Orbits of Rational Maps over Finite Rings and Fields

Igor E. Shparlinski

Macquarie University

Introduction

Given:

- an algebraic domain $\mathcal{D}$
- a map $\mathcal{F} : \mathcal{D} \to \mathcal{D}$

we consider orbits

$$\mathbf{x}_{n+1} = \mathcal{F}(\mathbf{x}_n), \qquad n = 0, 1, \ldots,$$

starting with some initial point $\mathbf{x}_0 \in \mathcal{D}$.

$\mathcal{F}^{(k)} =$ the kth iteration of $\mathcal{F}$

For any $n, k \geq 0$

$$\mathbf{x}_{n+k} = \mathcal{F}^{(k)}(\mathbf{x}_n),$$

Traditionally, $\mathcal{D}$ is infinite: $\mathcal{D} = \mathbb{C}, \mathbf{Z}, \mathbb{Q}_p, \mathbb{C}_p \ldots$.

Common Knowledge: Number-theoretic transformations lead to very interesting dynamical systems:

- continued fractions,
- various numeration systems,
- the $3x + 1$ transformation,
- and others ....

We mainly concentrate on dynamical systems associated with transformations generated by

- rational functions (and polynomials in particular)
- over finite fields and residue rings: $\mathcal{D} = \mathbb{F}_q^s$ or $\mathcal{D} = \mathbf{Z}_m^s$ ($s = 1$ is of special interest).

Sequences of elements of $\mathbb{F}_q$ and $\mathbb{Z}_m$ generated by $\mathbf{x}_{n+1} = \mathcal{F}(\mathbf{x}_n)$ have been studied for a long time in parallel

- in the theory of pseudorandom number generators and cryptography
- in the theory of dynamical systems

... unfortunately without too much interaction.

Basic questions (common for both areas):

- Period length
- Fixed points
- Distribution
- Embedded linear structures
- ....

We hope that this talk will help to establish some links between these two areas, and two groups of researchers:

We describe open problems and show some obstacles, of **purely algebraic** nature, related to some algebraic properties of iterations of rational maps.

Thus, we hope that the dynamical system community may find a scope of new interesting problems which may succumb to their efforts.

Notation

General:

$\mathbb{F}_q$ = finite field of q elements.

$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ residue ring modulo m.

p = prime number.

Period:

If $\mathcal{D}$ is finite, then any sequence generated by $\mathbf{x}_{n+1} = \mathcal{F}(\mathbf{x}_n)$ becomes eventually periodic with least period $t \leq \#\mathcal{D}$.

We always assume that it is *purely periodic* (which can be achieved by a shift).

Uniformity of Distribution

Discrepancy:

For a sequence of N points in $[0,1)^s$

$$\Gamma = \left(\gamma_{1,n}, \dots, \gamma_{s,n}\right)_{n=1}^{N} \in [0,1)^s$$

its *discrepancy* $\Delta(\Gamma)$ is

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

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

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes.

Informally In the $2D$-case the discrepancy shows how uniformly grey the picture looks like if we plot the points Γ.

Modulo m Discrepancy

For a sequence of N points in $\mathbf{Z}_m^s$

$$\mathcal{U} = \left(u_{1,n}, \ldots, u_{s,n}\right)_{n=1}^{N} \in \mathbf{Z}_m^s$$

its *modulo m discrepancy* $D_m(\mathcal{U})$ is defined as the ordinary discrepancy $\Delta(\Gamma)$ of the sequence

$$\Gamma = \left(\frac{u_{1,n}}{m}, \ldots, \frac{u_{s,n}}{m}\right)_{n=1}^{N}.$$

We also apply this definition to points over $\mathbb{F}_p$.

Survey of the Results

Linear generator:

$f(X) = aX + b$, case $b = 0$ is of special interest:

$$f^{(k)}(X) = a^k X$$

Linear congruential generator has been in use for decades: *Knuth, Korobov, Krawczyk, Niederreiter, Shparlinski,* **BC – 2005**

Exhibits some major disadvantages:

- Bad Distribution of s-tuples $(x_n, \ldots, x_{n+s-1})$.
- It is "too linear". This can be formalised in terms of **linear complexity** which makes it bad for both
  - Monte Carlo
  - Cryptography

  applications

Polynomial generator:

$$x_{n+1} = f(x_n), \qquad n = 0, 1, \ldots,$$

where $f(X) \in \mathbf{Z}_m[X]$, $\deg f = d \geq 2$ and $x_0 \in \mathbf{Z}_m$.

