AAECC manuscript No.
(will be inserted by the editor)

An extension of the (strong) primitive normal basis theorem

Giorgos Kapetanakis

Received: October 18, 2012 / Accepted: June 11, 2014

Abstract An extension of the primitive normal basis theorem and its strong version is proved. Namely, we show that for nearly all $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, there exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(-dx+b)/(cx-a)$ are simultaneously primitive elements of $\mathbb{F}_{q^m}$ and produce a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, granted that q and m are large enough.

Keywords Finite field · Primitive element · Normal basis

Mathematics Subject Classification (2000) 11T30 · 11T06 · 11T24 · 12E20

1 Introduction

Let q be a power of some prime number p. We denote by $\mathbb{F}_q$ the finite field of q elements, by $\mathbb{F}_{q^m}$ its extension of degree m and by $\bar{\mathbb{F}}_q$ its algebraic closure. A generator of the multiplicative group $\mathbb{F}_{q^m}^*$ is called *primitive* and an element $x \in \mathbb{F}_{q^m}$ is called *free* over $\mathbb{F}_q$ if the set $\{x, x^q, x^{q^2}, \ldots, x^{q^{m-1}}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. Such a basis is called *normal*.

Hensel [15], in 1888, proved the existence of normal basis for arbitrary finite field extensions and 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 [12] and the references therein. Also, the existence of primitive elements for all finite fields is well-known. Besides their theoretical interest, primitive elements of finite fields are widely used

G. Kapetanakis
Department of Mathematics and Applied Mathematics, University of Crete, Voutes Campus, 70013, Heraklion, Crete, Greece
Tel.: +30-2810-393771
Fax: +30-2810-393881
E-mail: gkapet@math.uoc.gr

in various applications, including cryptographic schemes, such as the Diffie-Hellman key exchange [11], and the construction of Costas arrays [14], used in sonar and radar technology. A natural step is to wonder whether there exists an element combining those two properties for arbitrary finite field extension. The following result answers that question.

Theorem 1.1 (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 [20] were the first to provide a complete proof of the above, completing partial proofs of Carlitz [1,2] and Davenport [10]. Recently, Cohen and Huczynska [8] provided a computer-free proof, with the help of sieving techniques, previously introduced by Cohen [5]. Also, several generalizations of Theorem 1.1 have been investigated [7,16,18,27]. More recently, a stronger result was proved.

Theorem 1.2 (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 [26] were the first to prove this result for $m \geq 32$, but Cohen and Huczynska [9] were those who extended it to its stated form, once again with the help of their sieving techniques. The reader is referred to [6,17] and the references therein, for complete surveys of this, very active, line of research.

We consider an action of $\mathrm{GL}_2(\mathbb{F}_q)$, 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 $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$ and $F \in \mathbb{I}_n$, $n \geq 2$. We define

$$F^A(X) := (cX+d)^n F\left(\frac{aX+b}{cX+d}\right).$$

It is not hard to see [13,25] that the above rule defines an action of $\mathrm{GL}_2(\mathbb{F}_q)$ on $\mathbb{I}_n$, $n \geq 2$ and that $x \in \overline{\mathbb{F}}_q$ is a root of F if and only if $(-dx+b)/(cx-a)$ is a root of F^A. The problem of the enumeration of the fixed points of this action has recently gained attention [13,25].

In this work we are interested in whether there exists an irreducible $F \in \mathbb{F}_q[X]$, of degree m such that all its roots and all the roots of F^A are simultaneously primitive and free over $\mathbb{F}_q$. Clearly, $x \in \mathbb{F}_{q^m}$ is primitive or free over $\mathbb{F}_q$ if and only if all the other roots of its irreducible polynomial over $\mathbb{F}_q$ are also primitive or free over $\mathbb{F}_q$, thus the problem can be restated as follows.

Problem 1.3 Let q be a prime power, m a positive integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$. Does there exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(-dx+b)/(cx-a)$ are simultaneously primitive and free over $\mathbb{F}_q$?

Clearly, Theorems 1.1 and 1.2 solve the above problem completely for some special matrices, namely for matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & a \\ a & 0 \end{smallmatrix}\right)$ respectively. In this paper,

we prove that the above problem can be solved for most $A \in \mathrm{GL}_2(\mathbb{F}_q)$, if $q \geq 23$ and $m \geq 17$ (Theorem 6.9), providing an extension to these powerful and important theorems.

This work is influenced by the work of Lenstra and Schoof [20], while a character sum estimate [3,4,22] plays a crucial role in our proof. Moreover, much of this paper is inspired by the work of Cohen and Huczynska [8,9], whose sieving techniques have been adjusted and partially implemented. All non-trivial calculations were performed with MAPLE (v. 13). Finally, we note that, in several cases, simplicity and elegance were favored over optimality.

More specifically, in Section 2 we express the characteristic functions of the properties, we are interested in, with the help of characters. The aim of this is to use the character sums estimates, presented in Section 3, to obtain a sufficient condition for the existence of elements with the desired properties in Section 4. In Section 5, we implement the sieving techniques mentioned earlier, in order to further relax the condition of Section 4, while in Section 6 we prove the validity of the conditions of previous sections, hence the existence of elements with the desired properties.

2 Primitive and free elements

In this section, we present the concepts of G-free and d-free elements, where G is a polynomial and d a number. These concepts generalize the concepts of free and primitive elements respectively. Additionally, we give the definition of a character of an arbitrary group and give some basic properties of the characters of the additive and multiplicative groups of a finite field. Finally, we give the characteristic function of the properties we are interested in, in terms of characters.

Let $x \in \bar{\mathbb{F}}_q$ and $F = \sum_{i=0}^{n} f_i X^i \in \mathbb{F}_q[X]$. We define $F \circ x := \sum_{i=0}^{n} f_i x^{q^i}$. It is clear that, under the above action, the additive group $\bar{\mathbb{F}}_q$ is an $\mathbb{F}_q[X]$-module, therefore the annihilator of an element $x \in \bar{\mathbb{F}}_q$ is an ideal of $\mathbb{F}_q[X]$ and, as such, has a unique monic generator, called *Order* of x and denoted by $\mathrm{Ord}(x)$. In particular, we see that $x \in \mathbb{F}_{q^m} \iff (X^m - 1) \circ x = 0$, that is $x \in \mathbb{F}_{q^m} \iff \mathrm{Ord}(x) \mid X^m - 1$. In particular, it is clear that the elements of $\mathbb{F}_{q^m}$ that are free over $\mathbb{F}_q$ are exactly those of Order $X^m - 1$.

