Normal bases and primitive elements over finite fields

Giorgos Kapetanakis[1]

Department of Mathematics, University of Crete, Voutes Campus, 70013, Heraklion, Greece

Abstract

Let q be a prime power, $m \geq 2$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, where $A \neq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ if $q = 2$ and m is odd. We prove an extension of the primitive normal basis theorem and its strong version. Namely, we show that, except for an explicit small list of genuine exceptions, for every q, m and A, 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 $\mathbb{F}_q$.

Keywords: Primitive element, Free element, Normal basis, Character sum, Finite field
2010 MSC: 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 and by $\mathbb{F}_{q^m}$ its extension of degree m. 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*, 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*.

It is well-known that both primitive and free elements exist. The existence of elements that are simultaneously primitive and free is also known:

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.*

Lenstra and Schoof [14] were the first to provide a complete proof of the above, completing partial proofs of Carlitz [1, 2] and Davenport [10]. Later, 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, 11, 19]. Recently, an even stronger result was shown.

Email address: gkapet@math.uoc.gr (Giorgos Kapetanakis)
[1]Tel: (+30) 2810 393771, Fax: (+30) 2810 393881

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, unless the pair (q, m) is one of $(2, 3)$, $(2, 4)$, $(3, 4)$, $(4, 3)$ or $(5, 4)$.*

Tian and Qi [18] 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, 12] and the references therein, for more complete surveys of this, very active, line of research.

More recently, an extension of both theorems was considered [13]:

Theorem 1.3. *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 $\mathbb{F}_{q^m}$. There exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(ax + b)/(cx + d)$ are simultaneously primitive and free.*

Clearly, Theorems 1.1 and 1.2 are special cases of the above, for matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & a \\ a & 0 \end{smallmatrix}\right)$, where $a \neq 0$, respectively. It s clear though, that despite Theorem 1.3 being a natural extension of Theorems 1.1 and 1.2, the large number of possible exceptions leaves room for improvement. It is worth noting though, that, since the mentioned sieving techniques have been employed in this work, one would not expect much improvement. On the other hand, thanks to a notice of Stephen Cohen, if the condition of $(ax + b)/(cx + d)$ to be primitive was missing from Theorem 1.3, the resulting problem would still be an extension of Theorems 1.1 and 1.2 (to make this clear, notice that the two conditions of x and x^{-1} to be primitive in Theorem 1.2 overlap, i.e. the latter actually has three genuine conditions) and also would be of comparable complexity with Theorem 1.2, thus a pursue to a complete solution would be more realistic.

In this paper, we omit the condition of $(ax + b)/(cx + d)$ to be primitive in Theorem 1.3 and completely solve the resulting problem. In particular, we prove the following:

Theorem 1.4. *Let q be a prime power, $m \geq 2$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, where $A \neq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ 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 $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ or $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$,*
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. It is interesting to notice that, not only we have no new exceptions than those appearing in Theorem 1.2, 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 tranformations that the various A's define. Also, note that the (infinite) family $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $q = 2$ and m odd consists solely of genuine

exceptions. See the remark following Proposition 3.1 for a more detailed account of this delicate case.

This work completes [13]. It is also influenced by the work of Lenstra and Schoof [14], while a character sum estimate [3, 4, 16] plays a crucial role in our proof. Moreover, much of this paper is inspired by and follows the work of Cohen and Huczynska [8, 9], whose techniques have been adjusted.

2. Preliminaries

Let $x \in \mathbb{F}_{q^m}$ and $F = \sum_{i=0}^{n} f_i X^i \in \mathbb{F}_q[X]$. We define $F \circ x := \sum_{i=0}^{n} f_i x^{q^i}$. Under the above action, $\mathbb{F}_{q^m}$ is an $\mathbb{F}_q[X]$-module, i.e. the annihilator of x has a unique monic generator, called the *Order* of x and denoted by $\mathrm{Ord}(x)$. It is also clear that, $\mathrm{Ord}(x) \mid X^m - 1$ and that the elements that are free are exactly those of Order $X^m - 1$. Furthermore, if x is of Order G, 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*, if $x = H \circ y$ for some $y \in \mathbb{F}_{q^m}$ and $H \mid G$, 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 *d-free*, if $w \mid d$ and $x = y^w$ implies $w = 1$. Furthermore, it follows from the definitions that $q^m - 1$ and $X^m - 1$ may be freely replaced by their radicals q_0 and $F_0 := X^{m_0} - 1$ respectively, where m_0 is 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 $\mathfrak{G} \to \mathbb{C}^*$. The characters of $\mathfrak{G}$ form a group under multiplication, which is isomorphic to $\mathfrak{G}$ and denoted by $\widehat{\mathfrak{G}}$. Furthermore, the character χ_o, where $\chi_o(g) = 1$ for all $g \in \mathfrak{G}$ is the *trivial character* of $\mathfrak{G}$.

From now on, we will call the characters of $\mathbb{F}_{q^m}^*$ *multiplicative characters* and the characters of $\mathbb{F}_{q^m}$ *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

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

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 $y \in \mathbb{F}_{q^m}$, and 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 $y=1$, also known as the *canonical* character. For the above well-known facts the reader is referred to classic textbooks [15, 17].

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:

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

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

In order to define the additive analogue of ω_r, the analogues of θ, ϕ, μ and the order 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 the monic polynomial generating the annihilator of ψ in $\mathbb{F}_q[X]$ and is 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 [14], states that for $G \in \mathbb{F}_q[X]$, with $G \mid X^m-1$ we have that

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

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

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

Now, we can define the analogue of ω_r, namely for $F \mid X^m-1$, we have

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

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.

