Asymptotic Dynamics on Arithmetic Curves

Marvin Castellon, Cole Miller, and Cigole Thomas
Advisor: Dr. Sean Lawton

George Mason University, MEGL

December 8, 2017

Table of Contents

Problem

To understand the dynamics of the action of $Out(F_2)$ on the character variety $\mathfrak{X}_\lambda(F_2, \mathrm{SL}_2(\mathbb{F}_q))$.

Background

Let $\kappa = x^2 + y^2 + z^2 - xyz - 2$. Then the character variety can be thought of as the solutions of $\kappa = \lambda$ over affine 3-space.

Counting points in the variety

Let $\mathbb{F}_q$ be the finite field of q elements. We consider the equation

$$x^2 + y^2 + z^2 = axyz + b \tag{1}$$

for $(x, y, z) \in \mathbb{F}_q^3$, where $a, b \in Z/(p)$ are parameters. Let $M^3_{a,b}\mathbb{F}_q$ be the set of points in $\mathbb{F}_q^3$ solving this equation.

Theorem (J. Mariscal)

$$|M^3_{a,b}\mathbb{F}_q| = \begin{cases} q^2+3\epsilon q+1 & b \ = 0 \\ q^2+2\epsilon q+1 & b \text{ is a quadratic residue} \\ q^2+4\epsilon q+1 & b \text{ is a nonzero-quadratic residue} \end{cases}$$

$$\textit{where } \epsilon = \begin{cases} 1 & ba^2-4 \text{ is a quadratic residue of } \mathbb{F}_q \\ -1 & ba^2-4 \text{ is a quadratic non residue of } \mathbb{F}_q \\ 0 & ba^2-4=0 \end{cases}$$

Background, ctd.

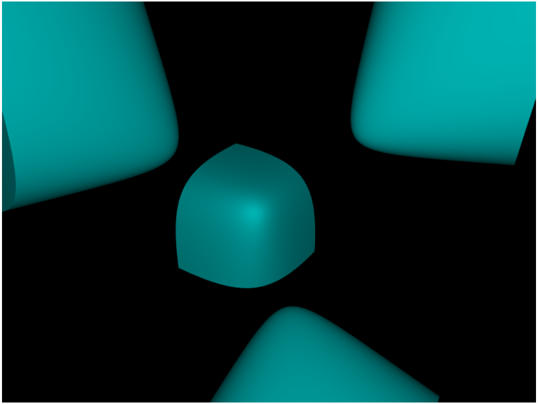
The polynomial κ arises naturally when we consider $\mathrm{SL}_2(k)$-representations of the free group F_2, where k is a field. *Vogt* and *Fricke* studied such representations.

- Note first that $\mathrm{Hom}(F_2, \mathrm{SL}_2(k))$ can be naturally identified with $H = \mathrm{SL}_2(k) \times \mathrm{SL}_2(k)$. The group $\mathrm{SL}_2(k)$ acts on H by componentwise conjugation.
- Define $\tau : H \to k^3$ by $\tau : (\zeta, \eta) \mapsto (\mathrm{tr}\,\zeta, \mathrm{tr}\,\eta, \mathrm{tr}\,\zeta\eta)$. Vogt and Fricke showed that if $f : H \to k$ is regular and invariant under the conjugation action, then it factors through τ: there is a polynomial function $F : k^3 \to k$ such that $f = F \circ \tau$.

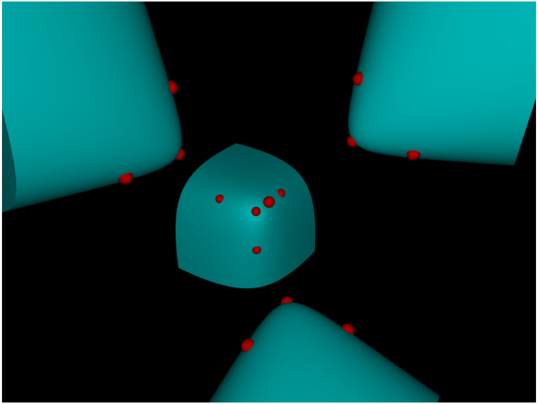
Background, ctd.

- We view τ as giving an isomorphism between k^3 and the quotient (suitably defined) of H by the conjugation action of $\mathrm{SL}_2(k)$.
- We have $\kappa(\tau(\zeta, \eta)) = \mathrm{tr}[\zeta, \eta]$, where $[\cdot, \cdot]$ is the multiplicative commutator.
- The Vogt-Fricke result lets us relate representations of F_2 to polynomials over k^3.

