On the multiplicative order of the roots of $bX^{q^r+1} - aX^{q^r} + dX - c$

F.E. Brochero Martínez[a], Theodoulos Garefalakis[b], Lucas Reis[a], Eleni Tzanaki[b]

[a] *Departamento de Matemática, Universidade Federal de Minas Gerais, Belo Horizonte, MG, 30123-970, Brazil*
[b] *Department of Mathematics and Applied Mathematics, University of Crete, 70013 Heraklion, Greece*

Abstract

In this paper, we find a lower bound for the order of the group $\langle \theta + \alpha \rangle \subset \overline{\mathbb{F}}_q^*$, where $\alpha \in \mathbb{F}_q$, θ is a generic root of the polynomial $F_{A,r}(X) = bX^{q^r+1} - aX^{q^r} + dX - c \in \mathbb{F}_q[X]$ and $ad - bc \neq 0$.

Keywords: Multiplicative order; Group action on irreducible polynomials; Invariant polynomial
PACS: 11T06, 11T55

1. Introduction

Let $\mathbb{F}_q$ be the field with q elements, where q is a power of a prime p. Given a positive integer n, it is natural to ask how to find elements of very high order in the multiplicative group $\left(\frac{\mathbb{F}_q[X]}{f(x)}\right)^*$, where $f(x)$ is an irreducible polynomial of degree n. Elements of this type are used in the AKS algorithm (see [1]), for determining primality in polynomial time. This question is closely related to the problem of efficiently constructing a primitive element of a given finite field, which has practical applications in Coding Theory and Cryptography. This last problem has been considered by many authors: In [4], Gao gives an algorithm for explicitly constructing elements for a general extension $\mathbb{F}_{q^n}$ of the field $\mathbb{F}_q$, with order bounded below by a function of the form $\exp\left(c(p)\frac{\log^2 \log q}{\log\log\log q}\right)$, where $c(p)$ depends only on the characteristic of the field. In [2], Cheng shows how to find, given q and N, an integer n in

Email addresses: fbrocher@mat.ufmg.br (F.E. Brochero Martínez), tgaref@uoc.gr (Theodoulos Garefalakis), lucasreismat@gmail.com (Lucas Reis), etzanaki@uoc.gr (Eleni Tzanaki)

the interval $[N, 2qN]$, and a θ in the field $\mathbb{F}_{q^n}$ with order larger than $5.8^{n \log q / \log n}$. In [7] and [8], Popovych considers the case where $f(X) = \Phi_r(X)$, the r-th cyclotomic polynomial, and $f(X) = X^n - a$ are irreducible polynomials in $\mathbb{F}_q[X]$ and finds a lower bound of the order of $\langle \theta + c \rangle$, where θ is a root of $f(X) = 0$. Finally in [6], the authors consider the same problem with the polynomial $f(X) = X^p - X + c \in \mathbb{F}_q[X]$.

On the other hand, in [10], Stichtenoth and Topuzoğlu show that, given a matrix $[A] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in \mathrm{PGL}_2(\mathbb{F}_q)$, every irreducible factor f of $F_{A,r}(X) = bX^{q^r+1} - aX^{q^r} + dX - c$ in $\mathbb{F}_q[X]$ is invariant by an appropriate natural action of $[A]$ and reciprocally, every irreducible polynomial f, invariant by the action of $[A]$, is a factor of $F_{A,r}(X)$ for some $r \geq 0$. This relation is used in [10] to estimate, asymptotically, the number of irreducible monic polynomial of given degree and invariant by $[A]$ and they conclude that, in general, the irreducible factors of $F_{A,r}(X)$ has degree Dr, where D is the order of $[A]$ in $\mathrm{PGL}_2(\mathbb{F}_q)$.

In this paper we study the problem of finding elements of high order arising from fields $\left(\frac{\mathbb{F}_q[X]}{f(X)}\right)^*$, where $f(X)$ is an irreducible factor of $F_{A,r}(X)$ and we obtain the following:

Theorem 1.1. *Let $\alpha \in \mathbb{F}_q$, $A \in \mathrm{GL}_2(\mathbb{F}_q)$, $[A] \neq [I]$ and θ be a generic root of $F_{A,r}$, i.e. $\theta \in \overline{\mathbb{F}}_q$ satisfies $\dim_{\mathbb{F}_q} \mathbb{F}_q[\theta] = Dr$ where $D = \mathrm{ord}([A])$ and $r > 2$. The multiplicative order of $\theta + \alpha$ is bounded below by*

$$\frac{1}{\sqrt{2}\pi D} \sqrt{\frac{r-2}{r+2}} \cdot \left(\frac{(r+2)^{r+2}}{(r-2)^{r-2}}\right)^{\frac{D}{4}} \exp\left(-\frac{5}{24D} \cdot \frac{r^2+4}{r^2-4}\right), \tag{1}$$

in the case that $(1, 0)$ and $(0, 1)A^j$ are linearly independent for all j and

$$\frac{\sqrt{2}}{\pi D} \sqrt{\frac{r}{r+1}} \cdot \left(\frac{4(r+1)^{r+1}}{r^r}\right)^{\frac{D}{2}} \exp\left(-\frac{1}{12D} \cdot \frac{5r^2+5r+2}{r^2+r}\right) \tag{2}$$

otherwise.

