

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

# Divisibility of function field class numbers

Jeff Achter

[j.achter@colostate.edu](mailto:j.achter@colostate.edu)  
Department of Mathematics  
Colorado State University

25 April 2006  
Galois theory workshop

# Outline

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

## 1 Introduction

- Basic question
- Motivation

## 2 Main theorem

- Statement of theorem
- Interlude on monodromy (I)
- Proof for  $\mathcal{M}_g$

## 3 Interlude on monodromy (II)

## 4 Arbitrary families

## 5 Cyclic covers of $\mathbb{P}^1$

# Basic question

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $E/\mathbb{F}$  be an elliptic curve over a finite field.
- Let  $\ell$  be a prime number.
- What's the chance that  $\ell \mid \#E(\mathbb{F})$ ?
- Actually, this was answered by Lenstra ( $\mathbb{F} = \mathbb{F}_p$ ) and Howe ( $\mathbb{F} = \mathbb{F}_q$ ).
- In this talk, we'll give an answer for:
  - Abelian varieties of arbitrary dimension
  - Jacobians of curves of arbitrary genus

# Basic question

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $E/\mathbb{F}$  be an elliptic curve over a finite field.
- Let  $\ell$  be a prime number.
- What's the chance that  $\ell \mid \#E(\mathbb{F})$ ?
- Actually, this was answered by Lenstra ( $\mathbb{F} = \mathbb{F}_p$ ) and Howe ( $\mathbb{F} = \mathbb{F}_q$ ).
- In this talk, we'll give an answer for:
  - Abelian varieties of arbitrary dimension
  - Jacobians of curves of arbitrary genus

# Sneak preview

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Roughly, we show: The answer is approximately  $\frac{1}{\ell}$ .
- *Actually, it's closer to  $\frac{1}{\ell-1}$*
- Let  $\alpha(g, r)$  be the chance that a curve  $C$  of genus  $g$  satisfies  $\text{Jac}(C)(\mathbb{F})[\ell] \cong (\mathbb{Z}/\ell)^r$ .

# Sneak preview

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Roughly, we show: The answer is approximately  $\frac{1}{\ell}$ .
- *Actually, it's closer to  $\frac{1}{\ell-1}$*
- Let  $\alpha(g, r)$  be the chance that a curve  $C$  of genus  $g$  satisfies  $\text{Jac}(C)(\mathbb{F})[\ell] \cong (\mathbb{Z}/\ell)^r$ .

# Sneak preview

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

$g$	$r$	$\alpha(g, r)$
1	0	$\frac{\ell^2 - \ell - 1}{\ell^2 - 1}$
1	1	$\frac{1}{\ell}$
1	2	$\frac{1}{\ell(\ell^2 - 1)}$

# Sneak preview

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

$g$	$r$	$\alpha(g, r)$
2	0	$\frac{\ell^6 - \ell^5 - \ell^4 + \ell + 1}{(\ell^2 - 1)(\ell^4 - 1)}$
2	1	$\frac{\ell^3 - \ell - 1}{\ell^2(\ell^2 - 1)}$
2	2	$\frac{\ell^3 - \ell - 1}{\ell^2(\ell^2 - 1)^2}$
2	3	$\frac{1}{(\ell^2 - 1)\ell^4}$
2	4	$\frac{1}{\ell^4(\ell^2 - 1)(\ell^4 - 1)}$

# Sneak preview

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

$g$	$r$	$\alpha(g, r)$
3	0	$\frac{\ell^{12} - \ell^{11} - \ell^{10} + \ell^7 + \ell^5 + \ell^4 - \ell^3 - \ell - 1}{(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$
3	1	$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)(\ell^4 - 1)}$
3	2	$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)^2(\ell^4 - 1)}$
3	3	$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2}$
3	4	$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2(\ell^4 - 1)}$
3	5	$\frac{1}{(\ell^2 - 1)(\ell^4 - 1)\ell^9}$
3	6	$\frac{1}{\ell^9(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$

# Sample spaces: example

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

$$\begin{array}{ccc} \mathcal{E} & & y^2 = x(x-1)(x-\lambda) \\ \downarrow & & \downarrow \\ S = \mathbb{P}^1 - \{0, 1, \infty\} & & \lambda\text{-line} \end{array}$$

- Fiber over  $\lambda = \lambda_0$  is

$$\mathcal{E}_{\lambda_0} : y^2 = x(x-1)(x-\lambda_0).$$

- Varying choice of  $\lambda_0 \in S(\mathbb{F})$  varies elliptic curve  $\mathcal{E}_{\lambda_0}/\mathbb{F}$ .

# Basic question: abelian varieties

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $X \rightarrow S$  be an abelian scheme over a finite field.

What is

$$\frac{|\{s \in S(\mathbb{F}) : \ell \mid |X_s(\mathbb{F})|\}|}{|S(\mathbb{F})|}?$$

- Especially,  $\mathcal{C} \rightarrow S$  a relative curve. What is

$$\frac{|\{s \in S(\mathbb{F}) : \ell \mid |\text{Jac}(\mathcal{C}_s)(\mathbb{F})|\}|}{|S(\mathbb{F})|}?$$

Think of this as a parametrized family of abelian varieties.

# Jacobians and class groups

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $C/\mathbb{F}$  be a proper, smooth curve of genus  $g \geq 1$ .
- Jacobian  $\text{Jac}(C)$  is a  $g$ -dimensional abelian variety which is:
  - the smallest group variety containing  $C$ .
  - the variety parametrizing degree zero line bundles on  $C$ .
  - the variety such that  $\text{Jac}(C)(\mathbb{F})$  is the ideal class group of  $\mathbb{F}(C)$ .
- For  $g = 1$ , canonical isomorphism  $\text{Jac}(E) \cong E$ .

