

Dynamical Irreducibility Over Finite Fields

Ansley Rickson

Agnes Scott College

Wednesday, May 27th, 2026

What is Dynamics?

Let f be a rational map defined over a field K .

Definition

$$f^n(x) = \underbrace{(f \circ f \circ f \circ \dots \circ f)}_{n \text{ times}}(x)$$

What is Dynamics?

Let f be a rational map defined over a field K .

Definition

$$f^n(x) = \underbrace{(f \circ f \circ f \circ \dots \circ f)}_{n \text{ times}}(x)$$

We are interested in the behavior of points under iteration.

Definition

We say α is a periodic point of f if there exists $n \in \mathbb{N}$ such that $f^n(\alpha) = \alpha$. This integer n is called the period of α .

What is Dynamical Irreducibility?

If $f^n(x)$ is irreducible for all $n \in \mathbb{N}$, we say f is *dynamically irreducible*. This has applications in arboreal Galois representations.

What is Dynamical Irreducibility?

If $f^n(x)$ is irreducible for all $n \in \mathbb{N}$, we say f is *dynamically irreducible*. This has applications in arboreal Galois representations.

We know that if f is reducible, then f^n is reducible, but the converse is not true.

What is Dynamical Irreducibility?

If $f^n(x)$ is irreducible for all $n \in \mathbb{N}$, we say f is *dynamically irreducible*. This has applications in arboreal Galois representations.

We know that if f is reducible, then f^n is reducible, but the converse is not true.

Example

Let $f(x) = x^3 + 16 \in \mathbb{F}_{19}[x]$. Then f is irreducible, but

$$\begin{aligned} f(f(x)) &= x^9 + 10x^6 + 8x^3 + 8 \\ &= (x^3 + x^2 + 3)(x^3 + 7x^2 + 3)(x^3 + 11x^2 + 3), \end{aligned}$$

so f^2 is reducible.

Dynamical Irreducibility Over Finite Fields

Let $f(x) = x^3 + 3 \in \mathbb{F}_7[x]$.

Dynamical Irreducibility Over Finite Fields

Let $f(x) = x^3 + 3 \in \mathbb{F}_7[x]$.

Since -3 is not a cube in \mathbb{F}_7 , f is not reducible.

Dynamical Irreducibility Over Finite Fields

Let $f(x) = x^3 + 3 \in \mathbb{F}_7[x]$.

Since -3 is not a cube in \mathbb{F}_7 , f is not reducible.

What about $f(f(x)) = x^9 + 2x^6 + 6x^3 + 2$?

Dynamical Irreducibility Over Finite Fields

Let $f(x) = x^3 + 3 \in \mathbb{F}_7[x]$.

Since -3 is not a cube in \mathbb{F}_7 , f is not reducible.

What about $f(f(x)) = x^9 + 2x^6 + 6x^3 + 2$?

In fact, $f(f(x))$ is irreducible over \mathbb{F}_7 as well!

Question

So, is it dynamically irreducible?

Dynamical Irreducibility Over Finite Fields

Our research focuses on polynomials of the form
 $f(x) = ax^d + c \in \mathbb{F}_p[x]$ for a prime $p \equiv 1 \pmod{3}$, where
 $a, c \in \mathbb{F}_p$ and $d = 3^j$ for $j \in \mathbb{N}$.

Dynamical Irreducibility Over Finite Fields

Our research focuses on polynomials of the form $f(x) = ax^d + c \in \mathbb{F}_p[x]$ for a prime $p \equiv 1 \pmod{3}$, where $a, c \in \mathbb{F}_p$ and $d = 3^j$ for $j \in \mathbb{N}$.

Let γ be a critical point (in the calculus sense) of f .

Definition

The *critical orbit* of f is $\{f^n(\gamma)\}_{n \in \mathbb{Z}_{>0}}$.

Dynamical Irreducibility Over Finite Fields

Our research focuses on polynomials of the form $f(x) = ax^d + c \in \mathbb{F}_p[x]$ for a prime $p \equiv 1 \pmod{3}$, where $a, c \in \mathbb{F}_p$ and $d = 3^j$ for $j \in \mathbb{N}$.

Let γ be a critical point (in the calculus sense) of f .

Definition

The *critical orbit* of f is $\{f^n(\gamma)\}_{n \in \mathbb{Z}_{>0}}$.

The critical orbit of a polynomial is generally important in dynamics, but in our case, we care about the *adjusted critical orbit* of f , denoted $ACO(f)$.

