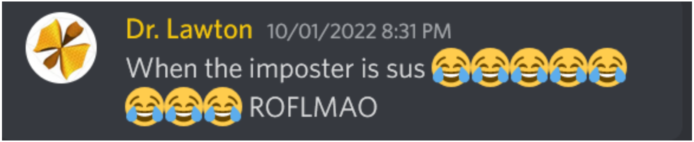
Dynamics on Polynomials over Finite Fields

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

George Mason University, MEGL

December 2nd, 2022



Definition

- A group is a set with an associative binary operation with an identity and per-element inverses.
- A group action of a group G on a set X is an operation $\cdot : G \times X \to X$ such that
  1. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$, and
  2. $e \cdot x = x$,

  for all $g_1, g_2 \in G$ and $x \in X$, and e is the identity of G.
- $\mathrm{GL}_m(\mathbb{F}) = \{A \in \mathrm{Mat}_{m\times m} \mid \det(A) \neq 0\}$ is the group of invertible matrices over a field $\mathbb{F}$.
- $\mathbb{F}[x_1, \ldots, x_m]$ is the set of polynomials with coefficients in $\mathbb{F}$ of the formal symbols $x_1, \ldots, x_m$.

Definitions and Notation

Definition

Let $m, d \in \mathbb{N}^+$ and $\mathbb{F}$ be a finite field.
We define $\mathcal{P}^*_{m,d}(\mathbb{F}) = \{f \in \mathbb{F}[x_1, \dots, x_m] \mid \mathrm{totaldeg}(f) \le d\} - \{0\}$, and let $\mathrm{GL}_m(\mathbb{F}) \circlearrowleft \mathcal{P}^*_{m,d}(\mathbb{F})$ by

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

for $g \in \mathrm{GL}_m(\mathbb{F}), f \in \mathcal{P}^*_{m,d}(\mathbb{F})$, and formal symbols $\vec{x} = (x_1, \dots, x_m)$. This action is linear and degree-preserving.

Note

In cases where $\mathbb{F} = \mathbb{Z}_p$ for some prime p, we amend our notation to $\mathcal{P}^*_{m,d,p} := \mathcal{P}^*_{m,d}(\mathbb{F})$, and we mean that $\mathbb{F} = \mathbb{Z}_p$ when we say "let p be ..."

Remark

$|\mathcal{P}^*_{m,d}(\mathbb{F})| = |\mathbb{F}|^{\binom{m+d}{m}} - 1$ (Proof: "Stars and Bars").

Simple Example

Example 1.1

Let $m = d = p = 2$. 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,

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

and then compose with the polynomial function:

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

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

Simple Example Cont.

Definition

For a polynomial $f \in \mathcal{P}^*_{m,d}(\mathbb{F})$, its orbit is $\mathrm{Orb}(f) = \{g \cdot f \mid g \in \mathrm{GL}_m(\mathbb{F})\}$, and its stabilizer is $\mathrm{Stab}(f) = \{g \in \mathrm{GL}_m(\mathbb{F}) \mid g \cdot f = f\}$. An element f of $\mathcal{P}^*_{m,d}(\mathbb{F})$ is *fixed* if $\mathrm{Orb}(f) = \{f\}$, or equivalently, $\mathrm{Stab}(f) = \mathrm{GL}_m(\mathbb{F})$. All constant polynomials will be fixed.

Example 1.2

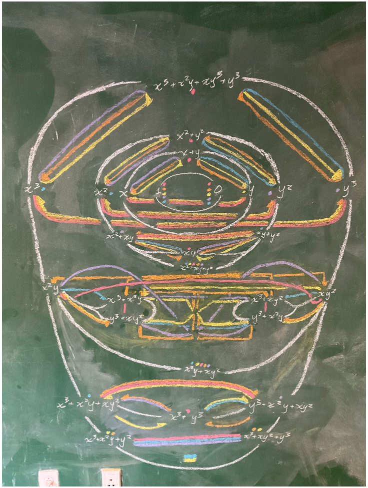
In the previous case,

$$\mathrm{Orb}(x^2 + xy) = \{x^2 + xy, y^2 + xy, xy\}$$

and

$$\mathrm{Stab}(x^2 + xy) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Orbits when $m = 3$ and $d = p = 2$:



Linear Polynomials

Definition

A polynomial is *homogeneous* if each term is of the same total degree. We define
$\mathcal{H}_{m,d}(\mathbb{F}) = \{f \in \mathcal{P}^*_{m,d}(\mathbb{F}) \mid \text{totaldeg}(f) = d, \text{ and } f \text{ is homogeneous}\}$. The action preserves homogeneity.

Theorem

Let $d = 1$, $m \in \mathbb{N}^+$, and $\mathbb{F}$ be a finite field. Define $\mathcal{M}_{m,d}(\mathbb{F}) = \{\text{Orb}(f) \mid f \in \mathcal{P}^*_{m,d}(\mathbb{F})\}$. We get that $|\mathcal{M}_{m,d}(\mathbb{F})| = 2|\mathbb{F}| - 1$, and if $f = q + k$, where $q \in \mathcal{H}_{m,d}(\mathbb{F})$ and $k \in \mathbb{F}$,

$$\text{Orb}(f) = \text{Orb}(q) + \text{Orb}(k) = \begin{cases} \mathcal{H}_{m,d}(\mathbb{F}) + k & \textit{if } q \neq 0 \\ \{k\} & \textit{otherwise} \end{cases}$$

Proof and Corollary

Lemma

Let $q \in \mathcal{H}_{m,1}(\mathbb{F})$. *There exists* $g \in \mathrm{GL}_m(\mathbb{F})$ *such that* $q = gx_1$.

Proof (Sketch).