# Applications

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- *Algorithm for producing papers:*
  - 1 identify algorithm or protocol over  $\mathbb{Z}/N$ .
  - 2 realize it only uses addition *or* multiplication.
  - 3 replace  $\mathbb{Z}/N$  or  $(\mathbb{Z}/N)^\times$  with  $\text{Jac}(C)(\mathbb{F})$ .
- Some algorithms involve many choices of curve.
- Quantities like
$$\text{how often does } \ell \mid \#\text{Jac}(C)(\mathbb{F})$$
important for security / run-time analysis

# Applications

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- *Algorithm for producing papers:*
  - 1 identify algorithm or protocol over  $\mathbb{Z}/N$ .
  - 2 realize it only uses addition *or* multiplication.
  - 3 replace  $\mathbb{Z}/N$  or  $(\mathbb{Z}/N)^\times$  with  $\text{Jac}(C)(\mathbb{F})$ .
- Some algorithms involve many choices of curve.
- Quantities like
$$\text{how often does } \ell \mid \#\text{Jac}(C)(\mathbb{F})$$
important for security/run-time analysis

# Motivation: Cohen-Lenstra heuristics

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Cohen and Lenstra (1983) conjecturally describe asymptotics of class groups of quadratic imaginary number fields.
- Concretely, a (finite abelian) group  $H$  occurs in such class groups with frequency  $|\mathrm{Aut}(H)|^{-1}$ .
- In particular,  $\ell \mid \mathrm{Cl}(\mathcal{O}_K)$  with frequency

$$\frac{1}{|\mathrm{Aut}(\mathbb{Z}/\ell)|} = \frac{1}{\ell - 1}.$$

# Function-field Cohen-Lenstra

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Replace quadratic imaginary number field with quadratic *function field*.
- Consider ideal class groups of fields  $(f(x) \in \mathbb{F}[x])$

$$K_{2,f} = \mathbb{F}(x)[y]/(y^2 - f(x)) \cong \mathbb{F}(x)[\sqrt{f(x)}].$$

- Equivalently, study hyperelliptic Jacobians.
- Friedman and Washington 1989 conjecture: An abelian  $\ell$ -group  $H$  occurs as  $\text{Cl}(K)[\ell]$  with frequency proportional to  $1/|\text{Aut}(H)|$ . (They take a limit over all  $g$ .)

*This conjecture is now a theorem (A.-)*

# Previous work

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Consider  $K_{d,f} = \mathbb{F}_q(X)[Y^d - f(X)]$ ,  $f(X) \in \mathbb{F}_q[X]$  monic and separable,  $\deg f = n$ .

- Friesen 2000 gathers data, bounds, for  $(d, n) = (2, 4)$ .
- Cardon and Murty 2001: Fix  $n$  odd. The number of  $f$  with  $\ell | h(K_{2,f})$  is at least

$$q^{n(1/2+1/\ell)}.$$

Gives infinite supply of such function fields, but the number of such  $f$  is  $\sim q^n$ , thus

$$\lim_{q \rightarrow \infty} \frac{q^{n(1/2+1/\ell)}}{\#K_{2,f}/\mathbb{F}_q} = 0.$$

# Previous work

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Consider  $K_{d,f} = \mathbb{F}_q(X)[Y^d - f(X)]$ ,  $f(X) \in \mathbb{F}_q[X]$  monic and separable,  $\deg f = n$ .

- Friesen 2000 gathers data, bounds, for  $(d, n) = (2, 4)$ .
- Cardon and Murty 2001: Fix  $n$  odd. The number of  $f$  with  $\ell | h(K_{2,f})$  is at least

$$q^{n(1/2+1/\ell)}.$$

- Chakraborty and Mukhopadhyay 2004:  $n$  even. They produce at least  $q^{n/\ell} / \ell^2$   $f$  with  $\ell | h(K_{2,f})$ .
- Lee and Pacelli [2004-2006]: (Dedekind rings in) higher degree extensions of  $\mathbb{F}(x)$ , e.g.,  $K_{d,f}$ .

# Previous work – elliptic curves

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_2$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Lenstra 1987: the proportion of elliptic curves  $E/\mathbb{F}_p$  with  $\ell \mid |E(\mathbb{F}_p)|$  is about  $1/(\ell - 1)$ , if  $p \equiv 1 \pmod{\ell}$ .
- Howe 1993: Generalizes to  $\mathbb{F}_q$ , computes proportion of  $E/\mathbb{F}_q$  with given group structure.
- Gekeler 2003: Computes number of elliptic curves over  $\mathbb{F}_p$  with given trace and determinant of Frobenius.