Furthermore, if $x \in \mathbb{F}_{q^m}$ is of Order G, then there exists some $y \in \mathbb{F}_{q^m}$ such that $H \circ y = x$, where $H(X) := (X^m - 1)/G(X)$, while elements of $\mathbb{F}_{q^m}$ which can be written in that manner are exactly those whose Order divides G. The above argument enables us to extend the definition of a free element. Suppose $G \mid X^m - 1$. We call $x \in \mathbb{F}_{q^m}$ *G-free* over $\mathbb{F}_q$ if $x = H \circ y$ for some $y \in \mathbb{F}_{q^m}$ and some $H \mid G$ implies $H = 1$.

Similarly, $x \in \mathbb{F}_{q^m}^*$ is primitive if $\mathrm{ord}(x) = q^m - 1$, where $\mathrm{ord}(x)$ stands for the multiplicative order of x. This means that x is primitive if and only if $x = y^d$, for some $y \in \mathbb{F}_{q^m}$ and $d \mid q^m - 1$, implies $d = 1$. Let $d \mid q^m - 1$, we call $x \in \mathbb{F}_{q^m}^*$ *d-free* if and only if, for $w \mid d$, $x = y^w$ implies $w = 1$. Furthermore, it follows from the definitions that $q^m - 1$ may be freely replaced by its radical q_0 and $X^m - 1$ may be replaced by its radical, $F_0 := X^{m_0} - 1$, where m_0 such that $m = m_0 p^b$ and $\gcd(m_0, p) = 1$.

In the rest of this section we present a couple of functions that characterize primitive and free elements. The concept of a character of a finite abelian group is necessary.

Definition 2.1 Let $\mathfrak{G}$ be a finite abelian group. A *character* of $\mathfrak{G}$ is a group homomorphism $\mathfrak{G} \to \mathbb{C}^*$, where $\mathbb{C}^*$ stands for the multiplicative group of $\mathbb{C}$. It is well known that 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 $\chi_o : \mathfrak{G} \to \mathbb{C}^*$, where $\chi_o(g) = 1$ for all $g \in \mathfrak{G}$, is called the *trivial character* of $\mathfrak{G}$. Finally, by $\bar{\chi}$ we denote the inverse of χ.

From now on, we will call the characters of the multiplicative group $\mathbb{F}_{q^m}^*$ *multiplicative characters* and the characters of the additive group $\mathbb{F}_{q^m}$ *additive characters*. Furthermore, we will denote by χ_o and ψ_o the trivial multiplicative and additive character respectively and we will extend the multiplicative characters to zero with the rule

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

A special multiplicative character is the *quadratic character*, which is defined for odd q and we denote by τ. Namely we have that

$$\tau(x) := \begin{cases} 1, & \text{if } x \text{ is a square in } \mathbb{F}_{q^m}^*, \\ -1, & \text{otherwise,} \end{cases}$$

and it is clear that τ is the only multiplicative character of order 2.

Before we continue further, we indicate some more well-known facts about additive and multiplicative characters. As mentioned before, $\widehat{\mathbb{F}_{q^m}^*} \cong \mathbb{F}_{q^m}^*$, hence $\widehat{\mathbb{F}_{q^m}^*}$ is cyclic of order $q^m - 1$, thus for every $d \mid q^m - 1$,

$$\sum_{\chi \in \widehat{\mathbb{F}_{q^m}^*},\ \mathrm{ord}(\chi)=d} 1 = \phi(d), \tag{1}$$

where ϕ stands for the Euler function. Furthermore, we denote by χ_g a generator of $\widehat{\mathbb{F}_{q^m}^*}$ and it follows that any non-trivial multiplicative character can be written as χ_g^n for some $n \in \{1, \ldots, q^m - 2\}$. Similarly, every additive character is of the form $\psi(x) = \exp((2\pi i \mathrm{Tr}(yx))/p)$, where Tr stands for the trace function of $\mathbb{F}_{q^m}$ over $\mathbb{F}_p$ and $y \in \mathbb{F}_{q^m}$. Conversely, every function of that form is an additive character. It is clear that ψ_o, the trivial character, corresponds to $y = 0$, while we denote by ψ_g the character that corresponds to $y = 1$. For the above well-known facts the reader is referred to classic textbooks [21,24].

Let $r \mid q^m - 1$. Following Cohen and Huczynska [8,9], we define the characteristic function of the r-free elements of $\mathbb{F}_{q^m}$ as follows:

$$\begin{aligned} &\omega_r : \mathbb{F}_{q^m} \to \mathbb{C}, \\ &\qquad x \mapsto \theta(r) \sum_{d \mid r} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in \widehat{\mathbb{F}_{q^m}^*}, \mathrm{ord}(\chi)=d} \chi(x), \end{aligned}$$

where μ denotes the Möbius function and $\theta(r) := \phi(r)/r = \prod_{l|r,l \text{ prime}}(1-l^{-1})$

In order to define the additive analogue of ω_r, the analogues of θ, ϕ, μ and the order of a character have to be defined. First observe that, $\widehat{\mathbb{F}_{q^m}}$ is an $\mathbb{F}_q[X]$-module under the rule $\psi^F(x) = \psi(F \circ x)$, for $\psi \in \widehat{\mathbb{F}_{q^m}}$, $F \in \mathbb{F}_q[X]$ and $x \in \mathbb{F}_{q^m}$. The *Order* of $\psi \in \widehat{\mathbb{F}_{q^m}}$ is defined as the monic polynomial generating the annihilator of ψ in $\mathbb{F}_q[X]$ and denoted by $\mathrm{Ord}(\psi)$. Let $F \in \mathbb{F}_q[X]$ be a non-zero polynomial, then $\phi(F) := |(\mathbb{F}_q[X]/F\mathbb{F}_q[X])^*|$, the analogue of the Euler function. The analogue of Eq. (1), shown in [20], states that for $G \in \mathbb{F}_q[X]$, with $G \mid X^m - 1$ we have that

$$\sum_{\psi \in \widehat{\mathbb{F}_{q^m}},\ \mathrm{Ord}(\psi)=G} 1 = \phi(G). \tag{2}$$

More interesting similarities between the two versions of ϕ can be shown [23, Ch. 1 and 2]. The definition of the analogues θ and the Möbius function are straightforward, namely for $F \in \mathbb{F}_q[X]$ define $\theta(F) := \phi(F)/q^{\deg(F)}$ and

$$\mu(F) := \begin{cases} (-1)^r, & \text{if } F \text{ is divisible by } r \text{ distinct monic irreducibles,} \\ 0, & \text{otherwise.} \end{cases}$$

We are now in position to define the analogue of ω_r, namely for $F \mid X^m - 1$, we define

$$\begin{aligned} &\Omega_F : \mathbb{F}_{q^m} \to \mathbb{C}, \\ &\qquad x \mapsto \theta(F) \sum_{G|F,\, G \text{ monic}} \frac{\mu(G)}{\phi(G)} \sum_{\psi \in \widehat{\mathbb{F}_{q^m}},\, \mathrm{Ord}(\psi)=G} \psi(x). \end{aligned}$$

It can be shown [8,9] that Ω_F is the characteristic function for the elements of $\mathbb{F}_{q^m}$ that are F-free over $\mathbb{F}_q$.

