Longest Orbits over Varieties of Generalised Markoff Equations over Finite Fields

Marvin Castellon, Seth Lee, Kira Wolpert

Mason Experimental Geometry Lab

Aug 13, 2017

Abstract

- The automorphism group of the polynomial $\boldsymbol{k(x,y,z) = x^2 + y^2 + z^2 - xyz - 2}$ over a finite field $\mathbb{F}_p^3$ has a subgroup $\boldsymbol{\Gamma}$, consisting of polynomial automorphisms, whose orbit lengths are of particular fascination. The group $\boldsymbol{\Gamma}$ is generated by the automorphisms ι, τ, η and acts on the variety $\mathbb{V}(\boldsymbol{k - \lambda})$, for λ in $\mathbb{F}$. We are interested in the length of the longest orbit, denoted $\mathcal{L}_{\langle w \rangle}(\boldsymbol{p}, \lambda)$, for a fixed λ and prime $\boldsymbol{p}$, where $\langle \boldsymbol{w} \rangle$ is the cyclic subgroup generated by $\boldsymbol{w}$ in $\boldsymbol{\Gamma}$. The evaluation of our $\mathcal{L}$ function is complete for ι, τ, $\iota\tau$, and $\eta\iota$.
- A motivating conjecture is that these automorphisms will act transitively on the variety as $\boldsymbol{p}$ tends toward infinity. We hope to gain insight into how the group action is approaching transitivity by studying automorphisms of exceptionally large order. The automorphism $\eta\tau$ is of interest due to its orbits rate of growth as $\boldsymbol{p}$ increases; It appears to tend toward $\boldsymbol{p \log p}$. This is significantly larger than the linear growth rate of η, or the constant orders of ι, τ, $\iota\tau$, and $\eta\iota$.

Definitions

- The Markoff type Diophantine equation used here is $\boldsymbol{\kappa(x,y,z) = x^2 + y^2 + z^2 - xyz - 2}$
- We denote the κ varieties $\boldsymbol{\kappa(x,y,z) - \lambda = 0}$ as $\mathbb{V}(\kappa - \lambda)$
- There is a group of polynomial κ-automorphisms, $\boldsymbol{\Gamma}$, generated by three elements ι, τ and η given by the following maps (define the maps):

$$\tau \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \\ \boldsymbol{z} \end{pmatrix} = \begin{pmatrix} \boldsymbol{y} \\ \boldsymbol{x} \\ \boldsymbol{z} \end{pmatrix} \qquad \iota \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \\ \boldsymbol{z} \end{pmatrix} = \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \\ \boldsymbol{xy - z} \end{pmatrix} \qquad \eta \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \\ \boldsymbol{z} \end{pmatrix} = \begin{pmatrix} \boldsymbol{z} \\ \boldsymbol{y} \\ \boldsymbol{yz - x} \end{pmatrix}$$

- ι Is called a **Vieta involution** and η is a Vieta involution on the second coordinate followed by a permutation on the coordinates.
- For any $\varphi \in \boldsymbol{\Gamma}$ we define $\mathcal{L}_{\langle \varphi \rangle}(\boldsymbol{p}, \lambda)$ as $\boldsymbol{\max\{|Orb_{\langle \varphi \rangle}(v)| : v \in \mathbb{V}(\kappa - \lambda)\}}$
- We define

$$\mathcal{L}^{\boldsymbol{max}}_{\langle \varphi \rangle}(\boldsymbol{p}) := \max\{\mathcal{L}_{\langle \varphi \rangle}(\boldsymbol{p}, \lambda) : \lambda \in \mathbb{Z}_{\boldsymbol{p}}\}$$

$$\mathcal{L}^{\boldsymbol{avg}}_{\langle \varphi \rangle}(\boldsymbol{p}) := \frac{\boldsymbol{1}}{\boldsymbol{p}} \sum_{\lambda \in \mathbb{Z}_{\boldsymbol{p}}} \mathcal{L}_{\langle \varphi \rangle}(\boldsymbol{p}, \lambda)$$

