HURWITZ MONODROMY AND FULL NUMBER FIELDS

DAVID P. ROBERTS AND AKSHAY VENKATESH

Abstract. We give conditions for the monodromy group of a Hurwitz space over the configuration space of branch points to be the full alternating or symmetric group on the degree. Specializing the resulting coverings suggests the existence of many number fields with surprisingly little ramification — for example, the existence of infinitely many A_m or S_m number fields unramified away from $\{2, 3, 5\}$.

Contents

1. Introduction

1.1. **Overview.** The motivation of this paper is an open problem posed in [16] concerning number fields, as follows. Say that a degree m number field K is *full* if its associated Galois group is either A_m or S_m. Fix a finite set of primes $\mathcal{P}$. The problem is, *Are there infinitely many full fields K for which the discriminant of K is divisible only by primes in $\mathcal{P}$?*

In this paper we present a construction, with origins in work of Hurwitz, which gives many fields of this type. On the basis of this construction we propose:

Conjecture 1.1. *Suppose $\mathcal{P}$ contains the set of prime divisors of the order of a nonabelian finite simple group. Then there exist infinitely many full fields unramified outside $\mathcal{P}$.*

Our construction amounts to specializing suitable coverings of $\mathbb{Q}$-algebraic varieties at suitable rational points. In the current paper, we analyze the geometric part of the construction, defining the varieties and proving that the *geometric* monodromy group is A_m or S_m. A sequel paper [22] provides experimental evidence that fullness is sufficiently preserved by the specialization step for Conjecture 1.1 to be true.

Now some words as to why we find this surprising: In [19] the first-named author applied Bhargava's mass heuristic [1] to the open question. For given $\mathcal{P}$, a finite number was obtained for the total expected number of full fields K. Accordingly, it was conjectured in [19] that the answer to the question is *no* for all $\mathcal{P}$. However, the construction given in this paper systematically gives fields which escape the influence of the mass heuristic. It is clear from these fields that [19] applied the mass heuristic out of its regime of applicability.

Sections 2, 3 and 4 provide short summaries of large theories and serve to establish our setting. Section 5 states our main theorem, which we call the full-monodromy theorem. It has the form that two statements I and II are equivalent. Sections 6 and 7 prove the theorem by establishing I $\Rightarrow$ II and II $\Rightarrow$ I respectively. §1.2 provides an overview of this material.

§1.3 provides an overview of our construction of full number fields. Section 8 concludes the paper with more details, a sampling of the numerical evidence for Conjecture 1.1, and further discussion of full number fields in large degree ramified within a prescribed $\mathcal{P}$.

1.2. **The full-monodromy theorem.** Define a *Hurwitz parameter* to be a triple $h = (G, C, \nu)$ where G is a finite group, $C = (C_1, \dots, C_r)$ is a list of conjugacy classes generating G, and $\nu = (\nu_1, \dots, \nu_r)$ is a list of positive integers, with ν *allowed* in the sense that $\prod [C_i]^{\nu_i} = 1$ in the abelianization G^{ab}. A Hurwitz parameter determines an unramified covering of complex algebraic varieties:

$$\pi_h : \mathsf{Hur}_h \to \mathsf{Conf}_\nu. \tag{1.1}$$

Here the cover Hur_h is a Hurwitz variety parameterizing certain covers of the complex projective line P^1, where the coverings are "of type h." The base Conf_ν is the variety whose points are tuples $(D_1, \dots, D_r)$ of disjoint divisors D_i of P^1, with $\deg(D_i) = \nu_i$. The map π_h sends a cover to its branch locus.

In complete analogy with the use of the term for number fields, we say that a cover of connected complex algebraic varieties $\mathsf{X} \to \mathsf{Y}$ is *full* if its monodromy group is the entire alternating or symmetric group on the degree. There are two relatively simple obstructions to (1.1) being full. One is associated to G having a non-trivial outer automorphism group and we deal with it by replacing Hur_h by a quotient variety Hur_h^* also covering Conf_ν. The other is associated to G having a non-trivial Schur multiplier and we deal with it by a decomposition $\mathsf{Hur}_h^* = \coprod_\ell \mathsf{Hur}_{h,\ell}^*$. Here ℓ runs over an explicit quotient set of the Schur multiplier and each $\mathsf{Hur}_{h,\ell}^*$ is a union of connected components.

The most important direction of the full-monodromy theorem is I $\Rightarrow$ II. When G is nonabelian and simple, this direction is as follows.