Niederreiter & Shparlinski, **1999**: $\boxed{m = p}$

For any $1 \leq N \leq t$ and $s \geq 1$ for the modulo p discrepancy of set

$$\mathcal{X}_{s,N} = \left(x_n, \ldots, x_{n+s-1}\right), \qquad 0 \leq n \leq N-1,$$

the bound

$$D_p(\mathcal{X}_{s,N}) = O\left(N^{-1/2} p^{1/2} (\log p)^{-1/2} \ (\log\log p)^s\right)$$

holds.

Nontriviality range is rather narrow (but not void)

$$p \geq t \geq N \gg p(\log p)^{-1+\varepsilon}.$$

Question: Find polynomials f with $t \approx p$.

Birthday paradox: For "random" f one expects $t \approx p^{1/2}$

. . . bad for us;

. . . good for the *Pollard factorisation algorithm*.

To achieve $t \approx p$ special constructions are needed: e.g. f must be an "almost" permutation polynomial because

$$t \leq \#f(\mathbb{F}_p)$$

Dickson polynomials are our primary suspects!
. . . not just because they are nice, but because of some "semirigorous" reasons to believe so.

Rational generator:

Question: What if we take a rational function instead of a polynomial?

Additional complications: zero divisors in the denominator.

This case, although theoretically interesting, has never been worked out in detail, because it does not seem to give any advantages compared to the polynomial generator (and is computationally more expensive).

However (!!!) there is a very special case which brings many nice surprises:

$$f(X) = \frac{\alpha X + \beta}{\gamma X + \delta}$$

with $\alpha\delta - \beta\gamma \neq 0$.

A substitution reduces it to less symmetric but simpler functions of the form

$$f(X) = aX^{-1} + b$$

(with convention that $0^{-1} = 0$).

This case is known as the *inversive generator*.

Inversive generator:

Gutierrez & Niederreiter & Shparlinski, **2000**:

$\boxed{m = p}$

Discrepancy bound:

$$D_p(\mathcal{X}_{s,N}) = O\left(N^{-1/2} p^{1/4} (\log p)^s\right)$$

Nontriviality range is much wider range than that known for the polynomial generator:

$$t \geq N \gg p^{1/2} (\log p)^{2s+\varepsilon}$$

Question: Find a and b with $t \approx p$.

Not too hard!! t is related to some properties of $X^2 - bX - a \in \mathbb{F}_p[X]$.

The inner structure is likely to beat the birthday paradox!

Flahive and Niederreiter, **1993**:

It is known how to achieve $t = p$.

What else?

Multidimensional case:

$$x_{n+r} = f\left(x_{n+r-1}, \ldots, x_n\right), \qquad n = 0, 1, \ldots,$$

Extending previous results results to general polynomials leads to an algebraic problem about linear independence of iterations $f^{(k)}$, which we will discuss later.

For some polynomials it works:

Griffin & Niederreiter & Shparlinski, **1999**,
Gutierrez & Gomes-Perez, **2001**:

$$D_p(\mathcal{X}_{s,N}) = O\left(N^{-1/2} p^{1/2} (\log p)^{-1/2} \ (\log\log p)^s\right)$$

(as in the case $r = 1$).

Monomial case — Power generator:

In the above we have always assumed that the degrees of the involved functions are bounded

One of the reason is that otherwise it is hard to evaluate these functions).

However, high degree monomials $f(x) = x^e$ are easy to evaluate via *repeated squaring*.

Power generator

$$x_{n+1} = x_n^e, \qquad n = 0, 1, \ldots .$$

which has been introduced for some cryptographic applications.

Special case: $m = pl$, p and l are primes, *RSA modulus*, (we iterate *RSA encryption*).

