alpha.append(m)
list

[[17,4,9000000000000,4,12],[16,2,9000000000000,3,10],[13,4,7000000000000,4,13],[11,4,5000000000000,4,14],
[9,3,2000000000000,4,15],[8,2,9000000000000,3,13],[7,4,4,17],[5,3,7000000000000,4,20],[4,2,9000000000000,
3,19],[3,3,2000000000000,4,29],[2,2,9000000000000,3,37]]

list=[[11,4,5,1],[10,3,7,2],[9,3,2,1],[8,2,9,1],[7,4,1],[6,3,2,2],[6,2,9,3],
[5,3,7,1],[4,2,9,1],[4,4,9,2],[3,3,2,1]]
for alpha in list:
    q=0
    while q^(alpha[0]/4) <= 3*4^alpha[2]*alpha[1]:
        q=q+1
    alpha.append(q)
list

[[11,4,5000000000000,1,5],[10,3,7000000000000,2,8],[9,3,2000000000000,1,6],[8,2,9000000000000,1,6],[7,4,1,
10],[6,3,2000000000000,2,29],[6,2,9000000000000,3,68],[5,3,7000000000000,1,21],[4,2,9000000000000,1,35],[4,
4,9000000000000,2,236],[3,3,2000000000000,1,130]]

"""
Here, we create the list of possible exceptions so far
"""
A=[[16,6],[16,4],[9,12],[9,6],[8,12],[8,6],[7,14],[7,7],[5,15],[5,10],[5,5],[4,16],
[4,12],[4,8],[4,6],[3,27],[3,18],[3,12],[3,9],[3,6],[2,32],[2,24],[2,16],[2,12],
[2,8],[2,6],[64,6],[12,6],[27,6],[2,4],[4,4],[8,4],[16,4],[32,4]]
for q in range(2,236):
    if is_prime_power(q) and q%4==3:
        A.append([q,4])
for q in range(2,130):
    if is_prime_power(q) and q%3!=1:
        A.append([q,3])
print len(A),A

86

"""
Here, we compute m_0 for better results, taking into account Lemma 4.14.
"""
def m0(q,m):
    if m==3:
        n=1
```

```

elif m==4:
    n=2
else:
    n=m
while n%(divisors(q)[1])==0:
    n=n/divisors(q)[1]
return n
"""
chk performs the actual check, with all quantities explicitly computed.
"""
def chk(beta):
    delta=1; q0=beta[0]^beta[1]-1; lis=prime_divisors(q0); i=len(lis); lis2=[]
    while delta>0 and i>=0:
        t=len(lis)-i
        if beta[0]^(beta[1]/2) > 3*2^len(lis)*4^m0(beta[0],beta[1])
            *2^(-t)*((t-1)/delta+2):
            return "success",lis2
        i=i-1; delta=delta-1/lis[i]
        lis2.append(lis[i])
    if delta<=0:
        return "fail","delta<=0"
    if i<0:
        return "fail","no more primes"
B=[]; C=[]; D=[]
for beta in A:
    print beta,chk(beta)
    if chk(beta)[0]=='fail':
        B.append(beta)
    elif chk(beta)[1]==[]:
        C.append(beta)
    else:
        D.append(beta)

[16, 6] ('success', [241, 17, 13, 7, 5]) [16, 4] ('success', []) [9, 12] ('success', []) [9, 6] ('success', [73, 13, 7, 5]) [8, 12]
('success', []) [8, 6] ('fail', 'no more primes') [7, 14] ('success', []) [7, 7] ('success', []) [5, 15] ('success', []) [5, 10] ('success',
[]) [5, 5] ('fail', 'no more primes') [4, 16] ('success', []) [4, 12] ('success', [241, 17, 13, 7, 5]) [4, 8] ('success', []) [4, 6] ('fail',
'no more primes') [3, 27] ('success', []) [3, 18] ('success', []) [3, 12] ('fail', 'no more primes') [3, 9] ('success', []) [3, 6]
('fail', 'no more primes') [2, 32] ('success', []) [2, 24] ('success', [241, 17, 13, 7, 5]) [2, 16] ('success', []) [2, 12] ('fail', 'no
more primes') [2, 8] ('fail', 'no more primes') [2, 6] ('fail', 'no more primes') [64, 6] ('success', []) [12, 6] ('success', [157,
19, 13, 11, 7]) [27, 6] ('success', []) [2, 4] ('fail', 'no more primes') [4, 4] ('fail', 'no more primes') [8, 4] ('fail', 'no more
primes') [16, 4] ('success', []) [32, 4] ('success', []) [3, 4] ('fail', 'no more primes') [7, 4] ('fail', 'delta<=0') [11, 4] ('fail',
'delta<=0') [19, 4] ('fail', 'delta<=0') [23, 4] ('fail', 'delta<=0') [27, 4] ('success', [73, 13, 7, 5]) [31, 4] ('success', [37, 13, 5])
[43, 4] ('success', [37, 11, 7]) [47, 4] ('success', [23, 17, 13]) [59, 4] ('success', []) [67, 4] ('success', []) [71, 4] ('success', [])
[79, 4] ('success', []) [83, 4] ('success', []) [103, 4] ('success', []) [107, 4] ('success', []) [127, 4] ('success', []) [131, 4]
('success', []) [139, 4] ('success', []) [151, 4] ('success', []) [163, 4] ('success', []) [167, 4] ('success', []) [179, 4] ('success', [])
[191, 4] ('success', []) [199, 4] ('success', []) [211, 4] ('success', []) [223, 4] ('success', []) [227, 4] ('success', []) [2, 3] ('fail',
'no more primes') [3, 3] ('fail', 'no more primes') [5, 3] ('fail', 'no more primes') [8, 3] ('fail', 'no more primes') [9, 3] ('fail',
'no more primes') [11, 3] ('fail', 'no more primes') [17, 3] ('success', []) [23, 3] ('fail', 'no more primes') [27, 3] ('success',
[]) [29, 3] ('success', [67, 13]) [32, 3] ('success', []) [41, 3] ('success', []) [47, 3] ('success', []) [53, 3] ('success', []) [59, 3]
('success', []) [71, 3] ('success', []) [81, 3] ('success', []) [83, 3] ('success', []) [89, 3] ('success', []) [101, 3] ('success', [])
[107, 3] ('success', []) [113, 3] ('success', []) [125, 3] ('success', []) [128, 3] ('success', [])

```

```
len(B), len(C), len(D)
```

(23, 53, 10)

These are the commands used to prove Proposition 4.16.

```

"""
The commands here follow closely the proof of Proposition 4.16
and are self-explanatory.
"""
for m in range(1,8):
    q=1
    while q^(m*(q-1)/4) < 3*2^(q-1)*(q^2-2*q+2)*4.9:
        q=q+1
    print [m,q]

[1, 43] [2, 14] [3, 9] [4, 7] [5, 6] [6, 5] [7, 4]

A=[[41, 40], [37, 36], [32, 31], [31, 30], [29, 28], [27, 26], [25, 24], [23, 22], [19, 18], [17, 16],
[16, 15], [13, 12], [11, 10], [9, 8], [8, 7], [7, 6], [5, 4], [4, 3], [8, 14], [5, 20]]
B=[]

```

```

for alpha in A:
    if alpha[0]^(alpha[1]/2) < 3*2^(alpha[0]-1)*(alpha[0]^2-2*alpha[0]+2)*
        2^len(prime_divisors(alpha[0]^alpha[1]-1)):
        B.append(alpha)
len(B),B

```

(8, [[16, 15], [13, 12], [11, 10], [9, 8], [8, 7], [7, 6], [5, 4], [4, 3]])

These are the commands utilized to prove Proposition 4.17

```

"""
The commands here follow closely the proof of Proposition 4.17
and are self-explanatory.
"""
m0=12; A=[]
while m0>2:
    q=2*m0+1; mulier=1
    while q^(mulier*m0/4) <= 3*4.9*(q*(2*m0-1)/(q-2*m0)+2):
        mulier=mulier+1
    if m0 in [3,4]:
        mulier=2
    for i in range(1,mulier):
        q=2*m0+1
        while q^(i*m0/4) <= 3*4.9*(q*(2*m0-1)/(q-2*m0)+2):
            q=q+1
        A.append([m0,q,i])
    m0=m0-1
A

```

[[11, 24, 1], [10, 23, 1], [9, 24, 1], [8, 26, 1], [7, 31, 1], [6, 41, 1], [5, 66, 1], [5, 13, 2], [4, 139, 1], [3, 488, 1]]