Remark 1.2. *For every $\epsilon > 0$ and $r > R_\epsilon$, the lower bound (1) is greater than*

$$\frac{1}{\sqrt{2}\pi D}((e-\epsilon)(r+2))^D$$

and the lower bound (2) is greater than

$$\frac{\sqrt{2}}{\pi D}(2(e-\epsilon)(r+1))^{D/2}.$$

Remark 1.3. *We note that, θ is a root of $F_{A,r}$ if and only if $\theta+\alpha$ is root of $F_{B,r}$, where*

$$B = \begin{pmatrix} a+b\alpha & b \\ c+d\alpha-a\alpha-b\alpha^2 & d-b\alpha \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q),$$

and the matrices A and B have the same eigenvalues, hence their multiplicative order are the same. Since our bounds essencially depend of the order of A and r, in the following, unless otherwise stated, we assume that $\alpha = 0$. In particular, when $b \neq 0$, taking $\alpha = -ab^{-1}$ we can find a better bound for the order of the element $\theta - ab^{-1}$; the case $r = 1$ implies the bound found by Cheng, Gao and Wan (see Theorem 2.4 of [3]).

We also note that the element θ is implicitely defined, as a root of a "generic" irreducible factor of $F_{A,r}$. In practice, construction of the field $\left(\frac{\mathbb{F}_q[X]}{f(X)}\right)^*$ requires computation of the irreducible polynomial f. A straitforward factorization of $F_{A,r}$ requires time polynomial in q^r. It would be desirable to have an algorithm that costructs the field $\mathbb{F}_{q^{rD}}$ in time polynymial in $r, D, \log q$. As the value of D can be of the same order of magnitude as q, see Remark 2.6, we see that for $D = \Omega(q^\epsilon)$ (for any fixed $\epsilon > 0$) and small values of r, most notably for $r = 1$, the straitforward factorization of $F_{A,r}$ does indeed take time polynomial in D. The general case, that is, for arbitrary r and D, remains an interesting open problem.

In addition, in the case when A is a triangular matrix this lower bound can also be improved, see Remark 3.5.

2. Preliminaries

Throughout this paper, $\mathbb{F}_q$ is the finite field with q elements, where q is a power of a prime p; given a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, $[A]$ denotes its class in $\mathrm{PGL}_2(\mathbb{F}_q)$ and $D = \mathrm{ord}([A])$. Observe that, in the case $\det(A) = 1$ and A is diagonalizable, the eigenvalues of A are γ and γ^{-1} and we have that $D = \mathrm{ord}([A]) = \frac{\mathrm{ord}\gamma}{(\mathrm{ord}\gamma, 2)}$ and then $A^D = (-1)^{D+1}I$. In addition, for each non-negative integer r, $F_{A,r}(X)$ denotes the polynomial $bX^{q^r+1} - aX^{q^r} + dX - c$. For any integer n, we will refer to the rows of the matrix A^n by (a_n, b_n) and (c_n, d_n) for the first and second row respectively. By this convention, we note that $(a_n, b_n) = (1, 0)A^n$ and $(c_n, d_n) = (0, 1)A^n$.

There is an action of the general linear group $\mathrm{GL}_2(\mathbb{F}_q)$ on the set of irreducible polynomials of degree at least 2, which was studied in [5, 10]. In this work, we adopt the notation of [10].

Definition 2.1. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$. For an irreducible polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $n \geq 2$ and $\theta \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$, define*

1. $(A \circ f)(X) := (bX + d)^n \cdot f\left(\frac{aX + c}{bX + d}\right)$.
2. $[A] \circ f(X) :=$ *the unique monic polynomial* $g(X)$ *such that* $(A \circ f)(X) = \lambda g(X)$ *for some* $\lambda \in \mathbb{F}_q$.
3. $[A] \circ \theta = A \circ \theta := \dfrac{d\theta - c}{-b\theta + a}$.

It turns out that the above rules define actions of $\mathrm{GL}_2(\mathbb{F}_q)$ on the set of irreducible polynomials of degree at least 2 in $\mathbb{F}_q[X]$ and on $\overline{\mathbb{F}}_q \setminus \mathbb{F}_q$ respectively and these actions are closely related: from Lemma 2.7 in [10], it follows that θ is a root of f if and only if $A \circ \theta$ is a root of $A \circ f$.

One of the goals of [10] is the characterization and counting the monic irreducible polynomials that are fixed by the action of a given matrix. The following theorems provide such a characterization.

Theorem 2.2 ([10], Theorems 4.2 and 4.5)**.** *Let* $f(X) \in \mathbb{F}_q[X]$ *be a monic irreducible polynomial of degree* $n \geq 2$*. The following are equivalent:*

1. $[A] \circ f = f$
2. $f \mid F_{A,r}$ *for some non-negative integer* $r < n$*.*

In addition, every irrreducible factor of $F_{A,r}$ *has degree* ≤ 2 *or* Dk*, where* $k|r$ *and* $\gcd(\frac{r}{k}, D) = 1$.