In the following sections we will encounter various character sums and a valuation, or at least an estimation, of those sums will be necessary. The following results are well-known. A proof for the first result can be found in classic textbooks [15, 17].

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*

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

The following proposition plays a crucial role in our proof.

Proposition 2.3. *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 $\bar{\mathbb{F}}_q$, 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 result was initially proved by Perel'muter [16], but Castro and Moreno [3] improved the result to its stated form. Recently, Cochrane and Pinner [4] presented a proof, which uses the elementary Stepanov-Schmidt method.

3. Some estimates

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $q_1 \mid q_0$ 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.

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 $\sum_{d|r}|\mu(d)| = W(r)$ and $\sum_{G|F}|\mu(G)| = W(F)$. 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. Clearly, our purpose is to show that $N_A(\mathbf{w}) > 0$. The proposition below is our first step towards this.

Proposition 3.1. *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 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:

$$N_A(\mathbf{k}) = \sum_x \omega_{q_1}(x)\Omega_{F_1}(x)\Omega_{F_2}((ax+b)/(cx+d)), \tag{3}$$

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

First, assume $c \neq 0$. Eq. (3) gives

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\substack{\mathbf{l}|\mathbf{k} \\ \mathbf{l}=(d_1,G_1,G_2)}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\substack{\mathrm{ord}(\chi_1)=d_1, \\ \mathrm{Ord}(\psi_1)=G_1, \\ \mathrm{Ord}(\psi_2)=G_2}} \mathcal{X}_A(\chi_1, \psi_1, \psi_2), \tag{4}$$

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 $0 \leq n_1 \leq q^m - 2$, $\mathcal{G}(X) := (y_1X(cX+d) + y_2(aX+b)/(cX+d) \in \mathbb{F}_q[X]$ 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. Proposition 2.3 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 it can be shown [13, §4.1], that $|\mathcal{X}_A(\chi_1, \psi_1, \psi_2)| \leq 2q^{m/2}$. If $\mathcal{G} = \mathcal{H}^p - \mathcal{H} + y$ for some $y \in \mathbb{F}_{q^m}$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$, it follows that, see [13, §4.1], $y_1 = y_2 = 0$ and in that case $|\mathcal{X}_A(\chi_1, \psi_1, \psi_2)| = 1$ from Lemma 2.2, if $n_1 \neq 0$. 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), implies

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

which combined with Eqs. (1) and (2), 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 $c = 0$. As before, Eq. (3) gives

$$N_A(\mathbf{k}) = \theta(\mathbf{k}) \sum_{\substack{\mathbf{l}|\mathbf{k} \\ \mathbf{l}=(d_1,G_1,G_2)}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\substack{\mathrm{ord}(\chi_1)=d_1, \\ \mathrm{Ord}(\psi_1)=G_1, \\ \mathrm{Ord}(\psi_2)=G_2}} \psi_2(b/d)\mathcal{Y}_A(\chi_1,\psi_1,\psi_2), \qquad (5)$$

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 directly from Lemma 2.2 and Proposition 2.3, that if at least one of χ_1 or (ψ_1, ψ_2') is non-trivial, then $|\mathcal{Y}_A(\chi_1,\psi_1,\psi_2)| \le q^{m/2}$. Now, Eq. (5) gives:

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

The coefficient of q^m in the above can be shown, see [13, §4.2], to be 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 $q \neq 2$. □

REMARK. 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 can be $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, hence our demand is to exists 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 1.1.

REMARK. 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 $c = 0$.

In the rest of this section, following Cohen and Huczynska [8, 9], we introduce a sieve that will help us get improved results. The propositions below are those of Cohen and Huczynska [9], 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 $\{\mathbf{k}_1, \ldots, \mathbf{k}_r\}$, 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 $\mathbf{k}_1, \ldots, \mathbf{k}_r$ are such that $\mathbf{k}_i = \mathbf{k}_0\mathbf{p}_i$, where $\mathbf{p}_1, \ldots, \mathbf{p}_r$ are distinct prime divisor 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 $\Delta := (r-1)/\delta + 2$.

Proposition 3.2 (Sieving inequality). *Let $A \in \mathrm{GL}_2(\mathbb{F}_q)$, $\mathbf{k}$ be a divisor triple 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 proof is identical to the proof of [13, Proposition 5.1], where the word "quadruple" may be replaced by the word "triple". □

Proposition 3.3. *Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $\mathbf{k}$ 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 $\mathbf{p}_1, \ldots, \mathbf{p}_r$ be the primes of the $(\mathbf{k}_0, r)$-decomposition. Proposition 3.2 implies

$$N_A(\mathbf{k}) \geq \delta N_A(\mathbf{k}_0) + \sum_{i=1}^{r} \left(N_A(\mathbf{k}_0\mathbf{p}_i) - \left(1 - \frac{1}{|\mathbf{p}_i|}\right) N_A(\mathbf{k}_0) \right). \tag{6}$$

Suppose $c \neq 0$. Taking into account the analysis done in the corresponding part of the proof of Proposition 3.1, Eq. (6) implies

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

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 3.1, Eq. (6) imples

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

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 $q \geq 3$. □

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 $\phi(d)/s_d$ 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 the above, the reader is referred to [15, §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 will prove to be useful.