Special subcases:

- $\gcd(e, \varphi(m)) = 1$, — *RSA generator*
- $e = 2$ — *Blum–Blum–Shub generator*

Friedlander & Pomerance & Shparlinski, **2001**:
Period t is likely to be close to m

Friedlander & Shparlinski, **1999**:
$\boxed{m = pl, \text{ RSA modulus}}$

For any integer $\nu \geq 1$,

$$D_m(\mathcal{X}_{1,t}) = O(t^{-(2\nu+1)/2\nu(\nu+1)} m^{(3\nu+2)/4\nu(\nu+1)+\varepsilon})$$

Nontriviality range:

$$m \geq t \geq m^{3/4+\varepsilon}$$

$$t \geq m^{1-\varepsilon} \qquad \Longrightarrow \qquad D_m(\mathcal{X}_{1,t}) = O\left(m^{-1/8+\varepsilon}\right).$$

Open Questions

- Distribution of s-tuples $(x_n, \dots, x_{n+s-1})$?

  No visible approaches . . .

  except if e is "small", say $e = 2$, then the same method works for $s = o(\log m / \log\log m)$.

- Distribution of x_n, $n = 0, \dots, N-1$, where $N < t$?

  Could be doable via reduction to complete sums.

Friedlander & Hansen & Shparlinski, **2001**:

For $m = p$ the results are stronger

Nontriviality range:

$$p \ge t \ge p^{1/2+\varepsilon}$$

Gomez-Perez & Gutierrez & Shparlinski, **2003**

Similar results for iterations of Dickson polynomials.

Generators on Elliptic Curves

Let $\mathbf{E}$ be given by a *Weierstraß equation* over $\mathbb{F}_p$

$$y^2 = x^3 + ax + b,$$

Main Facts:

- Hasse–Weil: $|\#\mathbf{E}(\mathbb{F}_p) - p - 1| \leq 2p^{1/2}$
- $\mathbf{E}(\mathbb{F}_p)$ is an Abelian group

Fix a point $G \in \mathbf{E}(\mathbb{F}_p)$.

- EC linear congruential generator

$$U_k = G \oplus U_{k-1} = kG \oplus U_0, \qquad k = 1, 2, \ldots .$$

- EC power generator

$$W_k = eW_{k-1} = e^k G, \qquad k = 1, 2, \ldots,$$

How Does the Method Work?

Generic principle: to study the distribution and other "statistical" properties of any sequence $(\mathbf{x}_n)_{n=0}^{\infty}$ in any domain $\mathcal{D}$ having an abelian group structure, one usually considers character sums

$$S(\chi) = \sum_{n=0}^{N-1} \chi\left(\mathbf{x}_n\right),$$

where χ is a nonprincipal character of the corresponding group.

Step 1. Typically, individual single sums are hard to study. — Let us to create a **double sum** $W(\chi)$ which is closely associated with $S(\chi)$.

For any integer $k \geq 0$:

$$S(\chi) = \sum_{n=k}^{N+k-1} \chi\left(\mathbf{x}_n\right) + O(k).$$

Indeed, the sums on the LHS and the RHS "disagree" for at most $2k$ values of n and since $|\chi(\mathbf{x})| = 1$, we obtain the above identity.

Sum up these identities for $k = 0, \ldots, K-1$:

$$KS(\chi) = W(\chi) + O(K^2),$$

where

$$\begin{aligned} W(\chi) &= \sum_{k=0}^{K-1} \sum_{n=k}^{N+k-1} \chi\left(\mathbf{x}_n\right) \\ &= \sum_{k=0}^{K-1} \sum_{n=0}^{N-1} \chi\left(\mathbf{x}_{n+k}\right) \\ &= \sum_{k=0}^{K-1} \sum_{n=0}^{N-1} \chi\left(\mathcal{F}^{(k)}\left(\mathbf{x}_n\right)\right) \end{aligned}$$

because $\mathbf{x}_{n+k} = \mathcal{F}^{(k)}\left(\mathbf{x}_n\right)$.

We have a double sum!!

Step 2. Our next step is to reduce $W(\chi)$ to a sum which **does not depend** on the specific sequence $(\mathbf{x}_n)_{n=0}^{\infty}$ at all!!

