Bull. Aust. Math. Soc. **82** (2010), 232–239
doi:10.1017/S0004972709001270

EXPANSION OF ORBITS OF SOME DYNAMICAL SYSTEMS OVER FINITE FIELDS

JAIME GUTIERREZ and IGOR E. SHPARLINSKI ✉

(Received 23 November 2009)

Abstract

Given a finite field $\mathbb{F}_p = \{0, \ldots, p-1\}$ of p elements, where p is a prime, we consider the distribution of elements in the orbits of a transformation $\xi \mapsto \psi(\xi)$ associated with a rational function $\psi \in \mathbb{F}_p(X)$. We use bounds of exponential sums to show that if $N \ge p^{1/2+\varepsilon}$ for some fixed ε then no N distinct consecutive elements of such an orbit are contained in any short interval, improving the trivial lower bound N on the length of such intervals. In the case of linear fractional functions

$$\psi(X) = (aX + b)/(cX + d) \in \mathbb{F}_p(X), \quad \text{with } ad \ne bc \text{ and } c \ne 0,$$

we use a different approach, based on some results of additive combinatorics due to Bourgain, that gives a nontrivial lower bound for essentially any admissible value of N.

2000 *Mathematics subject classification*: primary 11A07; secondary 11L40, 37A45, 37P05.
Keywords and phrases: dynamical systems, orbits, exponential sums, additive combinatorics.

1. Introduction

For a prime p we denote by $\mathbb{F}_p$ the finite field of p elements which we assume to be represented by the set $\{0, \ldots, p-1\}$.

Given a rational function $\psi \in \mathbb{F}_p(X)$, we consider the distribution of elements in the orbits of a transformation $\xi \mapsto \psi(\xi)$. More precisely, for $u \in \mathbb{F}_p$ we consider the orbit

$$u_0 = u, \quad u_{n+1} = \psi(u_n), \ n = 0, 1, \ldots,$$

which we terminate if u_n is a pole of ψ. Clearly any orbit of ψ (as of any other transformation of a finite set) either terminates or eventually becomes periodic.

Given $u \in \mathbb{F}_p$, we consider the sequence (u_n) as a dynamical system on $\mathbb{F}_p$ and study how far it propagates in N steps. That is, we study

$$L_u(N) = \max_{0 \le n \le N} |u_n - u|.$$

During the preparation of this paper, the first author was supported in part by Spain Ministry of Education and Science Grant MTM2007-67088 and the second author by the Australian Research Council Grant DP0556431.

Let T_u be the smallest positive integer T with

$$\{u_n : n = 0, \dots, T-1\} = \{u_n : u_n \text{ is defined}, n = 0, 1, \dots\}.$$

Trivially, for any $u \in \mathbb{F}_p$ and $N < T_u$ we have $L_u(N) \geq N$. Here we use bounds of exponential sums to show that $L_u(N) = p^{1+o(1)}$, provided that $T_u \geq N \geq p^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$.

Furthermore, for linear fractional functions $\psi(X) = (aX + b)/(cX + d) \in \mathbb{F}_p(X)$ with $ad \neq bc$ we use a different approach, based on some results of additive combinatorics due to Bourgain [1], to obtain a bound which is nontrivial for essentially any N.

Finally, we discuss some possible improvements and applications of both methods used in this paper.

Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may depend on a real parameter ε, an integer parameter $\nu \geq 2$ and the degree of the rational function ψ. We recall that $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \leq C_0 V$ holds with some constant $C_0 > 0$.

2. Preliminaries

2.1. Linear independence of iterates. The result we present here is more general than we need, but we hope it may be of independent interest.

Let $\mathbb{K}$ be an arbitrary field. We denote by $\mathcal{R} \subseteq \mathbb{K}(X)$ the set of all nonconstant rational functions. This set is a semigroup with identity X, under the composition of rational functions; that is, given $r(X), s(X) \in \mathcal{R}$, then $r(s(X)) \in \mathcal{R}$.

