POLYNOMIAL VALUES IN SUBFIELDS AND AFFINE SUBSPACES OF FINITE FIELDS

OLIVER ROCHE-NEWTON AND IGOR E. SHPARLINSKI

ABSTRACT. For an integer r, a prime power q, and a polynomial f over a finite field $\mathbb{F}_{q^r}$ of q^r elements, we obtain an upper bound on the frequency of elements in an orbit generated by iterations of f which fall in a proper subfield of $\mathbb{F}_{q^r}$. We also obtain similar results for elements in affine subspaces of $\mathbb{F}_{q^r}$, considered as a linear space over $\mathbb{F}_q$.

1. Introduction

1.1. **Background.** For a prime power q and an integer $r > 1$ we consider finite fields $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_{q^r}$ of q and q^r elements, respectively.

The motivation behind this work comes from some questions of polynomial dynamics, however to address these questions we first obtain new results which fall in the domain of additive combinatorics as are of independent interest.

More precisely, given a polynomial $f \in \mathbb{F}[X]$ and an element $u \in \mathbb{F}$, we define the orbit

$$\mathrm{Orb}_f(u) = \{f^{(n)}(u) \ : \ n = 0, 1, \ldots\}, \tag{1}$$

where $f^{(n)}$ is the nth iterate of f, that is,

$$f^{(0)} = X, \quad f^{(n)} = f(f^{(n-1)}), \quad n \geq 1.$$

Here we consider the question about the frequency of elements in orbits $\mathrm{Orb}_f(u)$ that fall in the proper subfield $\mathbb{K} \subseteq \mathbb{F}$. Our first result is based on some combinatorial argument and shows that unless some iterate $f^{(s)}$ of f is defined over $\mathbb{F}$ (for a rather small s) then the frequency of this event is low.

Furthermore, we also study the frequency of orbit elements that fall in an affine subspace of $\mathbb{F}$ considered as a linear vector space over $\mathbb{K}$. This question is motivated by a recent work of Silverman and Viray [25] (in characteristic zero and using a very different technique), see also [1].

Date: July 29, 2014.

2010 *Mathematics Subject Classification.* 11T06, 37P05, 37P55.

Key words and phrases. finite fields, polynomial dynamics, orbits.

Using new results from additive combinatorics we obtain a lower bound on the dimension of an affine space that may contain N consecutive elements in an orbit. This result may also be considered as an analogue of the results on the diameters of polynomial orbits in prime fields $\mathbb{F}_p$, see [6, 7, 8, 10, 14]. More precisely, in [6, 7, 8, 10, 14] various lower bounds are given on the length H of the shortest interval $[a+1, a+H]$ that contains residues modulo p of the N consecutive iterations $f^{(n)}(u)$, $n = 0, \ldots, N-1$.

There are also related results where bounds on the size of the intersection $\#\left(f(\mathcal{A}) \cap \mathcal{B}\right)$ are given, where $\mathcal{A}$ and $\mathcal{B}$ are some 'interesting' sets and $f(\mathcal{A}) = \{f(a) \ : \ a \in \mathcal{A}\}$ is the value set of a polynomial f on $\mathcal{A}$; see [8, 10] for the case when both sets $\mathcal{A}$ and $\mathcal{B}$ are intervals of consecutive integers and [13, 24] for the case when $\mathcal{A}$ is such an interval and $\mathcal{B}$ is a multiplicative subgroup of $\mathbb{F}_p$. Unfortunately in the very interesting case when both sets $\mathcal{A}$ and $\mathcal{B}$ are subgroups of $\mathbb{F}_q$ no results are known. We also note that bounds on $\#\left(f(\mathcal{A}) \cap \mathcal{B}\right)$ for intervals $\mathcal{A}$ and $\mathcal{B}$ play an important role in the analysis of some algorithms [9].

Finally, we also mention that the intersection of $\mathcal{L}^{-1} \cap \mathcal{M}$ for two linear subspaces of $\mathbb{F}$ over $\mathbb{K}$ has been studied by Mattarei [17, 18] by using different methods (certainly 0 should be discarded from $\mathcal{L}$ in the definition of $\mathcal{L}^{-1}$). It is quite likely that the methods of additive combinatorics can be applied to this question as well.

1.2. **Our results.** Here we consider affine subspaces in high degree extensions of finite fields as natural analogues of intervals. To obtain results about orbits in affine subspaces of $\mathbb{F}$, we extend a result of Bukh and Tsimerman [5] on a polynomial version of the celebrated sum-product theorem to the case of arbitrary finite fields.

Recall that Bukh and Tsimerman [5, Theorem 1] give a lower bound on $\max\{\#(\mathcal{A}+\mathcal{A}), \#\left(f(\mathcal{A})+f(\mathcal{A})\right)\}$ for subsets $\mathcal{A}$ of prime fields. Their technique can be extended to arbitrary fields. However, motivated by our application we obtain a result of this kind with multifold sums of the set $\mathcal{A}$, see Theorem 4 below, which in turn gives stronger versions of our principal results. We believe that this result and some technical innovations in its proof can be of independent interest as well and may have several other applications. For example, using this result we derive an upper bound on the intersection $\#\left(\mathbb{A} \cap f(\mathbb{A})\right)$ of an affine subspace $\mathbb{A}$ of $\mathbb{F}$ over $\mathbb{K}$ and its polynomial image $f(\mathbb{A})$, see Theorem 7 below.