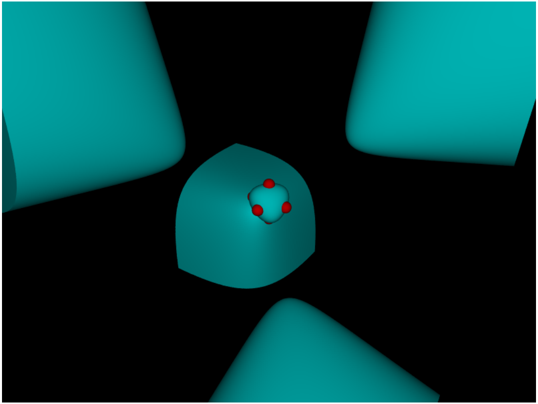
$\lambda = -3$ over $\mathbb{R}^3$



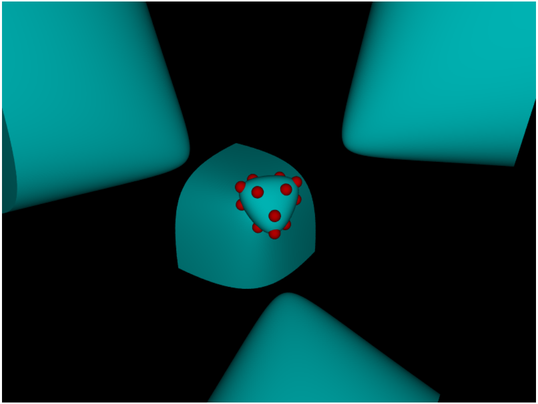
$\lambda = -2$ over $\mathbb{R}^3$



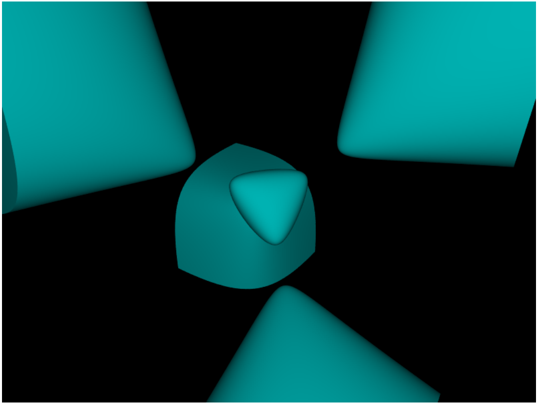
$\lambda = -1$ over $\mathbb{R}^3$



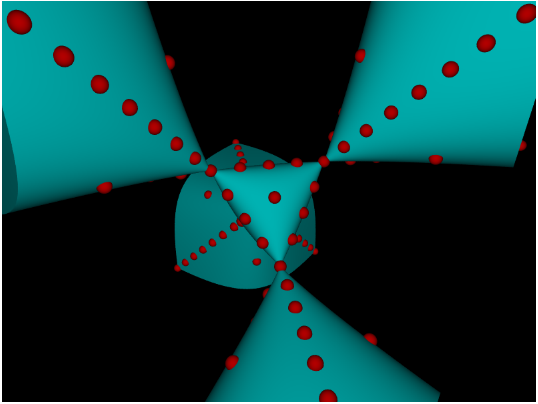
$\lambda = 0$ over $\mathbb{R}^3$



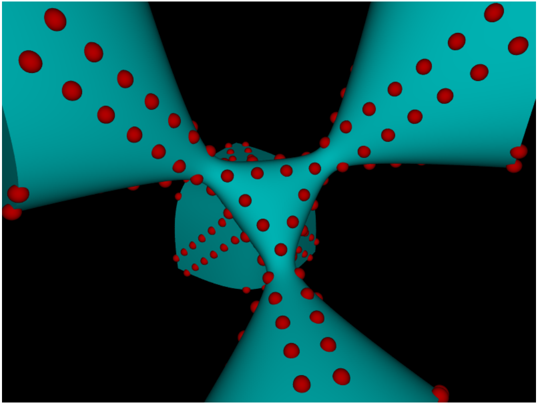
$\lambda = 1$ over $\mathbb{R}^3$



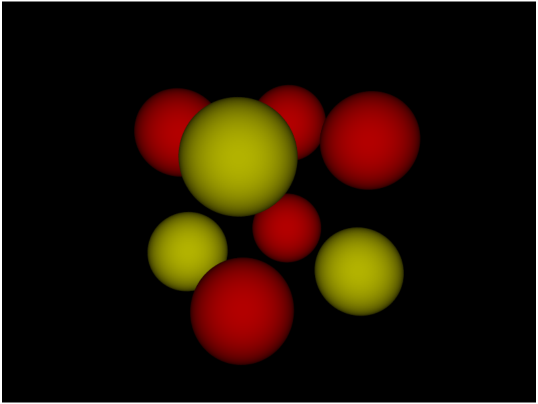
$\lambda = 2$ over $\mathbb{R}^3$



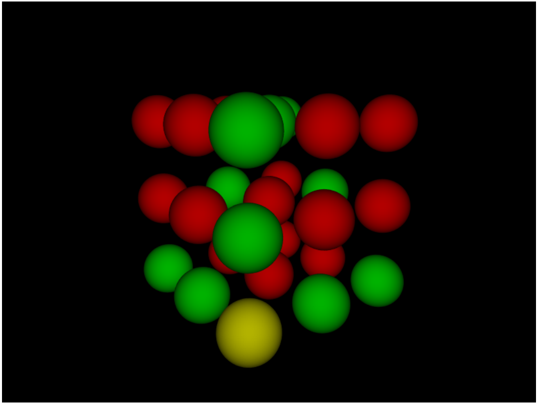
$\lambda = 3$ over $\mathbb{R}^3$



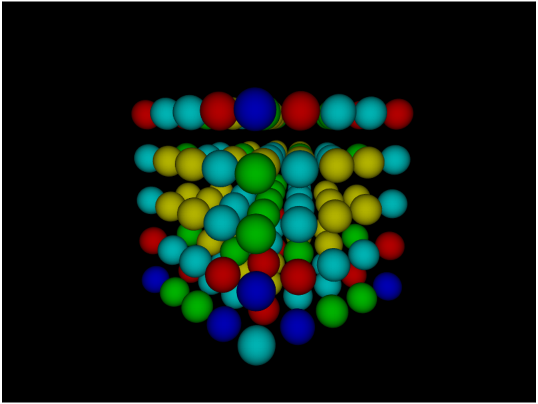
$\mathbb{Z}_2$ All varieties



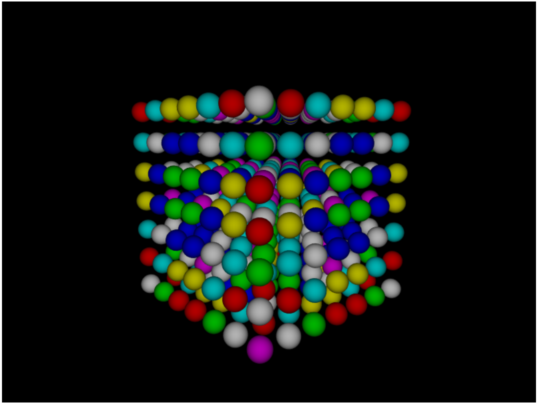
$\mathbb{Z}_3$ All varieties



$\mathbb{Z}_5$ All varieties



$\mathbb{Z}_7$ All varieties



Generators of $Out(F_2)$

Let F_2 be the free group of rank 2, generated by $\{\gamma_1, \gamma_2\}$. Then $Out(F_2) = \langle \iota, \tau, \eta \rangle$ where

