Fractional jumps: complete characterisation and an explicit infinite family*

Federico Amadio Guidi[1] and Giacomo Micheli[2]

[1] Mathematical Institute, University of Oxford, Oxford, UK
federico.amadio@maths.ox.ac.uk
[2] Mathematical Institute, University of Oxford, Oxford, UK
giacomo.micheli@maths.ox.ac.uk

Abstract. In this paper we provide a complete characterisation of transitive fractional jumps by showing that they can only arise from transitive projective automorphisms. Furthermore, we prove that such construction is feasible for arbitrarily large dimension by exhibiting an infinite class of projectively primitive polynomials whose companion matrix can be used to define a full orbit sequence over an affine space.

1 Introduction

The study of dynamical systems over finite fields have a long history (see for example [2, 4, 5, 6, 9, 12, 13, 18]) and is an interesting and still hot topic (see for example [7, 8, 10, 14, 15, 16, 17, 19]), both for its number theoretical impact in finite fields theory, and for its practical applications, in particular for random number generation.

Let q be a prime power, let $\mathbb{F}_q$ denote the finite field with q elements, and let m be a positive integer. One of the most interesting questions for applications consists of constructing sequences over the m-dimensional affine space over $\mathbb{F}_q$ defined by iterations of rational maps $f : \mathbb{F}_q^m \to \mathbb{F}_q^m$ satisfying the following conditions:

1. The period of the recursive sequence $\{f^k(0)\}_{k\in\mathbb{N}}$ they define is "long".
2. Their iterations as rational maps have "low degree growth".

* The second author would like to thank the Swiss National Science Foundation grant number 171248.

The motivation for (1) is rather clear: since we generally want to use these sequences for pseudorandom number generation, we do not want to revisit an element twice too soon, or otherwise the entire sequence will repeat. The motivation for (2) is a little more subtle and comes from the uniformity conditions we want the sequence to satisfy (for additional information on this see [16]).

In [1] we introduced the theory of fractional jumps to address this problem by showing a natural way to build full orbit sequences from projective automorphisms, recovering as a particular case the construction of the Inversive Congruential Generator.

In this paper we complete the theory of fractional jumps by both proving the uniqueness of the construction, i.e. transitive fractional jumps can only arise from transitive projective automorphisms (except from a couple of degenerate cases which we entirely classify), and by providing an explicit infinite class of projectively primitive polynomials, see definition [1, Definition 3.1], whose companion matrix can be used to define a full orbit sequence over $\mathbb{F}_p^{p-1}$, for p a prime. For this family of fractional jumps, which we call *Artin-Schreier fractional jumps*, we show that the computation of the $(k+1)$-th affine point of the full orbit sequence they define, given the k-th one, is as expensive as reading out a look-up table once for each entry.

This latter construction entirely addresses points (1) and (2) above, since the corresponding sequences have full orbit (they cover the entire affine space) and they have zero degree growth. The main technique we use is the fractional jump construction provided in [1].

1.1 Notation

We denote by $\mathbb{N}$ the set of natural numbers, and by $\mathbb{Z}$ the set of integers. Given $a \in \mathbb{Z}$, we let $\mathbb{Z}_{\geq a}$ denote the set of integers $k \in \mathbb{Z}$ such that $k \geq a$.

Given a commutative ring with unity R, we let R^* be the (multiplicative) group of invertible elements in R.

For a prime power q, we denote by $\mathbb{F}_q$ the finite field of cardinality q. For $m \in \mathbb{N}$, we denote the m-dimensional affine space $\mathbb{F}_q^m$ by $\mathbb{A}^m$, and the m-dimensional projective space over $\mathbb{F}_q$ by $\mathbb{P}^m$. More generally, for any vector space V over $\mathbb{F}_q$ we denote by $\mathbb{P}V$ the projectivisation of V. Also, we denote by $\mathbb{F}_q[x_1, \ldots, x_m]$ the ring of polynomials in m variables with coefficients in $\mathbb{F}_q$.

For $m \in \mathbb{N}$, let us denote by $\mathrm{GL}_m(\mathbb{F}_q)$ the general linear group over $\mathbb{F}_q$, that is the group of $m \times m$ invertible matrices with entries in $\mathbb{F}_q$. Also, we denote by $\mathrm{PGL}_m(\mathbb{F}_q)$ the group of automorphisms of $\mathbb{P}^{m-1}$. Recall that $\mathrm{PGL}_m(\mathbb{F}_q)$ can be identified with the quotient group $\mathrm{GL}_m(\mathbb{F}_q)/\mathbb{F}_q^*\mathrm{Id}_m$, where $\mathbb{F}_q^*\mathrm{Id}$ is the subgroup of $\mathbb{F}_q^*$-multiples of the identity matrix Id_m. For $M \in \mathrm{GL}_m(\mathbb{F}_q)$, we denote by $[M]$ its class in $\mathrm{PGL}_m(\mathbb{F}_q)$.

We say that a polynomial $\chi(T) \in \mathbb{F}_q[T]$ of degree $\deg \chi(T) = d$ is *projectively primitive* if it is irreducible and if given any root α in $\mathbb{F}_{q^d} \cong \mathbb{F}_q[T]/(\chi(T))$ the class $\overline{\alpha}$ of α in the quotient group $G = \mathbb{F}_{q^d}^*/\mathbb{F}_q^*$ generates G.

