University of Crete
School of Sciences and Engineering
Dept. of Mathematics and Applied Mathematics

Polynomials with special properties over finite fields

Giorgos Kapetanakis

Supervisor: Theodoulos Garefalakis

Tuesday June 2, 2015

Here, $\mathbb{F}_q$ will stand for the finite field of q elements and $\mathbb{F}_{q^m}$ for its extension of degree m. Our purpose is to prove some existence results for irreducible polynomials over finite fields, with special properties. These properties include combinations of

- primitiveness,
- freeness (a root of the polynomial forms a normal basis) and
- having some coefficients prescribed.

The main idea behind our techniques dates back to the 50's and the work of Carlitz and remains popular among authors. Roughly, our method is:

1. We express the characteristic or a characteristic-like function for a polynomial (or its roots) with the desired properties with help of characters,
2. this leads us to a sufficient condition for the existence of our desired polynomial.
3. With the the help of characters sum estimates, we end up with asymptotic results, for the existence of the elements we seek.
4. If necessary and desirable, we deal with the remaining cases with a case-by-case approach.

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

Definition

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

A character or exponential sum is a sum that involves characters.

The simplest, albeit very important, form of character sum is the following.

Lemma (Orthogonality relations)

Let χ be a non-trivial character of a group $\mathfrak{G}$ and g a non-trivial element of $\mathfrak{G}$. Then

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

- The orthogonality relations are true for arbitrary group $\mathfrak{G}$.

Definition

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

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

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

- Dirichlet characters are originally defined over $\mathbb{Z}$,
- Dirichlet characters modulo F are essentially the characters of $(\mathbb{F}_q[X]/F\mathbb{F}_q[X])^*$, extended to zero.

For χ a Dirichlet character modulo $M \in \mathbb{F}_q[X]$ and $n \in \mathbb{N}$ set

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

In particular the logarithmic derivative of the Dirichlet L-function of χ (multiplied by u) is $\sum_{n=0}^{\infty} c_n(\chi) u^n$. It follows from a famous result of Weil (1948) that:

Theorem (Weil)

Let χ be a Dirichlet character modulo M. Then

1. *If $\chi \neq \chi_o$ then*
$$|c_n(\chi)| \leq (\deg(M) - 1) q^{\frac{n}{2}}.$$
2. *If $\chi \neq \chi_o$ and $\chi(\mathbb{F}_q^*) = 1$, then*
$$|1 + c_n(\chi)| \leq (\deg(M) - 2) q^{\frac{n}{2}}.$$

We will also use the following result.

Theorem (Garefalakis)

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

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

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

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

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

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

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

It follows directly from the definition of Λ, that

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

Combining all of the above, we prove:

Proposition

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

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

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

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

- We will call the characters of $\mathbb{F}_{q^m}^*$ multiplicative characters and the characters of $\mathbb{F}_{q^m}$ additive characters. We will denote by χ_0 and ψ_0 the trivial multiplicative and additive character respectively.
- We denote a generator of $\widehat{\mathbb{F}_{q^m}^*}$ by χ_g and call it a generator character. It follows that every non-trivial multiplicative character χ satisfies $\chi(x) = \chi_g(x^n)$ for some n.
- Similarly, the canonical character is the mapping $\psi_g(x) = \exp(2\pi i \mathrm{Tr}(x)/p)$, where Tr stands for the absolute trace function from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_p$. It is well-known that the additive characters are the functions $\psi(x) = \psi_g(yx)$, for some $y \in \mathbb{F}_{q^m}$.

We will use additive and multiplicative characters to express the characteristic functions of the properties we are interested in. Consequently, character sums of those types will emerge and computations, or estimates of those will be crucial. The following results provides us such estimates.

The following were originally proved by Weil (1948). Stepanov (1969) and Schmidt (1976) developed an elementary method for those proofs, known as the Stepanov-Schmidt method.

Theorem

Let χ be a non-trivial multiplicative character of order n, and $F \in \mathbb{F}_{q^m}[X]$, with l distinct roots (in its splitting field), such that $F \neq yH^{q^m-1}$, then

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

Lemma (Kloosterman sums)

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

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

Theorem

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 $\mathcal{F} \neq y\mathcal{H}^n$ and $\mathcal{H} \in \mathbb{F}_{q^m}(X)$, and $\mathcal{G} \neq \mathcal{H}^p - \mathcal{H} + y$. 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 theorem was initially proved by Perel'muter (1969). Castro and Moreno (2000) improved the result to its stated form. Cochraine and Pinner (2006) presented a proof with the elementary Stepanov-Schmidt method.

Part I: The Hansen-Mullen conjecture for self-reciprocal irreducible polynomials

This work is joint work with Theodoulos Garefalakis and published:

T. Garefalakis and G. Kapetanakis.
On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials.
Finite Fields Appl., 18(4):832–841, 2012.

T. Garefalakis and G. Kapetanakis.
A note on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials.
Finite Fields Appl., 35(C):61–63, 2015.

Hansen and Mullen (1992) conjectured that there exists an irreducible polynomial of $\mathbb{F}_q$ with a coefficient prescribed, with some exceptions.