$$\tau = \begin{cases} \gamma_1 \to & \gamma_2 \\ \gamma_2 \to & \gamma_1 \end{cases}$$

$$\iota = \begin{cases} \gamma_1 \to & \gamma_1^{-1} \\ \gamma_2 \to & \gamma_2 \end{cases}$$

$$\eta = \begin{cases} \gamma_1 \to & \gamma_1\gamma_2 \\ \gamma_2 \to & \gamma_2 \end{cases}$$

Action of $Out(F_2)$ on $\mathfrak{X}(F_2, \mathrm{SL}_2(\mathbb{F}_q))$

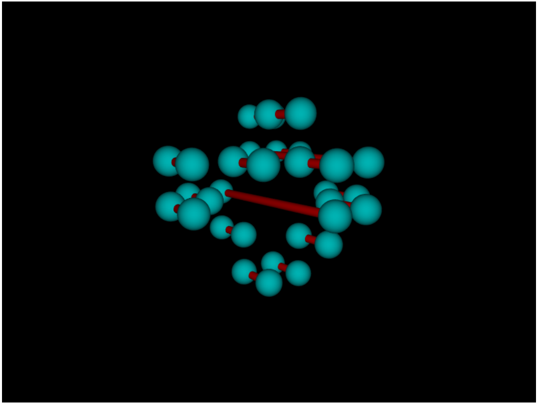
Consider the action of the outer automorphism group of F_2 on the character variety as given below.

$$\iota((x, y, z)) = (x, y, xy - z)$$

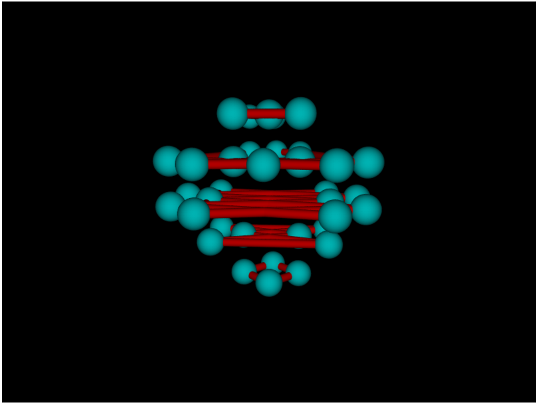
$$\tau((x, y, z)) = (y, x, z)$$

$$\eta((x, y, z)) = (z, y, yz - x)$$

ι on a $p = 5$ Variety



η on a $p = 5$ Variety



Few Definitions

Definition

$\mathcal{L}_G(q, \lambda)$ is the length of the largest G-orbit in $\mathbb{V}(\kappa - \lambda)$ over $\mathbb{F}_q$ where $G \leq \Gamma$.