Proposition 3.4. *Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $(q, c) \neq (2, 0)$, $\{l_1, \dots l_t\}$ 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*

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

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 3.3 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

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

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

Before continuing further, we focus on the delicate case $m = 2$. Although Proposition 3.4 holds in that case as well, much weaker conditions for $N_A(\mathbf{w}) > 0$ can be achieved. Moreover, the fact that this case is absent in related previous works [8, 9] 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

$$N_A(q_1, F_1) := \sum_x \omega_{q_1}(x) \Omega_{F_1}((ax+b)/(cx+d)), \tag{7}$$

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 3.5. *Suppose $m = 2$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $q_1 \mid q_0$ 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 3.1, first assume that $c \neq 0$. Eq. (7) implies

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

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 3.1, we use Proposition 2.3 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. (7) yields

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

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 Proposition 2.3 imply $|\mathcal{W}_A(\chi_1, \psi_1)| \leq q$, unless both χ_1 and ψ_1 are trivial. t 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. □

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 3.2, 3.3 and 3.4 in this case are straightforward. We state the analogue of Proposition 3.4.

Proposition 3.6. *Suppose $m = 2$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, $(q, c) \neq (2, 0)$, $\{l_1, \dots l_t\}$ 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 $N_A(\mathbf{w}) > 0$, provided that the above denominator is positive.

In the proceeding section, an estimation for $W(q_0)$ will be necessary. The lemma below provides us with one, while its proof is immediate using multiplicativity.

Lemma 3.7. *For any $r \in \mathbb{N}$, $W(r) \leq c_r r^{1/4}$, where $c_r = 2^s/(p_1 \cdots p_s)^{1/4}$ and $p_1, \dots, p_s$ are the primes ≤ 16 that divide r, whilst for all $r \in \mathbb{N}$, $c_r < 4.9$. Moreover, $W(r) \leq d_r r^{1/8}$, where $d_r = 2^t/(p_1 \cdots p_t)^{1/8}$ and $p_1, \dots, p_t$ are the primes $\leq 2^8$ that divide r, while for all $r \in \mathbb{N}$, $d_r < 4514.7$.*

REMARK. The lemma above provides us a universal estimate for the numbers c_r and d_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. In the proceeding section c_r is replaced by 4.9, a (smaller) estimate or by its exact value.

4. Evaluations

Proposition 3.4 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 MAPLE (v. 13). Moreover, in this section we assume that $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$ and $(q, c) \neq (2, 0)$. The lemma below (analogue to [9, Lemma 2.5]) will prove to be useful.

Lemma 4.1. *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 $x = y^{q^2} + y$, i.e. $x = x^{q^2}$, 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. □

Proposition 4.2. *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 1.*

PROOF. It follows from Proposition 3.1 and Lemma 3.7, that $N_A(\mathbf{w}) > 0$, if

$$q^{m/4} > 3c_{q_0}4^{m_0}. \tag{8}$$

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

For $m = 11$, we have $m_0 = 1$ and $c_{q_0} < 4.5$, i.e. Eq. (8) holds for $q \geq 5$. If $m = 10$, then $m_0 = 2$ and $c_{q_0} < 3.7$ and Eq. (8) 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. (8) 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. (8) holds for $q \geq 29$, or 3, in which case $c_{q_0} < 2.9$ and Eq. (8) holds for $q \geq 68$. If $m = 5$, then $m_0 = 1$, $c_{q_0} < 3.7$ and Eq. (8) 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. (8) holds for $q \geq 35$, or 4, in which case, accounting Lemma 4.1, we may assume that $m_0 = 2$ and $c_{q_0} < 4.9$, i.e. Eq. (8) is satisfied for $q \geq 235$. Finally, if $m = 3$, thanks to Lemma 4.1 we can assume that $m_0 = 1$ and $c_{q_0} < 3.2$, hence Eq. (8) holds for $q \geq 130$.

Summing up, we end up with 83 remaining pairs (q, m). A computation shows that all but 31 of them satisfy $q^{m/2} > 3W(q_0)4^{m_0}$, where $W(q_0)$ is explicitly computed for each pair. Another sufficient condition, according to Proposition 3.3, for our purposes, would be

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

where $\{l_1, \ldots, l_t\}$ are distinct primes dividing q_0 and $\delta := 1 - \sum_{i=1}^{t} 1/l_i$ should be > 0. This is satisfied when (q, m) is $(47, 4)$ and $\{13, 17, 23\}$ is our set, $(43, 4)$ and $\{7, 11, 37\}$, $(31, 4)$ and $\{5, 13, 37\}$, $(29, 3)$ and $\{13, 67\}$, $(27, 4)$ or $(9, 6)$ and $\{5, 7, 13, 73\}$, and, finally, $(16, 6)$ or $(4, 12)$ for $\{5, 7, 13, 17, 241\}$. The remaining pairs are listed in Table 1. □

Proposition 4.3. *If $m_0 = q - 1$ and $m > 2$, then $N_A(\mathbf{w}) > 0$ for all (q, m) not listed in Table 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 3.3 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 3 \cdot 2^{q-1}((q-1)^2 + 1)W(q_0). \tag{9}$$

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 3.3 yields that if Eq. (9) holds, then $N_A(\mathbf{w}) > 0$, in that case as well. With the help of Lemma 3.7, Eq. (9) may be replaced by

$$q^{m/4} > 3 \cdot 4.9 \cdot 2^{q-1}((q-1)^2 + 1). \tag{10}$$

First of all we can restrict ourselves to pairs (q, m) with $q > 3$, since those cases have already been investigated in Proposition 4.2. Afterwards, we easily check that Eq. (10) holds for $q \geq 43$ and $m \geq m_0$. If $m \geq 2m_0$ then Eq. (10) is satisfied for any $q \geq 14$. If $m \geq 3m_0$, then Eq. (10) is satisfied for $q \geq 9$. If $m \geq 4m_0$, then Eq. (10) holds for $q \geq 7$. For $m \geq 5m_0$, Eq. (10) is true for $q \geq 6$ and if $m \geq 8m_0$, then Eq. (10) holds for any $q \geq 4$.