3 Character sums

The characteristic functions from the previous section involve characters, leading to consider character sums and a computation, or at least an estimation, of those will be necessary. The following results are well-known, while proofs for the first three results can be found in classic textbooks [21,24].

Lemma 3.1 (Orthogonality relations) *Let χ be a non-trivial character of a group $\mathfrak{G}$ and g a non-trivial element of $\mathfrak{G}$. Then*

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

Remark 3.2 Lemma 3.1 holds for arbitrary group $\mathfrak{G}$, i.e. it can be applied to both additive and multiplicative characters.

Lemma 3.3 (Kloosterman sums) *Let χ be a multiplicative character (may be trivial or non-trivial) and ψ a non trivial additive character. If $y_1, y_2 \in \mathbb{F}_{q^m}$ are not both zero, then*

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

Theorem 3.4 *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, then*

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

The following theorem plays a crucial role in our proof.

Theorem 3.5 *Let χ be a non-trivial multiplicative character of order n and ψ be a non-trivial additive character. Let $\mathscr{F}, \mathscr{G}$ be rational functions in $\mathbb{F}_{q^m}(X)$ such that $\mathscr{F} \neq y\mathscr{H}^n$, for any $y \in \mathbb{F}_{q^m}$ and $\mathscr{H} \in \mathbb{F}_{q^m}(X)$, and $\mathscr{G} \neq \mathscr{H}^p - \mathscr{H} + y$, for any $y \in \mathbb{F}_{q^m}$ and $\mathscr{H} \in \mathbb{F}_{q^m}(X)$. Then*

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

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

A slightly weaker (lacking the term l'') version of the above theorem was initially proved by Perel'muter [22], but Castro and Moreno [3] improved the result to its stated form. Recently, Cochraine and Pinner [4] presented a proof, which involves the elementary Stepanov-Schmidt method instead of concepts from algebraic geometry.

4 Some estimates

The purpose of this section is to prove Proposition 4.3, 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 4.3. 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 $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $q_i \mid q_0$ 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

$(-dx+b)/(cx-a)$ 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 $\mathbf{1}$, then their product can be defined naturally.

Example 4.1 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:

$$N_A(\mathbf{k}) = \sum_x \omega_{q_1}(x)\Omega_{F_1}(x)\omega_{q_2}\left(\frac{-dx+b}{cx-a}\right)\Omega_{F_2}\left(\frac{-dx+b}{cx-a}\right), \tag{3}$$

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

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 $F \in \mathbb{F}_q[X]$. It is clear that

$$\sum_{d \mid r} |\mu(d)| = 2^{t_r} \quad \text{and} \quad \sum_{G \mid F} |\mu(G)| = 2^{t_F}.$$

Additionally, set $W(r) := 2^{t_r}$, $W(F) := 2^{t_F}$. The lemma below provides us with an estimate for $W(r)$, where $r \in \mathbb{N}$. The proof, similar to [9, Lemma 3.7], is immediate using multiplicativity.

Lemma 4.2 *For any $r, \alpha \in \mathbb{N}$, $W(r) \leq c_{\alpha,r} r^{1/\alpha}$, where $c_{r,\alpha} = 2^s/(p_1 \cdots p_s)^{1/\alpha}$ and $p_1, \ldots, p_s$ are the primes $\leq 2^\alpha$ that divide r. In particular, we are interested in $c_r := c_{r,8}$ and $d_r := c_{r,12}$. Furthermore, for all $r \in \mathbb{N}$, $c_r < 4514.7$ and $d_r < 1.06 \cdot 10^{24}$.*

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. The purpose of the rest of this section is to prove the following.

Proposition 4.3 *Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$ 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.*

In the following subsections we will prove the above proposition for all possible forms of A.

Remark 4.4 In the following subsections it will become clear why the restriction $q \neq 2$ as well as the restriction regarding the entries are indeed necessary.

4.1 Matrices that are neither upper triangular nor anti-diagonal

In this subsection we assume that $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, 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. (3) can be rewritten as:

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{x \neq a/c} \sum_{d_1 | q_1} \frac{\mu(d_1)}{\phi(d_1)} \sum_{\mathrm{ord}(\chi_1)=d_1} \chi_1(x) \sum_{G_1|F_1} \frac{\mu(G_1)}{\phi(G_1)} \sum_{\mathrm{Ord}(\psi_1)=G_1} \psi_1(x)$$
$$\sum_{d_2|q_2} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\mathrm{ord}(\chi_2)=d_2} \chi_2\left(\frac{-dx+b}{cx-a}\right) \sum_{G_2|F_2} \frac{\mu(G_2)}{\phi(G_2)} \sum_{\mathrm{Ord}(\psi_2)=G_2} \psi_2\left(\frac{-dx+b}{cx-a}\right)$$

$$\Rightarrow N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}|\mathbf{k}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\chi_i, \psi_i} \mathscr{X}_A(\chi_1, \chi_2, \psi_1, \psi_2), \tag{4}$$

where

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

Proposition 4.5 *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*

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

Proof There exist some $n_i \in \{0, 1, \ldots, q^m - 2\}$ 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

$$\mathscr{X}_A(\chi_1, \chi_2, \psi_1, \psi_2) = \sum_{x \neq a/c} \chi_g(\mathscr{F}(x))\psi_g(\mathscr{G}(x)), \tag{5}$$

where $\mathscr{F}(X) := (X^{n_1}(-dX+b)^{n_2})/(cX-a)^{n_2} \in \mathbb{F}_q(X)$ and $\mathscr{G}(X) := (y_1 X(cX-a) + y_2(-dX+b))/(cX-a) \in \mathbb{F}_q(X)$. We prove the desired result for all possible forms of $\mathscr{F}$ and $\mathscr{G}$.

