GNTS Fall 2022 Presentation Notes

- Written by: Hyun Jong Kim

- Created: 11/19/2022
- Last updated: 11/21/2022

These are notes for my fall 2022 GNTS presentation notes on Tuesday, 11/22/2022.

I would greatly appreciate comments and corrections to these notes; please send such suggestions to me at `hyunjong<dot>kim<at>math<dot>wisc<dot>edu`.

Disclaimer

You might find it useful to use Obsidian.md if you are reading this as a Markdown file so that you can use the internal links in these notes. However, I may or may not make other notes that this note links to publicly available, so such links may be useless to you. Nevertheless, reading this as a Markdown file on Obsidian.md (alongside as a pdf file) could supplement your reading experience.

Title

Points on certain Hurwitz schemes correspond to surjections from Jacobians of curves

Abstract

I will introduce Hurwitz spaces to partially explain how Ellenberg-Venkatesh-Westerland proved a Cohen-Lenstra result for function fields and how Ellenberg-Li-Shusterman bounded the proportion of hyperelliptic zeta functions that vanish at fixed numbers.

References:

- Jordan Ellenberg, Akshay Venkatesh, Craig Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, Annals of Mathematics, Vol 183, Issue 3, p. 729-786, 2016.
  - Available at https://arxiv.org/abs/0912.0325

- Jordan Ellenberg, Wanlin Li, Mark Shusterman, *Nonvanishing of hyperelliptic zeta functions over finite fields*, Alg. Number Th. 14 1895-1909, 2020.
    - Available at https://arxiv.org/abs/1901.08202

- Matthieu Romagny and Stefan Wewers, *Hurwitz Spaces*, In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Séminaires & Congrès*, Soc. Math. France, pages 313-341, 2006.
    - available at https://perso.univ-rennes1.fr/matthieu.romagny/articles/hurwitz_spaces.pdf

---

Outline

- Configuration spaces and Hurwitz spaces
    - Configuration spaces parameterize distinct points in a space.
    - Hurwitz spaces parameterize tame G-covers of $\mathbb{P}^1$.
    - There are many variants of either type of space.
    - One main idea is an application of class field theory - the rational points of a certain class of Hurwitz schemes (constructed based on an abelian ℓ-group A) roughly correspond to surjections from class groups/Jacobians of hyperelliptic covers of $\mathbb{P}^1$ to a A.
- Ellenberg-Venkatesh-Westerland's Cohen Lenstra result
    - The proportion of imaginary quadratic extensions of $\mathbb{F}_q(t)$ whose class group has ℓ-part isomorphic to a fixed nontrivial abelian ℓ-group is proportional to $\frac{1}{|A|}$
    - One can reduce the problem of determining this proportion to counting the number of surjections from class groups of various extensions into A.
- Ellenberg-Li-Shusterman's bound on the proportion of hyperelliptic zeta functions that vanish at a fixed number
    - The proportion of zeta functions of hyperelliptic curves over $\mathbb{F}_q$ vanishing at a fixed number $s = \frac{1}{2} + it$ is asymptotically 0.
    - If $\zeta_C(s)$ vanishes at s, then there are nontrivial surjections $J_C[\ell](\overline{\mathbb{F}}_q) \to \mathbb{Z}/\ell\mathbb{Z}$ which are a-eigenvectors of Frob_q.

Configuration spaces of $\mathbb{A}^1$ or $\mathbb{P}^1$ and Hurwitz spaces of tame G-covers of $\mathbb{P}^1$

Configuration spaces

Let D denote a closed disc in $\mathbb{C}$ with a marked point $*$ in the boundary. Let Conf_n be the configuration space of n unordered, distinct points in the interior of a closed disc. More precisely,

$$\mathrm{Conf}_n := \{\{P_1, \dots, P_n\} \in D^n : P_i \neq P_j \text{ for all } i \neq j\}.$$

The above configuration is quite topological; there is also an algebraic version of this configuration space. If we topologically identify the (open) disc as $\mathbb{A}^1_{\mathbb{C}} = \mathbb{P}^1_{\mathbb{C}} - \{\infty\}$, then we would want the analogue of Conf_n to be the configuration space of $\mathbb{A}^1$.

