Counting extensions of function fields with bounded discriminant and specified Galois group

Jordan S. Ellenberg and Akshay Venkatesh*

2 Jul 2004

Abstract

We discuss the enumeration of function fields and number fields by discriminant. We show that Malle's conjectures agree with heuristics arising naturally from geometric computations on Hurwitz schemes. These heuristics also suggest further questions in the number field setting.

1 Introduction

The enumeration of number fields subject to various local and global conditions is an old problem, which has in recent years been the subject of renewed interest (a sampling includes [2], [3], [5], [7], [10], [12].) For a good survey of recent work, see [1]. We begin by reprising some important conjectures.

If L/K is an extension of number fields, we denote by $\mathcal{D}_{L/K}$ the relative discriminant, an ideal of K, and by $\mathbf{N}_{\mathbb{Q}}^{K}\mathcal{D}_{L/K}$ its norm, a positive integer. For $X \in \mathbb{R}^{+}$, we set $N_{K,n}(X)$ to be the number of degree-n extensions L/K (up to K-isomorphism) such that $\mathbf{N}_{\mathbb{Q}}^{K}\mathcal{D}_{L/K} < X$. It is a classical problem to understand the asymptotics of $N_{K,n}(X)$ as X goes to infinity; in particular, we have the folk conjecture:

Conjecture 1.1. There is a constant $c_{K,n}$ such that, as $X \to \infty$,

$$N_{K,n}(X) \sim c_{K,n}X.$$

This conjecture is now known for $n \leq 5$.

A more general conjecture applies to enumerating extensions with specified Galois group. It is due to Malle [13] and refines a previous conjecture of Cohen. To describe Malle's conjecture, we need to introduce some notation.

Let $G \leq S_n$ be a transitive subgroup. For $g \in G$, we set $\mathrm{ind}(g) = n - r$, where r is the number of orbits of g on $\{1, 2, \ldots, n\}$. Denote by $\mathscr{C}$ the set of non-trivial conjugacy classes of G; then ind descends to a function $\mathrm{ind} : \mathscr{C} \to \mathbb{Z}$. The group $\mathrm{Gal}(\bar{K}/K)$ acts on $\mathscr{C}$ via $g \cdot c = c^{\chi(g)}$, where $g \in \mathrm{Gal}(\bar{K}/K), c \in \mathscr{C}$ and $\chi : \mathrm{Gal}(\bar{K}/K) \to \hat{\mathbb{Z}}^{*}$ is the cyclotomic character. Set $a(G) = \max_{c \in \mathscr{C}}(\mathrm{ind}(c)^{-1})$, and set $b_K(G)$ to be the number of $\mathrm{Gal}(\bar{K}/K)$-orbits on the set $\{c \in \mathscr{C} : \mathrm{ind}(c) = 1/a(G)\}$.

*First author: Department of Mathematics, Princeton University. ellenber@math.princeton.edu Partially supported by NSF Grant DMS-0401616. Second author: Department of Mathematics, Massachusetts Institute of Technology. akshayv@math.mit.edu Partially supported by NSF Grant DMS-0245606

Let H be any point stabilizer in the G-action on $\{1, 2, \ldots, n\}$. For each Galois extension L/K with Galois group G, let L_0/K be the degree n subextension of L/K corresponding to the subgroup $H \leq G$. Since G acts transitively on $\{1, 2, \ldots, n\}$, the K-isomorphism class of L_0 is independent of the choice of H. We then denote by $N_{K,G}(X)$ the number of Galois G-extensions L/K such that $\mathbf{N}_{\mathbb{Q}}^{K}\mathcal{D}_{L_0/K} < X$.

Conjecture 1.2. (Malle) There is a nonzero constant $C_K(G)$ such that

$$N_{K,G}(X) \sim C_K(G)X^{a(G)}(\log X)^{b_K(G)-1}.$$

This conjecture is known to be correct in certain special cases, including that where $G = S_3$ or D_4 (embedded in S_3 and S_4 respectively) and that where G is abelian. In general, however, little is known about Malle's conjecture – and indeed, its difficulty is ensured by the fact that implies a positive solution to the inverse Galois problem.

A related problem, raised for example in [9], is the question of multiplicity of a fixed discriminant.

Conjecture 1.3. The number of number fields $K/\mathbb{Q}$ with degree n and discriminant D is $\ll_{\epsilon,n} D^{\epsilon}$.

Conjecture (1.3) is unknown, and seems quite difficult, even for $n = 3$. In that case it is intimately related to questions about 3-torsion in class groups of quadratic fields.

The arithmetic of function fields and their covers is often much more approachable than that of number fields, since one can appeal to the geometry of varieties over finite fields. In particular, one may replace K by $\mathbb{F}_q(t)$ in the above discussion, and ask whether Conjecture 1.1 and 1.2 remain true (with evident modifications) in this setting. We note that this is known to be the case when $G = S_3$, by the work of Datskovsky and Wright [7]

We do not know how to prove Conjecture 1.2 even in the function field setting. However, we will establish in the present paper certain (weak) approximations to Conjecture 1.2. In Lemma 2.4 we show that the upper bound of Malle's conjecture is nearly valid when q is large relative to $|G|$. Moreover, we prove in Proposition 3.1 a result showing that Malle's conjecture is compatible with a heuristic arising from the geometry of Hurwitz spaces. A little more precisely, Prop. 3.1 studies Malle's conjecture using the following heuristic:

> **(A)** If X is a geometrically irreducible d-dimensional variety over $\mathbb{F}_q$, one has $|X(\mathbb{F}_q)| = q^d$.

The heuristic **(A)** can be thought of as an assertion of extremely (indeed, implausibly) strong cancellation between Frobenius eigenvalues on the cohomology of X. Despite its crudeness, **(A)** allows one to recover, in the function field setting, the precise constants $a(G)$ and $b_K(G)$ found in Malle's conjecture.

This line of reasoning suggests further questions about the distribution of discriminants of number fields. We discuss these in Section 4. For instance, Section 4.2 gives a heuristic for the number of icosahedral number forms of conductor $\leq N$, and Section 4.3 proposes some still more general heuristics for number fields with prescribed ramification data.

We note that the approach via **(A)** is very much in the spirit of that used by Batyrev in developing precise heuristics for the distribution of rational points on Fano varieties; we thank Yuri Tschinkel for explaining this to us.

The authors thank Karim Belabas, Manjul Bhargava, Henri Cohen, and Johan de Jong for many useful conversations about the topic of this chapter, and the organizers of the Miami Winter School in Geometric Methods in Algebra and Number Theory for inviting the first author to give the lecture on which this article is based.

Notation: Throughout this paper, G will be a transitive subgroup of the permutation group S_n and q will be a prime power that is coprime to $|G|$.