Definition

$$ACO(f) = \left\{-\frac{c}{a}\right\} \cup \left\{\frac{f^n(c)}{a}\right\}_{n \in \mathbb{Z}_{>0}}$$

Dynamical Irreducibility Over Finite Fields

Theorem (Day et al.)

Let r be prime and q a prime power with $q \equiv 1 \pmod{r}$, and let $f(x) \in \mathbb{F}_q[x]$ be a unicritical polynomial of degree r with the critical point at γ and lead coefficient a . Then f is dynamically irreducible over \mathbb{F}_q if and only if

$$\left\{ -\frac{f(\gamma)}{a} \right\} \cup \left\{ \frac{f^n(\gamma)}{a} : n \in \mathbb{Z}_{>1} \right\}$$

contains no r -th powers in \mathbb{F}_q .

This is a generalization of a theorem by Nigel Boston and Rafe Jones.

Dynamical Irreducibility Over Finite Fields

Theorem (Day et al.)

Let r be prime and q a prime power with $q \equiv 1 \pmod{r}$, and let $f(x) \in \mathbb{F}_q[x]$ be a unicritical polynomial of degree r with the critical point at γ and lead coefficient a . Then f is dynamically irreducible over \mathbb{F}_q if and only if

$$\left\{ -\frac{f(\gamma)}{a} \right\} \cup \left\{ \frac{f^n(\gamma)}{a} : n \in \mathbb{Z}_{>1} \right\}$$

contains no r -th powers in \mathbb{F}_q .

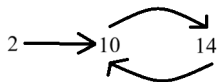
This is a generalization of a theorem by Nigel Boston and Rafe Jones.

For $d = 3$, f is dynamically irreducible over \mathbb{F}_p if and only if $ACO(f)$ contains no cubes.

Dynamical Irreducibility Over Finite Fields

Example

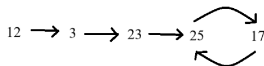
$$f(x) = x^3 + 2 \in \mathbb{F}_{19}[x]$$



Since 17, 10, and 14 are not cubes in \mathbb{F}_{19} , f is dynamically irreducible.

Example

$$f(x) = 5x^3 + 12 \in \mathbb{F}_{31}[x]$$



$ACO(f) = \{10, 13, 17, 5, 22\}$,
so f is dynamically irreducible
(no cubes)

Dynamical Irreducibility Over Finite Fields

The cubes in \mathbb{F}_7 are $\{0, 1, 6\}$.

The cubes in \mathbb{F}_{19} are $\{0, 1, 7, 8, 11, 12, 18\}$.

The cubes in \mathbb{F}_{31} are $\{0, 1, 2, 4, 8, 15, 16, 23, 27, 29, 30\}$.

Example

$$f(x) = x^3 + 3 \in \mathbb{F}_7[x] \Rightarrow ACO(f) = \{4, 2\}$$

$$f(x) \in \mathbb{F}_{19}[x] \Rightarrow ACO(f) = \{16, 11, 4, 10, 15\}$$

$$f(x) \in \mathbb{F}_{31}[x] \Rightarrow ACO(f) = \{28, 30, 2, 11, 1, 4, 5\}$$

Dynamical Irreducibility Over Finite Fields

Let $\varphi(x) = \alpha x$, and define $f^\varphi = \varphi^{-1} \circ f \circ \varphi$. Then f and f^φ have the same dynamical behavior.

Example

If α is a periodic point for f , then $\varphi^{-1}(\alpha)$ is also periodic for f^φ .

Dynamical Irreducibility Over Finite Fields

Let $\varphi(x) = \alpha x$, and define $f^\varphi = \varphi^{-1} \circ f \circ \varphi$. Then f and f^φ have the same dynamical behavior.

Example

If α is a periodic point for f , then $\varphi^{-1}(\alpha)$ is also periodic for f^φ .

Since $f(x) = ax^d + c$, $f^\varphi(x) = a(\alpha^{d-1})^{-1}x^d + c\alpha$.

Dynamical Irreducibility Over Finite Fields

Theorem (Day et al.)

Let $f(x) \in \mathbb{F}_p[x]$ and $\varphi(x) = \alpha x + c \in \mathbb{F}_p[x]$ for $\alpha \neq 0$. Define $g(x) = f^\varphi(x)$. Then $f^n(x)$ is irreducible over \mathbb{F}_p if and only if $g^n(x) - c$ is irreducible over \mathbb{F}_p .

