Contemporary Mathematics

Results of Cohen-Lenstra type for quadratic function fields

Jeffrey D. Achter

Abstract. Consider hyperelliptic curves C of fixed genus over a finite field $\mathbb{F}$. Let L be a finite abelian group of exponent dividng N. We give an asymptotic formula in $|\mathbb{F}|$, with explicit error term, for the proportion of C for which $\mathrm{Jac}(C)[N](\mathbb{F}) \cong L$.

1. Introduction

Let C be a smooth, proper curve of positive genus g over a finite field $\mathbb{F}$. Its Jacobian $\mathrm{Jac}(C)$ is a g-dimensional abelian variety. On one hand, if an explicit model of C is chosen, then there are efficient methods for computing in the finite abelian group $\mathrm{Jac}(C)(\mathbb{F})$. Varying the coefficients of C yields a *family* of groups. On the other hand, since $\mathrm{Jac}(C)(\mathbb{F})$ is isomorphic to the class group of the function field of C, studying these groups is tantamount to analyzing the class groups of certain families of global fields, an endeavor with a rich history of its own.

The groups $\mathrm{Jac}(C)(\mathbb{F})$ are extremely useful in public-key cryptography and computational number theory. For instance, the security of ElGamal's encryption scheme relies on the difficulty of the discrete logarithm problem in $\mathbb{Z}/p$: given $a, b \in \mathbb{Z}/p^\times$, find e such that $a^e \equiv b \bmod p$. There is an an analogous problem in the abelian group $\mathrm{Jac}(C)(\mathbb{F})$: given $A, B \in \mathrm{Jac}(C)(\mathbb{F})$, find e such that $eA = B$. One can use to this to create an encryption scheme based on Jacobian varieties. Understanding the security of such a system relies on understanding the expected structure of the group $\mathrm{Jac}(C)(\mathbb{F})$. Such groups also arise in primality testing [**3**] and integer factorization [**19, 20**]; again, results on expected divisibility properties of $|\mathrm{Jac}(C)(\mathbb{F})|$ as C varies are crucial to estimates of efficiency.

The Cohen-Lenstra heuristics conjecturally describe the frequency with which a given abelian group occurs as the class group of a quadratic imaginary number field [**9**]. Although these heuristics remain unproven, they have inspired detailed studies of class groups of function fields. Friedman and Washington conjecturally [**10**] describe the probability with which a given abelian ℓ-group occurs as the ℓ-Sylow part of the class group of a function field drawn randomly from all, or even all hyperelliptic, function fields. (Since the function field of a hyperelliptic curve admits a presentation as $\mathbb{F}(x)[y]/(y^2 - f(x))$ for some polynomial $f(x) \in \mathbb{F}[x]$, such fields are a good analogue for quadratic number fields.) A variety of

2000 *Mathematics Subject Classification.* 11G20; 11R58, 52B30.

computational [**5, 11**] and analytic [**7, 22**] methods have been brought to bear on the distribution of class groups of hyperelliptic function fields. Roughly speaking, these works produces families of such fields whose class numbers are divisible by a given prime ℓ. While these families are infinite, they account for a proportion of polynomials which *vanishes* as $|\mathbb{F}|$ increases.

In this note, we explain how deep equidistribution results due to Katz [**16**, Chapter 9] yield the solution of the Friedman-Washington conjecture. Moreover, we take advantage of recent refinements to Katz's method by Kowalski [**17**] to give explicit bounds on the error terms which arise, by bounding the ℓ-adic Betti numbers of étale covers of hyperplane arrangements.

It's a pleasure to thank Kristin Lauter and Ken Ribet for organizing this workshop, and Rachel Pries for comments on this note.

2. Equidistribution

Let $S/\mathbb{F}$ be a geometrically irreducible variety, and let $\bar{\eta} \hookrightarrow S$ be a geometric point. Let G^{geom} be a finite group. An irreducible étale G^{geom}-cover of $S_{\bar{\mathbb{F}}}$ corresponds to a surjective homomorphism $\rho^{\mathrm{geom}} : \pi_1(S_{\bar{\mathbb{F}}}, \bar{\eta}) \to G^{\mathrm{geom}}$. To a point $s \in S(\mathbb{F})$ corresponds a Frobenius element $\mathrm{Fr}_{s/\mathbb{F}}$ in $\pi_1(S)$, well-defined up to conjugacy. Katz proves a strong Chebotarev-type theorem, which states that the images of these Frobenius elements under ρ are equidistributed.