```

B=[]
for alpha in A:
    for q in range(2,alpha[1]):
        if is_prime_power(q) and q%alpha[0]==1 and alpha[0]!=(q-1) and alpha[2] in divisors(q):
            B.append([q,alpha[0]^alpha[2]])
len(B)

```

89

```

def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])==0:
        n=n/divisors(beta[0])[1]
    return n
C=[]
for beta in B:
    if beta[0]^(beta[1]/2) <= 3*2^(len(prime_divisors(beta[0]^beta[1]-1)))*
        (beta[0]*(2*m0(beta)-1)/(beta[0]-2*m0(beta))+2):
        C.append(beta)
len(C),C

```

(20, [[13, 6], [11, 5], [16, 5], [9, 4], [13, 4], [17, 4], [29, 4], [7, 3], [13, 3], [16, 3], [19, 3], [25, 3], [31, 3], [37, 3], [43, 3], [49, 3], [61, 3], [67, 3], [79, 3], [121, 3]])

```

def chk(beta):
    delta=1-2*m0(beta)/beta[0]; lis=prime_divisors(beta[0]^beta[1]-1); i=len(lis); lis2=[]
    while delta>0 and i>=0:
        t=len(lis)-i
        if beta[0]^(beta[1]/2) > 3*2^(len(lis)-t)*((2*m0(beta)+t-1)/delta+2):
            return "success",lis2
        i=i-1; delta=delta-1/lis[i]
        lis2.append(lis[i])
    if delta<=0:
        return "fail","delta<=0"
    if i<0:
        return "fail","no more primes"
for gamma in C:
    print gamma,chk(gamma)

```

[13, 6] ('fail', 'delta<=0') [11, 5] ('fail', 'delta<=0') [16, 5] ('success', [41, 31]) [9, 4] ('fail', 'delta<=0') [13, 4] ('fail', 'delta<=0') [17, 4] ('fail', 'delta<=0') [29, 4] ('success', [421]) [7, 3] ('fail', 'delta<=0') [13, 3] ('fail', 'delta<=0') [16, 3] ('fail', 'delta<=0') [19, 3] ('fail', 'delta<=0') [25, 3] ('fail', 'delta<=0') [31, 3] ('success', [331, 5]) [37, 3] ('success', [67]) [43, 3] ('success', [631]) [49, 3] ('success', [43]) [61, 3] ('success', [97]) [67, 3] ('success', [31]) [79, 3] ('success', [43]) [121, 3] ('success', [37])

These are the computer commands used in the proof of Proposition 4.19.

```

"""
The commands follow closely the procedure described in the proof.
First, we consider rho=1/2.
"""
m0=8; m=3*m0; q=6
print q^(m/4)>3*2^m0*4.9*(q^2*(q-2)/(q^2-q+1)+2)
m=5*m0; q=5
print q^(m/4)>3*2^m0*4.9*(q^2*(q-2)/(q^2-q+1)+2)

True True

m=m0
while q^(3*m/8)<=3*2^m0*4514.7*(q^2*(q-2)/(q^2-q+1)+2):
    q=q+1
q

1863

m=8; q=m/2+1
while q^(3*m/8)<=3*2^m0*4514.7*(q^2*(q-2)/(q^2-q+1)+2):
    m=m+1; q=m/2+1
m,q

(33, 35/2)

def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])!=0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for m in range(8,33):
    for q in range(5,1863):
        if is_prime_power(q) and is_odd(q) and m==m0([q,m]) and m==2*gcd(m,q-1):
            A.append([q,m])
len(A)

310

B=[]
for alpha in A:
    if alpha[0]^(alpha[1]/4)<=3*4.9*2^alpha[1]*
        (alpha[0]^2*(alpha[1]-2)/(2*alpha[0]^2-alpha[1]+2)):
        B.append(alpha)
len(B),B

(22, [[5, 8], [13, 8], [29, 8], [37, 8], [53, 8], [61, 8], [101, 8], [109, 8], [125, 8], [7, 12], [19, 12], [31, 12], [43, 12], [67, 12], [9,
16], [25, 16], [41, 16], [11, 20], [31, 20], [13, 24], [37, 24], [17, 32]])

def chk(beta):
    delta=2*beta[0]^2-m0(beta); q0=beta[0]^beta[1]-1
    lis=prime_divisors(q0); i=len(lis); lis2=[]
    while delta>0 and i>=0:
        t=len(lis)-i
        if beta[0]^(beta[1]/2) > 3*2^(len(lis)-t)*2^m0(beta)*
            (beta[0]^2*(m0(beta)+2*(t-1))/delta+2):
            return "success",lis2
        i=i-1; delta=delta-2*beta[0]^2/lis[i]
        lis2.append(lis[i])
    if delta<=0:
        return "fail","delta<=0"
    if i<0:
        return "fail","no more primes"
for beta in B:
    print beta,chk(beta)

[5, 8] ('fail', 'delta<=0') [13, 8] ('fail', 'delta<=0') [29, 8] ('success', []) [37, 8] ('success', []) [53, 8] ('success', []) [61, 8]
('success', []) [101, 8] ('success', []) [109, 8] ('success', []) [125, 8] ('success', []) [7, 12] ('fail', 'delta<=0') [19, 12] ('success',
[]) [31, 12] ('success', []) [43, 12] ('success', []) [67, 12] ('success', []) [9, 16] ('success', [21523361, 193]) [25, 16] ('success',
[]) [41, 16] ('success', []) [11, 20] ('success', []) [31, 20] ('success', []) [13, 24] ('success', []) [37, 24] ('success', []) [17, 32]
('success', [])

```

```

"""
Now we consider rho=3/5
"""
m0=8; m=5*m0; q=5
print q^(3*m/8) > 3*2^(3*m0/4)*4514.7*(5*q^5-q^4-10*q+10)/(4*q^4-5*q+5)
m0=8; m=3*m0; q=9
print q^(3*m/8) > 3*2^(3*m0/4)*4514.7*(5*q^5-q^4-10*q+10)/(4*q^4-5*q+5)

True True

A=[]
for m in [16, 32, 48, 64, 80, 96, 112, 128, 144]:
    q=5
    while q^(3*m/8) <= 3*2^(3*m/4)*4514.7*(5*q^5-q^4-10*q+10)/(4*q^4-5*q+5):
        q=q+1
    A.append([q,m])
A

[[37, 16], [11, 32], [8, 48], [7, 64], [6, 80], [6, 96], [6, 112], [6, 128], [5, 144]]

B=[]
for alpha in A:
    for q in range(5, alpha[0]):
        if is_prime_power(q) and q%4==1 and alpha[1]==4*gcd(alpha[1], q-1):
            B.append([q, alpha[1]])
B

[[5, 16], [13, 16], [29, 16], [9, 32]]

for beta in B:
    if beta[0]^(beta[1]/2) <= 3*2^(3*beta[1]/4)*2^(len(prime_divisors(beta[0]^beta[1]-1)))
        *((5*beta[0]^4*beta[1]-16*beta[0]^4)/(16*beta[0]^4-5*beta[1])+2):
        print beta

[5, 16]

"""
Here, we deal with rho=13/36
"""
m0=16; m=3*m0; q=7
numerical_approx(q^(3*m/8)-3*2^(13*m0/18)*4514.7*((23*q^6*(q-1)-18*q^6)/(18*q^6-23*(q-1))+2))

1.62841324457041e15

A=[]
for m in [36, 72]:
    q=7
    while q^(3*m/8) <= 3*2^(13*m/18)*4514.7*((23*q^6*(q-1)-18*q^6)/(18*q^6-23*(q-1))+2):
        q=q+1
    A.append([q,m])
A

[[10, 36], [7, 72]]

q=7; m=36
numerical_approx(q^(m/2)-3*2^(13*m/18)*2^(len(prime_divisors(q^m-1)))
*((23*q^6*(q-1)-18*q^6)/(18*q^6-23*(q-1))+2))

1.62484000598269e15

```

These are the Sage commands used in the proof of Proposition 4.20.