Furthermore, let us define the dimension $\dim \mathcal{S}$ of a set $\mathcal{S} \subseteq \mathbb{F}$ as the smallest dimension of all affine subspaces of $\mathbb{F}$ over $\mathbb{K}$ that contain $\mathcal{S}$. In Corollary 5 we obtain a lower bound on $\dim f(\mathbb{A})$ for an affine

subspace $\mathbb{A}$ of $\mathbb{F}$ over $\mathbb{K}$. Questions of this type sometimes appear in theoretical computer science, see [2, 3] and references therein. Note that some results of this kind for very special affine subspaces are also given in [11].

Finally, as we have mentioned, we apply these results to achieve our main goal: bound on the frequency of polynomial orbits in subspaces.

1.3. **Notation.** Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may depend on $\deg f$. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \le cV$ holds with some constant $c > 0$.

2. Polynomial Version of Sum-Product Estimates

2.1. **Preparations.** We now obtain a version of the result of Bukh and Tsimerman [5, Theorem 1] for polynomials over arbitrary finite fields.

As usual given m sets $\mathcal{A}_1, \ldots, \mathcal{A}_m \subseteq \mathbb{F}$ and a polynomial

$$F(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m],$$

we define the set

$$F(\mathcal{A}_1, \ldots, \mathcal{A}_m) = \{F(a_1, \ldots, a_m) \ : \ (a_1, \ldots, a_m) \in (\mathcal{A}_1 \times \ldots \times \mathcal{A}_m)\}.$$

In particular, $\mathcal{A} + \mathcal{A}$ and $\mathcal{A} \cdot \mathcal{A}$ are the sum set and the product set of $\mathcal{A}$, respectively.

We note that in our version of [5, Theorem 1] we use the set $\mathcal{A}+\mathcal{A}+\mathcal{A}+\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}$ instead of $\mathcal{A}+\mathcal{A}$ and $f(\mathcal{A})-f(\mathcal{A})$ instead of $f(\mathcal{A})+f(\mathcal{A})$, which leads for stronger expansion factor and is more suitable for our applications.

Throughout, the notation $\mathcal{A} : \mathcal{B}$ is used to denote the ratio set (assuming that $\mathcal{B} \subseteq \mathbb{F}^*$). Furthermore, we need the idea of a *restricted ratio set*. Namely, if $\mathcal{E} \subseteq \mathcal{A} \times \mathcal{B}$, then the ratio set of $\mathcal{A}$ and $\mathcal{B}$ restricted to $\mathcal{E}$ is the set

$$\mathcal{A} \stackrel{\mathcal{E}}{:} \mathcal{B} = \{a/b \ : \ (a, b) \in \mathcal{E}\}.$$

The following result is a small modification of [16, Theorem 1.4]. The necessary sum-ratio estimate is mentioned (without a proof) in [16]; a full proof can be found in [19].

Lemma 1. *Let $\mathcal{A}$ be a subset of $\mathbb{F}$ with the property that for any subfield $\mathbb{G}$, and any $a \in \mathbb{F}$,*

$$\#(\mathcal{A} \cap a\mathbb{G}) \le \max\left\{(\#\mathbb{G})^{1/2}, \frac{\#\mathcal{A}}{8}\right\}.$$

Then either,

$$(\#(\mathcal{A}:\mathcal{A}))^4\,(\#(\mathcal{A}+\mathcal{A}+\mathcal{A}+\mathcal{A}))^5 \gg (\#\mathcal{A})^{10}$$

or

$$(\#(\mathcal{A}:\mathcal{A}))^5\,(\#(\mathcal{A}+\mathcal{A}+\mathcal{A}+\mathcal{A}))^4 \gg (\#\mathcal{A})^{10}.$$

We also define

$$\mathcal{A} \overset{\mathcal{E}}{-} \mathcal{B} = \{a-b \ : \ (a,b) \in \mathcal{E}\}.$$

Furthermore, we extend in a natural way the definition of the sum set $\mathcal{A}+\mathcal{B}$ and difference set $\mathcal{A}-\mathcal{B}$ to subsets of an arbitrary group, written additively.

We also require a version of the Balog-Szemerédi-Gowers Theorem. The following result is essentially given in [4, Lemma 2.2]. Note that in the statement of [4, Lemma 2.2] it is assumed that the group in question is the additive group of the prime field $\mathbb{F}_p$, however, one can verify that the same proof works for an arbitrary group $\mathcal{G}$.

Lemma 2. *Let $\mathcal{G}$ be an arbitrary group, written additively, and let $\mathcal{U}, \mathcal{V} \subseteq \mathcal{G}$. Let $\mathcal{E} \subseteq \mathcal{U} \times \mathcal{V}$ such that*

$$\#\mathcal{E} \geq \frac{\#\mathcal{U}\#\mathcal{V}}{K}.$$

for some real $K \geq 1$. Then there exists a subset $\mathcal{U}_0 \subseteq \mathcal{U}$ such that

$$\#\mathcal{U}_0 \geq \frac{\#\mathcal{U}}{10K} \qquad \text{and} \qquad \#\left(\mathcal{U} \overset{\mathcal{E}}{-} \mathcal{V}\right)^4 \geq \frac{\#(\mathcal{U}_0-\mathcal{U}_0)\#\mathcal{U}(\#\mathcal{V})^2}{10^4K^5}.$$

Finally, we use a form of the Plünnecke-Ruzsa inequality which follows from [20, Theorem 1.1.1] (see also [5, Lemma 9]).

