Periods on Arithmetic Moduli Spaces

Diaaledin (Dia) Taha, Jermain McDermott, Robert Argus, Patrick Brown

MEGL Symposium, August 2015

Outline

Terminology and Notation

Definition (1.1)

The **free group** F_S over a given set S consists of all expressions (a.k.a. words, or terms) that can be built from members of S, considering two expressions different unless their equality follows from the group axioms.

Definition (1.2)

A **finite field** is a finite set on which the four operations multiplication, addition, subtraction and division (excluding by zero) are defined, satisfying the rules of arithmetic known as the field axioms.

Terminology and Notation (cont'd)

Let $\mathbb{F}_q$ be a finite field of order q.

Definition (1.3)

The **general linear group of degree n** over a field $\mathbb{F}_q$ is the set of $n \times n$ invertible matrices together with the operation of matrix multiplication. We denote this group by $GL_n(\mathbb{F}_q)$.

Definition (1.4)

The **special linear group of degree n** over a field $\mathbb{F}_q$ is the set of $n \times n$ matrices with determinant 1 together with the operation of matrix multiplication. We denote this group by $SL_n(\mathbb{F}_q)$.

Dynamical System

Let S be a set and let $F : S \to S$ be a map from S to itself. The iterate of F with itself n times is denoted

$$F^{(n)} = F \circ F \circ \cdots \circ F$$

.

A point $P \in S$ is **periodic** if $F(n)(P) = P$ for some $n > 1$. The point is **preperiodic** if $F(k)(P)$ is periodic for some $k \geq 1$. The (forward) orbit of P is the set

$$O_F(P) = \left\{ P, F(P), F^{(2)}(P), F^{(3)}(P), \cdots \right\}.$$

Thus P is preperiodic if and only if its orbit $O_F(P)$ is finite.

The Setup

Define $Onj(F_r) := Inj(F_r)/Inn(F_r)$, where $Inj(F_r)$ and $Inn(F_r)$ are the monomorphisms and inner automorphisms from the free group of rank r to itself, respectively. Consider $Q := Hom(F_r, SL_n(\mathbb{F}_q))/SL_n(\mathbb{F}_q)$ and let $Onj(F_r)$ act on Q.

The Process

1. Fix $[\alpha] \in Onj(F_r)$ and $[f] \in Q$.
2. Choose $\alpha^{'} \in [\alpha]$ and $f^{'} \in [f]$.
3. Compute $\alpha(f^{'}) := f^{'} \circ \alpha^{'}$.
4. Find $[\alpha^{'}(f^{'})] \in Q$ and iterate.

This defines a dynamical system. As $\mathbb{F}_q$ is a finite field, it is reasonable to ask whether there exist periodic orbits.

The Moduli Space

It turns out that $Hom(F_r, SL_n(\mathbb{F}_q))$ is a variety. One might then ask:

1. Is $Q = Hom(F_r, SL_n(\mathbb{F}_q))/SL_n(\mathbb{F}_q)$ a variety? **No**!
2. Does there exist an approximation to Q that is a variety $\mathfrak{X}$, where $\mathfrak{X} \subset Q$? **Yes**!
3. How do we find such a variety $\mathfrak{X}$?

The variety $\mathfrak{X} := [Hom(F_r, SL_n)//SL_n](\mathbb{F}_q)$ is obtained from Q by throwing out the strictly upper triangularizable matrices to obtain the following $Hom(F_r, SL_n(\mathbb{F}_q))^*/SL_n(\overline{\mathbb{F}}_q)$, which is a moduli space.

definitions

- Denote $Q_{1,q} = \mathrm{Hom}(F_1, \mathrm{SL}(2, \mathbb{F}_q))/\mathrm{SL}(2, \mathbb{F}_q)$ (this is an instance of the set Q Robert introduced, the instance where $r = 1$).
- Note that this set $\mathfrak{X}_{F_1}(\mathrm{SL}(2, \mathbb{F}_q))$ is not the same as the set $\mathfrak{X}_{F_1}(\mathrm{SL}(2, \mathbb{F}_q)) = \mathrm{Hom}(\mathrm{F}_1, \mathrm{SL}(2, \mathbb{F}_\mathrm{q}))//\mathrm{SL}(2, \mathbb{F}_q) \subset Q_{1,q}$ which discards "nondiagonalizable" elements.
- Also, define by $\mathcal{O}(\phi, \alpha)$ the dynamical system $\alpha(\phi), \alpha^2(\phi), \alpha^3(\phi), \dots$ ($\phi \in Q_{1,q}, \alpha \in Onj(F_1)$ where F_1 is the free group of rank 1).
- Since $(F_1, \cdot) \cong (\mathbb{Z}, +)$ (F_1 is cyclic generated by a, Z is cyclic generated by 1), we have $\mathrm{Inn}(F_1) \cong \mathrm{Inn}(\mathbb{Z}) = \{\mathrm{id}_\mathbb{Z}\}$, the trivial group.