```

"""
Most of the commands follow the flow of the proof of Proposition 4.20.
First, we assume m0>=8.
"""
m=8; q=5
while q^(m/4) <= 3*4.9*4^(m/3)*(2*m-1):
    q=q+1
q

```

```

m=8; q=5
while q^(3*m/8) <= 3*4514.7*4^(m/3)*(2*m-1):
    m=m+1
m

106

"""
m0 computes m0. In this proof, the large length of the lists of exceptions makes it preferable
to omit the listing itself, but rather list just the number of possible exceptions.
"""
def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])!=0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for q in range(5,95):
    if is_prime_power(q):
        for m in range(8,106):
            if m0([q,m])>=8 and (q-1)%m0([q,m])!=0 and (m0([q,m])!=2*gcd(m,q-1) or is_even(q))
            and (m0([q,m])!=4*gcd(m,q-1) or q%4!=1) and (m0([q,m])!=6*gcd(m,q-1) or q%6!=1):
                A.append([q,m])
len(A)

2675

B=[]
for alpha in A:
    if alpha[0]^(alpha[1]/4) <= 3*4.9*4^(m0(alpha)/3)*(2*m0(alpha)-1):
        B.append(alpha)
len(B)

430

C=[]
for alpha in B:
    if alpha[0]^(alpha[1]/2) <= 3*2^(len(prime_divisors(alpha[0]^alpha[1]-1)))
    *4^(m0(alpha)/3)*(2*m0(alpha)-1):
        C.append(alpha)
len(C)

31

"""
sigma computes s and rho computes rho.
"""
def sigma(beta):
    s=1
    while (beta[0]^s-1)%m0(beta)!=0:
        s=s+1
    return s
def rho(beta):
    x=PolynomialRing(GF(beta[0], 'a'), 'x').gen()
    i=0; mo=m0(beta); s=sigma(beta)
    for g in divisors(x^mo-1):
        if g.is_irreducible() and g.degree()!=s:
            i=i+1
    return i/mo
D=[]
for alpha in C:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha); r=rho(alpha)
    if q^(m/2) <= 3*2^(len(prime_divisors(q^m-1)))*4^(r*mo)*
    ((2*q^s*(1-r)*mo-s*q^s)/(s*q^s-2*(1-r)*mo)+2):
        D.append(alpha)
len(D),D

(4, [[5, 9], [5, 12], [7, 8], [7, 9]])

"""
Now, we consider 5<=m0<=7
"""
mo=5; m=mo; q=5
while q^(m/4) <= 3*4.9*4^(2*mo/3):
    q=q+1
q

```

347

```
q=5; m=4*mo
bool(q^(m/4)>3*4.9*4^(2*mo/3))
```

True

```
A=[]
for q in range(5,347):
    if is_prime_power(q):
        for m in range(5,29):
            if (q-1)%m0([q,m])!=0 and (m0([q,m])==5 or m0([q,m])==6 or m0([q,m])==7):
                A.append([q,m])
len(A)
```

184

```
for alpha in A:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha); r=rho(alpha)
    if q^(m/2) <= 3*2^(len(prime_divisors(q^m-1)))*4^(r*mo)*
        ((2*q^s*(1-r)*mo-s*q^s)/(s*q^s-2*(1-r)*mo)+2):
        B.append(alpha)
len(D),D

(12, [[5, 9], [5, 12], [7, 8], [7, 9], [5, 6], [7, 5], [8, 5], [9, 5], [11, 6], [17, 6], [23, 6], [29, 6]])
```

```
"""
Here, we try to apply multiplicative sieving as well...
"""
def chk(beta):
    mo=m0(beta); s=sigma(beta); r=rho(beta); delta=s*beta[0]^s-2*(1-r)*mo
    q0=beta[0]^beta[1]-1; lis=prime_divisors(q0); i=len(lis); lis2=[]
    while delta>0 and i>=0:
        t=len(lis)-i
        if beta[0]^(beta[1]/2) > 3*2^(len(lis)-t)*4^(r*mo)*
            ((2*beta[0]^s*(1-r)*mo+s*beta[0]^s*(t-1))/(delta)+2):
            return "success", lis2
        i=i-1; delta=delta-s*beta[0]^s/lis[i]
        lis2.append(lis[i])
        if delta<=0:
            return "fail", "delta<=0"
        if i<0:
            return "fail", "no more primes"
for beta in D:
    print beta,chk(beta)
```

```
[5, 9] ('success', [829, 31]) [5, 12] ('fail', 'delta<=0') [7, 8] ('success', [1201, 5]) [7, 9] ('success', [1063, 37, 19, 3]) [5, 6] ('fail',
'delta<=0') [7, 5] ('fail', 'no more primes') [8, 5] ('success', [151, 31]) [9, 5] ('success', [61, 11]) [11, 6] ('fail', 'delta<=0') [17,
6] ('success', [307]) [23, 6] ('success', [79]) [29, 6] ('success', [271])
```

These are the commands used in the proof of Proposition 4.22.

```
"""
The commands follow (not so closely as before) the flow of the proof
of Proposition 4.22. Here B will always stand as the list of possible
exception, to be consider in the end for the possibility of successful
multiplicative sieving. We begin with q=4.
"""
```

```
q=4; m=4; r=1/5
bool(q^m>3*2.9*4^(3*m/5))
```

True

```
while q^(3*m/8)<=3*2461.7*4^(r*m)*(4*m-3):
    m=m+1
m
```

60

```
m=8
while q^(3*m/8)<=3*2461.7*4^(r*m/2)*(2*m-3):
    m=m+1
m
```

35

```

"""
m0 will compute m_0 for given q,m.
"""
def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])!=0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for m in range(5,60):
    mo=m0([q,m])
    if (q-1)%mo!=0 and mo>4 and (mo==m or (mo==2*m and m<35)):
        A.append([q,m])
len(A)

```

28

```

"""
sigma computes s, rho computes rho, while w computes d_r.
"""
def sigma(beta):
    s=1
    while (beta[0]^s-1)%m0(beta)!=0:
        s=s+1
    return s
def rho(beta):
    x=PolynomialRing(GF(beta[0], 'a'), 'x').gen()
    i=0; mo=m0(beta); s=sigma(beta)
    for g in divisors(x^mo-1):
        if g.is_irreducible() and g.degree()!=s:
            i=i+1
    return i/mo
def w(a,n):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if n%p==0:
            gin=gin*p
            s=s+1
        p=Primes().next(p)
    return 2^s/gin.nth_root(a)
"""
The computation of rho seems to be even more expensive (in computer time) than the
computation of W(q_0). As a result we first use the generic bounds for rho and use
its exact value only as a last resort. This is the difference here between the
lists B and C.
"""
C=[[4,45]]
for alpha in A:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha)
    if q^(3*m/8) <= 3*w(8,q0)*4^(r*mo)*((2*q^s*(1-r)^mo-s*q^s)/(s*q^s-2*(1-r)^mo)+2):
        C.append(alpha)
len(C),C

```

(7, [[4, 45], [4, 5], [4, 7], [4, 9], [4, 11], [4, 13], [4, 15]])

```

"""
Here, we eventually compute rho for the remaining pairs.
"""
B=[]
for alpha in C:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha); r=rho(alpha)
    if q^(m/2) <= 3*2^(len(prime_divisors(q^m-1)))*4^(r*mo)*
        ((2*q^s*(1-r)^mo-s*q^s)/(s*q^s-2*(1-r)^mo)+2):
        B.append(alpha)
len(B),B

```

(4, [[4, 5], [4, 7], [4, 9], [4, 15]])

```

"""
Now, we consider q=3.
"""

```



```

q=3; m=16; r=1/4
while q^(3*m/8)<=3*2589.6*4^(r*m)*(3*m-2):
    m=m+1
m

```

238

```

m=12
while q^(3*m/8)<=3*2589.6*4^(r*m/3)*(m-2):
    m=m+1
m

```

43

```

m=4
bool(q^(27*m/8)>3*2589.6*4^(m/4)*(3*m-2))

```

True

```

A=[]
for m in range(5,238):
    mo=m0([q,m])
    if (q-1)%mo!=0 and mo>4 and (mo==m or (mo==3*m and m<43)):
        A.append([q,m])
len(A)

```

155

```

"""
We use C to avoid the computation of both rho and w(q_0) for large numbers and D
to avoid the computation of rho.
"""

```

```

C=[]
for alpha in A:
    q=alpha[0]; m=alpha[1]; mo=m0(alpha);
    if q^(3*m/8) <= 3*w(8,q^m-1)*2^(mo/2)*(3*m-2):
        C.append(alpha)
len(C)

```

78

```

D=[]
for alpha in C:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha)
    if q^(m/2) <= 3*2^(len(prime_divisors(q^m-1)))*4^(r*m)*
        ((2*(1-r)*mo-s)/(s-2*(1-r)*mo/q^s)+2):
        D.append(alpha)
len(D),D

```