Then define

$$\mathcal{L}_{G,\mathbb{V}_{\mathbb{F}_q}} = \max\{\mathcal{L}_G(q, \lambda) | \lambda \in \mathbb{F}_q\}$$

$$\mathcal{L}_G^{avg}(q) = \frac{1}{q} \sum_{\lambda \in \mathbb{F}_q} \mathcal{L}_G(q, \lambda)$$

Arithmetic Ergodicity

Let G be a group and $\mathbb{V}$ be a variety. Suppose $|G| \circlearrowleft \mathbb{V}_{\mathbb{F}_q}$, for all $q = p^n$, for prime p.

Definition

$G \circlearrowleft \mathbb{V}$ is arithmetically ergodic (AE) if

$$\lim_{q \to \infty} \frac{\mathcal{L}_{G,\mathbb{V}_{\mathbb{F}_q}}}{|\mathbb{V}_{\mathbb{F}_q}|} = 1$$

Questions

1. Find the length of largest orbit under the action on the finite field character variety.
2. Find elements that act arithmetically ergodically.

Special Words

- Goal: Find non-conjugate Γ words so that have the same asymptotics of $\eta\tau$. Recall we expect this to have a growth rate of $q \log q$
- To find such words we ran the computation $\mathcal{L}^{avg}$ for prime fields up to $p = 40$
- This was compared to 1, p, and $p \log p$. We work with the assumption that these the only possible orders. More on this later
- We found that the class of functions $\eta^k\tau$ appear to have $q \log q$ growth
- The $\mathcal{L}$ functions did not match identically, so these words in general are non-conjugate

Classification of Order Types

- We performed this special words project with the assumption that every element was of order 1, p, or $p \log p$
- Comparison was done by treating a finite data sets, x and y, as a vector and using:

$$\mathcal{C}(x, y) = \left(\frac{x \cdot y}{|x||y|}\right)^2$$

- This takes on a value close to 1 if x and y have similar asymptotics and close to 0 otherwise.
- Consistent values for $\mathcal{C}$ are around 0.99, giving the impression that all elements fall into one of these categories
- Classification of Order Conjecture: Every element in Γ will be asymptotic to 1, q, and $q \log q$

Progress on Classification Conjecture

- Constant order elements, other than the identity, include $\tau, \iota, \eta\iota$, and $\iota\tau$
- We showed during Summer 2017 that there exists elements of linear growth rate. Examples include η^k and their conjugates over Γ
- Strong experimental data suggests that at least $\eta\tau$ has $q \log q$ growth

Goal

- We suspect that the action of Γ should be arithmetically ergodic on all of the κ varieties
- One of our goals is to find a proper subset of Γ, S, so for all but a "small amount" of $v \in \mathbb{F}_q^3$:

$$\bigcup_{w \in S} \mathrm{Orb}_{\langle s \rangle}(v)$$

gives the arithmetically ergodicity result.
- This can be thought of as not needing all of Γ for arithmetic ergodicity

Suspects

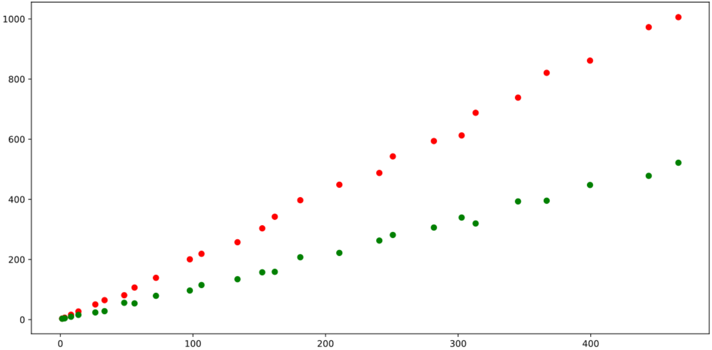
- Our first guess for such a set were the conjugates of $\eta\tau$, i.e. the set $\{\gamma\eta\tau\gamma^{-1}|\gamma \in \Gamma\}$
- This was promising in simulations that were run to $p = 50$. Right around $p = 100$ this began to fail, resulting a vanishing subset of the kappa varieties.
- Currently we have a promising set that may work. Recall the family f functions $\eta^k\tau$
- So far our simulations give that a subset of these functions cover about 99% of the varieties

The $q \log q$ Conjecture

- Conjecture: As a function of q we suspect $\mathcal{L}_{\langle \eta\tau \rangle}(q)$ $q \log(q)$
- We further suspect that the family of functions $\eta^k \tau$ also satisfy this property
- Even further we suspect that there are more $\eta\tau$-like elements