Summing up, we end up with 22 pairs (q, m), not shown to satisfy Eq. (10) yet, but 12 of them satisfy Eq. (9), if each appearing quantity is computed explicitly. From the 10 remaining pairs, we can exclude $(4, 6)$ and $(4, 12)$, who have already been investigated in Proposition 4.2. The remaining 8 pairs are listed in Table 1. □

Proposition 4.4. *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 1.*

Proof. In our case, $G_0 = F_0$ and $s = 1$ and it is clear that the denominator of the inequality in Proposition 3.4 is positive, since $m_0 \leq (q-1)/2$. It follows that $N_A(\mathbf{w}) > 0$ if

$$q^{m/2} > 3W(q_0)\left(\frac{q(2m_0-1)}{q-2m_0}+2\right). \tag{11}$$

Lemma 3.7 implies that another sufficient condition for our purposes would be

$$q^{m/4} > 3 \cdot 4.9\left(\frac{q(2m_0-1)}{q-2m_0}+2\right). \tag{12}$$

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. (12) 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 $m_0 = 9$ 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. (12) is true for $q \geq 66$. If $m = 2m_0$ and $m_0 = 5$, then Eq. (12) 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. (12) 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 4.2.

Summing up, we end up with a set of 89 pairs (q, m), not yet shown to satisfy Eq. (12), but an exact computation reveals that only 20 of them fail to satisfy Eq. (11). Moreover, the pair $(121, 3)$ satisfies the demands of Proposition 3.4, 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 1. □

Next, we focus on the case $m_0 > 4$ 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. Furthermore, Proposition 3.4 implies that $N_A(\mathbf{w}) > 0$, if

$$q^{m/2} > 3 \cdot 4^{\rho m_0} W(q_0)\left(\frac{2q^s(1-\rho)m_0 - sq^s}{sq^s - 2(1-\rho)m_0}+2\right), \tag{13}$$

since $t_{F_0/G_0} \leq r_0$ and $\rho m_0 = t_{F_0/G_0}$ .The lemma below, proven in [8], provides us an estimation of ρ, for $q > 4$.

Lemma 4.5. *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 4.6. *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 1.*

Proof. According to Lemma 4.5, ρ may be $1/2$, $3/8$ or $13/36$. First, assume $\rho = 1/2$. With the help of Lemma 4.5, Eq. (13) gives 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 3.7. If $m = m_0$, it is satisfied for $m \geq 8$ and $q \geq 1863$ and for $m \geq 33$ and $q \geq 38$, 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 61 fail to satisfy

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

another condition deriving from Lemma 4.5 and Eq. (13), for $W(q_0) \leq 4.9q^{m/4}$. From those pairs, all but four satisfy this inequality, if $W(q_0)$ is computed explicitly. These pairs are $(5, 8)$, $(7, 12)$, $(9, 16)$ and $(13, 8)$, 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 3.7 and 4.5, Eq. (13) gives another condition for $N_A(\mathbf{w}) > 0$, namely

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

This inequality is always true for $m > m_0$. If $m = m_0$, then this inequality holds, for $m \geq 16$ and $q \geq 28$, $m \geq 32$ and $q \geq 10$ and for $m \geq 48$ and $q \geq 8$. After taking into account the implied restrictions from Lemma 4.5, it follows that the possible exception pairs are $(9, 32)$ and $(q, 16)$, with $5 \leq q \leq 25$. In this region, there are only three pairs satisfying $m = m_0 = 4\gcd(m, q-1)$, but only $(5, 16)$ fails to satisfy

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

another condition deriving from Lemma 4.5 and Eq. (13).

Finally, assume $\rho = 13/36$. With the help of Lemma 4.5, Eq. (13) 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 $q \geq 6$, for $W(q_0) < 4514.7q^{m/8}$. It follows from Lemmas 3.7 and 4.5, that the only possible exception pair is $(7, 36)$, which satisfies the above inequality, if $W(q_0)$ is exactly computed. □

Proposition 4.7. *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 1.*

Proof. We begin with the case $m_0 \geq 8$. In that case, see [9, 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. (13) 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. (13) implies that if

$$q^{m/2} > 3W(q_0)4^{m_0/3}(2m_0 - 1), \tag{14}$$

then $N_A(\mathbf{w}) > 0$. With the help of Lemma 3.7, 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 80 do not satisfy Eq. (14), for $W(q_0) < 4.9q^{m/4}$ and just 5 who fail to satisfy Eq. (14), if we compute $W(q_0)$ explicitly. A computation reveals that all 5 pairs satisfy Eq. (13), 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 3.1 and Lemma 3.7, 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 $(5, 6)$, $(7, 4)$ and $(11, 6)$, fail to satisfy Eq. (13), with all appearing quantities computed explicitly. Finally, it turns out that we can exclude $(11, 6)$ from our list, since we can successfully apply multiplicative sieving on this pair, with $\{37, 19, 7, 5\}$ as our set of sieving primes. □

Our next aim is to prove our result when $2 \leq q \leq 4$ and $m_0 \geq 4$. The lemma below, proven in [8], is very useful towards that proof.