2 Counting extensions of function fields

2.1 Hurwitz spaces

In this section, we recall basic facts about Hurwitz spaces, i.e. moduli spaces for covers of $\mathbb{P}^1$. We will make constant use of the fact that the category of finite extensions $L/\mathbb{F}_q(t)$, with the morphisms being field homomorphisms fixing $\mathbb{F}_q(t)$, is equivalent to the category of finite (branched) covers of smooth curves $f : Y \to \mathbb{P}^1$ defined over $\mathbb{F}_q$, the morphisms being maps of covers over $\mathbb{P}^1$. Recall that q is coprime to $|G|$, eliminating painful complications concering the residue characteristic.

Let Y be a geometrically connected curve over $\mathbb{F}_q$ and $f : Y \to \mathbb{P}^1$ a Galois covering equipped with an isomorphism $G \to \mathrm{Aut}(Y/\mathbb{P}^1)$. We refer to such a pair (Y, f) as a *G-cover.* Let H be a point stabilizer in the G-action on $\{1, 2, \dots, n\}$, and let $f_0 : Y_0 \to \mathbb{P}^1$ be the degree-n covering corresponding to the subgroup $H \leq G$. We then set $r(f)$ to be the degree of the ramification divisor of f_0. Call $q^{r(f)}$ the discriminant of f.

We denote by $N_{q,G}(X)$ the number of isomorphism classes of G-covers $f : Y \to \mathbb{P}^1/\mathbb{F}_q$ with $q^{r(f)} < X$. Note that, by requiring that Y be geometrically connected, we have excused ourselves from counting extensions of $\mathbb{F}_q(t)$ which contain some $\mathbb{F}_{q^f}/\mathbb{F}_q$ as a subextension. This decision will not affect the powers of X and $\log X$ in the heuristics we compute, though it may change the constant terms.

The G-covers $\mathbb{P}^1$ with discriminant q^r are parametrized by a Hurwitz variety $\mathcal{H}_r$. More precisely:

Proposition 2.1. *There is a smooth scheme $\mathcal{H}_r$ over $\mathbb{Z}[\frac{1}{|G|}]$ which is a coarse moduli space for G-covers of $\mathbb{P}^1$ with discriminant r. The natural map*

$$\{\textit{isomorphism classes of } G\textit{-covers of } \mathbb{P}^1/\mathbb{F}_q\} \to \mathcal{H}(\mathbb{F}_q) \tag{2.1}$$

is surjective, and the fibers have size at most $|Z|$, where Z is the center of G.

Proof. We refer to [16] for details of the construction of $\mathcal{H}_r$ in positive characteristic. Let h be an $\mathbb{F}_q$-rational point of $\mathcal{H}$. Then the obstruction to h arising from a cover $Y \to \mathbb{P}^1$ defined over $\mathbb{F}_q$ lies in $H^2(\mathbb{F}_q, Z)$ where Z is the center of G; since $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ has cohomological dimension 1, this obtruction is trivial (see [8, Cor. 3.3] for more discussion of this point.) Further, the isomorphism classes of covers f parametrized by the point h are indexed by the cohomology group $H^1(\mathbb{F}_q, Z)$, which has size at most $|Z|$. □

What's more, $\mathcal{H}_r$ is the union of open and closed subschemes which parametrize G-covers with specified ramification data. In order to express this decomposition, we need a bit more notation.

We call a multiset $\underline{c} = \{c_1, \dots, c_k\}$ of conjugacy classes of G a *Nielsen class*, and denote by $r(\underline{c})$ the total index $\sum_{i=1}^k \mathrm{ind}(c_i)$. We also write $|\underline{c}|$ for the number of branch points k. Finally, for each Nielsen class $\underline{c}$ we define $\tilde{\Sigma}_{\underline{c}}$ to be the subset of G^k consisting of all k-tuples $(g_1, \dots, g_k)$ such that

- The multisets $\underline{c}$ and $\{c(g_i), \dots, c(g_k)\}$ are equal, where $c(g)$ denotes the conjugacy class of g;
- $g_1 g_2 \dots g_k = 1$;
- the g_i generate G.

Note that $\tilde{\Sigma}_{\underline{c}}$ is preserved by the action of G sending $(g_1, \dots, g_k)$ to $(gg_1g^{-1}, \dots, gg_kg^{-1})$. We denote by $\Sigma_{\underline{c}}$ the quotient of $\tilde{\Sigma}_{\underline{c}}$ by this action.

Let $f : Y \to \mathbb{P}^1_{\bar{\mathbb{F}}_q}$ be a G-cover whose branch locus in $\mathbb{P}^1(\bar{\mathbb{F}}_q)$ is $\{x_1, \dots, x_k\}$. By consideration of the action of tame inertia at $x_1, \dots, x_k$, we can associate a Nielsen class $\underline{c}$ to f which is fixed

by $\mathrm{Gal}(\bar{K}/K)$ and which satisfies $r(\underline{c}) = r(f)$. [4, 1.2.4]. The set of Nielsen classes inherits a $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-action from the cyclotomic action on $\mathscr{C}$, as described in section 1; we call a Nielsen class which is fixed by this action an *$\mathbb{F}_q$-rational Nielsen class.* If f descends to a G-cover $Y \to \mathbb{P}^1_{\mathbb{F}_q}$, it follows that the Nielsen class $\underline{c}$ is $\mathbb{F}_q$-rational.

Denote by C_k the configuration space of k disjoint points in $\mathbb{P}^1$. The (geometric) fundamental group of C_k is the (spherical) braid group of k-strands. We denote by $\sigma_k \in C_k$ the braid that pulls strand i past strand $i+1$.

Proposition 2.2. *For each Nielsen class $\underline{c}$, there is a Hurwitz space $\mathcal{H}_{\underline{c}}/\bar{\mathbb{F}}_q$ which is a coarse moduli space for G-covers $f : Y \to \mathbb{P}^1_{\bar{\mathbb{F}}_q}$ with Nielsen class $\underline{c}$. The action of $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ sends $\mathcal{H}_{\underline{c}}$ to $\mathcal{H}_{\underline{c}^\sigma}$; so the $\mathbb{F}_q$-rational connected components of $\mathcal{H}_r$ are each contained in $\mathcal{H}_{\underline{c}}$ for some $\mathbb{F}_q$-rational $\underline{c}$ with $r(\underline{c}) = r$.*

The map $\pi : \mathcal{H}_{\underline{c}} \to C_{|\underline{c}|}$ that sends a cover f to its ramification divisor is étale. Moreover, the geometric points of the fiber of π above $\{x_1, \dots, x_k\} \in C_k$ are naturally identified with $\Sigma_{\underline{c}}$. The action of $\pi_1(C_k)$ on $\pi^{-1}(\{x_1, \dots, x_k\})$ is given by

$$\sigma_i(g_1, \dots, g_k) = (g_1, \dots, g_i g_{i+1} g_i^{-1}, g_i, \dots, g_k)$$

so that the connected components of $\mathcal{H}_{\underline{c}}$ are in bijection with the $\pi_1(C_k)$-orbits on $\Sigma_{\underline{c}}$.