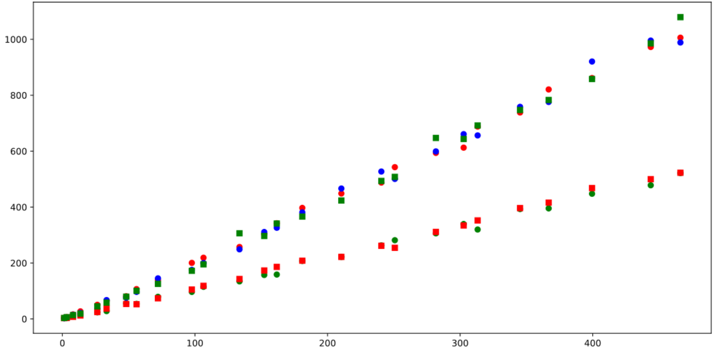
$\mathcal{L}^{avg}_{\eta^k\tau}$ Against $p \log p$ for $k = 1, 2$

Linear trend suggests that $\mathcal{L}^{avg}_{\eta\tau}$ and $\mathcal{L}^{avg}_{\eta^2\tau}$ have $p \log p$ growth



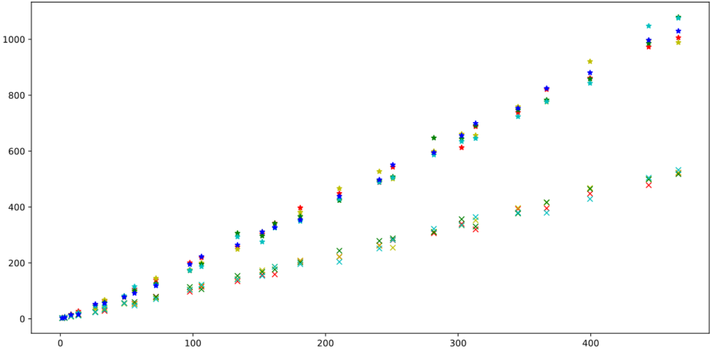
$\mathcal{L}^{avg}_{\eta^k T}$ Against $p \log p$ for $k = 1, 2, 2, 3, 5$

There appears to be a pattern. They all appear as having $p \log p$ growth, but with one set of them growing twice as fast as the others.



$\mathcal{L}^{avg}_{\eta^k \tau}$ Against $p \log p$ for $k = 1, \ldots, 9$

The Pattern: Odd powers of η composed with τ grow twice as fast as the even powers.



The Pisano Period Approach

- In the case when $\lambda = 2$, $\eta\tau$ takes on a Fibonacci Sequence pattern
- This equates to finding the order of the following matrix

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

  modulo some divisor of $(q^2 - 1)p$
- This allows us to find an upper bound on maximal length of an $\langle \eta\tau \rangle$ orbit
- So far our experimental results are inconclusive and largely incomplete
- As for theoretical bounds this would be as difficult as studying the Pisano Periods, which is hard

$\eta\tau$ Decomposition

- We note that $\eta\tau$ is a 3-cycle composed with a Vieta involution
- We can attempt to analyze the orbits of the 3-cycle and of the Vieta involution and see how they interact
- Idea: count how many times the orbits of the 3-cycle connect distinct Vieta orbits.
- This may be able to place an upper bound on the order of $\eta\tau$

Some useful results

Theorem (Bourgain, Gamburd and Sarnak)

Fix $\epsilon > 0$. Then for p large there is a Γ orbit $C(p)$ in $X^*(p)$ for which

$$|X^*(p) \setminus C(p)| \leq p\epsilon$$

(note that $|X^*(p)| \sim p^2$), and any Γ orbit $\mathcal{D}(p)$ satisfies

$$|\mathcal{D}(p)| \gg (logp)^{\frac{1}{3}}$$

Techniques Used

1. The Markoff surface $\mathbb{X}$ is the affine surface in $(\mathbb{Z}/p\mathbb{Z})^3$ given by $x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3 = 0$.
2. $X^*(p) = \mathbb{X}(\mathbb{Z}/p\mathbb{Z}) \setminus \{(0,0,0)\}$
3. Define conic sections of the variety $C_j(a) = \{x_j = a\} \cap X^*(p)$.
4. Define the incidence graph $I(p)$ as the graph with the above defined cones as vertices and number of edges between $C_j(a)$ and $C_j(b) = |C_j(a) \cap C_j(a)|$.
5. Then $I(p)$ is connected and $diam(I(p)) = 2$.

Define $rot(3x_1)\begin{pmatrix} x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ 3x_1x_3 - x_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 3x_1 \end{pmatrix}\begin{pmatrix} x_2 \\ x_3 \end{pmatrix}$

Theorem

If $x = (x_1, x_2, x_3)$ is in $X^*(p)$ and for some $j \in 1, 2, 3$ the order of the induced rotation $rot(x_j)$ is at least $p^{\frac{1}{2}+\delta}(\delta > 0$ fixed), then x is joined to a point y in $X^*(p)$ one of whose induced rotations is of maximal order.

Cage

A point $x = (x_1, x_2, x_3) \in X^*(p)$ is called maximal if $ord(rot(x_j))$ is maximal if it is of maximal order and an element b in $\mathbb{F}_p$ is maximal if it is of maximal order.