Lemma 4.8. *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 4.9. *If $m_0 > 4$, $s \neq 1$ and $q < 5$, then $N_A(\mathbf{w}) > 0$, unless (q, m) is listed in Table 1.*

Proof. First, assume $q = 4$. Lemma 4.8 implies that if $m > 45$, then $\rho \leq 1/5$. Moreover, Proposition 3.1 and Lemma 3.7 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 $m \geq 4m_0$, thus we can focus on the cases $m \leq 45$ and $m_0 \leq m \leq 2m_0$. Working as in the proof of Proposition 4.7, we show that if

$$q^{3m/8} > 3 \cdot 4514.7 \cdot 4^{m_0/5}(4m_0 - 3),$$

then $N_A(\mathbf{w}) > 0$. This condition is satisfied for $m_0 \geq 62$, if $m = m_0$ and for $m_0 \geq 19$, if $m = 2m_0$. Now we can focus on $m \leq 61$. A quick computation reveals that there are 50 pairs $(4, m)$ not examined in previous propositions for those values of m, but only $(4, 5)$ fails to satisfy Eq. (13), if we compute all appearing quantities.

Next, assume $q = 3$. If $m > 16$, 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 $m \leq 16$ and $m_0 \leq m \leq 3m_0$. As in the previous case, we have that $N_A(\mathbf{w}) > 0$, if

$$q^{3m/8} > 3 \cdot 4514.7 \cdot 4^{m_0/4}(3m_0 - 2).$$

This is true for $m_0 \geq 247$, if $m = m_0$ and $m_0 \geq 15$, if $m = 3m_0$. A quick computation reveals that there exist 231 pairs $(3, m)$ not settled yet. Among those pairs, there are exactly 6 who fail to satisfy Eq. (13), for $W(q_0) < 3.2q^{m/4}$, but only $(3, 5)$ and $(3, 7)$ fail to satisfy Eq. (13), if $W(q_0)$ is computed explicitly.

Finally, assume $q = 2$. If $m > 21$, 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 $m \leq 21$ and $m_0 \leq m \leq 4m_0$. As in the previous cases, we have that $N_A(\mathbf{w}) > 0$, if

$$q^{3m/8} > 3 \cdot 4514.7 \cdot 4^{m_0/6}(5m_0 - 4).$$

This inequality holds for $m_0 \geq 607$ if $m = m_0$, for $m_0 \geq 53$ if $m = 2m_0$ and for $m_0 \geq 18$ if $m = 4m_0$. Another computation reveals that there are 588 pairs $(2, m)$ not settled yet, all of which satisfy Eq. (13), with the simple bound $W(q_0) < 2.9q^{m/4}$. □

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

Proposition 4.10. *Suppose $m = 2$. If (q, m) is not listed in Table 1, then $N_A(\mathbf{w}) > 0$.*

Table 1: Possible exceptions (q, m) from Section 4.

Proposition	Possible exception pairs (q, m)	#
4.2	$(2,3)$, $(2,4)$, $(2,6)$, $(2,8)$, $(2,12)$, $(3,3)$, $(3,4)$, $(3,6)$, $(3,12)$, $(4,4)$, $(4,6)$, $(5,3)$, $(5,5)$, $(7,4)$, $(8,3)$, $(8,4)$, $(8,6)$, $(9,3)$, $(11,3)$, $(11,4)$, $(19,4)$, $(23,3)$, $(23,4)$	23
4.3	$(4,3)$, $(5,4)$, $(7,6)$, $(8,7)$, $(9,8)$, $(11,10)$, $(13,12)$, $(16,15)$	8
4.4	$(7,3)$, $(9,4)$, $(11,5)$, $(13,3)$, $(13,4)$, $(13,6)$, $(16,3)$, $(17,4)$, $(19,3)$, $(25,3)$	10
4.6	$(5,8)$, $(7,12)$, $(13,8)$, $(5,16)$	4
4.7	$(5,6)$, $(7,5)$	2
4.9	$(4,5)$, $(3,5)$, $(3,7)$	3
4.10	$(2,2)$, $(3,2)$, $(4,2)$, $(5,2)$, $(7,2)$, $(11,2)$	6
	Total:	56

PROOF. Proposition 3.6 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 3.7. From the 34 remaining pairs, only 10 fail to 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 1. □

Summing up, in this section we proved the following.

Theorem 4.11. *Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$. If $q \neq 2$ or $A \neq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, 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 56 pairs listed in Table 1.*

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 C, using Victor Shoup's NTL library. All pairs (q, m) appearing in Table 1 were dealt with fairly quickly. In this section, $A \circ x$ stands for $(ax + b)/(cx + d)$, where $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$ and $x \in \mathbb{F}_{q^m}$.

Our first and simplest case is $q = 2$, see Table 2. Here, only three matrices had to be investigated, namely $A_0 := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $A_1 := \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $A_2 := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. In Table 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 2, we see that when $q = 2$, the only exceptions are $m = 3$ and $m = 4$, the exceptions already present in Theorem 1.2.

Next, in Tables 3 and 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 1.1 and 1.2 respectively.