*Results stated here for divisibility, but can extract group structure, too.*

# Outline

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- 1 Introduction
  - Basic question
  - Motivation
- 2 Main theorem
  - Statement of theorem
  - Interlude on monodromy (I)
  - Proof for  $\mathcal{M}_g$
- 3 Interlude on monodromy (II)
- 4 Arbitrary families
- 5 Cyclic covers of  $\mathbb{P}^1$

# Proportions

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- $X \rightarrow S \rightarrow \mathbb{F}_{q_0}$  an abelian scheme of relative dimension  $g$ .

$$\mathcal{P}(X \rightarrow S, \ell, \mathbb{F}_q) = \frac{|\{s \in S(\mathbb{F}_q) : X_s[\ell](\mathbb{F}_q) \neq \{0\}\}|}{|S(\mathbb{F}_q)|}$$

$$\mathcal{Q}(X \rightarrow S, \ell, \mathbb{F}_q) = \frac{|\{s \in S(\mathbb{F}_q) : X_s[\ell](\mathbb{F}_q) \cong (\mathbb{Z}/\ell)^{2g}\}|}{|S(\mathbb{F}_q)|}.$$

# Proportions

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- $C \rightarrow S \rightarrow \mathbb{F}_{q_0}$  a relative smooth, proper curve.

$$\mathcal{P}(C \rightarrow S, \ell, \mathbb{F}_q) = \mathcal{P}(\text{Jac}(C) \rightarrow S, \ell, \mathbb{F}_q)$$

$$\mathcal{Q}(C \rightarrow S, \ell, \mathbb{F}_q) = \mathcal{Q}(\text{Jac}(C) \rightarrow S, \ell, \mathbb{F}_q)$$

Thus,  $\mathcal{P}(C \rightarrow S, \ell, \mathbb{F}_q)$  is the proportion of elements with class number a multiple of  $\ell$ .

# Main result – connected monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

## Theorem

Suppose  $X \rightarrow S$  has connected  $\ell$ -adic monodromy group,  $q_0 \equiv 1 \pmod{\ell}$ . If  $q$  sufficiently large, then:

$$\mathcal{Q}(X \rightarrow S, \ell, \mathbb{F}_q) > \frac{1}{\ell g(2g+1)}.$$

If  $\ell \in \mathbb{L}$ , a set of primes of positive density, then:

$$\mathcal{P}(X \rightarrow S, \ell, \mathbb{F}_q) > \frac{1}{\ell} - \mathcal{O}(1/\ell^2).$$

*If monodromy group is known, get much more precise result.*

# Main result – unspecified monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

## Theorem

*Given  $X \rightarrow S$ , there exist  $\beta$  and  $\nu$  such that if  $q \equiv 1 \pmod{\ell^\beta}$  is sufficiently large, then:*

$$\mathcal{Q}(X \rightarrow S, \ell, \mathbb{F}_q) > \frac{1}{\delta \ell^{g(2g+1)}}.$$

*If  $\ell \in \mathbb{L}$ , a set of primes of density  $\delta > 0$ , then:*

$$\mathcal{P}(X \rightarrow S, \ell, \mathbb{F}_q) > \frac{1}{\delta \ell} - \mathcal{O}(1/\ell^2).$$

*There are bounds on  $\beta$ ,  $\nu$  and  $\delta$  purely in terms of  $g$ .*

# Corollaries: $\ell$ -rank of class numbers often positive

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

In any reasonable family of function fields, the proportion of members for which the class group:

- has maximal  $\ell$ -rank ( $2g$ ) is **positive**;
- has an element of order  $\ell$  is **at least  $1/\nu\ell$** .

For universal families of curves, or of hyperelliptic curves,  $\nu = 1$ ,  $\delta = 1$ , and the proportion members with an element of order  $\ell$  in the class group is **at least  $1/\ell$** .

# Corollaries: Friedman-Washington conjecture

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Get a corrected, proven Friedman-Washington conjecture.
- Frequency with which  $H$  appears as  $\ell$ -part of class group is inversely proportional to a “symplectic automorphism group” of  $H$ .

*Recall: Friedman-Washington say this frequency should be  $1/|\mathrm{Aut}(H)|$ .*

# Corollaries: Cyclic covers of $\mathbb{P}^1$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $\mathcal{H}_n$  be space of monic separable polynomials of degree  $n$ .
- If  $f \in \mathcal{H}_n(\mathbb{F})$ , let  $K_{d,f} = \text{Frac } \mathbb{F}[T, Y]/[Y^d - f(T)]$ .
- $K_{d,f} = \mathbb{F}(C_{d,f})$ ,  $C_{d,f}$  smooth, projective of genus  $g = \frac{1}{2}((n-1)(d-1) + 1 - \gcd(d, n))$ .
- If  $q \gg_{\ell, d, n} 0$  then:

$$\frac{|\{f \in \mathcal{H}_n(\mathbb{F}_q) : \ell \mid |\text{Cl}(K_{d,f})|\}|}{|\mathcal{H}_n(\mathbb{F}_q)|} > \frac{1}{2d\ell g(2g+1)}.$$

This yields a **lower bound** for the **density** of such extensions in families.

# $\ell$ -torsion: elliptic curves

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- We know that

$$E[\ell](\overline{\mathbb{F}}) \cong (\mathbb{Z}/\ell)^2.$$

- $P \in E[\ell](\overline{\mathbb{F}})$  is actually defined over  $\mathbb{F}$  if it is fixed by the Frobenius map  $\text{Fr}_E$ .
- Our question reduces to:

*Explain the distribution of  $\text{Fr}_E$  in  $\text{GL}_2(\mathbb{Z}/\ell)$  as the choice of  $E$  varies.*

# $\ell$ -torsion: curves of genus $g$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- We know that

$$\mathrm{Jac}(C)[\ell](\overline{\mathbb{F}}) \cong (\mathbb{Z}/\ell)^{2g}.$$

- A  $P \in \mathrm{Jac}(C)[\ell](\overline{\mathbb{F}})$  is actually defined over  $\mathbb{F}$  if it is fixed by the Frobenius map  $\mathrm{Fr}_C$ .
- Our question reduces to:

*Explain the distribution of  $\mathrm{Fr}_C$  in  $\mathrm{GL}_{2g}(\mathbb{Z}/\ell)$  as the choice of  $C$  varies.*

# Topological monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

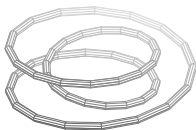
Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

A cover  $X$  of  $S$  corresponds to  $\pi_1(S, s) \rightarrow \text{Aut}(X_s)$ .



$$\pi_1(S, s) = \langle \gamma \rangle \rightarrow \text{Aut}(T_s)$$

*try it*

# Algebraic monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- A variety  $S$  has a fundamental group,  $\pi_1(S, s)$ .
- A cover  $X \rightarrow S$  corresponds to

$$\pi_1(S, s) \longrightarrow \text{Aut}(X_s)$$

- A local system  $\mathcal{F}$  of rank  $n$   $\Lambda$ -modules corresponds to

$$\pi_1(S, s) \xrightarrow{\rho_{\mathcal{F}}} \text{GL}(\mathcal{F}_s) \cong \text{GL}_n(\Lambda)$$

- The monodromy group  $G$  of  $\mathcal{F}$  is (the isomorphism class of the Zariski closure of) the image of this representation.

# Frobenius

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- $x \in S(k)$  gives

$$\pi_1(\mathrm{Spec} k) \xrightarrow{x_*} \pi_1(S, \eta)$$

- If  $k = \mathbb{F}$  finite, set

$$\mathrm{Fr}_{x, \mathbb{F}} = x_*(a \mapsto a^q).$$

- Given  $\mathcal{F}/X$ , get  $\rho_{\mathcal{F}}(\mathrm{Fr}_{x, \mathbb{F}}) \in \mathrm{GL}_n(\Lambda)$ .

# Equidistribution: finite

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Suppose monodromy group  $G$  finite.
- $W \subset G$  stable under conjugation.
- **Theorem** [Katz, Deligne]

$$\lim_{\#\mathbb{F} \rightarrow \infty} \frac{\#\{x \in S(\mathbb{F}) : \rho_{\mathcal{F}}(\text{Fr}_{x,\mathbb{F}}) \in W\}}{\#S(\mathbb{F})} = \frac{\#W}{\#G}$$

- gap between left-hand and right-hand sides is  $\sim \frac{1}{\sqrt{\#\mathbb{F}}}$ .

*Throughout, we'll assume  $|\mathbb{F}| \equiv 1 \pmod{\ell}$ .*

# Equidistribution: examples

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- In triple cover of  $S^1$

$$\pi_1(S^1, s) \xrightarrow{\rho} \text{Aut}(T_s)$$

$$\mathbb{Z} \longrightarrow \text{Sym}(1, 2, 3)$$

image is  $\{\text{id}, (123), (132)\}$ .

For each  $g$ ,  $\rho^{-1}(g)$  has density  $1/3$ .

- Chebotarev: If  $L/K$  Galois, then local Frobenius elements are equidistributed in  $\text{Gal}(L/K)$ .

# Strategy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

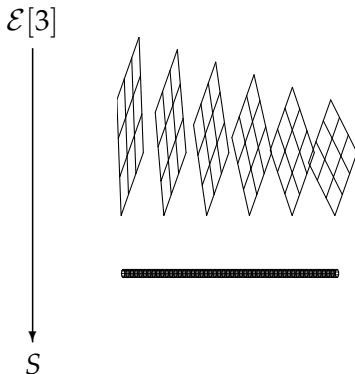
Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $X \rightarrow S$  be a family of abelian varieties. Glue  $X[\ell]$  together to get local system of  $\mathbb{Z}/\ell$ -vector spaces on  $S$ .



- $X_S[\ell] \neq 0 \iff \rho(\text{Fr}_S - \text{id})$  is not invertible.

# Strategy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Study the mod  $-\ell$  monodromy representation

$$\pi_1(S, \bar{\eta}_S) \xrightarrow{\rho} \text{Aut}(X_{\bar{\eta}_S}[\ell]) \cong \text{GL}_{2g}(\mathbb{F}_\ell) :$$

- Compute  $G = M(X \rightarrow S, \ell) = \rho(\pi_1(S, \bar{\eta}_S))$
- Calculate  $W = \{g \in G : 1 \text{ is an eigenvalue of } g\}$ .

Then

$$\frac{|\{s \in S(\mathbb{F}) : \ell \mid |X_s(\mathbb{F})|\}|}{|S(\mathbb{F})|} \approx \frac{|W|}{|G|}.$$

# Monodromy group of curves: Examples

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

The monodromy group is known when the family is:

- $\mathcal{M}_g$ , the universal family of curves of genus  $g$ ;  $G \cong \mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$  [Deligne-Mumford].
- $\mathcal{H}_g$ , the universal family of hyperelliptic curves of genus  $g$ ;  $G \cong \mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$  [JK Yu, A.-Pries]
- $\mathcal{T}_g^\alpha$ , a component of the universal family of cyclic cubic covers of  $\mathbb{P}^1$  of genus  $g$ ;  $G^0 \cong U^\alpha(\mathbb{Z}/\ell)$  for a certain unitary group  $U^\alpha$  [A.-Pries]

# Counting in $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Can write down a formula, by studying:

- structure of unipotent classes in  $G(\overline{\mathbb{F}}_\ell)$ ;
- how these classes behave over  $\mathbb{F}_\ell$ ;
- the structure of their centralizers;
- and induction.