Let X be a set, and let G be a group acting on it. For any $x \in X$ we denote by $\mathcal{O}_G(x)$ the orbit of x with respect to the action of G on X. Given a bijective map $f : X \to X$, for any $x \in X$ we set $\mathcal{O}_f(x) = \mathcal{O}_{\langle f \rangle}(x)$, where $\langle f \rangle$ denotes the cyclic subgroup of the group of maps from X to itself generated by f, and we define $o_f(x) = |\mathcal{O}_f(x)|$. We say that a bijective map $f : X \to X$ *acts transitively* on X, or simply that it is *transitive*, if for any $x, y \in X$ there exists $k \in \mathbb{Z}$ such that $y = f^k(x)$. Equivalently, f acts transitively on X if and only if for any $x_0 \in X$, the f-orbit of x_0 has size $o_f(x_0) = |X|$. Finally, we say that a sequence $\{x_k\}_{k\in\mathbb{N}}$ in X has *full orbit* if $\{x_k : k \in \mathbb{N}\} = X$.

2 Transitive fractional jumps

For the sake of completeness, we recall the definition of fractional jump of a projective automorphism, as introduced in [1].

Fix the standard projective coordinates $X_0, \ldots, X_n$ on $\mathbb{P}^n$, and fix the canonical decomposition

$$\mathbb{P}^n = U \cup H,$$

where

$$U = \{[X_0 : \ldots : X_n] \in \mathbb{P}^n \, : \, X_n \neq 0\},$$
$$H = \{[X_0 : \ldots : X_n] \in \mathbb{P}^n \, : \, X_n = 0\}.$$

Fix also the isomorphism

$$\pi : \mathbb{A}^n \xrightarrow{\sim} U, \quad (x_1, \ldots, x_n) \mapsto [x_1 : \ldots : x_n : 1].$$

Let now Ψ be an automorphism of $\mathbb{P}^n$. For $P \in U$, we define the *fractional jump index of* Ψ *at* P as

$$\mathfrak{J}_P = \min\left\{k \in \mathbb{Z}_{\geq 1} \,:\, \Psi^k(P) \in U\right\}.$$

The *fractional jump of* Ψ is then defined as the map

$$\psi : \mathbb{A}^n \to \mathbb{A}^n, \quad x \mapsto \pi^{-1}\Psi^{\mathfrak{J}_{\pi(x)}}\pi(x).$$

Essentially, the map ψ is defined on a point $x \in \mathbb{A}^n$ as follows: we firstly send x in $\mathbb{P}^n$ via the canonical map π, then we iterate Ψ on $\pi(x)$ until we end up with a point in U, and finally we take its image in $\mathbb{A}^n$ via π^{-1}.

When Ψ acts transitively on $\mathbb{P}^n$, its fractional jump ψ admits an explicit description in terms of multivariate linear fractional transformations. More precisely, we have the following:

Theorem 1 ([1, Section 5]). *Let Ψ be a transitive automorphism of $\mathbb{P}^n$, and let ψ be its fractional jump. Then, for $i \in \{1, \dots, n+1\}$ there exist*

$$a_1^{(i)}, \dots, a_n^{(i)}, b^{(i)} \in \mathbb{F}_q[x_1, \dots, x_n]$$

of degree 1 *such that, if*

$$\begin{aligned}
U_1 &= \left\{x \in \mathbb{A}^n \,:\, b^{(1)}(x) \neq 0\right\},\\
U_i &= \left\{x \in \mathbb{A}^n \,:\, b^{(i)}(x) \neq 0, \text{ and } b^{(j)}(x) = 0,\, \forall j \in \{1, \dots, i-1\}\right\},\\
&\quad \text{for } i \in \{2, \dots, n+1\},\\
&\quad \text{and}\\
f^{(i)} &= \left(\frac{a_1^{(i)}}{b^{(i)}}, \dots, \frac{a_n^{(i)}}{b^{(i)}}\right),\\
&\quad \text{for } i \in \{1, \dots, n+1\},
\end{aligned}$$

then $\psi(x) = f^{(i)}(x)$ if $x \in U_i$. Moreover, the rational maps $f^{(i)}$ can be explicitly computed.

Proof (sketch). Let us denote by K the field $\mathbb{F}_q(x_1, \dots, x_n)$ of rational functions on $\mathbb{A}^n$. We construct a map

$$\imath : \mathrm{PGL}_{n+1}(\mathbb{F}_q) \to K^n$$

in the following way. Let $\Phi \in \mathrm{PGL}_{n+1}(\mathbb{F}_q)$, and write

$$\Phi = [F_0 : \ldots : F_n],$$

for $F_0, \ldots, F_n \in \mathbb{F}_q[X_0, \ldots, X_n]$ homogeneous polynomials of degree 1. Define then $\imath(\Phi) \in K^n$ to be the n-tuple of elements of K whose j-th entry for $j \in \{1, \ldots, n\}$ is given by

$$\imath(\Phi)_j = \frac{F_{j-1}(x_1, \ldots, x_n, 1)}{F_n(x_1, \ldots, x_n, 1)}.$$

It is immediate to check that $\imath$ is well defined, that for any $f = (f_1, \ldots, f_n)$ in the image of $\imath$ all the f_j's are rational functions of degree 1, whose denominators are all equal up to a non-zero constants, and that $\imath(\Phi_1 \circ \Phi_2) = \imath(\Phi_1) \circ \imath(\Phi_2)$, where $\imath(\Phi_1) \circ \imath(\Phi_2)$ is simply defined by plugging in the components of $\imath(\Phi_2)$ into the variables of $\imath(\Phi_1)$.