Furthermore, if

$$w(X) = \frac{f(X)}{g(X)} \in \mathcal{R}$$

is such that $f(X), g(X) \in \mathbb{K}[X]$ are relatively prime polynomials, we say that $w(X)$ is in the *prime form*. In this case, we define the degree of w as the maximum of the degrees of f and g, that is, $\deg w = \max\{\deg f, \deg g\}$. Thus the degree of rational functions always means the degree of the corresponding prime form. It is easy to verify that if $v(X) = r(s(X))$ for $r(X), s(X) \in \mathcal{R}$, then $\deg v = \deg r \cdot \deg s$.

As usual, we define the degree of the identically zero rational function as -1, and the degree of any other constant rational function as 0.

We define the sequence of iterates $w_0(X) = X$ and

$$w_{n+1}(X) = w(w_n(X)), \quad n = 0, 1, \dots.$$

LEMMA 1. *With the above notation, let* $r(X), w(X) \in \mathcal{R}$ *and let* $\deg w > 1$. *Then, the rational functions*

$$r_{-1}(X) = 1, \quad r_0(X) = X, \quad r_i(X) = r(w_i(X)), \ i = 1, \dots, m,$$

are linearly independent over $\mathbb{K}$.

https://doi.org/10.1017/S0004972709001270 Published online by Cambridge University Press

PROOF. Suppose that for some $a_i \in \mathbb{K}$, $i = -1, 0, 1, \ldots, m$,

$$a_{-1} + a_0 X + \sum_{i=1}^{m} a_i r_i(X) = 0.$$

Without loss of generality we can assume that $a_m \neq 0$. Then

$$a_{-1} + a_0 X + \sum_{i=1}^{m-1} a_i r(w_i(X)) = -a_m r(w_m(X)).$$

We write

$$r_i(X) = r(w_i(X)) = \frac{f_i(X)}{g_i(X)},$$

and then derive

$$a_{-1} + a_0 X + \sum_{i=1}^{m-1} a_i \frac{f_i(X)}{g_i(X)} = \frac{f(X)}{g(X)} = -a_m \frac{f_m(X)}{g_m(X)}, \tag{1}$$

where

$$f(X) = a_{-1} \prod_{j=1}^{m-1} g_i(X) + a_0 X \prod_{j=1}^{m-1} g_i(X) + \sum_{i=1}^{m-1} a_i f_i(X) \prod_{\substack{j=1 \\ j \neq i}}^{m-1} g_j(X)$$

and

$$g(X) = \prod_{j=1}^{m-1} g_j(X).$$

Let $s = \deg w > 1$. Since the degree of rational functions is multiplicative with respect to the composition, we have $\deg r_i = s^i \deg r$, $i = 0, 1, \ldots, m$. Hence,

$$\deg f \leq (1 + s + \cdots + s^{m-1}) \deg r \quad \text{and} \quad \deg g \leq (1 + s + \cdots + s^{m-1}) \deg r.$$

From (1), we obtain

$$\deg \frac{f}{g} \leq (1 + s + s^2 + \cdots + s^{m-1}) \deg r. \tag{2}$$

On the other hand, also from (1), we obtain

$$\deg \frac{f}{g} = \deg a_m \frac{f_m}{g_m} = s^m \deg r \tag{3}$$

(since $a_m \neq 0$). However, the bounds (2) and (3) are contradictory, because $1 + s + s^2 + \cdots + s^{m-1} < s^m$ if $s > 1$, which concludes the proof. □

2.2. Discrepancy. Given a sequence Γ of M points

$$\Gamma = \left\{ (\gamma_{m,1}, \ldots, \gamma_{m,\nu})_{m=0}^{M-1} \right\} \tag{4}$$

https://doi.org/10.1017/S0004972709001270 Published online by Cambridge University Press

in the ν-dimensional unit torus $\mathcal{T}^\nu = (\mathbb{R}/\mathbb{Z})^\nu$, it is natural to measure the level of its statistical uniformity in terms of the *discrepancy* $\Delta(\Gamma)$. More precisely,

$$\Delta(\Gamma) = \sup_{B \subseteq [0,1)^\nu} \left| \frac{T_\Gamma(B)}{M} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of Γ inside the box

$$B = [\alpha_1, \beta_1) \times \cdots \times [\alpha_\nu, \beta_\nu) \subseteq \mathcal{T}^\nu$$

and the supremum is taken over all such boxes (see [5, 9]).