# Sneak preview

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

$g$	$r$	$\alpha(g, r)$
3	0	$\frac{\ell^{12} - \ell^{11} - \ell^{10} + \ell^7 + \ell^5 + \ell^4 - \ell^3 - \ell - 1}{(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$
3	1	$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)(\ell^4 - 1)}$
3	2	$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)^2(\ell^4 - 1)}$
3	3	$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2}$
3	4	$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2(\ell^4 - 1)}$
3	5	$\frac{1}{(\ell^2 - 1)(\ell^4 - 1)\ell^9}$
3	6	$\frac{1}{\ell^9(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$

# Summary

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- If  $C$  is a hyperelliptic curve over a finite field  $\mathbb{F}$ , then the chance that  $\ell \mid \#\text{Jac}(C)[\ell](\mathbb{F})$  is about

$$\frac{1}{\ell - 1}.$$

- The proportion of hyperelliptic curves  $C$  for which  $\text{Jac}(C)[\ell](\mathbb{F}) \cong H$  is the proportion of  $\gamma \in \text{Sp}_{2g}(\mathbb{F}_\ell)$  for which

$$\ker(\gamma - \text{id}) \cong H.$$

*And that's the Friedman-Washington conjecture!*

# Outline

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- 1 Introduction
  - Basic question
  - Motivation
- 2 Main theorem
  - Statement of theorem
  - Interlude on monodromy (I)
  - Proof for  $\mathcal{M}_g$
- 3 Interlude on monodromy (II)
- 4 Arbitrary families
- 5 Cyclic covers of  $\mathbb{P}^1$

# Analogy: $E/K$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Let  $E/K$  be an elliptic curve without complex multiplication. Serre proves:

- $T_\ell E = \lim_{\leftarrow n} E[\ell^n](K)$  has  $\text{Gal}(K)$ -action.
- Characteristic polynomial of  $\sigma \in \text{Gal}(K)$  acting on  $T_\ell E$  is in  $\mathbb{Z}[X]$ , and is independent of  $\ell$ .
- For  $\ell \gg 0$ , image of  $\text{Gal}(K)$  in  $\text{Aut}(T_\ell(E))$  is large.

# Monodromy group: Philosophy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- $\pi : X \rightarrow S$  proper smooth.
- Consider the sheaf  $R^n \pi_* \mathbb{Q}_\ell$ .
- Get a system of representations

$$\pi_1(S, \bar{\eta}) \xrightarrow{\rho_\ell} \text{Aut}(H^i(X_{\bar{\eta}}, \mathbb{Q}_\ell))$$

which is *compatible*:

For  $s \in S(\mathbb{F}_q)$ , the characteristic polynomial of  $\rho_\ell(\text{Fr}_{s/\mathbb{F}_q})$  has  $\mathbb{Z}$ -coefficients, and is independent of  $\ell$ .

and, Frobenius elements generate the fundamental group

# Compatible systems

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

**Conjecture** Let  $\{\mathcal{F}_\ell\}$  be a compatible system of representations of  $\pi_1(S, s)$ .

- There exists a number field  $E$  and a group  $G/F$  such that  $M(R^i \pi_*(\mathbb{Q}_\ell)) \otimes E_\lambda \cong G \otimes E_\lambda$ .
- Moreover, the monodromy representation comes from a representation of  $G$  via base change.

Chin proves something very close to this for  $G^0$ .

# Compatible systems

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

**Conjecture** Let  $\{\mathcal{F}_\ell\}$  be a compatible system of representations of  $\pi_1(S, s)$ .

- There exists a number field  $E$  and a group  $G/F$  such that  $M(R^i \pi_*(\mathbb{Q}_\ell)) \otimes E_\lambda \cong G \otimes E_\lambda$ .
- Moreover, the monodromy representation comes from a representation of  $G$  via base change.

Chin proves something very close to this for  $G^0$ .

# Integral monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Serre:  $E$  an elliptic curve without CM, then image of Galois in  $T_\ell(E)$  is  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  for almost all  $\ell$ .
- **Conjecture** Actual image of monodromy is hyperspecial in  $G(E_\lambda)$ , e.g., is  $G(\mathcal{O}_\lambda)$ , for almost all  $\ell$ .
- Larsen proves this for a set of primes of density one.

# Outline

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- 1 Introduction
  - Basic question
  - Motivation
- 2 Main theorem
  - Statement of theorem
  - Interlude on monodromy (I)
  - Proof for  $\mathcal{M}_g$
- 3 Interlude on monodromy (II)
- 4 Arbitrary families
- 5 Cyclic covers of  $\mathbb{P}^1$

# Arbitrary families

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Use a general result of Larsen on compatible systems of Galois representations:
- **Theorem** [Larsen] For fixed  $X \rightarrow S$ , there exist a group  $G$  and a set of rational primes  $\mathbb{L}$  of density one such that if  $\ell \in \mathbb{L}$ , then

$$M(X \rightarrow S, \ell) \cong G(\mathbb{Z}/\ell).$$

# Next step

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Let  $\mathbb{F} = \mathbb{F}_\ell$ .

## Theorem

*$V/\mathbb{F}$   $n$ -dimensional vector space,  $G/\mathbb{F}$  connected split semisimple,  $G \rightarrow \mathrm{GL}(V)$  a representation. If maximal  $T_0 \subset G$  acts via a character which isn't a power of a root, then:*

$$\frac{|\{\gamma \in G(\mathbb{F}) : \gamma \text{ fixes an element of } V\}|}{|G(\mathbb{F})|} > \frac{1}{\ell - 1} - \frac{\delta(n)}{\ell - 1}$$

where  $\delta(n) = (n! + n)/(\ell - 1)$ .