Example

Let $f(x) = x^3 + 9 \in \mathbb{F}_{31}[x]$, and let $\varphi(x) = 4x$. Then $f^\varphi(x) = 2x^3 + 5$.

$$\text{ACO}(f) = \{22, 25, 10, 17, 24, 7, 11\}$$

$$\text{ACO}(f^\varphi) = \{13, 19, 20, 3, 17, 14, 22\}$$

Research Questions

Our goal is to reduce the number of polynomials of the form $ax^d + c$ that we need to test for dynamical irreducibility over \mathbb{F}_p , which leads us to look for patterns.

Research Questions

Our goal is to reduce the number of polynomials of the form $ax^d + c$ that we need to test for dynamical irreducibility over \mathbb{F}_p , which leads us to look for patterns.

- Can we establish a relationship between the adjusted critical orbits of two conjugate polynomials?
- When do two polynomials have the same adjusted critical orbit?
- Can we predict pairs a, c that yield polynomials which remain dynamically irreducible even after increasing degree?
- When do two conjugate polynomials with degree 3 remain conjugate with degree 3^j ?

Theorem

Let $f(x) = ax^d + c \in \mathbb{F}_p[x]$, and let $k \in \mathbb{F}_p$ such that $k^d \equiv 1 \pmod{p}$. Then $ACO(f) = ACO(kf)$.

Results

Theorem

Let $f(x) = ax^d + c \in \mathbb{F}_p[x]$, and let $k \in \mathbb{F}_p$ such that $k^d \equiv 1 \pmod{p}$. Then $ACO(f) = ACO(kf)$.

Example

Let $f(x) = x^3 + 5 \in \mathbb{F}_{19}[x]$ and $k = 7$, so $kf(x) = 7x^3 + 16$.

Since $7^3 \equiv 1 \pmod{19}$, $ACO(f) = \{14, 16\} = ACO(kf)$.

Results

Theorem

Suppose $f(x) = ax^3 + c$ and $g(x) = \hat{a}x^3 + \hat{c}$ for $f, g \in \mathbb{F}_p[x]$, $p > 7$ such that $\hat{a}\hat{c}^2 = ac^2$. Then $f^\varphi = g$ for some $\varphi(x) = \alpha x$ if and only if $\ell \text{ACO}(f) = \text{ACO}(g)$ where $\ell \equiv \alpha^3 \pmod{p}$ and $(a/\hat{a})^3 = \ell^2$.

Proof.

(\Rightarrow) First element of $\text{ACO}(g)$ is $-\frac{c\alpha}{a(\alpha^2)^{-1}}$, or $\alpha^3 \left(-\frac{c}{a}\right)$. Proceed with induction

(\Leftarrow) $\alpha^3(c/a) = \hat{c}/\hat{a}$, so $\hat{c} = \alpha^3(c\hat{a}/a)$, and $\alpha^3(f(c)/a) = g(\hat{c})/\hat{a}$. Then we see that $(\alpha c)^3 = (\hat{c})^3$, so $\hat{c} = \alpha c$, and then we can solve for \hat{a} and find that $\hat{a} = a/\alpha^2$. □

Example

Let $f(x) = 4x^3 + 18, g(x) = x^3 + 2 \in \mathbb{F}_{19}[x]$.

$ACO(f) = \{5, 13, 3\}$ and $ACO(g) = \{17, 10, 14\}$

Let $\ell = 11$. Then $4^3 \equiv 7 \equiv 11^2 \pmod{19}$.

$\ell ACO(f) = \{11 \cdot 5, 11 \cdot 13, 11 \cdot 3\} = \{17, 10, 14\} = ACO(g)$

$17^3 \equiv 11 \pmod{19} \Rightarrow \varphi(x) = 17x$ conjugates f to g

Theorem

Suppose $f(x) = ax^3 + c \in \mathbb{F}_p[x]$ is dynamically irreducible. If $c^3 \equiv 1 \pmod{p}$ and $(a+c)^3 \equiv 1 \pmod{p}$, or if $c^3 \equiv -1 \pmod{p}$ and $(c-a)^3 \equiv -1$, then $f_d(x) = ax^d + c$ is dynamically irreducible for all $d = 3^j$ where $j > 0$.

Results

Theorem

Suppose $f(x) = ax^3 + c \in \mathbb{F}_p[x]$ is dynamically irreducible. If $c^3 \equiv 1 \pmod{p}$ and $(a+c)^3 \equiv 1 \pmod{p}$, or if $c^3 \equiv -1 \pmod{p}$ and $(c-a)^3 \equiv -1$, then $f_d(x) = ax^d + c$ is dynamically irreducible for all $d = 3^j$ where $j > 0$.