```

(16, [[3, 5], [3, 7], [3, 8], [3, 10], [3, 11], [3, 13], [3, 14], [3, 16], [3, 17], [3, 19], [3, 20], [3, 22], [3, 26], [3, 28], [3, 32], [3, 40]])

```

```

"""
We do not initiate B, new possible exception pairs are simply added to the list.
"""

```

```

for alpha in D:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha); r=rho(alpha)
    if q^(m/2) <= 3*2^(len(prime_divisors(q^m-1)))*4^(r*m)*
        ((2*(1-r)*mo-s)/(s-2*(1-r)*mo/q^s)+2):
        B.append(alpha)
len(B),B

```

```

(11, [[4, 5], [4, 7], [4, 9], [4, 15], [3, 5], [3, 7], [3, 8], [3, 10], [3, 11], [3, 16], [3, 20]])

```

```

"""
Finally, we consider q=2. Previous comments regarding A,B,C and D apply here as well.
"""

```

```

q=2; m=4; r=1/6
bool(q^(8*m/4)>3*2.9*4^(7*m/12))

```

True

```

m=4
while q^(3*m/8)<=3*2461.7*4^(m/6)*(5*m-4):
    m=m+1
m
585

m=4
while q^(3*m/8)<=3*2461.7*4^(m/12)*(5*m/2-4):
    m=m+1
m
100

m=4
while q^(3*m/8)<=3*2461.7*4^(m/24)*(5*m/4-4):
    m=m+1
m
66

A=[]
for m in range(5,585):
    mo=m0([q,m])
    if (q-1)%mo!=0 and mo>4 and (mo==m or (mo==2*m and m<100) or (mo==4*m and m<66)):
        A.append([q,m])
len(A)
290

C=[]
for alpha in A:
    q=alpha[0]; m=alpha[1]; mo=m0(alpha);
    if q^(3*m/8) <= 3*w(8,q^m-1)*4^(mo/6)*(5*m-2):
        C.append(alpha)
len(C)
148

D=[]
for alpha in C:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha)
    if q^(m/2) <= 3*2^(len(prime_divisors(q^m-1)))*4^(r*mo)*
        ((2*q^s*(1-r)^mo-s*q^s)/(s*q^s-2*(1-r)^mo)+2):
        D.append(alpha)
len(D),D
(22, [[2, 5], [2, 7], [2, 9], [2, 11], [2, 13], [2, 15], [2, 17], [2, 19], [2, 21], [2, 23], [2, 25], [2, 27], [2, 29], [2, 31], [2, 33], [2, 35],
[2, 39], [2, 43], [2, 45], [2, 51], [2, 55], [2, 63]])

for alpha in D:
    s=sigma(alpha); q=alpha[0]; m=alpha[1]; mo=m0(alpha); r=rho(alpha)
    if q^(m/2) <= 3*2^(len(prime_divisors(q^m-1)))*4^(r*mo)*
        ((2*(1-r)^mo-s)/(s-2*(1-r)^mo/q^s)+2):
        B.append(alpha)
len(B),B
(17, [[4, 5], [4, 7], [4, 9], [4, 15], [3, 5], [3, 7], [3, 8], [3, 10], [3, 11], [3, 16], [3, 20], [2, 5], [2, 7], [2, 9], [2, 11], [2, 15], [2, 21]])

"""
The function chk checks whether multiplicative sieving can be successfully applied.
"""
def chk(beta):
    mo=m0(beta); s=sigma(beta); r=rho(beta); delta=s*beta[0]^s-2*(1-r)^mo
    q0=beta[0]^beta[1]-1; lis=prime_divisors(q0); i=len(lis); lis2=[]
    while delta>0 and i>=0:
        t=len(lis)-i
        if beta[0]^(beta[1]/2) > 3*2^(len(lis)-t)*4^(r*mo)*
            ((2*beta[0]^s*(1-r)^mo+s*beta[0]^s*(t-1))/(delta)+2):
            return "success",lis2
        i=i-1; delta=delta-s*beta[0]^s/lis[i]
        lis2.append(lis[i])
    if delta<=0:
        return "fail","delta<=0"
    if i<0:
        return "fail","no more primes"
for beta in B:
    print beta,chk(beta)

```

```
[4, 5] ('fail', 'no more primes') [4, 7] ('fail', 'no more primes') [4, 9] ('fail', 'no more primes') [4, 15] ('fail', 'delta<=0') [3, 5]
('fail', 'no more primes') [3, 7] ('fail', 'no more primes') [3, 8] ('fail', 'delta<=0') [3, 10] ('fail', 'no more primes') [3, 11]
('success', [3851]) [3, 16] ('fail', 'no more primes') [3, 20] ('success', [1181]) [2, 5] ('fail', 'no more primes') [2, 7] ('fail', 'no
more primes') [2, 9] ('fail', 'no more primes') [2, 11] ('fail', 'no more primes') [2, 15] ('fail', 'no more primes') [2, 21] ('fail',
'no more primes')
```

These are the commands used in the proof of Proposition 4.23.

```
"""
The commands simply follow the flow of the proof of Proposition 4.24.
"""
m=2; q=2
while q^(m/4)<=2*4.9:
    q=q+1
q

97

A=[]
for q in range(2,97):
    if is_prime_power(q):
        A.append([q,m])
len(A),A

(34, [[2, 2], [3, 2], [4, 2], [5, 2], [7, 2], [8, 2], [9, 2], [11, 2], [13, 2], [16, 2], [17, 2], [19, 2], [23, 2], [25, 2], [27, 2], [29, 2], [31,
2], [32, 2], [37, 2], [41, 2], [43, 2], [47, 2], [49, 2], [53, 2], [59, 2], [61, 2], [64, 2], [67, 2], [71, 2], [73, 2], [79, 2], [81, 2], [83,
2], [89, 2]])

"""
chk tries to perform multiplicative sieving, if necessary. If its returned value is
('success', []) it means that no multiplicative sieving was necessary.
"""
def chk(alpha):
    q=alpha[0]; m=alpha[1]; delta=1-1/q; lis=prime_divisors(q^m-1); i=len(lis); lis2=[]
    while delta>0 and i>=0:
        t=len(lis)-i
        if q^(m/2) > 2^(len(lis)-t)*(t/delta+2):
            return "success", lis2
        i=i-1; delta=delta-1/lis[i]
        lis2.append(lis[i])
        if delta<=0:
            return "fail", "delta<=0"
        if i<0:
            return "fail", "no more primes"
for alpha in A:
    print alpha, chk(alpha)

[2, 2] ('fail', 'delta<=0') [3, 2] ('fail', 'delta<=0') [4, 2] ('fail', 'no more primes') [5, 2] ('fail', 'delta<=0') [7, 2] ('fail',
'delta<=0') [8, 2] ('success', [7]) [9, 2] ('success', []) [11, 2] ('fail', 'delta<=0') [13, 2] ('success', [7, 3]) [16, 2] ('success',
[17]) [17, 2] ('success', []) [19, 2] ('success', []) [23, 2] ('success', []) [25, 2] ('success', []) [27, 2] ('success', []) [29, 2]
('success', [7]) [31, 2] ('success', []) [32, 2] ('success', []) [37, 2] ('success', []) [41, 2] ('success', []) [43, 2] ('success', []) [47,
2] ('success', []) [49, 2] ('success', []) [53, 2] ('success', []) [59, 2] ('success', []) [61, 2] ('success', []) [64, 2] ('success', [])
[67, 2] ('success', []) [71, 2] ('success', []) [73, 2] ('success', []) [79, 2] ('success', []) [81, 2] ('success', []) [83, 2] ('success',
[]) [89, 2] ('success', [])
```

These are the commands used for the proof of Theorem 4.25.