To construct this configuration space, we first construct the configuration space Conf'_{n+1} of $\mathbb{P}^1$ of $n+1$ (unordered, distinct) points. We construct this configuration space Conf'_{n+1} as an open subscheme of projective n-space $\mathbb{P}^n$ with projective coordinates $a_0 : a_1 : \cdots : a_{n+1}$. A point $[a_0 : a_1 : \cdots : a_{n+1}]$ of Conf'_{n+1} parameterizes a binary form/homogeneous polynomial/divisor $a_0 X^n + a_1 X^{n-1} W + \cdots + a_{n+1} W^{n+1}$. To ensure that the zeros of this homogeneous polynomial do not have any repeated roots, we require that the discriminant $\Delta([a_0 : a_1 : \cdots : a_{n+1}]) = \Delta(\sum_{i=0}^{n+1} a_i X^{n+1-i} W^i)$ does not vanish. To summarize,

$$\mathsf{Conf}'_{n+1} := \{[a_0 : \cdots : a_{n+1}] : \Delta([a_0 : \cdots : a_{n+1}]) \neq 0\}$$

Now we can construct the configuration space Conf_n as the closed subscheme of Conf'_{n+1} cut out by $a_0 = 0$[1]. As desired, the points of Conf_n are exactly the degree n (squarefree) divisors of $\mathbb{A}^1$[2].

Note that Conf'_{n+1} and Conf_n can both be constructed as schemes over $\mathbb{Z}$.

Tame G-covers of $\mathbb{P}^1$

Let G denote a finite group.

Definition

Let k be a field. A **tame G-cover of $\mathbb{P}^1$** is a triple (X, f, ϕ) where

- X is a smooth proper geometrically connected curve X/k;
- $f : X \to \mathbb{P}^1$ is **tame**: that is, there exists a reduced divisor D on $\mathbb{P}^1$ such that f is étale over $\mathbb{P}^1 - D$, and such that the ramification of f over each geometric point of D is nontrivial and prime to the characteristic of k;
- f is **Galois**: that is, $\mathrm{Aut}(f)$ acts transitively on the geometric fibers of f;
- ϕ is an isomorphism from G to $\mathrm{Aut}(f)$.

#_meta/TODO change this definition to use romagny_wewers_2.1 - the definition in EVW donly considers curves over k, whereas Romagny and Wewers' definition considers curves over general schemes.

Example

Any hyperelliptic cover of $\mathbb{P}^1$ outside of characteristic 2 is a tame $\mathbb{Z}/2\mathbb{Z}$-cover.

Hurwitz spaces

Romagny and Wewers [Romagny and Wewers, Theorem 4.11, Theorem 2.1] construct a coarse moduli scheme $H_{G,n}$[3] for the functor of tame G-covers of $\mathbb{P}^1$ with branch locus of degree n in $\mathbb{P}^1$[4]. This scheme is smooth and finite type over $\mathbb{Z}$. If G is center free, then $H_{G,n}$ is a fine moduli scheme, see [Romagny and Wewers, Corollary 2.2].

There is also a finite etale morphism

$$\begin{aligned} \pi : H_{G,n} &\to \mathsf{Conf}'_n / \operatorname{Spec} R \\ (f : C \to \mathbb{P}^1) &\mapsto (\text{branch locus of } f) \end{aligned}$$

Remark

There is a topological analogue of this Hurwitz scheme. One can construct $\mathrm{Hur}_{G,n}$ as $\widetilde{\mathrm{Conf}}_n \times_{B_n} \mathrm{Hom}(\pi, G)$ where

- $\widetilde{\mathrm{Conf}}_n$ is the universal cover of Conf_n
- $B_n = \pi_1(\mathrm{Conf}_n, c_n)$ is the **Artin Braid group** where $c_n = \{P_1, \dots, P_n\}$ is a fixed basepoint for Conf_n.
- $\pi = \pi_1(\Sigma, *)$ where $\Sigma := D - \{P_1, \dots, P_n\}$ is the punctured unit disc; note that $\mathrm{Hom}(\pi, G) \cong G^n$ since π is the free group generated by the homotopy classes of basic loops γ_i going around only P_i counterclockwise.
- $\times_{B_n}$ is the Borel construction of spaces with B_n-actions; B_n acts on π by "braiding" the punctures around and thus B_n acts on the (discrete, finite) space $\mathrm{Hom}(\pi, G)$.