identifications

- Again, F_1 is cyclic, so a homomorphism $\rho : F_1 \to G$ is determined by where a (the generator of F_1) is sent in G.
- From now on, identify an injective homomorphism $a \to a^n : n \in \mathbb{Z} - \{0\}$ with n
- Similarly, we identify $\phi \in \mathrm{Hom}(F_1, \mathrm{SL}(2, \mathbb{F}_q))$ with A where $\phi(a) = A \in \mathrm{SL}(2, \mathbb{F}_q)$.
- We will identify $\gamma \mathrm{Inn}(F_1) = \{\gamma \circ \mathrm{id}_{\mathbb{Z}}\} = \{\gamma\} \in Onj(F_1)$ by γ.

how to study Dyn

- This turns $\mathcal{O}(\phi, \alpha)$ into $\mathcal{O}(A, n)$ where $\phi(a) = A$, $\alpha(a) = a^n$.
- Thus we have $\alpha(\phi), \alpha^2(\phi), \alpha^3(\phi), \ldots$ equivalent to $A, A^n, A^{n^2}, A^{n^3}, \ldots$
- Notice that in the set $Q_{1,q}$, we aren't dealing with $\phi \in Hom(F_1, \mathrm{SL}(2, \mathbb{F}_q))$ per se, but rather the conjugacy class of ϕ under the action of $\mathrm{SL}(2, \mathbb{F}_q)$.
- This identification of the conjugacy class of ϕ with the element ϕ will make sense after the following.

$\mathcal{P} : Q_{1,q} \times \mathrm{Onj}(F_1) \to \mathbb{N}$

- We now want to define the map $\mathcal{P} : Q_{1,q} \times \mathrm{Onj}(F_1) \to \mathbb{N}$ by sending (ϕ, α) (considered as (A,n)) to the smallest positive number m if $\mathcal{O}(\phi, \alpha)$ has so called "prime" period m, or 0 if $\mathcal{O}(\phi, \alpha)$ isn't periodic.
- "Periodic" simply means there is a kth place in the sequence $A, A^n, A^{n^2}, A^{n^3}, \ldots$ where we have $A^{n^k} = A$. The "period" of the system is the integer k.

finding the period

- The reason we are identifying the conjugacy class of A with the element A is because the period is conjugate invariant.
- This comes from noting that $(gAg^{-1})^n = I_{2x2}$ iff $A^n = I_{2x2}$ for any $g \in \mathrm{SL}(2, \mathbb{F}_q)$.
- We have shown in this case that the element A has order relatively prime to n iff A has a prime period.

orders?

- The question now arises of orders of elements in $\mathrm{SL}(2, \mathbb{F}_q)$.
- Two important facts mostly answer this question: that order and characteristic polynomial are also conjugate invariant; i.e., a conjugacy class of matrices has its own period and characteristic polynomial.

orders?

- The question now arises of orders of elements in $\mathrm{SL}(2, \mathbb{F}_q)$.
- Two important facts mostly answer this question: that order and characteristic polynomial are also conjugate invariant; i.e., a conjugacy class of matrices has its own period and characteristic polynomial.
- If the characteristic polynomial of $M \in \mathrm{SL}(2, \mathbb{F}_q)$ $(p_M(t))$has two distinct roots, then our matrix is diagonalizable (Jordan form).

orders?

- The question now arises of orders of elements in $\mathrm{SL}(2, \mathbb{F}_q)$.
- Two important facts mostly answer this question: that order and characteristic polynomial are also conjugate invariant; i.e., a conjugacy class of matrices has its own period and characteristic polynomial.
- If the characteristic polynomial of $M \in \mathrm{SL}(2, \mathbb{F}_q)$ $(p_M(t))$has two distinct roots, then our matrix is diagonalizable (Jordan form).
- If the characteristic polynomial has no roots in $\mathbb{F}_q$, then it is diagonalizable over $\mathbb{F}_{q^2}$.

orders?

- The question now arises of orders of elements in $\mathrm{SL}(2, \mathbb{F}_q)$.
- Two important facts mostly answer this question: that order and characteristic polynomial are also conjugate invariant; i.e., a conjugacy class of matrices has its own period and characteristic polynomial.
- If the characteristic polynomial of $M \in \mathrm{SL}(2, \mathbb{F}_q)$ $(p_M(t))$has two distinct roots, then our matrix is diagonalizable (Jordan form).
- If the characteristic polynomial has no roots in $\mathbb{F}_q$, then it is diagonalizable over $\mathbb{F}_{q^2}$.
- Otherwise, our matrix is "parabolic", and has a double root in $\mathbb{F}_q$ (given the matrix isn't $\pm I_{2x2}$, these are in their own class)

orders in $\mathrm{SL}(2, \mathbb{F}_q)$

The following table gives orders of elements in $\mathrm{SL}(2, \mathbb{F}_q)$.