```
"""
exc is a dictionary where the keys are the cardinalities of the base fields who appear as
possible exceptions and each key is a list of all possible exception degrees. This agrees
with Table 4.1.
"""
exc={2:[12,8,6,4,3,5,7,9,11,15,21,2], 3:[12,6,4,3,5,7,8,10,16,2], 4:[6,4,3,5,7,9,15,2],
5:[5,3,4,8,16,6,12,2], 7:[4,6,3,12,5,2], 8:[6,4,3,7], 9:[3,8,4], 11:[4,3,10,5,6,2],
13:[12,3,4,6,8], 16:[15,3], 17:[4], 19:[4,3], 23:[4,3], 25:[3]}

"""
mat takes as input the finite field F and returns a list with all the matrices (where each
matrix is a list itself) to be investigated. It was built according the arguments of
Section 4.5.
"""
def mat(F):
    q=F.cardinality()
```

```

if q==2:
    return [[1,1,1,0],[1,0,1,1],[0,1,1,1]]
lis=[]
for i,a in enumerate(F):
    for j,b in enumerate(F):
        for k,c in enumerate(F):
            for l,d in enumerate(F):
                if (a*d-b*c)!=0 and ((d==1 and b==1 and a*c!=0) or
                    (d==0 and a!=0 and b==1 and c=1) or (a=1 and d==1 and b=0 and c!=0)
                    or (d==1 and b=1 and c=0 and a!=0) or (d==1 and b=1 and c!=0 and a==0)):
                    lis.append([l,x,y,z])
return lis

"""
is_primitive checks whether f is primitive. Note that f is an element of  $F_{\{q^n\}}$ ,
represented as a polynomial of  $F_q[X]/\langle g(X) \rangle$ . Here we check whether  $f^{((q^n-1)/p)}=1$  for
all prime divisors of  $q^n-1$ . If not then f is primitive.
"""
def is_primitive(f):
    f1=f(Y)
    for p in prime_divisors(F.cardinality()^g.degree()-1):
        if f1^((F.cardinality()^g.degree()-1)/p)==1:
            return False
    return True

"""
is_free checks whether f (the element) is free. This criterion is based on
Corollary 2.38 of [44].
"""
def is_free(f):
    f1=f(Y)
    m=matrix(S, n, lambda i, j: f1^(q^((i+j)%n)))
    return bool(m.determinant()!=0)

"""
numtopoly transforms a number into a polynomial. Its purpose is to turn integers into
elements of  $F_{\{q^n\}}$ , who are represented as polynomials.
"""
def numtopoly(m):
    m0=m; poly=0; i=0
    while m0!=0:
        poly=poly+list(F)[m0%q]*X^i
        i=i+1; m0=floor(m0/q)
    return poly

"""
chkmatrix takes a 2x2 matrix as input and assumes the presence of a list of elements that are
already known to be primitive and free. Then it seeks for an element in that list, such that
the Mobius transformation of this element that this matrix defines is free. Once the first
such element is found it exits, returning True and the successful element, but if the list is
exhausted without success it returns False and the matrix.
"""
def chkmatrix(A):
    for f in lopn:
        if is_free((A[0]*f+A[1])/(A[2]*f+A[3])):
            return True,f
    return False,A

"""
Here, we perform the actual calculations. First we the dictionary exc is opened and for each
q we first build  $F_q$  and a list of matrices to be considered. For each n in exc[q] we build
an irreducible g in  $F_q[X]$  of degree n, such that  $F_{\{q^n\}}=F_q[X]/\langle g(X) \rangle$ . Then we build a list,
named lopn of primitive and free elements of  $F_{\{q^n\}}$ , of size  $\leq \max\_pn$ , a number initially
defined, in order to speed up the list creation. This, of course, means that lopn can be
incomplete and insufficient results may occur; a warning is displayed if this is the case.
Then for all the matrices we check the validity of our statement.
"""
max_pn=200
for q in exc:
    F.<a>=GF(q,'a'); FX=PolynomialRing(F,'X'); X=FX.gen(); matrices=mat(F)
    print '-----'
    print '-----'
    print '          Checking q=',q

```

```

print ' F_',q,'= (Z /',F.characteristic(),'Z)[x] /',F.modulus()
print '-----'
print '-----'
for n in exc[q]:
    g=FX.irreducible_element(n)
    S=FX.quotient(g,'Y'); Y=S.gen()
    print '\n-----'
    print '          Checking n=',n
    print '    g=',g
    print '-----'
    i=1; lopn=[]
    while i<max_pn and i<q^n:
        f=numtopoly(i)
        if is_free(f) and is_primitive(f):
            lopn.append(f)
        i=i+1
    if i==max_pn:
        print 'Warning: max_pn reached, if not satisfied consider increasing it...'
    for j in range(0,len(matrices)):
        print j,chkmatrix(matrices[j])

```

The output of this program is too large to be included here, but the interested reader can find it online⁴. Moreover, the results are nicely presented in the tables of Section 4.5.

Here, note that on the first attempt (where $\text{max_pn}=200$ as above) for some pairs, namely $(3, 12)$, $(5, 5)$, $(8, 12)$, $(8, 7)$ and $(13, 6)$, the results were insufficient, while for $(5, 4)$ this restriction prohibited the full construction of the list of primitive and free elements, hence not finding a suitable element for some matrices did not necessarily imply a genuine exception. Nonetheless, we executed the program again for the pairs in question, with $\text{max_pn}=5000$, and those issues were resolved.

A.3 Computations of Chapter 5

These are the commands used for the proof of Proposition 5.15.

```

"""
Here, we follow the flow of the proof of Proposition 5.15 closely.
"""
q=23; m=17; c=4514.7
while q^(m/4)<=4^5*c^2:
    q=q+1
q

```

268

```

q=23; m=17; c=4514.7
while q^(m/4)<=4^5*c^2:
    m=m+1
m

```

31

```

def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])==0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for q in range(23,268):
    for m in range(17,31):
        if is_prime_power(q) and m0([q,m])<=4:
            A.append([q,m])
len(A),A

```

⁴<http://www.math.uoc.gr/~gkapet/pn/pn-results.txt>

20

```

for [q,m] in A:
    if q^(m/2)<=4^(len(prime_divisors(q^m-1))+1+m0([q,m])):
        print q,m

```

These are the Sage commands of Proposition 5.16.

```

"""
The commands follow closely the arguments of the proof.
"""
c=4514.7; q=23; m=q-1
while q^(m/4)<=2^(q+1)*((q-1)^2+1)*c^2:
    q=q+1; m=q-1
q

```

73

```

c=4514.7; q=23; m=2*(q-1)
while q^(m/4)<=2^(q+1)*((q-1)^2+1)*c^2:
    q=q+1; m=2*(q-1)
q

```

27

```

c=4514.7; q=23; m=3*(q-1)
while q^(m/4)<=2^(q+1)*((q-1)^2+1)*c^2:
    q=q+1; m=2*(q-1)
q

```

23

```

def cq(a,alpha):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if (alpha[0]^alpha[1]-1)%p==0:
            gin=gin*p; s=s+1;
            p=Primes().next(p)
        return 2^s/gin.nth_root(a)
A=[]
for q in range(23,73):
    m=q-1
    if is_prime_power(q) and q^(m/4)<=2^(q+1)*((q-1)^2+1)*cq(8,[q,m]):
        A.append(q)
A

```

[23, 25, 27, 29, 31, 32, 37, 41, 43]

```

for q in A:
    if q^((q-1)/2)<=2^(q+1)*((q-1)^2+1)^4^(len(prime_divisors(q^(q-1)-1))):
        print q

```

25

```

q=25; m=24
prime_factors(q^m-1)

```

[2, 3, 7, 13, 17, 31, 313, 601, 11489, 390001, 152587500001]

```

delta=1/25+2/152587500001+2/390001+2/11489+2/601+2/313; Delta=33/delta+2
q^m/2>2^(q+12)*Delta

```

True

These are the commands used in the proof of Proposition 5.17.