Proof. For the existence of $\mathcal{H}_{\underline{c}}$, see [4, §1.2.4]. The description of the connected components of $\mathcal{H}_{\underline{c}}$ is due to Fried; see e.g [11, §1.3], and [16, Cor 4.2.3] for the extension of Fried's results to positive characteristic prime to $|G|$. □

2.2 An upper bound on the number of extensions of $\mathbb{F}_q(t)$

Proposition 2.1 shows that, up to a constant factor, one can reduce the problem of controlling $N_{\mathbb{F}_q(t),G}(X)$ to the problem of controlling the number of $\mathbb{F}_q$-rational points on the varieties $\mathcal{H}_r$, as r ranges up to $\log_q X$. Bounding the number of $\mathbb{F}_q$-points on a variety of high dimension over a small finite field is a difficult matter. In the context at hand, we may give a straightforward upper bound, but the exponent is far from the one appearing in Malle's conjecture. We carry this out below; to clarify matters, we fix q and G and consider only the dependence as $X \to \infty$.

We will use the following easy lemma to bound various sequences arising in this paper.

Lemma 2.3. *Suppose $\{a_n\}$ is a sequence of real numbers with $a_n = 0$ whenever n is not a power of q, and suppose*

$$\sum_{r=1}^{\infty} a_{q^r} q^{-rs},$$

considered as a formal power series, is a rational function $f(t)$ of $t = q^s$. Let a be a positive real number. If $f(t)$ has no poles with $|t| \geq q^a$, then:

$$\sum_{n=1}^{X} a_n \ll X^a.$$

If $f(t)$ has a pole of order b at $t = q^a$ and no other poles with $|t| \geq q^a$, then:

$$\sum_{n=1}^{X} a_n \asymp X^a (\log X)^{b-1}$$

Here we use the notation $A(X) \asymp B(X)$ to mean that there are real constants $C_1, C_2 > 0$ such that $C_1 A(X) \le B(X) \le C_2 A(X)$.

Proof. It follows immediately from the decomposition of $f(t)$ in partial fractions that

$$\sum_{r=1}^{R} a_{q^r} \ll q^{aR}$$

when $f(t)$ has no poles with $|t| > q^a$. Moreover, if $f(t)$ has a pole of order b at $t = q^a$ and no other poles with $|t| \ge q^a$, then

$$\sum_{r=1}^{R} a_{q^r} \sim C q^{aR} R^{b-1}$$

for some $C \in \mathbb{R}$. Then the Lemma follows, since $q^{\lfloor \log_q X \rfloor} \asymp X$. □

Lemma 2.4. *Let q and G be fixed. Denote by $E(j)$ the number of elements g of G with $\mathrm{ind}(g) = j$, and set $e(G) = \sup_j E(j)^{1/j}$. Then*

$$\limsup_{X \to \infty} \frac{\log N_{q,G}(X)}{\log X} \le a(G) + \frac{\log(2e(G))}{\log q}$$

In particular

$$\limsup_{X \to \infty} \frac{\log N_{q,S_n}(X)}{\log X} \le 1 + \frac{\log(4n^2)}{\log q}. \tag{2.2}$$

Note that the right-hand-side of the first inequality in Lemma 2.4 approaches Malle's constant $a(G)$ when q becomes large relative to $|G|$.

Proof. Define a sequence of integers a_n such that $a_{q^r} = |\mathcal{H}_r(\mathbb{F}_q)|$ and $a_n = 0$ if n is not a power of q. So

$$N_{q,G}(X) \asymp \sum_{n=1}^{X} a_n.$$

We have seen in Proposition 2.2 that the $\mathbb{F}_q$-rational components of $\mathcal{H}_r$ are the union of Hurwitz varieties $\mathcal{H}_{\underline{c}}/\mathbb{F}_q$. Since $\mathcal{H}_{\underline{c}}$ is a finite cover of degree $|\Sigma_{\underline{c}}|$ of $C_{|\underline{c}|} \cong \mathbb{P}^{|\underline{c}|}/\mathbb{F}_q$, we have

$$|\mathcal{H}_{\underline{c}}(\mathbb{F}_q)| \ll_{q,G} |\Sigma_{\underline{c}}| q^{|\underline{c}|}$$

and

$$a_{q^r} \ll_{q,G} \sum_{\underline{c}: r(\underline{c}) = r} |\Sigma_{\underline{c}}| q^{|\underline{c}|}.$$

Let $f(r)$ the sum of q^k over all k-tuples $(g_1, \ldots, g_k)$ in G satisfying $\sum_i \mathrm{ind}(g_i) = r$. (Here, k is allowed to vary.) Then evidently

$$\sum_{\underline{c}: r(\underline{c}) = r} |\Sigma_{\underline{c}}| q^{|\underline{c}|} \le f(r).$$

On the other hand,

$$\sum_r f(r) q^{-rs} = (1 - \sum_{g \in G} (q^{1 - \mathrm{ind}(g) s}))^{-1}.$$

We conclude that

$$\sum_r a_{q^r} q^{-rs} \ll_{q,G} (1 - \sum_{g \in G} (q^{1-\mathrm{ind}(g)s}))^{-1} = (1 - \sum_{j \geq a(G)^{-1}} E(j) q^{1-js})^{-1} \tag{2.3}$$

It is easy to see that (2.3) has no poles once we have

$$|q^s| > 2q^{a(G)} E(j)^{1/j}$$

for every j. The first part of the proposition now follows from Lemma 2.3.

We now show that, when $G = S_n$, we have $E(j)^{1/j} < 2n^2$ for all j; this proves the second part of the lemma.

Any $\sigma \in S_n$ with $\mathrm{ind}(\sigma) = j$ fixes at least $n - 2j$ elements of $\{1, 2, \ldots, n\}$. Enumerating such σ by their number l of fixed points, we obtain $E(j) \leq \sum_{n-2j \leq l \leq n-1} \frac{n!}{l!} < 2jn^{2j}$. Thus $E(j)^{1/j} < n^2 (2j)^{1/j} \leq 2n^2$. □

Remark 2.5. It is interesting to contrast the "trivial" upper bounds of Lemma 2.4 with what can be obtained in the number field setting.

The upper bounds of Lemma 2.4 used explicit knowledge of the fundamental group of a punctured $\mathbb{P}^1$. In the number field setting, such tools are unavailable. Nevertheless in [10] an upper bound for $N_n(X)$ was derived, similar to (2.2), with the exponent $\log(n)$ is replaced by a quantity of the form $e^{\sqrt{\log(n)}}$. The proof was considerably more complicated, but nevertheless geometric: the key idea is to find in each number field K a small set $\{x_1, x_2, \ldots, x_r\}$ of algebraic integers which are "nondegenerate" in the sense that they do not satisfy an algebraic relation of low degree, and then to show that an appropriate set of traces $\mathrm{Tr}(x_1^{g_1} \ldots x_r^{g_r})$ suffice to determine K.