Motivation $\boldsymbol{p \log p}$

- We suspect that of all the elements of $\boldsymbol{\Gamma}$ $\eta\tau$ and its conjugates produce the fastest growing $\mathcal{L}^{\boldsymbol{max}}_{\langle \varphi \rangle}$ and $\mathcal{L}^{\boldsymbol{avg}}_{\langle \varphi \rangle}$ functions
- We also suspect that the growth rate for the the $\mathcal{L}$ functions mentioned is $\boldsymbol{p \log p}$

Code

- The code we produced to compute orbits and the $\mathcal{L}$ function attempted to optimize one of two criteria, speed (usually at the cost of memory) or memory (at the cost of time)
- The code produced to maximize speed followed this formulation:
  - Store the entire space $\mathbb{Z}_{\boldsymbol{p}}^{\boldsymbol{3}}$ in memory and sort the points into their respective varieties
  - compute an orbit for a given point and set subtract that orbit from the stored space
- The code to optimize memory usage followed this formula:
  - induce a well ordering on $\mathbb{Z}_{\boldsymbol{p}}^{\boldsymbol{3}}$
  - go through each point in the space systematically and compute an orbit. If an orbit contains a another point less that the original point then computation of that orbit is terminated (this avoids redundancy and requires an extremely low amount of memory to run)

Figures

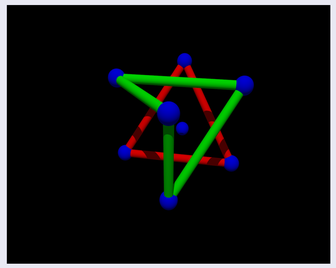

Figure: $\eta\tau$ orbits in $\mathbb{Z}_2^3$

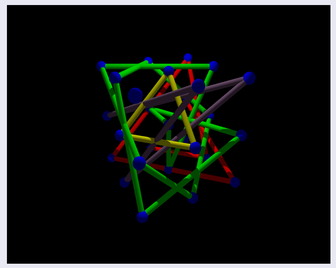

Figure: $\eta\tau$ orbits in $\mathbb{Z}_3^3$

Proofs for bounds on $\mathcal{L}$ function

- The orders of $\iota, \tau, \iota\tau$, and $\eta\iota$ are 2, So the maximum the $\mathcal{L}$ function is 2 for their cyclic subgroups
- Each of these only have finitely many examples where the $\mathcal{L}$ function evaluates to 1 instead of 2

Outline of Proof for an upper bound on $\mathcal{L}_{\langle \eta \rangle}(\boldsymbol{p}, \lambda)$

- We assume $\boldsymbol{char(\mathbb{F}) > 2}$
- Notice $\boldsymbol{y}$ is fixed by η, so fix a value for $\boldsymbol{y}$ and look at η restricted on the first and third coordinate
- Notice the resulting transformation is linear and is in $\boldsymbol{SL_2(\mathbb{Z}_p)}$
- Repeated application of a linear transformation can be understood by diagonalizing the matrix
- Using the Galois Group of the extension $\mathbb{F}_{\boldsymbol{p^2}}$ over $\mathbb{Z}_{\boldsymbol{p}}$ gives that the order of this linear transformation is bounded by $\boldsymbol{p + 1}$
- When the matrix is not diagonalizable it can be put in Jordan Normal Form, and this puts a bound of $\boldsymbol{2p}$ on the order, and hence the $\mathcal{L}$ function is bounded by $\boldsymbol{2p}$
- This result generalizes and results in a bound of $\boldsymbol{p^n + 1}$ in $\mathbb{F}_{\boldsymbol{p^n}}$ when $\boldsymbol{n > 1}$

- The end behavior of the $\mathcal{L}$ function for these elements is constant or linear
- $\eta\tau$ has a growth rate that appears to be larger than linear