Let now $\Psi \in \mathrm{PGL}_{n+1}(\mathbb{F}_q)$ be transitive. Define $f^{(i)} = \imath(\Psi^i)$ for $i \in \mathbb{Z}_{\geq 1}$. Then, by construction for any $i \in \mathbb{Z}_{\geq 1}$ there exist $a_1^{(i)}, \ldots, a_n^{(i)}, b^{(i)} \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree 1 such that

$$f^{(i)} = \left(\frac{a_1^{(i)}}{b^{(i)}}, \ldots, \frac{a_n^{(i)}}{b^{(i)}} \right).$$

It can be proved, see [1, Section 5] for the details, that the transitivity of Ψ implies that

$$\bigcap_{i=1}^{n+2} \left\{ x \in \mathbb{A}^n \,:\, b^{(i)}(x) = 0 \right\} = \emptyset. \tag{2.1}$$

Define then

$$\begin{aligned} U_1 &= \left\{ x \in \mathbb{A}^n \,:\, b^{(1)}(x) \neq 0 \right\}, \\ U_i &= \left\{ x \in \mathbb{A}^n \,:\, b^{(i)}(x) \neq 0, \text{ and } b^{(j)}(x) = 0, \forall j \in \{1, \ldots, i-1\} \right\}, \\ &\quad \text{for } i \in \{2, \ldots, n+1\}. \end{aligned}$$

By (2.1) we have that $\{U_i\}_{i \in \{1,\ldots,n+1\}}$ is a disjoint covering of $\mathbb{A}^n$. Also, we clearly have that $\psi(x) = f^{(i)}(x)$ if $x \in U_i$.

Remark 1. The reader should notice that the $b^{(i)}$ are equal on each component, and therefore the evaluation of ψ only requires one inversion in the base field.

Remark 2. Another important fact to notice is that the definition of ψ depends uniquely on the rows of M^i's, where $M \in \mathrm{GL}_{n+1}(\mathbb{F}_q)$ is any matrix in the class

of Ψ. In fact, notice that if the last row of M^i is $(m^{(i)}_{n+1,1}, \dots, m^{(i)}_{n+1,n+1})$, then $b^{(i)} = m^{(i)}_{n+1,n+1} + \sum_{j=1}^{n} m^{(i)}_{n+1,j} x_j$. On the other hand, for any $j \in \{1, \dots, n\}$, if $(m^{(i)}_{j,1}, \dots, m^{(i)}_{j,n+1})$ is the j-th row of M^i, then $a^{(i)}_j = m^{(i)}_{j,n+1} + \sum_{j=1}^{n} m^{(i)}_{j,n+1} x_j$. What is done here is essentially dehomogenising the projective map induced by the class of M^i and then restricting that to the affine points.

We now provide a simple example to fix the ideas.

Example 1. Let $q = 5$ and $n = 2$. Consider the automorphism of $\mathbb{P}^2$ defined by

$$\Psi([X_0 : X_1 : X_2]) = [3X_0 + 2X_1 + X_2 : 3X_0 + 3X_1 + X_2 : 3X_1 + 4X_2].$$

A representative for Ψ in $\mathrm{GL}_3(\mathbb{F}_5)$ is given by

$$M = \begin{pmatrix} 3 & 2 & 1 \\ 3 & 3 & 1 \\ 0 & 3 & 4 \end{pmatrix},$$

whose characteristic polynomial

$$\chi_M(T) = T^3 + 4T + 3$$

is projectively primitive, since it is irreducible, and $(5^3 - 1)/(5 - 1) = 31$ is prime. By [1, Theorem 3.4], it follows that Ψ acts transitively on $\mathbb{P}^2$, and then Theorem 1 applies to the fractional jump ψ of Ψ. Direct computations show that for

$$\begin{aligned} U_1 &= \left\{(x_1, x_2) \in \mathbb{A}^2 \,:\, 3x_2 + 4 \neq 0\right\}, \\ U_2 &= \left\{(x_1, x_2) \in \mathbb{A}^2 \,:\, 3x_2 + 4 = 0, \text{ and } 4x_1 + x_2 + 4 \neq 0\right\}, \\ U_3 &= \left\{(1, 2)\right\}, \end{aligned}$$

and

$$\begin{aligned} f^{(1)}(x_1, x_2) &= \left(\frac{3x_1 + 2x_2 + 1}{3x_2 + 4}, \frac{3x_1 + 3x_2 + 1}{3x_2 + 4}\right), \\ f^{(2)}(x_1, x_2) &= \left(\frac{4}{4x_1 + x_2 + 4}, \frac{3x_1 + 3x_2}{4x_1 + x_2 + 4}\right), \\ f^{(3)}(x_1, x_2) &= \left(\frac{2x_2 + 1}{3x_2 + 1}, \frac{3x_1 + 1}{3x_2 + 1}\right), \end{aligned}$$

we have that $\{U_i\}_{i \in \{1,2,3\}}$ is a disjoint covering of $\mathbb{A}^2$ such that $\psi(x) = f^{(i)}(x)$ if $x \in U_i$.

The purpose of this section is to show that transitive fractional jumps can only arise from transitive projective automorphisms, except from some very special cases, which can be entirely classified. Before proving the main theorem, let us recall a standard linear algebra fact, which follows from the results in [11, XIV, §2, §3].

Lemma 1. *Let $\Bbbk$ be a field, let V be a finite dimensional vector space over $\Bbbk$, and let M be a $\Bbbk$-linear endomorphism of V. Assume that the minimal polynomial and the characteristic polynomial of M are equal. Then, there exists $v_0 \in V$ such that the set $\left\{M^k v_0 \,:\, k \in \mathbb{Z}_{\geq 0}\right\}$ spans V over $\Bbbk$.*

We also need the following lemma:

Lemma 2. *Let $p(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial, and let $e \geq 1$ be a positive integer. Let $[T]$ be the class of T in $\Gamma = (\mathbb{F}_q[T]/(p(T)^e))^*$, and let $[[T]]$ be the class of T in $G = \Gamma/\mathbb{F}_q^*$. Then, the order of $[[T]]$ in G equals the order of $[T]^{q-1}$ in Γ.*

Proof. Let k be the order of $[[T]]$ in G and let h be the order of $[T]^{q-1}$ in Γ. Then, $[[T]]^k = 1$ in G gives $[T]^k \in \mathbb{F}_q^*$. But then $1 = ([T]^k)^{q-1} = ([T]^{q-1})^k$, and so $h \mid k$.