Lemma 3. *Let $\mathcal{G}$ be an arbitrary group, written additively, and let $\mathcal{U} \subseteq \mathcal{G}$. Then*

$$\#\left(\mathcal{U}+\mathcal{U}-\mathcal{U}-\mathcal{U}\right)^4 \leq \left(\frac{\#(\mathcal{U}-\mathcal{U})}{\#\mathcal{U}}\right)^4 \#\mathcal{U}.$$

2.2. **Main result.** Let p be the characteristic of $\mathbb{F} = \mathbb{F}_{q^r}$.

Theorem 4. *Let $\mathcal{A}$ be a subset of $\mathbb{F}$ with the property that, for any subfield $\mathbb{G} \subseteq \mathbb{F}$ and any $a \in \mathbb{F}$,*

$$\#\left((\mathcal{A}-\mathcal{A}) \cap a\mathbb{G}\right) \leq \max\left\{(\#\mathbb{G})^{1/2}, \frac{\#\mathcal{A}^{1-\vartheta_d}}{8}\right\}.$$

Then, for any polynomial $f \in \mathbb{F}[X]$ of degree $d = \deg f$ with $p > d \ge 2$ we have

$$\max\{\#(\mathcal{A}+\mathcal{A}+\mathcal{A}+\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}),\#\left(f(\mathcal{A})-f(\mathcal{A})\right)\} \ge c_d(\#\mathcal{A})^{1+\eta_d},$$

where $\eta_2 = \vartheta_2 = 1/69$, and $c_2 = c$ for some absolute constant $c > 0$ and then

$$\eta_d = \frac{\eta_{d-1}}{5+\eta_{d-1}}, \quad \vartheta_d = \vartheta_{d-1} + \eta_d - \vartheta_{d-1}\eta_d, \quad c_d = \left(\frac{c_{d-1}}{d^3}\right)^{1/(5+\eta_{d-1})}$$

for $d \ge 3$.

Proof. Let $\#\mathcal{A} = M$. We define α, β, γ and ξ by the relations:

$$\#(\mathcal{A}+\mathcal{A}) = \alpha M, \quad \#(\mathcal{A}-\mathcal{A}) = \beta M, \quad \#\left(f(\mathcal{A})-f(\mathcal{A})\right) = \xi M.$$

and

$$\#(\mathcal{A}+\mathcal{A}+\mathcal{A}+\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}) = \gamma M$$

The proof uses induction on d.

Consider first the base case $d = 2$. In this case the condition on the set $\mathcal{A}$ is simply

$$\#\left((\mathcal{A}-\mathcal{A}) \cap a\mathbb{G}\right) \le \max\left\{(\#\mathbb{G})^{1/2}, \frac{(\#\mathcal{A})^{1-\eta_2}}{8}\right\}. \tag{2}$$

Without loss of generality, we can assume that the polynomial f is monic and with the zero constant coefficient, since the cardinality of $f(\mathcal{A}) - f(\mathcal{A})$ does not vary under these changes to f. The polynomial f can then be written as $f(x) = x^2 + bx$, for some $b \in \mathbb{F}$. Note that, for any $x, y \in \mathcal{A}$,

$$f(x) - f(y) = x^2 + bx - y^2 - by = (x-y)(x+y+b). \tag{3}$$

Next, define a set $\mathcal{E} \subseteq (\mathcal{A}-\mathcal{A}) \times (\mathcal{A}+\mathcal{A}+b)^{-1}$ by the equation

$$\mathcal{E} = \{(x-y, (x+y+b)^{-1}) \ : \ x, y \in \mathcal{A}, x+y+b \ne 0\}.$$

Note that for $p > 2$ each pair (x, y) with $x, y \in \mathcal{A}$ and $x + y + b \ne 0$ leads to a different element of $\mathcal{E}$. Hence

$$\#\mathcal{E} \ge M^2 - M \ge \frac{M^2}{2} = \frac{\#\left(\mathcal{A}-\mathcal{A}\right)\#\left(\mathcal{A}+\mathcal{A}+b\right)}{2\alpha\beta}. \tag{4}$$

Moreover, by (3) we have

$$(\mathcal{A}-\mathcal{A}) \overset{\mathcal{E}}{\cdot} (\mathcal{A}+\mathcal{A}+b)^{-1} \subseteq f(\mathcal{A}) - f(\mathcal{A}), \tag{5}$$

where we define

$$(\mathcal{A}+\mathcal{A}+b)^{-1} = \{(x+y+b)^{-1} \ : \ x, y \in \mathcal{A}, x+y+b \ne 0\}.$$

We now apply Lemma 2 in this setting, with with the group $\mathcal{G} = \mathbb{F}^*$, the sets

$$\mathcal{U} = (\mathcal{A} - \mathcal{A})\backslash\{0\} \qquad \text{and} \qquad \mathcal{V} = (\mathcal{A} + \mathcal{A} + b)^{-1},$$

and thus, by (4), with $K = 2\alpha\beta$. Without loss of generality we can assume that $\#\mathcal{A} \geq 2$, so $\#(\mathcal{A} - \mathcal{A}) \geq \#\mathcal{A} \geq 2$, and thus

$$\#(\mathcal{A} - \mathcal{A}) - 1 \geq \frac{1}{2}\#(\mathcal{A} - \mathcal{A}).$$