In particular, there is a natural covering map $\mathrm{Hur}_{G,n} \to \mathrm{Conf}_n$.

Fixing a point $\tilde{c}_n$ over c_n, the fiber of this covering map above c_n can be identified with the set $\mathrm{Hom}(\pi, G) \cong G^n$. One can show that the points in this fiber correspond to (isomorphism classes of) regular[5] covering maps $Y \to \Sigma$ whose automorphism/deck transformation group is a subgroup of G. The fibral point corresponding to $(g_1, \dots, g_n) \in G^n$ is the $\langle g_1, \dots, g_n \rangle$-cover $Y \to \Sigma$ whose monodromy by γ_i is g_i[6].

There are variants of the Hurwitz scheme $H_{G,n}$. In particular, there exist Hurwitz schemes

- $\mathsf{Hn}_{G,n}$, which parameterizes tame G-covers of $\mathbb{P}^1$ whose branch loci over $\mathbb{A}^1$ are of degree n (in particular, there may or may not be ramification over ∞, and hence the branch locus over $\mathbb{P}^1$ has degree either n or $n+1$).
- $\mathsf{Hn}^c_{G,n}$, which parameterizes tame G-covers of $\mathbb{P}^1$ whose branch loci over $\mathbb{A}^1$ are of degree n and whose monodromy is of type c, where c is a rational union of conjugacy classes in G.

The definitions or monodromy type and rational union of conjugacy classes are in order:

Definition

Let G be a finite group. A union c of conjugacy classes (or equivalently, a subset of G that is preserved under conjugation) is called **rational** if $g^N \in c$ for all $g \in c$ and N relatively prime to G.

Remark

In general, $\mathsf{Hn}^c_{G,n}$ is a subscheme of $\mathsf{Hn}_{G,n}$. We can in fact construct $\mathsf{Hn}^c_{G,n}$ over $\mathbb{F}_q$ (of characteristic prime to $|G|$) even if c is not a rational union of conjugacy classes as long as $g^q \in c$ for all $g \in c$. Let us say that c **is an** $\mathbb{F}_q$**-rational union of conjugacy classes** in this case. In this case, the approaches of Ellenberg, Venkatesh, and Westerland's work (as well as those in Ellenberg, Li, and Shusterman work) continue to apply.
See also a later remark in these notes.

Definition

Let $f : X \to \mathbb{P}^1$ be a tame G-cover over a field k. We say that f has **monodromy of type** c if the images of fixed generators of the tame inertia groups at each branch point of f lie in c.

The case of interest is $G = A \rtimes \mathbb{Z}/2\mathbb{Z}$, where A is a finite abelian ℓ-group (where ℓ is an odd prime), $\mathbb{Z}/2\mathbb{Z}$ acts on A by involution, and c is the conjugacy class consisting of all involutions.

Idea

Roughly speaking, the $\mathbb{F}_q$-rational points of $\mathsf{Hn}^c_{G,n}$ correspond to surjections of the ℓ-part of the class group to A or to surjections of the (ℓ-torsion of the) Jacobian to A which are fixed under Frob_q.

Results of Ellenberg-Venkatesh-Westerland and Ellenberg-Li-Shusterman

Ellenberg-Venkatesh-Westerland's Cohen-Lenstra result for function fields

Definition

A quadratic extension of $\mathbb{F}_q(t)$ is **imaginary** if it is ramified at ∞.
Equivalently, a quadratic extension $L \supset K$ is imaginary if it is of the form $\mathbb{F}_q(t)(\sqrt{f(t)})$ for some squarefree polynomial f of odd degree.

Remark

Note that quadratic extensions of $\mathbb{F}_q(t)$ correspond to double covers of $\mathbb{P}^1_{\mathbb{F}_q}$, i.e. hyperelliptic curves. By the hyperelliptic Riemann-Hurwitz formula, such a double cover has branch degree $2g+2$, where g is the genus of the curve. For an imaginary hyperelliptic curve with function field $L = \mathbb{F}_q(t)(\sqrt{f(t)})$ with $f(t)$ a polynomial of odd degree n, we have that $n+1 = 2g+2$, so $g = \frac{n-1}{2}$.

