Divisibility of function field class numbers

Jeff Achter

j.achter@colostate.edu
Department of Mathematics
Colorado State University

25 April 2006
Galois theory workshop
Basic question

- Let $E / \mathbb{F}$ be an elliptic curve over a finite field.
- Let $\ell$ be a prime number.
- What’s the chance that $\ell | \#E(\mathbb{F})$?
  - 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

- Let $E / \mathbb{F}$ be an elliptic curve over a finite field.
- Let $\ell$ be a prime number.
- What’s the chance that $\ell | \#E(\mathbb{F})$?
- 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

- 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

- 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

<table>
<thead>
<tr>
<th>g</th>
<th>r</th>
<th>( \alpha(g, r) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>( \frac{\ell^2 - \ell - 1}{\ell^2 - 1} )</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>( \frac{1}{\ell} )</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>( \frac{1}{\ell(\ell^2 - 1)} )</td>
</tr>
</tbody>
</table>
Sneak preview

<table>
<thead>
<tr>
<th>g</th>
<th>r</th>
<th>( \alpha(g, r) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
<td>( \frac{\ell^6 - \ell^5 - \ell^4 + \ell + 1}{(\ell^2 - 1)(\ell^4 - 1)} )</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>( \frac{\ell^3 - \ell - 1}{\ell^2(\ell^2 - 1)} )</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>( \frac{\ell^3 - \ell - 1}{\ell^2(\ell^2 - 1)^2} )</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>( \frac{1}{(\ell^2 - 1)\ell^4} )</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>( \frac{1}{\ell^4(\ell^2 - 1)(\ell^4 - 1)} )</td>
</tr>
</tbody>
</table>
**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 $\mathbb{P}^1$**

---

**Sneak preview**

<table>
<thead>
<tr>
<th>$g$</th>
<th>$r$</th>
<th>$\alpha(g, r)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>$\frac{\ell^{12} - \ell^{11} - \ell^{10} + \ell^7 + \ell^5 + \ell^4 - \ell^3 - \ell - 1}{(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)(\ell^4 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)^2(\ell^4 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2}$</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2(\ell^4 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>$\frac{1}{(\ell^2 - 1)(\ell^4 - 1)\ell^9}$</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>$\frac{1}{\ell^9(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$</td>
</tr>
</tbody>
</table>
Sample spaces: example

\[ E \quad y^2 = x(x - 1)(x - \lambda) \]

\[ S = \mathbb{P}^1 - \{0, 1, \infty\} \quad \lambda \text{-line} \]

- Fiber over \( \lambda = \lambda_0 \) is

\[ E_{\lambda_0} : y^2 = x(x - 1)(x - \lambda_0) \]

- Varying choice of \( \lambda_0 \in S(\mathbb{F}) \) varies elliptic curve \( E_{\lambda_0}/\mathbb{F} \).
Basic question: abelian varieties

- Let $X \to S$ be an abelian scheme over a finite field. What is
  $$\frac{|\{s \in S(F) : \ell | X_s(F)\}|}{|S(F)|}?$$
- Especially, $C \to S$ a relative curve. What is
  $$\frac{|\{s \in S(F) : \ell | \text{Jac}(C_s)(F)\}|}{|S(F)|}?$$

Think of this as a parametrized family of abelian varieties.
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

- **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
  
  \[ \ell | \text{#Jac}(C)(\mathbb{F}) \]

  important for security/run-time analysis.
Applications

- **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

- 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 $|\text{Aut}(H)|^{-1}$.
- In particular, $\ell \mid \text{Cl}(\mathcal{O}_K)$ with frequency
  \[ \frac{1}{|\text{Aut}(\mathbb{Z}/\ell)|} = \frac{1}{\ell - 1}. \]
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 $\mathbb{P}^1$

Function-field Cohen-Lenstra

- Replace quadratic imaginary number field with quadratic \textit{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 $g$.)

\textit{This conjecture is now a theorem (A.-)}
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

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

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
  $$q^n(\frac{1}{2} + \frac{1}{\ell}).$$
- 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., $K_{d,f}$. 