On the other hand, let us firstly show that if $s \in \mathbb{F}_q[T]/(p(T)^e)$ satisfies $s^{q-1} - 1 = 0$, then $s \in \mathbb{F}_q^*$. In fact, by reducing s modulo $p(T)$ we get that

$$s = c + k(T)p(T) \mod p(T)^e, \qquad \text{for } c \in \mathbb{F}_q^* \text{ and } k(T) \in \mathbb{F}_q[T].$$

Now, by multiplying the equation $s^{q-1} - 1 = 0$ by s, and plugging in the above special form for s, we get

$$\begin{aligned}(c + k(T)p(T))^q - (c + k(T)p(T)) &\equiv (k(T)p(T))^q - k(T)p(T) \\ &\equiv k(T)p(T)((k(T)p(T))^{q-1} - 1) \equiv 0 \mod p(T)^e.\end{aligned}$$

But now $k(T)p(T))^{q-1} - 1$ is invertible modulo $p(T)^e$, and so $k(T)p(T)$ must be zero modulo $p(T)^e$, which forces s to be c modulo $p(T)^e$.

It then follows that $1 = ([T]^{q-1})^h = ([T]^h)^{q-1}$ in Γ gives $[T]^h \in \mathbb{F}_q^*$, from which we get $[[T]]^h = 1$ in G, and so $k \mid h$.

The main result of this section is the following:

Theorem 2. *Let Ψ be an automorphism of $\mathbb{P}^n$ and let ψ be its fractional jump. Then, Ψ acts transitively on $\mathbb{P}^n$ if and only if ψ acts transitively on $\mathbb{A}^n$, unless q is prime and $n = 1$, or $q = 2$ and $n = 2$, with explicit examples in both cases.*

Proof. For any q and n, it is immediate to show that if Ψ is transitive then ψ is transitive. In the case of q prime and $n = 1$ or $q = 2$ and $n = 2$ there exist explicit examples of transitive affine transformations, namely

$$\begin{aligned} \varphi_1(x) &= x + 1, && \text{if } q \text{ is prime and } n = 1, \\ \varphi_2(x_1, x_2) &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix}, && \text{if } q = 2 \text{ and } n = 2. \end{aligned}$$

Define then

$$\begin{aligned} \Phi_1([X_0 : X_1]) &= [X_0 + X_1 : X_1], && \text{if } q \text{ is prime and } n = 1, \\ \Phi_2([X_0 : X_1 : X_2]) &= [X_0 + X_1 + X_2 : X_1 + X_2 : X_2], && \text{if } q = 2 \text{ and } n = 2. \end{aligned}$$

Clearly, φ_i is the fractional jump of Φ_i for $i \in \{1, 2\}$. However, it is immediate to see that Φ_i fixes the hyperplane at infinity, so cannot be transitive for $i \in \{1, 2\}$.

Let us now assume that we are not in the above pathological cases, and that ψ is transitive. Write $\Psi = [M] \in \mathrm{PGL}_{n+1}(\mathbb{F}_q)$ for some $M \in \mathrm{GL}_{n+1}(\mathbb{F}_q)$, and let $\chi_M(T), \mu_M(T) \in \mathbb{F}_q[T]$ be respectively the characteristic polynomial and the minimal polynomial of M. The vector space $V = \mathbb{F}_q^{n+1}$ over $\mathbb{F}_q$ has a natural structure of $\mathbb{F}_q[T]$-module given by

$$f(T)v = f(M)v, \quad \text{for } f(T) \in \mathbb{F}_q[T], \text{ and } v \in V.$$

Let $\mathbb{F}_q[M]$ be the subalgebra of the algebra of $\mathbb{F}_q$-linear endomorphisms of V generated by M, and let G_Ψ be the quotient (multiplicative) group $\mathbb{F}_q[M]^*/\mathbb{F}_q^*$.

We firstly prove that $\mu_M(T) = \chi_M(T)$. Assume by contradiction $\mu_M(T) \neq \chi_M(T)$, so that $\deg \mu_M(T) \leq n$. Then, given any $P \in U$, and any $x \in \mathbb{A}^n$ such that $P = \pi(x)$, we have

$$\begin{aligned} q^n = o_\psi(x) &\leq o_\Psi(P) \\ &\leq |G_\Psi| \\ &\leq \frac{q^n - 1}{q - 1} < q^n, \end{aligned}$$

a contradiction, which implies $\mu_M(T) = \chi_M(T)$.

Define now

$$N = \left\{ P \in H \,:\, \Psi^i(P) \in H,\, \forall i \in \mathbb{Z} \right\}.$$

We want to show that $N = \emptyset$. Note that this would immediately imply that Ψ is transitive. To see this, given any $P, Q \in \mathbb{P}^n$, if $N = \emptyset$ then there exist $i, j \in \mathbb{Z}$ such that $P' = \Psi^i(P), Q' = \Psi^j(Q) \in U$. Let $x', y' \in \mathbb{A}^n$ be such that $P' = \pi(x')$ and $Q' = \pi(y')$. As ψ acts transitively on $\mathbb{A}^n$ by hypothesis, there exists $\ell \in \mathbb{Z}$ such that $y' = \psi^\ell(x')$. Then, by the definition of ψ, there exists an integer $k \geq \ell$ such that $Q' = \Psi^k(P')$. In conclusion, we get $Q = \Psi^{i+k-j}(P)$, and so we have that if $N = \emptyset$ then Ψ is transitive.