Theorem 2.1 (Katz). [**16**, Thm. 9.7.13] *Let $S/\mathbb{F}$ be a smooth geometrically irreducible variety, and let $\bar{\eta} \hookrightarrow S$ be a geometric point. Suppose we are given a commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1^{\mathrm{geom}}(S,\bar{\eta}) & \longrightarrow & \pi_1(S,\bar{\eta}) & \longrightarrow & \mathrm{Gal}(\mathbb{F}) \cong \hat{\mathbb{Z}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \rho} & & \downarrow & & \\ 1 & \longrightarrow & G^{\mathrm{geom}} & \longrightarrow & G & \xrightarrow{m} & \Gamma & \longrightarrow & 1 \end{array} \tag{2.1}$$

where Γ is abelian, G is finite and $|G|$ is invertible in $\mathbb{F}$. Let $\gamma \in \Gamma$ be the image of the inverse of the Frobenius substitution $x \mapsto x^{|\mathbb{F}|}$. There exists a constant B such that if $C \subset G$ is stable under conjugation and if $\mathbb{F}'/\mathbb{F}$ is an extension of degree n, then

$$\left| \frac{\left|\{s \in S(\mathbb{F}') : \rho(\mathrm{Fr}_{s/\mathbb{F}'}) \in C\}\right|}{|S(\mathbb{F}')|} - \frac{\left|C \cap G^{(\gamma^n)}\right|}{|G^{\mathrm{geom}}|} \right| < \frac{B}{\sqrt{|\mathbb{F}'|}}, \tag{2.2}$$

where $G^{(\gamma^n)} = m^{-1}(\gamma^n)$.

One can calculate an effective value for B in (2.2) in terms of certain ℓ-adic Betti numbers. If X is a variety over a field k in which a rational prime ℓ is invertible, the i^{th} ℓ-adic Betti number of X is $h^i(X, \bar{\mathbb{Q}}_\ell) := \dim H^i(X_{\bar{k}}, \bar{\mathbb{Q}}_\ell)$. The sum of these numbers is $\sigma(X, \bar{\mathbb{Q}}_\ell)$, and the ℓ-adic Euler characteristic of X is the alternating sum $\chi(X, \bar{\mathbb{Q}}_\ell) := \sum_i (-1)^i h^i(X, \bar{\mathbb{Q}}_\ell)$.

We will also need to use the Betti numbers with compact support $h_c^i(X, \bar{\mathbb{Q}}_\ell) := \dim H_c^i(X_{\bar{k}}, \bar{\mathbb{Q}}_\ell)$. The sum of these compact Betti numbers of X is $\sigma_c(X, \bar{\mathbb{Q}}_\ell)$, and the alternating sum of these numbers is $\chi_c(X, \bar{\mathbb{Q}}_\ell)$. If X is smooth, then Poincaré duality yields the equality $\sigma(X, \bar{\mathbb{Q}}_\ell) = \sigma_c(X, \bar{\mathbb{Q}}_\ell)$.

LEMMA 2.2 (Kowalski). [**17**, Prop. 4.7] *In the situation of Theorem 2.1, for B one may take $2|G|B_1$ where B_1 is any number such that for every étale Galois cover $\phi : Y \to S$ with $\deg \phi$ invertible in $\mathbb{F}$, we have $\sigma_c(Y, \bar{\mathbb{Q}}_\ell) \leq \deg \phi \cdot B_1$.*

PROOF. A representation $\varpi : G \to \mathrm{GL}_n(\bar{\mathbb{Q}}_\ell)$ induces a lisse E_λ sheaf on S, denoted $\mathcal{F}_\varpi$, for some finite extension E_λ of $\mathbb{Q}_\ell$. By [**16**, 9.2.6.(4)], for B one may take $2B_2$ where B_2 is any number such that for all ϖ,

$$\sum \dim H^i_c(S_{\bar{\mathbb{F}}}, \mathcal{F}_\varpi) \leq \dim(\varpi) B_2.$$