From Eq. (5), Theorem 3.5 implies that if $\mathscr{F} \neq y\mathscr{H}^{q^m-1}$, for any $y \in \mathbb{F}_{q^m}$ and $\mathscr{H} \in \mathbb{F}_{q^m}(X)$, and $\mathscr{G} \neq \mathscr{H}^p - \mathscr{H} + y$, for any $y \in \mathbb{F}_{q^m}$ and $\mathscr{H} \in \mathbb{F}_{q^m}(X)$, then

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

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

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

Since H_1 and H_2 are co-prime, the above equation implies $H_2^{q^m-1} \mid (cX-a)^{n_2}$, 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 $(-dX+b)^{n_2} = y'(cX-a)^{n_2}$, where

$y' := yH_1^{q^m-1}H_2^{1-q^m} \in \mathbb{F}_{q^m}$, impossible for $A \in \mathrm{GL}_2(\mathbb{F}_q)$, unless $n_2 = 0$. Additionally, if $y_1 = 0$ and $y_2 \neq 0$, then, from Eq. (5), we have that

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

according to Lemma 3.1. Similarly, if $y_1 \neq 0$ and $y_2 = 0$, then

$$\begin{aligned}|\mathscr{X}_A(\chi_1,\chi_2,\psi_1,\psi_2)| &= \left|\sum_{x\neq a/c}\psi_g(y_1 x)\right| = \left|-\psi_g(y_1 a/c)+\sum_{x\in\mathbb{F}_{q^m}}\psi_1(x)\right| \\ &= |-\psi_g(y_1 a/c)| = 1.\end{aligned}$$

Finally, if $y_1, y_2 \neq 0$, then Eq. (5) yields

$$\begin{aligned}|\mathscr{X}_A(\chi_1,\chi_2,\psi_1,\psi_2)| &= \left|\sum_{x\neq a/c}\psi_g((y_1 x(cx-a)+y_2(-dx+b))/(cx-a))\right| \\ &= \left|\sum_{y\neq 0}\psi_g(yy_1/c+y^{-1}y_2(-da+bc)/c+(y_1 a-y_2 d)/c)\right| \\ &= \left|\psi_g(z_0)\sum_{y\neq 0}\psi_g(z_1 y+z_2 y^{-1})\right| = \left|\sum_{y\neq 0}\psi_g(z_1 y+z_2 y^{-1})\right|,\end{aligned}$$

where $z_0 := (y_1 a - y_2 d)/c$, $z_1 := y_1/c$ 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 3.3.

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

$$\mathscr{G} = \mathscr{H}^p - \mathscr{H} + y \Rightarrow \frac{y_1 X(cX-a)+y_2(-dX+b)}{cX-a} = \frac{H_1^p - H_1 H_2^{p-1} + yH_2^p}{H_2^p}.$$

It follows immediately from the restrictions on A that $cX-a$ is co-prime to $y_1X(cX-a)+y_2(-dX+b)$ and it is clear that H_2^p is co-prime to $H_1^p - H_1H_2^{p-1} + yH_2^p$, hence $cX - a = H_2^p$, a contradiction since $c \neq 0$. It follows that $\mathscr{G} = 0$, 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 $X^{n_1}(-dX+b)^{n_2}(cX-a)^{q^m-1-n_2}$ 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), we have

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

but the last sum is bounded by $2q^{m/2}$, from Theorem 3.4. □

Proposition 4.5 and Eq. (4) imply

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

The above, combined with Eqs. (1) and (2), is rewritten as

$$N_A(\mathbf{k}) \geq \theta(\mathbf{k}) q^{m/2} \left(q^{m/2} - \frac{1}{q^{m/2}} - 4 \sum_{\mathbf{l}|\mathbf{k},\mathbf{l}\neq\mathbf{1}} \mu(\mathbf{l}) \right)$$
$$\Rightarrow N_A(\mathbf{k}) \geq \theta(\mathbf{k}) q^{m/2} (q^{m/2} - q^{-m/2} - 4(2^{t_{q_1}+t_{q_2}+t_{F_1}+t_{F_2}} - 1)).$$

Summing up, we have proved the following, which clearly implies Proposition 4.3, provided A is of the described form.

Proposition 4.6 *Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, 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.*

4.2 Upper triangular matrices that are not diagonal

In this section we focus on matrices of the form $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, with $b \neq 0$. Before proceeding, we have to study a bit more the behavior of the Order of an additive character.

Lemma 4.7 *Let $\psi \in \widehat{\mathbb{F}_{q^m}}$ be an additive character, then $\psi|_{\mathbb{F}_q}$ is trivial if and only if* $\mathrm{Ord}(\psi) \mid X^{m-1} + X^{m-2} + \cdots + 1$.

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

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

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

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

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

Lemma 4.8 *If $\gcd(p,m) = 1$, then $\{\psi|_{\mathbb{F}_q} : \psi \in \widehat{\mathbb{F}_{q^m}}, \mathrm{Ord}(\psi) \mid X - 1\} = \widehat{\mathbb{F}_q}$.*

Proof From Eq. (2), 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 4.7 yields $\mathrm{Ord}(\psi_1\bar{\psi}_2) \mid X^{m-1} + \cdots + 1$. It is clear though that $\mathrm{Ord}(\psi_1\bar{\psi}_2) \mid X - 1$ and it follows that $\mathrm{Ord}(\psi_1\bar{\psi}_2) = 1$, i.e. $\psi_1 = \psi_2$. $\square$

Lemma 4.9 *Let* $G_1, G_2 \in \mathbb{F}_q[X]$ *such that* $G_1G_2 \mid X^m-1$ *and* $\gcd(G_1,G_2)=1$. *If* $\mathfrak{G}_i := \{\psi \in \widehat{\mathbb{F}_{q^m}} : \mathrm{Ord}(\psi) = G_i\}$ *(*$i=1,2$*) and* $\mathfrak{G} := \{\psi \in \widehat{\mathbb{F}_{q^m}} : \mathrm{Ord}(\psi) = G_1G_2\}$, *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 $F = \mathrm{Ord}(\psi_1\psi_2)$. It is clear that $(\psi_1\psi_2)^{G_1G_2} = \psi_o$, thus $F \mid G_1G_2$. It is also clear that $(\psi_1\psi_2)^F = \psi_o$, that is $\psi_1^F = \bar{\psi}_2^F$. Since $\mathrm{Ord}(\psi_1^F) \mid G_1$ and $\mathrm{Ord}(\bar{\psi}_2^F) \mid G_2$, it follows that $\psi_1^F = \psi_2^F = \psi_o$, consequently $G_1 \mid F$ and $G_2 \mid F$, i.e. $G_1G_2 \mid F$. $\square$

As in Subsection 4.1, we have

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}\mid\mathbf{k}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\chi_i,\psi_i} \psi_2(b/a)\mathscr{Y}_A(\chi_1,\chi_2,\psi_1,\psi_2), \tag{6}$$

where

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

where $\psi_2'(x) := \psi_2(-dx/a)$ 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 $|\mathscr{Y}_A(\chi_1,\chi_2,\psi_1,\psi_2)| \le 2q^{m/2}$, from Theorem 3.5. If exactly two of $\chi_1,\chi_2,(\psi_1\psi_2')$ are non-trivial, then Theorems 3.4 and 3.5 imply $|\mathscr{Y}_A(\chi_1,\chi_2,\psi_1,\psi_2)| \le q^{m/2}$. If exactly one of $\chi_1,\chi_2,\psi_1\psi_2'$ is non-trivial, Lemma 3.1 implies $\mathscr{Y}_A(\chi_1,\chi_2,\psi_1,\psi_2) = 0$. Now, as in section 4.1, we get

$$\left|\frac{N_A(\mathbf{k})}{\theta(\mathbf{k})} - q^m \sum_{G\mid\gcd(F_1,F_2)} \frac{\mu(G)^2}{\phi(G)^2} \sum_{\mathrm{Ord}(\psi_2)=G} \psi_2\left(\frac{b}{a}\right)\right| \le 2q^{m/2}(W(\mathbf{k})-4). \tag{7}$$