By linearity, we get that if f decomposes into $q + k$, where $q \in \mathcal{H}_{m,1}$ and $k \in \mathbb{F}$, $\mathrm{Orb}(f) = \mathrm{Orb}(q) + k$. It suffices to show that $\mathrm{Orb}(q) = \mathcal{H}_{m,1}(\mathbb{F})$. Let $q_1, q_2 \in \mathcal{H}_{m,1}(\mathbb{F})$ and define g_1 and g_2 by the previous lemma. Then $q_2 = g_2 g_1^{-1} q_1$, so $\mathrm{Orb}(q) = \mathcal{H}_{m,1}(\mathbb{F})$. □

Corollary

All degree one polynomials have an orbit of size $|\mathbb{F}|^m - 1$, *and therefore have a stabilizer of order* $\prod_{i=1}^{m-1} \left(|\mathbb{F}|^m - |\mathbb{F}|^i\right)$ *via the Orbit-Stabilizer Theorem.*

Trying to work out $m = p = 2$, $d \in \mathbb{N}^+$

Theorem

Let $m = p = 2$ and $2 \leq d \in \mathbb{N}^+$. There exists polynomials that are fixed of total degree d, precisely, linear combinations of

$$\begin{cases} x^d + x^{\frac{d}{2}} y^{\frac{d}{2}} + y^d & \text{if } d \text{ is even} \\ x^{d-1}y + xy^{d-1} & \text{if } d \text{ is odd} \\ x^s y^r + x^r y^s & \text{if } d = s + r, \text{ where } s \text{ and } r \text{ are powers of } 2 \end{cases}$$

We do not know if these are the only fixed polynomials in this case.

Remark

Other than those above, we have yet to find any non-constant fixed points.

Super Ziqi Conjecture

Excluding constants, there are *NO* fixed points if $d \neq 2$ or $p \neq 2$.

The Data We Have (Initial Naive Implementation)

Fixed Point Data

$m = 2$

d \ p	2	3	5	7
1	$\star$	$\star$	$\star$	$\star$
2	$\square$	$\star$	$\star$	$\star$
3	$\square$	—	—	—
4	$\square$	—	—	—

$m = 3$

d \ p	2	3	5
1	$\star$	$\star$	$\star$
2	$\star$	—	—

Legend:

$\star$: No non-constant fixed points

$\square$: Existence of non-constant fixed points

—: No data

Note: Cardinalities blow up quickly. $|\mathcal{P}^*_{5,3,5}| \approx 1.39 \times 10^{39}$.

COUNTEREXAMPLE TO SUPER ZIQI CONJECTURE

A random paper that we found 2 weeks ago from 1911 shows us that this polynomial in particular is fixed if $m = 2$ and $p = 3$!!

$$x^6 + x^4y^2 + x^2y^4 + y^6$$

Wow. Look at that. So impressive, so cool. It doesn't care about what matrices think about it.

Asymptotic Transitivity

Definition

The action is *transitive* if $\mathcal{M}_{m,d}(\mathbb{F}) = \{\mathcal{P}^*_{m,d}(\mathbb{F})\}$, or that for every pair of f_1 and f_2, there exists $g \in \mathrm{GL}_m(\mathbb{F})$ such that $g \cdot f_1 = f_2$.
Let $M = \max\{|O| \mid O \in \mathcal{M}_{m,d,p}\}$. We say that the action is *asymptotically transitive* if

$$\lim_{p\to\infty} \frac{M}{|\mathcal{P}^*_{m,d,p}|} = 1.$$

The action is not transitive. However, is it ever asymptotically transitive for specific choices of m and d?

Remark

If $m^2 \leq \binom{m+d}{m}$, $\lim_{p\to\infty} |\mathrm{GL}_m(\mathbb{Z}_p)|/|\mathcal{P}^*_{m,d,p}| = 0$, and we have no hope of asymptotic transitivity.

Additional Theorems

Additional things we have proved:

Theorem (Fixed Points)

Every fixed polynomial must be symmetric, and $|\mathbb{F}| - 1$ *must divide each component of the multiexponent for each term. This is not a sufficient condition.*

Theorem (Maximal Orbits)

An orbit is _maximal_ *if it has the same cardinality as* $\mathrm{GL}_m(\mathbb{F})$*. There will always be a maximal orbit if* $d > m$*. In the special case where* $p = 2$*, there will always be a maximal orbit if* $d \geq m$*.*

Review of Accomplishments

- Came up with the problem for the project.
- Developed code to compute smaller cases that helped us prove some theorems.
- Proved that the action is linear, preserves homogeneity, and preserves multiplication.
- Solved the cases for $m = 1$ and $d = 1$ fully.
- Finding classes of fixed points for $m = p = 2$.
- Found necessary conditions for maximal orbits and fixed points.
- (Mostly) developed the improved code that will be use next semester.
- Basic observations for asymptotic transitivity using cardinality arguments.

Next Semester

- Interface our current results with the “local dynamics” of $\mathrm{Stab}(f) \circlearrowleft V(f)$, the variety of f.
- Finish and run the faster and more efficient code to find more patterns.
- Read *On Dickson’s theorem on invariants* by Robert Steinberg, which we think solves the fixed point problem and in particular disproves the Super Ziqi Conjecture.
- Work more on asymptotic transitivity, and find when it occurs.
- Sharpen the bound for maximal orbits.
- Wrap up the $d = 2$ case in general, and start working on $d = 3$.

Thanks

Many thanks to MEGL leadership and Dr. Bray for running the lab, and giving us the opportunity to work on this project.

Thanks to Michael Merkle for providing his time, energy, and ideas towards the project.

And lastly, thanks to Dr. Lawton for starting the lab in the first place, and his continued advising, support, and expertise throughout the semester—well past any reasonable expectation.