Definition

A cage is a set of maximal elements in $X^*(p)$.

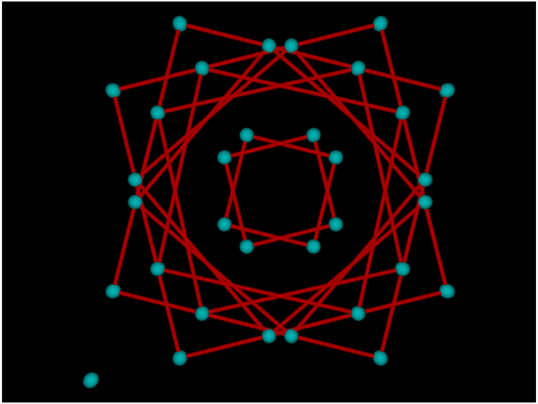
The cage is connected. $C(p)$ is the connected component of $X^*(p)$ under the Γ action that contains the cage and gives the largest component.

Future Work

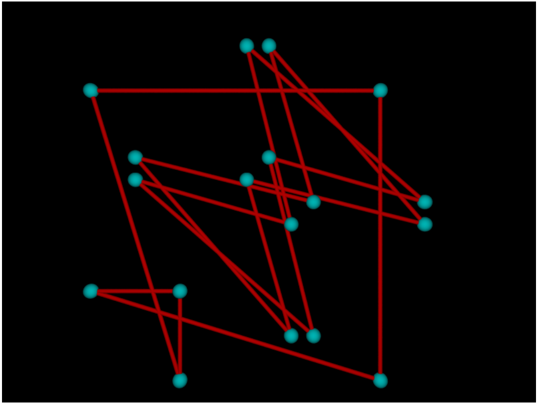
Let $C_j(a) = \{x_j = a\} \cap X^*(p)$ where $X^*(p)$ is the solution set of κ in the affine space excluding zero.

1. $\forall a \in \mathbb{F}_q$, does η act transitively on $C_2(a)$?
2. Let $a \neq b$. Then $\forall x \in C_2(a)$, and $y \in C_2(b)$, does $\exists \alpha \in Out(F_2)$ such that $\alpha(x) = y$.

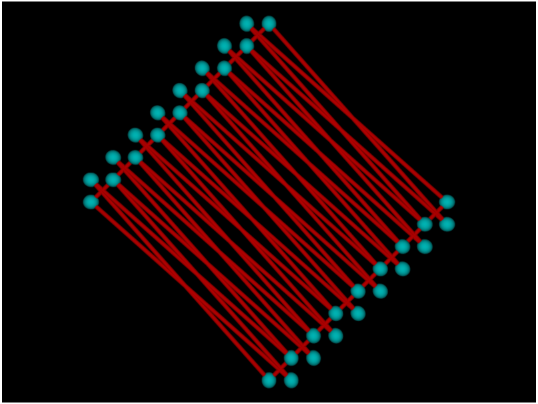
Action of η on Conic on $C_2(0)$ with $p = 17$



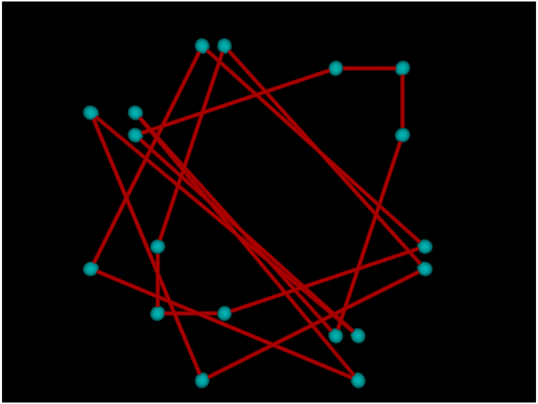
Action of η on Conic on $C_2(1)$ with $p = 17$



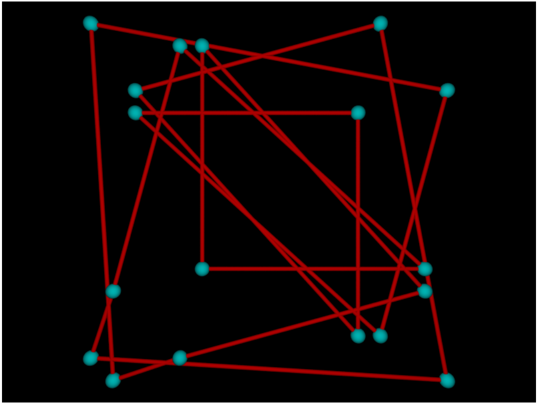
Action of η on Conic on $C_2(2)$ with $p = 17$