Further, let $N_{q,n}^{\mathrm{Gal}}(X)$ denote the number of *Galois* extensions of $\mathbb{P}^1_{\mathbb{F}_q}$ of degree n and discriminant less than X. Lemma 2.4 implies that $N_{q,n}^{\mathrm{Gal}}(X) \ll_{q,n} X^{\frac{2}{n} + \frac{\log(2n)}{\log(q)}}$. Again, a result of a similar flavor was shown in [10], where it was shown that $N_{q,n}^{\mathrm{Gal}}(X) \ll X^{3/8}$ if $n \geq 3$. Again, the proof in the number field case was more elaborate and in fact relied on the classification of finite simple groups; the main idea is to prove the theorem using a low-degree permutation representation of G when G is simple, and to proceed by induction on a composition series otherwise.

3 Counting points on Hurwitz spaces under heuristic (A)

Lemma 2.4 asserts, at least, that the upper bound of Malle's conjecture is close to valid when q is large compared to $|G|$. Beyond Lemma 2.4, we can do no more than speculate about the exact number of $\mathbb{F}_q$-points on $\mathcal{H}_r$. The situation improves somewhat if we are willing to assume the heuristic (**A**) from the introduction: that is, we suppose that a geometrically irreducible d-dimensional variety over $\mathbb{F}_q$ has q^d points. This heuristic reduces the problem of estimating $|\mathcal{H}_r(\mathbb{F}_q)|$ to the substantially simpler problem of computing the number of geometric connected components of the spaces $\mathcal{H}_r$ and their fields of definition.

Let $h(q, r)$ be the sum of $q^{\dim C}$ over all geometrically connected components C of $\mathcal{H}_r$ which are defined over $\mathbb{F}_q$. Denote by $b_{\mathbb{F}_q}(G)$ the number of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbits on the set $\{c \in \mathscr{C} : \mathrm{ind}(c) = 1/a(G)\}$.

We shall prove:

Proposition 3.1.

$$\sum_{q^r \leq X} h(q, r) \asymp X^{a(G)} \log(X)^{b_{\mathbb{F}_q}(G) - 1}$$

Proposition 3.1 amounts, roughly speaking, to the assertion that Malle's conjectures are compatible with naive dimension computations for Hurwitz spaces. The proof is more difficult than that of Lemma 2.4 but is still elementary.

The problem here is that the decomposition of $\mathcal{H}_r$ into geometrically connected components is somewhat subtle. Let $h'(q,r)$ be the sum of $q^{|\underline{c}|}$ over all $\mathbb{F}_q$-rational Nielsen classes $\underline{c}$ with $r(\underline{c}) = r$. If $\mathcal{H}_{\underline{c}}$ were a non-empty geometrically connected variety for every $\mathbb{F}_q$-rational Nielsen class $\underline{c}$ with $r(\underline{c}) = r$, we would have $h'(q,r) = h(q,r)$. (We remark that, in many cases, $\mathcal{H}_{\underline{c}}$ is known to be geometrically connected by the theorem of Conway and Parker [11, Appendix].) In the following proposition we show that h' is a reasonable approximation to h, at least on average.

Proposition 3.2. *Under the assumption on q in Proposition 3.1, there exist constants m, C_1, C_2, depending only on G, such that*

$$C_1 \sum_{r<R-m} h'(q,r) < \sum_{r<R} h(q,r) < C_2 \sum_{r<R} h'(q,r) \tag{3.4}$$

for all $R \gg 0$.

Proof. Recall that $\tilde{\Sigma}_{\underline{c}}$ consists of $(g_1, \dots, g_k) \in G^k$ such that the multiset $\{c(g_i), \dots, c(g_k)\}$ equals $\underline{c}$; $g_1, \dots, g_k$ generate G; and $g_1 g_2 \dots g_k = 1$. Write $n(\underline{c})$ for the number of orbits of the braid group $\pi_1(C_{|\underline{c}|})$ on $\tilde{\Sigma}_{\underline{c}}$. The right-hand inequality above thus follows immediately from the following lemma.

Lemma 3.3. *There exists a constant C_2 such that $n(\underline{c}) < C_2$ for all $\underline{c}$.*

Proof. If $\underline{g} = (g_1, \dots, g_k)$ and $\underline{g}' = (g_1', \dots, g_k')$ are two elements of G^k, we write $\underline{g} \sim \underline{g}'$ when $\underline{g}$ and $\underline{g}'$ are in the same orbit of the action of the braid group on G^k. We shall need a simple fact about the action of the braid group on G^k: suppose $\underline{g} = (g_1, \dots, g_k) \in G^k$ with $g_1 \dots g_k = 1$. Then, for any $1 \le j \le k$, there exists $(g_1', \dots, g_{k-1}') \in G^{k-1}$ such that

$$(g_1, \dots, g_k) \sim (g_1', \dots, g_{k-1}', g_j). \tag{3.5}$$

Moreover, one knows (see, e.g., [17, Cor. 9.4]) that

$$(gg_1g^{-1}, gg_2g^{-1}, \dots, gg_kg^{-1}) \sim (g_1, \dots, g_k) \tag{3.6}$$

whenever g belongs to the subgroup generated by $(g_1, \dots, g_k)$.

We show that $n(\underline{c}) \le |G|^{|G|^2}$. This is clear if $|\underline{c}| \le |G|^2$.

Suppose $k = |\underline{c}| > |G|^2$. Then any k-tuple $(g_1, g_2, \dots, g_k)$ in $\tilde{\Sigma}_{\underline{c}}$ contains an element $g_0 \in G$ with multiplicity at least $|G| + 1$. Let g_0' be any element in G conjugate to g_0. Thus, applying the braid operations (3.5) and (3.6) above, we deduce

$$(g_1, g_2, \dots, g_k) \sim (g_1', g_2', \dots, g_{k-|G|-1}', g_0, g_0, \dots, g_0) \sim (g_1'', g_2'', g_{k-|G|-1}'', g_0', g_0', \dots, g_0') \tag{3.7}$$

for certain $g_j', g_j'' \in G$, where both g_0 and g_0' occur $|G| + 1$ times at the end of each expression.

On the other hand $g_0'^{|G|} = 1$. Thus, if $(g_1, g_2, \dots, g_k) \in \Sigma_{\underline{c}}$, then $(g_1'', \dots, g_{k-|G|-1}'', g_0')$ belongs to $\Sigma_{\underline{c}'}$ where $\underline{c}'$ is $\underline{c}$ with $|G|$ copies of the conjugacy class of g_0 removed. So $n(\underline{c}) \le n(\underline{c}')$. If $|\underline{c}'| > |G|^2$ we may apply the procedure that led to (3.7) again; indeed, repeatedly applying (3.7) we can bring elements of $\Sigma_{\underline{c}}$ to a "standard form." We see in particular that $n(\underline{c}) \le n(\underline{c}')$ for some $|\underline{c}'| \le |G|^2$. The result now follows.

□

We now turn to the left-hand inequality in (3.4). Here we will make use of the theorem of Conway and Parker [11, Appendix] in order to show that $\mathcal{H}_{\underline{c}}$ has geometric components defined over $\mathbb{F}_q$ for many choices of $\underline{c}$.

We first show that $\mathcal{H}_{\underline{c}}$ is nonempty for many choices of $\underline{c}$.