Typically the bounds on the discrepancy of a sequence are derived from bounds of exponential sums with elements of this sequence. The relation is made explicit in the celebrated *Erdős–Turan–Koksma inequality* (see [5, Theorem 1.21]), which we present in the following form.

LEMMA 2. *For any integer $H > 1$ and any sequence Γ of N points (4) the discrepancy $\Delta(\Gamma)$ satisfies the following bound:*

$$\Delta(\Gamma) = O\left(\frac{1}{H} + \frac{1}{M} \sum_{0 < |\mathbf{h}| \le H} \prod_{j=1}^{\nu} \frac{1}{|h_j| + 1} \left| \sum_{m=0}^{M-1} \exp\left(2\pi i \sum_{j=1}^{\nu} h_j \gamma_{m,j} \right) \right| \right)$$

where the sum is taken over all integer vectors $\mathbf{h} = (h_1, \ldots, h_\nu) \in \mathbb{Z}^\nu$ with $|\mathbf{h}| = \max_{j=1,\ldots,\nu} |h_j| < H$.

2.3. Exponential sums. In our applications of Lemma 2 we use the Weil bound on exponential sums that we present in the following form given by [10, Theorem 2].

LEMMA 3. *For any polynomials $f, g \in \mathbb{F}_p[X]$ over a field $\mathbb{F}_p$ of p elements, such that the rational function $F(X) = f(X)/g(X)$ is nonconstant on $\mathbb{F}_p$, we have the bound*

$$\left| \sum_{\substack{x \in \mathbb{F}_p \\ g(x) \ne 0}} \mathbf{e}_p(F(x)) \right| \le (\max(\deg f, \deg g) + r - 2) p^{1/2} + \delta,$$

where

$$(r, \delta) = \begin{cases} (s, 1) & \text{if } \deg f \le \deg g, \\ (s+1, 0) & \text{if } \deg f > \deg g, \end{cases}$$

and s is the number of distinct zeros of $g(X)$ in the algebraic closure of $\mathbb{F}_p$.

As before, we write $\psi_0(X) = X$ and

$$\psi_{n+1}(X) = \psi(\psi_n(X)), \quad n = 0, 1, \ldots.$$

We now combine Lemmas 1 and 3 to derive the following lemma.

https://doi.org/10.1017/S0004972709001270 Published online by Cambridge University Press

LEMMA 4. *For any fixed $\nu \ge 2$ nonconstant and nonlinear rational function $\psi \in \mathbb{F}_p(X)$, and all integers $h_0, \ldots, h_{\nu-1}$ with* $\gcd(h_0, \ldots, h_{\nu-1}) = 1$,

$$\sum_{u \in \mathcal{U}_\nu} \exp\left(\frac{2\pi i}{p} \sum_{i=0}^{\nu-1} h_i \psi_i(u)\right) \ll p^{1/2},$$

where $\mathcal{U}_\nu \subseteq \mathbb{F}_p$ is the set of $u \in \mathbb{F}_p$ which are not the poles of any of the functions ψ_i, $i = 0, \ldots, \nu - 1$.

2.4. Additive combinatorics. For a set $\mathcal{A} \subseteq \mathbb{F}_p^*$ we define the sets

$$\mathcal{A} + \mathcal{A} = \{a_1 + a_2 : a_1, a_2 \in \mathcal{A}\},$$
$$\mathcal{A}^{-1} + \mathcal{A}^{-1} = \{a_1^{-1} + a_2^{-1} : a_1, a_2 \in \mathcal{A}\}.$$

In the case of linear fractional functions, our bound on $L_u(N)$ depends on the following result of Bourgain [1, Theorem 4.1].