Eq. (7) 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 $\gamma := b/a \neq 0$. It follows immediately from Lemma 4.7 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 3.1, 4.8 and 4.9, we evaluate:

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

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

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

Summing up, Eqs. (6) and (7) 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 4.10 *Let $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, 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 4.11 If $q = 2$, then the left part of the latter is zero and the inequality holds only for $\mathbf{k} = \mathbf{1}$. This is not a surprise, since one easily checks that in this case $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and, therefore, problem 1.3 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 4.3 is clearly implied, provided that A is of the described form.

4.3 Anti-diagonal matrices

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

Lemma 4.12 *Let α, β be integers such that β/α is an odd integer and β is square-free. Then*

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

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

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

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

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

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

As in Subsection 4.1, we conclude

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\mathbf{l}|\mathbf{k}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\chi_i, \psi_i} \chi_2(\gamma) \mathscr{Z}_A(\chi_1, \chi_2, \psi_1, \psi_2), \tag{8}$$

where

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

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 $|\mathscr{Z}_A(\chi_1, \chi_2, \psi_1, \psi_2)|$ is bounded by $2q^{m/2}$, from Lemma 3.3. If exactly one of ψ_1, ψ_2 and $\chi_1\bar{\chi}_2$ is non-trivial, then $|\mathscr{Z}_A(\chi_1, \chi_2, \psi_1, \psi_2)| = 0$, from Lemma 3.1. We eventually get

$$\left| \frac{N_A(\mathbf{k})}{\theta(\mathbf{k})} - (q^m - 1) \sum_{d | \gcd(q_1, q_2)} \frac{\mu^2(d)}{\phi^2(d)} \sum_{\mathrm{ord}(\chi_2) = d} \chi_2(\gamma) \right| \leq 2q^{m/2}(W(\mathbf{k}) - 4). \tag{9}$$

Eq. (9) implies that a lower bound for the coefficient of q^m is desirable. Set $q_3 := \gcd(q_1, q_2)$. Furthermore, we observe that the function

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

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. (9) can be rewritten as

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

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

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

With the help of these observations, the coefficient of q^m in Eq. (9) can be rewritten as

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

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 4.12 that the last expression of the coefficient of q^m in Eq. (9) is larger than $1/2$. Now, Eqs. (8) and (9) 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 4.13 *Let $A = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, 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 4.14 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 $\gamma \in \mathbb{F}_{q^m}$ is not a square, i.e. $\tau(\gamma) = -1$, then one easily checks that $(\gamma x)^{(q^m-1)/2} = 1$, i.e. γx is not primitive. Additionally, it is clear that Proposition 4.13 implies Proposition 4.3, provided that A is of the described form.

4.4 Diagonal matrices

In this subsection we prove Proposition 4.3, when A is diagonal. Suppose $A = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $\gamma := d/a$ and $\tau(\gamma) = 1$, where τ is the quadratic character; Eq. (3) 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 $F_3 := \mathrm{lcm}(F_1, F_2)$, 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 4.1, we get

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

where

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

Lemma 3.1 implies that $\mathscr{W}(\chi_1,\chi_2,\psi) = 0$, 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 3.5 implies that $|\mathscr{W}(\chi_1,\chi_2,\psi)| \leq q^{m/2}$. Now, as in previous subsections, we get

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

The coefficient of q^m in the above equation was proved to be larger than $1/2$ in Subsection 4.3, 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 4.15 *Let $A = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, where $\tau(d/a) = 1$, 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 4.16 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 4.15 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 4.14 apply in this case as well.

5 The sieve

Following Cohen and Huczynska [8,9], 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 [9], 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 $\{\mathbf{k}_1, \ldots, \mathbf{k}_r\}$, where the $\mathbf{k}_i$'s are divisor quadruples 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 $\mathbf{k}_1, \ldots, \mathbf{k}_r$ are such that $\mathbf{k}_i = \mathbf{k}_0\mathbf{p}_i$, where $\mathbf{p}_1, \ldots, \mathbf{p}_r$ 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 Example 4.1 and help us understand the new concepts defined here.

Example 5.1 Make all the assumptions of Example 4.1. 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 5.2 (Sieving inequality) *Let $A \in \mathrm{GL}_2(\mathbb{F}_q)$, $\mathbf{k}$ be a divisor quadruple and $\{\mathbf{k}_1,\ldots,\mathbf{k}_r\}$ 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 $\mathbf{k}_2,\ldots,\mathbf{k}_{k+1}$, then it is clear that $\{\mathbf{k}',\mathbf{k}_1\}$ is a set of complementary divisor quadruples of $\mathbf{k}$ with common divisor $\mathbf{k}_0$. The desired result follows immediately from the induction hypothesis. □

Proposition 5.3 *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 $A \in \mathrm{GL}_2(\mathbb{F}_q)$, $q > 2$ and $q^{m/2} > 4W(\mathbf{k}_0)\Delta$, then $N_A(\mathbf{k}) > 0$.*

Proof Suppose $\mathbf{p}_1,\ldots,\mathbf{p}_r$ are the primes of the $(\mathbf{k}_0,r)$-decomposition. Proposition 5.2 implies

$$N_A(\mathbf{k}) \geq \delta N_A(\mathbf{k}_0) + \sum_{i=1}^{r}\left(N_A(\mathbf{k}_0\mathbf{p}_i) - \left(1-\frac{1}{|\mathbf{p}_i|}\right)N_A(\mathbf{k}_0)\right). \tag{10}$$

Suppose A is of the form described in Subsection 4.1. In that case, taking into account the analysis done in subsection 4.1, Eq. (10) 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 4.2 and 4.3. With the help of the analysis of those subsections and Eq. (10), 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 4.4. Eq. (10) 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 $\mathbf{p}_1,\ldots,\mathbf{p}_{r'}$ 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. □

Clearly, if $m_0 = q-1$, then F_0 splits into linear factors. If $m_0 \neq q-1$, then $F_0 = \prod_{d|m_0} Q_d$, where Q_d is the d-th cyclotomic polynomial. The d-th cyclotomic polynomial splits into $\phi(d)/s_d$ 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 these well-known facts, the reader is referred to [21, §2.4].