Expecifically, denoting

$$N_{A,r}(n) = \left|\left\{f \in \mathbb{F}_q[X] \ : \ f \text{ monic, irreducible }, \deg(f) = n, f|F_{A,r}\right\}\right|,$$

it follows that

Theorem 2.3 ([10], Theorems 5.2)**.** *Let* $A \in \mathrm{GL}_2(\mathbb{F}_q)$ *and* $\mathrm{ord}([A]) = D \geq 2$*. Then*

1. $N_{A,r}(n) = 0$*, if* $D \nmid n$*,* $n \geq 2$*.*
2. $N_{A,r}(Dr) \sim \frac{q^r}{Dr}$*, as* $r \to \infty$*,*

that is, all non-linear irreducible factors of $F_{A,r}$ *have degree divisible by* D *and almost all have degree* Dr*, as* r *tends to infinity.*

In order to bound the order of a generic root θ of the polynomial $F_{A,r}(X)$, i.e. θ is a root of $F_{A,r}(X)$ such that $\dim_{\mathbb{F}_q} \mathbb{F}_q[\theta] = Dr$, it is enough to find a set $J \subset \mathbb{N}$ such that $\theta^i \neq \theta^j$ for every $i \neq j$ elements of J and thus $\mathrm{ord}(\theta) \geq |J|$. In order to find such set, observe that θ satisfies the relation $\theta^{q^r} = A \circ \theta$, and inductively we obtain that

$$\theta^{q^{jr}} = A^j \circ \theta, \quad \text{for } j \in \mathbb{Z}_{\geq 0}. \tag{3}$$

The main idea lies on the construction of an appropriate set J having elements of the form $u_0 + u_1 q^r + \cdots + u_{D-1} q^{r(D-1)}$, with some restriction on $u_j \in \mathbb{Z}$, and use the relation (3) to show that the elements in $\{\theta^j, j \in J\}$ are all different.

In order to prove Theorem 1.1, we need the following technical lemmas:

Lemma 2.4. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_q)$*, with* $\det(A) = 1$ *and* $bc \neq 0$ *. Let us denote* (a_n, b_n) *and* (c_n, d_n) *the first and second row, respectively, of* A^n*,* $n \in \mathbb{N}$*. Then for any* $0 \leq k < n < D$*, the vectors* $(a_n, b_n), (a_k, b_k)$ *are linearly independent over* $\overline{\mathbb{F}}_q$*. The same holds for the vectors* $(c_n, d_n), (c_k, d_k)$*.*

Proof. Let us suppose that A is a diagonalizable matrix and denote by α, α^{-1} the two eigenvalues of A. Since A is a diagonalizable matrix, we can write

$$A = M \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} M^{-1}, \quad \text{where} \quad M = \begin{pmatrix} t & u \\ v & w \end{pmatrix}$$

is an invertible matrix . The assumption $bc \neq 0$ implies $tuvw \neq 0$.

By direct calculation, we have that

$$A^n = \begin{pmatrix} \delta(tw\alpha^n - uv\alpha^{-n}) & \delta ut(\alpha^{-n} - \alpha^n) \\ \delta vw(\alpha^n - \alpha^{-n}) & \delta(wt\alpha^{-n} - uv\alpha^n) \end{pmatrix}, \quad n \in \mathbb{N}.$$

where $\delta := (tw - uv)^{-1} = (\det(M))^{-1}$. Let us suppose that $(a_n, b_n) = \gamma(a_k, b_k)$ for some $0 \leq k < n < D$ and some $\gamma \in \overline{\mathbb{F}}_q$, then

$$\begin{aligned} tw\alpha^n - uv\alpha^{-n} &= \gamma(tw\alpha^k - uv\alpha^{-k}) \\ ut(\alpha^{-n} - \alpha^n) &= \gamma ut(\alpha^{-k} - \alpha^k), \end{aligned}$$

which implies

$$\begin{aligned} tw(\alpha^n - \gamma\alpha^k) &= uv(\alpha^{-n} - \gamma\alpha^{-k}) \\ \alpha^n - \gamma\alpha^k &= \alpha^{-n} - \gamma\alpha^{-k}. \end{aligned}$$

If $\alpha^n \neq \gamma\alpha^k$, we obtain $tw = uv$, a contradiction since M is invertible. Therefore $\alpha^n = \gamma\alpha^k$ and $\alpha^{-n} = \gamma\alpha^{-k}$, hence $\alpha^{2(n-k)} = 1$, i.e., $\mathrm{ord}(\alpha)$ divides $2(n-k)$. If $\mathrm{ord}(\alpha)$ is even, then $2D = \mathrm{ord}(\alpha)$ and $0 < 2(n-k) < 2D$. If $\mathrm{ord}(\alpha)$ is odd, then $\mathrm{ord}(\alpha)$ divides $(n-k)$, $D = \mathrm{ord}(\alpha)$ and $0 < n-k < D$. Both cases lead us to a contradiction. The proof of the linear independence of (c_n, d_n) and (c_k, d_k) follows similarly.