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 $\mathbb{P}^1$
Previous work – elliptic curves

- Lenstra 1987: the proportion of elliptic curves $E/\mathbb{F}_p$ with $\ell||E(\mathbb{F}_p)|$ is about $1/(\ell - 1)$, if $p \equiv 1 \mod \ell$.
- 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.*
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 $\mathbb{P}^1$

Proportions

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

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

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

- \( C \rightarrow S \rightarrow \mathbb{F}_{q_0} \) 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

Theorem

Suppose $X \to S$ has connected $\ell$-adic monodromy group, $q_0 \equiv 1 \mod \ell$. If $q$ sufficiently large, then:

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

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

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

If monodromy group is known, get much more precise result.
Main result – unspecified monodromy

Theorem

Given $X \to S$, there exist $\beta$ and $\nu$ such that if $q \equiv 1 \mod \ell^\beta$ is sufficiently large, then:

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

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

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

There are bounds on $\beta$, $\nu$ and $\delta$ purely in terms of $g$. 
Corollaries: $\ell$-rank of class numbers often positive

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

- 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 $1/|\text{Aut}(H)|$. 
Corollaries: 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 $q \gg \ell, d, n$ then:

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

This yields a lower bound for the density of such extensions in families.
We know that

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

\( P \in E[\ell](\overline{F}) \) is actually defined over \( F \) 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.*
We know that

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

A \( P \in \text{Jac}(C)[\ell](\overline{F}) \) is actually defined over \( F \) if it is fixed by the Frobenius map \( \text{Fr}_C \).

Our question reduces to:

*Explain the distribution of \( \text{Fr}_C \) in \( \text{GL}_{2g}(\mathbb{Z}/\ell) \) as the choice of \( C \) varies.*
A cover $X$ of $S$ corresponds to $\pi_1(S,s) \to \text{Aut}(X_s)$.

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

*try it*
A variety $S$ has a fundamental group, $\pi_1(S, s)$.

A cover $X \to S$ 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

- \( x \in S(k) \) gives

\[
\pi_1(\text{Spec } k) \xrightarrow{x_*} \pi_1(S, \eta)
\]

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

\[
\text{Fr}_{x, \mathbb{F}} = x_*(a \mapsto a^q).
\]

- Given \( \mathcal{F}/X \), get \( \rho_{\mathcal{F}}(\text{Fr}_{x, \mathbb{F}}) \in \text{GL}_n(\Lambda) \).
Suppose monodromy group $G$ finite.

$W \subset G$ stable under conjugation.

**Theorem** [Katz, Deligne]

\[
\lim_{#F \to \infty} \frac{\# \{ x \in S(F) : \rho_F(Fr_{x,F}) \in W \} }{#S(F)} = \frac{#W}{#G}
\]

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

*Throughout, we’ll assume $|F| \equiv 1 \text{ mod } \ell$.***
Equidistribution: examples

- 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

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

- $X_s[\ell] \neq 0 \iff \rho(Fr_s - id)$ is not invertible.
Strategy

Study the mod $-\ell$ monodromy representation

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

- 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

The monodromy group is known when the family is:

- $\mathcal{M}_g$, the universal family of curves of genus $g$; $G \cong \text{Sp}_{2g}(\mathbb{Z}/\ell)$ [Deligne-Mumford].

- $\mathcal{H}_g$, the universal family of hyperelliptic curves of genus $g$; $G \cong \text{Sp}_{2g}(\mathbb{Z}/\ell)$ [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 $\text{Sp}_{2g}(\mathbb{F}_\ell)$

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

<table>
<thead>
<tr>
<th>$g$</th>
<th>$r$</th>
<th>$\alpha(g, r)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>$\frac{\ell^{12} - \ell^{11} - \ell^{10} + \ell^7 + \ell^5 + \ell^4 - \ell^3 - \ell - 1}{(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)(\ell^4 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>$\frac{\ell^8 - \ell^6 + \ell^2 - \ell^5 + \ell - \ell^4 + 1}{\ell^3(\ell^2 - 1)^2(\ell^4 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2}$</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>$\frac{\ell^5 - \ell^3 - 1}{\ell^7(\ell^2 - 1)^2(\ell^4 - 1)}$</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>$\frac{1}{(\ell^2 - 1)(\ell^4 - 1)(\ell^9)}$</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>$\frac{1}{\ell^9(\ell^2 - 1)(\ell^4 - 1)(\ell^6 - 1)}$</td>
</tr>
</tbody>
</table>
Summary

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

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: $E/K$

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

- $T_\ell E = \lim_{n \to \infty} E[\ell^n](K)$ 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

- $\pi : X \to S$ 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 $s \in S(\overline{\mathbb{F}}_q)$, 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
**Conjecture** Let \( \{ F_\ell \} \) 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

**Conjecture** Let \( \{ F_\ell \} \) 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 \( G^0 \).
Serre: $E$ an elliptic curve without CM, then image of Galois in $T_\ell(E)$ is $\text{GL}_2(\mathbb{Z}_\ell)$ 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.
Arbitrary families

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

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

Let $F = F_\ell$.