Hence there exists a subset $\mathcal{A}_0 \subseteq \mathcal{A} - \mathcal{A}$ such that

$$\#\mathcal{A}_0 \geq \frac{\#(\mathcal{A} - \mathcal{A}) - 1}{20\alpha\beta} \geq \frac{\#(\mathcal{A} - \mathcal{A})}{40\alpha\beta} = \frac{M}{40\alpha} \tag{6}$$

and

$$\begin{aligned}\# \left((\mathcal{A} - \mathcal{A}) \stackrel{\mathcal{E}}{\cdot} (\mathcal{A} + \mathcal{A} + b)^{-1}\right)^4 &\geq \frac{\#(\mathcal{A}_0 : \mathcal{A}_0)\, \alpha^2\beta M^3}{10^4(2\alpha\beta)^5} \\ &= \frac{\#(\mathcal{A}_0 : \mathcal{A}_0)\, M^3}{32 \cdot 10^4\alpha^3\beta^4}.\end{aligned}$$

Applying the upper bound on the restricted ratio set which comes from (5), and simplifying, gives

$$\alpha^3\beta^4\xi^4 M \geq \frac{\#(\mathcal{A}_0 : \mathcal{A}_0)}{32 \cdot 10^4}.$$

If $\alpha > M^{\eta_2}/40$ there is nothing to prove. Otherwise we see from (6) that $\#\mathcal{A}_0 \geq M^{1-\eta_2}$. Note that it now follows from (2) that

$$\begin{aligned}\#(\mathcal{A}_0 \cap a\mathbb{G}) &\leq \#((\mathcal{A} - \mathcal{A}) \cap a\mathbb{G}) \\ &\leq \max\left\{(\#\mathbb{G})^{1/2}, \frac{M^{1-\eta_2}}{8}\right\} \leq \max\left\{(\#\mathbb{G})^{1/2}, \frac{\#\mathcal{A}_0}{8}\right\}.\end{aligned}$$

Therefore Lemma 1 applies to $\mathcal{A}_0$ and if interpreted as a lower bound for $\#(\mathcal{A}_0 : \mathcal{A}_0)$ yields either

$$\left(\#(\mathcal{A}_0 + \mathcal{A}_0 + \mathcal{A}_0 + \mathcal{A}_0)\right)^5 \alpha^{12}\beta^{16}\xi^{16}M^4 \gg (\#\mathcal{A}_0)^{10} \gg \frac{M^{10}}{\alpha^{10}}, \tag{7}$$

or

$$\left(\#(\mathcal{A}_0 + \mathcal{A}_0 + \mathcal{A}_0 + \mathcal{A}_0)\right)^4 \alpha^{15}\beta^{20}\xi^{20}M^5 \gg (\#\mathcal{A}_0)^{10} \gg \frac{M^{10}}{\alpha^{10}}. \tag{8}$$

Note that

$$\mathcal{A}_0 + \mathcal{A}_0 + \mathcal{A}_0 + \mathcal{A}_0 \subseteq \mathcal{A} + \mathcal{A} + \mathcal{A} + \mathcal{A} - \mathcal{A} - \mathcal{A} - \mathcal{A} - \mathcal{A},$$

so that $\#(\mathcal{A}_0+\mathcal{A}_0+\mathcal{A}_0+\mathcal{A}_0)\le\gamma M$. It is also straightforward to check that $\alpha,\beta\le\gamma$. Putting this information into (7), we conclude that

$$\gamma^{43}\xi^{16}\gg M. \tag{9}$$

On the other hand, the inequality (8) gives

$$\gamma^{49}\xi^{20}\gg M. \tag{10}$$

Since (9) also implies (10) it can be concluded that

$$\max\{\#(\mathcal{A}+\mathcal{A}+\mathcal{A}+\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}),\#\left(f(\mathcal{A})-f(\mathcal{A})\right)\} \gg (\#\mathcal{A})^{1+\frac{1}{69}}.$$

Taking a sufficiently small value of c we obtain the desired result for $d=2$, which concludes the base case.

Now assume that the result holds with $d-1$ instead of d.

Let

$$r(t)=\#\{(x,y)\in\mathcal{A}\times\mathcal{A}\ :\ t=x-y\}.$$

Since

$$\sum_{t\in\mathcal{A}-\mathcal{A}}r(t)=M^2,$$

it follows that there exists some $t\in\mathcal{A}-\mathcal{A}$ such that

$$r(t)\ge\frac{M^2}{\#(\mathcal{A}-\mathcal{A})}=\frac{M}{\beta}.$$

Define $\mathcal{B}=\{a\in\mathcal{A}\ :\ a+t\in\mathcal{A}\}$, and so

$$\#\mathcal{B}\ge M/\beta. \tag{11}$$

Now, if $\beta>M^{\eta_d}$ then there is nothing to prove. Otherwise we have

$$\#\mathcal{B}\ge M/\beta\ge M^{1-\eta_d}. \tag{12}$$

We now define a new polynomial $g(X)=f(X+t)-f(X)$, and note that $\deg g=d-1$ as $\deg f<p$. It is easy to check that $\mathcal{B}$ satisfies the subfield intersection conditions. Indeed, using (12) we derive

$$\begin{aligned}\#\left((\mathcal{B}-\mathcal{B})\cap a\mathbb{G}\right)&\le\#\left((\mathcal{A}-\mathcal{A})\cap a\mathbb{G}\right)\le\max\left\{(\#\mathbb{G})^{1/2},\frac{M^{1-\vartheta_d}}{8}\right\}\\&\le\max\left\{(\#\mathbb{G})^{1/2},\frac{(\#\mathcal{B})^{(1-\vartheta_d)/(1-\eta_d)}}{8}\right\}\\&=\max\left\{(\#\mathbb{G})^{1/2},\frac{(\#\mathcal{B})^{1-\vartheta_{d-1}}}{8}\right\}.\end{aligned}$$