When A is non diagonalizable matrix, then

$$A = M^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} M, \quad \text{where} \quad M = \begin{pmatrix} t & u \\ v & w \end{pmatrix}$$

and

$$A^n = \begin{pmatrix} 1 - n\delta tu & -n\delta u^2 \\ n\delta t^2 & 1 + n\delta tu \end{pmatrix}, \quad n \in \mathbb{N}.$$

By the same process of the diagonalizable case, we conclude the proof. □

Lemma 2.5. *Let* $A = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_q)$ *with* $c \neq 0$ *and* (c_n, d_n) *as in the previous lemma. Then for any* $0 \leq k < n < D$*, the vectors* $(c_n, d_n), (c_k, d_k)$ *are linearly independent over* $\overline{\mathbb{F}}_q$*.*

Proof. By a direct calculation, we have that

$$A^n = \begin{pmatrix} a^n & 0 \\ c\frac{a^n - d^n}{a - d} & d^n \end{pmatrix} \quad \text{if } a \neq d$$

and

$$A^n = \begin{pmatrix} a^n & 0 \\ nca^{n-1} & a^n \end{pmatrix} \quad \text{if } a = d.$$

Let us suppose that $(c_n, d_n) = \gamma(c_k, d_k)$ for some $0 \leq k < n < D$ and some $\gamma \in \overline{\mathbb{F}}_q$, in the case $a \neq d$, it follows that $\gamma = d^{n-k}$ and

$$c\frac{a^n - d^n}{a - d} = cd^{n-k}\frac{a^k - d^k}{a - d}.$$

Since $c \neq 0$, we obtain that $a^{n-k} = d^{n-k}$ and therefore $A^{n-k} = a^{n-k}I$, which is impossible since $0 < n - k < D$. The second case is similar. □

Remark 2.6. *When* $A = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_q)$ *is a triangular matrix,* $[A] \neq [I]$*, then*

$$\mathrm{ord}([A]) = \begin{cases} \mathrm{ord}(\frac{a}{d}) & \text{if } a \neq d \\ p & \text{if } a = d \text{ and } c \neq 0. \end{cases}$$

In the case that $\det(A) = 1$ *and* A *has eigenvalues* $\gamma, \gamma^{-1} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$*, we have* $\mathrm{ord}([A]) = \mathrm{ord}(\gamma)/(\mathrm{ord}(\gamma), 2)$*. Moreover,* $\gamma^{-1} = \gamma^q$*, so that the order of* γ *has to divide* $q + 1$*. The converse is also true: any element* $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *of order dividing* $q + 1$ *is a root of an irreducible polynomial of the form* $X^2 - cX + 1 \in \mathbb{F}_q[X]$*. Therefore, any matrix* A *with* $\mathrm{tr}(A) = c$ *and* $\det(A) = 1$ *will have eigenvalues* γ, γ^{-1}*. It follows, that for matrices of this type the maximum possible value for* $\mathrm{ord}([A])$ *is* $\epsilon(q + 1)$*, where* $\epsilon = 1$ *for* q *even and* $\epsilon = 1/2$ *for* q *odd.*

Lemma 2.7. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_q)$ *and denote by* (a_n, b_n) *and* (c_n, d_n) *the first and second row, respectively, of* A^n*,* $n \in \mathbb{N}$*. Assume that* $(c_n, d_n) = \gamma(a_k, b_k)$ *for some* $0 \le k, n < D$ *and* $\gamma \in \overline{\mathbb{F}}_q$*. Then, denoting* $g = n - k$*, we have*

$$(c_i, d_i) = \epsilon_i \gamma(a_{i-g}, b_{i-g}), \quad 0 \le i \le D - 1,$$

where $\epsilon_i \in \{-1, 1\}$ *and the indexes are computed modulo D.*

Proof. By definition, $(a_k, b_k) = (1, 0)A^k$ and $(c_n, d_n) = (0, 1)A^n$, hence $(0, 1)A^g = \gamma(1, 0)$, where $g = n - k$. Therefore $(0, 1)A^{g+i} = \gamma(1, 0)A^i$, that is,

$$(c_{g+i}, d_{g+i}) = \gamma(a_i, b_i), \quad \forall i \ge 0. \tag{4}$$

Assume $k < n$. From this it follows that

$$\begin{aligned} (c_{g+i}, d_{g+i}) &= \gamma(a_i, b_i), \quad i = 0 \ldots, D - g - 1, \\ (c_{D+i}, d_{D+i}) &= \gamma(a_{D-g+i}, b_{D-g+i}), \quad i = 0, \ldots, g - 1, \end{aligned}$$

where the second identity follows by changing $D - g + i$ for i in Eq. (4). Now, since $A^D = (-1)^{D+1}I$ we have that $(c_{D+i}, d_{D+i}) = (0, 1)A^{D+i} = (-1)^{D+1}(c_i, d_i)$, so we have

$$\begin{aligned} (c_i, d_i) &= \gamma(-1)^{D-1}(a_{D-g+i}, b_{D-g+i}), \quad i = 0, \ldots, g - 1, \\ (c_i, d_i) &= \gamma(a_{i-g}, b_{i-g}), \quad i = g, \ldots, D - 1. \end{aligned}$$

If $k > n$ the computation is entirely similar and the case $k = n$ is not possible since (a_k, b_k) and (c_k, d_k) are linearly independent. □

