Dynamics on Polynomials over Finite Fields

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

Mason Experimental Geometry Lab

George Mason University

Fall 2022

Introduction

The aim of this project is to study dynamical systems of polynomials. We replace indeterminants in a multivariate polynomial with degree-1 polynomials with coefficients from the rows of invertible matrices over finite fields. We are broadly interested in the system's "level of stability" and the "size of the orbits". More specifically we attempt to:

1. Find a general form for the fixed points.
2. Find out what variables we can tweak in the problem setting to ensure or eliminate fixed points.
3. Find polynomials that achieve maximum orbit cardinality.
4. Describe the dynamical system's structure for each degree d.

Foundational Definitions

Definition (Fields, Polynomials, and Matricies)

1. General fields are denoted $\mathbb{F}$, and a finite field with cardinality q is denoted $\mathbb{F}_q$.
2. The set of polynomials in m variables over a field $\mathbb{F}$ is $\mathbb{F}[x_1, \cdots, x_m]$. Those with degree at most d are denoted $\mathcal{P}_{m,d}(\mathbb{F})$, or $\mathcal{P}^*_{m,d}$ if 0 is removed. The subset of degree d *homogeneous* polynomials—polynomials that only contain degree d terms—is written as $\mathcal{H}_{m,d}(\mathbb{F})$.
3. The collection of $m \times m$ matrices over a field $\mathbb{F}$ is denoted $\mathcal{M}_m(\mathbb{F})$. The invertible matrices are denoted $\mathrm{GL}_m(\mathbb{F})$.

Definition (Group Actions)

- A group is a set G with an operation $\cdot : G \times G \to G$ that is associative, has an identity element, and has per-element inverses. Given any set X, the collection of permutations on its elements—denoted S_X—is a group.
- A *homomorphism* $\varphi : G \to H$ is a function between two groups (G and H) that preserves their operation, in that $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$.
- Given a group G and a set X, an *action* of $G \circlearrowleft X$ is a homomorphism $\varphi : G \to S_X$.
- Given an action $G \circlearrowleft X$, the *orbit* of $x \in X$ is the set $\mathrm{Orb}_G(x) = \{g \cdot x : g \in G\}$. The collection of orbits is denoted X/G. If there is a single orbit, it is said to be *transitive*.
- Given an action $G \circlearrowleft X$, the *stabilizer* of $x \in X$ is the set $\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$. If $\mathrm{Stab}_G(x) = G$, then x is said to be a *fixed point*.

Definition (How to Replace Indeterminants)

1. We define an action $\mathrm{GL}_m(\mathbb{F}) \circlearrowleft \mathbb{F}[x_1, \ldots, x_m]$ by, if $g \in \mathrm{GL}_m(\mathbb{F})$ has form $g = [\![g_{ij}]\!]$ and $f \in \mathbb{F}[x_1, \ldots, x_m]$ has form $f = \sum_{\alpha \in \mathbb{N}^m} \lambda_\alpha x_1^{\alpha_1} \cdots x_m^{\alpha_m}$, then $g^{-1} \cdot f = \sum_{\alpha \in \mathbb{N}^m} \lambda_\alpha (\sum_{j=1}^m g_{1j} x_j)^{\alpha_1} \cdots (\sum_{j=1}^m g_{mj} x_j)^{\alpha_m}$.

Summary

- The action is linear and degree preserving over finite fields—in fact it permutes the degree d homogeneous polynomials.
- The orbits and stabilizers of the polynomials of $\mathcal{P}_{m,d=1}$ are known.
- Fixed points are rare.
- To have $f \in \mathcal{P}_{m,d}$ with $|\mathrm{Orb}_{\mathrm{GL}_m(\mathbb{F}_q)}(f)| = |\mathrm{GL}_m(\mathbb{F}_q)|$, it is sufficient to let $d > m$.
- There is... so much code.
- There is a truly frightening amount of code documentation.

Some Details

Structure of the Action:

When working with any field $\mathbb{F}$, one can prove via induction that $\mathrm{GL}_m(\mathbb{F})$'s action permutes the degree d homogeneous polynomials ($\forall d \in \mathbb{N}$). Then since the action is linear, the orbit of a polynomial f is determined entirely by the orbits of its homogeneous components.

Orbits in the Degree $d = 1$ Case: (Finite Field)

All elements of $\mathcal{H}_{m,d=1}(\mathbb{F}_q)$ belong to a single orbit. Since $(g \cdot g^{-1})f = f$ for all $g \in \mathrm{GL}_m(\mathbb{F}_q)$ and $f \in \mathbb{F}_q[x_1, \ldots, x_m]$, this (mostly) resolves to checking that for every $h \in \mathcal{H}_{m,d=1}$, there is $g \in G$ for which $g^{-1} \cdot x_1 = h$. But $g^{-1} \cdot x_1 = \sum_{j=1}^m g_{1j} x_j$, so this resolves to confirming that for every ordered selection of field elements, there is an invertible matrix with that selection as a row. The linearity of the action and fixture of constants finish the orbit description.