```

"""
The commands follow more or less the flow of the proof of Proposition 5.17. We begin by
assuming that m0=(q-1)/2.
"""
cq=4514.7; q=23; m=17
while q^(m/4)<=4*cq^2*((q-1)^2+1):
    m=m+1
m

```

32

```

cq=4514.7; q=23; m=17
while q^((q-1)/8)<=4*cq^2*((q-1)^2+1):
    q=q+1
q

```

54

```

def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])==0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for q in range(23,54):
    for m in range(17,32):
        if is_prime_power(q) and m0([q,m])==(q-1)/2:
            A.append([q,m])
A

```

[[37, 18], [41, 20], [43, 21], [47, 23], [49, 24], [53, 26]]

```

for alpha in A:
    q=alpha[0]; m=alpha[1]; mo=m0(alpha)
    if q^(m/2)<=4^(1+len(prime_divisors(q^m-1)))*(q*(2*mo-1)/(q-2*mo)+2):
        print alpha
"""
The proof for the case m0=(q-1)/2 is now complete. We now move on to the case m0=(q-1)/3.
"""
cq=4514.7; q=23; m=17
while q^(m/4)<=4*cq^2*((2*q^2-3*q+4)/(q+2)):
    m=m+1
m

```

28

```

cq=4514.7; q=23; m=17
while q^((q-1)/12)<=4*cq^2*((2*q^2-3*q+4)/(q+2)):
    q=q+1
q

```

67

```

A=[]
for q in range(23,67):
    for m in range(17,28):
        if is_prime_power(q) and m0([q,m])==(q-1)/3:
            A.append([q,m])
A

```

[[61, 20], [64, 21]]

```

for alpha in A:
    q=alpha[0]; m=alpha[1]; mo=m0(alpha)
    if q^(m/2)<=4^(1+len(prime_divisors(q^m-1)))*(q*(2*mo-1)/(q-2*mo)+2):
        print alpha
"""
The proof for the case m0=(q-1)/3 is complete. Now we assume that m0<=(q-1)/4, which is the
most challenging case. First, we consider the case where q0 less than 17 prime divisors.
"""
q=23; m=17
while q^(m/2)<=4^18*(q^2-2*q+2)/(q+1):
    q=q+1
q

```

28

```

q=23; m=17
while q^(m/2)<=4^18*(q^2-2*q+2)/(q+1):
    m=m+1
m

```

18

```

for q in range(23,28):
    if is_prime_power(q) and (q-1)%m0([q,17])==0:
        print q
"""
Now we can move on to the final case, where q0 has at least 17 prime divisors. Now that we have
some large prime divisors, i.e. we can apply multiplicative sieving as well... The commands
below find the 17th, 16th and 15th prime respectively.
"""
Primes().unrank(17), Primes().unrank(16), Primes().unrank(15)

```

(61, 59, 53)

```

a=1-2/53-2/59-2/61; cq=4514.7; q=23; m=17
while 16*q^(m/4)<=cq^2*(q^2-(4*a+7)*q+2)/((2*a-1)*q+1):
    m=m+1
m

```

22

```

q=23; m=17
while 16*q^(m/4)<=cq^2*(q^2-(4*a+7)*q+2)/((2*a-1)*q+1):
    q=q+1
q

```

78

```

"""
cq computes d_r.
"""
def cq(a,alpha):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if (alpha[0]^alpha[1]-1)%p==0:
            gin=gin*p; s=s+1;
            p=Primes().next(p)
    return 2^s/gin.nth_root(a)
for q in range(23,78):
    for m in range(17,22):
        if is_prime_power(q) and 16*q^(m/4)<=cq(8,[q,m])^2*(q^2-(4*a+7)*q+2)/((2*a-1)*q+1):
            print [q,m]

```

These are the Sage commands of Proposition 5.18.

```

"""
The commands here follow closely the arguments of the proof.
"""
q=23; m=20; c=4514.7
while (q^(1/4)/2)^m<=4*cq^2*((q^2*(q-2))/(q^2-q+1)+2):
    m=m+1
m

```

236

```

q=23; m=20; c=4514.7
while (q^(1/4)/2)^m<=4*cq^2*((q^2*(m-2))/(2*q^2-m)+2):
    q=q+1
q

```

988

```

def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])==0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for q in range(20,988):
    for m in range(20,236):
        if is_prime_power(q) and is_odd(q) and m0([q,m])==2*gcd(q-1,m):
            A.append([q,m])
len(A)

```


310

```

def cq(a,alpha):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if (alpha[0]^alpha[1]-1)%p==0:
            gin=gin*p; s=s+1;
            p=Primes().next(p)
    return 2^s/gin.nth_root(a)
for alpha in A:
    q=alpha[0]; m=alpha[1]
    if (q^(1/2)/2)^m<=4*cq(8,alpha)^2*((q^2*(m0(alpha)-2))/(2*q^2-m0(alpha))+2):
        print alpha

```

These are the commands we used in the proof of Proposition 5.19.

```

"""
The commands follow closely the arguments of the proof of Proposition 5.19.
"""
q=25; m=32; c=4514.7
while (q/8)^(m/4)<=4*c^2*((5*q-9)/(4-5*(q-1)/q^4)+2):
    m=m+1
m

```

77

```

q=25; m=32; c=4514.7
while (q/8)^(m/4)<=4*c^2*(q^4*(5*m-16)/(16*q^4-5*m)+2):
    q=q+1
q

```

106

```

def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])==0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for m in range(32,77):
    for q in range(25,106):
        if is_prime_power(q) and q%4==1 and m0([q,m])==4*gcd(m,q-1):
            A.append([q,m])
len(A),A

(8, [[25, 32], [41, 32], [73, 32], [89, 32], [37, 48], [61, 48], [49, 64], [81, 64]])

```

```

def cq(a,alpha):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if (alpha[0]^alpha[1]-1)%p==0:
            gin=gin*p; s=s+1;
            p=Primes().next(p)
    return 2^s/gin.nth_root(a)
for alpha in A:
    q=alpha[0]; m=alpha[1]
    if (q/8)^(m/4)<=4*cq(8,alpha)^2*(q^4*(5*m-16)/(16*q^4-5*m)+2):
        print alpha

```

These are the Sage commands of Proposition 5.20.

```

"""
The commands follow closely the arguments of the proof of Proposition 5.20.
"""
q=25; m=36; c=4517.4
while (q/4^(13/9))^m<=4*c^2*((46*q-82)/(36-46*(q-1)/q^6)+2):
    m=m+1
m

```

72

```

q=25; m=36; c=4517.4
while (q/4^(13/9))^(m/4)<=4*c^2*(q^6*(23*m-108)/(108*q^6-23*m)+2):
    q=q+1
q

```

72

```

def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])!=0:
        n=n/divisors(beta[0])[1]
    return n
A=[]
for q in range(25,72):
    if is_prime_power(q) and q%6==1 and m0([q,36])==6*gcd(m,q-1):
        A.append([q,36])
len(A),A

```

(3, [[31, 36], [43, 36], [67, 36]])

```

def cq(a,alpha):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if (alpha[0]^alpha[1]-1)%p==0:
            gin=gin*p; s=s+1;
            p=Primes().next(p)
    return 2^s/gin.nth_root(a)
for alpha in A:
    q=alpha[0]; m=alpha[1]
    if (q/4^(13/9))^(m/4)<=4*cq(8,alpha)^2*(q^6*(23*m-108)/(108*q^6-23*m)+2):
        print alpha

```

These are the commands used in the proof of Proposition 5.21.

```

"""
The commands are complicated, but they follow the flow of the proof of Proposition 5.21.
First, we consider q>=27.
"""

```

```

q=27; m=17; e=1.06*10^24
while (q/16)^(m/3)<=4*e^2:
    m=m+1
m

```

643

```

q=27; m=17; c=4514.7
while (q^(1/4)/4^(1/3))^m<=4*c^2*((q^2*(2*m-3))/(3*q^2-2*m)+2):
    m=m+1
m

```

61

```

q=27; m=17; c=4514.7
while (q^(1/4)/4^(1/3))^m<=4*c^2*((q^2*(2*m-3))/(3*q^2-2*m)+2):
    q=q+1
q

```

834

```

"""
cq computed d_{q_0} explicitly.
"""
def cq(a,alpha):
    s=0; gin=1.0; p=2
    while p < 2^a:
        if (alpha[0]^alpha[1]-1)%p==0:
            gin=gin*p; s=s+1;
            p=Primes().next(p)
    return 2^s/gin.nth_root(a)
A=[]
for m in range(17,61):
    for q in range(27,834):
        if is_prime_power(q) and (q^(1/4)/4^(1/3))^m<=4*cq(8,[q,m])^2*
            ((q^2*(2*m-3))/(3*q^2-2*m)+2):
            A.append([q,m])
len(A),A

```

(26, [[31, 17], [27, 18], [29, 18], [31, 18], [32, 18], [37, 18], [41, 18], [43, 18], [47, 18], [49, 18], [61, 18], [27, 20], [29, 20], [31, 20], [32, 20], [37, 20], [41, 20], [43, 20], [47, 20], [29, 22], [27, 24], [29, 24], [31, 24], [32, 24], [37, 24], [43, 24]])

```
for alpha in A:
    q=alpha[0]; m=alpha[1]
    if (q^(1/2)/4^(1/3))^m<=4^(1+len(prime_divisors(q^m-1)))*((q^2*(2*m-3))/(3*q^2-2*m)+2):
        print alpha
```

Since the last command yields no output, we have completed the case $q \geq 27$.

Now, we move on to the case $q=23$ or $q=25$. First, assume $s=2$ and $m \geq 530$.