By [**17**, Prop. 4.7], for B_2 one may take $|G|B_1$, where B_1 is any number such that for every étale Galois cover $\phi : Y \to S$ with $\deg \phi$ invertible in $\mathbb{F}$, $\sigma_c(Y, \bar{\mathbb{Q}}_\ell) \leq \deg \phi \cdot B_1$. □

3. Cohen-Lenstra for function fields

We introduce some notation necessary for stating our form of the Friedman-Washington conjecture (Theorem 3.1).

First, we require some notation about the group of symplectic similitudes. Let N be an odd natural number, and fix a natural number g. Let V be a free $\mathbb{Z}/N$-module of rank $2g$ equipped with a symplectic pairing $\langle \cdot, \cdot \rangle$. We use this as a model for $\mathrm{GSp}_{2g}(\mathbb{Z}/N)$:

$$\begin{aligned}\mathrm{GSp}_{2g}(\mathbb{Z}/N) &\cong \mathrm{GSp}(V, \langle \cdot, \cdot \rangle) \\ &= \{A \in \mathrm{GL}(V) | \exists m(A) \in (\mathbb{Z}/N)^\times : \forall v, w \in V, \langle Av, Aw \rangle = m(A)\langle v, w \rangle\}.\end{aligned}$$

The map $A \mapsto m(A)$ is a homomorphism $\mathrm{GSp}_{2g}(\mathbb{Z}/N) \to (\mathbb{Z}/N)^\times$. For $r \in (\mathbb{Z}/N)^\times$, let $\mathrm{GSp}^{(r)}_{2g}(\mathbb{Z}/N) = m^{-1}(r)$; each $\mathrm{GSp}^{(r)}_{2g}(\mathbb{Z}/N)$ is a torsor over $\mathrm{Sp}_{2g}(\mathbb{Z}/N)$.

If L is any finite abelian group annihilated by N, let

$$\alpha(g, r, N, L) = \frac{\left|\{x \in \mathrm{GSp}_{2g}(\mathbb{Z}/N)^{(r)} : \ker(x - \mathrm{id}) \cong L\}\right|}{\left|\mathrm{Sp}_{2g}(\mathbb{Z}/N)\right|}.$$

In the special case where N is prime and $r = 1$, an explicit formula for $\alpha(g, r, N, L)$ is given by [**1**, Lemma 2.2]; see [**12**] for a formula for $\alpha(1, r, N, L)$ for arbitrary N and L. For general N, Goursat's lemma lets one reduce the calculation to the case where N is a prime power. We will see below (Theorem 3.1) that $\alpha(g, |\mathbb{F}|, N, L)$ is a good approximation for the proportion of genus g quadratic function fields over $\mathbb{F}$ for which the N-torsion in the class group is isomorphic to L.

Second, we introduce a family of hyperelliptic curves. For a natural number n, let $\mathcal{H}_n$ be the space parametrizing all monic separable polynomials of degree n. Let $\mathcal{C}_g \to \mathcal{H}_{2g+2}$ be the relative smooth proper curve whose fiber over $f(x) \in \mathcal{H}_{2g+2}(\mathbb{F})$ has affine model $y^2 = f(x)$. (Note that every hyperelliptic curve admits such a model.)

With these preparations, we can state and prove a theorem of Cohen-Lenstra type for quadratic function fields.