Stabilizer Subgroups of Actions:

Given an action $G \circlearrowleft X$ and an element $g \in G$, the stabilizer subgroup of $g \cdot x$ is given by $g^{-1}\mathrm{Stab}_G(x)g = \{ghg^{-1} : h \in \mathrm{Stab}_G(x)\}$. If $k \in g\,\mathrm{Stab}_G(x)g^{-1}$, then $k = ghg^{-1}$ $h \in \mathrm{Stab}_G(x)$, so $k \cdot (g \cdot x) = (ghg^{-1}g) \cdot x = (g \cdot (h \cdot x)) = g \cdot x$. By this same argument, if $h \in \mathrm{Stab}_G(gx)$, then $g^{-1}hg \in \mathrm{Stab}_G(x)$, so $g(g^{-1}hg)g^{-1} \in g\,\mathrm{Stab}_G(x)g^{-1}$.

This is useful as it gives an isomorphism between stabilizer subgroups of "set elements" in the same orbit. It is especially nice when all elements belong to a single orbit. In particular $\mathrm{Stab}_{\mathrm{GL}_m(\mathbb{F}_q)}(f)$ can be found from $\mathrm{Stab}_{\mathrm{GL}_m(\mathbb{F}_q)}(x_1)$, for all $f \in \mathcal{H}_{m,d=1}(\mathbb{F}_q)$.

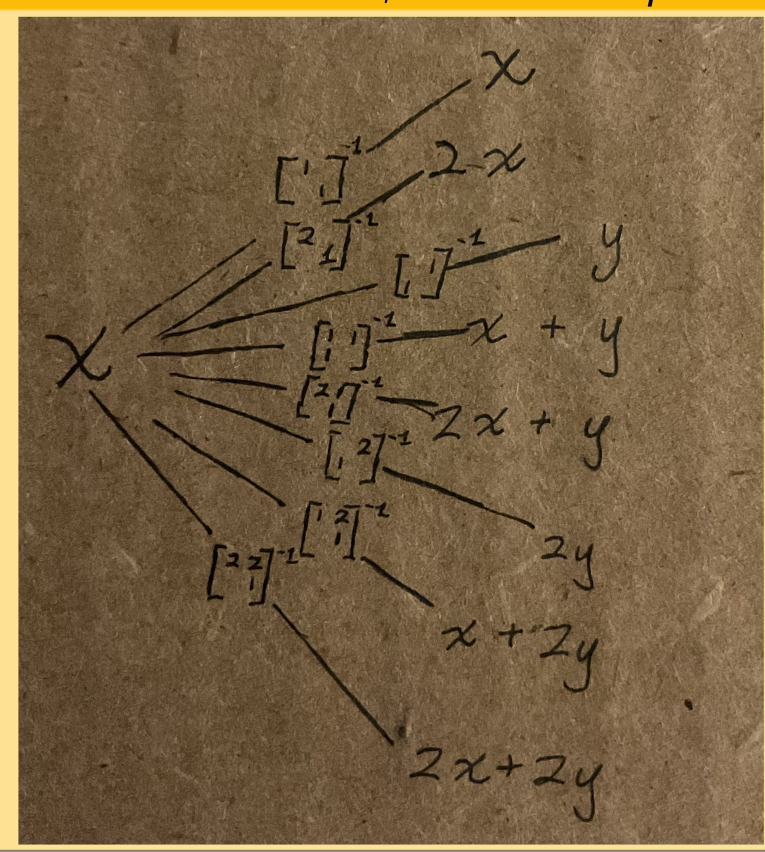
Maximizing Orbits: (Finite Field)

If a non-identity $g^{-1} \in \mathrm{GL}_m(\mathbb{F}_q)$ is diagonal, its action changes coefficients, but "fixes" monomials, and so $x_1 + \cdots + x_m$ will be moved by g^{-1}. If the g^{-1} has off-diagonal entries on some row i, it won't fix any power of the monomial x_i. Thus, $|\mathrm{Orb}_{\mathrm{GL}_m(\mathbb{F}_q)}(\sum_{i=1}^m x_i + \sum_{i=1}^m x_i^{i+1})| = |\mathrm{GL}_m(\mathbb{F}_q)|$.

Fixed Points: (Finite Field)

For $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ to be fixed, it is necessary that every exponent α_i of every term $\lambda x_1^{\alpha_1} \cdots x_m^{\alpha_m}$ be a multiple of $|\mathbb{F}_q - \{0\}|$, or else we can engineer a diagonal matrix that fixes monomials but changes λ. This is not a sufficient condition—in fact no element of $\mathcal{H}_{m=2,d=3}(\mathbb{F}_2)$ is fixed. (see graph to right)

Example for Orbit Traversal, $d = 1$ and $q = 3$ Case



Future Work

1. Read Robert Steinberg's *On Dickson's Theorem on Invariants* (it may solve the fixed point part of our project).
2. Finish transition of code from Python to C.
3. Full classification of the degree $d = 2$ case.
4. Sharpen conditions on occurrence of cardinality $|\mathrm{GL}_m(\mathbb{F}_q)|$ orbits.
5. Explore the dynamics induced on polynomial roots.
6. Explore the behavior of the orbits for large $m, d, \&\ q$.

Acknowledgments

- We would like to collectively thank Dr. Lawton for providing his enthusiasm for mathematics well past any scheduled time constraints would require, for providing his advice and expertise, and for starting the lab in the first place
- We would like to thank Michael Merkle for providing his time, energy, and ideas to this project
- We would like to thank Dr. Bray and Martha Hartt for managing the MEGL lab, and we would like to thank Dr. Lukyanenko for managing it the year prior.

A Graph of Homogeneous Orbits when $m = 2, q = 2$, and $d \leq 3$

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$