It follows that F_0 splits into $\phi(m_0)/s$ 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 is more or less a restatement of Proposition 5.3, where we have exploited the predictable factorization of F_0, in order to choose a suitable universal decomposition of $\mathbf{w}$.

Proposition 5.4 *Let $\{l_1,\ldots l_t\}$ 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 5.3 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 $sr_1 = m_0 - r_0$. □

6 Evaluations

From Proposition 5.4 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 6.1 sieving is unnecessary, but is essential for all the rest.

Proposition 6.1 *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 4.3 and Lemma 4.2, since $W(F_0) \leq 2^4$, it suffices to show that

$$q^{m/4} > 4^5 c_{q_0}^2, \tag{11}$$

where $c_{q_0} < 4514.7$. 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 nineteen pairs (q,m) satisfying $m_0 \leq 4$, but only eight of them, namely $(23,23)$, $(25,20)$, $(25,25)$, $(27,18)$, $(27,27)$, $(32,24)$, $(49,21)$ and $(81,18)$, do not satisfy Eq. (11) for $c_{q_0} < 4514.7$. For those pairs we compute $W(q_0) \leq 2^{15}$ and now a sufficient condition would be $q^{m/2} > 4^{20}$, which is satisfied from all eight mentioned pairs. □

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 6.2 *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 $\mathbf{w} = (q_0, q_0, F_o, F_0)$, 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 5.3 that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 2^{q+1}((q-1)^2+1) W^2(q_0). \tag{12}$$

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 5.3 yields that if Eq. (12) holds, then $N_A(\mathbf{w}) > 0$, hence if Eq. (12) holds, then $N_A(\mathbf{w}) > 0$ in any case. With the help of Lemma 4.2, Eq. (12) may be replaced with

$$q^{m/4} > 2^{q+1}((q-1)^2+1)c_{q_0}^2. \tag{13}$$

Eq. (13) is easily verified for $q > 72$, since $m \geq q-1$ and $c_{q_0} \leq 4514.7$. Similarly, if $m \neq q-1$, then $m \geq 2(q-1)$ and Eq. (13) is easily verified for $q \geq 27$.

The remaining cases are those when $m = q-1$ and $23 \leq q \leq 71$. For those values we compute $c_{q_0} < 45.2$ and now Eq. (13) holds for $q > 55$. For $23 \leq q \leq 55$, q a prime power and $m = q-1$ we verify directly that Eq. (12) 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 5.3 are satisfied, i.e. $N_A(\mathbf{w}) > 0$. □

Proposition 6.3 *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 5.4, 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 5.4 is positive, since $m_0 \leq (q-1)/2$. It follows that $N_A(\mathbf{w}) > 0$ if

$$q^{m/2} > 4W^2(q_0)\left(\frac{q(2m_0-1)}{q-2m_0} + 2\right). \tag{14}$$

Assume $m_0 = (q-1)/2$. With the help of Lemma 4.2, Eq. (14) can be replaced by $q^{m/4} > 4c_{q_0}^2((q-1)^2+1)$, where $c_{q_0} < 4514.7$. 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 $q^{(q-1)/8} > 4c_{q_0}^2((q-1)^2+1)$. This is satisfied for $q \geq 54$. For the remaining pairs (q,m), q is an odd prime power $23 \leq q < 54$ and $17 \leq m < 32$. Since $m_0 = (q-1)/2$ and $m_0 \mid m$ it follows that $2m \equiv 0 \pmod{q-1}$ and a computation shows that this condition holds for nine pairs, but only six of them, 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. (14) can be verified directly.

Next, assume $m_0 = (q-1)/3$. As above, it turns out that $N_A(\mathbf{w}) > 0$, if $q^{m/4} > 4c_{q_0}^2 \frac{2q^2-3q+4}{q+2}$, where $c_{q_0} < 4514.7$. 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 $q^{(q-1)/12} > 4c_{q_0}^2 \frac{2q^2-3q+4}{q+2}$, which holds for $q \geq 67$. For the remaining pairs (q,m), q is a prime power $23 \leq q < 67$ and $17 \leq m < 28$. Since $m_0 = (q-1)/3$ and $m_0 \mid m$ it follows that $3m \equiv 0 \pmod{q-1}$ and a computation shows that this condition holds for seven pairs, but only two of them, namely $(61,20)$ and $(64,21)$, satisfy $m_0 = (q-1)/3$. For both pairs, Eq. (14) can be verified directly.

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. (14) 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 5.4 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 5.4 and Lemma 4.2 imply that $N_A(\mathbf{w})$ is positive, granted that

$$4^2 q^{m/4} > c_{q_0}^2 \frac{q^2 - (4\alpha+7)q + 2}{(2\alpha-1)q+1}, \tag{15}$$

where $\alpha := 1 - 2/l_i - 2/l_2 - 2/l_3$. Since $\alpha \geq 1 - 2/53 - 2/59 - 2/61$ and $c_{q_0} < 4514.7$, Eq. (15) 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 $c_{q_0} < 28.5$ and Eq. (15) holds for $q \geq 23$ and $m \geq 9$. □

In the rest of this section we focus on the remaining cases, i.e. when $m_0 > 4$ and $s \neq 1$. Following Cohen and Huczynska [8,9] 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 lemma below, proven in [8], provides an estimation of ρ.

Lemma 6.4 *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 $\rho \leq 1/3$.*

Clearly, the demand $m_0 > 4$ is not a restriction at all, since in Proposition 6.1 the cases where $m_0 \leq 4$ have already been settled. Furthermore, Proposition 5.4 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 4^{\rho m_0 + 1} W^2(q_0) \left(\frac{\frac{2(1-\rho)m_0}{s} - 1}{1 - \frac{2(1-\rho)m_0}{sq^s}} + 2 \right), \tag{16}$$

since $t_{F_0/G_0} \leq r_0$ and $\rho m_0 = t_{F_0/G_0}$, for $m_0 < \frac{sq^s}{2(1-\rho)}$.

Proposition 6.5 *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 6.4 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. (16) as a sufficient condition for $N_A(\mathbf{w}) > 0$. It follows from Lemma 4.2 that if

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

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 $c_{q_0} < 4514.7$, $q \geq 23$ and $m \geq 236$.