Conjugacy class type	Representative	Order
$\pm I$	$\begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}$	If I, 1; if -I, 2
Parabolic ($\alpha \in \mathbb{F}_q$, *alpha* $= 1$ or$\alpha \neq \omega^2$)	$A = \begin{bmatrix} \pm 1 & \alpha * \\ 0 & \pm 1 \end{bmatrix}$	If tr(A)=2, char($\mathbb{F}_q$); if tr(A) $=$ -2, 2char(
Diagonalizable over $\mathbb{F}_q$	$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$	$\frac{q-1}{\gcd(\bar{a}**, q-1)}$
Diagonalizable over $\mathbb{F}_{q^2}$	$\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}$	$\frac{q^2-1}{\gcd(\tilde{c}***, q^2-1)}$ (will divide $q+1$)

In this table:

*$\alpha = 1$ or is not a square in $\mathbb{F}_q$.

**$\bar{a}$ represents $\phi(a)$ where $\phi : (\mathbb{F}_q, \cdot) \to (\mathbb{Z}_{q-1}, +)$

***$\tilde{c}$ represents $\gamma(c)$ where $\gamma : (\mathbb{F}_{q^2}, \cdot) \to (\mathbb{Z}_{q^2-1}, +)$ with ϕ, γ being isomorphisms.

does $\mathcal{P}(\phi, \alpha)$ return 0 or n?

- We now know the orders of elements in $\mathrm{SL}(2, \mathbb{F}_q)$. This along with the n corresponding to alpha determines whether $\mathcal{P}$ returns 0 or not.
- This answers the question of whether $\mathcal{O}(\phi, \alpha)$ has a prime period.
- To find this prime period is equivalent to solving $n^k \equiv 1$ mod $ord(A)$ for k.
- This yields that factors of $\phi(ord(A))$ are the only candidates for k (ϕ is the euler phi function).

does $\mathcal{P}(\phi, \alpha)$ return 0 or n?

- In any group G with $a \in G$ of finite order $k = |a|$, a is periodic under $\tau_n(a) = a^n$ if and only if $\gcd(k, n) = 1$ (assume $n > 1$).

does $\mathcal{P}(\phi, \alpha)$ return 0 or n?

- In any group G with $a \in G$ of finite order $k = |a|$, a is periodic under $\tau_n(a) = a^n$ if and only if $\gcd(k, n) = 1$ (assume $n > 1$).
- $(\leftarrow)$ If $\gcd(k, n) = 1$, then by Euler's theorem, $n^{\phi(k)} = 1$ mod k. Thus, in the sequence $A, A^n, A^{n^2}, \ldots$, since $A^{n^j} = A^m$ with $n^j = m$ mod k for any $j \in \mathbb{N}$, we will find A again in at most the $\phi(k)$'th position.

does $\mathcal{P}(\phi, \alpha)$ return 0 or n?

- In any group G with $a \in G$ of finite order $k = |a|$, a is periodic under $\tau_n(a) = a^n$ if and only if $\gcd(k, n) = 1$ (assume $n > 1$).
- $(\leftarrow)$ If $\gcd(k, n) = 1$, then by Euler's theorem, $n^{\phi(k)} = 1$ mod k. Thus, in the sequence $A, A^n, A^{n^2}, ...,$ since $A^{n^j} = A^m$ with $n^j = m$ mod k for any $j \in \mathbb{N}$, we will find A again in at most the $\phi(k)$'th position.
- $(\rightarrow)$ If A is periodic, assume $\gcd(k, n) \neq 1$. Then n is a zero divisor modulo k. Since an element of a ring is a zero divisor if and only if it is not a unit, there is no $s \in \mathbb{N}$ such that $n^s = 1$ mod k or else n^{s-1} would be an inverse of n, making n a unit modulo k. This is a contradiction, hence $\gcd(k, n) = 1$.

what is the set $Q_{r,q}$?

- We used the language of an element of $Q_{1,q}$ as being "diagonalizable" because we could identify an equivalence class with a diagonalizable matrix in $\mathrm{SL}(2, \mathbb{F}_q)$.
- In fact, for general r, we can identify an element of $Q_{r,q}$ to be an element in $\mathrm{SL}(2, \mathbb{F}_q)^r / \mathrm{SL}(2, \mathbb{F}_q) = \mathrm{SL}(2, \mathbb{F}_q) \times \mathrm{SL}(2, \mathbb{F}_q) \times ... \times \mathrm{SL}(2, \mathbb{F}_q)/\mathrm{SL}(2, \mathbb{F}_q)$.
- To see how to identify $\mathrm{Hom}(F_r, \mathrm{SL}(2, \mathbb{F}_q))$ with $\mathrm{SL}(2, \mathbb{F}_q)^r$, send an element $\rho \to (\rho(w_1), \rho(w_2), ..., \rho(w_r))$ where $w_1, ..., w_r$ are the generators of F_r. This map is a bijection.