# Sketch

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Fix maximally split torus  $T_0 \subset G$ .
- $T_0$  acts on  $V$  by character  $\chi_0$ ; at least  $T_0(\mathbb{F})/(\ell - 1)$  elements fix something.
- Look for similar elements in other tori.

# Example: $GL_2$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Two  $GL_2(\mathbb{F})$ -conjugacy classes of tori:

- $T_0 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$
- $T_1 = \begin{pmatrix} \alpha & \beta \\ \epsilon\beta & \alpha \end{pmatrix}$ , for fixed  $\epsilon$  with  $\sqrt{\epsilon} \notin \mathbb{F}$ .

Note that  $T_1(\mathbb{F}) \cong \{\alpha + \beta\sqrt{\epsilon}\} \cong \mathbb{F}(\sqrt{\epsilon})^\times$ .

$T_1$  is obtained from  $T_0$  by twisting with  $w := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

# Example: $GL_2$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Suppose  $\chi_0 = \det : \text{diag}(\lambda_1, \lambda_2) \mapsto \lambda_1 \lambda_2$ .
- Gives  $\mathbb{F}$ -rational character of  $T_1$ :  
$$\gamma := \alpha + \beta \sqrt{\epsilon} \mapsto N_{\mathbb{F}(\sqrt{\epsilon})/\mathbb{F}}(\gamma).$$
- Find  $|T_i|/(\ell - 1)$  elements in each  $T_i$ .

# Example: $GL_2$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Suppose  $\chi_0$  is  $\text{diag}(\lambda_1, \lambda_2) \mapsto \lambda_1$ .
- $\chi_0$  *does not* twist to  $\mathbb{F}$ -rational character of  $T_1$ .
- Balanced by action of  $T_0$  on  $V$  via  $\chi_1 : \text{diag}(\lambda_1, \lambda_2) \mapsto \lambda_2$ .

# So far...

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- If  $\ell$ -adic monodromy is hyperspecial in a split connected reductive group, then

$$\mathcal{P}(X \rightarrow S, \ell, q) > \frac{1}{\ell} - \mathcal{O}(1/\ell^2).$$

- Larsen: hyperspecial is density-one condition on primes  $\ell$ .
- What if monodromy group isn't connected?

# Disconnected monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

**Lemma** There exists étale Galois  $\tilde{S} \rightarrow S$  and extension  $\mathbb{F}_{q_1}/\mathbb{F}_{q_0}$ , so that image of

$$\pi_1(\tilde{S}) \hookrightarrow \pi_1(S) \longrightarrow \mathrm{GL}(X_{\overline{\eta}}[\ell^\infty])$$

is connected.

- In fact, image is connected component of identity of original monodromy group.
- Existence of  $\tilde{S}$  for one  $\ell$  is easy.
- Independence of  $\ell$  due to Serre (and Larsen).
- Can find *a priori* bound on  $\deg(S' \rightarrow S)$ ,  $[\mathbb{F}_{q_1} : \mathbb{F}_{q_0}]$ .

# Disconnected monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

**Lemma** There exists étale Galois  $\tilde{S} \rightarrow S$  and extension  $\mathbb{F}_{q_1}/\mathbb{F}_{q_0}$ , so that image of

$$\pi_1(\tilde{S}) \hookrightarrow \pi_1(S) \longrightarrow \mathrm{GL}(X_{\overline{\eta}}[\ell^\infty])$$

is connected.

- In fact, image is connected component of identity of original monodromy group.
- Existence of  $\tilde{S}$  for one  $\ell$  is easy.
- Independence of  $\ell$  due to Serre (and Larsen).
- Can find *a priori* bound on  $\deg(S' \rightarrow S)$ ,  $[\mathbb{F}_{q_1} : \mathbb{F}_{q_0}]$ .

# Disconnected monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

## Lemma

Suppose  $X \rightarrow S$  has disconnected monodromy group  
 $M(X \rightarrow S, \ell) = G$ ,  $\phi : \tilde{S} \rightarrow S$  étale Galois of degree  $\nu$ ,  
 $M(X \times \tilde{S} \rightarrow \tilde{S}, \ell) = G^0$ ,  $W \subset G^0$ , then

$$\frac{|\{s \in S : \rho(\text{Fr}_{X_s, \mathbb{F}}) \in W\}|}{|S(\mathbb{F}_q)|} > \frac{1}{\nu} \cdot \frac{|W|}{|G^0|}.$$

Ingredients:

- $\rho(\text{Fr}_{X_s, \mathbb{F}})$  constant in fibers of  $\phi$ .
- Equidistribution for  $\tilde{S} \rightarrow S$ .

# Disconnected monodromy

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

## Lemma

Suppose  $X \rightarrow S$  has disconnected monodromy group  
 $M(X \rightarrow S, \ell) = G$ ,  $\phi : \tilde{S} \rightarrow S$  étale Galois of degree  $\nu$ ,  
 $M(X \times \tilde{S} \rightarrow \tilde{S}, \ell) = G^0$ ,  $W \subset G^0$ , then

$$\frac{|\{s \in S : \rho(\text{Fr}_{X_s, \mathbb{F}}) \in W\}|}{|S(\mathbb{F}_q)|} > \frac{1}{\nu} \cdot \frac{|W|}{|G^0|}.$$

Ingredients:

- $\rho(\text{Fr}_{X_s, \mathbb{F}})$  constant in fibers of  $\phi$ .
- Equidistribution for  $\tilde{S} \rightarrow S$ .