Example

Let $f(x) = 6x^3 + 1 \in \mathbb{F}_{19}[x]$, so f is dynamically irreducible. Since $1^3 \equiv 1 \pmod{19}$ and $(6+1)^3 \equiv 7^3 \equiv 343 \equiv 1 \pmod{19}$, $f_d = 6x^d + 1$ is dynamically irreducible for all $d = 3^j$ where $j > 0$.

Results

When are two conjugate polynomials of degree 3 still conjugate with degree 3^j ?

Results

When are two conjugate polynomials of degree 3 still conjugate with degree 3^j ?

Theorem

Let $f_3(x) = ax^3 + c \in \mathbb{F}_p[x]$ and $\varphi(x) = \alpha x$ for $\alpha \in \mathbb{F}_p$ such that $\text{ord}(\alpha) = n$, and consider $g_3(x) = \hat{a}x^3 + \hat{c} \in \mathbb{F}_p[x]$ where $g_3 = f_3^\varphi$. Then $f_d^\varphi = g_d$ for all $d = 3^j$, $j \in \mathbb{Z}_{>0}$ if and only if $3^j \equiv 3 \pmod n$.

Proof.

$(\Rightarrow) g_d(x) = a(\alpha^{d-1})^{-1}x^d + c\alpha$ and $g_3(x) = a(\alpha^2)^{-1}x^3 + c\alpha$, so $d - 1 \equiv 2 \pmod n$

$(\Leftarrow) d \equiv 3 \pmod n$, so $(\alpha^{d-1})^{-1} \equiv (\alpha^2)^{-1} \pmod p$ □

$$\begin{array}{ccc}
 f_3 & \xrightarrow{\varphi} & g_3 \\
 \downarrow & & \downarrow \\
 f_d & \xrightarrow{\varphi?} & g_d
 \end{array}$$

Example

Let $f_3(x) = x^3 + 5 \in \mathbb{F}_{19}[x]$, and take $\varphi(x) = 8x$. Then $f_3^\varphi(x) = 11x^3 + 2$, and $\text{ord}(8) = 6$. Since $3^2 \equiv 3 \pmod{6}$, $f_9(x) = x^9 + 5$ is conjugate to $f_9^\varphi(x) = 11x^9 + 2$.

Some Data

When do dynamically irreducible polynomials of degree 3 remain dynamically irreducible over degree 3^j ?

Some Data

When do dynamically irreducible polynomials of degree 3 remain dynamically irreducible over degree 3^j ?

Let $p = 31$. Below is a table of some pairs a, c that yield dynamically irreducible polynomials of the form $ax^d + c \in \mathbb{F}_{31}[x]$ where $d = 3^j$.

a	c	conditions
1	9	$j \not\equiv 0 \pmod{4}$
2	5	$j \equiv 1, 3 \pmod{4}$
2	22	$j \equiv 1 \pmod{4}$
3	2	$j \equiv 0, 1 \pmod{4}$
4	11	$j \equiv 1, 2 \pmod{4}$

Further Questions

If $f(x) = ax^d + c \in \mathbb{F}_p[x]$ and $k \in \mathbb{F}_p$ where $k^d \not\equiv 1 \pmod{p}$, can we predict the changes to the adjusted critical orbits?

Example

$$f(x) = 4x^3 + 1 \in \mathbb{F}_{19}[x], ACO(f) = \{14, 6, 16\}$$

k	$\text{ord}(k)$	$ACO(kf)$
5	9	$\{14, 16\}$
8	6	$\{14, 4, 13, 16\}$
13	18	$\{14, 17\}$
18	2	$\{14, 4, 13, 16\}$

Further Questions

Conjecture

Let $f(x) = ax^d + c \in \mathbb{F}_p[x]$ be dynamically irreducible, and suppose there exists $k \in \mathbb{F}_p$ such that $kf(x)$ is dynamically irreducible. Then there exists a dynamically irreducible $g(x) = \hat{a}x^d + \hat{c} \in \mathbb{F}_p[x]$ such that $ACO(kf) = ACO(g)$, and there exists $j \in \mathbb{F}_p$ such that $fg(x)$ is dynamically irreducible and $ACO(jg) = ACO(f)$.

Example

$$f(x) = x^3 + 10 \in \mathbb{F}_{31}[x], ACO(f) = \{21, 18, 14, 26, 9\}$$

$$k = 23 \Rightarrow kf(x) = 23x^3 + 13, ACO(kf) = \{21, 6, 26\}$$

$$g(x) = 22x^3 + 3, j = 11 \Rightarrow jg(x) = 25x^3 + 2$$

$$ACO(kf) = ACO(g) \text{ and } ACO(jg) = ACO(f)$$

Thank you!