So the inductive hypothesis can be applied with g and $\mathcal{B}$. There are two possibilities; either

$$\#\left(g(\mathcal{B})-g(\mathcal{B})\right) \geq c_{d-1}\left(\#\mathcal{B}\right)^{1+\eta_{d-1}} \tag{13}$$

or

$$\#\left(\mathcal{B}+\mathcal{B}+\mathcal{B}+\mathcal{B}-\mathcal{B}-\mathcal{B}-\mathcal{B}-\mathcal{B}\right) \geq c_{d-1}\left(\#\mathcal{B}\right)^{1+\eta_{d-1}}. \tag{14}$$

If (13) holds, we note that $g(\mathcal{B})-g(\mathcal{B}) \subseteq f(\mathcal{A})+f(\mathcal{A})-f(\mathcal{A})-f(\mathcal{A})$. Also, by Lemma 3, we have

$$\#\left(f(\mathcal{A})+f(\mathcal{A})-f(\mathcal{A})-f(\mathcal{A})\right) \leq \frac{\left(\#\left(f(\mathcal{A})-f(\mathcal{A})\right)\right)^4}{\left(\#f(\mathcal{A})\right)^3}.$$

So, using the trivial bound $\#f(\mathcal{A}) \geq M/d$, we obtain

$$c_{d-1}\left(\#\mathcal{B}\right)^{1+\eta_{d-1}} \leq d^3\xi^4 M.$$

Recalling (11) we derive

$$c_{d-1}d^{-3}M^{\eta_{d-1}} \leq \beta^{1+\eta_{d-1}}\xi^4.$$

Therefore

$$\max\{\beta,\xi\} \geq \left(c_{d-1}d^{-3}M^{\eta_{d-1}}\right)^{1/(5+\eta_{d-1})},$$

and so the desired result holds.

If (14) holds, then it follows from the fact that $\mathcal{B} \subseteq \mathcal{A}$ that

$$c_{d-1}\left(\#\mathcal{B}\right)^{1+\eta_{d-1}} \leq \gamma M \leq \gamma M d^3.$$

By applying (11), we derive

$$c_{d-1}d^{-3}M^{\eta_{d-1}} \leq \beta^{1+\eta_{d-1}}\gamma.$$

Therefore, using the fact that $\gamma \geq \beta$ we obtain

$$\max\{\gamma,\xi\} \geq \gamma \geq \left(c_{d-1}d^{-3}M^{\eta_{d-1}}\right)^{1/(2+\eta_{d-1})},$$

and so in this case the desired result holds as well. This closes the induction and concludes the proof. □

It is easy to see that

$$\lim_{d\to\infty}\frac{\log \eta_d}{d} = -\log 5.$$

Note that a similar result can also be obtained for the exponent of the bound of Bukh and Tsimerman [5, Theorem 1] (instead of $16^{-1}\cdot 6^{-d}$). This in turn implies that

$$\lim_{d\to\infty}\frac{\log c_d}{\log d} = -3.$$

We now recall the definition of the dimension $\dim \mathcal{S}$ of a set $\mathcal{S} \subseteq \mathbb{F}$ as the smallest dimension of all affine subspaces of $\mathbb{F}$ over $\mathbb{K}$ that contain $\mathcal{S}$.

Corollary 5. *Let $f \in \mathbb{F}[X]$ be of degree $d = \deg f$ with $p > d \geq 2$. Let $\mathbb{A} \subseteq \mathbb{F}$ be an affine subspace of dimension s over $\mathbb{K}$ such that for any subfield $\mathbb{G} \subseteq \mathbb{F}$ and any $a \in \mathbb{F}$, we have*

$$\# \left(\mathcal{L} \cap a\mathbb{G}\right) \leq \max \left\{ (\#\mathbb{G})^{1/2}, \frac{q^{s(1-\vartheta_d)}}{8} \right\},$$

where $\mathbb{A} = b + \mathcal{L}$ for some $b \in \mathbb{F}$ and a linear subspace $\mathcal{L} \subseteq \mathbb{F}$. Then

$$\dim f(\mathbb{A}) \geq (1 + \eta_d + o(1)) \dim \mathbb{A},$$

as $\#\mathbb{A} \to \infty$ where η_d and ϑ_d are as in Theorem 4.

Proof. Since we obviously have $\#(\mathbb{A}+\mathbb{A}+\mathbb{A}+\mathbb{A}-\mathbb{A}-\mathbb{A}-\mathbb{A}-\mathbb{A}) = \#\mathbb{A}$ and $\mathbb{A} - \mathbb{A} = \mathcal{L}$, then Theorem 4 implies $\# \left(f(\mathbb{A}) - f(\mathbb{A})\right\} \geq c_d(\#\mathbb{A})^{1+\eta_d}$ and the result follows. □

2.3. **Some remarks on Theorem 4.** Regarding the condition in Theorem 4 that the degree of f satisfies $d \leq p$, we note that some condition is necessary in order to account for the possibility that our polynomial f is additive. If f has the property that $f(x+y) = f(x) + f(y)$ for all $x, y \in \mathbb{L}$, then we can take $\mathcal{A}$ to be an affine subspace of $\mathbb{F}$ and observe that $\#(\mathcal{A}+\mathcal{A}), \#(f(\mathcal{A}) + f(\mathcal{A})) \ll \#\mathcal{A}$. For example, if $f(X) = X^p$, then f is an additive polynomial, and this is why the inductive argument breaks down at this point.