Conjecture (Hansen-Mullen)

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

By considering primitive polynomials with given trace, Cohen (1990) proved the conjecture for $j = n - 1$, while Hansen and Mullen proved their conjecture for $j = 1$. Wan (1997) proved that the conjecture holds, for $q > 19$ or $n \geq 36$ and Ham and Mullen (1998) proved the remaining cases with the help of computers.

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

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

One class of polynomials that has been intensively investigatedis that of self-reciprocal irreducible polynomials, that is, irreducible polynomials that satisfy $Q^R(X) = Q(X)$. Besides the theoretical interest in their existence and density, self-reciprocal irreducible polynomials have been useful in applications, and in particular in the construction of error-correcting codes.

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

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

- With this result in mind, we show that we can prescribe the k-th coefficient of a self-reciprocal irreducible polynomial of degree $2n$, provided that $k \leq \lfloor n/2 \rfloor$, with a small number of genuine exceptions.
- Our proof is based on an estimate of a weighted sum, similar to the one that Wan considers, the character sums presented earlier and Carlitz's (1967) characterization of self-reciprocal irreducible monic polynomials.

- Carlitz (1967) characterized self-reciprocal irreducible monic polynomials over $\mathbb{F}_q$ (srimp): Q is a srimp iff

$$Q(X) = X^n \hat{P}(X + X^{-1})$$

for some monic irreducible $\hat{P}$ of degree n, such that $\psi(\hat{P}) = -1$, where $\psi(\hat{P}) = (\hat{P}|X^2 - 4)$, the Jacobi symbol of $\hat{P}$ modulo $X^2 - 4$.

- We compute

$$Q(X) = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j} \hat{P}_i X^{n-i+2j},$$

which imples

$$Q_k = \sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} \hat{P}_{n-j}.$$

- In the last expression, Q_k is written in terms of the large degree coefficients of $\hat{P}$. In order to express in terms of the low degree coefficients of a polynomial, we define.

$$\hat{P} = X^n P(4X^{-1})$$

and prove that $\hat{P}_i = 4^{n-i} P_{n-i}$ and $\psi(P) = -\varepsilon\psi(\hat{P})$, where $\varepsilon = \pm 1$, depending on q and n.

- It follows that

$$Q_k = \sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = \sum_{j=0}^{k} \delta_j P_j,$$

where

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

We define $\tau_{n,k} : \mathbb{G}_k \to \mathbb{F}_q,\ H \mapsto \sum_{j=0}^{k} \delta_j H_j$, where $\mathbb{G}_k := \{H \in \mathbb{F}_q[X] \ : \ \deg(H) \leq k \text{ and } H_0 = 1\}$. We have proved:

Proposition

Let $n \geq 2, 1 \leq k \leq n$, and $a \in \mathbb{F}_q$. Suppose there exists an irreducible $P \in \mathbb{F}_q[X]$ with $P_0 = 1$, such that $\psi(P) = \varepsilon$ and $P \equiv H \pmod{X^{k+1}}$ for some $H \in \mathbb{G}_k$ with $\tau_{n,k}(H) = a$. Then there exists a srimp Q, of degree $2n$, with $Q_k = a$.

Next, we need to correlate the inverse image of $\tau_{n,k}$ with $\mathbb{G}_{k-1}$. In this direction, we prove.

Proposition

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

Let $n \geq 2, 1 \leq k \leq n$ and $a \in \mathbb{F}_q$. Inspired by Wan's work (1997) we introduce the following weighted sum.

$$w_a(n,k) = \sum_{H \in \tau_{n,k}^{-1}(a)} \Lambda(FH) \sum_{\psi(P)=\varepsilon,\ P \equiv H \pmod{X^{k+1}}} 1.$$

It is clear that if $w_a(n,k) > 0$, then there exists some P such that $P \equiv H \pmod{X^{k+1}}$ for some $H \in \mathbb{G}_k$, with $\tau_{n,k}(H) = a$ and $\psi(P) = \varepsilon$. Then there exists a srimp Q, of degree n with $Q_k = a$.

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

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

$$= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in \mathbb{J}_n \\ \psi(P) = \varepsilon}} \chi(P)\bar{\chi}(G) \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H)\bar{\chi}(H),$$

where G is the inverse of F modulo X^{k+1}.

We separate the term that corresponds to χ_0 and we get

$$\left| w_a(n,k) - \frac{\pi_q(n,\varepsilon)}{q^k} \sum_{H \in \mathbb{G}_{k-1}} \Lambda(H) \right| \leq$$

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

where $\pi_q(n,\varepsilon) = |\{P \text{ irreducible of degree } n : \psi(P) = \varepsilon\}|$.

Then we use estimates for $\sum_{H\in\mathbb{G}_{k-1}}\Lambda(H)$ and $\sum_{H\in\mathbb{G}_{k-1}}\Lambda(H)\bar{\chi}(H)$ and prove the theorem below.

Theorem

Let $n\geq 2, 1\leq k\leq n$, and $a\in\mathbb{F}_q$. There exists a srimp $Q\in\mathbb{F}_q[X]$, of degree $2n$ with $Q_k=a$ if the following bound holds.