THEOREM 3.1. *Let g be a natural number, let N be an odd natural number, and let $\mathbb{F}$ be a sufficiently large finite field in which $\left|\mathrm{GSp}_{2g}(\mathbb{Z}/N)\right|$ is invertible. Then*

$$\left|\frac{|\{f(x) \in \mathcal{H}_{2g+2}(\mathbb{F}) : \mathrm{Jac}(\mathcal{C}_{g,f})(\mathbb{F})[N] \cong L\}|}{|\mathcal{H}_{2g+2}(\mathbb{F})|} - \alpha(g, |\mathbb{F}|, N, L)\right| < \frac{2(2g+1)!\left|\mathrm{GSp}_{2g}(\mathbb{Z}/N)\right|}{\sqrt{|\mathbb{F}|}}.$$

PROOF. Consider the étale sheaf $\mathcal{F}_N = \mathrm{Jac}(\mathcal{C}_g)[N] \to \mathcal{H}_{2g+2}$, which corresponds (after fixing a basepoint $\bar{\eta}$) to a representation $\rho : \pi_1(\mathcal{H}_{2g+2}, \bar{\eta}) \to \mathrm{Aut}(\mathcal{F}_{N,\bar{\eta}}) \cong \mathrm{GL}_{2g}(\mathbb{Z}/N)$. Computing the proportion of points $f \in \mathcal{H}_{2g+2}(\mathbb{F})$ for which $\mathrm{Jac}(\mathcal{C}_{g,f})[N] \cong L$ is the same as computing the proportion of points $f \in \mathcal{H}_{2g+2}(\mathbb{F})$ for which $\ker(\rho(\mathrm{Fr}_{f,\mathbb{F}}) - \mathrm{id}) \cong L$; the latter task is accomplished using Katz's theorem 2.1. In the notation of (2.1), $G^{\mathrm{geom}} \cong \mathrm{Sp}_{2g}(\mathbb{Z}/N)$. If N is prime, this is attributed to an unpublished work of J.K. Yu (see [**8**, 2.4]) and is proved in [**2**, Thm. 3.4] and in [**13**, Thm. 4.1]. The case where N is a prime power follows formally from this [**2**, Cor. 3.5], while the case of general N (still prime to the characteristic) follows from Goursat's lemma [**17**, Cor. 2.6].

By Lemma 2.2, for B in (2.2) one may take $\left|\mathrm{GSp}_{2g}(\mathbb{Z}/N)\right|B_2$, where B_2 is any number such that for every étale Galois cover $\phi : Y \to \mathcal{H}_{2g+2}$ with $\deg\phi$ invertible in $\mathbb{F}$, $\sigma_c(Y, \bar{\mathbb{Q}}_\ell) \leq \deg\phi \cdot B_2$.

We provide an explicit value for B_2 as follows. Let $z_1, \cdots, z_{2g+2}$ be coordinates on affine space $\mathbb{A}^{2g+2}$, and let $\widetilde{\mathcal{H}}_{2g+2} = \mathbb{A}^{2g+2} - \cup_{i\neq j}(z_i = z_j)$ be the complement of the fat diagonal. It is an irreducible, étale S_{2g+2}-cover of $\mathcal{H}_{2g+2}$; the geometric fiber over $f \in \mathcal{H}_{2g+2}(\mathbb{F})$ is the set of labelings of the roots of f.

Let $\phi : Y \to \mathcal{H}_{2g+2}$ be an étale Galois cover with automorphism group G. Trivially one has $\sigma_c(Y, \bar{\mathbb{Q}}_\ell) \leq \sigma_c(Y \times_{\mathcal{H}_{2g+2}} \widetilde{\mathcal{H}}_{2g+2}, \bar{\mathbb{Q}}_\ell)$. Let r be the number of connected components of $Y \times_{\mathcal{H}_{2g+2}} \widetilde{\mathcal{H}}_{2g+2}$. Each component is isomorphic to a K-cover Z of $\widetilde{\mathcal{H}}_{2g+2}$, where K is a subgroup of G of index r. By Lemma 3.3, $\sigma_c(Z, \bar{\mathbb{Q}}_\ell) \leq |K| \cdot \sigma_c(\widetilde{\mathcal{H}}_{2g+2}, \bar{\mathbb{Q}}_\ell)$. Since $\widetilde{\mathcal{H}}_{2g+2}$ is smooth, $\sigma_c(\widetilde{\mathcal{H}}_{2g+2}, \bar{\mathbb{Q}}_\ell) = \sigma(\widetilde{\mathcal{H}}_{2g+2}, \bar{\mathbb{Q}}_\ell)$. The calculation $\sigma(\widetilde{\mathcal{H}}_{2g+2}, \bar{\mathbb{Q}}_\ell) = (2g+1)!$, originally due to Arnol′d [**4**], may also be recovered from equation (3.2) below. □

The space $\widetilde{\mathcal{H}}_{2g+2}$ introduced in the proof of Theorem 3.1 is the braid arrangement studied by Arnol′d. In Lemma 3.3 we prove a case of [**17**, Prop. 4.5] optimized for hyperplane arrangements.