Fix a nonabelian simple group G and a list $C = (C_1, \dots, C_r)$ of conjugacy classes generating G. Consider varying allowed ν and thus varying Hurwitz parameters $h = (G, C, \nu)$. Then as soon as $\min_i \nu_i$ is sufficiently large, the covers $\mathsf{Hur}_{h,\ell}^* \to \mathsf{Conf}_\nu$ are full and pairwise non-isomorphic.

The complete implication I $\Rightarrow$ II is similar, but G is allowed to be "pseudosimple", and therefore groups such as S_d are included. There are considerable complications arising from non-trivial abelianizations G^{ab}, even in the case $|G^{\mathrm{ab}}| = 2$. The extra generality is required for obtaining the natural converse II $\Rightarrow$ I.

Our proof of I $\Rightarrow$ II in general starts from the Conway-Parker theorem about connectivity of Hurwitz covers [6, 12, 15, 11]. We deal with complications from nontrivial G^{ab} in the framework of comparing two Hochschild-Serre five-term exact sequences. We upgrade connectivity to fullness by using a Goursat lemma adapted to our current situation and the explicit classification of 2-transitive groups. Our general approach has much in common with the proof of Theorem 7.4 in [8], which is in a different context.

While there is a substantial literature on Hurwitz covers, our topic of asymptotic fullness has not been systematically pursued before. In related directions there are the papers [10, 14, 13]. We will indicate relations with some of this literature at various points in this paper.

1.3. **Specialization to number fields.** We say that a Hurwitz parameter $h = (G, C, \nu)$ is *strongly rational* if all classes C_i are rational. For strongly rational Hurwitz parameters, (1.1) descends to a covering

$$\pi_h : \textsc{Hur}_h \to \textsc{Conf}_\nu \tag{1.2}$$

of $\mathbb{Q}$-varieties. The full-monodromy theorem says that every nonabelian finite simple group G is part of infinitely many Hurwitz parameters h leading to full covers of $\mathbb{Q}$-varieties of the modified form $\pi : \textsc{Hur}^*_{h,\ell} \to \textsc{Conf}_\nu$.

The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on fibers $\pi^{-1}(u)$ over rational points $u \in \textsc{Conf}_\nu(\mathbb{Q})$. The fullness of π, together with the Hilbert irreduciblity theorem, says that for *generic* u, the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ contains the full alternating group on the fiber. In this case one gets a full field $K^*_{h,\ell,u}$ corresponding to the fiber.

There is a natural action of $\mathrm{PGL}_2(\mathbb{Q})$ on $\textsc{Conf}_\nu(\mathbb{Q})$ and, if u, u' lie in the same PGL_2-orbit, then $K^*_{h,\ell,u} \simeq K^*_{h,\ell,u'}$. Another application of the Hilbert irreducibility theorem shows that, generically, different orbits give nonisomorphic fields.

Let $\mathcal{P}$ be the set of prime divisors of $|G|$. The general theory of algebraic fundamental groups says that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\pi^{-1}(u)$ is unramified away from $\mathcal{P}$ so long as u is a $\mathcal{P}$-integral point. As ν varies, the number of PGL_2 equivalence classes of such specialization points can be arbitrarily large. Thus, *so long as even a weak version of Hilbert irreducibility remains valid for such $\mathcal{P}$-integral points*, we obtain sufficiently many full fields for Conjecture 1.1. As we explain in our last section, the available evidence is that there is in fact a strong tendency for specializations to be full, and specializations from different orbits to be distinct.

Of course, there are many other coverings of varieties that, like (1.2), have full geometric monodromy. However, examples with the favorable ramification properties of the Hurwitz covers are rare.

1.4. **Acknowledgements.** We thank Simon Rubinstein-Salzedo and John Voight for helpful comments on earlier drafts of this paper. DR was supported by grant #209472 from the Simons foundation. AV was supported by a grant from the NSF and from the Packard foundation.

2. Hurwitz covers

In this section we summarize the theory of Hurwitz covers, taking the purely algebraic point of view necessary for the application to Conjecture 1.1. We consider Hurwitz parameters $h = (G, C, \nu)$, with G assumed centerless to avoid technical complications. The central focus is an associated cover $\pi_h : \textsc{Hur}_h \to \textsc{Conf}_\nu$ and related objects. A more detailed summary is in [18] and a comprehensive reference is [4].

2.1. **Configuration spaces** $\textsc{Conf}_\nu$**.** Let $\nu = (\nu_1, \ldots, \nu_r)$ be a vector of positive integers; we write $|\nu| = \sum \nu_i$. For k a field, let $\textsc{Conf}_\nu(k)$ be the set of tuples $(D_1, \ldots, D_r)$ of disjoint k-rational divisors on $\mathbb{P}^1_k$ with D_i consisting of ν_i distinct geometric points.