Ellenberg, Venkatesh, and Westerland proved the following Cohen-Lenstra result:

Theorem

Let $\ell > 2$ be prime and A a nontrivial finite abelian ℓ-group. Write $\delta^+(q)$(resp. $\delta^-(q)$) for the upper density (resp. lower density) of imaginary quadratic extensions of $\mathbb{F}_q(t)$ for which the ℓ-part of the class group is isomorphic to A.

Then $\delta^+(q)$ and $\delta^-(q)$ converge, as $q \to \infty$ with $q \neq 1 (\bmod \ell)$, to $\frac{\Pi_{i>1}(1-\ell^{-i})}{|\operatorname{Aut}(A)|}$.

Definition

Fix a prime $\ell > 2$. The upper and lower densities $\delta^+(q)$ and $\delta^-(q)$ (which are really dependent on A as well) are more precisely defined as follows:

- Let $\mathfrak{S}_n$ denote the set of isomorphism classes of imaginary quadratic extensions $L \supset \mathbb{F}_q(t)$ of discriminant degree $n+1$[7] (where n is odd).
- Let $\iota : \mathfrak{S}_n \to \{0,1\}$ be given by

$$\iota(L) = \begin{cases} 1 & \text{if } \operatorname{Cl}(\mathcal{O}_L)_\ell \cong A \\ 0 & \text{otherwise} \end{cases}$$

- Define

$$\delta^+(q) := \limsup_{n\to\infty} \frac{\sum_{L\in\mathfrak{S}_n} \iota(L)}{|\mathfrak{S}_n|} \quad \text{and} \quad \delta^-(q) := \liminf_{n\to\infty} \frac{\sum_{L\in\mathfrak{S}_n} \iota(L)}{|\mathfrak{S}_n|}$$

Intuitively, the theorem says that the proportion of imaginary quadratic extensions L of $\mathbb{F}_q(t)$ such that $(\operatorname{Cl}\mathcal{O}_L)_\ell \cong A$ is proportional to $\frac{1}{|\operatorname{Aut}(A)|}$ (the factor of $\prod_{i>1}(1-\ell^{-i})$ is present so that the the sum of these proportions over all (isomorphism classes of) finite abelian ℓ-groups is 1).

Reducing this Cohen-Lenstra problem into a problem of bounding rational points in a Hurwitz scheme

Let $\mathcal{L}$ denote the set of isomorphism classes of finite abelian ℓ-groups. Let μ denote the **Cohen-Lenstra distribution**, i.e. the probability distribution on $\mathcal{L}$ sending A to $\prod_{i\geq 1}(1-\ell^{-i})|\operatorname{Aut}(A)|^{-1}$. In other words, the theorem states that, for a nontrivial finite abelian ℓ-group A, the proportion of imaginary quadratic extensions of $\mathbb{F}_q(t)$ whose class groups have ℓ-part isomorphic to A is given by $\mu(A)$.

[Ellenberg, Venkatesh, and Westerland, Lemma 8.2, Proposition 8.3, Lemma 8.4] show that μ is roughly characterized as the probability distribution on $\mathcal{L}$ such that, for any fixed $A \in \mathcal{L}$, the expected value of the counting function $\mathcal{L} \to \mathbb{N}, \quad A' \mapsto \#\operatorname{Sur}(A', A)$ is (close to) 1.

Using such ideas, they show that it suffices to show that the fraction $\frac{\sum_{L\in\mathfrak{S}_n}\#\operatorname{Sur}(\mathcal{O}_L,A)}{|\mathfrak{S}_n|}$ is close to 1[8].

To finally reduce the Cohen-Lenstra problem to a point-bounding problem, we correspond the points of a Hurwitz scheme to the sum $\sum_{L \in \mathfrak{S}_n} \# \mathrm{Sur}(\mathcal{O}_L, A)$:

Proposition

Let $\mathbb{F}_q$ be a finite field , let $\ell \nmid q$ be an odd prime. Fix A to be a nontrivial finite abelian ℓ-group. Let $G = A \rtimes (\mathbb{Z}/2\mathbb{Z})$, where $\mathbb{Z}/2\mathbb{Z}$ acts on A by inversion. Let c be the conjugacy class in G consisting of all involutions. Let n be an odd integer.