For $m < 236$ the denominator of the fraction of Eq. (16) remains positive for $q \geq 23$, even if we substitute m_0 with m. It follows that a sufficient condition is

$$\left(\frac{\sqrt[4]{q}}{2}\right)^m > 4c_{q_0}^2\left(\frac{q^2(m-2)}{2q^2-m}+2\right). \tag{17}$$

This inequality holds for $c_{q_0} < 4514.7$, $q \geq 988$ and $20 \leq m < 236$. For each remaining pair (q,m), where $23 \leq q < 988$ is an odd prime power and $20 \leq m < 236$, with $m \equiv 0 \pmod 4$, we compute c_{q_0} explicitly and exclude those pairs who do not satisfy Eq. (17). In what remains, a computation reveals that the only pairs (q,m), satisfying the implied restrictions of Lemma 6.4, i.e. $m_0 = 2\gcd(m,q-1)$, are $(23,92)$, $(25,80)$ and $(27,36)$. For the those three pairs $m_0 \leq 16$ and $c_{q_0} < 15.7$. It follows, from Eq. (16), that a sufficient condition for those pairs would be $q^{m/4} > 4^9 15.7^2\left(\frac{7q^2}{q^2-8}+2\right)$, which is satisfied by all three of them. □

Proposition 6.6 *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 6.4 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. (16) as a sufficient condition for $N_A(\mathbf{w}) > 0$. It follows from Lemma 4.2 that if

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

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 $c_{q_0} < 4514.7$, $q \geq 25$ and $m \geq 77$.

For $m < 77$ the denominator appearing in Eq. (16) remains positive, even if we substitute m_0 with m. It follows that $N_A(\mathbf{w}) > 0$ if

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

This condition is satisfied for $q \geq 106$, $32 \leq m < 77$ and $c_{q_0} < 4514.7$. For each remaining pair (q,m), i.e. where $25 \leq q < 106$, a prime power with $q \equiv 1 \pmod 4$ and $32 \leq m < 77$, with $16 \mid m$, we compute c_{q_0} explicitly and check that the above condition holds in any case. □

Proposition 6.7 *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 6.4 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. (16) as a sufficient condition for $N_A(\mathbf{w}) > 0$. It follows, from Lemma 4.2. that if

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

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 $c_{q_0} < 4514.7$, $q \geq 25$ 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

$$(q/4^{13/9})^{m/4} > 4c_{q_0}^2 \left(\frac{q^6(23m-108)}{108q^6-23m} + 2 \right). \tag{18}$$

This condition is satisfied for $q \geq 72$, $m = 36$ and $c_{q_0} < 4514.7$. For the remaining pairs, i.e. $25 \leq q < 72$, a prime power with $q \equiv 1 \pmod 6$, and $m = 36$, we compute $c_{q_0} < 20.1$. For this bound of c_{q_0}, Eq. (18) is satisfied by all the possible exceptions described previously, with the sole exception of $(25, 36)$, which fails to satisfy $m_0 = 6\gcd(m, q-1)$. □

Proposition 6.8 *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 4.3 and Lemma 4.2 that $N_A(\mathbf{w}) > 0$, if $(q/16)^{m/3} > 4d_{c_0}^2$, where $d_{c_0} < 1.06 \cdot 10^{24}$. 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. (16) for the remaining cases. This means that if

$$(\sqrt[4]{q}/\sqrt[3]{4})^m > 4c_{q_0}^2 \left(\frac{q^2(2m-3)}{3q^2-2m} + 2 \right), \tag{19}$$

from Lemma 4.2, then $N_A(\mathbf{w}) > 0$. This condition is satisfied for $q \geq 27$ and $61 \leq m < 642$ and for $q \geq 834$ and $17 \leq m < 642$, provided that $c_{q_0} < 4514.7$. In the remaining region, we compute c_{q_0}, for each pair (q, m), and it follows that Eq. (19) is satisfied for all but 26 pairs. Moreover, Eq. (16) implies that if

$$(\sqrt{q}/\sqrt[3]{4})^m > 4W^2(q_0) \left(\frac{q^2(2m-3)}{3q^2-2m} + 2 \right), \tag{20}$$

then $N_A(\mathbf{w}) > 0$. We explicitly compute $W(q_0)$ for all 26 remaining pairs and check that all 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 $c_{q_0} < 3340.6$. 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 4.3 and Lemma 4.2 that $N_A(\mathbf{w}) > 0$ if $q^{m/4} > 4^{1+\frac{2 \cdot 624}{3}} c_{q_0}^2$. This condition is satisfied for $q = 23$, $m \geq 759$ and $c_{q_0} < 3340.6$ and for $q = 25$, $m \geq 739$ and $c_{q_0} < 2760.4$. We also verify that $N_A(\mathbf{w}) > 0$ the remaining pairs (q, m), where $q \in \{23, 25\}$ and $m \geq 530$, since all those pairs satisfy $q^{m/4} > 4W(F_0)^2 c_{q_0}^2$, where $W(F_0)$ and c_{q_0} is computed explicitely for each pair.

For $m \leq 529$, we have that $m_0 \leq m \leq 529 < \frac{sq^s}{2(1-\rho)}$, which means we can use Eq. (16) for the remaining cases, i.e. if Eq. (19) is satisfied, then $N_A(\mathbf{w}) > 0$. This

condition is satisfied for $q \geq 23$, $67 \leq m \leq 529$ and $c_{q_0} < 3340.6$. For the remaining cases, namely $q \in \{23,25\}$ and $17 \leq m < 67$, we compute c_{q_0} for each pair and check that Eq. (19) is satisfied for all but 16 pairs (q,m). We explicitly check all the remaining pairs and find that only $(23,24)$ satisfies $s = 2$. For that pair $W(q_0) = 2^2$ and it satisfies Eq. (20).

Finally, assume $q = 23$ or 25 and $s \geq 3$. It follows from Proposition 4.3 and Lemma 4.2 that, for our purposes, a sufficient condition would be $q^{m/4} > 4^{1+\frac{5m}{9}} c_{q_0}^2$. This condition holds for $q \geq 23$, $m \geq 1285$ and $c_{q_0} < 3340.6$. For the remaining cases we can use Eq. (16) 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

$$q^{m/4} > 4^{\frac{m}{3}+1} c_{q_0}^2 \left(\frac{q^3(4m-9)}{9q^3-4m} + 2 \right), \tag{21}$$

which holds for $q \geq 23$, $66 \leq m < 1285$ and $c_{q_0} < 3340.6$. From the remaining pairs, i.e. (q,m) where $q \in \{23,25\}$ and $17 \leq m < 66$, we exclude those who satisfy Eq. (21) (where c_{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 12 possible exception pairs, namely $(23,17)$, $(23,18)$, $(23,20)$, $(23,21)$, $(23,28)$, $(23,30)$, $(23,36)$, $(25,17)$, $(25,18)$, $(25,21)$, $(25,22)$ and $(25,30)$. Moreover, a computation reveals that all 12 remaining pairs 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). □

Summing up, in this section we proved the following.