We write

$$|W(\chi)| \leq \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi\left(\mathcal{F}^{(k)}\left(\mathbf{x}_n\right)\right) \right|,$$

Cauchy inequality:

$$|W(\chi)|^2 \leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi\left(\mathcal{F}^{(k)}\left(\mathbf{x}_n\right)\right) \right|^2.$$

If $1 \le N \le t$ then $\mathbf{x}_0, \dots, \mathbf{x}_{N-1}$ are pairwise distinct.

We can only add more nonnegative terms to the last sum if we replace $\mathbf{x}_n$ with $\mathbf{x}$ running through the whole$\mathcal{D}$:

$$|W(\chi)|^2 \le N \sum_{\mathbf{x} \in \mathcal{D}} \left| \sum_{k=0}^{K-1} \chi\left(\mathcal{F}^{(k)}(\mathbf{x})\right) \right|^2 .$$

$\boxed{\mathbf{x}_n \text{ are gone !!}}$

Step 3. Estimate the last sum.

We have

- $|z|^2 = z\overline{z}$ for any complex z
- $\overline{\chi(\mathbf{u})} = \chi(-\mathbf{u})$ for any $\mathbf{u} \in \mathcal{D}$

After changing the order of summation, we derive

$$|W(\chi)|^2 \le N \sum_{k,l=0}^{K-1} \sum_{\mathbf{x} \in \mathcal{D}} \chi\left(\mathcal{F}^{(k)}(\mathbf{x}) - \mathcal{F}^{(l)}(\mathbf{x})\right).$$

The contribution of the terms with $k = l$ is $K\#\mathcal{D}$.

Time to use something specific about f and $\mathcal{D}$:

To estimate the terms with $k \neq l$, we need some additional information about the character sums with functions of the form $\mathcal{F}^{(k)}(\mathbf{x}) - \mathcal{F}^{(l)}(\mathbf{x})$.

Assume that generally these functions fall into a class of functions for which nontrivial upper bounds on character sums are known (e.g. polynomials)

. . . but we still have one more problem to overcome:

We have to show that $\chi\left(\mathcal{F}^{(k)}(\mathbf{x}) - \mathcal{F}^{(l)}(\mathbf{x})\right)$ is not constant!!

Easy case/Weak result — Polynomial generator:

if $\deg(f) = d \geq 2$ then $\deg f^{(k)} = d^k$

The degree of $f^{(k)}$ grows very fast:

- good for the proof;
- bad for the result: Using the **Weil bound**, which calims that

$$\sum_{x \in \mathbb{F}_p} \exp(2\pi i G(x)/p) = O\left(\deg G p^{1/2}\right)$$

for any nonconstant rational function $G(X) \in \mathbb{F}_p(X)$ we derive

$$|W(\chi)|^2 = O\left(KNp + K^2 d^{K+s-2} N p^{1/2}\right).$$

Harder case/Stronger result — Inversive generator:

The above argument does not apply:

$$f^{(k)}(X) = \frac{A_k X + B_k}{C_k X + D_k}$$

One needs to study these functions more carefully!!

- bad for the proof;

- good for the result: Using the **Weil bound**:

$$|W(\chi)|^2 = O\left(KNp + K^2 Np^{1/2}\right).$$

Special case/Special result — Power generator:

For $f(X) = X^e$ the degree of

$$f^{(k)}(X) - f^{(l)}(X) = X^{e^k} - X^{e^l}$$

could be very large even for small k and l (e.g. for $k = 1$, $l = 0$).

. . . there is a nice trick related to substitution $X \to X^r$ for some r which helps to reduce the degree!

s-Dimensional Distribution

. . . follows the same pattern with the linear combination

$$\sum_{j=0}^{s-1} \mathbf{a}_j \left(\mathcal{F}^{(k+j)}(\mathbf{x}) - \mathcal{F}^{(l+j)}(\mathbf{x}) \right)$$

instead of

$$\mathcal{F}^{(k)}(\mathbf{x}) - \mathcal{F}^{(l)}(\mathbf{x}).$$

Additional Difficulty: If $\mathcal{F}$ is a polynomial in several variables then the degree argument is not working.