Assume by contradiction that $N \neq \emptyset$. Define

$$W = \left\{ v \in V \,:\, (M^i v)_{n+1} = 0,\, \forall i \in \mathbb{Z} \right\},$$

where $(M^i v)_{n+1}$ denotes the $(n+1)$-th component of $M^i v$. It is immediate to check that W is a subspace of V, and that $N = \mathbb{P}W$. Also, W is clearly $\mathbb{F}_q[M]$-invariant, and so it is an $\mathbb{F}_q[T]$-submodule of V. Let $g(T) \in \mathbb{F}_q[T]$ is a monic generator of the annihilator $\mathrm{Ann}_{\mathbb{F}_q[T]}(W)$ of W as $\mathbb{F}_q[T]$-module. We have that $g(T) \mid \mu_M(T)$, since $\mu_M(M)w = 0$ for any $w \in W$. Also, $g(T) \neq 1$ as $N \neq \emptyset$ by assumption, and $g(T) \neq \mu_M(T)$, since $N \subseteq H$ gives $\deg g(T) \leq n$. This shows that if $N \neq \emptyset$ the $\mu_M(T)$ is reducible.

Let us now prove instead that $\mu_M(T)$ is irreducible, so that we get a contradiction. We firstly prove that $\mu_M(T) = p(T)^e$ for some irreducible polynomial $p(T) \in \mathbb{F}_q[T]$ and some integer $e \geq 1$.

Since $\mu_M(T) = \chi_M(T)$, then by Lemma 1 we know that there exists $v_0 \in V$ such that the set $\left\{ M^k v_0 \,:\, k \in \mathbb{Z}_{\geq 0} \right\}$ spans V over $\mathbb{F}_q$. Clearly, $v_0 \notin W$, since otherwise we would have $W = V$, as W is $\mathbb{F}_q[M]$-invariant, which is a contradiction as $N \subseteq H$. We show now that $d(M)v_0 \in W \setminus \{0\}$ for any $d(T) \in \mathbb{F}_q[T]$ such that $d(T) \mid \mu_M(T)$, and $d(T) \neq 1, \mu_M(T)$. Let $d(T)$ be any of such polynomials. Clearly $d(M)v_0 \neq 0$, as otherwise the span of $\left\{ M^k v_0 \,:\, k \in \mathbb{Z}_{\geq 0} \right\}$ over $\mathbb{F}_q$ would have dimension less or equal than $\deg d(T)$, which is less or equal than n by assumption. Define then W_d to be the span of $\left\{ M^k d(M) v_0 \,:\, k \in \mathbb{Z}_{\geq 0} \right\}$ over $\mathbb{F}_q$. It is immediate to see that W_d is an $\mathbb{F}_q[M]$-invariant subspace of V of dimension less or equal than $\deg(\mu_M(T)/d(T))$, which is less or equal than n by assumption. Assume by contradiction $d(M)v_0 \notin W$. Then, if we let P_d be the class of $d(M)v_0$ in $\mathbb{P}^n$, we have $P_d \notin N$, and so there exists $i \in \mathbb{Z}$ such that

$Q_d = \Psi^i(P_d) \in U$. Let $y_d \in \mathbb{A}^n$ be such that $Q_d = \pi(y_d)$. Then,

$$\begin{aligned} q^n = o_\psi(y_d) &\leq o_\Psi(Q_d) \\ &= |\mathcal{O}_\Psi(P_d)| \\ &\leq |\mathbb{P}W_d| \\ &\leq \frac{q^n - 1}{q - 1} < q^n, \end{aligned}$$

a contradiction. This proves that $d(M)v_0 \in W \setminus \{0\}$ for any $d(T) \in \mathbb{F}_q[T]$ such that $d(T) \mid \mu_M(T)$, and $d(T) \neq 1, \mu_M(T)$.

Recall that we want to prove that $\mu_M(T) = p(T)^e$ for some irreducible polynomial $p(T) \in \mathbb{F}_q[T]$ and some integer $e \geq 1$. Assume then by contradiction that there exist $p_1(T), p_2(T) \in \mathbb{F}_q[T]$ distinct irreducible polynomials such that $p_1(T), p_2(T) \mid \mu_M(T)$. Then, by Bézout's identity, there exist $a(T), b(T) \in \mathbb{F}_q[T]$ such that $a(T)p_1(T)+b(T)p_2(T) = 1$, and so $a(M)p_1(M)v_0+b(M)p_2(M)v_0 = v_0$. Now, $p_i(M)v_0 \in W$ for $i \in \{1, 2\}$ by the claim above, and so $v_0 \in W$, as W is an $\mathbb{F}_q[M]$-invariant subspace of W, which is a contradiction. Therefore, we conclude that $\mu_M(T) = p(T)^e$ for some irreducible $p(T) \in \mathbb{F}_q[T]$ and some $e \geq 1$.

We finally show that $\mu_M(T)$ is irreducible, that is $e = 1$. Let us set $f = \deg p(T)$, and let $[[T]]$ be the class of T in G_Ψ. We want to show that the order of $[[T]]$ in G_Ψ divides

$$A(q, e, f) = q^{\lceil \log_q e \rceil} \frac{q^f - 1}{q - 1}.$$

Let $[T]$ be the class of T in $\mathbb{F}_q[M]^*$. As $\mathbb{F}_q[M]^* \cong (\mathbb{F}_q[T]/(p(T)^e))^*$, by Lemma 2 it is enough to show that the order of $[T]^{q-1}$ in $\mathbb{F}_q[M]^*$ divides $A(q, e, f)$. Now, since $[T]^{q^f-1} \equiv 1 \mod p(T)$, we have $[T]^{q^f-1} = 1 + k(T)p(T)$ for some $k(T) \in \mathbb{F}_q[T]$, and so

$$\begin{aligned} ([T]^{q-1})^{A(q,e,f)} &= ([T]^{q^f-1})^{q^{\lceil \log_q e \rceil}} \\ &= [1 + k(T)p(T)]^{q^{\lceil \log_q e \rceil}} \\ &= [1 + k(T)^{q^{\lceil \log_q e \rceil}} p(T)^{q^{\lceil \log_q e \rceil}}] = 1 \quad \text{in } \mathbb{F}_q[M]^*, \end{aligned}$$

as $q^{\lceil \log_q e \rceil} \geq e$.