Moving to a Free Group of 2 Letters

- We move from a single matrix $A \in SL_2(F_q)$ to $\{(A, B) : (A, B) \in SL_2(F_q)^2\}$ and several things change.
- We go from having $q + 4$ Conjugation Classes to $2q^3 + q^2 + 4q + 1$
- We change from $Onj(F1)$ to $Out(F2)$

$Out(F2)$

- $Out(F2)$ is generated by 3 Nielson Transformation
- Denote the Nielson transformations on $F_2 = \langle x_1, x_2 \rangle$ as follows:

$$\begin{aligned} \iota &= \begin{bmatrix} x_1 & x_2 \\ x_1^{-1} & x_2 \end{bmatrix}, \\ \tau &= \begin{bmatrix} x_1 & x_2 \\ x_2 & x_1 \end{bmatrix}, \text{ and} \\ \eta &= \begin{bmatrix} x_1 & x_2 \\ x_1 x_2 & x_2 \end{bmatrix}. \end{aligned}$$

$Out(F2)$ Cont.

- $Out(F2)$ is isomorphic to $GL_2(\mathbb{Z})$
- $x_1 \approx \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $x_2 \approx \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $\iota \approx \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$
- $\tau \approx \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- $\eta \approx \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$

Products of the Nielson Transformations

1. $\iota^m = \iota^{m \pmod 2}$
2. $\tau^m = \tau^{m \pmod 2}$
3. $\eta^m = \begin{bmatrix} x_1 & x_2 \\ x_1 x_2^m & x_2 \end{bmatrix}$
4. $\iota\tau = \begin{bmatrix} x_1 & x_2 \\ x_2 & x_1^{-1} \end{bmatrix}$ and $\tau\iota = \begin{bmatrix} x_1 & x_2 \\ x_2^{-1} & x_1 \end{bmatrix}$
5. $\iota\eta^m = \begin{bmatrix} x_1 & x_2 \\ x_1^{-1} x_2^m & x_2 \end{bmatrix}$ and $\eta^m\iota = \begin{bmatrix} x_1 & x_2 \\ x_2^{-m} x_1^{-1} & x_2 \end{bmatrix}$
6. $\tau\eta^m = \begin{bmatrix} x_1 & x_2 \\ x_2 x_1^m & x_1 \end{bmatrix}$ and $\eta^m\tau = \begin{bmatrix} x_1 & x_2 \\ x_2 & x_1 x_2^m \end{bmatrix}$

Action of $Aut(F_2)$ on $Hom(F_2, SL_2(\mathbb{F}_Q))$

For any $(A, B) \in SL(2, \mathbb{F}_q)$ and $m \in \mathbb{Z}$, the Nielson transformations act as follows:

$$\begin{aligned} \iota^m \cdot (A, B) &= (A^{(-1)^m}, B), \\ \tau^m \cdot (A, B) &= \begin{cases} (B, A) & m \text{ is odd} \\ (A, B) & m \text{ is even} \end{cases}, \text{ and} \\ \eta^m \cdot (A, B) &= (AB^m, B). \end{aligned}$$

Periods for $Out(\mathbb{F}2)$ Length 1

Let $(A, B) \in SL(2, \mathbb{F}_q)^{\times 2}$.

1. **Case ι:** Since $\iota^2 = id$, we have that $\mathcal{O}_\iota((A, B))$ is periodic, with period at most 2.
2. **Case τ:** Same as for ι.
3. **Cases η and η^{-1} (and η^m for $m \in \mathbb{Z}$):** Since $\#SL_2(\mathbb{F}_q) = q^3 - q < \infty$ is a finite group, raising any element in it to its order gives the identity. We thus get $\eta^{\pm ord(B)} \cdot (A, B) = (AB^{\pm ord(B)}, B) = (A, B)$. So $\mathcal{O}_\eta((A, B))$ is periodic with period $ord(B) \mid \#SL_2(\mathbb{F}_q)$. In fact, for any $m \in \mathbb{Z}$ we have that $\mathcal{O}_{\eta^m}((A, B))$ is periodic of period

$$\frac{ord(B)}{\gcd(m, ord(B))}.$$

Periods for $Out(\mathbb{F}2)$ $\iota and \eta$

Case for $\iota\eta$ and $\eta\iota$ (and $\iota\eta^m$ and $\eta^m\iota$ for $m \in \mathbb{Z}$) The period of (A, B) is

$$\mathcal{O}_{\iota\eta^m}((A,B)) : (A,B) \to (A^{-1}B^m, B) \to$$
$$(B^{-m}AB^m, B) \to (B^{-m}A^{-1}B^{m+1}, B) \to$$
$$\cdots$$
$$(B^{-km}AB^{km}, B) \to (B^{-km}A^{-1}B^{(k+1)m}, B) \to$$
$$\cdots$$

Note that

$$(\iota\eta^m)^{2k} \cdot (A,B) = (B^{-km}AB^{km}, B) = (\sigma_{B^{-m}}(A), B),$$

and so $\mathcal{O}_{\iota\eta^m}((A,B))$ is periodic of period at most

$$2 \times \frac{ord(B)}{\gcd(ord(B), mk)}.$$

We get the same behavior for $\eta^m\iota$.