# Outline

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- 1 Introduction
  - Basic question
  - Motivation
- 2 Main theorem
  - Statement of theorem
  - Interlude on monodromy (I)
  - Proof for  $\mathcal{M}_g$
- 3 Interlude on monodromy (II)
- 4 Arbitrary families
- 5 Cyclic covers of  $\mathbb{P}^1$

# Cyclic covers of $\mathbb{P}^1$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

Fix  $d, n$ ,  $\gcd(d, n) = 1$ . Study

$$\mathcal{O}_{d,f} = \mathbb{F}_q[Y, T]/(Y^d - f(T))$$

$$h_{d,f} = |\mathrm{Cl}(\mathcal{O}_{d,f})|$$

where  $f \in \mathcal{H}_n(\mathbb{F}_q)$ ,  $\mathcal{H}_n$  being the space of monic, separable polynomials of degree  $n$ .

How is  $h_{d,f} \bmod \ell$  distributed?

# Cyclic covers of $\mathbb{P}^1$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

In special cases, we can also work out the error term:

## Theorem

For  $\ell$  in a set of positive density, if  $q \equiv 1 \pmod{\ell}$ , then

$$\frac{|\{f(T) \in \mathcal{H}_n(\mathbb{F}_q) : \ell | h(d, f)\}|}{|\mathcal{H}_n(\mathbb{F}_q)|} > \frac{1}{2n} \left( \frac{1}{\ell} - \epsilon(g(d, n), \ell) \right) - \frac{2(2n)(n-1)! |\mathrm{Sp}_{2g(d, n)}(\mathbb{Z}/\ell)|}{\sqrt{q}}.$$

where  $g(d, n) = \frac{1}{2}((n-1)(d-1) + 1 - \gcd(d, n))$ .

*Even without error term, strengthens work of Cardon, Murty, Chakraborty, Pacelli, Lee.*

# Cyclic covers of $\mathbb{P}^1$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $C_{d,f}^{\text{aff}} = \text{Spec}(\mathcal{O}_{d,f})$ .
- Then  $C_{d,f}^{\text{aff}}$  is open in  $C_{d,f}$ , a smooth, projective curve of genus  $g$ . It's a cyclic cover of the projective line.
- Hypothesis on  $d, n$  implies

$$\text{Cl}(\mathcal{O}_{d,f}) \cong \text{Cl}(\mathbb{F}_q(C_{d,f})) \cong \text{Jac}(C_{d,f})(\mathbb{F}_q)$$

So, study the family  $\text{Jac}(C_d) \rightarrow \mathcal{H}_n$ .

Let  $G = M(\text{Jac}(\tilde{C}_d) \rightarrow \mathcal{H}_n, \ell)$ .

# Cyclic covers of $\mathbb{P}^1$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Error in equidistribution is of the form  $2|G|B/\sqrt{q}$ , where  $B$  is such that if  $\phi : Y \rightarrow \mathcal{H}_n$  Galois, étale,  $p \nmid \deg \phi$ , then

$$\sigma_c(Y) := \sum_i \dim H_c^i(Y, \overline{\mathbb{Q}}_\ell) \leq \deg \phi \cdot B.$$

- Estimate  $B$  by pulling back to  $\tilde{\mathcal{H}}_n$ :

$$\begin{array}{ccc} \tilde{\mathcal{H}}_n = \mathbb{A}^n - \{z_i = z_j : i \neq j\}(a_1, \dots, a_n) & & \\ \downarrow & & \downarrow \\ \mathcal{H}_n & & \prod (T - a_n) \end{array}$$

# Cyclic covers of $\mathbb{P}^1$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

For sums of Betti numbers of covers of  $\tilde{\mathcal{H}}_n$ , use general result on hyperplane arrangements:

## Lemma

*Let  $\mathcal{A}$  be a hyperplane arrangement in a vector space  $V$  with complement  $\mathcal{M}(\mathcal{A})$ . Let  $\phi : Y \rightarrow \mathcal{M}(\mathcal{A})$  be an irreducible étale tame Galois cover. Then*

$$\sigma_c(Y) \leq (\deg \phi) \sigma_c(\mathcal{A}).$$

Ingredients:

- Poincaré duality:  $\sigma_c(Y) = \sigma(Y)$ .
- Deligne and Illusie: If  $\phi : Y \rightarrow X$  étale, then  $\chi(Y) = (\deg \phi) \chi(X)$ , where  $\chi(U) = \sum_i (-1)^i h^i(U)$ .
- Induction on  $\dim V$ .

# Cyclic covers of $\mathbb{P}^1$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

For sums of Betti numbers of covers of  $\tilde{\mathcal{H}}_n$ , use general result on hyperplane arrangements:

## Lemma

*Let  $\mathcal{A}$  be a hyperplane arrangement in a vector space  $V$  with complement  $\mathcal{M}(\mathcal{A})$ . Let  $\phi : Y \rightarrow \mathcal{M}(\mathcal{A})$  be an irreducible étale tame Galois cover. Then*

$$\sigma_c(Y) \leq (\deg \phi) \sigma_c(\mathcal{A}).$$

Ingredients:

- Poincaré duality:  $\sigma_c(Y) = \sigma(Y)$ .
- Deligne and Illusie: If  $\phi : Y \rightarrow X$  étale, then  $\chi(Y) = (\deg \phi) \chi(X)$ , where  $\chi(U) = \sum_i (-1)^i h^i(U)$ .
- Induction on  $\dim V$ .