```
q=23; m=17; c=3340.6
while q^(m/4)<=4^(1+2*624/3)*c^2:
    m=m+1
m
```

759

```
q=25; m=17; c=2760.4
while q^(m/4)<=4^(1+2*624/3)*c^2:
    m=m+1
m
```

739

```
"""
m0 computes m_0 (necessary for the computation of s) and sigma computes s,
in order to quickly exclude pairs from exception lists.
"""
```

```
def m0(beta):
    n=beta[1]
    while n%(divisors(beta[0])[1])==0:
        n=n/divisors(beta[0])[1]
    return n
def sigma(beta):
    s=1
    while (beta[0]^s-1)%m0(beta)!=0:
        s=s+1
    return s
A=[]; q=23
for m in range(530,759):
    if q^(m/4)<=4^(1+2*624/3)*cq(8,[q,m])^2 and sigma([q,m])==2:
        A.append([q,m])
q=25
for m in range(530,739):
    if q^(m/4)<=4^(1+2*624/3)*cq(8,[q,m])^2 and sigma([q,m])==2:
        A.append([q,m])
len(A),A
```

(3, [[23, 552], [25, 624], [25, 650]])

```
"""
Here we deal with the three 'nasty' possible exception pairs. The ugliness of the following
code is due to the fact that W(F_0) is computed.
"""
```

```
q=23; m=552; x=PolynomialRing(GF(q), 'x').gen()
print bool(q^(m/4)>4^(1+len(list((x^m-1).factor())))*cq(8,[q,m])^2)
q=25; x=PolynomialRing(GF(q), 'a', 'x').gen()
for m in [624,650]:
    print bool(q^(m/4)>4^(1+len(list((x^m-1).factor())))*cq(8,[q,m])^2)
```

True True True

```
"""
The case  $m \geq 530$  is over. We continue with the case  $m < 530$ .
"""
```

```
q=23; m=17; c=3340.6
while (q^(1/4)/4^(1/3))^m<=4*c^2*((q^2*(2*m-3))/(3*q^2-2*m)+2):
    m=m+1
m
```

67

```

A=[]
for m in range(17,67):
    for q in [23,25]:
        if (q^(1/4)/4^(1/3))^m<=4*cq(8,[q,m])^2*((q^2*(2*m-3))/(3*q^2-2*m)+2):
            A.append([q,m])
len(A),A

(16, [[23, 17], [25, 17], [23, 18], [25, 18], [23, 20], [25, 20], [23, 21], [25, 21], [23, 22], [25, 22], [23, 24], [25, 24], [23, 28], [23, 30], [25, 30], [23, 36]])

for alpha in A:
    if sigma(alpha)==2:
        print alpha

[23, 24]

"""
(23,24) turned out to be another 'nasty' individual.
"""
q=23; m=24
bool(((q^(1/2)/4^(1/3))^m>4^(1+len(prime_divisors(q^m-1)))*((q^2*(2*m-3))/(3*q^2-2*m)+2))

True

"""
Our final case is q=23,25 and s>=3; nothing special here...
"""
q=23; m=17; c=3340.6
while q^(m/4)<=4^(1+5*m/9)*c^2:
    m=m+1
m

1285

q=23; m=17; c=3340.6
while q^(m/4)<=4^(1+m/3)*c^2*((q^3*(4*m-9))/(9*q^3-4*m)+2):
    m=m+1
m

66

A=[]
for q in [23,25]:
    for m in range(17,66):
        if m0([q,m])>4 and sigma([q,m])>2 and q^(m/4)<=4^(1+m/3)*cq(8,[q,m])^2*
            ((q^3*(4*m-9))/(9*q^3-4*m)+2):
            A.append([q,m])
len(A),A

(11, [[23, 17], [23, 18], [23, 20], [23, 21], [23, 28], [23, 30], [23, 36], [25, 17], [25, 18], [25, 21], [25, 22]])

for alpha in A:
    q=alpha[0]; m=alpha[1]
    if q^(m/2)<=4^(1+len(prime_divisors(q^m-1)))*((q^3*(4*m-9))/(9*q^3-4*m)+2):
        print alpha

```

These are the commands that we used in the example in page 60.

```

"""
All the functions used here were borrowed from the proof of Theorem 4.25. is_primitive and
is_free do what their naming suggests, numtopoly creates the elements of F_{q^m}, g is the
modulus polynomial and maxpn determines the maximum number of elements to be found.
"""
q=23; m=18; maxpn=3
F=GF(q,'a'); FX=PolynomialRing(F,'X'); X=FX.gen()
g=FX.irreducible_element(m); S=FX.quotient(g,'Y'); Y=S.gen()
def is_primitive(f):
    f1=f(Y)
    for p in prime_divisors(F.cardinality())^g.degree()-1):
        if f1^((F.cardinality())^g.degree()-1)/p==1:
            return False
    return True

```