Periods for $Out(\mathbb{F}2)$ $\tau and \eta$

Case for $\tau\eta$ and $\eta\tau$
We have that

$$\eta\tau = \begin{bmatrix} x_1 & x_2 \\ x_2 & x_1x_2 \end{bmatrix}.$$

It can be easily seen that for any $(A, B) \in SL(2, \mathbb{F}_q)$ and$n \in \mathbb{N}$ that

$$(\eta\tau)^n((A, B)) = (s_n, s_{n+1}),$$

where

$$\begin{aligned} s_0 &= A, \\ s_1 &= B, \text{ and} \\ s_{n+2} &= s_n s_{n+1} \text{ for } n \geq 0. \end{aligned}$$

Note that $(s_n)_{n\in\mathbb{N}}$ is the "Fibonacci sequence" on the group $SL(2, \mathbb{F}_q)$.

Periods on $Hom(F_2, SL_2(\mathbb{F}_Q))$

We have the following fact about finite dynamical systems.

Proposition

Let X be a finite set, and $f : X \to X$ be a function. It follows that:

1. *any element $x \in X$ is preperiodic, and*
2. *if f is invertible, then every $x \in X$ is periodic.*

From the invertibility of the action of ι, τ, and η we get the following:

Corollary

Let G be a finite group, then under the action of $Aut(F_2) \curvearrowright Hom(F_2, G)$ every orbit is periodic.

Moving from $Hom(F_2, SL_2(\mathbb{F}_Q))/SL_2(\mathbb{F}_q)$ to $Hom(F_2, SL_2(\mathbb{F}_Q))//SL_2(\mathbb{F}_q)$

- $Hom(F_2, SL_2(\mathbb{F}_Q))/SL_2(\mathbb{F}_q)$ is computationally intensive.
- We have a better option $Hom(F_2, SL_2(\mathbb{F}_Q))//SL_2(\mathbb{F}_q)$
- This allows us to transition from $\{(A, B) : A, B \in SL_2(\mathbb{F}_q)\}$ to $\{(x, y, z) : x, y, z \in \mathbb{F}_q \;\&\; x = Tr(A), y = Tr(B), z = Tr(AB)\}$

Trace Functions

The traces of the generators X, Y, XY parametrize $SL(2, \mathbb{F}_q)^{\times 2} /\!\!/ SL(2, \mathbb{F}_q)$ as the affine space $\mathbb{F}_q^3$.

Trace Functions

The traces of the generators X, Y, XY parametrize $SL(2, \mathbb{F}_q)^{\times 2} /\!\!/ SL(2, \mathbb{F}_q)$ as the affine space $\mathbb{F}_q^3$.
The character map $Tr : SL(2, \mathbb{F}_q)^{\times 2} /\!\!/ SL(2, \mathbb{F}_q) \to \mathbb{F}_q^3$ given by

$$[\![A, B]\!] \mapsto (trA, trB, tr(AB))$$

is an isomorphism.

Automorphisms

The action of $Out(F_2)$ on $SL(2, \mathbb{F}_q)^{\times 2} /\!\!/ SL(2, \mathbb{F}_q)$ is generated by the three involutions

Automorphisms

The action of $Out(F_2)$ on $SL(2, \mathbb{F}_q)^{\times 2} /\!\!/ SL(2, \mathbb{F}_q)$ is generated by the three involutions

$$\begin{aligned} \iota^* : [\![A, B]\!] &\mapsto [\![A^{-1}, B]\!] \\ \tau^* : [\![B, A]\!] &\mapsto [\![A, B]\!] \\ \nu^* : [\![A, B]\!] &\mapsto [\![A^{-1}, AB]\!] \end{aligned}$$

Automorphisms

The action of $Out(F_2)$ on $SL(2, \mathbb{F}_q)^{\times 2} /\!\!/ SL(2, \mathbb{F}_q)$ is generated by the three involutions

$$\begin{array}{rcl} \iota^* : [\![A, B]\!] & \mapsto & [\![A^{-1}, B]\!] \\ \tau^* : [\![B, A]\!] & \mapsto & [\![A, B]\!] \\ \nu^* : [\![A, B]\!] & \mapsto & [\![A^{-1}, AB]\!] \end{array}$$

This induces the following polynomial automorphisms on the affine space $\mathbb{F}_q^3$

Automorphisms

The action of $Out(F_2)$ on $SL(2,\mathbb{F}_q)^{\times 2} /\!\!/ SL(2,\mathbb{F}_q)$ is generated by the three involutions

$$\begin{aligned} \iota^* : [\![A,B]\!] &\mapsto [\![A^{-1},B]\!] \\ \tau^* : [\![B,A]\!] &\mapsto [\![A,B]\!] \\ \nu^* : [\![A,B]\!] &\mapsto [\![A^{-1},AB]\!] \end{aligned}$$