The condition that $\mathcal{A} - \mathcal{A}$ does not have an overly large intersection with a dilate of a subfield is needed in order to apply the sum-product estimate from [16]. Again, some condition of this kind is necessary, since it could be the case that $\mathcal{A} = \mathbb{G}$ for some subfield $\mathbb{G} \subseteq \mathbb{F}$. Then, if the coefficients of f are all taken from $\mathbb{G}$, we obviously have

$$\mathcal{A}+\mathcal{A}+\mathcal{A}+\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A}-\mathcal{A},\ f(\mathcal{A}) - f(\mathcal{A}) \subseteq \mathcal{A},$$

and so the estimate in Theorem 4 does not hold. It seems likely that the result holds under the cleaner condition that $\mathcal{A}$ does not have an overly large intersection with any subfield. We note that if $\#\mathcal{A} \geq (\#\mathbb{F})^{1/2}$, then this simplification of the condition can be obtained, since one does not need to worry about the subfield intersection conditions in the sum-product estimate for larger subsets of a finite field. Sum-product estimates for large subsets of a finite field can be found in [12] and [26].

It remains an interesting and open problem to give a full classification of the polynomials f and sets $\mathcal{A}$ for which

$$\max\{\#(\mathcal{A}+\mathcal{A}), \#\left(f(\mathcal{A})-f(\mathcal{A})\right)\} = (\#\mathcal{A})^{1+o(1)},$$

as $\#\mathcal{A} \to \infty$.

3. Distribution of Polynomial Orbits

3.1. **Polynomials orbits in subfields.** Clearly, for any $u \in \mathbb{F}$, the orbit (1) is a finite set as the sequence $f^{(n)}(u)$, $n = 0, 1, \ldots$, is eventually periodic. Let $T_u = \#\mathrm{Orb}_f(u)$ be the size of the orbit.

We now show that if a segment of an orbit of length $N \le T_u$ has a large intersection with $\mathbb{K}$ then there is an iterate of f which is defined over $\mathbb{K}$.

We note that the argument of this section works for any fields $\mathbb{K} \subseteq \mathbb{F}$, not necessary finite fields.

Theorem 6. *Let $f \in \mathbb{F}[X]$ be of degree $d \ge 1$ and let $u \in \mathbb{F}$. Assume that for some real $\eta > 0$ and an integer $N \le T_u$ we have*

$$\#\{0 \le n < N \ : \ f^{(n)}(u) \in \mathbb{K}\} \ge c(d)\frac{N}{\log N} + 1,$$

where $c(d) = 2\log(4d)$. Then for some integer k we have $f^{(k)}(X) \in \mathbb{K}[X]$.

Proof. Let $1 \le n_1 < \ldots < n_M \le N$ be all values with the property that $f^{(n_i)}(u) \in \mathbb{K}$. We denote by $A(h)$ the number of $i = 1, \ldots, M-1$ with $n_{i+1} - n_i = h$. Clearly

$$\sum_{h=1}^{N} A(h) = M - 1 \qquad \text{and} \qquad \sum_{h=1}^{N} A(h)h = n_M - n_1 \le N.$$

Thus for any integer $H \ge 1$ we have

$$\begin{aligned}\sum_{h=1}^{H} A(h) &= M - 1 - \sum_{h=H+1}^{N} A(h) \\ &\ge M - 1 - (H+1)^{-1} \sum_{h=H+1}^{N} A(h)h \ge M - 1 - (H+1)^{-1}N.\end{aligned}$$

Hence there exists $k \in \{1, \ldots, H\}$ with

$$A(k) \ge H^{-1}\left(M - 1 - (H+1)^{-1}N\right). \tag{15}$$

We now set

$$H = \left\lfloor \frac{2N}{(M-1)} \right\rfloor.$$

Clearly $H \geq 1$. Then

$$H^{-1}\left(M - 1 - (H+1)^{-1}N\right) \geq \frac{M-1}{2H} \geq \frac{N}{H(H+1)}$$

and we derive from (15) that

$$A(k) \geq \frac{N}{H(H+1)}. \tag{16}$$

Assume that $d^k \geq A(k)$. Then the inequality (16) implies that

$$d^H \geq d^k \geq \frac{N}{H(H+1)}.$$

Since $H < H+1 \leq 2^H$ for $H \geq 1$, we derive

$$(4d)^H > H(H+1)d^H \geq N$$

which in turn implies that

$$\frac{2N}{(M-1)} \geq H > \frac{\log N}{\log(4d)}$$

which contradicts our assumption on the frequency of orbit elements that belong to $\mathbb{K}$.

Therefore, $d^k < A(k)$.

Let $\mathcal{J}$ be the set of $j \in \{0, \ldots, M-1\}$ with $n_{j+1} - n_j = k$. Then we have

$$f^{(n_j)}(u) \in \mathbb{K} \qquad \text{and} \qquad f^{(n_{j+1})}(u) = f^{(k)}\left(f^{(n_j)}(u)\right) \in \mathbb{K}.$$

Since

$$\deg f^{(k)} = d^k < A(k) = \#\mathcal{J}$$

we now see that $f^{(k)}(w) \in \mathbb{K}$ for more than $\deg f^{(k)}$ elements $w \in \mathbb{K}$. Then by Lagrange interpolation we have $f^{(k)}(X) \in \mathbb{K}[X]$, which concludes the proof. □

3.2. **Polynomials orbits in affine subspaces.** As before we denote by p the characteristic of $\mathbb{F} = \mathbb{F}_{q^r}$.