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

Using known estimates for $\pi_q(n,-1)$, we conclude that:

Theorem

Let $n\geq 2, 1\leq k\leq n$, and $a\in\mathbb{F}_q$. There exists a srimp $Q\in\mathbb{F}_q[X]$, of degree $2n$ with $Q_k=a$ if the following bound holds.

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

Our final step is to content ourselves for $k \leq n/2$ and solve the resulting problem. Using the theory developed earlier, we conclude that there exists a srimp over $\mathbb{F}_q$ of degree $2n$ with its k-th coefficient prescribed, if

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

This bound is always true for $n \geq 27$. For $n < 27$ this bound is satisfied for the pairs (q,n) described below

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

Summing up, we have theoretically proved that:

Corollary

If $n \geq 3$ an integer and q a power of an odd prime, then there exists a srimp of degree $2n$ such that any of its $\lfloor n/2 \rfloor$ low degree coefficients is prescribed, if either $n \geq 27$ or $q \geq 839$.

For the remaining cases, computers searches have been employed. The computer results, combined with the above imply the following.

Theorem

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

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

Part II: Extending the (strong) primitive normal basis theorem I

This work is published in:

G. Kapetanakis.
Normal bases and primitive elements over finite fields.
Finite Fields Appl., 26:123–143, 2014.

- A generator of the multiplicative group $\mathbb{F}_{q^m}^*$ is called primitive. It is well-known that primitive elements exist for every q and m. Primitive elements are used in various applications, such as the Diffie-Hellman key exchange and the construction of Costas arrays, used in sonar and radar technology.
- An element $x \in \mathbb{F}_{q^m}$ is called free over $\mathbb{F}_q$ (or just free) if 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 (1888) proved the existence of normal basis (normal basis theorem). He also observed their computational advantages for fast arithmetic. Naturally, software and hardware implementations, used mostly in coding theory and cryptography, use normal bases.
- Both primitiveness and freeness are properties common to either all or none of the roots of an irreducible polynomial, hence one can define primitive polynomials and free polynomials naturally.

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

Theorem (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 (1987) were the first prove this result. Cohen and Huczynska (2003) provided a computer-free proof, using sieving techniques. More recently, a stronger result was shown.

Theorem (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 (2006) proved this for $m \geq 32$, but Cohen and Huczynska (2010) extended it to its stated form, with the help of their sieving techniques.

The problem we are considering here is the following.

Problem

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 exist some primitive $x \in \mathbb{F}_{q^m}$ such that both x and $(ax+b)/(cx+d)$ are free over $\mathbb{F}_q$?

- We solve this problem completely.
- Although not quite clear, this problem qualifies as an extension of the strong primitive normal basis theorem, since they both have three genuine conditions. Namely, here we demand that the arbitrary Möbius tranformation $(ax+b)/(cx+d)$ to be free, instead of just x^{-1}.

- $\mathbb{F}_{q^m}^*$ (the multiplicative group) can be seen as a $\mathbb{Z}$-module under the rule $r \circ x := x^r$ and $\mathbb{F}_{q^m}$ (the additive group), can be seen as an $\mathbb{F}_q[X]$-module, under the rule $F \circ x := \sum_{i=0}^{n} F_i x^{q^i}$.
- The fact that primitive elements exist for every finite field and the normal basis theorem, imply that both modules are cyclic, while the elements that are interesting for us, i.e. primitive and free elements, are the generators of those modules.
- It is now clear that we are interested in characterizing generators of cyclic modules over Euclidean domains.

- Let R be a Euclidean domain and $\mathcal{M}$ a cyclic finite R-module and g a generator. $\mathcal{M}$ has also the structure of an abelian group, hence $\widehat{\mathcal{M}}$ is well-defined and can also be seen as an R-module, while it is not hard to show that $\widehat{\mathcal{M}}$ is also cyclic.
- Let $x \in \mathcal{M}$. The annihilator of x is an ideal or R and, as such, has a unique generator. This is called the order of x and denoted by $\mathrm{ord}(x)$.
- Fix some $r \in R$, with $r \mid \mathrm{ord}(g)$. We call x r-free if $x = d \circ y$, for some $d \mid r$ and $y \in \mathcal{M}$ implies $d = 1$. Clearly, x is an R-generator of $\mathcal{M}$ if and only if it is $\mathrm{ord}(g)$-free.

We define the following functions for $d \in R$, $d \mid \mathrm{ord}(g)$:

1. The Euler function is defined as $\phi(d) := |(R/dR)^*|$,
2. the Möbius function is defined as

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

3. and $\theta(d) := \phi(d)/|(R/dR)|$.

Now, with the help of the orthogonality relations, we prove the following.

Proposition (Vinogradov's formula)

The characteristic function for r-free elements is

$$\omega_r(x) := \theta(r') \sum_{d \mid r} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in \widehat{\mathcal{M}},\ \mathrm{ord}(\chi)=d} \chi(x),$$

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

We call Order of $x \in \mathbb{F}_{q^m}$ (note the big 'O') its additive order and denote it by $\mathrm{Ord}(x)$. This means that $\mathrm{Ord}(x) \mid X^m - 1$. The Order of the additive character ψ is defined accordingly. For $G \mid X^m - 1$, we call x G-free, if $x = H \circ y$ for some $y \in \mathbb{F}_{q^m}$ and $H \mid G$, implies $H = 1$. Then the characteristic function of G-free elements is

$$\Omega_G(x) := \theta(G') \sum_{F \mid G,\, F \text{ monic}} \frac{\mu(F)}{\phi(F)} \sum_{\psi \in \widehat{\mathbb{F}_{q^m}},\, \mathrm{Ord}(\psi) = F} \psi(x),$$

where G' is the square-free part of G. Also, free elements are exactly those of Order $X^m - 1$, i.e. those that are F_0-free, where F_0 is the square-free part of $X^m - 1$, i.e. $F_0 := X^{m_0} - 1$, where m_0 is such that $m = m_0 p^b$ and $(m_0, p) = 1$.