Let $P \in U$, and let $x \in \mathbb{A}^n$ be such that $P = \pi(x)$. Then

$$\begin{aligned} q^n = o_\psi(x) &\leq o_\Psi(P) \\ &\leq A(q, e, f), \end{aligned}$$

since the size of $\mathcal{O}_\Psi(P)$ is less or equal than the order of $[[T]]$ in G_Ψ. Notice also that here $n = ef - 1$, since $\mu_M(T) = p(T)^e$ and $f = \deg p(T)$.

Assume by contradiction that $e \geq 2$. We firstly prove that this forces $f = 1$. Rewrite the inequality $q^{ef-1} \leq A(q, e, f)$ as

$$q^{ef-1-\lceil \log_q e \rceil} \leq \frac{q^f - 1}{q - 1}. \tag{2.2}$$

Since the quantity

$$q^{ef-1-\lceil \log_q e \rceil} - \frac{q^f - 1}{q - 1}$$

is increasing in e and f, it is enough to show that (2.2) is never verified for $e = 2$ and $f = 2$. Now, inequality (2.2) for $e = 2$ and $f = 2$ becomes

$$q^2 \leq q + 1,$$

which is false for every q. Then $f = 1$.

We want now to show that for $f = 1$ the inequality (2.2) forces q to be prime and $n = 1$, or $q = 2$ and $n = 2$, which are exactly the pathological cases we excluded. For $f = 1$, inequality (2.2) becomes

$$q^{e-1-\lceil \log_q e \rceil} \leq 1,$$

which is equivalent to

$$e - 1 - \lceil \log_q e \rceil \leq 0.$$

The quantity $e-1-\lceil \log_q e \rceil$ is clearly increasing in e. Then, for $e \geq 4$ it is enough to show that it never holds for $e = 4$. In this case, in fact, we have $\lceil \log_q 4 \rceil \leq 2$ for every q, and so $4 - 1 - \lceil \log_q 4 \rceil \geq 1$ for every q. For $e = 3$, in which case $n = 2$, we have $\lceil \log_2 3 \rceil = 2$, and $\lceil \log_q 3 \rceil = 1$ otherwise. Then, the inequality is satisfied for $q = 2$, and never satisfied for $q \neq 2$. Finally, for $e = 2$ we have $n = 1$. Since for $n = 1$ if Ψ sends a point of U to the point at infinity, then ψ transitive gives Ψ transitive by [1, Proposition 2.6], and so $e = 1$ by [1, Theorem 3.4], a contradiction. We have then that Ψ maps no point of U to the point at infinity, and so ψ is an affine map. But then, since ψ is transitive (and in particular the inequality holds) then q is prime by [1, Theorem 2.7]. In conclusion, we proved that if $e \geq 2$ then q is prime and $n = 1$, or $q = 2$ and $n = 2$, which are the pathological cases excluded at the beginning. Therefore $e = 1$, and so $\mu_M(T)$ is irreducible.

3 Artin-Schreier fractional jumps

Let $q = p$ be a prime number. In this section we consider fractional jumps of automorphisms of $\mathbb{P}^{p-1}$ defined by companion matrices of Artin-Schreier polynomials

$$\alpha_c(T) = T^p - T - c \in \mathbb{F}_p[T], \quad \text{for } c \in \mathbb{F}_p^*.$$

Proposition 1. *The polynomial $\alpha_c(T)$ is projectively primitive for every $c \in \mathbb{F}_p^*$.*

Proof. Notice that it is well known that the polynomials $\alpha_c(T)$ are irreducible for every $c \in \mathbb{F}_p^*$ by the theory of Artin-Schreier extensions. Let now $c \in \mathbb{F}_p^*$ be fixed. We want to show that $\alpha_c(T)$ is projectively primitive. Let $c' \in \mathbb{F}_p^*$ be such that c/c' generates $\mathbb{F}_p^*$. Then, the polynomial $T^p - T - c/c'$ is primitive by [3, Theorem 1.2], and so projectively primitive. Now, this implies that the polynomial $c'T^p - c'T - c = (c'T)^p - c'T - c$ is projectively primitive, and so $\alpha_c(T)$ is projectively primitive.

Fix $c \in \mathbb{F}_p^*$, let $M \in \mathrm{GL}_p(\mathbb{F}_q)$ be the companion matrix of $\alpha_c(T)$, let $\Psi = [M]$, and let ψ be the fractional jump of Ψ. Let $x_0 \in \mathbb{A}^{p-1}$, and let $\{x^{(k)}\}_{k\in\mathbb{N}}$ be the sequence recursively defined by $x^{(k+1)} = \psi(x^{(k)})$. By [1, Theorem 3.4] we know that the sequence $\{x^{(k)}\}_{k\in\mathbb{N}}$ has full orbit.

3.1 Explicit description

In what follows we want to give the explicit description of the Artin-Schreier fractional jump ψ.