# Hyperplane complements

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $V$  be an  $n$ -dimensional vector space.
- Let  $\mathcal{A} = \{X_1, \dots, X_r\}$  be a finite set of hyperplanes in  $V$ .
- Goal: understand cohomology ring of  $\mathcal{M}(\mathcal{A}) = V - \cup_{X \in \mathcal{A}} X$ .

# Hyperplane complements

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Construct  $\mathcal{L}(A)$ , lattice of intersections of elements of  $A$ , ordered by inclusion.
- Let  $\mu$  be the Möbius function of  $\mathcal{L}(A)$ .
- The rank of an element  $X \in \mathcal{L}(A)$  is  $r_{\mathcal{A}}(X) = \text{codim}_V(X)$ .
- Cohomology groups of  $\mathcal{M}(A)$  given by

$$\dim H^i(\mathcal{M}(A), \overline{\mathbb{Q}}_\ell) = (-1)^i \sum_{X \in \mathcal{L}(A): r_{\mathcal{A}}(X)=i} \mu(X).$$

In particular, note that  $i^{\text{th}}$  Betti number depends only on elements of  $\mathcal{L}(A)$  with codimension at most  $i$  in  $V$ .

# Hyperplane complements

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Construct  $\mathcal{L}(A)$ , lattice of intersections of elements of  $\mathcal{A}$ , ordered by inclusion.
- Let  $\mu$  be the Möbius function of  $\mathcal{L}(A)$ .
- The rank of an element  $X \in \mathcal{L}(A)$  is  $r_{\mathcal{A}}(X) = \text{codim}_V(X)$ .
- Cohomology groups of  $\mathcal{M}(A)$  given by

$$\dim H^i(\mathcal{M}(A), \overline{\mathbb{Q}}_\ell) = (-1)^i \sum_{X \in \mathcal{L}(A): r_{\mathcal{A}}(X)=i} \mu(X).$$

In particular, note that  $i^{\text{th}}$  Betti number depends only on elements of  $\mathcal{L}(A)$  with codimension at most  $i$  in  $V$ .

# Hyperplane complements

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Let  $H \subset V$  be a hyperplane.
- Define  $\mathcal{A}_H = \{H \cap X : X \in \mathcal{A}\}$ , an arrangement in  $H$ .
- If  $H$  is *generic*,  $X \in \mathcal{L}(\mathcal{A})$  of positive dimension, then

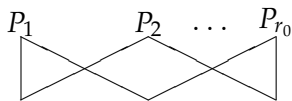
$$r_{\mathcal{A}}(X) = r_{\mathcal{A}_H}(X_H);$$

$\mathcal{L}(\mathcal{A}_H)$  obtained from  $\mathcal{L}(\mathcal{A})$  by removing top row.

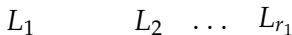
- Conclusion: If  $H \subset V$  generic, then

$$h^i(\mathcal{M}(\mathcal{A}_H), \overline{\mathbb{Q}}_\ell) = \begin{cases} h^i(\mathcal{M}(\mathcal{A}), \overline{\mathbb{Q}}_\ell) & 0 \leq i \leq n-1 \\ 0 & i = n. \end{cases} .$$

# $\mathcal{L}(\mathcal{A})$

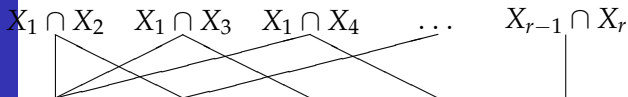


points

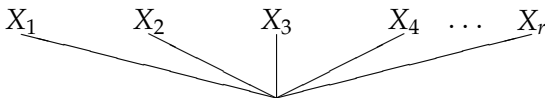


lines

$\vdots$



codim 2



hyperplanes

$\mathbb{A}^n$

ambient space

Divisibility of function field class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on monodromy (I)

Proof for  $M_g$

Interlude on monodromy (II)

Arbitrary families

Cyclic covers of  $\mathbb{P}^1$

# $\mathcal{L}(\mathcal{A}_H)$

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $\mathcal{M}_g$

Interlude on  
monodromy  
(II)

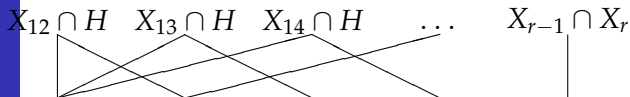
Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

$$L_1 \cap H \quad L_2 \cap H \dots L_{r_1} \cap H$$

points

$\vdots$

$$X_{12} \cap H \quad X_{13} \cap H \quad X_{14} \cap H \quad \dots \quad X_{r-1} \cap X_r$$


codim 2

$$X_1 \cap H \quad X_2 \cap H \quad X_3 \cap H \quad X_4 \cap H \dots X_r \cap H$$


hyperplanes

$H$

ambient space

# Conclusion

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Function field class numbers are often divisible.
- Thanks!

# Conclusion

Divisibility of  
function field  
class numbers

Jeff Achter

Introduction

Basic question

Motivation

Main theorem

Statement of theorem

Interlude on  
monodromy (I)

Proof for  $M_g$

Interlude on  
monodromy  
(II)

Arbitrary  
families

Cyclic covers  
of  $\mathbb{P}^1$

- Function field class numbers are often divisible.
- Thanks!