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

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

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

- 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 $i = 1, 2$. Set $\mathbf{k} := (q_1, F_1, F_2)$ and call it a divisor triple. We call $x \in \mathbb{F}_{q^m}$ $\mathbf{k}_A$-free, if x is q_1-free and F_1-free and $(ax+b)/(cx+d)$ is F_2-free. Also, $N_A(\mathbf{k})$ stands for the number of $x \in \mathbb{F}_{q^m}$ that are $\mathbf{k}_A$-free.
- Set $\mathbf{w} = (q_0, F_0, F_0)$ and $\mathbf{1} = (1, 1, 1)$.
- We also define some arithmetic between divisor triples (division, multiplication, prime divisor triples, gcd of divisor triples)
- Set t_r to be the number of prime (or irreducible) divisors of r and $W(r) := 2^{t_r}$. It follows that $\sum_{d|r} |\mu(d)| = W(r)$.
- 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.

Lemma

For any $r \in \mathbb{N}$, $W(r) \leq c_{r,a} r^{1/a}$, where $c_{r,a} = 2^s/(p_1 \cdots p_s)^{1/a}$ and $p_1, \ldots, p_s$ are the primes $\leq 2^a$ that divide r.

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

Proposition

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* $q^{m/2} \geq 3\, W(\mathbf{k})$, *then* $N_A(\mathbf{k}) > 0$.

- If $q = 2$ and $c = 0$, then $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, hence we are looking for some free x, such that $x + 1$ is also free, impossible for odd m and always true for even m.
- The proof is divided in two parts, $c \neq 0$ and $c = 0$, since different types of character sums arise in each case.

Sketch of the proof for the case $c \neq 0$.

Since ω and Ω are characteristic functions, we have:

$$N_A(\mathbf{k}) = \sum_{x \neq -d/c} \omega_{q_1}(x)\Omega_{F_1}(x)\Omega_{F_2}((ax+b)/(cx+d))$$

$$= \theta(\mathbf{k}) \sum_{\substack{\mathbf{l}|\mathbf{k} \\ \mathbf{l}=(d_1,G_1,G_2)}} \frac{\mu(\mathbf{l})}{\phi(\mathbf{l})} \sum_{\substack{\mathrm{ord}(\chi_1)=d_1, \\ \mathrm{Ord}(\psi_1)=G_1, \\ \mathrm{Ord}(\psi_2)=G_2}} \sum_{x \neq -d/c} \chi_g(x^{n_1})\psi_g(\mathcal{G}(x)),$$

for some $n_1 \in \mathbb{N}$ and $\mathcal{G} \in \mathbb{F}_q(X)$. By using the character sum estimates presented earlier and separating some cases, we prove that the inner sum is bounded by $3q^{m/2}$, unless $(d_1, G_1, G_2) = \mathbf{1}$. We then separate the term that corresponds to that triple and show that

$$N_A(\mathbf{k})/\theta(\mathbf{k}) \geq q^{m/2}(q^{m/2} - q^{-m/2} - 3(W(\mathbf{k}) - 1))$$

and the desired result follows. □

Following Cohen and Huczynska (2003 and 2010), we introduce a sieve that will help us get improved results.

- Let $\mathbf{k}$ 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 $\mathbf{k}_i \mid \mathbf{k}$ for all i, their least common multiplier is divided by $\mathbf{k}$ and $(\mathbf{k}_i, \mathbf{k}_j) = \mathbf{k}_0$ for $i \neq j$.
- 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 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 $\delta := 1 - \sum_{i=1}^{r} 1/|\mathbf{p}_i|$ and $\Delta := (r-1)/\delta + 2$.

With a help of a tricky induction, we prove:

Proposition (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

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

Which implies

Proposition

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 $q^{m/2} > 3\, W(\mathbf{k}_0) \Delta$, then $N_A(\mathbf{k}) > 0$.

It follows from well-known results that F_0 splits into $\phi(m_0)/s$ irreducibles of degree s, where s is minimal such that $q_0 \mid q^s - 1$ and some others of degree dividing s. We denote the product of those with degree s by G_0.

Proposition

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.*

Using previous results, we begin to prove that $N_A(\mathbf{w}) > 0$, by distinguishing the following special cases:

$m_0 \leq 4$: Additive sieving is unnecessary.

$m_0 = q - 1$: F_0 splits into $q - 1$ linear factors. We use additive sieving on roughly half of those factors.

$m_0 \mid q - 1$: F_0 splits into linear factors. We sieve all those factors.

$m = 2$: This is a special case altogether, treated separately.