This induces the following polynomial automorphisms on the affine space $\mathbb{F}_q^3$

$$\begin{aligned} h : (x,y,z) &\mapsto (x,y,xy-z) \\ u : (x,y,z) &\mapsto (y,x,z) \\ v : (x,y,z) &\mapsto (x,z,y) \end{aligned}$$

Automorphisms

The action of $Out(F_2)$ on $SL(2, \mathbb{F}_q)^{\times 2} /\!\!/ SL(2, \mathbb{F}_q)$ is generated by the three involutions

$$\begin{aligned} \iota^* : [\![A, B]\!] &\mapsto [\![A^{-1}, B]\!] \\ \tau^* : [\![B, A]\!] &\mapsto [\![A, B]\!] \\ \nu^* : [\![A, B]\!] &\mapsto [\![A^{-1}, AB]\!] \end{aligned}$$

This induces the following polynomial automorphisms on the affine space $\mathbb{F}_q^3$

$$\begin{aligned} h : (x, y, z) &\mapsto (x, y, xy - z) \\ u : (x, y, z) &\mapsto (y, x, z) \\ v : (x, y, z) &\mapsto (x, z, y) \end{aligned}$$

In what follows, denote the group they generate $\langle h, u, v\rangle \leq Aut(\mathbb{F}_q^3)$ by $\Gamma_{\mathbb{F}_q}$.

What We Do?

Study the dynamics of $\Gamma_{\mathbb{F}_q} \curvearrowright \mathbb{F}_q^3$

What We Do?

Study the dynamics of $\Gamma_{\mathbb{F}_q} \curvearrowright \mathbb{F}_q^3$

- What is the structure of $\Gamma_{\mathbb{F}_q}$?

What We Do?

Study the dynamics of $\Gamma_{\mathbb{F}_q} \curvearrowright \mathbb{F}_q^3$

- What is the structure of $\Gamma_{\mathbb{F}_q}$?
- Any interesting invariants?

What We Do?

Study the dynamics of $\Gamma_{\mathbb{F}_q} \curvearrowright \mathbb{F}_q^3$

- What is the structure of $\Gamma_{\mathbb{F}_q}$?
- Any interesting invariants?
- What do the orbits/periods look like?

The Structure of $\Gamma_{\mathbb{F}_q}$

In the integer case, it was shown by *Goldman (2003)* that

$$\Gamma_{\mathbb{Z}} \cong PSL(2, \mathbb{Z}).$$

The Structure of $\Gamma_{\mathbb{F}_q}$

In the integer case, it was shown by *Goldman (2003)* that

$$\Gamma_{\mathbb{Z}} \cong PSL(2, \mathbb{Z}).$$

Orbits Group (two days ago) showed that if $q = p^n$, then $\Gamma_{\mathbb{F}_q}$ is a quotient of the $(2, 3, \frac{1}{2}p(p^{2n} - 1))$ Coxeter group,

The Structure of $\Gamma_{\mathbb{F}_q}$

In the integer case, it was shown by *Goldman (2003)* that

$$\Gamma_{\mathbb{Z}} \cong PSL(2, \mathbb{Z}).$$

Orbits Group (two days ago) showed that if $q = p^n$, then $\Gamma_{\mathbb{F}_q}$ is a quotient of the $(2, 3, \frac{1}{2}p(p^{2n} - 1))$ Coxeter group, i.e.

$$\langle x_1, x_2, x_3 \mid (x_i)^2, (x_1x_2)^2, (x_2x_3)^3, (x_1x_3)^{\frac{1}{2}p(p^{2n}-1)} = 1 \rangle.$$

The Structure of $\Gamma_{\mathbb{F}_q}$

In the integer case, it was shown by *Goldman (2003)* that

$$\Gamma_{\mathbb{Z}} \cong PSL(2, \mathbb{Z}).$$

Orbits Group (two days ago) showed that if $q = p^n$, then $\Gamma_{\mathbb{F}_q}$ is a quotient of the $(2, 3, \frac{1}{2}p(p^{2n} - 1))$ Coxeter group, i.e.

$$\langle x_1, x_2, x_3 \mid (x_i)^2, (x_1x_2)^2, (x_2x_3)^3, (x_1x_3)^{\frac{1}{2}p(p^{2n}-1)} = 1 \rangle.$$

We also demonstrated $\mathbb{Z}_2 \times \mathbb{Z}_2$, S_3, and $D_{\frac{1}{2}p(p^{2n}-1)}$ as subgroups.