Table 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	$1 + X + X^2$	β for $i = 0, 1, 2$
3	$1 + X + X^3$	$1 + \beta$ for $i = 0, 2$; None for $i = 1$
4	$1 + X + X^4$	None for $i = 0$; $1 + \beta^3$ for $i = 1, 2$
6	$1 + X + X^6$	β^5 for $i = 0$; $1 + \beta^5$ for $i = 1, 2$
8	$1 + X + X^3 + X^4 + X^8$	$1 + \beta^5$ for $i = 0, 1, 2$
12	$1 + X^3 + X^{12}$	$\beta+\beta^2+\beta^3+\beta^9$ for $i = 0$; $1+\beta+\beta^9$ for $i = 1, 2$

Table 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	$2 + X + X^2$	β (6); $1 + \beta$ (4)
	3	$2 + 2X + 2X^2 + X^3$	$1 + \beta$ (7); $2 + \beta$ (3)
	4	$2+2X+X^2+X^3+X^4$	$2 + 2\beta + \beta^2$ (3); $1 + \beta + 2\beta^2$ (1); β (3); 2β (3)
	5	$1 + X^2 + 2X^3 + X^5$	$1 + 2\beta$ (6); $2 + 2\beta$ (3); $\beta + \beta^2$ (1)
	6	$1+2X+2X^2+2X^3+$ $2X^4 + X^5 + X^6$	$2\beta + \beta^2$ (3); $2 + \beta + \beta^2$ (7)
	7	$1 + X + 2X^2 + X^4 +$ $X^5 + X^6 + X^7$	β (6); $1 + 2\beta$ (3); $\beta + \beta^2$ (1)
	12	$1 + 2X + X^2 + 2X^4 +$ $X^9 + 2X^{10} + X^{12}$	$2 + \beta + \beta^5$ (5); $1 + 2\beta + \beta^5$ (5)
5	2	$4 + 3X + X^2$	$1 + \beta$ (22); $2 + \beta$ (6)
	3	$1 + 3X + X^2 + X^3$	$1 + \beta$ (22); $2 + \beta$ (5); $1 + 2\beta$ (1)
	4	$4 + 3X + X^2 + 2X^3 +$ X^4	$4 + 2\beta$ (7); $2 + \beta$ (15); $1 + 3\beta$ (2); None (4)
	5	$1+2X+4X^2+3X^3+$ $2X^4 + X^5$	$4 + \beta$ (23); $1 + 2\beta$ (5)
	6	$3 + 2X + X^3 + 3X^4 +$ $2X^5 + X^6$	$4 + 2\beta + \beta^2$ (18); $3\beta + \beta^2$ (4); $2 + 3\beta + \beta^2$ (5); $4 + \beta + 2\beta^2$ (1)
	8	$3+2X+3X^3+2X^4+$ $3X^5 + 4X^6 + X^8$	$3 + 2\beta$ (7); $2 + 3\beta$ (2); $4 + \beta$ (15); $4 + \beta^3$ (4)
	16	$1+2X+3X^4+X^5+$ $3X^6 + 3X^8 + 3X^9 +$ $X^{10} + 3X^{11} + X^{12} +$ $4X^{13}+4X^{14}+2X^{15}+$ X^{16}	$4 + 3\beta + \beta^3$ (3); $3\beta + \beta^3$ (10); $1 + 3\beta + \beta^3$(8); $4 + 2\beta + \beta^3$ (7)