Let $N \subset G$ be the normal subgroup consisting of all products $g_1 \dots g_k$, where the Nielsen class of $(g_1, \dots, g_k)$ is $\mathbb{F}_q$-rational. We claim that for every element $g \in N$ there exists, for some k, a k-tuple $(g_1, \dots, g_k)$ such that

- $g_1 \dots g_k = g$;
- the Nielsen class of $(g_1, \dots, g_k)$ is $\mathbb{F}_q$-rational;
- the g_i generate G.

It suffices to show that this assertion holds for $g = 1$; for if we have $(g_1, \dots g_k)$ satisfying the last two conditions and having product 1, we can concatenate it with $(g_{k+1}, \dots, g_\ell)$ having product g and representing an $\mathbb{F}_q$-rational Nielsen class. To see that the assertion holds for $g = 1$, merely choose $(g_1, g_1^{-1}, \dots, g_k, g_k^{-1})$ where $(g_1, \dots, g_k)$ is a generating set for G which represents a $\mathbb{F}_q$-rational Nielsen class.

Now let $\underline{d}_1, \dots, \underline{d}_K$ be a finite set of $\mathbb{F}_q$-rational Nielsen classes such that, for each $g \in N$, there exists $(g_1, \dots, g_k)$ representing some $\underline{d}_i$ which generates G and has product g.

If $\underline{c}$ and $\underline{d}$ are two Nielsen classes, we denote their concatenation by $\underline{c} + \underline{d}$.

For each $\mathbb{F}_q$-rational Nielsen class $\underline{c}$, choose a representative $(g_1, \dots, g_k)$. By the discussion above there exists an m-tuple $(g_1, \dots, g_k, g_{k+1}, \dots, g_m)$ which is contained in $\Sigma_{\underline{c}+\underline{d}_i}$ for some i. It follows that $\mathcal{H}_{\underline{c}+\underline{d}_i}$ is nonempty for some i.

We now need to show that there are many Hurwitz spaces which are not only non-empty but which possess a geometric component defined over $\mathbb{F}_q$. Our main tool is the following assertion, which follows immediately from Proposition 1 and Lemma 2 of [11]:

Lemma 3.4. *There exists a group $\tilde{G}$, a surjective homomorphism $\tilde{G} \to G$, and a constant $C_3(G)$ such that, for any Nielsen class $\underline{\tilde{c}}$ of $\tilde{G}$ which contains at least $C_3(G)$ copies of each nontrivial conjugacy class of $\tilde{G}$, the Hurwitz space $\mathcal{H}_{\underline{\tilde{c}}}$ is geometrically connected.*

By the argument prior to Lemma 3.4, applied to $\tilde{G}$ instead of G, there exists a finite set of $\mathbb{F}_q$-rational Nielsen classes $\underline{\tilde{e}}_1, \dots, \underline{\tilde{e}}_L$ such that, for every $\mathbb{F}_q$-rational Nielsen class $\underline{\tilde{c}}$ of $\tilde{G}$, the Hurwitz scheme $\mathcal{H}_{\underline{\tilde{c}}+\underline{\tilde{e}}_i}$ is nonempty.

Now consider an $\mathbb{F}_q$-rational Nielsen class $\underline{c}$ of G. We want to find an $\mathbb{F}_q$-rational Nielsen class $\underline{\tilde{c}}$ of $\tilde{G}$ which "approximately" projects to $\underline{c}$. For each $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbit $\mathscr{O}$ on the nontrivial conjugacy classes in $\mathscr{C}$, let $\tilde{\mathscr{O}}$ be a $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbit of conjugacy classes in $\tilde{G}$ which projects to $\mathscr{O}$. We note that the projection of the multiset $\tilde{\mathscr{O}}$ to G will be some multiple $k_{\mathscr{O}}\mathscr{O}$ of $\mathscr{O}$, where $k_{\mathscr{O}} \geq 1$. We know that $\underline{c}$ can be expressed as

$$\sum_{\mathscr{O}} c_{\mathscr{O}} \mathscr{O}$$

for some set of integers $\{c_{\mathscr{O}}\}$. Then the Nielsen class

$$\underline{\tilde{c}} = \sum_{\mathscr{O}} \lceil \frac{c_{\mathscr{O}}}{k_{\mathscr{O}}} \rceil \tilde{\mathscr{O}}$$

is $\mathbb{F}_q$-rational; moreover, the projection of $\underline{\tilde{c}}$ to G can be written as $\underline{c} + \underline{c}'$, where $\underline{c}'$ is drawn from a finite list of $\mathbb{F}_q$-rational Nielsen classes $\underline{c}'_1, \dots, \underline{c}'_M$.

Now we fix, once and for all, a $\mathbb{F}_q$-rational Nielsen class $\tilde{\underline{c}}''$ for $\tilde{G}$, containing at least $C_3(G)$ copies of each conjugacy class of $\tilde{G}$. We know already that, for some i, the Hurwitz space attached to $\tilde{\underline{c}} + \tilde{\underline{c}}'' + \tilde{\underline{e}}_i$ is nonempty; what's more, it is $\mathbb{F}_q$-rational, and by Lemma 3.4 it is geometrically connected.

The projection of $\tilde{\underline{c}} + \tilde{\underline{c}}'' + \tilde{\underline{e}}_i$, under the map $\tilde{G} \to G$, can be written as $\underline{c} + \underline{d}_i + n_i\mathbf{1}$, where $\underline{d}_i$ is drawn from some finite list $\underline{d}_1, \dots, \underline{d}_N$, and $n_i\mathbf{1}$ refers to n_i copies of the trivial conjugacy class.

We claim that $\mathcal{H}_{\underline{c}+\underline{d}_i}$ has an $\mathbb{F}_q$-rational geometrically connected component. Indeed, to any $\tilde{G}$-cover $Y \to \mathbb{P}^1$ with Nielsen class $\tilde{\underline{c}} + \tilde{\underline{c}}'' + \tilde{\underline{e}}_i$, there is canonically associated a G-cover of $\mathbb{P}^1$ with Nielsen class $\underline{c} + \underline{d}_i$; namely, take the quotient of Y by $\ker(\tilde{G} \to G)$.

The associated map $\mathcal{H}_{\tilde{\underline{c}}+\tilde{\underline{c}}''+\tilde{\underline{e}}_i} \to \mathcal{H}_{\underline{c}+\underline{d}_i}$ has as its image is a geometrically connected $\mathbb{F}_q$-rational component of $\mathcal{H}_{\underline{c}+\underline{d}_i}$.

For notational convenience, define $h(q, \underline{c})$ to be the number of $\mathbb{F}_q$-rational geometric components of $\mathcal{H}_{\underline{c}}$ multiplied by $q^{|\underline{c}|}$. By the discussion above, $h(q, \underline{c} + \underline{d}_i) \geq q^{|\underline{c}+\underline{d}_i|}$ for some i.