Remark 2.8. *If* ρ *is the smallest prime factor of D and g is defined as in Lemma 2.7, it is clear that*

$$(g, D) \le D/\rho$$

and this bound is sharp: for instance, suppose that q is not a power of ρ*, let* $\beta \in \mathbb{F}_q$ *be a* $2\rho n$*-th primitive root of the unity and* $\alpha = \beta^n$ *. Consider* $M = \begin{pmatrix} 1 & 1 \\ \alpha & \alpha^{-1} \end{pmatrix}$ *and*

$$A = M^{-1} \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} M.$$

Observe that $\mathrm{ord}([A]) = \rho n$ *and if g is the minimum positive integer such that*

$$\beta^{2g} = \frac{uv}{tw} = \frac{\alpha}{\alpha^{-1}} = \beta^{2n},$$

then $g = n = \frac{D}{\rho}$*, where* t, u, v *and* w *are defined as in Lemma 2.4. In the proof of our main result we use the general bound* $(g, D) \le \lfloor \frac{D}{2} \rfloor$*.*

3. Bounds for the order of $\langle\theta\rangle \subset \overline{\mathbb{F}_q}^*$

Before the proof of our main result, as in [6], we need the following definition:

Definition 3.1. *For each $s, t, m \in \mathbb{N}$, $m < D$, define the set*

$$I_{s,t,m} := \left\{ (u_0, \dots, u_{D-1}) \in \mathbb{Z}^D \;\middle|\; \begin{array}{l} \sum_{u_j>0} u_j \le s, \sum_{u_j<0} |u_j| \le t \quad \textit{and} \\ \textit{the first } m \textit{ coordinates are zero} \end{array} \right\}$$

Lemma 3.2. *Let $I_{s,t,m}$ be as in the Definition 3.1. Then*

$$|I_{s,t,m}| = \sum_{i=0}^{D-m} \binom{D-m}{i}\binom{s}{i}\binom{D-m-i+t}{t}.$$

In particular, for $t \ge \frac{D-m}{2}$

$$|I_{t,t,m}| > \binom{\frac{D-m}{2}+t}{D-m}\binom{2D-2m}{D-m}.$$

Proof. Let us denote $R = D - m$. Notice that, for each $0 \le i \le R$ and $0 \le j \le R - i$ there are $\binom{R}{i}\binom{R-i}{j}$ different ways to select j coordinates of $u_m, \dots, u_{D-1}$ to be negative and i coordinates to be positive. In addition, the number of positive solutions of $x_1 + x_2 + \cdots + x_i \le s$ is $\binom{s}{i}$ and the number of positive solutions of $x_1 + x_2 + \cdots + x_j \le t$ is $\binom{t}{j}$. Thus, for each pair i, j, there exist $\binom{R}{i}\binom{R-i}{j}\binom{s}{i}\binom{t}{j}$ elements of $I_{s,t,m}$. Summing over all i and j, we obtain

$$|I_{s,t,m}| = \sum_{i=0}^{R}\binom{R}{i}\binom{s}{i}\sum_{j=0}^{R-i}\binom{R-i}{j}\binom{t}{j} = \sum_{i=0}^{R}\binom{R}{i}\binom{s}{i}\binom{R-i+t}{t}. \tag{5}$$

An easy calculation gives $\binom{s}{i}\binom{R+t-i}{t} = \binom{R}{i}\binom{R-i+t}{R}\frac{\binom{s}{i}}{\binom{t}{i}}$. In particular, if $s = t$ we get

$$\begin{aligned} |I_{t,t,m}| &= \sum_{i=0}^{R}\binom{R}{i}^2\binom{R-i+t}{R} = \frac{1}{2}\sum_{i=0}^{R}\binom{R}{i}^2\left[\binom{R-i+t}{R} + \binom{i+t}{R}\right] \\ &\ge \frac{1}{2}\left[\binom{\lfloor\frac{R}{2}\rfloor+t}{R} + \binom{\lceil\frac{R}{2}\rceil+t}{R}\right]\sum_{i=0}^{R}\binom{R}{i}^2 \\ &= \frac{1}{2}\left[\binom{\lfloor\frac{R}{2}\rfloor+t}{R} + \binom{\lceil\frac{R}{2}\rceil+t}{R}\right]\binom{2R}{R} \\ &\ge \binom{\frac{R}{2}+t}{R}\binom{2R}{R}, \end{aligned}$$

where the last inequality follows from the fact that $\Gamma_N(x) := \binom{x}{N}$ is a convex function for all $x \geq N$. $\square$

Proposition 3.3. *For every $D \geq 2$ and $r \geq 3$ the following inequalities are hold*

a) $|I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, 0}| > \dfrac{1}{\sqrt{2}\pi D} \sqrt{\dfrac{r-1}{r+1}} \cdot \left(\dfrac{4(r+1)^{r+1}}{(r-1)^{r-1}}\right)^{\frac{D}{2}} \exp\left(-\dfrac{1}{12D} \cdot \dfrac{5r^2+3}{r^2-1}\right).$

b) $|I_{\lfloor \frac{Dr}{4} \rfloor, \lfloor \frac{Dr}{4} \rfloor, 0}| > \dfrac{1}{\sqrt{2}\pi D} \sqrt{\dfrac{r-2}{r+2}} \cdot \left(\dfrac{(r+2)^{r+2}}{(r-2)^{r-2}}\right)^{\frac{D}{4}} \exp\left(-\dfrac{5}{24D} \cdot \dfrac{r^2+4}{r^2-4}\right).$

c) $|I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{D}{2} \rfloor}| > \dfrac{\sqrt{2}}{\pi D} \sqrt{\dfrac{r}{r+1}} \cdot \left(\dfrac{4(r+1)^{r+1}}{r^r}\right)^{\frac{D}{2}} \exp\left(-\dfrac{1}{12D} \cdot \dfrac{5r^2+5r+2}{r^2+r}\right).$