The Structure of $\Gamma_{\mathbb{F}_q}$

In the integer case, it was shown by *Goldman (2003)* that

$$\Gamma_{\mathbb{Z}} \cong PSL(2, \mathbb{Z}).$$

Orbits Group (two days ago) showed that if $q = p^n$, then $\Gamma_{\mathbb{F}_q}$ is a quotient of the $(2, 3, \frac{1}{2}p(p^{2n} - 1))$ Coxeter group, i.e.

$$\langle x_1, x_2, x_3 \mid (x_i)^2, (x_1x_2)^2, (x_2x_3)^3, (x_1x_3)^{\frac{1}{2}p(p^{2n}-1)} = 1\rangle.$$

We also demonstrated $\mathbb{Z}_2 \times \mathbb{Z}_2$, S_3, and $D_{\frac{1}{2}p(p^{2n}-1)}$ as subgroups.
Note that $PSL(2, \mathbb{Z})$ is a $(2, 3, \infty)$ Coxeter group. It all fits together!

Invariants

The trace of a commutator $[X, Y] = XYX^{-1}Y^{-1}$ gives us the Fricke polynomial

$$\kappa(x, y, z) = x^2 + y^2 + z^2 - xyz - 2.$$

Invariants

The trace of a commutator $[X, Y] = XYX^{-1}Y^{-1}$ gives us the Fricke polynomial

$$\kappa(x, y, z) = x^2 + y^2 + z^2 - xyz - 2.$$

Turns out κ is invariant under the generators h, u, v.

Invariants

The trace of a commutator $[X, Y] = XYX^{-1}Y^{-1}$ gives us the Fricke polynomial

$$\kappa(x, y, z) = x^2 + y^2 + z^2 - xyz - 2.$$

Turns out κ is invariant under the generators h, u, v.
This implies two things:

Invariants

The trace of a commutator $[X, Y] = XYX^{-1}Y^{-1}$ gives us the Fricke polynomial

$$\kappa(x, y, z) = x^2 + y^2 + z^2 - xyz - 2.$$

Turns out κ is invariant under the generators h, u, v.
This implies two things:

1. That $\Gamma_{\mathbb{F}_q} \leq Aut(\kappa)$.

Invariants

The trace of a commutator $[X, Y] = XYX^{-1}Y^{-1}$ gives us the Fricke polynomial

$$\kappa(x, y, z) = x^2 + y^2 + z^2 - xyz - 2.$$

Turns out κ is invariant under the generators h, u, v.
This implies two things:

1. That $\Gamma_{\mathbb{F}_q} \leq Aut(\kappa)$.
2. That $\kappa^{-1}(t)$ partitions $\mathbb{F}_q^3$ into $\Gamma_{\mathbb{F}_q}$-invariant surfaces.

Invariants

The trace of a commutator $[X, Y] = XYX^{-1}Y^{-1}$ gives us the Fricke polynomial

$$\kappa(x, y, z) = x^2 + y^2 + z^2 - xyz - 2.$$

Turns out κ is invariant under the generators h, u, v.
This implies two things:

1. That $\Gamma_{\mathbb{F}_q} \leq Aut(\kappa)$.
2. That $\kappa^{-1}(t)$ partitions $\mathbb{F}_q^3$ into $\Gamma_{\mathbb{F}_q}$-invariant surfaces.

So studying the dynamics $\Gamma_{\mathbb{F}_q} \curvearrowright \mathbb{F}_q^3$ is equivalent to studying the dynamics of $\Gamma_{\mathbb{F}_q} \curvearrowright \kappa^{-1}(t)$.

Interlude: The Markoff-Hurwitz Equation

The equation

$$x^2 + y^2 + z^2 = 3xyz$$

over $\mathbb{Z}$ is called the *Markoff-Hurwitz Equation*. It is closely related to Diophantine approx.

Interlude: The Markoff-Hurwitz Equation

The equation

$$x^2 + y^2 + z^2 = 3xyz$$

over $\mathbb{Z}$ is called the *Markoff-Hurwitz Equation*. It is closely related to Diophantine approx.

Hurwitz (1907) proved by a descent argument that you can start with $(1, 1, 1)$ and get all the other positive integer solutions in the orbit $\Gamma_{\mathbb{Z}} \cdot (1, 1, 1)$.

Interlude: The Markoff-Hurwitz Equation

The equation

$$x^2 + y^2 + z^2 = 3xyz$$

over $\mathbb{Z}$ is called the *Markoff-Hurwitz Equation*. It is closely related to Diophantine approx.

Hurwitz (1907) proved by a descent argument that you can start with $(1,1,1)$ and get all the other positive integer solutions in the orbit $\Gamma_{\mathbb{Z}} \cdot (1,1,1)$.

So in reality, we are studying a finitary Markoff-Hurwitz equation

$$x^2 + y^2 + z^2 = xyz + k.$$

Upper Bound on the size of $\Gamma_{\mathbb{F}_q}$−Orbits

A trivial bound is $\#\mathbb{F}_q^3 = q^3$.

Upper Bound on the size of $\Gamma_{\mathbb{F}_q}$−Orbits

A trivial bound is $\#\mathbb{F}_q^3 = q^3$. *Mariscal (2012)* showed that

$$\#\kappa^{-1}(t) = q^2 \pm \{0, 2, 3, \text{ or } 4\}\, q + 1,$$

Upper Bound on the size of $\Gamma_{\mathbb{F}_q}-$Orbits

A trivial bound is $\#\mathbb{F}_q^3 = q^3$. *Mariscal (2012)* showed that

$$\#\kappa^{-1}(t) = q^2 \pm \{0, 2, 3, \text{ or } 4\}\, q + 1,$$

this gives us a $\sim q^2$ upper bound for the $\Gamma_{\mathbb{F}_q}$-orbits.