Table 4: q is an odd 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	$4 + X + X^2$	$3 + \beta$ (46); $5 + \beta$ (8)
	3	$6 + 5X^2 + X^3$	$2 + \beta$ (34); $4 + 2\beta$ (15); $3 + 3\beta$ (2); $2 + 3\beta$ (2); $4 + 3\beta$ (1)
	4	$3 + X^2 + 4X^3 + X^4$	β (35); $4 + \beta$ (4); $2 + \beta$ (14); $1 + 2\beta$ (1)
	5	$4 + X + 3X^2 + 2X^3 + 5X^4 + X^5$	β (46); $2 + \beta$ (7); $6 + \beta$ (1)
	6	$6 + 2X + 4X^3 + 5X^4 + X^6$	$6 + \beta + \beta^2$ (17); $3 + 4\beta + \beta^2$ (10); $5 + 4\beta + \beta^2$ (2); $1 + 4\beta + \beta^2$ (25)
	12	$3 + 6X + X^2 + 5X^3 + 4X^5 + 3X^7 + 2X^8 + 3X^9 + 2X^{10} + X^{11} + X^{12}$	$1 + 6\beta + \beta^2$ (7); $4 + 3\beta + 3\beta^2$ (1); $6 + 2\beta + 2\beta^2$ (7); $6 + \beta + \beta^2$ (14); $3 + \beta + \beta^2$ (22); $5 + 2\beta + 2\beta^2$ (1); $3 + 5\beta + 2\beta^2$ (1); $5 + 6\beta + \beta^2$ (1)
11	2	$7 + 4X + X^2$	β (118); $4 + \beta$ (12)
	3	$10 + 2X + X^2 + X^3$	$6 + \beta$ (118); $2 + 2\beta$ (2); $10 + \beta$ (10)
	4	$5 + 7X + 4X^2 + 2X^3 + X^4$	$2 + \beta$ (118); $4 + 2\beta$ (12)
	5	$8 + 9X + 8X^2 + 6X^3 + 2X^4 + X^5$	$5 + \beta + \beta^2$ (13); $6 + \beta + \beta^2$ (3); $1 + \beta + \beta^2$ (78); $4 + \beta + \beta^2$ (35); $7 + \beta + \beta^2$ (1)
	10	$9 + 8X + 9X^2 + 7X^3 + 4X^4 + 7X^5 + 7X^6 + 2X^7 + X^8 + 8X^9 + X^{10}$	$4 + \beta + \beta^2$ (11); $4 + 3\beta + \beta^2$ (1); $1 + \beta^2$ (48); $9 + \beta + \beta^2$ (2); $6 + \beta + \beta^2$ (21); $7 + \beta + \beta^2$ (1); $4 + \beta^2$ (32); $9 + \beta^2$ (13); $2 + 3\beta + \beta^2$ (1)
13	3	$3 + X + 6X^2 + X^3$	$1 + \beta$ (142); $9 + \beta$ (33); $11 + \beta$ (4); $12 + \beta$ (1)
	4	$4 + 8X + 7X^2 + 9X^3 + X^4$	$6 + \beta$ (33); $4 + \beta$ (142); $11 + \beta$ (5)
	6	$10 + 11X + X^2 + 3X^3 + X^4 + 3X^5 + X^6$	$4 + 2\beta + \beta^2$ (119); $8 + 2\beta + \beta^2$ (43); $4 + 3\beta + \beta^2$ (14); $8 + 3\beta + \beta^2$ (2); $8 + 5\beta + \beta^2$ (1); $5 + 5\beta + \beta^2$ (1)
	8	$6 + 8X + 7X^2 + 2X^3 + 12X^4 + 2X^5 + 4X^6 + 2X^7 + X^8$	$4 + \beta$ (33); β (130); $5 + 2\beta$ (13); $8 + 2\beta$ (1); 2β (3)
	12	$4 + 11X + 3X^2 + 8X^3 + 7X^4 + 3X^5 + 2X^6 + 3X^7 + 9X^8 + 9X^9 + 3X^{10} + 10X^{11} + X^{12}$	$5 + \beta + \beta^2$ (94); $8 + 3\beta + \beta^2$ (2); $2 + 2\beta + \beta^2$ (2); $7 + \beta + \beta^2$ (41); $9 + \beta + \beta^2$ (27); $4 + 3\beta + \beta^2$ (1); $4 + 2\beta + \beta^2$ (1); $7 + 2\beta + \beta^2$ (12)
17	4	$4 + 12X + 5X^2 + X^4$	$5 + \beta$ (58); $10 + \beta$ (22); $4 + \beta$ (222); $13 + \beta$ (2)
19	3	$5 + 3X + 4X^2 + X^3$	β (322); $1 + \beta$ (51); $3 + \beta$ (5)
	4	$3 + 6X + 10X^2 + X^4$	$4 + \beta$ (358); $7 + \beta$ (20)
23	3	$1 + 4X + 7X^2 + X^3$	$1 + \beta$ (526); $2 + \beta$ (23); $3 + \beta$ (1)
	4	$13 + 8X + 18X^2 + 8X^3 + X^4$	$6 + \beta^2$ (482); $7 + \beta^2$ (63); $17 + \beta^2$ (4); $18 + \beta^2$ (1)

Table 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	$1+X+X^2$	2	$\alpha+\alpha X+X^2$	β (18)
		3	$1+\alpha+X^3$	$1+\alpha+\beta+\beta^2$ (3); $1+\beta+\beta^2$ (8); $\alpha+\alpha\beta+\beta^2$ (3); $1+\alpha+\alpha\beta+\beta^2$ (1); None (3)
		4	$\alpha+X+(1+\alpha)X^3+X^4$	β (14); $\alpha\beta$ (4)
		5	$1+\alpha X^3+X^4+X^5$	$\alpha+\beta$ (10); $1+\alpha+\beta$ (6); $\alpha\beta$ (1); $1+\beta+\beta^2$ (1)
		6	$\alpha+X+\alpha X^2+X^3+\alpha X^4+X^5+X^6$	$1+\beta^3$ (14); $1+\alpha+(1+\alpha)\beta+\beta^3$ (4)
8	$1+X+X^3$	3	$\alpha^2+(1+\alpha^2)X+(\alpha+\alpha^2)X^2+X^3$	$1+\beta$ (9); β (61)
		4	$\alpha^2+\alpha X+(1+\alpha+\alpha^2)X^2+X^3+X^4$	$1+\alpha+\beta$ (62); $\alpha^2+\beta$ (8)
		6	$\alpha+(1+\alpha+\alpha^2)X+(1+\alpha^2)X^2+(1+\alpha)X^3+(\alpha+\alpha^2)X^4+\alpha X^5+X^6$	$\alpha+\beta^3$ (70)
		7	$1+X+(1+\alpha^2)X^2+\alpha X^3+\alpha X^4+\alpha^2X^5+\alpha^2X^6+X^7$	$1+\beta+\beta^2$ (40); $1+\alpha+\beta+\beta^2$ (24); $1+\alpha^2+\beta+\beta^2$ (1); $\alpha+\alpha^2+\beta+\beta^2$ (1); $\alpha^2+\beta+\beta^2$ (4)
9	$2+X+X^2$	3	$2+2\alpha+2\alpha X^2+X^3$	β (80); $1+\beta$ (8)
		4	$2+\alpha+\alpha X+(1+\alpha)X^2+\alpha X^3+X^4$	β^2 (62); $2+\beta^2$ (22); $\alpha+\beta^2$ (4)
		8	$2+(1+\alpha)X+(2+2\alpha)X^2+(2+2\alpha)X^3+(1+\alpha)X^5+2X^6+(2+\alpha)X^7+X^8$	$1+\beta$ (27); $\alpha+\beta$ (2); $2+\beta$ (12); β (46); $1+\alpha+\beta$ (1)
16	$1+X+X^4$	3	$1+\alpha+\alpha^3+(1+\alpha^2+\alpha^3)X+X^2+X^3$	β (223); $\alpha+\beta$ (41); $\alpha+\alpha^2+\beta$ (4); $1\alpha+\beta$ (2)
		15	$(\alpha+\alpha^2+\alpha^3)+(1+\alpha+\alpha^2+\alpha^3)X+(1+\alpha+\alpha^2+\alpha^3)X^2+(\alpha+\alpha^2)X^3+(1+\alpha^2)X^4+(1+\alpha+\alpha^2+\alpha^3)X^5+(\alpha+\alpha^2)X^6+\alpha^3X^7+(\alpha^2+\alpha^3)X^8+(\alpha+\alpha^2)X^9+(1+\alpha^3)X^{10}+(1+\alpha+\alpha^2)X^{11}+(1+\alpha+\alpha^2+\alpha^3)X^{12}+(\alpha+\alpha^2)X^{13}+(\alpha+\alpha^2+\alpha^3)X^{14}+X^{15}$	$\alpha+\beta^3$ (103); $\alpha+\alpha^3+\beta^3$ (62); $1+\alpha^2+\alpha^3+\beta^3$ (4); $1+\alpha+(1+\alpha^2)\beta+\beta^3$ (15); $1+\alpha+(1+\alpha+\alpha^2)\beta+\beta^3$ (1); $1+\alpha^2+\alpha^3+\alpha\beta+\beta^3$ (1); $\alpha+\alpha^2+\beta^3$ (63); $1+\alpha^3+\alpha\beta+\beta^3$ (1); $1+\alpha+\alpha^2+\alpha\beta+\beta^3$ (2); $\alpha^3+\alpha\beta+\beta^3$ (3); $\alpha+\alpha\beta+\beta^3$ (15)
25	$4+3X+X^2$	3	$\alpha+(2+4\alpha)X+(4+4\alpha)X^2+X^3$	β (574); $1+\beta$ (68); $2+\beta$ (6)