Proof. The steps of the proof are essentially the same that ones used to prove Theorem 2.3 in [6]. In fact,

$$\binom{\frac{D}{2} + \frac{Dr}{4} - 1}{D} = \frac{\frac{D}{2} + \frac{Dr}{4} - D}{\frac{D}{2} + \frac{Dr}{4}} \cdot \binom{D \cdot \frac{r+2}{4}}{D} = \frac{r-2}{r+2} \cdot \binom{D \cdot \frac{r+2}{4}}{D}$$

From Corollary 1 in [9]

$$\begin{aligned}\binom{\frac{D}{2} + \frac{Dr}{4} - 1}{D} &\geq \frac{r-2}{r+2} \cdot \sqrt{\frac{\frac{r+2}{4}}{2\pi \frac{r-2}{4}}} \left(\frac{\left(\frac{r+2}{4}\right)^{\frac{r+2}{4}}}{\left(\frac{r-2}{4}\right)^{\frac{r-2}{4}}}\right)^D \frac{1}{\sqrt{D}} \exp\left(-\frac{1}{12D}\left(1 + \frac{16}{r^2-4}\right)\right) \\ &= \frac{1}{\sqrt{2\pi D}} \sqrt{\frac{r-2}{r+2}} \cdot \left(\frac{(r+2))^{\frac{r+2}{4}}}{4(r-2)^{\frac{r-2}{4}}}\right)^D \exp\left(-\frac{r^2+12}{12D(r^2-4)}\right).\end{aligned}$$

Finally, from Lemma 3.2 and inequality $\binom{2D}{D} > \frac{4^D}{\sqrt{\pi D}} \exp\left(-\frac{1}{8D}\right)$, we conclude that

$$\begin{aligned}|I_{\lfloor \frac{Dr}{4} \rfloor, \lfloor \frac{Dr}{4} \rfloor, 0}| &\geq \binom{\frac{D}{2} + \lfloor \frac{Dr}{4} \rfloor}{D} \cdot \binom{2D}{D} \geq \binom{\frac{D}{2} + \frac{Dr}{4} - 1}{D} \cdot \binom{2D}{D} \\ &> \frac{1}{\sqrt{2}\pi D} \sqrt{\frac{r-2}{r+2}} \cdot \left(\frac{(r+2)^{r+2}}{(r-2)^{r-2}}\right)^{\frac{D}{4}} \exp\left(-\frac{5}{24D} \cdot \frac{r^2+4}{r^2-4}\right).\end{aligned}$$

By the same process we obtain items a) and c). $\square$

The main result of this paper is consequence of following theorem

Theorem 3.4. *Let $A \in \mathrm{GL}_2(\mathbb{F}_q)$, $[A] \neq [I]$ and θ be a generic root of $F_{A,r}$. Then the map*

$$\begin{aligned}\Lambda : \quad I_{s,t,m} &\longrightarrow \langle \theta \rangle \\ (u_0, \dots, u_{D-1}) &\longmapsto \prod_{j=0}^{D-1} \theta^{u_j q^{jr}}\end{aligned}$$

is one to one in the following cases:

1) *A is a triangular matrix , $m = 0$ and $s + t < Dr$.*
2) *A is not a triangular matrix, $(0, 1)A^i$ and $(1, 0)A^j$ are linearly independent for all i, j, $m = 0$ and $s + t < \frac{Dr}{2}$.*
3) *A is not a triangular matrix, there exists $0 < g < D$ such that $(1, 0)$ and $(0, 1)A^g$ are linearly dependent, $m = \gcd(g, D)$ and $s + t < Dr$.*

Proof. Clearly $I_{s,t,g} \subseteq I_{s,t}$ for any $1 \leq g < D$. For $(u_0, \ldots, u_{D-1}) \in I_{s,t}$, we compute

$$\Lambda(u_0, \ldots, u_{D-1}) = \prod_{j=0}^{D-1} \left(\theta^{q^{jr}}\right)^{u_j} = \prod_{j=0}^{D-1} \left(A^j \circ \theta\right)^{u_j}.$$

For any matrix B in the class $[A] \in \mathrm{PGL}_2(\overline{\mathbb{F}}_q)$, we have $A^j \circ \theta = B^j \circ \theta$, so we may substittute A with $\delta^{-1}A$, where $\delta^2 = \det(A)$. This allows us to assume that $\det(A) = 1$, with $A \in \mathrm{GL}_2(\mathbb{F}_{q^2})$. We have

$$\Lambda(u_0, \ldots, u_{D-1}) = \prod_{j=0}^{D-1} \left(A^j \circ \theta\right)^{u_j} = \prod_{j=0}^{D-1} \left(\frac{d_j\theta - c_j}{-b_j\theta + a_j}\right)^{u_j}.$$