Explicitly, we may regard

$$\textsc{Conf}_\nu \subseteq \mathbb{P}^{\nu_1} \times \cdots \times \mathbb{P}^{\nu_r},$$

where we regard $\mathbb{P}^{\nu_i}$ as the projectivized space of binary homogeneous forms $q(x, y)$ of degree ν_i, and $\textsc{Conf}_\nu$ is then the open subvariety defined by nonvanishing of the discriminant $\mathrm{disc}(q_1 \cdots q_r)$. The divisor D_i associated to an r-tuple $(q_1, \ldots, q_r)$ of such forms is simply the zero locus of q_i.

2.2. **Standard Hurwitz varieties** $\textsc{Hur}_h$**.** Let k be an algebraically closed field of characteristic zero. Consider pairs (Σ, f) consisting of a proper smooth connected curve Σ over k together with a Galois covering $f : \Sigma \to \mathbb{P}^1$.

Such a pair has the following associated objects:

- An automorphism group $\mathrm{Aut}(\Sigma/\mathbb{P}^1)$ of size equal to the degree of f,
- A branch locus $Z \subset \mathbb{P}^1(k)$ of degree $n = |Z|$;
- For every $t \in Z$, a local monodromy element $g_t \in \mathrm{Aut}(\Sigma/\mathbb{P}^1)$ defined up to conjugacy. (To define this requires a compatible choice of roots of unity, i.e. an element of $\varprojlim_n \mu_n(k)$; we assume such a choice has been made).

Consider triples (Σ, f, ι) with $\iota : G \to \mathrm{Aut}(\Sigma/\mathbb{P}^1)$ a given isomorphism. We say that such a triple has type h if $\sum \nu_i = n$ and for each i there are exactly ν_i elements $t \in Z$ such that $g_t \in C_i$. The branch locus Z then defines an element of $\textsc{Conf}_\nu(k)$ is a natural way.

The theory of Hurwitz varieties implies that there exists a $\overline{\mathbb{Q}}$-variety $\textsc{Hur}_h$, equipped with an étale map

$$\pi_h : \textsc{Hur}_h \to \textsc{Conf}_\nu, \tag{2.1}$$

with the following property holding for all k: For any $u \in \textsc{Conf}_\nu(k)$, the fiber $\pi_h^{-1}(u)$ is, $\mathrm{Aut}(k/\mathbb{Q}(\mu_\infty))$-equivariantly, in bijection with the set of isomorphism classes of covers of $\mathbb{P}^1$ of type h, with branch locus equal to u.

2.3. **Quotiented Hurwitz varieties** $\textsc{Hur}_h^*$**.** If (Σ, f, ι) is as above, we can modify ι by an element $\alpha \in \mathrm{Aut}(G)$, to obtain a new triple $(\Sigma, f, \iota \circ \alpha^{-1})$. If α is inner, the resulting triple is actually isomorphic to (Σ, f, α). As a result we obtain actions not of groups of automorphisms, but rather groups of outer automorphisms.

Let $\mathrm{Aut}(G, C)$ be the subgroup consisting of those elements which fix every C_i. Then $\mathrm{Out}(G, C) = \mathrm{Aut}(G, C)/G$ acts naturally on $\textsc{Hur}_h$ giving a quotient

$$\textsc{Hur}_h^* = \textsc{Hur}_h/\mathrm{Out}(G, C),$$

still lying over $\textsc{Conf}_\nu$. This quotient parameterizes pairs (Σ, f) equipped with an element $(D_1, \ldots, D_r)$ of $\textsc{Conf}_\nu(k)$ so that the branch locus is precisely $\coprod D_i$, and there exists an isomorphism $\iota : G \to \mathrm{Aut}(\Sigma/\mathbb{P}^1)$ so that the monodromy around each point of D_i is of type $\iota(C_i)$. Our main theorem focuses on $\textsc{Hur}_h^*$ rather than $\textsc{Hur}_h$.

2.4. **Descent to $\mathbb{Q}$.** The abelianized absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}} = \hat{\mathbb{Z}}^\times$ acts on the set of conjugacy classes in any finite group by raising representing elements to powers. In particular, one can talk about "rational" classes, i.e. conjugacy classes fixed by this action. As in the introduction, we say that h is *strongly rational* if all C_i are rational. In this case, (2.1) and its starred version $\pi_h^* : \mathrm{H{\small UR}}_h^* \to \mathrm{C{\small ONF}}_\nu$ canonically descend to covers over $\mathbb{Q}$.