We thus have, on the one hand,

$$\sum_{i, \underline{c}: r(\underline{c}) < R} h(q, \underline{c} + \underline{d}_i) \geq \sum_{\underline{c}: r(\underline{c}) < R} q^{|\underline{c}+\underline{d}_i|} \geq \sum_{\underline{c}: r(\underline{c}) < R} h'(q, \underline{c})$$

and on the other,

$$\sum_{i, \underline{c}: r(\underline{c}) < R} h(q, \underline{c} + \underline{d}_i) \leq N \sum_{\underline{c}: r(\underline{c}) < R + r(\underline{d}_i)} h(q, \underline{c}).$$

This finishes the proof of the proposition, taking C_1 to be $1/N$ and m to be the supremum of $r(\underline{d}_i)$. □

We are now in a position to prove Prop. 3.1:

Proof. (of Prop. 3.1). By definition $\sum_{r=0}^{\infty} h'(q, r) q^{-rs} = \sum_{\underline{c}} q^{|\underline{c}|} q^{-r(\underline{c})s}$, the sum being taken over all $\mathbb{F}_q$-rational Nielsen classes $\underline{c}$. This sum factorizes as a product indexed by the $\mathrm{Gal}(\mathbb{F}_q)$-orbits $\mathscr{O}$ of conjugacy classes of G:

$$\sum_{r=0}^{\infty} h'(q, r) q^{-rs} = \prod_{\mathscr{O}} (1 - q^{|\mathscr{O}|(1-\mathrm{ind}(\mathscr{O})s)})^{-1} \tag{3.8}$$

Here by $\mathrm{ind}(\mathscr{O})$ we mean the ramification index of any representative of the orbit $\mathscr{O}$, and by $|\mathscr{O}|$ the number of conjugacy classes in $\mathscr{O}$.

Now (3.8) implies, via Lemma 2.3, that $\sum_{q^r < X} h'(q, r) \asymp X^{a(G)} \log(X)^{b_{\mathbb{F}_q}(G)-1}$, where $a(G), b_{\mathbb{F}_q}(G)$ are as in Malle's conjecture. The claim of Proposition 3.1 now follows at once from this and Proposition 3.2. □

4 Further conjectures

In this section, we discuss first (Section 4.1) some further questions in the function field case. The heuristics used for Proposition 3.1 also suggest certain "refined" heuristics for extensions of number fields; we discuss some of these in Section 4.2. Finally in Section 4.3 we discuss some more speculative questions about the enumeration of higher-dimensional varieties.

We note by way of caution that there is little numerical evidence to suggest that some of the questions posed below have an affirmative answer.

4.1 More questions about function fields.

The following question was raised by N. Katz and J. de Jong.

Question 4.1. Let q be fixed. Is it true that there is a constant $c := c(q)$ such that the number of isomorphism classes of genus g curves over $\mathbb{F}_q$ is less than c^g, for all $g \geq 1$?

The emphasis of this question is on the case where q is fixed and $g \to \infty$. The upper bound $c^{g \log(g)}$ was established by Katz and de Jong in unpublished work. In a certain sense this bound is analogous to Lemma 2.4. Note that this problem, again, amounts to counting the number of $\mathbb{F}_q$ points on a variety (namely the moduli space $\mathfrak{M}_g$) of high dimension. One difficulty in using, e.g., the Lefshetz fixed point formula, is that the Betti numbers of $\mathfrak{M}_g$ grow very rapidly with g.

Returning to the distribution of discriminants, one may also study the properties of certain zeta functions; this serves to one may smooth out the irregularity in the distribution of discriminants. For instance, consider the function $\xi_{q,G}(s) := \sum_L D_{L/\mathbb{F}_q(t)}^{-s}$, where L varies over degree n extensions of $\mathbb{F}_q(t)$ with Galois group G, and $\mathcal{D}_L$ is the discriminant of L. A "geometric" variant of $\xi_{q,G}$ is the zeta function:

$$\zeta_{q,G}(s) = \sum_{r=0}^{\infty} |\mathcal{H}_r(\mathbb{F}_q)| q^{-rs}. \tag{4.9}$$

Question 4.2. What are the analytic properties of $\zeta_{q,G}(s)$? In particular, is it the case that $\zeta_{q,G}(s)$ has an analytic continuation to the left of $\Re s = 1/a(G)$, with a pole of order $b_{\mathbb{F}_q}(G)$ at $s = 1/a(G)$?

4.2 Questions about number fields.

The discriminant of a number field $K/\mathbb{Q}$ may be regarded as a measure of ramification, where each ramified prime is weighted according to the conjugacy class of tame inertia. In the present section, we discuss first (sections 4.2.1 and 4.2.2) generalizations of Malle's conjecture that allow for varying this weighting. In section 4.2.3 we take up the question of multiplicity of discriminants, already raised in Conjecture 1.3. As an example of these heuristics, we give heuristics for the number of icosahedral modular forms with conductor $\leq N$ (Ex. 4.4).

The questions proposed in this section are interrelated. In particular, the upper bounds implicit in Question (4.5), Question (4.3), and Conjecture 1.3 are close to equivalent (see Remark 4.7.) In fact, these weak upper bounds seem on considerably safer ground then the general questions, as they do not presuppose a positive solution to the inverse Galois problem.

4.2.1 Malle's conjecture with modified weights

Set $K = \mathbb{Q}$ and let other notations be as described prior to Conjecture 1.2. Let $f : \mathscr{C} \to \mathbb{Z}_{\geq 0}$ be invariant under the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action and such that

$$f(g) = 0 \Longleftrightarrow g = \{\mathrm{id}\}.$$

We call such an f a *rational class function.* Set $a(f) = \max_{c \in \mathscr{C}, c \neq \{\mathrm{id}\}} f(c)^{-1}$. Let $b_{\mathbb{Q}}(f)$ be the number of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbits on the set $\{c \in \mathscr{C} : f(c) = a(f)^{-1}\}$.

If $L/\mathbb{Q}$ is a Galois extension with group G and p is a prime not dividing $|G|$, let $c_p \in \mathscr{C}$ be the image of a generator of tame inertia at p. Now we define the f-discriminant of L to be:

$$\mathcal{D}_f(L) = \prod_{p \not| |G|} p^{f(c_p)}. \tag{4.10}$$

For instance, if $f = \mathrm{ind}$, then $\mathcal{D}_f(L)$ is the prime-to-$|G|$ part of $\mathcal{D}_{L_0}$, notations being as prior to Conjecture 1.2, taking $K = \mathbb{Q}$.

Let $N_{G,f}(X)$ (or, when the group is clear from context, just $N_f(X)$) be the number of Galois extensions $L/\mathbb{Q}$ with Galois group G and $D_f(L) < X$.

Question 4.3. Is it true that $N_{G,f}(X) \sim cX^{a(f)}(\log X)^{b_{\mathbb{Q}}(f)-1}$?

We note that this type of generalization is already, in some sense, anticipated in Malle's conjecture. A given G can be equipped with many different embeddings into symmetric groups; Malle's conjecture already predicts an asymptotic for $N_f(X)$ when f is the index function corresponding to *any* such embedding.