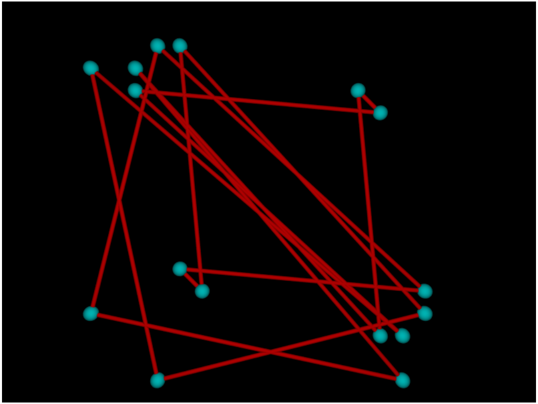
Action of η on Conic on $C_2(3)$ with $p = 17$



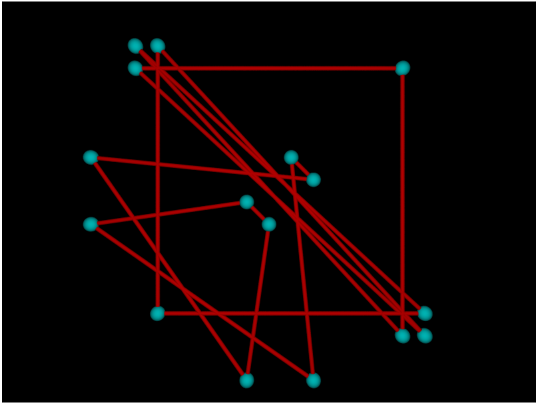
Action of η on Conic on $C_2(4)$ with $p = 17$



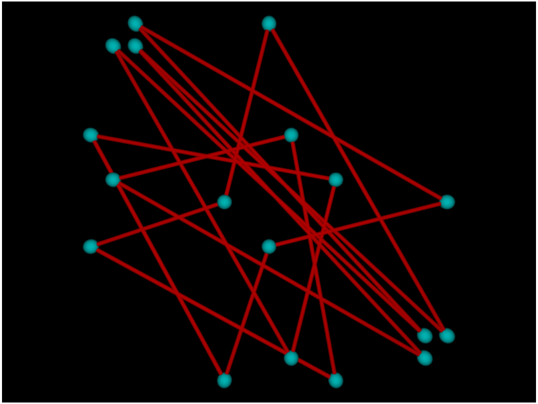
Action of η on Conic on $C_2(5)$ with $p = 17$



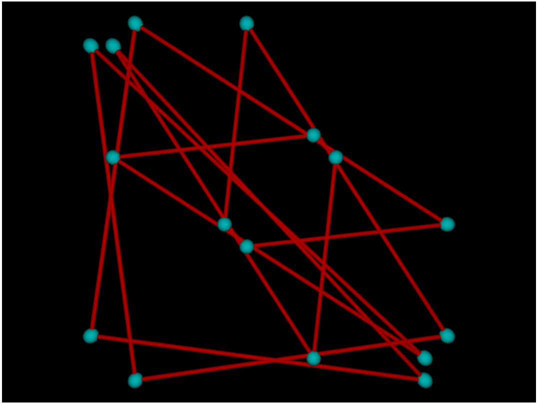
Action of η on Conic on $C_2(6)$ with $p = 17$



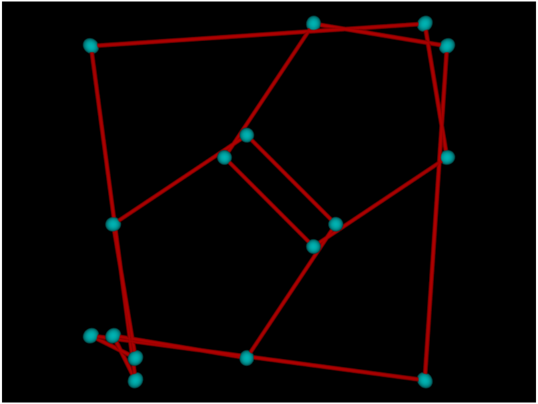
Action of η on Conic on $C_2(7)$ with $p = 17$



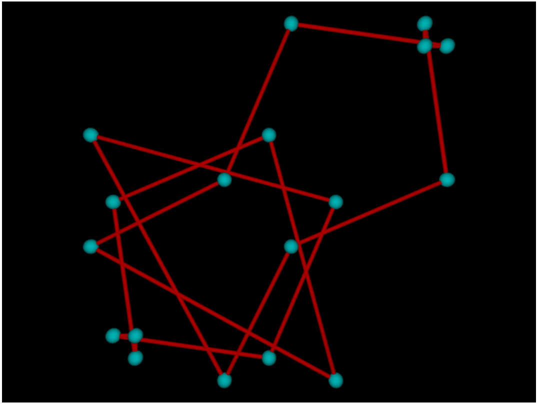
Action of η on Conic on $C_2(8)$ with $p = 17$