More generally, we say that h is *rational* if conjugate classes appear with equal associated multiplicities. In the main case when all the classes are different, this just means $\nu_i = \nu_j$ whenever C_i and C_j lie in the same Galois orbit. Rationality is a substantially weaker condition than strong rationality. For example, any finite group G has rational h, but only when G^{ab} is trivial or of exponent 2 can G have strongly rational h.

For rational h, there is again canonical descent to $\mathbb{Q}$, although now the maps take the form $\mathrm{H{\small UR}}_h \to \mathrm{H{\small UR}}_h^* \to \mathrm{C{\small ONF}}_\nu^\rho$, with ρ indicating a suitable Galois twisting. The subtlety of twisting is not seen at all in our main sections §5-§7. Our purpose in briefly discussing twisting here is to make clear that a large subset of the covers considered in §5-§7 are useful in constructing fields for Conjecture 1.1.

3. Braid groups

In this section we switch to a group-theoretic point of view, describing the monodromy of Hurwitz covers $\pi_h : \mathsf{Hur}_h \to \mathsf{Conf}_\nu$ and $\pi_h^* : \mathsf{Hur}_h^* \to \mathsf{Conf}_\nu$ in terms of braid groups and their actions on explicit sets. General references for braid groups and their monodromy actions include [15, Chapter 3] and [10, §2].

Our main theorem concerns these monodromy representations only, i.e. it is a theorem in pure topology. As a notational device, used in the introduction and just now again, we denote complex points by a different font as in $\mathsf{Hur}_h = \mathrm{H{\small UR}}_h(\mathbb{C})$ and $\mathsf{Conf}_\nu = \mathrm{C{\small ONF}}_\nu(\mathbb{C})$.

3.1. **Braid groups** Br_ν**.** The Artin braid group on n strands is defined by generators and relations:

$$\mathrm{Br}_n = \left\langle \sigma_1, \dots, \sigma_{n-1} : \begin{array}{rclll} \sigma_i\sigma_j & = & \sigma_j\sigma_i, & \text{if } |i-j| & > & 1 \\ \sigma_i\sigma_j\sigma_i & = & \sigma_j\sigma_i\sigma_j, & \text{if } |i-j| & = & 1 \end{array} \right\rangle.$$

The rule $\sigma_i \mapsto (i, i+1)$ extends to a surjection $\mathrm{Br}_n \twoheadrightarrow S_n$. For every subgroup of S_n, one gets a subgroup of Br_n by pullback. In particular, from the last component $\nu = (\nu_1, \dots, \nu_r)$ of a Hurwitz parameter one gets a subgroup $S_\nu := S_{\nu_1} \times \cdots \times S_{\nu_r}$. We denote its pullback by Br_ν. The extreme Br_n above and the other extreme Br_{1^n} play particularly prominent roles in the literature, the latter often being called the colored or pure braid group.

3.2. **Fundamental groups.** Let $\star = (1, \dots, n) \in \mathsf{Conf}_{1^n}$. We will use it as a basepoint. We use the same notation $\star$ for its image in Conf_ν for any ν. There is a standard surjection $\mathrm{Br}_n \twoheadrightarrow \pi_1(\mathsf{Conf}_n, \star)$ with kernel the smallest normal subgroup containing $\sigma_1 \cdots \sigma_{n-2}\sigma_{n-1}^2\sigma_{n-2} \cdots \sigma_1$ [15, Theorem III.1.4]. This map identifies σ_i with a small loop in Conf_n that swaps the points i and $i+1$. Because of this very tight connection, the group $\pi_1(\mathsf{Conf}_n, \star)$ is often called the spherical braid group or the Hurwitz braid group.

Similarly, we have surjections

$$\mathrm{Br}_\nu \twoheadrightarrow \pi_1(\mathsf{Conf}_\nu, \star). \tag{3.1}$$

Let $\mathcal{F}_h$ and $\mathcal{F}_h^*$ be the fibers of Hur_h and Hur_h^* over $\star$. To completely translate into group theory, we need group-theoretical descriptions of these fibers as Br_ν-sets. The remainder of this section accomplishes this task.

3.3. **Catch-all actions.** We use the standard notational convention $g^h = h^{-1}gh$. If G is any group then Br_n acts on G^n by means of a braiding rule, whereby σ_i substitutes $g_i \to g_{i+1}$ and $g_{i+1} \to g_i^{g_{i+1}}$:

$$(\ldots, g_{i-1}, g_i, g_{i+1}, g_{i+2}, \ldots)^{\sigma_i} = (\ldots, g_{i-1}, g_{i+1}, g_i^{g_{i+1}}, g_{i+2}, \ldots). \tag{3.2}$$

Also $\mathrm{Aut}(G)$ acts on G^n diagonally:

$$(g_1, \ldots, g_n)^\alpha = (g_1^\alpha, \ldots, g_n^\alpha). \tag{3.3}$$

The braiding action and the diagonal action commute, so one has an action of the product group $\mathrm{Br}_n \times \mathrm{Aut}(G)$ on G^n.