Example 4.4. Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation. Then $g \in G \mapsto \mathrm{codim} V^g$, the codimension of the invariant space, defines a rational class function. If $L/\mathbb{Q}$ has Galois group G, $\mathcal{D}_f(L)$ is the prime-to-$|G|$ part of the Artin conductor of the Galois representation associated to L.

For example, we may take G to be the finite subgroup of order 240 in $GL_2(\mathbb{C})$ whose image in $\mathrm{PGL}_2(\mathbb{C})$ is isomorphic to A_5. For this group, there is a unique conjugacy class (the conjugacy class of non-central involutions) which has $f(c) = 1$. Subject to Artin's conjecture, the holomorphic modular forms of weight 1, conductor N, quadratic Dirichlet character, and icosahedral type are in bijection with the Galois extensions with group G and Artin conductor N such that complex conjugation is sent to a non-central involution.

Question 4.3 then suggests that, if $s(N)$ is the number of icosahedral holomorphic weight-1 modular forms with quadratic character and conductor at most N, then

$$s(N) \sim cN$$

for some constant c. The best upper bound at present is $s(N) \ll_\epsilon N^{13/7+\epsilon}$ due to Michel and the second author [14]. Serre [15] speculated that the number of such forms with conductor *exactly* N is $\ll_\epsilon N^\epsilon$.

4.2.2 Multidiscriminants

One can use the function field heuristics described here to produce even more refined (i.e. optimistic!) heuristics for counting number fields, in which we attach to each field not just an element of $\mathbb{R}_{\geq 0}$ but an element of $\mathbb{R}^k_{\geq 0}$ for some $k > 1$. We could call such a map a "multidiscriminant."

Let G be a finite group, and let the orbits of the nontrivial conjugacy classes under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be denoted $\mathscr{O}_1, \mathscr{O}_2, \ldots \mathscr{O}_m$. Given a Galois G-extension $L/\mathbb{Q}$, set $D_{\mathscr{O}_i}(L)$ to be the product of all primes $p \not| G$ such that the image in G of tame inertia at p is conjugate to $\mathscr{O}_i$; the map $L \mapsto (D_{\mathscr{O}_i}(L))_{1 \leq i \leq m}$ can be regarded as a multidiscriminant. Set $N_G(X_1, \ldots, X_n)$ to be the number of $L/\mathbb{Q}$ such that $D_{\mathscr{O}_i}(L) < X_i$ for all i. We can then ask:

Question 4.5. Is it true that, if $X_j \to \infty$ for all $1 \leq j \leq n$, then the ratio

$$\frac{N_G(X_1, \ldots, X_m)}{X_1 \ldots X_m} \tag{4.11}$$

approaches a fixed limit $c = c(G)$?

As before, (4.11) can be heuristically justified by dimension computations over finite fields. Indeed, let notation be as above but let $\{\mathscr{O}_i\}$ now denote the orbits of the conjugacy classes in G under the cyclotomic character of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Let $N_{G,q}(X_1, \ldots, X_m)$ be the number of Galois

G-covers $f : Y \to \mathbb{P}^1/\mathbb{F}_q$ such that the number of branch points of f in $\mathbb{P}^1$ with monodromy in $\mathscr{O}_i$ is less than $a_i = \lfloor \frac{\log(X_i)}{\log(q)} \rfloor$. Such covers are parametrized (as usual, up to uniformly bounded finite ambiguity arising from descent problems) by the $\mathbb{F}_q$-points of a variety, whose largest-dimensional connected component is a Hurwitz space of dimension about $\sum_i a_i$. So our usual heuristic suggests that this variety has about $\prod_i q^{a_i}$, or $X_1 \dots X_m$ points.

Lemma 4.6. *An affirmative answer to Question (4.5) implies an affirmative answer to Question (4.3).*

The proof of the Lemma is straightforward but tedious.

4.2.3 The multiplicity of discriminants

A problem of a rather different flavor is to count the extensions $L/\mathbb{Q}$ with Galois group G whose discriminant is *exactly* X. One can show, e.g. by genus theory, that this number can grow as fast as $X^{c/\log\log(X)}$. On the other hand Conjecture 1.3 asserts that this multiplicty is $\ll_{\epsilon,G} X^{\epsilon}$.

Conjecture (1.3) implies that the l-torsion part of the class group of a number field $K/\mathbb{Q}$ is $\ll_{l,[K:\mathbb{Q}]} \mathcal{D}_{K/\mathbb{Q}}^{\epsilon}$. (This follows immediately from class field theory, as l-torsion in the class group of K would give rise to unramified extensions of degree l.)

Remark 4.7. The following conjectures are equivalent:

1. Conjecture (1.3),
2. The upper bound $N_{G,f}(X) \ll_{\epsilon,G,f} X^{a(f)+\epsilon}$ in Question 4.3,
3. The upper bound $N_G(X_1, \dots, X_n) \ll (X_1 X_2 \dots X_n)^{1+\epsilon}$ in Question (4.5).

The implications (1) $\implies$ (3) $\implies$ (2) are trivial. We show the remaining implication in the following Proposition.

Proposition 4.8. *An affirmative answer to Question (4.3) – or even the weaker assumption*

$$N_{G,f}(X) \ll_{\epsilon,G,f} X^{a(f)+\epsilon}, \tag{4.12}$$

implies Conjecture 1.3.

Proof. Let $a_G(X)$ be the number of extensions $L/\mathbb{Q}$ with Galois group G and with discriminant X. Clearly it will suffice to show $a_G(X) \ll_{\epsilon,G} X^{\epsilon}$. The main idea will be to apply (4.12) with G replaced by G^k and some of its subgroups.

Fix $k > 0$ an integer. We write an element of G^k as a k-tuple $(g_1, g_2, \dots, g_k)$. Let F be the class function on G^k that is identically 1, i.e. $F(c_1, \dots, c_k) = 1$ for all conjugacy classes c_j of G.

Let $\mathscr{S}$ be the class of subgroups of G^k which project surjectively onto each copy of G; for each $H \in \mathscr{S}$ we also write F for the rational class function on H that is identically 1. Then the k-tuples of G-extensions $L_1, \dots, L_k$ are in bijection with the H-extensions $L/\mathbb{Q}$, where H ranges over $\mathscr{S}$. We denote by $[L_1, \dots, L_k]$ the H-extension associated to a k-tuple in this way, and by $\mathcal{D}_F([L_1, \dots, L_k])$ the F-discriminant of this extension, given by the formula (4.10).

$\mathcal{D}_F([L_1, \dots, L_k])$ is, away from primes dividing $|G|$, the squarefree part of the product $\prod_{j=1}^k \mathcal{D}_{L_j/\mathbb{Q}}$. Thus $\mathcal{D}_F([L_1, \dots, L_k])$ is (relatively) large whenever the $\mathcal{D}_{L_i}$ have few common factors with each other. On the other hand, if $\mathcal{D}_{L_1/\mathbb{Q}} = \mathcal{D}_{L_2/\mathbb{Q}} = \dots = \mathcal{D}_{L_k/\mathbb{Q}} = X$, it follows that $D_F([L_1, \dots, L_k]) \leq X$. In particular,

$$\sum_{H \in \mathscr{S}} N_{H,F}(X) \geq a_G(X)^k \tag{4.13}$$

Combining (4.13) and (4.12), and noting the exponent a of (4.12) equals 1 whenever (G, f) is replaced by (H, F) as above, we see that $a_G(X)^k \ll_{G,k} X^{1+\epsilon}$. The result follows, k being arbitrary. □

4.3 The scarceness of arithmetic objects with prescribed bad reduction

We have discussed in previous sections heuristics for counting function fields, number fields, and Galois representations. In a certain sense all of these can be regarded as "0-dimensional" arithmetic objects. We now briefly discuss a plausible statement in higher dimensions, at least as regards *upper bounds*.