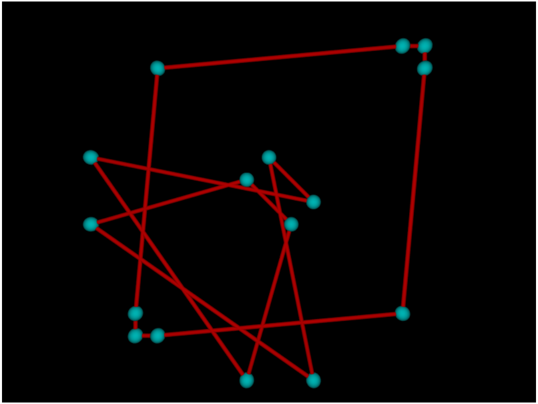
Action of η on Conic on $C_2(9)$ with $p = 17$



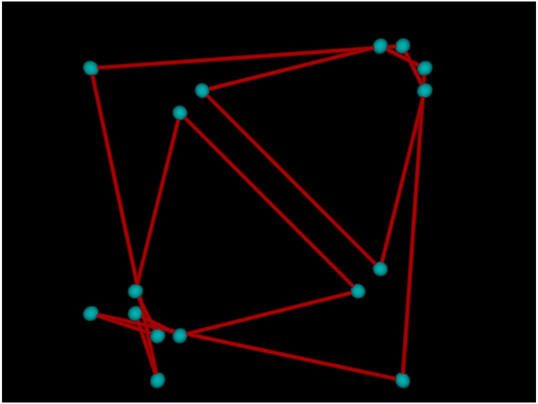
Action of η on Conic on $C_2(10)$ with $p = 17$



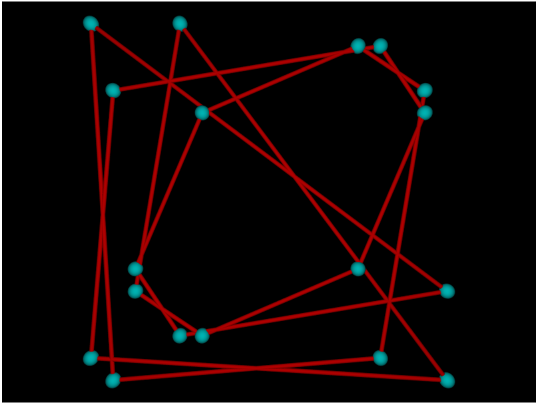
Action of η on Conic on $C_2(11)$ with $p = 17$



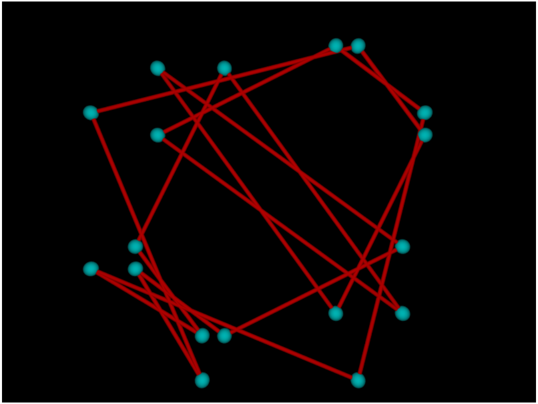
Action of η on Conic on $C_2(12)$ with $p = 17$



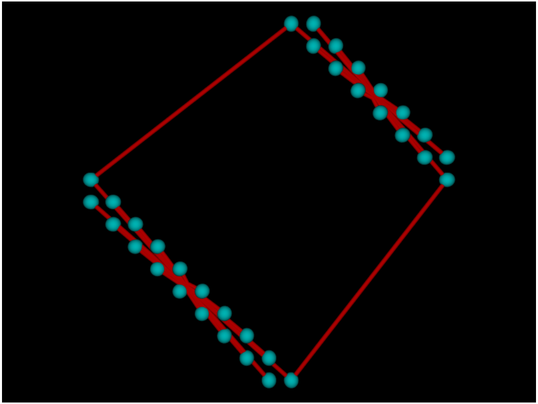
Action of η on Conic on $C_2(13)$ with $p = 17$



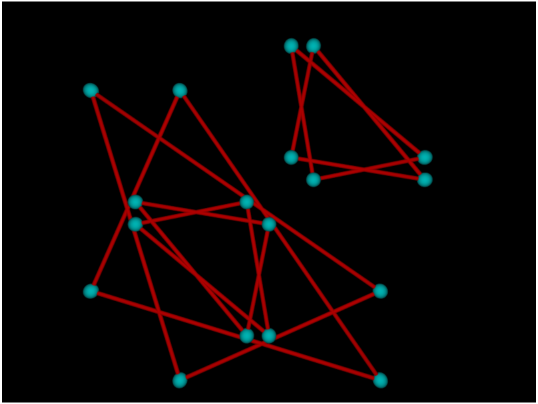
Action of η on Conic on $C_2(14)$ with $p = 17$



Action of η on Conic on $C_2(15)$ with $p = 17$



Action of η on Conic on $C_2(16)$ with $p = 17$



Acknowledgment

We thank Dr. Lawton for his guidance and MEGL and GMU for presenting the opportunity to carryout this work.

Q&A

Questions?
Comments?