```

def is_free(f):
    f1=f(Y)
    ma=matrix(S, m, lambda i, j: f1^(q^((i+j)%m)))
    return bool(ma.determinant()!=0)
def numtopoly(n):
    m0=n; poly=0; i=0
    while m0!=0:
        poly=poly+list(F)[m0%q]*X^i
        i=i+1; m0=floor(m0/q)
    return poly
i=1; j=0
while j<maxpn and i<q^m:
    f=numtopoly(i)
    if is_free(f) and is_primitive(f) and is_free((2*f+1)/(f+1)) and
        is_primitive((2*f+1)/(f+1)):
        print f
        j=j+1
    i=i+1

```

$$\begin{array}{l}
 X + 1 \\
 2^*X + 5 \\
 3^*X + 3
 \end{array}$$

g

$$X^{18} + X^{12} + 18^*X^{11} + 2^*X^{10} + X^9 + 18^*X^8 + 3^*X^7 + 16^*X^6 + 21^*X^5 + 11^*X^3 + 3^*X^2 + 19^*X + 5$$

Bibliography

- [1] E. Bombieri. Counting points on curves over finite fields. In *Séminaire N. Bourbaki*, volume 1972/73, pages 234–241. Springer-Verlag, 1973. exp. no. 430.
- [2] L. Carlitz. Primitive roots in finite fields. *Trans. Amer. Math. Soc.*, 73(3):373–382, 1952.
- [3] L. Carlitz. Some problems involving primitive roots in a finite field. *Proc. Nat. Acad. Sci. U.S.A.*, 38(4):314–318, 1952.
- [4] L. Carlitz. Some theorems on irreducible reciprocal polynomials over a finite field. *J. Reine Angew. Math.*, 1967(227):212–220, 1967.
- [5] F. N. Castro and C. J. Moreno. Mixed exponential sums over finite fields. *Proc. Amer. Math. Soc.*, 128(9):2529–2537, 2000.
- [6] T. Cochrane and C. Pinner. Using Stepanov’s method for exponential sums involving rational functions. *J. Number Theory*, 116(2):270–292, 2006.
- [7] S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.
- [8] S. D. Cohen. The explicit construction of irreducible polynomials over finite fields. *Des. Codes Cryptogr.*, 2(2):169–174, 1992.
- [9] S. D. Cohen. Gauss sums and a sieve for generators of Galois fields. *Publ. Math. Debrecen*, 56(2-3):293–312, 2000.
- [10] S. D. Cohen. Explicit theorems on generator polynomials. *Finite Fields Appl.*, 11(3):337–357, 2005.
- [11] S. D. Cohen and D. Hachenberger. Primitive normal bases with prescribed trace. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):383–403, 1999.
- [12] S. D. Cohen and S. Huczynska. The primitive normal basis theorem – without a computer. *J. London Math. Soc.*, 67(1):41–56, 2003.
- [13] S. D. Cohen and S. Huczynska. The strong primitive normal basis theorem. *Acta Arith.*, 143(4):299–332, 2010.
- [14] S. D. Cohen and M. Prešern. Primitive polynomials with prescribed second coefficient. *Glasgow Math. J.*, 48:281–307, 2006.
- [15] S. D. Cohen and M. Prešern. The Hansen-Mullen primitivity conjecture: completion of proof. In *Number theory and polynomials*, volume 352 of *LMS Lecture notes*, pages 89–120. Cambridge University Press, Cambridge, 2008.

- [16] H. Davenport. Bases for finite fields. *J. London Math. Soc.*, 43(1):21–39, 1968.
- [17] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.
- [18] S. Fan. Primitive normal polynomials with the last half coefficients prescribed. *Finite Fields Appl.*, 15(5):604–614, 2009.
- [19] S. Fan, W. Han, and K. F. and. Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result. *Finite Fields Appl.*, 13(4):1029–1044, 2007.
- [20] S. Fan, W. Han, K. Feng, and X. Zhang. Primitive normal polynomials with the first two coefficients prescribed: A revised p -adic method. *Finite Fields Appl.*, 13(3):577–604, 2007.
- [21] S. Fan and X. Wang. Primitive normal polynomials with a prescribed coefficient. *Finite Fields Appl.*, 15(6):682–730, 2009.
- [22] É. Galois. Sur la théorie des nombres. *Bull. Sci. Math.*, 13:428–435, 1830.
- [23] S. Gao. *Normal Basis over Finite Fields*. PhD thesis, University of Waterloo, 1993.
- [24] T. Garefalakis. Irreducible polynomials with consecutive zero coefficients. *Finite Fields Appl.*, 14(1):201–208, 2008.
- [25] T. Garefalakis. On the action of $GL_2(\mathbb{F}_q)$ on irreducible polynomials over \mathbb{F}_q . *J. Pure Appl. Algebra*, 215(8):1835–1843, 2010.
- [26] T. Garefalakis. Self-reciprocal irreducible polynomials with prescribed coefficients. *Finite Fields Appl.*, 17(2):183–193, 2011.
- [27] T. Garefalakis and G. Kapetanakis. On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials. *Finite Fields Appl.*, 18(4):832–841, 2012.
- [28] T. Garefalakis and G. Kapetanakis. A note on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials. *Finite Fields Appl.*, 35(C):61–63, 2015.
- [29] C. F. Gauss. *Disquisitiones Arithmeticae*. Fleischer, Lipsiae, 1801.
- [30] S. W. Golomb. Algebraic constructions of Costas arrays. *J. Combin. Theory Ser. A*, 37(1):13–21, 1984.
- [31] K. H. Ham and G. L. Mullen. Distribution of irreducible polynomials of small degrees over finite fields. *Math. Comp.*, 67(221):337–341, 1998.
- [32] T. Hansen and G. L. Mullen. Primitive polynomials over finite fields. *Math. Comp.*, 59(200):639–643, 1992.
- [33] K. Hensel. Ueber die darstellung der zahlen eines gattungsbereiches für einen beliebigen primdivisor. *J. Reine Angew. Math.*, 103:230–237, 1888.
- [34] S. Hong and D. Bossen. On some properties of self-reciprocal polynomials. *IEEE Trans. Information Theory*, 21(4):462–464, 1975.
- [35] C. Hsu and T. Nan. A generalization of the primitive normal basis theorem. *J. Number Theory*, 131(1):146–157, 2011.
- [36] S. Huczynska. Existence results for finite field polynomials with specified properties. In P. Charpin, A. Pott, and A. Winterhof, editors, *Finite Fields and Their Applications: Character Sums and Polynomials*, pages 65–87, Berlin Boston, 2013. De Gruyter.
- [37] S. Huczynska, G. L. Mullen, D. Panario, and D. Thomson. Existence and properties of k -normal elements over finite fields. *Finite Fields Appl.*, 24:170–183, 2013.
- [38] G. James and M. Liebeck. *Representations and Characters of Groups*. Cambridge University Press, Cambridge, second edition, 2004.

- [39] G. Kapetanakis. The prime number theorem in function fields. Master's thesis, University of Crete, Heraklion, 2008. In Greek.
- [40] G. Kapetanakis. An extension of the (strong) primitive normal basis theorem. *Appl. Algebra Engrg. Comm. Comput.*, 25(5):311–337, 2014.
- [41] G. Kapetanakis. Normal bases and primitive elements over finite fields. *Finite Fields Appl.*, 26:123–143, 2014.
- [42] H. D. Kloosterman. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.
- [43] H. W. Lenstra, Jr and R. J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.
- [44] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, second edition, 1997.
- [45] J. L. Massey. Reversible codes. *Information and Control*, 7(3):369–380, 1964.
- [46] H. Meyn. On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):43–53, 1990.
- [47] H. Meyn and W. Götz. Self-reciprocal polynomials over finite fields. *Publ. Inst. Rech. Math. Av.*, 413/S-21:82–90, 1990.
- [48] G. L. Mullen and D. Panario. *Handbook of Finite Fields*. CRC Press, Boca Raton, 2013.
- [49] D. Panario and G. Tzanakis. A generalization of the Hansen-Mullen conjecture on irreducible polynomials over finite fields. *Finite Fields Appl.*, 18:303–315, 2012.
- [50] G. I. Perel'muter. Estimate of a sum along an algebraic curve. *Mat. Zametki*, 5(3):373–380, 1969.
- [51] M. Rosen. *Number Theory in Function Fields*, volume 210 of *Grad. Texts in Math*. Springer-Verlag, New York, 2002.
- [52] W. M. Schmidt. *Equations over Finite Fields, An Elementary Approach*. Springer-Verlag, Berlin Heidelberg, 1976.
- [53] S. A. Stepanov. The number of points of a hyperelliptic curve over a finite prime field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 33:1171–1181, 1969. In Russian.
- [54] H. Stichtenoth. *Algebraic Function Fields and Codes*, volume 254 of *Grad. Texts in Math*. Springer, Berlin Heidelberg, second edition, 2009.
- [55] H. Stichtenoth and A. Topuzoğlu. Factorization of a class of polynomials over finite fields. *Finite Fields Appl.*, 18(1):108–122, 2012.
- [56] T. Tian and W. F. Qi. Primitive normal element and its inverse in finite fields. *Acta Math. Sinica (Chin. Ser.)*, 49(3):657–668, 2006.
- [57] D. Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.
- [58] P. Wang, X. Cao, and R. Feng. On the existence of some specific elements in finite fields of characteristic 2. *Finite Fields Appl.*, 18(4):800–813, 2012.
- [59] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.*, 34(5):204–207, 1948.
- [60] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Hermann, Paris, 1948.
- [61] J. L. Yucas and G. L. Mullen. Self-reciprocal irreducible polynomials over finite fields. *Des. Codes Cryptogr.*, 33(3):275–281, 2004.

- absolute value of a polynomial, 8
- character, 7
 - additive, 11
 - canonical, 11
 - Dirichlet, 8
 - generator, 11
 - lifted, 11
 - multiplicative, 11
 - of a module, 13
 - quadratic, 11
 - trivial, 7
- character sum, 7
 - hybrid, 12
- characteristic function
 - of G -free elements, 15
 - of r -free elements, 15
- characteristic of a field, 3
- cyclotomic polynomial, 31
- Dirichlet L -function, 8
- divisor quadruple, 45
 - absolute value of, 53
 - decomposition of, 53
 - prime, 45
 - set of complementary divisor quadruples, 52
- divisor triple, 25
 - decomposition of, 29
 - prime, 25
 - absolute value of, 29
 - set of complementary divisor triples of, 29
- Euclidean domain, 13
- Euler function
 - for rings, 13
- Euler product, 9
- exponential sum, 7
- free element, 5
 - G -free, 15
 - k_A -free, 25
 - r -free, 13, 15
- free polynomial, 5
- Galois field, 3
- generalized Riemann hypothesis, 9
- group
 - additive, 11
 - dual of a , 7
 - multiplicative, 11
- Hansen-Mullen conjecture, 4, 5
- Jacobi symbol, 9, 17
- Kloosterman sums, 12
- Möbius function
 - for rings, 14
- Möbius transformation, 6
- module of a ring, 13
- norm, 11
- normal basis, 5
- normal basis theorem, 5, 13
- Order

<ul style="list-style-type: none"> of a character, 15 of an element, 15 order <ul style="list-style-type: none"> of a character, 15 of a module character, 13 of a module element, 13 of an element, 15 orthogonality relations, 7 primitive element, 5 primitive normal basis theorem, 5 primitive polynomial, 5 reciprocal of a polynomial, 4 Riemann hypothesis for function fields, 9 	<ul style="list-style-type: none"> self-reciprocal irreducible polynomial, 4 sieve, 5 sieving inequality <ul style="list-style-type: none"> for divisor quadruples, 53 for divisor triples, 30 sieving primes, 31 Stepanov-Schmidt method, 11, 13 strong primitive normal basis theorem, 5 trace, 11 <ul style="list-style-type: none"> absolute, 11 Vinogradov's formula, 13 von Mangoldt function, 10 Weil's theorem, 9
---	--