Dynamics of Polynomials over Finite Fields

Holly Miller and Violet Nguyen
Advised by Michael Merkle and Dr. Lawton

Mason Experimental Geometry Lab

May 5, 2023

Motivation

Definition

A *planar conic section* is the set of zeroes (variety) in the plane to a polynomial of the form $C_1x^2 + C_2xy + C_3y^2 + C_4x + C_5y + C_6$. For example, the unit circle $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 - 1 = 0\}$ is a conic section.

We can represent each conic section with a point in 5 dimensional projective space $\mathbb{R}\mathrm{P}^5$, the classical moduli space of conic sections.

Creating a Dynamical System

We put a dynamical system on the space of polynomials of arbitrary degree and variable count over finite fields.

Definition

Let $n, d \in \mathbb{N}$ and $\mathbb{F}_q$ be a finite field of order q. We let $\mathrm{GL}_n(\mathbb{F}_q)$ act on $\mathcal{P}_{n,d,q} = \{f \in \mathbb{F}_q[x_1, \dots, x_n] \mid \mathrm{totaldeg}(f) \le d\}$ by

$$A \cdot f(\vec{x}) = f(A^{-1}\vec{x}),$$

where $f \in \mathcal{P}_{n,d,q}$ and $A \in \mathrm{GL}_n(\mathbb{F}_q)$.

Simple Example

Example

Let $n = d = q = 2$. This is the effect of a generator of $\mathrm{GL}_2(\mathbb{Z}_2)$ on $x^2 + xy$. First compute multiplication on the formal symbols,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix},$$

and then compose with the polynomial function:

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \cdot (x^2 + xy) &= (x+y)^2 + (x+y)y \\ &= x^2 + 2xy + y^2 + xy + y^2 \\ &= x^2 + 2xy + xy + 2y^2 \\ &= x^2 + xy. \end{aligned}$$

Note: $2xy = 2y^2 = 0$ since $2 = 0 \bmod 2$.

Fixed Points

Definition

A polynomial f is *fixed* or an *invariant* if for all $A \in \mathrm{GL}_n(\mathbb{F}_q)$, $A \cdot f = f$.

Theorem

Let $[f]$ denote the equivalence class of $f \mod \sim$. Then, f is fixed if and only if $[f]$ is fixed. This allows us focus just on the non-projective case for now.

Invariant Counting

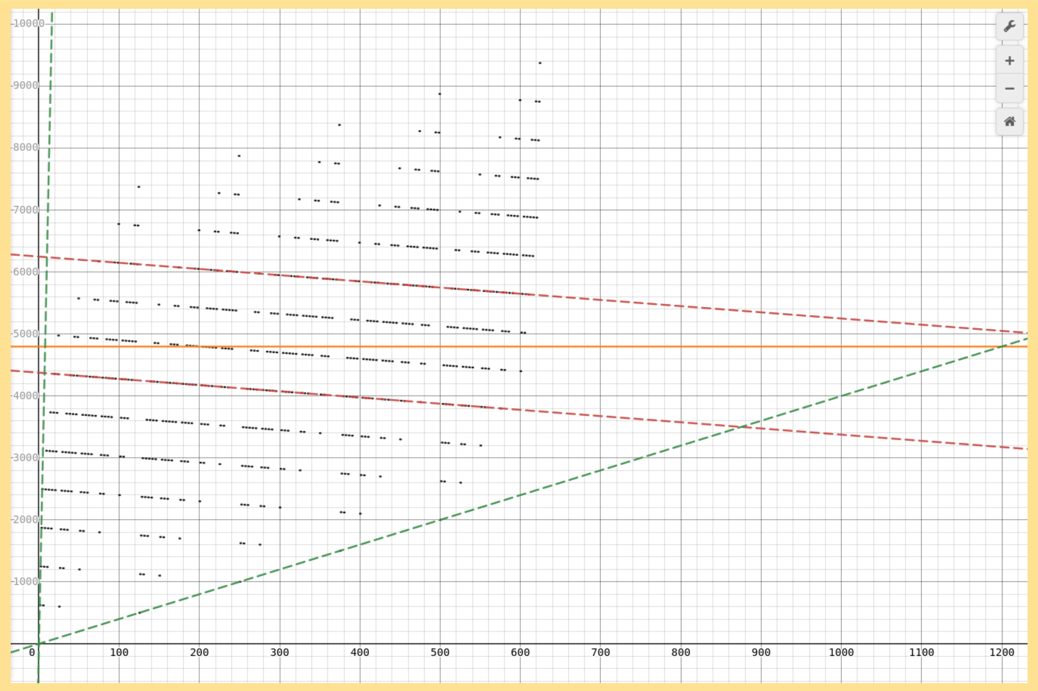

Figure: Bounding C-lines (red) for total degree (orange) and fastest + slowest growing degrees (green) ($q = 5$, $n = 4$)

Definition

We define a mapping of the I-monomials into $\mathbb{N}^2$ by

$$I^{\vec{\alpha}} \mapsto \left(\sum_{i=0}^{n-1} \alpha_i q^i, \mathrm{totaldeg}_{\vec{x}}(I^{\vec{\alpha}}) \right).$$

Counting the number of invariants under a certain total degree d then resolves to finding the number of points in the image that lie "along and under the line $y = d$".