Theorem 6.9 *Let $q \geq 23$ be a prime power, $m \geq 17$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, 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 $(-dx+b)/(cx-a)$ are simultaneously primitive and free over $\mathbb{F}_q$.*

Example 6.10 As a demonstration of the above, assume $q = 29$, $m = 18$ and $A = \left(\begin{smallmatrix} 1 & 4 \\ 0 & 7 \end{smallmatrix}\right)$. In that case, our aim is to find some $x \in \mathbb{F}_{29^{18}}$, such that both x and $7x-4$ are simultaneously primitive and free over $\mathbb{F}_{29}$. It is clear that $\mathbb{F}_{29^{18}} = \mathbb{Z}_{29}(\alpha)$, where α is a root of $10 + X + 15X^2 + 27X^3 + 15X^5 + 25X^6 + 23X^7 + 18X^8 + 10X^9 + 5X^{10} + 17X^{11} + 24X^{12} + 28X^{13} + 16X^{14} + 24X^{15} + 18X^{16} + 24X^{17} + X^{18}$. It is not hard to check that the set of elements satisfying these conditions include $12 + \alpha + \alpha^2$, $27 + 3\alpha + \alpha^2$, $5 + 5\alpha + \alpha^2$, $18 + 5\alpha + \alpha^2$ and $26 + 5\alpha + \alpha^2$ among others.

7 Conclusion

In this paper, an extension to Theorems 1.1 and 1.2 was considered, Problem 1.3. This was partially solved by Theorem 6.9. We also note that pursuing the problem to

a complete solution, i.e. identify exactly for which q, m and A, Problem 1.3 cannot be answered positively, although probably possible, would lead to an exhausting case-by-case approach and require heavy computer usage. In this work, we proved that Problem 1.3 can be answered positively for most A, when q and m are large enough and identified some infinite families of genuine exceptions, see Remarks 4.11, 4.14 and 4.16. We also left an infinite number of cases unresolved. In particular, we did not solve Problem 1.3 for $q \leq 19$ or $m \leq 16$, with the exception of the cases described in Remarks 4.11, 4.14 and 4.16.

Moreover, an interesting observation, thanks to Prof. Stephen D. Cohen, is that if the condition of $(-dx+b)/(cx-a)$ to be primitive was missing from Problem 1.3, then one would end up with an easier problem, which would still qualify as an extension of Theorems 1.1 and 1.2. The complete solution to the resulting problem was performed in [19].

Acknowledgements I would like to thank my supervisor, Prof. Theodoulos Garefalakis, for pointing out this problem to me and for his useful suggestions. I would also like to thank my friend Maria Chlouveraki for her comments and Prof. Stephen D. Cohen for pointing out a serious mistake in the manuscripts and for his comments. Finally, I wish to thank the anonymous reviewers for their suggestions, that vastly improved the quality of this paper. This work was supported by the University of Crete's research grant No. 3744.

References

1. Carlitz, L.: Primitive roots in finite fields. Trans. Amer. Math. Soc. **73**(3), 373–382 (1952)
2. Carlitz, L.: Some problems involving primitive roots in a finite field. Proc. Nat. Acad. Sci. U.S.A. **38**(4), 314–318 (1952)
3. Castro, F.N., Moreno, C.J.: Mixed exponential sums over finite fields. Proc. Amer. Math. Soc. **128**(9), 2529–2537 (2000)
4. Cochrane, T., Pinner, C.: Using Stepanov's method for exponential sums involving rational functions. J. Number Theory **116**(2), 270–292 (2006)
5. Cohen, S.D.: Gauss sums and a sieve for generators of Galois fields. Publ. Math. Debrecen **56**(2-3), 293–312 (2000)
6. Cohen, S.D.: Explicit theorems on generator polynomials. Finite Fields Appl. **11**(3), 337–357 (2005)
7. Cohen, S.D., Hachenberger, D.: Primitive normal bases with prescribed trace. Appl. Algebra Engrg. Comm. Comput. **9**(5), 383–403 (1999)
8. Cohen, S.D., Huczynska, S.: The primitive normal basis theorem – without a computer. J. London Math. Soc. **67**(1), 41–56 (2003)
9. Cohen, S.D., Huczynska, S.: The strong primitive normal basis theorem. Acta Arith. **143**(4), 299–332 (2010)
10. Davenport, H.: Bases for finite fields. J. London Math. Soc. **43**(1), 21–39 (1968)
11. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Information Theory **22**(6), 644–654 (1976)
12. Gao, S.: Normal basis over finite fields. Ph.D. thesis, University of Waterloo (1993)
13. Garefalakis, T.: On the action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible poynomials over $\mathbb{F}_q$. J. Pure Appl. Algebra **215**(8), 1835–1843 (2010)
14. Golomb, S.W.: Algebraic constructions of Costas arrays. J. Combin. Theory Ser. A **37**(1), 13–21 (1984)
15. Hensel, K.: Ueber die darstellung der zahlen eines gattungsbereiches für einen beliebigen primdivisor. J. Reine Angew. Math. **103**, 230–237 (1888)
16. Hsu, C., Nan, T.: A generalization of the primitive normal basis theorem. J. Number Theory **131**(1), 146–157 (2011)
17. Huczynska, S.: Existence results for finite field polynomials with specified properties. In: P. Charpin, A. Pott, A. Winterhof (eds.) Finite Fields and Their Applications: Character Sums and Polynomials, pp. 65–87. De Gruyter, Berlin Boston (2013)

18. Huczynska, S., Mullen, G.L., Panario, D., Thomson, D.: Existence and properties of k-normal elements over finite fields. Finite Fields Appl. **24**, 170–183 (2013)
19. Kapetanakis, G.: Normal bases and primitive elements over finite fields. Finite Fields Appl. **26**, 123–143 (2014)
20. Lenstra Jr, H.W., Schoof, R.J.: Primitive normal bases for finite fields. Math. Comp. **48**(177), 217–231 (1987)
21. Lidl, R., Niederreiter, H.: Finite Fields, second edn. Cambridge University Press, Cambridge (1997)
22. Perel'muter, G.I.: Estimate of a sum along an algebraic curve. Mat. Zametki **5**(3), 373–380 (1969)
23. Rosen, M.: Number Theory in Function Fields, *Grad. Texts in Math.*, vol. 210. Springer-Verlag, New York (2002)
24. Schmidt, W.M.: Equations over Finite Fields, An Elementary Approach. Springer-Verlag, Berlin Heidelberg (1976)
25. Stichtenoth, H., Topuzoğlu, A.: Factorization of a class of polynomials over finite fields. Finite Fields Appl. **18**(1), 108–122 (2012)
26. Tian, T., Qi, W.F.: Primitive normal element and its inverse in finite fields. Acta Math. Sinica (Chin. Ser.) **49**(3), 657–668 (2006)
27. Wang, P., Cao, X., Feng, R.: On the existence of some specific elements in finite fields of characteristic 2. Finite Fields Appl. **18**(4), 800–813 (2012)