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 $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, where either $d = b = 1$ and $c, a \neq 0$, $d = 0 \neq a$ 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 $A \in \mathrm{GL}_2(\mathbb{F}_q)$ we investigated and found $A \circ x$ to be free. An interesting notice in Table 3 is that, not only we have no new exceptions, than those of Theorem 1.2, 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 $\left(\begin{smallmatrix} a & 1 \\ 1 & 0 \end{smallmatrix}\right)$, where $a \neq 0$. It follows that $(5, 4)$ is an exception for all $A = \left(\begin{smallmatrix} a & b \\ c & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_5)$.

Finally, in Table 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 1.2, yields exceptions, for the 3 matrices $\left(\begin{smallmatrix} a & 1 \\ 1 & 0 \end{smallmatrix}\right)$, where $a \neq 0$, hence $(4, 3)$ is an exception for all $A = \left(\begin{smallmatrix} a & b \\ c & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_4)$.

The proof of Theorem 1.4 is now complete.

Acknowledgements

I would like to thank my supervisor, Prof. Theodoulos Garefalakis for his encouragment and support and the anonymous referee for her/his useful corrections and improvements to the original manuscript. This work was funded by the University of Crete's research grant No. 3744.

References

[1] L. Carlitz. Primitive roots in finite fields. *Trans. Amer. Math. Soc.*, 73(3):373–382, 1952.

[2] L. Carlitz. Some problems involving primitive roots in a finite field. *Proc. Nat. Acad. Sci. U.S.A.*, 38(4):314–318, 1952.

[3] F. N. Castro and C. J. Moreno. Mixed exponential sums over finite fields. *Proc. Amer. Math. Soc.*, 128(9):2529–2537, 2000.

[4] T. Cochrane and C. Pinner. Using Stepanov's method for exponential sums involving rational functions. *J. Number Theory*, 116(2):270–292, 2006.

[5] S. D. Cohen. Gauss sums and a sieve for generators of Galois fields. *Publ. Math. Debrecen*, 56(2-3):293–312, 2000.

[6] S. D. Cohen. Explicit theorems on generator polynomials. *Finite Fields Appl.*, 11(3):337–357, 2005.

[7] S. D. Cohen and D. Hachenberger. Primitive normal bases with prescribed trace. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):383–403, 1999.

[8] S. D. Cohen and S. Huczynska. The primitive normal basis theorem – without a computer. *J. London Math. Soc.*, 67(1):41–56, 2003.

[9] S. D. Cohen and S. Huczynska. The strong primitive normal basis theorem. *Acta Arith.*, 143(4):299–332, 2010.

[10] H. Davenport. Bases for finite fields. *J. London Math. Soc.*, 43(1):21–39, 1968.

[11] C. Hsu and T. Nan. A generalization of the primitive normal basis theorem. *J. Number Theory*, 131(1):146–157, 2011.

[12] 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, 2013.

[13] G. Kapetanakis. An extension of the (strong) primitive normal basis theorem. Submitted.

[14] H. W. Lenstra, Jr and R. J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.

[15] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, second edition, 1997.

[16] G. I. Perel'muter. Estimate of a sum along an algebraic curve. *Mat. Zametki*, 5(3):373–380, 1969.

[17] W. M. Schmidt. *Equations over Finite Fields, An Elementary Approach.* Springer-Verlag, Berlin Heidelberg, 1976.

[18] 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.

[19] 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.