Consider now $(u_0, \ldots, u_{D-1}), (v_0, \ldots, v_{D-1}) \in I_{s,t}$ and let $\Lambda(u_0, \ldots, u_{D-1}) = \Lambda(v_0, \ldots, v_{D-1})$. Then we have

$$\begin{aligned} &\prod_{\substack{0\leq j\leq D-1\\ u_j>0}} \left(d_j\theta - c_j\right)^{u_j} \prod_{\substack{0\leq j\leq D-1\\ u_j<0}} \left(-b_j\theta + a_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D-1\\ v_j<0}} \left(d_j\theta - c_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D-1\\ v_j>0}} \left(-b_j\theta + a_j\right)^{v_j} \\ = &\prod_{\substack{0\leq j\leq D-1\\ v_j>0}} \left(d_j\theta - c_j\right)^{v_j} \prod_{\substack{0\leq j\leq D-1\\ v_j<0}} \left(-b_j\theta + a_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D-1\\ u_j<0}} \left(d_j\theta - c_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D-1\\ u_j>0}} \left(-b_j\theta + a_j\right)^{u_j}. \end{aligned}$$

So, θ is a root of $F(X) - G(X)$, where

$$\begin{aligned} F(X) &= \prod_{\substack{0\leq j\leq D-1\\ u_j>0}} \left(d_jX - c_j\right)^{u_j} \prod_{\substack{0\leq j\leq D-1\\ u_j<0}} \left(-b_jX + a_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D-1\\ v_j<0}} \left(d_jX - c_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D-1\\ v_j>0}} \left(-b_jX + a_j\right)^{v_j} \\ G(X) &= \prod_{\substack{0\leq j\leq D-1\\ v_j>0}} \left(d_jX - c_j\right)^{v_j} \prod_{\substack{0\leq j\leq D-1\\ v_j<0}} \left(-b_jX + a_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D-1\\ u_j<0}} \left(d_jX - c_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D-1\\ u_j>0}} \left(-b_jX + a_j\right)^{u_j}. \end{aligned}$$

We consider the following three cases:

Case 1: Suppose that A is a triangular matrix. Observe that if θ is root of $F_{A,r}(x)$, then θ^{-1} is root of the polynomial $F_{B,r}(x)$ where $B = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$. Therefore, changing θ by θ^{-1}, we can suppose, without loss of generality that A is lower triangular matrix. Thus $b_j = 0$ for all j and the degrees of the polynomials $F(X)$ and $G(X)$ are respectively

$$\sum_{u_j\geq 0} u_j - \sum_{v_j\leq 0} v_j \leq s+t \quad \text{and} \quad \sum_{v_j\geq 0} v_j - \sum_{u_j\leq 0} u_j \leq s+t.$$

Since $\deg(F(X)) \leq s+t < Dr$ and $\deg(G(X)) \leq s+t < Dr$ and $F(X) - G(X)$ is divisible by the minimal irreducible polynomial that θ is root, that has degree Dr, it follows that $F(X) = G(X)$. According to Lemma 2.5, the binomials $d_jX - c_j$ $(0 \leq j \leq D-1)$ are pair-wise distinct. It follows from the unique factorization property of $\mathbb{F}_q[X]$ that $(u_0, \dots, u_{D-1}) = (v_0, \dots, v_{D-1})$, that is, Λ is injective.

Case 2: The argument in this case is analogous to that of case 1, using Lemma 2.4 instead of Lemma 2.5. According to Lemma 2.4, the binomials $-b_jX + a_j$ $(0 \leq j \leq D-1)$ are pair-wise distinct. The same holds for the binomials $d_jX - c_j$ $(0 \leq j \leq D-1)$. The binomials $-b_jX + a_j$, $d_jX - c_j$ $(0 \leq j \leq D-1)$ are pair-wise distinct by the assumption of case 2.

Case 3: There exist $0 \leq k, n < D$, such that $(c_n, d_n) = \gamma(a_k, b_k)$, for some $\gamma \in \mathbb{F}_{q^2}^*$. Let us define $g = n - k$ and $m = \gcd(g, D)$. In this case, it turns out that we have to restrict Λ to the set $I_{s,t,m}$ to maintain injectivity. Indeed, by Lemma 2.7, we have

$$d_jX - c_j = \epsilon_j\gamma(b_{j-g}X - a_{j-g}), \quad \text{for } 0 \leq j \leq D-1$$

and we obtain

$$\begin{aligned} F(X) &= \epsilon_F\gamma^{e_F}\prod_{u_j<0}(b_jX - a_j)^{-u_j}\prod_{v_j>0}(b_jX - a_j)^{v_j}\prod_{u_j>0}(b_{j-g}X - a_{j-g})^{u_j}\prod_{v_j<0}(b_{j-g}X - a_{j-g})^{-v_j} \\ G(X) &= \epsilon_G\gamma^{e_G}\prod_{v_j<0}(b_jX - a_j)^{-v_j}\prod_{u_j>0}(b_jX - a_j)^{u_j}\prod_{v_j>0}(b_{j-g}X - a_{j-g})^{v_j}\prod_{u_j<0}(b_{j-g}X - a_{j-g})^{-u_j}, \end{aligned}$$

where $\epsilon_F, \epsilon_G \in \{-1, 1\}$, $e_F = \sum_{u_j>0} u_j - \sum_{v_j<0} v_j$ and $e_G = \sum_{v_j>0} v_j - \sum_{u_j<0} u_j$. By the definition of $I_{s,t,m}$, again we have $\deg(F), \deg(G) < Dr$, so that $F(X) = G(X)$, and we obtain