Sketch of the proof for the case $m_0 \mid q-1$.

Here, $G_0 = F_0$ and $s = 1$. It follows that $N_A(\mathbf{w}) > 0$ if

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

Since $W(q_0) < 4.9 q^{m/4}$ this implies that another sufficient condition would be

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

The latter always true for $m_0 \geq 12$. We explicitly check the validity of the two above conditions for $3 \leq m_0 \leq 11$ and end up with a set of 89 pairs (q, m) of possible exceptions. If 4.9 above is replaced by the exact value of $c_{q_0,4}$ then the list is furtherer reduced to 20 pairs. For those pairs we try to apply sieving on the multiplicative part as well and succeed on half of them. □

Next, we focus on the case $m_0 > 4$ and $s \neq 1$. We define $\rho := t_{F_0/G_0}/m_0$, where t_{F_0/G_0} stands for the number of irreducible factors of F_0/G_0. Now, $N_A(\mathbf{w}) > 0$, if

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

It follows that some knowledge regarding the value of ρ is required.

Lemma (Cohen-Huczynska)

1. *Assume* $m_0 > 4$ *and* $q > 4$. *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* $\rho \leq 1/3$.
5. *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* $\rho \leq 1/6$.

We explicitly check each of the cases described in the last lemma and we deduce the following.

Theorem

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 70 pairs listed below.

Case	Possible exception pairs (q, m)	#
$m_0 \leq 4$	$(8,6),\ (5,5),\ (4,6),\ (3,12),\ (3,6),\ (2,12),\ (2,8),\ (2,6),\ (2,4),\ (4,4),$ $(8,4),\ (3,4),\ (7,4),\ (11,4),\ (19,4),\ (23,4),\ (2,3),\ (3,3),\ (5,3),\ (8,3),$ $(9,3),\ (11,3),\ (23,3)$	23
$m_0 = q-1$	$(4,3), (5,4), (7,6), (8,7), (9,8), (11,10), (13,12), (16,15)$	8
$m_0 \mid q-1$	$(7,3),\ (9,4),\ (11,5),\ (13,3),\ (13,4),\ (13,6),\ (16,3),\ (17,4),\ (19,3),$ $(25,3)$	10
$\rho > 1/3$	$(5,8), (7,12), (13,8), (5,16)$	4
$\rho \leq 1/3$	$(5,6), (5,12), (7,5), (11,6)$	4
$q < 5$	$(4,5),\ (4,7),\ (4,9),\ (4,15),\ (3,5),\ (3,7),\ (3,8),\ (3,10),\ (3,16),\ (2,5),$ $(2,7), (2,9), (2,11), (2,15), (2,21)$	15
$m = 2$	$(2,2), (3,2), (4,2), (5,2), (7,2), (11,2)$	6
	Total:	**70**

Our final step is to examine the remaining cases one-by-one and identify the true exceptions to our problem. In order to perform all the necessary tests, a computer program was written in Sage. These are the results.

Table: $q = 2$.

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

Table: $q = 3$.

m	$f \in \mathbb{F}_3[X]$ irreducible	$x \in \mathbb{F}_{3^m}$ primitive, such that x and $A \circ x$ free
2	$X^2 + 2X + 2$	$\beta + 2$ (4); β (6)
3	$X^3 + 2X + 1$	$2\beta^2 + 1$ (3); $\beta^2 + 1$ (7)
4	$X^4 + 2X^3 + 2$	β (7); 2β (3)
5	$X^5 + 2X + 1$	$\beta + 1$ (6); $\beta + 2$ (3); $\beta + 2$ (1)
6	$X^6 + 2X^4 + X^2 + 2X + 2$	$\beta^2 + 1$ (5); $\beta^2 + \beta + 2$ (3); $\beta^4 + 2\beta^2$ (2)
7	$X^7 + 2X^2 + 1$	$\beta^2 + 1$ (2); $2\beta + 2$ (2); $\beta + 2$ (6)
8	$X^8 + 2X^5 + X^4 + 2X^2 + 2X + 2$	$\beta^4 + \beta + 1$ (4); $\beta^4 + \beta^2 + 2\beta + 1$ (3); $\beta^4 + \beta^3 + 1$ (1); $\beta^4 + 2\beta$ (2)
10	$X^{10} + 2X^6 + 2X^5 + 2X^4 + X + 2$	$\beta^3 + 2\beta + 1$ (7); $\beta^3 + 2\beta^2 + 1$ (1); $2\beta^3 + \beta + 2$ (2)
12	$X^{12} + X^6 + X^5 + X^4 + X^2 + 2$	$\beta^7 + 2\beta + 2$ (5); $\beta^7 + \beta^2 + \beta$ (3); $\beta^7 + \beta^2 + \beta + 2$ (2)
16	$X^{16} + 2X^7 + 2X^6 + 2X^4 + 2X^3 + 2X^2 + X + 2$	$\beta + 2$ (3); $2\beta + 1$ (3); $\beta^2 + 2$ (1); $2\beta^2 + 1$ (1); $2\beta^3 + \beta^2 + 1$ (1); $\beta^3 + 2\beta^2 + 2$ (1)

Table: $q = 5$.