Facts

- Any two elements in $\boldsymbol{\Gamma}$ that are conjugate to each other produce the same values for the $\mathcal{L}$ function (Conjugation is just a change of coordinates that preserves the varieties)
  - To see this note that $\boldsymbol{g\varphi g^{-1}}$ maps $\boldsymbol{g(v)}$ to $\boldsymbol{g(\varphi(v))}$
  - $\boldsymbol{\kappa(v) = \kappa(g(v)) = \kappa(g(\varphi(v)))}$ since all functions are κ automorphisms
  - This implies that $\boldsymbol{|Orb_{\langle \varphi \rangle}(v)| = |Orb_{\langle g\varphi g^{-1} \rangle}(gv)|}$
  - This produces a 1-to-1 correspondence between the orbits of φ and $\boldsymbol{g\varphi g^{-1}}$ that preserves orbit length since conjugation is invertable
- The end behavior of $\langle \iota, \tau \rangle$ and $\eta\iota$, are constant (all stabilize at 2)
- The end behavior of η is linear, ending at $\boldsymbol{2p}$
- The values of the $\mathcal{L}$ can never exceed quadratic growth since the size of the varieties is quadratic.

Data For $\mathcal{L}^{max}$ and $\mathcal{L}^{avg}$

- The graphs below show $\mathcal{L}^{\boldsymbol{max}}$ and $\mathcal{L}^{\boldsymbol{avg}}$ graphed against $\boldsymbol{p \log p}$ (that is the points plotted are $\boldsymbol{(p \log p, \mathcal{L}(p))}$).
- If the corresponding $\mathcal{L}$ functions tend to $\boldsymbol{p \log p}$ then there should be a linear relationship in the points as $\boldsymbol{p}$ becomes large

Graphs

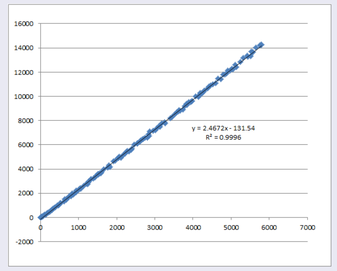

Figure: $\mathcal{L}^{\boldsymbol{avg}}_{\langle \eta\tau \rangle}$ graphed against $\boldsymbol{p \log p}$. The strong linear fit supports the $\boldsymbol{p \log p}$ conjecture

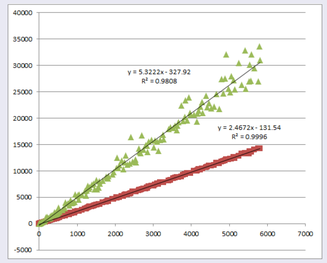

Figure: $\mathcal{L}^{\boldsymbol{avg}}_{\langle \eta\tau \rangle}$ and $\mathcal{L}^{\boldsymbol{max}}_{\langle \eta\tau \rangle}$ graphed against $\boldsymbol{p \log p}$. The max variant appears to not be as well behaved as the average, but still approximately has $\boldsymbol{p \log p}$ growth

Orbit length frequency

- There does appear to be (although not known to us) distribution curve for the frequency of each orbit length

Graphs

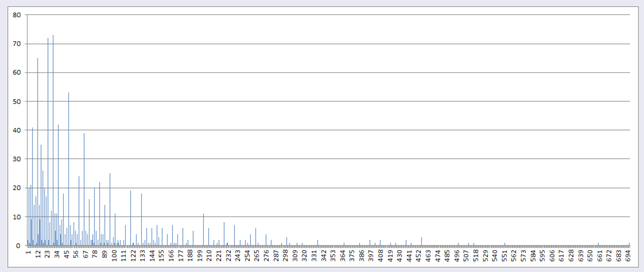

Figure: $\eta\tau$ orbit lengths when $\boldsymbol{p = 43}$ are placed on the horizontal axis with frequency in the vertical. There does appear to be a well behaved distribution curve for the frequencies.

Future Work

- Generalizing some statements and code to handle general finite fields
- Compare $\eta\tau$ data to other words of larger length from other nontrivial conjugacy classes

Acknowledgments

- Thanks to Dr. Lawton and Dr. Manon for the opportunity to work in the lab over the summer and providing an exciting environment to explore mathematics.
- Thanks to Dr. Wolpert for his sharp eyes.
- And thanks to the National Science Foundation for funding our lab!