$$\epsilon\gamma^{e_G - e_F}\prod_{j=0}^{D-1}(b_jX - a_j)^{u_j - u_{j+g}} = \prod_{j=0}^{D-1}(b_jX - a_j)^{v_j - v_{j+g}},$$

with $\epsilon \in \{-1, 1\}$. By Lemma 2.4, we obtain

$$u_j - u_{j+g} = v_j - v_{j+g}, \quad 0 \leq j \leq D-1.$$

Let us define $x_j = u_j - v_j$, $0 \leq j < D$. Then we have $x_{j+g} = x_j$ for $j \geq 0$ (where we take the indices mod D). Let $J = \{\overline{j} \; : \; x_j = 0\}$. We know that $\{\overline{0}, \dots, \overline{(g, D) - 1}\} \subseteq$

J and the recursion gives us that $\left\{\overline{a+ig}\ :\ 0 \leq a < (g,D),\ i \geq 0\right\} \subseteq J$. It is easy to see that $J = \mathbb{Z}_D$, therefore $(u_0, \ldots, u_{D-1}) = (v_0, \ldots, v_{D-1})$ and Λ is injective. □

Remark 3.5. *If A is a triangular matrix, from Theorem 3.4 ($s = t = \lfloor \frac{Dr}{2} \rfloor, m = 0$) and (a) of Proposition 3.3 we have that a generic root θ of $F_{A,r}$ has multiplicative order bounded below by*

$$\frac{1}{\sqrt{2\pi D}} \sqrt{\frac{r-1}{r+1}} \cdot \left(\frac{4(r+1)^{r+1}}{(r-1)^{r-1}}\right)^{\frac{D}{2}} \exp\left(-\frac{1}{12D} \cdot \frac{5r^2+3}{r^2-1}\right).$$

For every $\epsilon > 0$ and $r > R_\epsilon$, this bound is greater than $\frac{1}{\sqrt{2\pi D}}(2(e-\epsilon)(r+1))^D$.

Corollary 3.6. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ with $b \neq 0$ and let θ be a generic root of $F_{A,r}$ as in Theorem 1.1. The multiplicative order of $\theta - ab^{-1}$ is bounded below by $\left|I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, 1}\right|$*

Proof. By Remark 1.3, it is equivalent to bound the order of a generic root α of $F_{A,r}$ in the case $A = \begin{pmatrix} 0 & 1 \\ c & -d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, i.e., $F_{A,r}(X) = X^{q^r+1} - dX - c$. Therefore

$$\alpha^{q^{jr}} = \frac{d_j\alpha + c_j}{d_{j-1}\alpha + c_{j-1}} \quad 0 \leq j \leq D,$$

where $d_0 = 1$, $c_0 = 0$, $d_1 = d$, $c_1 = c$, $d_{D-1} = c_D = 0$ and $d_D = c_{D-1}$. It follows that $(1,0)$ and $(0,1)A^{D-1}$ are linearly dependent and then $m = \gcd(D, D-1) = 1$. The corollary follows from Theorem 3.4. □

For $D > 1862$ and r small, the following table gives a lower bound $L_{D,r}$ for $\left|I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, 1}\right|$

r	1	2	3	4	5
$L_{D,r}$	5.8^D	11.03^D	16.36^D	21.73^D	27.11^D

In particular, observe that the case $r = 1$ of the corollary above implies Theorem 2.4 in [3].

Acknowledgement

The authors would like to thank the anonymous reviewers for pointing out the work in [3] and for providing helpful comments and suggestions for improving the present work.

Bibliography

[1] Agrawal, M., Kayal, N., Saxena, N., Primes is in P. *Ann. of Math. (2)* 160:781–793, 2004.

[2] Cheng, Q., Constructing finite field extensions with large order elements. *SIAM J. Discrete Math.* 213:726–730. 2007.

[3] Cheng, Q., Gao, S., Wan, D. Constructing high order elements through subspace polynomials. *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms*, 1457–1463, 2012.

[4] Gao, S. Elements of provable high orders in finite fields. *Proc. Amer. Math. Soc.* 127:1615–1623, 1999.

[5] T. Garefalakis. On the action of $\mathrm{GL}(2,q)$ on irreducible polynomials over $\mathbb{F}_q$. *J. Pure and Appl. Algebra*, 215:1835 – 1843, 2011.

[6] F.E. Brochero Martínez and L. Reis. Elements of high order in Artin-Schreier extensions of finite fields $\mathbb{F}_q$. *Finite Fields Appl.*, 41:24 – 33, 2016.

[7] Popovych, R. Elements of high order in finite fields of the form $\mathbb{F}_q[x]/\Phi_r(x)$. *Finite Fields Appl.* 18:700–710, 2012

[8] Popovych, R. Elements of high order in finite fields of the form $\mathbb{F}_q[x]/(x^m - a)$. *Finite Fields Appl.* 19:86–92, 2013.

[9] Sasvári, Z., *Inequalities for binomial coefficients.* J. Math. Anal. Appl. 236:223-226, 1999.

[10] H. Stichtenoth and A. Topuzoğlu. Factorization of a class of polynomials over finite fields. *Finite Fields Appl.*, 18:108 – 122, 2012.