One Letter: h, u, or v

Each generates a copy of $\mathbb{Z}_2$.

One Letter: h, u, or v

Each generates a copy of $\mathbb{Z}_2$.

$*$	$Fix(*)$	$\#Fix(*)$
h	$XY = 2Z$	q^2
u	$X = Y$	q^2
v	$Y = Z$	q^2

One Letter: h, u, or v

Each generates a copy of $\mathbb{Z}_2$.

$*$	$Fix(*)$	$\#Fix(*)$
h	$XY = 2Z$	q^2
u	$X = Y$	q^2
v	$Y = Z$	q^2

$$\#\mathcal{O}_*(x,y,z) := \begin{cases} 1, & (x,y,z) \in Fix(*) \\ 2, & (x,y,z) \notin Fix(*) \end{cases}$$

Two Letters: u and v

They generate S_3.

Two Letters: u and v

They generate S_3.

$*$	$Fix(*)$	$\#Fix(*)$
uv	$X = Y = Z$	q

Two Letters: u and v

They generate S_3.

$*$	$Fix(*)$	$\#Fix(*)$
uv	$X = Y = Z$	q

$$\#\mathcal{O}_{uv}(x,y,z) := \begin{cases} 1, & (x,y,z) \in Fix(uv) \\ 3, & (x,y,z) \notin Fix(uv) \end{cases}$$

Two Letters: h and u

They generate $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Two Letters: h and u

They generate $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$*$	$Fix(*)$	$\#Fix(*)$
hu	$X = Y, Z = 2^{-1}XY$	q

Two Letters: h and u

They generate $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$*$	$Fix(*)$	$\#Fix(*)$
hu	$X = Y, Z = 2^{-1}XY$	q

$$\#\mathcal{O}_{hu}(x,y,z) := \begin{cases} 1, & (x,y,z) \in Fix(hu) \\ 2, & (x,y,z) \notin Fix(hu) \end{cases}$$

Two Letters: h and v

They generate $D_{\frac{1}{2}p(p^{2n}-1)}$.

Two Letters: h and v

They generate $D_{\frac{1}{2}p(p^{2n}-1)}$.

$*$	$Fix(*)$	$\#Fix(*)$
hv	$Y = Z, Y(X-2) = 0$	$2q-1$

Two Letters: h and v

They generate $D_{\frac{1}{2}p(p^{2n}-1)}$.

$*$	$Fix(*)$	$\#Fix(*)$
hv	$Y = Z, Y(X-2) = 0$	$2q-1$

$$\#\mathcal{O}_{hv}(x,y,z) := \begin{cases} 1, & (x,y,z) \in Fix(*), \text{ else} \\ p, & x = \pm 2 \\ \text{div. of } q-1, & x^2-4 \text{ is a } \neq 0 \text{ quad. res.} \\ \text{div. of } q+1, & x^2-4 \text{ is not a quad. res.} \end{cases}$$

Oh, the Places You'll Go!

Lots of places, actually.

Oh, the Places You'll Go!

Lots of places, actually.

- Flesh out our understanding of the arithmetic dynamics of $\Gamma_{\mathbb{F}_q} \curvearrowright \mathbb{F}_q^3$.
  - What is the size of $\Gamma_{\mathbb{F}_q}$?
  - What exceptional subgroups does it have?
  - What is the exact size of the orbits?
  - When is the action transitive on a surface $\kappa^{-1}(t)$?
  - How many connected components can $\kappa^{-1}(t)$ have?
  - $\cdots$
- Start the same program for the action of $Out(F_3) \curvearrowright SL(2, \mathbb{F}_q)^\times \mathbin{/\!/} SL(2, \mathbb{F}_q)$.

Acknowledgment

- Prof. Sean Lawton
- GMU, MEGL
- GEAR, NSF

References

- Goldman, W. M, "The Modular Group Action on Real $SL(2)$-characters of a One-Holed Torus", Geom. Topol. 7 (2003).
- Hurwtiz, A., "Uber eine Aufgabe der unbestimmten analysis", Arch. Math. Phys., 3 (1907), 185 – 196. Also in A. Hurwitz, Mathematisch Werke Vol. 2, Chapter LXX, 1933 and 1962, 410 – 421.
- Mariscal, Juan, "The Zeta Function of Generalized Markoff Equations over Finite Fields" (2012). UNLV Theses/Dissertations/Professional Papers/Capstones. Paper 1593.
- Cavazos, Samuel, and Sean Lawton. "E-polynomial of SL 2 ($\mathbb{C}$)-character varieties of free groups." International Journal of Mathematics 25.06 (2014): 1450058.