m	$f \in \mathbb{F}_5[X]$ irreducible	$x \in \mathbb{F}_{5^m}$ primitive, such that x and $A \circ x$ free
2	$X^2 + 4X + 2$	β (22); $\beta + 4$ (6)
3	$X^3 + 3X + 3$	$\beta + 3$ (23); $2\beta + 4$ (1); $\beta + 4$ (4)
4	$X^4 + 4X^2 + 4X + 2$	$\beta^2 + \beta + 1$ (15); $\beta^2 + 3\beta + 3$ (5); $\beta^2 + 3\beta + 4$ (1); **None** (4); $\beta^2 + 4\beta$ (1); $2\beta^2 + \beta + 1$ (1); $2\beta^2 + 3\beta$ (1)
5	$X^5 + 4X + 3$	$\beta^4 + 1$ (23); $\beta^4 + 2$ (5)
6	$X^6 + X^4 + 4X^3 + X^2 + 2$	$\beta^2 + 1$ (11); $2\beta^2 + 4\beta + 3$ (4); $\beta^2 + 2\beta + 4$ (5); $\beta^2 + \beta$ (6); $2\beta^2 + 2\beta$ (1); $3\beta^2 + 3$ (1)
8	$X^8 + X^4 + 3X^2 + 4X + 2$	$\beta^3 + 2\beta + 2$ (9); $\beta^3 + 3\beta + 2$ (5); $\beta^3 + 2\beta + 1$ (10); $\beta^3 + 4\beta + 3$ (2); $\beta^3 + 3\beta + 4$ (1); $\beta^3 + 4\beta + 4$ (1)
12	$X^{12} + X^7 + X^6 + 4X^4 + 4X^3 + 3X^2 + 2X + 2$	$\beta + 4$ (14); $3\beta + 2$ (5); $2\beta + 3$ (7); $4\beta + 1$ (2)
16	$X^{16} + X^8 + 4X^7 + 4X^6 + 4X^5 + 2X^4 + 4X^3 + 4X^2 + X + 2$	$2\beta^2 + 4\beta + 1$ (1); $\beta^2 + 2\beta + 3$ (7); $\beta^2 + 2$ (10); $\beta^2 + 4\beta + 3$ (8); $3\beta^2 + 2\beta + 4$ (1); $2\beta^2 + 4$ (1)

Table: $q \in \{7, 11\}$.

q	m	$f \in \mathbb{F}_q[X]$ irreducible	$x \in \mathbb{F}_{q^m}$ primitive, such that x and $A \circ x$ free
7	2	$X^2 + 6X + 3$	β (46); $\beta + 1$ (8)
	3	$X^3 + 6X^2 + 4$	$\beta + 1$ (16); $\beta + 6$ (3); β (35)
	4	$X^4 + 5X^2 + 4X + 3$	$\beta + 1$ (46); $\beta + 3$ (8)
	5	$X^5 + X + 4$	$\beta + 1$ (46); $3\beta + 4$ (8)
	6	$X^6 + X^4 + 5X^3 + 4X^2 + 6X + 3$	$\beta^2 + 5\beta$ (8); $\beta^2 + 4\beta$ (9); $\beta^2 + 4\beta + 2$ (12); $\beta^2 + 5\beta + 4$ (6); $\beta^2 + 3\beta + 6$ (16); $2\beta^2 + \beta$ (1); $\beta^2 + 6\beta + 6$ (1); $\beta^2 + 6\beta + 1$ (1)
	12	$X^{12} + 2X^8 + 5X^7 + 3X^6 + 2X^5 + 4X^4 + 5X^2 + 3$	$\beta^2 + 4\beta + 1$ (15); $3\beta^2 + 3\beta + 4$ (1); $2\beta^2 + \beta + 2$ (1); $\beta^2 + \beta + 6$ (29); $\beta^2 + 5\beta + 4$ (5); $2\beta^2 + 3\beta + 1$ (1); $\beta^2 + 5\beta + 3$ (2)
11	2	$X^2 + 7X + 2$	β (118); $\beta + 7$ (12)
	3	$X^3 + 2X + 9$	$\beta + 7$ (12); $\beta + 4$ (118)
	4	$X^4 + 8X^2 + 10X + 2$	$\beta + 2$ (118); $\beta + 5$ (10); $\beta + 6$ (2)
	5	$X^5 + 10X^2 + 9$	$\beta + 7$ (6); $\beta + 4$ (78); $\beta + 5$ (35); $\beta + 10$ (1); $\beta + 9$ (10)
	6	$X^6 + 3X^4 + 4X^3 + 6X^2 + 7X + 2$	$\beta + 3$ (118); $\beta + 8$ (10); $2\beta + 5$ (2)
	10	$X^{10} + 7X^5 + 8X^4 + 10X^3 + 6X^2 + 6X + 2$	$\beta + 10$ (22); $\beta + 4$ (59); $\beta + 7$ (33); $2\beta + 3$ (13); $2\beta + 9$ (2); $2\beta + 8$ (1)

Table: q is a prime ≥ 13.

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

Table: $q = 4$.