Consider the scheme $\mathsf{Hn}^c_{G,n}$ as a scheme over $\mathbb{F}_q$.

There is a bijection between $\mathsf{Hn}^c_{G,n}(\mathbb{F}_q)$ and the set of isomorphism classes of pairs (L, α), where

- L is an imaginary quadratic extension of $\mathbb{F}_q(t)$ of discriminant degree $n+1$[7-1] and
- α is a surjective homomorphism $\alpha : \mathrm{Cl}\, \mathcal{O}_L \to A$.

Two pairs (L, α) and (L', α') are isomorphic if there exists an isomorphism $f : L \to L'$ over $\mathbb{F}_q(t)$ such that $f^* \alpha' = \alpha$.

This proposition then implies that

$$\sum_{L \in \mathfrak{S}_n} \# \mathrm{Sur}(\mathcal{O}_L, A) = 2 |\mathsf{Hn}^c_{G,n}(\mathbb{F}_q)|.$$

One can also count $\# \mathfrak{S}_n$ as $2(q^n - q^{n-1})$[9]. Showing the theorem then reduces to showing that $\frac{\# \mathsf{Hn}^c_{G,n}(\mathbb{F}_q)}{q^n}$ is close to 1.

Remark

We explain why the points of $\mathsf{Hn}^c_{G,n}(\mathbb{F}_q)$ should represent *imaginary* quadratic extensions as opposed to *imaginary or nonimaginary* quadratic extensions.

Recall that $\mathsf{Hn}^c_{G,n}$ is the Hurwitz scheme parameterizing tame G-covers of $\mathbb{P}^1$ whose branch loci over $\mathbb{A}^1$ are of degree n and whose monodromy is of type c.
Since $G = A \rtimes \mathbb{Z}/2\mathbb{Z}$, such a cover factors as $C \to H \to \mathbb{P}^1$ where $H \to \mathbb{P}^1$ is a hyperelliptic cover and $C \to H$ is the quotient map $C \to C/A$, which must be unramified everywhere. Thus, the ramification of $C \to \mathbb{P}^1$ must entirely come from $H \to \mathbb{P}^1$. Moreover, since n is odd and since the hyperelliptic cover $C \to \mathbb{P}^1$ must have a branch locus of even degree, there must in fact be ramification over ∞ and hence $C \to \mathbb{P}^1$ must be imaginary.

Remark

Furthermore, the correspondence requires surjective homomorphisms $\alpha : \mathrm{Cl}\, \mathcal{O}_L \to A$ along with extensions L due to class field theory - the specific map α corresponds to the etale cover $C \to C/A$ by class field theory.

Remark

#_meta/TODO explain why monodromy is c.

Remark

If A is nontrivial, then G is center free. A consequence of this is that $\mathsf{Hn}^c_{G,n}$ is a fine moduli scheme, cf. the exposition on Hurwitz spaces earlier.

Remark

As remarked above, $\mathsf{Hn}^c_{G,n}$ can be constructed over $\mathbb{F}_q$ because c is an $\mathbb{F}_q$-rational conjugacy class of G.

Ellenberg-Li-Shusterman's result on the proportion of hyperelliptic zeta functions that vanish at a fixed number

Ellenberg, Li, and Shusterman significantly used the machinery of Ellenberg-Venkatesh-Westerland to prove that the proportion of hyperellitpic curves over finite fields of a fixed characteristic that vanish at a fixed number is 0:

Theorem

Fix a prime p, and a number $s = \frac{1}{2} + it$ for a fixed real number t. For a power $q = p^k$, define

$$h_{q,s} := \sup_g \frac{\left|\{C \in \mathcal{H}_g(\mathbb{F}_q) : \zeta_C(s) = 0\}\right|}{\left|\mathcal{H}_g(\mathbb{F}_q)\right|}$$

where $\mathcal{H}_g(\mathbb{F}_q)$ is the family of genus g hyperelliptic curves over $\mathbb{F}_q$ and where ζ_C is the zeta function of the hyperelliptic curve $C \in \mathcal{H}_g(\mathbb{F}_q)$. Then

$$h^{p^k,s} \ll p^{-k/276}$$

as $k \to \infty$. In particular, $h_{p^k,s} \to 0$ as $k \to \infty$.