Let $T \to S$ be a Galois cover of smooth varieties, and let $S_H \subset S$ be a suitably generic hyperplane section. The strategy of [**17**, Prop. 4.5], which is a refinement of the argument of [**15**], is to relate the Betti numbers of T to those of $T_H = T \times_S S_H$. This inductive method produces explicit upper bounds for the Betti numbers of T, but they tend to be pessimistically large. For example, the bounds obtained from [**17**] for the Betti numbers of $\mathcal{H}_n$ are much larger than n^n.

In the special case where S is a hyperplane arrangement, we can replace the (abstract) Lefschetz theorem with an explicit calculation of $\sigma(S, \bar{\mathbb{Q}}_\ell) - \sigma(S_H, \bar{\mathbb{Q}}_\ell)$. Moreover, S_H is itself a hyperplane arrangement, so that we may use induction on the dimension of S without leaving the class of hyperplane arrangements.

Let V/k be an n-dimensional vector space over an algebraically closed field, and let $\mathcal{A}$ be a finite collection of hyperplanes in V. The complement of this

arrangement is $\mathcal{M}(\mathcal{A}) = V - \cup_{X\in\mathcal{A}} X$. The ℓ-adic Poincaré polynomial of $\mathcal{M}(\mathcal{A})$ is $P_\ell(\mathcal{M}(\mathcal{A}), t) = \sum_i h^i(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)t^i$.

Let $\mathcal{L}(\mathcal{A})$ be the set of nonempty intersections of elements of $\mathcal{A}$, ordered by reverse inclusion; if $X, Y \in \mathcal{A}$, then $X \leq Y$ if and only if $X \supseteq Y$. The lattice $\mathcal{L}(\mathcal{A})$ has a unique minimal element, V. The rank $r_{\mathcal{A}}(X)$ of $X \in \mathcal{L}(\mathcal{A})$ is the codimension of X in V. We will say that a hyperplane $H \subset V$ is generic with respect to $\mathcal{A}$ if for each $X \in \mathcal{L}(A)$ we have $\dim(X \cap H) = \dim(X) - 1$ if $r(X) < n$, and $X \cap H = \emptyset$ if $r(X) = n$. Being generic with respect to $\mathcal{A}$ is an open condition on the space of hyperplanes in V.

If $H \subset V$ is a hyperplane and $X \in \mathcal{A}$, let $X_H = H \cap X$; it is a hyperplane of H. Let $\mathcal{A}_H = \{X_H : X \in \mathcal{A}\}$; it is a hyperplane arrangement inside H.

LEMMA 3.2. *Let $\mathcal{A}$ be an arrangement of hyperplanes inside an n-dimensional vector space V over an algebraically closed field k, and let $H \subset V$ be a hyperplane which is generic with respect to $\mathcal{A}$. Then*

$$P_\ell(\mathcal{M}(\mathcal{A}), t) = P_\ell(\mathcal{M}(\mathcal{A}_H), t) + h^n(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)t^n.$$

PROOF. The Betti numbers of $\mathcal{M}(\mathcal{A})$ are independent of k and ℓ, in the following sense. Suppose that k' is an algebraically closed field, V'/k' is a vector space of dimension n, ℓ' is a rational prime invertible in k', and $\mathcal{A}'$ any arrangement of hyperplanes in V'. If $\mathcal{L}(\mathcal{A}') \cong \mathcal{L}(\mathcal{A})$, then $P_\ell(\mathcal{M}(\mathcal{A}), t) = P_{\ell'}(\mathcal{A}', t)$ [**6**, Section 5]. Therefore, we may replace $\mathcal{A}$ by a combinatorially equivalent arrangement over $\mathbb{C}$. For a complex hyperplane arrangement the ℓ-adic and topological Betti numbers agree [**18**, Thm. 1.1], so that we may compute the Poincare polynomial using the method of [**21**, Chapter 2].