In that case, $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, where α is a root of $X^2 + X + 1 \in \mathbb{F}_2[X]$.

m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_{q^m}$
2	$X^2 + X + \alpha$	$\alpha\beta + \alpha + 1$ (18)
3	$X^3 + \alpha X^2 + (\alpha + 1)X + \alpha$	$\alpha\beta^2 + (\alpha + 1)\beta + \alpha + 1$ (3); $\alpha\beta^2 + \alpha\beta$ (8); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (3); **None** (3); $\alpha\beta^2 + (\alpha + 1)\beta + 1$ (1)
4	$X^4 + X^2 + (\alpha + 1)X + \alpha$	$\alpha\beta^3$ (15); $\alpha\beta^3 + \alpha$ (3)
5	$X^5 + (\alpha + 1)X^4 + X + \alpha$	$\alpha\beta + \alpha$ (14); $(\alpha + 1)\beta$ (4)
6	$X^6 + (\alpha+1)X^5 + (\alpha+1)X^4 + X^3 + X + \alpha + 1$	$\alpha\beta^3 + \alpha\beta$ (11); $\alpha\beta^3 + \alpha$ (7)
7	$X^7 + \alpha X^6 + X^5 + (\alpha + 1)X^3 + X^2 + \alpha X + 1$	$\alpha\beta$ (13); $\alpha\beta + 1$ (5)
9	$X^9 + (\alpha + 1)X^8 + \alpha X^7 + X^6 + (\alpha + 1)X^5 + \alpha X^4 + X^3 + (\alpha + 1)X + 1$	$\alpha\beta^2 + \alpha\beta$ (8); $\alpha\beta^2 + \alpha\beta + 1$ (2); $(\alpha + 1)\beta^2 + \alpha\beta + 1$ (1); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (6); $\alpha\beta^2 + \beta + \alpha + 1$ (1)
15	$X^{15} + \alpha X^14 + (\alpha + 1)X^13 + X^12 + \alpha X^11 + \alpha X^10 + X^8 + X^7 + X^6 + X^4 + (\alpha+1)X^3 + \alpha X + 1$	$(\alpha + 1)\beta^2 + \alpha\beta + \alpha$ (4); $\alpha\beta^2 + \alpha\beta + 1$ (8); $\alpha\beta^2 + (\alpha + 1)\beta + 1$ (1); $\beta^2 + \beta + \alpha + 1$ (1); $\alpha\beta^2 + \beta + 1$ (2); $\beta^2 + \alpha\beta + \alpha + 1$ (1); $(\alpha + 1)\beta^2 + (\alpha + 1)\beta + \alpha$ (1)

Table: $q \in \{8, 9\}$.

q	$h \in \mathbb{F}_p[X]$	m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_{q^m}$
8	$X^3 + X + 1$	3	$X^3 + (\alpha^2+\alpha+1)X^2 + (\alpha^2+1)X + \alpha^2 + \alpha + 1$	$\alpha\beta$ (61); $\alpha\beta + \alpha$ (9)
		4	$X^4 + (\alpha^2+1)X^3 + (\alpha^2+\alpha)X^2 + (\alpha^2+\alpha)X + \alpha^2 + 1$	$\alpha\beta$ (62); $\alpha\beta + \alpha + 1$ (8)
		6	$X^6 + (\alpha^2+\alpha+1)X^5 + (\alpha^2+\alpha+1)X^3 + X^2 + (\alpha^2+\alpha+1)X + 1$	$\alpha\beta$ (70)
		7	$X^7 + (\alpha^2+\alpha+1)X^6 + (\alpha+1)X^5 + (\alpha^2+1)X^4 + \alpha^2X^3 + (\alpha+1)X^2 + (\alpha+1)X + \alpha^2 + 1$	$\alpha\beta^2 + \alpha\beta + \alpha^2 + \alpha$ (9); $\alpha\beta^2 + \alpha\beta + \alpha^2$ (8); $\alpha\beta^2 + \alpha\beta + \alpha$ (22); $\alpha\beta^2 + \alpha\beta$ (27); $\alpha\beta^2 + \alpha\beta + \alpha^2 + 1$ (2); $\alpha\beta^2 + \alpha\beta + \alpha^2 + \alpha + 1$ (2)
9	$X^2 + 2X + 2$	3	$X^3 + X^2 + \alpha + 1$	$\alpha\beta$ (80); $\alpha\beta + \alpha$ (8)
		4	$X^4 + (\alpha+2)X^3 + 2X^2 + (\alpha+1)X + 2\alpha + 1$	$\alpha\beta + \alpha + 1$ (63); $\alpha\beta + \alpha + 2$ (15); $\alpha\beta^2 + \alpha\beta + \alpha + 1$ (7); $(\alpha+1)\beta + 2\alpha + 1$ (1); $\alpha\beta^2 + (\alpha+2)\beta + 2$ (1); $(\alpha+1)\beta + 1)$ (1)
		8	$X^8 + (2\alpha+2)X^7 + 2\alpha X^5 + 2\alpha X^4 + 2X^3 + (2\alpha+1)X^2 + (2\alpha+2)X + \alpha + 2$	$\alpha\beta^2 + \alpha\beta + 2\alpha + 1$ (47); $\alpha\beta^2 + \alpha\beta + \alpha + 2$ (19); $\alpha\beta^2 + (2\alpha+1)\beta + 1$ (8); $\alpha\beta^2 + \alpha\beta + 2\alpha + 2$ (11); $\alpha\beta^2 + (2\alpha+1)\beta$ (2); $\alpha\beta^2 + 2\beta + 2\alpha + 1$ (1)