Theorem 7. *Let $f \in \mathbb{F}[X]$ be of degree $d = \deg f$ with $p > d \geq 2$ and let $\mathbb{A} \subseteq \mathbb{F}$ be an affine subspace of dimension s over $\mathbb{K}$ such that for any subfield $\mathbb{G} \subseteq \mathbb{F}$ and any $a \in \mathbb{F}$ we have*

$$\#\left(\mathcal{L} \cap a\mathbb{G}\right) \leq \max\left\{(\#\mathbb{G})^{1/2}, \frac{q^{s(1-\rho_d)}}{8}\right\},$$

where $\mathbb{A} = b + \mathcal{L}$ for some $b \in \mathbb{F}$ and a linear subspace $\mathcal{L} \subseteq \mathbb{F}$. Then

$$\#\left(\mathbb{A} \cap f(\mathbb{A})\right) \ll q^{s(1-\kappa_d)},$$

where

$$\kappa_d = \frac{\eta_d}{1+\eta_d} \qquad \text{and} \qquad \rho_d = \eta_d + \vartheta_d - \eta_d\vartheta_d,$$

and η_d and ϑ_d are as in Theorem 4.

Proof. Let $\mathcal{S} = \mathbb{A} \cap f(\mathbb{A})$. Now, for each $s \in \mathcal{S}$ we choose an element $a \in \mathbb{A}$ with $f(a) = s$. Let $\mathcal{A}$ be this set, so that $\#\mathcal{S} = \#\mathcal{A}$.

It is obvious that

$$\mathcal{A} + \mathcal{A} + \mathcal{A} + \mathcal{A} - \mathcal{A} - \mathcal{A} - \mathcal{A} - \mathcal{A} \subseteq \mathcal{L}$$

and also

$$f(\mathcal{A}) - f(\mathcal{A}) \subseteq \mathcal{S} - \mathcal{S} \subseteq \mathcal{L}.$$

If $\#\mathcal{A} < q^{s(1-\eta_d)}$ there is nothing to prove. Otherwise

$$\#\mathcal{A}^{1-\vartheta_d} \geq q^{s(1-\eta_d)(1-\vartheta_d)} = \#\mathcal{L}^{1-\rho_d}$$

Hence, since $\mathcal{A} - \mathcal{A} \subseteq \mathcal{L}$ we have

$$\begin{aligned}\#\left((\mathcal{A}-\mathcal{A}) \cap a\mathbb{G}\right) \leq \#\left(\mathcal{L} \cap a\mathbb{G}\right) &\leq \max\left\{(\#\mathbb{G})^{1/2}, \frac{\#\mathcal{L}^{1-\rho_d}}{8}\right\} \\ &\leq \max\left\{(\#\mathbb{G})^{1/2}, \frac{\#\mathcal{A}^{1-\vartheta_d}}{8}\right\}\end{aligned}$$

for any $a \in \mathbb{F}$. Therefore Theorem 4 applies to the set $\mathcal{A}$ and implies that

$$\#\mathcal{L} \gg (\#\mathcal{A})^{1+\eta_d}$$

from which we immediately derive the result. □

Corollary 8. *Let $f \in \mathbb{F}[X]$ be of degree $d = \deg f$ with $p > d \geq 2$. Let $\mathbb{A} \subseteq \mathbb{F}$ be an affine subspace of dimension s over $\mathbb{K}$ such that for any subfield $\mathbb{G} \subseteq \mathbb{F}$ and any $a \in \mathbb{F}$ we have*

$$\#\left(\mathcal{L} \cap a\mathbb{G}\right) \leq \max\left\{(\#\mathbb{G})^{1/2}, \frac{q^{s(1-\rho_d)}}{8}\right\},$$

where $\mathbb{A} = b + \mathcal{L}$ for some $b \in \mathbb{F}$ and a linear subspace $\mathcal{L} \subseteq \mathbb{F}$. If for some $u \in \mathbb{F}$ and an integer N with $2 \leq N \leq T_u$ we have

$$f^{(n)}(u) \in \mathbb{A}, \qquad n = 0, \ldots, N-1,$$

then

$$q^s \gg N^{1+\eta_d},$$

where η_d and ρ_d are as in Theorems 4 and 7, respectively.

Proof. Let $\mathcal{R} = \{f^{(n)}(u) \ : \ n = 1, \ldots, N-1\}$. Then clearly, under the condition of the theorem, we have $\mathcal{R} \subseteq \mathbb{A} \cap f(\mathbb{A})$. Using Theorem 7 we derive the result. □

4. Comments

It is certainly interesting to obtain a multiplicative analogue of Theorem 4 for the sets $\mathcal{A}\cdot\mathcal{A}$ and $f(\mathcal{A})\cdot f(\mathcal{A})$ (and their multifold analogues). A result of this type can be used to study the distribution of polynomial orbits in subgroups. We note that even over prime fields this question is still widely open, see [23]. It is related to the aforementioned open problem of estimating the size of the intersection $f(\mathcal{G}) \cap \mathcal{H}$ for two multiplicative subgroups $\mathcal{G}, \mathcal{H} \subseteq \mathbb{F}^*$. The case when $\mathcal{G} = \mathcal{H}$ is of direct relevance to studying orbits of dynamical systems in subgroups. It seems plausible that the method of Heath-Brown and Konyagin [15], that has recently been advanced by Shkredov [21, 22], is able to yield such results over prime fields.