For $i \in \{1, \dots, p-1\}$ we have that

$$M^i = \left(\begin{array}{c|c} 0_{i,p-i} & J_i(c)^t \\ \hline \mathrm{Id}_{p-i} & E^{(1,i)}_{p-i,i} \end{array}\right),$$

where $0_{i,p-i}$ is the $i \times (p-i)$ zero matrix, $J_i(c)^t$ is the transpose of a Jordan block of size $i \times i$ and eigenvalue c, that is

$$J_i(c)^t = \begin{pmatrix} c & 0 & \cdots & \cdots & 0 \\ 1 & c & 0 & & \vdots \\ 0 & 1 & c & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & c \end{pmatrix},$$

the matrix Id_{p-i} is the $(p-i)\times(p-i)$ identity, and $E^{(1,i)}_{p-i,i}$ is the $(p-i)\times i$ matrix with $(1,i)$-entry equal to 1, and all the other entries equal to zero. For $i=p$ we clearly have $M^p = M + c\mathrm{Id}_p$.

Following Remark 2, let us now compute explicitly the polynomials $b^{(i)}$'s and the sets U_i's, for $i\in\{1,\dots,p\}$, by looking at the last row of M^i.

$$\begin{aligned} b^{(i)} &= x_{p-i}, \\ &\quad \text{for } i\in\{1,\dots,p-2\}, \\ b^{(p-1)} &= x_1+1, \\ b^{(p)} &= x_{p-1}+c, \end{aligned}$$

which gives

$$\begin{aligned} U_1 &= \left\{x\in\mathbb{A}^{p-1} \,:\, x_{p-1}\neq 0\right\}, \\ U_i &= \left\{x\in\mathbb{A}^{p-1} \,:\, x_{p-i}\neq 0, \text{ and } x_{p-j}=0,\ \forall j\in\{1,\dots,i-1\}\right\}, \\ &\quad \text{for } i\in\{2,\dots,p-2\}, \\ U_{p-1} &= \left\{x\in\mathbb{A}^{p-1} \,:\, x_1+1\neq 0, \text{ and } x_{p-j}=0,\ \forall j\in\{1,\dots,p-2\}\right\}, \\ U_p &= \left\{x\in\mathbb{A}^{p-1} \,:\, x_{p-1}+c\neq 0,\ x_1+1=0, \text{ and } x_{p-j}=0,\ \forall j\in\{1,\dots,p-2\}\right\} \\ &= \{(-1,0,\dots,0)\}. \end{aligned}$$

The polynomials $a^{(i)}_j$, for $i\in\{1,\dots,p\}$ and $j\in\{1,\dots,p-1\}$, are easily computed as well by looking at the j-th row of M^i.

- for $i=1$ we have that
  - if $j=1$ then $a^{(1)}_1 = c$,
  - if $j=2$ then $a^{(1)}_2 = x_1+1$,
  - for any $j\in\{3,\dots,p-1\}$ then $a^{(1)}_j = x_{j-1}$.
- for $i\in\{2,\dots p-1\}$ we have that
  - if $j=1$ then $a^{(i)}_1 = cx_{p-i+1}$,
  - if $j\in\{2,\dots,i-1\}$ then $a^{(i)}_j = x_{p-i+j-1} + cx_{p-i+j}$,
  - if $j=i$ then $a^{(i)}_i = x_{p-1}+c$,
  - if $j=i+1$ then $a^{(i)}_{i+1} = x_1+1$,
  - if $j\in\{i+2,\dots,p-1\}$ then $a^{(i)}_j = x_{j-i}$.
- for $i=p$ we have that
  - if $j=1$ then $a^{(p)}_1 = cx_1+c$,
  - if $j=2$ then $a^{(p)}_2 = x_1+cx_2+1$,
  - if $j\in\{3,\dots,p-1\}$ then $a^{(p)}_j = x_{j-1}+cx_j$.

By Theorem 1 this provides the explicit structure of ψ.

3.2 Computational complexity

Now that we have the explicit description of the fractional jump, we are ready to establish the expected complexity of computing a random term in the sequence $\{x^{(k)}\}_{k\in\mathbb{N}}$ given by iterating the Artin-Schreier fractional jump ψ.

The expected complexity of computing $x^{(k+1)}$ given a term $x^{(k)}$ chosen uniformly at random in the sequence is

$$\mathbb{E} = \sum_{i=1}^{p} p_i c_i,$$

where p_i is the probability that $x^{(k)} \in U_i$, which is

$$p_i = \begin{cases} p^{-i}(p-1), & \text{if } i \in \{1,\dots,p-1\}, \\ p^{1-p}, & \text{if } i = p, \end{cases}$$

and c_i is the complexity of evaluating ψ at $x^{(k)}$ when $x^{(k)} \in U_i$.

We want now to evaluate c_i for $i \in \{1,\dots,p\}$. If $x^{(k)} \in U_i$, the number of sums needed to compute $x^{(k+1)} = \psi(x^{(k)}) = f^{(i)}(x^{(k)})$ is $s_i = \sum_{j=1}^{p}(r_j^{(i)} - 1)$, where $r_j^{(i)}$ is the number of non-zero entries in the j-th row of the matrix M^i.

Since the denominators of the components of $f^{(i)}$ are all equal, the number of inversions needed is always 1.

Also, the number of multiplications needed is given by the number m_i of entries different from 0 and 1 in the $p\times(p-1)$ submatrix of M^i given by dropping the last column (this can be seen as the last component of the projective point is set to 1 in the fractional jump) plus the number of multiplications of $b^{(i)}(x^{(k)})^{-1}$ by the $a_j^{(i)}$'s, which is simply $p-1$.

Since the length of the orbit p^{p-1} is superexponential, the size of p can be chosen relatively small in such a way that one can build look-up tables for the operations in $\mathbb{F}_p$ (so they will all have the same cost) and still get a huge orbit. Therefore

$$c_i = \underbrace{s_i}_{\text{sums}} + \underbrace{1}_{\text{inversions}} + \underbrace{m_i + p - 1}_{\text{multiplications}}.$$

It remains to compute s_i and m_i. Given the explicit description previously provided, we have $s_i = i$ for $i \in \{1,\dots,p-1\}$ and $s_p = p+1$, and $m_i = i-1$ for $i \in \{1,\dots,p\}$. Therefore, we have $c_i = p + 2i - 1$ for $i \in \{1,\dots,p-1\}$ and $c_p = 3p$.