Let $\mu : \mathcal{L}(\mathcal{A}) \times \mathcal{L}(\mathcal{A}) \to \mathbb{Z}$ be the Möbius function of the lattice of subspaces of $\mathcal{A}$, and let $\mu(X) = \mu(V, X)$. The Poincaré polynomial of $\mathcal{M}(A)$ is then [**21**, Def. 2.48 and Thm. 5.93]

$$P_\ell(\mathcal{M}(\mathcal{A}), t) = \sum_{X\in\mathcal{L}(\mathcal{A})} \mu(X)(-t)^{r_{\mathcal{A}}(X)} \tag{3.1}$$

$$= \sum_{i=0}^{n} (-1)^i \left(\sum_{X\in\mathcal{L}(\mathcal{A}):r_{\mathcal{A}}(X)=i} \mu(X) \right) t^i. \tag{3.2}$$

Note in particular that the i^{th} Betti number depends only on those elements of $\mathcal{L}(\mathcal{A})$ which have codimension at most i in V.

Now let $H \subset V$ be a hyperplane generic with respect to $\mathcal{A}$. Recall that if $r_{\mathcal{A}}(X) < n$, then $r_{\mathcal{A}_H}(X_H) = r_{\mathcal{A}}(X)$. The description (3.2) shows that the Poincaré polynomial of $\mathcal{M}(\mathcal{A}_H)$ is

$$\begin{aligned} P_\ell(\mathcal{M}(\mathcal{A}_H), t) &= \sum_{i=0}^{n-1} (-1)^i \left(\sum_{X_H\in\mathcal{L}(A_H):r_{\mathcal{A}_H}(X_H)=i} \mu(X_H) \right) t^i \\ &= \sum_{i=0}^{n-1} (-1)^i \left(\sum_{X\in\mathcal{L}(A):r_{\mathcal{A}}(X)=i} \mu(X) \right) t^i \\ &= \sum_{i=0}^{n-1} (-1)^i h^i(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)t^i. \end{aligned}$$

□

The proof of Lemma 3.3 is modeled closely on [**17**, Prop. 4.5], and we focus on the differences.

LEMMA 3.3. *Let $\mathcal{A}$ be a hyperplane arrangement in an n-dimensional vector space V over an algebraically closed field k, and let $\phi : Y \to \mathcal{M}(\mathcal{A})$ be an irreducible étale Galois cover of degree m which is invertible in k. Then*

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

PROOF. By Poincaré duality, it suffices to prove the analogous result for the sum of Betti numbers $\sigma(Y, \bar{\mathbb{Q}}_\ell)$. Since m is invertible in k, the cover ϕ is tamely ramified on the boundary of $\mathcal{M}(\mathcal{A})$ in V. A result of Deligne and Lusztig [**14**, 2.6, Cor. 2.8] shows that $\chi(Y, \bar{\mathbb{Q}}_\ell) = m\chi(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)$.

Our proof is by induction on $\dim V$. If $n = 1$, let $b_1 = h^1(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)$. Then $\chi(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell) = 1 - b_1$, so that $\chi(Y, \bar{\mathbb{Q}}_\ell) = m \cdot (1 - b_1)$, and $\sigma(Y, \bar{\mathbb{Q}}_\ell) = 1 + (1 + m(b_1 - 1)) \leq m \cdot (1 + b_1) = m\sigma(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)$.

Now assume that the lemma holds for any arrangement in a vector space of dimension $n - 1$. Using [**17**, Prop. 4.6], one may choose a hyperplane $H \subset V$, generic with respect to $\mathcal{A}$, such that the pullback $Y_H \to \mathcal{M}(\mathcal{A}_H)$ is an irreducible Galois cover of $\mathcal{M}(\mathcal{A}_H)$.