LEMMA 5. *For any $\varepsilon > 0$ there exists $\delta > 0$ such for any set $\mathcal{A} \subseteq \mathbb{F}_p^*$ of cardinality $\#\mathcal{A} \le p^{1-\varepsilon}$,*

$$\max\{\#(\mathcal{A} + \mathcal{A}), \#(\mathcal{A}^{-1} + \mathcal{A}^{-1})\} \gg (\#\mathcal{A})^{1+\delta}.$$

3. Main results

3.1. General rational functions.

THEOREM 6. *For every fixed $\nu \ge 2$ there exist positive constants $C_1(\nu)$ and $C_2(\nu)$ such that for any rational function $\psi \in \mathbb{F}_p(X)$ of degree* $\deg \psi > 1$ *and initial value $u \in \mathbb{F}_p$,*

$$L_u(N) \ge C_1(\nu) N^{1/\nu} p^{1-1/\nu},$$

provided that $T_u \ge N \ge C_2(\nu) p^{1/2} (\log p)^\nu$.

PROOF. As before, we write $\mathcal{T}^\nu = (\mathbb{R}/\mathbb{Z})^\nu$ and also define $\mathcal{U}_\nu \subseteq \mathbb{F}_p$ as the set of $u \in \mathbb{F}_p$ which are not poles of any of the functions ψ_i, $i = 0, \ldots, \nu - 1$. It follows immediately from a combination of Lemma 2 (applied with $M = H = p$) and Lemma 4 that the discrepancy Δ_ν of the point set

$$\left(\frac{u}{p}, \frac{\psi(u)}{p}, \ldots, \frac{\psi_{\nu-1}(u)}{p}\right) \in \mathcal{T}^\nu, \quad u \in \mathcal{U}_\nu,$$

satisfies $\Delta_n u = O(p^{-1/2} (\log p)^\nu)$.

Therefore, for any $\lambda \ge 1$ there are

$$p\lambda^\nu + O(p\Delta_n u) = p\lambda^\nu + O(p^{1/2} (\log p)^\nu)$$

values of $u \in \mathcal{U}_\nu$ such that the vector

$$\left(\frac{u}{p}, \frac{\psi(u)}{p}, \ldots, \frac{\psi_{\nu-1}(u)}{p}\right) \in \mathcal{T}^\nu$$

belongs to a given cube $\mathcal{B} \subseteq \mathcal{T}^\nu$ with side length λ.

https://doi.org/10.1017/S0004972709001270 Published online by Cambridge University Press

We now consider the vectors

$$\left(\frac{u_n}{p}, \frac{\psi(u_n)}{p}, \dots, \frac{\psi_{\nu-1}(u_n)}{p}\right), \quad 0 \le n \le N-\nu.$$

Clearly these all belong to a certain ν-dimensional cube inside $\mathcal{T}_\nu$ with side length $2L_u(N)/p$. Therefore

$$N - \nu \le p(L_u(N)/p)^\nu + O(p^{1/2}(\log p)^\nu)$$

which concludes the proof. □

In particular, we see that if for some fixed $\varepsilon > 0$ we have $T_u \ge N \ge p^{1/2+\varepsilon}$ then, taking ν as a slowly increasing function of p, we derive from Theorem 6 that $L_u(N) = p^{1+o(1)}$.

3.2. Linear fractional functions. We now use arguments similar to those of [4] to establish a better bound for linear fractional functions. That is, we essentially consider orbits of transformations

$$\xi \mapsto \frac{a\xi + b}{c\xi + d}$$

corresponding to the matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(p).$$

THEOREM 7. *For any $\varepsilon > 0$ there exists an absolute constant $\delta > 0$ such that, for every linear fractional function $\psi(X) = (aX + b)/(cX + d) \in \mathbb{F}_p(X)$ with $ad \ne bc$ and $c \ne 0$, and initial value $u \in \mathbb{F}_p$,*

$$L_u(N) \gg N^{1+\delta},$$

provided $N \le \min\{T_u, p^{1-\varepsilon}\}$.

PROOF. We consider the set

$$\mathcal{A} = \{cu_n + d : 0 \le n \le N-1\} \subseteq \mathbb{F}_p.$$

In particular, since $N < T_u$,

$$\#\mathcal{A} = N. \tag{5}$$

Clearly there exists an interval of length at most $2L_u(N-1) \le 2L_u(N)$ which contains all elements u_n, $0 \le n \le N$. Thus it is easy to see that

$$\#(\mathcal{A} + \mathcal{A}) \le 2L_u(N) + 1. \tag{6}$$

Furthermore,

$$u_{n+1} = \frac{au_n + b}{cu_n + d} = ac^{-1} + \frac{b - ac^{-1}d}{cu_n + d}.$$