. . . generally remains unresolved.

Questions:

- Polynomial generators in several variables?
  — *Better understanding of algebraic properties of iterated multivariate polynomials is needed.*

- s-dimensional distribution of the power generator?
  — *Some clever trick which will reduce the degree of several terms $X^{e^k}, \ldots, X^{e^{k+s-1}}$ simultaneously.*

- What are possible grows rates of $d_k = \deg f^{(k)}$ for rational functions?
  — *Is it always either $d_k = d^k$ or $d_k = O(1)$?*

- What about other interesting groups, e.g., groups of points on elliptic curves?

  Hess & Lange & Shparlinski, **2002**:
  Some partial results have recently been obtained.

Related Questions

Linear Complexity

Question: Are there any hidden linearity?

This makes **PRN** vulnerable to the LLL attack (e.g., the linear congruential generator)

Knuth; Boyar; Frieze & Håstad & Kannan & Lagarias; Krawczyk; Joux & Stern, **1980–. . .**

Linear Complexity of an infinite sequence (s_n) is the length L of the shortest linear recurrence relation

$$s_{n+L} = a_{L-1}s_{n+L-1} + \ldots + a_0 s_n,$$

which is satisfied by this sequence.

Inversive Generator

Niederreiter, **1992**:

Assume that the sequence (u_x), given by the inversive generator

$$x_{n+1} \equiv a x_n^{-1} + b \pmod{p}, \quad 0 \le x_n \le p-1,$$

is purely periodic with period $t = p$. Then for the linear complexity L of this sequence the bound

$$L \ge (p+3)/2$$

holds.

Niederreiter & Shparlinski, **1998**,
Gutierrez & Shparlinski & Winterhof, **2001**:

Some extensions to other nonlinear generators with polynomials and rational functions of low degree.

Power Generator

Shparlinski, **1998**:

Let $M = pl$, where p and l are two distinct primes. Assume that the sequence (x_n), given by the power generator

$$x_{n+1} \equiv x_n^e \pmod{M}, \quad 0 \le x_n \le m-1,$$

is purely periodic with period t. Then for the linear complexity L of this sequence the bound

$$L \ge t\varphi(m)^{-1/2}$$

holds.

The bound is tight!

Griffin and Shparlinski, **1998)**:

Generalization to linear complexity of finite segments of the power generator.

Predictability

Known: the general rule (and some of other parameters),

Unknown: the initial value.

Question: Given several consecutive elements

$$x_n, \ldots, x_{n+k-1}$$

(either their exact values or only some bits of them), continue to generate

$$x_{n+k}, x_{n+k+1}, x_{n+k+2} \cdots.$$

Linear Congruencial Generator

$$x_{n+1} \equiv ax_n + b \pmod{p}, \quad 0 \leq x_n \leq p-1,$$

Trivial: a, b, m are known, $x_n, \ldots, x_{n+k-1}$ are given in full

Knuth; Boyar; Frieze & Håstad & Kannan & Lagarias; Krawczyk, **1980–1992**:
a, b are known/unknown, m is known and only some bits of $x_n, \ldots, x_{n+k-1}$ are given — *rigorous results*

Joux & Stern, **1994**
Contini& Shparlinski, **2004** :
a, b, m are unknown, only some bits of $x_n, \ldots, x_{n+k-1}$ are given — *heuristic results*

Non-linear Generator

Lagarias & Reeds, **1990**:

$$\mathbf{x}_{n+1} = \mathcal{F}(\mathbf{x}_n), \qquad n = 0, 1, \ldots,$$

where $\mathcal{F}$ is an unknown polynomial map and

$$\mathbf{x}_n, \ldots, \mathbf{x}_{n+k-1}$$

are given in full.

Proof makes use of rather deep results about polynomial ideals.

Blackburn &Gomez-Perez & Gutierrez & Shparlinski, **2003**

One dimensional polynomial and inversive generators where only some bits of $x_n, \ldots, x_{n+k-1}$ are given.

Proofs make use of lattice reduction.