Computed Examples

- $\mathcal{F}(10, 2, 2) = 12288$
- $\mathcal{F}(20, 2, 2) = 16,492,674,416,640$
- $\mathcal{F}(50, 3, 3) = 13,122$
- $\mathcal{F}(80, 3, 3) = 62,762,119,218$
- $\mathcal{F}(400, 3, 5) = 381,469,726,562,500$

Dickson's Theorem [1]

Definition

Denote $|m_1m_2\cdots m_n|$ to mean $\det[x_i^{q^{m_j}}]_{ij}$. Then, define $I_r = |01\cdots(r-1)\ (r+1)\ \cdots n|/|01\cdots n-1|$.

Theorem

The set of fixed points $\mathbb{F}_q[x_1, \dots, x_n]^{\mathrm{GL}_n(\mathbb{F}_q)}$ is a polynomial algebra generated by $\{I_r : 0 \le r < n\}$.

Example

Let $n = q = 2$. Then, $\mathbb{Z}_2[x, y]^{\mathrm{GL}_n(\mathbb{Z}_2)}$ is generated by

- $I_0 =$

$$|12|/|01| = \frac{\begin{vmatrix} x^2 & x^4 \\ y^2 & y^4 \end{vmatrix}}{\begin{vmatrix} x & x^2 \\ y & y^2 \end{vmatrix}} = \frac{x^2y^4 + x^4y^2}{xy^2 + x^2y} = xy^2 + x^2y \text{ and}$$

Fixed Point Function

- $I_1 =$

$$|02|/|01| = \frac{\begin{vmatrix} x & x^4 \\ y & y^4 \end{vmatrix}}{\begin{vmatrix} x & x^2 \\ y & y^2 \end{vmatrix}} = \frac{xy^4 + x^4y}{xy^2 + x^2y} = x^2 + xy + y^2.$$

Definition

Define $\mathcal{F} : \mathbb{N}_+ \times \mathbb{N} \times \{p^m : p \text{ prime}, m \in \mathbb{N}_+\} \to \mathbb{N}$ by

$$\mathcal{F}(n, d, q) = \left| \mathcal{P}_{n,d,q}^{\mathrm{GL}_n(\mathbb{F}_q)} \right| = |\{f \in \mathbb{F}_q[x_1, \dots, x_n] : f \text{ fixed}\}|,$$

the number of fixed points of total degree d in $\mathbb{F}_q[x_1, \dots, x_n]$.

This function has a closed form when $n = 2$.

Asymptotic Transitivity

Definition

We say that the action is *asymptotically transitive* for a specific n and d if

$$\lim_{q \to \infty} \frac{\max\{|\mathrm{Orb}(f)| \ : \ f \in \mathcal{P}_{n,d,q}\}}{|\mathcal{P}_{n,d,q}|} = 1$$

Note: Asymptotic Transitivity was introduced by Cigole Thomas in her 2022 Ph.D. thesis [2].

Theorem

The action is never transitive nor asymptotically so before the quotient.

Theorem

The action NOT transitive but IS asymptotically so on linear projective space $\mathcal{P}^*_{1,d,q}/\sim$.

Transitivity

Definition

The action is transitive on a set of polynomials S if for all $f, g \in S$, there exists a matrix $A \in \mathrm{GL}_n(\mathbb{F}_q)$ so $A \cdot f = g$. Equivalently, S is a subset of a single orbit.

Theorem

Because of the degree preserving property of the action, it is never transitive on $\mathcal{P}_{n,d,q}$ nor $\mathcal{P}^*_{n,d,q}/\sim$.

Full Orbits

Definition

The *orbit* of a polynomial f is $\mathrm{Orb}(f) = \{A \cdot f : A \in \mathrm{GL}_n(\mathbb{F}_q)\}$. An orbit is *full* if it has the same cardinality as $\mathrm{GL}_n(\mathbb{F}_q)$.

Theorem

There is a full orbit in $\mathcal{P}_{n,d,q}$ if $d > n$. In the case where $q = 2$, it is sufficient for $d \ge n$.

Unanswered Questions

- Compute the stabilizer group $\mathrm{Stab}(f) = \{A \in \mathrm{GL}_n(\mathbb{F}_q) : A \cdot f = f\}$, and have it act on the variety $V(f) = \{\vec{u} \in \mathbb{R}^n : f(\vec{u}) = 0\}$. What is the relationship between these two dynamical systems?
- We only looked at the extreme orbits (fixed orbits, transitive orbits, and full orbits). What is the entire spectra of orbits?
- Will Dr. Lawton ever be satisfied of his thirst for blood?[a]

[a] Gabe's Conjecture: No.

Acknowledgments

Thank you to Dr. Lawton and Michael Merkle for their time spent making this project happen. Thank you as well to all of those other professors and graduate students, undergrad MEGLers, and all past and current members of the lab management team that make MEGL happen and make the lab a vibrant, enjoyable community.

References

[1] Robert Steinberg. On dickson's theorem on invariants. *Journal of the Faculty of Science. University of Tokyo. Section IA. Mathematics*, 34:699–707, 1987.

[2] Cigole Thomas. *Stratification and Arithmetic Dynamics on Character Varieties.* ProQuest LLC, Ann Arbor, MI, 2022. Thesis (Ph.D.)–George Mason University.