Table: $q \in \{16, 25\}$.

q	$h \in \mathbb{F}_p[X]$	m	$f \in \mathbb{F}_q[X]$	$x \in \mathbb{F}_{q^m}$
16	$X^4 + X + 1$	3	$X^3 + (\alpha + 1)X + \alpha^2$	$\alpha\beta+\alpha$ (223); $\alpha\beta+\alpha+1$ (41); $\alpha\beta+\alpha^2+\alpha+1$ (6)
		15	$X^{15} + (\alpha^3 + 1)X^{14} + (\alpha^3 + \alpha^2 + \alpha+1)X^{13} + \alpha^3 X^{12} + \alpha X^{11} + (\alpha^2 + \alpha + 1)X^{10} + (\alpha^3 + \alpha^2)X^9 + \alpha X^8 + (\alpha^2 + \alpha)X^7 + (\alpha^2 + 1)X^6 + (\alpha^3 + \alpha)X^5 + (\alpha^2 + \alpha + 1)X^4 + \alpha^2 X^3 + (\alpha^3 + \alpha^2)X^2 + (\alpha^2 + \alpha)X + \alpha^3 + \alpha$	$\alpha\beta + \alpha^3$ (93); $\alpha\beta + \alpha + 1$ (21); $\alpha\beta + \alpha$ (133); $\alpha\beta + \alpha^2 + 1$ (17); $\alpha\beta + \alpha^3 + \alpha + 1$ (4); $\alpha\beta + \alpha^3 + \alpha$ (2)
25	$X^2 + 4X + 2$	3	$X^3 + (3\alpha + 3)X^2 + 2\alpha X + 2\alpha + 2$	$\alpha\beta$ (575); $\alpha\beta + \alpha$ (67); $\alpha\beta + 2\alpha + 2$ (5); $\alpha\beta + 2\alpha + 1$ (1)

Summing up, we have proved:

Theorem

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* $d = 0$.

- We have exactly the exceptions appearing in the strong primitive normal basis theorem.
- We have no exceptions at all if all of the entries of A are non-zero!
- All the exceptions described above are genuine (not just possible).

Part III: Extending the (strong) primitive normal basis theorem II

This work is published in:

G. Kapetanakis.
An extension of the (strong) primitive normal basis theorem.
Appl. Algebra Engrg. Comm. Comput., 25(5):311–337, 2014.

The problem we consider here is the following.

Problem

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 exist some $x \in \mathbb{F}_{q^m}$ such that both x and $(ax+b)/(cx+d)$ are simultaneously primitive and free over $\mathbb{F}_q$?

- This problem and the problem we considered in Part II, are similar, but not identical, i.e. in Part II we had three conditions (x is primitive, x is free over $\mathbb{F}_q$ and $(ax+b)/(cx+d)$ is free over $\mathbb{F}_q$), while here we also demand $(ax+b)/(cx+d)$ to be primitive. Still both problems are natural extensions of the primitive normal basis theorem and its strong version.
- We do not solve this problem completely, but we show that it is true, provided that q and m are large enough.

- In this setting, we work with divisor quadruples, like for example $\mathbf{k} := (q_1, q_2, F_1, F_2)$, where $q_i \mid q_0$ and $F_i \mid F_0$.
- Their arithmetic is analogous to that of divisor triples.
- Two special quadruples are $\mathbf{w} := (q_0, q_0, F_0, F_0)$ and $\mathbf{1} := (1, 1, 1, 1)$.
- Similarly as before, our aim is to prove that $N_A(\mathbf{w}) > 0$.

Our first step is to prove the following.

Proposition

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* $q^{m/2} > 4\,W(\mathbf{k})$, *then* $N_A(\mathbf{k}) > 0$, *provided that* $q \neq 2$ *and if* A *has exactly two non-zero entries then their quotient is not a square in* $\mathbb{F}_q$.

The proof of the above is much more elaborate than its analogue in the previous setting. In particular, the following cases have to be distinguished:

1. matrices that are neither upper triangular nor anti-diagonal,
2. upper triangular matrices that are not diagonal,
3. anti-diagonal matrices and
4. diagonal matrices.

By introducing a sieve, like in the previous setting, we relax the condition we proved earlier and show the propositions below.

Proposition

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* $q^{m/2} > 4\,W(\mathbf{k}_0)\Delta$*, then* $N_A(\mathbf{k}) > 0$*.*

Proposition

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

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

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

As before, we use the theory developed earlier and show that $N_A(\mathbf{w}) > 0$ when $q \geq 23$ and $m \geq 17$ for the following cases:

1. $m_0 \leq 4$,
2. $m_0 = q - 1$,
3. $m_0 \mid q - 1$,
4. $\rho = 1/2$,
5. $\rho = 3/8$,
6. $\rho = 13/36$ and
7. $\rho \leq 1/3$.

Summing up, we have shown the following result.

Theorem

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 $(ax+b)/(cx+d)$ are simultaneously primitive and free over $\mathbb{F}_q$.

THANK YOU!