By way of motivation, we note that Conjecture 1.3 may be regarded as saying that *there are very few number fields with very little bad reduction.* If one replaces "number field" with "proper smooth variety," very little is known; however, it is generally believed that there are "relatively few" proper smooth varieties V over $\mathbb{Z}$. There are a few evident examples: one may take for V e.g. a flag variety associated to a Chevalley group over $\mathbb{Z}$. Further, one may blow up such a variety along an appropriate locus. However, as Jason Starr and Johan de Jong pointed out to us, all such varieties are *rational*, and it there seems to be no non-rational example known. A beautiful result of Fontaine states that there exist no abelian varieties over $\mathbb{Z}$.

The question we state aims to quantify this scarceness. For a finite set S of primes set $N(S) = \prod_{p \in S} p$. For concreteness and to avoid any technical hypotheses, we have phrased the question in terms of modular Galois representations.

Question 4.9. Fix a Hodge-Tate type π (i.e. a set of Hodge-Tate weights), positive integers n, d, and a prime l. Let $\mathrm{GR}(\pi, S)$ be the set of modular Galois representations $\rho_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$ with Hodge-Tate weights π and good reduction outside S. Here "modular" means "attached to an automorphic form on GL_n." Let $\mathrm{GR}_d(\pi, S) \subset \mathrm{GR}(\pi, S)$ be the subset consisting of ρ_l whose Frobenius traces lie in a field extension of $\mathbb{Q}$ with degree $\leq d$.

Is it true that $|\mathrm{GR}_d(\pi, S)| \ll_{\epsilon,d,n,\pi} N(S)^\epsilon$?

We can ask a similar question with a more "motivic" flavor; of course, one may expect that under suitable modularity conjectures the questions above and below are equivalent.

Question 4.10. Fix $K \in \mathbb{N}$ and let S be a finite set of primes. Consider the set $\mathcal{V}(K, S)$ of proper smooth varieties V over $\mathrm{Spec}\mathbb{Z}[\frac{1}{N(S)}]$ such that $\dim(V) \leq K$ and $\dim H^i(V_{\mathbb{C}}, \mathbb{C}) \leq K$ for each $0 \leq i \leq 2K$. To each variety $V \in \mathcal{V}(K, S)$ associate the sequence $\#(V(\mathbb{F}_p))_{p \notin S}$, indexed by the primes not in S. Then the number of distinct such sequences is $\ll_K N(S)^\epsilon$.

An affirmative answer to Question 4.9 would imply Conjecture 1.3. It would also imply that the number of elliptic curves over $\mathbb{Q}$ of conductor N is $\ll_\epsilon N^\epsilon$.

Note that even the *finiteness* of $\mathrm{GR}(\pi, S)$ would not be clear without the hypothesis of modularity! Using modularity, one may probably show that $|\mathrm{GR}(\pi, S)|$ is bounded by a polyomial in $N(S)$. The content of the assertion is then that $|\mathrm{GR}_d(\pi, S)|$ is much smaller. A related phenomenon is well-known in the context of holomorphic forms: fix $k \geq 2$ and consider the space $S_k(N)$ of holomorphic forms of level N and weight k. Although $\dim S_k(N) \sim \mathrm{const} \cdot N$ as $N \to \infty$, the number of Hecke eigenforms whose coefficient field has degree $\leq d$ seems to grow much more slowly with N.

One can enunciate a corresponding question in the function field case; it also seems quite difficult.

Remark 4.11. It is interesting to note the contrast between the number field and function field contexts. In the number field setting, the ability to average seems to make counting objects of conductor up to N much easier than counting objects of conductor exactly N. In the function field

setting, on the other hand, counting objects of conductor up to N means counting covers of $\mathbb{P}^1$ whose ramification locus varies among all divisors of $\mathbb{P}^1$ of degree less than $\log_q N$, while counting covers with a *fixed* conductor amounts to studying the arithmetic (in the case of finite covers, the étale fundamental group) of a *single* open curve inside $\mathbb{P}^1$, which might in some ways be easier. One way to express the contrast is to observe that our understanding of the étale fundamental group of an open subset of $\mathbb{P}^1_{\mathbb{F}_q}$, though very far from complete, is much greater than our understanding of the maximal Galois extension of $\mathbb{Q}$ unramified away from a fixed finite set of primes.

References

[1] K.Belabas. Paramétrisation de structures algébriques et densité de discriminants (d'après M. Bhargava) Seminaire Bourbaki, Exp. No. 935, 2004

[2] M. Bhargava. *Higher Composition Laws*. Ph.D. thesis, Princeton University, 2001.

[3] M. Bhargava. Higher composition laws, IV. Preprint.

[4] I. Bouw and S. Wewers. Reduction of covers and Hurwitz spaces. To appear, J. Reine Angew. Math.

[5] H. Cohen, F. Diaz y Diaz, and M. Olivier. A survey of discriminant counting. *Algorithmic number theory (Sydney, 2002)*, 80–94, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[6] H. Cohen, F. Diaz y Diaz, and M. Olivier. On the density of discriminants of cyclic extensions of prime degree. J. Reine Angew. Math. 550, 169–209, 2002.

[7] B. Datskovsky and D. J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math.* 386 (1988), 116–138.

[8] P. Debes and J.-C. Douai. Algebraic covers: field of moduli versus field of definition. Ann. Sci. École Norm. Sup. (4) 30 (1997), no.3, 303–338.

[9] W. Duke. Bounds for arithmetic multiplicities. Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), *Doc. Math.* 1998, Extra Vol. II, 163–172.

[10] J. Ellenberg and A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. Preprint.

[11] M. Fried and H. Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.* 290, no.4, 771-900 (1991)

[12] G. Malle. On the distribution of Galois groups. J. Number Theory 92, 315–329, 2002.

[13] G. Malle. On the distribution of Galois groups, II Preprint.

[14] P. Michel and A. Venkatesh. On the dimension of the space of cusp forms associated to 2-dimensional Galois representations. *Int. Math. Res. Not.* no. 38, 2021–2027, 2002.

[15] J.-P. Serre. Modular forms of weight one and Galois representations. in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos. Univ. Durham, Durham, 1975*, 193–268, 1977.

[16] S. Wewers. Construction of Hurwitz spaces. Ph.D. thesis, Essen, 1998.

[17] H. Völklein. *Groups as Galois groups*. Cambridge University Press, 1996.