Studying rational functions instead of polynomials is an interesting direction as well.

The methods of proofs of Theorems 6 and 7 do not seem to extend to multivariate polynomials and it is very desirable to find an alternative approach.

Acknowledgements

The authors are grateful to Boris Bukh for helpful discussions and to Mike Zieve for information about his work in progress on polynomial orbits in subfields over fields of characteristic zero (however both the technique used and actually the results seem to be of a different nature).

During the preparation of this paper Oliver Roche-Newton was supported by the EPSRC Doctoral Prize Scheme, Grant EP/K503125/1 and part of this research was performed while he was visiting the Institute for Pure and Applied Mathematics (IPAM), which is supported by the National Science Foundation; Igor Shparlinski was supported by the Australian Research Council, Grants DP130100237 and DP140100118.

References

[1] E. Amerik, P. Kurlberg, K. Nguyen, A. Towsley, B. Viray and J. F. Voloch, 'Evidence for the dynamical Brauer-Manin criterion', *Preprint*, 2013 (available from `http://arxiv.org/abs/1305.4398`).

[2] E. Ben-Sasson and A. Gabizon, 'Extractors for polynomial sources over fields of constant order and small characteristic', *Theory Comput.*, **9** (2013), 665–683.

[3] E. Ben-Sasson and S. Kopparty, 'Affine dispersers from subspace polynomials', *Proc. 41st Annual ACM Symp. Theory of Comp.*, ACM, 2009, 65–74.

[4] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Cambridge Philos. Soc.*, **146** (2009), 1–21.

[5] B. Bukh and J. Tsimerman, 'Sum-product estimates for rational functions', *Proc. Lond. Math. Soc.*, **104** (2012), 1–26.
[6] M.-C. Chang, 'Polynomial iteration in characteristic p', *J. Functional Analysis*, **263** (2012), 3412–3421.
[7] M.-C. Chang, 'Expansions of quadratic maps in prime fields', *Proc. Amer. Math. Soc.*, **142** (2014), 85–92.
[8] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, 'Points on curves in small boxes and applications', *Michigan Math. J.*, (to appear).
[9] O. Garcia-Morchon, R. Rietman, I. E. Shparlinski and L. Tolhuizen, 'Interpolation and approximation of polynomials in finite fields over a short interval from noisy values', *Experimental Math.*, (to appear).
[10] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, 'On the concentration of points of polynomial maps and applications', *Math. Zeit.*, **272** (2012), 825–837.
[11] J. Cilleruelo and I. E. Shparlinski, 'Concentration of points on curves in finite fields', *Monatsh. Math.*, **171** (2013), 315–327.
[12] M. Z. Garaev, 'The sum-product estimate for large subsets of prime fields', *Proc. Amer. Math. Soc.*, **136** (2008), 2735–2739.
[13] D. Gómez-Pérez and I. E. Shparlinski, 'Subgroups generated by rational functions in finite fields', *Preprint*, 2013 (available from `http://arxiv.org/abs/1309.7378`).
[14] J. Gutierrez and I. E. Shparlinski, 'Expansion of orbits of some dynamical systems over finite fields', *Bull. Aust. Math. Soc.*, **82** (2010), 232–239.
[15] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum', *Quart. J. Math.*, **51** (2000), 221–235.
[16] L. Li and O. Roche-Newton, 'An improved sum-product estimate for general finite fields', *SIAM J. Discr. Math.*, **25** (2011), 1285–1296.
[17] S. Mattarei, 'Inverse-closed additive subgroups of fields', *Isr. J. Math.*, **159** (2007), 343–347.
[18] S. Mattarei, 'A property of the inverse of a subspace of a finite field', *Finite Fields and Their Appl.*, **29** (2014), 268–274.
[19] O. Roche-Newton, 'Sum-ratio estimates over arbitrary finite fields', *Preprint*, 2014 (available from `http://arxiv.org/abs/1407.1654`).
[20] I. Z. Ruzsa, 'Sumsets and structure', *Combinatorial Number Theory and Additive Group Theory*, Birkhäuser, 2009, 87–210.
[21] I. D. Shkredov, 'Some new inequalities in additive combinatorics', *Moscow J. Comb. and Number Theory*, (to appear).
[22] I. D. Shkredov, 'On exponential sums over multiplicative subgroups of medium size', *Preprint*, 2013 (available from `http://arxiv.org/abs/1311.5726`).
[23] I. E. Shparlinski, 'Groups generated by iterations of polynomials over finite fields', *Proc. Edinburgh Math. Soc.*, (to appear).
[24] I. E. Shparlinski, 'Polynomial values in small subgroups of finite fields', *Preprint*, 2014 (available from `http://arxiv.org/abs/1401.0964`).
[25] J. H. Silverman and B. Viray, 'On a uniform bound for the number of exceptional linear subvarieties in the dynamical Mordell-Lang conjecture', *Math. Res. Letters.*, **20** (2013), 547–566.

[26] L. A. Vinh, 'The Szeméredi–Trotter type theorem and the sum-product estimate in finite fields', *European J. Combin.*, **32** (2011), 1177–1181.

Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, 4040 Linz, Austria
E-mail address: o.rochenewton@gmail.com

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: igor.shparlinski@unsw.edu.au