Reducing vanishing of the zeta function of a hyperelliptic curve to rational points on Hurwitz schemes

Let $Q_{n,q}$ denote the set of squarefree polynomials over $\mathbb{F}_q$ of degree n. Let J_f be the Jacobian of the hyperelliptic curve $y^2 = f(x)$ where $f \in Q_{n,q}$. Let $P_f(x) \in \mathbb{Z}[x]$[10] denote the (reverse) characteristic polynomial of (geometric) Frobenius (acting on ℓ-adic Tate modules). A consequence of the Weil conjectures is that

$$Z_{C_f}(T) = \frac{P_f(T)}{(1-T)(1-qT)}$$

where $Z_{C_f}(T)$ is such that $\zeta_{C_f}(s) = Z_{C_f}(q^{-s})$, so the vanishing of $\zeta_{C_f}(s)$ is equivalent to the vanishing of $P_f(q^{-s})$.

For a q-Weil number α of weight 1 (i.e. an algebraic integer whose absolute values under all complex embeddings equal $\sqrt{q}$) let $g_\alpha(x)$ be its minimal polynomial. Let $Q_{n,q}^{\alpha}$ be the subset of $Q_{n,q}$ defined by $\{f \in Q_{n,q} : P_f(\alpha^{-1}) = 0\}$. We want to bound the ratio $\frac{|Q_{n,q}^{\alpha}|}{|Q_{n,q}|}$.

With $s = \frac{1}{2} + it$ fixed (so $\alpha = q^{-s}$), use Chebotarev's density theorem (for sufficiently large k) to find a prime

$$\ell < \frac{1}{4}\left(\frac{q}{4}\right)^{1/276}$$

modulo which g_{p^s} splits completely. In particular, pick $a \in \mathbb{Z}/\ell\mathbb{Z}^{\times}$ so that $g_{p^s}(a) \equiv 0 \pmod{\ell}$[11].

If $P_f(q^{-s}) = 0$, then $P_f(p^{-sk}) = 0$, so $g_{p^{-s}}(x)$ must divide $P_f(x^{-k})$ or equivalently divide $P_f^{\text{rev}}(x^k)$ where $P_f^{\text{rev}}(x^k)$ is the reverse polynomial of P_f, i.e. the characteristic polynomial of Frob_q. Reducing mod ℓ, we had $g_{p^{-s}}(a) \equiv 0 \pmod{\ell}$, so $P_f^{\text{rev}}(a^k) \equiv 0 \pmod{\ell}$. This means that $J_f[\ell](\overline{\mathbb{F}}_q)$ has nonzero elements of eigenvalue a^k.

For $a \in \mathbb{Z}/\ell\mathbb{Z}^{\times}$, let $Q_{n,q}^{a,\ell}$ be the set of $f \in Q_{n,q}$ such that there are nonzero elements $R \in J_f[\ell](\overline{\mathbb{F}}_q)$ with

$$\mathrm{Frob}_q R = aR$$

where $a \in \mathbb{Z}/\ell\mathbb{Z}^{\times}$. With this notation, we have shown above that $|Q_{n,q}^{q^s}| \leq |Q_{n,q}^{a^k,\ell}|$, so it suffices to bound the ratio $\frac{|Q_{n,q}^{a^k,\ell}|}{|Q_{n,q}|}$.

Now the a-eigenspace of Frob_q on $J_f[\ell](\overline{\mathbb{F}}_q)$ is nontrivial (i.e. $f \in Q_{n,q}$ is in $Q_{n,q}^{a,\ell}$) exactly if the dual space of maps $s : J_f[\ell](\overline{\mathbb{F}}_q) \to \mathbb{Z}/\ell\mathbb{Z}$ in the a-eigenspace of $\mathrm{Frob}_q^{\vee}$ is nontrivial. In turn, this is equivalent to the existence of surjections $s : J_f[\ell](\overline{\mathbb{F}}_q) \twoheadrightarrow \mathbb{Z}/\ell\mathbb{Z}$ such that $\mathrm{Frob}_q^{\vee} s = as$.