The expected complexity is then

$$\begin{aligned}\mathbb{E} &= 3p^{2-p} + \sum_{i=1}^{p-1} p^{-i}(p-1)(p+2i-1) \\ &= 3p^{2-p} - \frac{3p^3 - (p^2+1)p^p - 4p^2 + 3p}{p^p(p-1)} = p + O\left(\frac{1}{p}\right).\end{aligned}$$

This means that the expected complexity of computing the $(k+1)$-th vector of the sequence roughly consists of p checks of the look-up tables, one for each component: morally, we are filling out each component of the term of the sequence by directly reading the look-up table, which is why the process is very efficient.

Remark 3. Clearly, the expected complexity can be further optimised by using the equations defining the U_i's, but this will not affect the asymptotic behaviour of $\mathbb{E}$.

4 Conclusions and further research

In this paper we proved that the transitivity of the fractional jumps and the transitivity of the projective automorphisms inducing them are equivalent conditions, except from some degenerate cases which are entirely classified. This puts the last stone for the foundational theory of this new construction: for fixed base field and fixed dimension, the problem of finding all transitive fractional jump is now reduced to finding transitive projective automorphisms. In addition, using the theory of Artin-Schreier polynomials, we showed that the construction is sistematically feasible when the dimension of the projective space is prime and equal to the characteristic of the field. The question now arising is:

Question 1. Can one give new explicit classes of projectively primitive polynomials?

Such new classes will allow to use companion matrices of such polynomials (or their conjugates) to build full orbit fractional jump sequences. In particular, it would be of interest to do this for any fixed dimension and in characteristic 2, and with sparse polynomials.

Acknowledgment

The authors are grateful to Andrea Ferraguti for preliminary reading of this manuscript, and for useful discussions and suggestions. The second author is thankful to the Swiss National Science Foundation grant number 171248.

Bibliography

[1] F. Amadio Guidi, S. Lindqvist, and G. Micheli. Full orbit sequences in affine spaces via fractional jumps and pseudorandom number generation. *arXiv preprint arXiv:1712.05258v2*, 2017.

[2] N. Brandstätter and A. Winterhof. Some notes on the two-prime generator of order 2. *IEEE Trans. Inform. Theory*, 51(10):3654–3657, 2005.

[3] X. Cao. On the order of the polynomial $x^p - x - a$. *Cryptology ePrint Archive, Report 2010/034*, 2010. `https://eprint.iacr.org/2010/034.pdf`.

[4] W.-S. Chou. On inversive maximal period polynomials over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 6(4):245–250, 1995.

[5] J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers avoid the planes. *Math. Comp.*, 56(193):297–301, 1991.

[6] E. D. El-Mahassni and D. Gómez-Pérez. On the distribution of nonlinear congruential pseudorandom numbers of higher orders in residue rings. In *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 195–203. Springer, 2009.

[7] A. Ferraguti, G. Micheli, and R. Schnyder. On sets of irreducible polynomials closed by composition. In *International Workshop on the Arithmetic of Finite Fields*, Lecture Notes in Comput. Sci., pages 77–83. Springer, 2016.

[8] D. Gómez-Pérez, A. Ostafe, and I. E. Shparlinski. Algebraic entropy, automorphisms and sparsity of algebraic dynamical systems and pseudorandom number generators. *Math. Comp.*, 83(287):1535–1550, 2014.

[9] J. Gutierrez, I. E. Shparlinski, and A. Winterhof. On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators. *IEEE Trans. Inform. Theory*, 49(1):60–64, 2003.

[10] D. R. Heath-Brown and G. Micheli. Irreducible polynomials over finite fields produced by composition of quadratics. *arXiv preprint arXiv:1701.05031*, 2017.

[11] S. Lang. *Algebra - Revised Third Edition*, volume 211 of *Grad. Texts in Math.* Springer-Verlag, New York, 2002.

[12] H. Niederreiter and I. E. Shparlinski. Recent advances in the theory of nonlinear pseudorandom number generators. In *Monte Carlo and Quasi-Monte Carlo Methods 2000*, pages 86–102. Springer, 2002.

[13] H. Niederreiter and I. E. Shparlinski. Dynamical systems generated by rational functions. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 6–17. Springer, 2003.

[14] A. Ostafe. Pseudorandom vector sequences derived from triangular polynomial systems with constant multipliers. In *International Workshop on the Arithmetic of Finite Fields*, Lecture Notes in Comput. Sci., pages 62–72. Springer, 2010.

[15] A. Ostafe, E. Pelican, and I. E. Shparlinski. On pseudorandom numbers from multivariate polynomial systems. *Finite Fields Appl.*, 16(5):320–328, 2010.

[16] A. Ostafe and I. E. Shparlinski. On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators. *Math. Comp.*, 79(269):501–511, 2010.

[17] A. Ostafe and I. E. Shparlinski. On the length of critical orbits of stable quadratic polynomials. *Proc. Amer. Math. Soc.*, 138(8):2653–2656, 2010.

[18] A. Topuzoğlu and A. Winterhof. Pseudorandom sequences. In A. Garcia and H. Stichtenoth, editors, *Topics in Geometry, Coding Theory and Cryptography*, pages 135–166, Dordrecht, 2006. Springer Netherlands.

[19] A. Winterhof. Recent results on recursive nonlinear pseudorandom number generators. In *SETA*, pages 113–124. Springer, 2010.