As in the proof of [**17**, Prop. 4.5], we find that

$$\sigma(Y, \bar{\mathbb{Q}}_\ell) \leq m\left((-1)^n\chi(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell) + (-1)^{n-1}\chi(\mathcal{M}(\mathcal{A}_H), \bar{\mathbb{Q}}_\ell)\right) + \sigma(Y_H, \bar{\mathbb{Q}}_\ell).$$

By Lemma 3.2, the first term on the right-hand side is simply $m \cdot h^n(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)$, while by the inductive hypothesis the other term is at most $m \cdot \sigma(\mathcal{M}(\mathcal{A}_H), \bar{\mathbb{Q}}_\ell)$. A second application of Lemma 3.2 shows that $\sigma(\mathcal{M}(\mathcal{A}_H), \bar{\mathbb{Q}}_\ell) = \sigma(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell) - h^n(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)$. Taken together, this shows that $\sigma(Y, \bar{\mathbb{Q}}_\ell) \leq m \cdot \sigma(\mathcal{M}(\mathcal{A}), \bar{\mathbb{Q}}_\ell)$. □

References

[1] Jeffrey D. Achter, *The distribution of class groups of function fields*, J. Pure and Appl. Algebra **204** (2006), no. 2, 316–333.

[2] Jeffrey D. Achter and Rachel J. Pries, *The integral monodromy of hyperelliptic and trielliptic curves*, Math. Ann. **338** (2007), no. 1, 187–206.

[3] Leonard M. Adleman and Ming-Deh A. Huang, *Primality testing and abelian varieties over finite fields*, Springer-Verlag, Berlin, 1992.

[4] V. I. Arnol′d, *The cohomology ring of the group of dyed braids*, Mat. Zametki **5** (1969), 227–231.

[5] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler, *Construction of hyperelliptic function fields of high three-rank*, Math. Comp. **77** (2008), no. 261, 503–530 (electronic).

[6] Anders Björner and Torsten Ekedahl, *Subspace arrangements over finite fields: cohomological and enumerative aspects*, Adv. Math. **129** (1997), no. 2, 159–187.

[7] David A. Cardon and M. Ram Murty, *Exponents of class groups of quadratic function fields over finite fields*, Canad. Math. Bull. **44** (2001), no. 4, 398–407.

[8] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180.

[9] Henri Cohen and Hendrik W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

[10] Eduardo Friedman and Lawrence C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 227–239.

[11] Christian Friesen, *Class group frequencies of real quadratic function fields: the degree 4 case*, Math. Comp. **69** (2000), no. 231, 1213–1228.

[12] Ernst-Ulrich Gekeler, *The distribution of group structures on elliptic curves over finite prime fields*, Doc. Math. **11** (2006), 119–142 (electronic).

[13] Chris Hall, *Big symplectic or orthogonal monodromy modulo ℓ*, Duke Math. J. **141** (2008), no. 1, 179–203.
[14] Luc Illusie, *Théorie de Brauer et caractéristique d'Euler-Poincaré (d'après P. Deligne)*, The Euler-Poincaré characteristic (French), Astérisque, vol. 82, Soc. Math. France, Paris, 1981, pp. 161–172.
[15] Nicholas M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), no. 1, 29–44.
[16] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society, Providence, RI, 1999.
[17] E. Kowalski, *The large sieve, monodromy and zeta functions of curves*, J. Reine Angew. Math. **601** (2006), 29–69.
[18] G. I. Lehrer, *The l-adic cohomology of hyperplane complements*, Bull. London Math. Soc. **24** (1992), no. 1, 76–82.
[19] H. W. Lenstra, Jr., J. Pila, and Carl Pomerance, *A hyperelliptic smoothness test. I*, Philos. Trans. Roy. Soc. London Ser. A **345** (1993), no. 1676, 397–408.
[20] Hendrik W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673.
[21] Peter Orlik and Hiroaki Terao, *Arrangements of hyperplanes*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 300, Springer-Verlag, Berlin, 1992.
[22] Allison M. Pacelli, *Abelian subgroups of any order in class groups of global function fields*, J. Number Theory **106** (2004), no. 1, 26–49.

E-mail address: j.achter@colostate.edu

Department of Mathematics, Colorado State University, Fort Collins, CO 80523
URL: http://www.math.colostate.edu/∼achter