**Theorem**

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

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

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

- Fix maximally split torus $T_0 \subset G$.
- $T_0$ acts on $V$ by character $\chi_0$; at least $T_0(F)/(\ell - 1)$ elements fix something.
- Look for similar elements in other tori.
Example: $\text{GL}_2$

Two $\text{GL}_2(F)$-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 $\sqrt{\epsilon} \notin F$.

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

$T_1$ is obtained from $T_0$ by twisting with $w := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. 
Example: $GL_2$

- 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: $GL_2$

- 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 $\chi_1 : \text{diag}(\lambda_1, \lambda_2) \mapsto \lambda_2$. 


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

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

Larsen: hyperspecial is density-one condition on primes $\ell$.

What if monodromy group isn’t connected?
Disconnected monodromy

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

$$\pi_1(\tilde{S}) \hookrightarrow \pi_1(S) \twoheadrightarrow \text{GL}(X_{\bar{\eta}}[\ell^{\infty}])$$

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

Lemma There exists étale Galois \( \tilde{S} \to S \) and extension \( \mathbb{F}_{q_1}/\mathbb{F}_{q_0} \), so that image of

\[
\pi_1(\tilde{S}) \hookrightarrow \pi_1(S) \to \text{GL}(X_\eta[\ell^\infty])
\]

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 \( \deg(S' \to S) \), \( [\mathbb{F}_{q_1} : \mathbb{F}_{q_0}] \).
Disconnected monodromy

Lemma

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

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

Ingredients:

- $\rho(Fr_{X_s,\mathbb{F}})$ constant in fibers of $\phi$.
- Equidistribution for $\tilde{S} \to S$. 
Disconnected monodromy

**Lemma**

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

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

**Ingredients:**

- $\rho(Fr_X, \mathbb{F})$ constant in fibers of $\phi$.
- Equidistribution for $\tilde{S} \to S$. 
Outline

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 $\mathbb{P}^1$

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

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

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

where $f \in \mathcal{H}_n(\mathbb{F}_q)$, $\mathcal{H}_n$ being the space of monic, separable polynomials of degree $n$. How is $h_{d,f}$ mod $\ell$ distributed?
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 $q \equiv 1 \mod \ell$, then

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

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 \( \mathbb{P}^1 \)

- 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 \( \text{Jac}(C_d) \to \mathcal{H}_n \).

Let \( G = M(\text{Jac}(\tilde{C}_d) \to \mathcal{H}_n, \ell) \).
Cyclic covers of $\mathbb{P}^1$

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

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

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

$$\tilde{\mathcal{H}}_n = \mathbb{A}^n - \{z_i = z_j : i \neq j\}(a_1, \cdots, a_n)$$

$$\mathcal{H}_n \quad \cdots \quad \prod(T - a_n)$$
Cyclic covers of $\mathbb{P}^1$

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

**Lemma**

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

$$\sigma_c(Y) \leq (\deg \phi)\sigma_c(A).$$

**Ingredients:**

- Poincaré duality: $\sigma_c(Y) = \sigma(Y)$.
- Deligne and Illusie: If $\phi : Y \to X$ 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 $\mathbb{P}^1$

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

**Lemma**

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

$$\sigma_c(Y) \leq (\deg \phi)\sigma_c(A).$$

**Ingredients:**

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

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

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

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

$$r_A(X) = \text{codim}_V(X).$$

Cohomology groups of $\mathcal{M}(A)$ given by

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

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

Define $A_H = \{ H \cap X : X \in A \}$, an arrangement in $H$.

If $H$ is generic, $X \in \mathcal{L}(A)$ of positive dimension, then

$$r_A(X) = r_{A_H}(X_H);$$

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

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

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

Diagram:

$L(A)$

Points

Lines

Codim 2

Hyperplanes

Ambient space

$\mathbb{A}^n$

$P_1 \ldots P_{r_0}$

$L_1 \ldots L_{r_1}$

$X_1 \cap X_2 \ldots X_{r-1} \cap X_r$

$X_1 \cap X_3 \ldots X_{r-2} \cap X_r$

$X_1 \cap X_4 \ldots X_{r-3} \cap X_r$

$\ldots$

$X_{r-1} \cap X_r$
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 $\mathbb{P}^1$

$\mathcal{L}(A_H)$

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

$\vdots$

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

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

$H$

points
codim 2
hyperplanes
ambient space
Conclusion

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

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