Since we have $ad \ne bc$, this can be written as

$$\frac{1}{cu_n + d} = \frac{cu_{n+1} - a}{bc - ad}.$$

https://doi.org/10.1017/S0004972709001270 Published online by Cambridge University Press

Therefore, we also have

$$\#(\mathcal{A}^{-1} + \mathcal{A}^{-1}) \le 2L_u(N) + 1. \tag{7}$$

We now see that (5), (6) and (7), combined with Lemma 5, imply the desired result. □

4. Comments

The requirement that $\deg \psi > 1$ in Theorem 6 excludes linear fractional functions from the class of functions to which it applies. However, they can easily be studied by the same method with an almost identical result.

Unfortunately, Theorem 6 applies only to orbits of length of order at least $p^{1/2}(\log p)^2$. In fact, using a well-known 'symmetrization' technique, one can easily remove the logarithmic factors from the restriction on N.

On the other hand, it is well known that the 'birthday paradox' usually leads to orbits of length of order $p^{1/2}$. Obtaining nontrivial estimates for such short orbits of this length is an important open question. In fact, if ψ is a polynomial then instead of the Weil bound one can use bounds of short of exponential sums obtained by the Vinogradov method (see [8, Theorem 17]). For instance, if ψ is a polynomial of degree d then this approach allows us to obtain nontrivial results in the range $T_u \ge N \ge p^{1/(d-1)+\varepsilon}$ for any fixed $\varepsilon > 0$. Thus for $d \ge 4$ it is already within the 'typical' cycle length.

The case of the affine map $x \mapsto ax + b$ is certainly of great interest. One can use various bounds of exponential sums with exponential functions (see [2, 3, 6, 7]) to obtain several versions of Theorem 6. Furthermore, it is feasible that a variant of the geometry of numbers argument used in the proof of [7, Theorem 4.2] can also be used to study the expansion of the affine map.

Finally, one can also apply similar arguments to many other maps, for example to the map $x \mapsto g^x$ for some fixed element $g \in \mathbb{F}_p$ (where x in the exponent is treated as an integer in the range $0 \le x \le p - 1$). For the analogue of the approach of Theorem 6 one can use the bounds of [2, 3, 6, 7]. For the analogue of the approach of Theorem 7 one can use a result of Bourgain and Garaev [3] in the same way as in [4, Theorem 4].

References

[1] J. Bourgain, 'More on the sum–product phenomenon in prime fields and its applications', *Int. J. Number Theory* **1** (2005), 1–32.
[2] J. Bourgain, 'Multilinear exponential sums in prime fields under optimal entropy condition on the sources', *Geom. Funct. Anal.* **18** (2009), 1477–1502.
[3] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Camb. Phil. Soc.* **146** (2008), 1–21.
[4] T. H. Chan and I. E. Shparlinski, On the concentration of points on modular hyperbolas and exponential curves, *Acta Arith.*, to appear.
[5] M. Drmota and R. Tichy, *Sequences, Discrepancies and Applications* (Springer, Berlin, 1997).

https://doi.org/10.1017/S0004972709001270 Published online by Cambridge University Press

[6] S. V. Konyagin, 'Bounds of exponential sums over subgroups and Gauss sums', *Proc. 4th Int. Conf. Modern Problems of Number Theory and its Applications* (Moscow Lomonosov State University, Moscow, 2002), pp. 86–114 (in Russian).
[7] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and their Applications* (Cambridge University Press, Cambridge, 1999).
[8] N. M. Korobov, *Exponential Sums and their Applications* (Kluwer, Dordrecht, 1992).
[9] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences* (Wiley-Interscience, New York, 1974).
[10] C. J. Moreno and O. Moreno, 'Exponential sums and Goppa codes I', *Proc. Amer. Math. Soc.* **111** (1991), 523–531.

JAIME GUTIERREZ, Department of Applied Mathematics and Computer Science, University of Cantabria, E-39071 Santander, Spain
e-mail: jaime.gutierrez@unican.es

IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@comp.mq.edu.au

https://doi.org/10.1017/S0004972709001270 Published online by Cambridge University Press