We previously established that $\mathsf{Hn}_{G,n}^{c}(\mathbb{F}_q)$ corresponds to a set of isomorphism classes of imaginary quadratic extensions L of $\mathbb{F}_q(t)$ and surjections $\mathrm{Cl}\,\mathcal{O}_L \to A$. Similarly, the set of surjections $s : \mathrm{Jac}(C)[\ell] \to (\mathbb{Z}/\ell\mathbb{Z})$ is naturally identified with the set of étale $(\mathbb{Z}/\ell\mathbb{Z})$ covers of C, which are tame G-covers of $\mathbb{P}^1$ where $G = \mathbb{Z}/\ell\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, and such covers are points of a Hurwitz scheme. Informally, a surjection s fixed by Frob_q should correspond to an $\mathbb{F}_q$-rational point of the Hurwitz scheme, and more generally, a surjection s with eigenvalue a should correspond to an $\mathbb{F}_q$-rational point of the "a-twist of the Hurwitz scheme". Ellenberg-Li-Shusterman then showed that number of $\mathbb{F}_q$-rational points of this twist is asymptotically close to q^n, just as for $\mathsf{Hn}_{G,n}^{c}$.

Notations used

- Conf_n denotes the configuration space of n (unordered, distinct) points of D.
- Conf_n denotes the configuration space of degree n squarefree divisors of $\mathbb{A}^1$. It is a scheme over $\mathbb{Z}$.
- Conf'_{n+1} denotes the configuration space of degree $n+1$ squarefree divisors of $\mathbb{P}^1$. It is a scheme over $\mathbb{Z}$. Its points $[a_0 : \cdots : a_{n+1}]$ can be regarded as degree $n+1$ binary forms/homogeneous polynomials/divisors $a_0X^n + a_1X^{n-1}W + \cdots a_{n+1}W^{n+1}$

- D denotes a closed disc in $\mathbb{C}$ with a marked point $*$ in the boundary.
- $\delta^+(q)$ denotes the upper density of imaginary quadratic extensions of $\mathbb{F}_q(t)$ whose class groups have ℓ-part isomorphic to a fixed abelian ℓ-group A.
- $\delta^-(q)$ denotes the lower density of imaginary quadratic extensions of $\mathbb{F}_q(t)$ whose class groups have ℓ-part isomorphic to a fixed abelian ℓ-group A.
- G denotes a finite group.
- g_α denotes the minimal polynomial of the q-Weil number α of weight 1.
- $H_{G,n}$ denotes the coarse moduli scheme for the functor of tame G-covers of $\mathbb{P}^1$ with branch locus of degree n in $\mathbb{P}^1$. If G is center free, then $\mathsf{H}_{G,n}$ is in fact a fine moduli scheme.
- $\mathsf{Hn}_{G,n}$ denotes the (coarse moduli) Hurwitz scheme parameterizing tame G-covers of $\mathbb{P}^1$ whose branch loci over $\mathbb{A}^1$ are of degree n.
- $\mathsf{Hn}^c_{G,n}$ denotes the (coarse moduli) Hurwitz scheme parameterizing tame G-covers of $\mathbb{P}^1$ whose branch loci over $\mathbb{A}^1$ are of degree n and whose monodromy is of type c, where c is a rational union of conjugacy classes in G, or, more generally if working over $\mathbb{F}_q$, where c is an $\mathbb{F}_q$-rational union of conjugacy classes in G.
- $h_{q,s}$ denotes

$$h_{q,s} := \sup_g \frac{\left|\{C \in \mathcal{H}_g(\mathbb{F}_q) : \zeta_C(s) = 0\}\right|}{\left|\mathcal{H}_g(\mathbb{F}_q)\right|}.$$

- J_f denotes the Jacobian of the hyperelliptic curve $y^2 = f(x)$ where $f \in Q_{n,q}$.
- $\mathcal{L}$ denotes the set of isomorphism classes of finite abelian ℓ-groups.
- μ denotes the Cohen-Lenstra distribution, i.e. the probability distribution on $\mathcal{L}$ sending A to $\prod_{i\geq 1}(1-\ell^{-i})|\operatorname{Aut}(A)|^{-1}$.
- $Q_{n,q}$ denotes the set of squarefree polynomials over $\mathbb{F}_q$ of degree n.
- $Q^\alpha_{n,q}$ denotes $\{f \in Q_{n,,q} : P_f(\alpha^{-1}) = 0\}$ where α is a q-Weil number of weight 1.
- $Q^{a,\ell}_{n,q}$ denotes the set of $f \in Q_{n,q}$ such that there are nonzero elements $R \in J_f[\ell](\overline{\mathbb{F}_q})$ with $\operatorname{Frob}_q R = aR$ where $a \in \mathbb{Z}/\ell\mathbb{Z}^\times$ and ℓ is a prime not dividing q.
- $\mathfrak{S}_n$ denotes the set of isomorphism classes of imaginary quadratic extensions $L \supset \mathbb{F}_q(t)$ of discriminant degree n where n is odd.
- ζ_C denotes the zeta function of the curve $C/\mathbb{F}_q$.

See Also

Meta

References

Citations and Footnotes

---

1. We can alternatively construct Conf_n as the open subscheme of Conf'_n via the embedding map $[a_0 = 0 : a_1 \cdots : a_n] \mapsto [a_1 : \cdots : a_n]$.↩

2. To see this, note that a point $[a_0 : \cdots : a_{n+1}]$ is a point of Conf_n if and only if $a_0 \neq 0$, i.e. the corresponding divisor $a_1 X^n W + \cdots + a_{n+1} W^{n+1}$ contains/vanishes at $\infty = [X = 1 : W = 0]$. Furthermore, squarefree divisors of $\mathbb{A}^1$ of degree n bijectively correspond to squarefree divisors of $\mathbb{P}^1$ of degree $n+1$ containing ∞.↩

3. Romagny and Wewers denote this scheme as $\mathcal{H} = \mathcal{H}_{n,G,\mathbb{Z}}$.↩

4. Ellenberg, Venkatesh, and Westerland, only require $H_{G,n}$ as a scheme over $\mathbb{Z}[1/|G|]$.↩

5. i.e. the deck transformation group acts transitively on fibers↩

6. Monodromy refers to the monodromy action - the action of $\pi = \pi_1(\Sigma, *)$ on the fiber of the base point under the covering map $Y \to \Sigma$. Since the covering is regular, $\pi_1(\Sigma, *)$ surjects onto the automorphism group of this covering; the monodromy by γ_i is the image of γ_i under this surjection.↩

7. The discriminant degree should refer to the branch locus degree of the double cover $C \to \mathbb{P}^1_{\mathbb{F}_q}$ corresponding to $L/\mathbb{F}_q(t)$. In this case, the double cover should be branched at ∞ and have n additional branches (for a total of $n+1$ branches).↩↩

8. In fact, they show that there exists a constant $B(A)$ such that

$$\left| \frac{\sum_{L \in \mathfrak{S}_n} m_A(L)}{|\mathfrak{S}_n|} - 1 \right| \leq B(A)/\sqrt{q}$$

for all n, q with $\sqrt{q} > B(A)$ and n an odd integer greater than $B(A)$.↩

9. This is true because the number of squarefree polynomials of degree n over $\mathbb{F}_q$ is $q^n - q^{n-1}$ and because fields $\mathbb{F}_q(t)(\sqrt{f_1(t)})$ and $\mathbb{F}_q(t)(\sqrt{f_2(t)})$ with the same branch loci are isomorphic if and only if $f_1(t)$ and $f_2(t)$ are scalar multiples by an element of $(\mathbb{F}_q^\times)^2$.↩

10. $P_f(x)$ should coincide with the L-polynomial. In particular, both have zeroes of norm $q^{-1/2}$ and are *not* a monic polynomial but rather the reverse of a monic polynomial. ↩

11. There must be at least one zero of g_{p^s} mod ℓ in $\mathbb{Z}/\ell\mathbb{Z}^\times$ because if all zeroes of g_{p^s} were to reduce to 0 mod ℓ, then a power of q would have to be divisible by ℓ, which cannot happen.↩