3.4. **The** Br_ν**-sets** $\mathcal{F}_h$ **and** $\mathcal{F}_h^*$**.** Next we replace G^n by a smaller set appropriate to a given Hurwitz parameter h. This smaller set is

$$\begin{aligned} \mathcal{G}_h \quad = \quad & \{(g_1, \ldots, g_n) \in G^n : g_1 \cdots g_n = 1, \langle g_1, \ldots, g_n \rangle = G, \\ & \quad \text{first } \nu_1 \text{ of the } g_i\text{'s lie in } C_1, \text{ next } \nu_2 \text{ lie in } C_2, \text{ etc.}\}. \end{aligned} \tag{3.4}$$

The subset $\mathcal{G}_h$ is not preserved by all of $\mathrm{Br}_n \times \mathrm{Aut}(G)$, but it is preserved by $\mathrm{Br}_\nu \times \mathrm{Aut}(G, C)$. The fibers then have the following group-theoretic description:

$$\mathcal{F}_h = \mathcal{G}_h/\mathrm{Inn}(G) \qquad \simeq (\text{fiber of } \mathsf{Hur}_h \to \mathsf{Conf}_\nu \text{ above } \star), \tag{3.5}$$

$$\mathcal{F}_h^* = \mathcal{G}_h/\mathrm{Aut}(G, C) \simeq (\text{fiber of } \mathsf{Hur}_h^* \to \mathsf{Conf}_\nu \text{ above } \star). \tag{3.6}$$

Here in both cases the isomorphisms $\simeq$ are isomorphisms of Br_ν-sets. Note that $\mathcal{F}_h^* = \mathcal{F}_h/\mathrm{Out}(G, C)$.

3.5. **The asymptotic mass formula.** Character theory gives exact formulas for degrees, called mass formulas [24]. We need only the asymptotic versions of these mass formulas, which are very simple:

$$|\mathcal{F}_h| \sim \prod_{i=1}^r \frac{|C_i|^{\nu_i}}{|G'||\mathrm{Inn}(G)|}, \qquad |\mathcal{F}_h^*| \sim \prod_{i=1}^r \frac{|C_i|^{\nu_i}}{|G'||\mathrm{Aut}(G, C)|}. \tag{3.7}$$

Here the meaning in each case is standard: the left side over the right side tends to 1 for any sequence of allowed ν with $\min_i \nu_i$ tending to ∞. The structure of the products on the right directly reflects the descriptions of the sets in §3.4.

4. Lifting invariants

In this section we summarize the theory of lifting invariants which plays a key role in the study of connected components of Hurwitz spaces. Group homology appears prominently and as a standing convention, we abbreviate $H_i(\Gamma, \mathbb{Z})$ by $H_i(\Gamma)$.

In brief summary, the theory being reviewed goes as follows. Let $h = (G, C, \nu)$ be a Hurwitz parameter. The group G determines its Schur multiplier $H_2(G)$. In turn, C determines a quotient group $H_2(G, C)$ of $H_2(G)$, and finally ν determines a certain torsor $H_h = H_2(G, C, \nu)$ over $H_2(G, C)$. The Conway-Parker theorem says that the natural map $\pi_0(\mathsf{Hur}_h) \to H_h$ is bijective whenever $\min_i \nu_i$ is sufficiently large.

4.1. **The Schur multiplier $H_2(G)$.** A stem extension of G is a central extension G^* such that the kernel of $G^* \to G$ is in the derived group of G^*. A stem extension of maximal order has kernel canonically isomorphic to the cohomology group $H_2(G)$. This kernel is by definition the Schur multiplier. A stem extension of maximal order is called a Schur cover. A given group can have non-isomorphic Schur covers, but this ambiguity never poses problems for us here.

4.2. **The reduced Schur multiplier $H_2(G, C)$.** If x, y are commuting elements of G, they canonically define an element $\langle x, y\rangle \in H_2(G)$: the commutator of lifts of x, y to a Schur cover. This pairing is independent of the choice of Schur cover. In fact, a more intrinsic description is that $\langle x, y\rangle$ is the push forward of the fundamental class of $H_2(\mathbb{Z}^2)$ under the map $\mathbb{Z}^2 \to G$ given by $(m, n) \mapsto x^m y^n$.

Fix a stem extension of maximal order $\tilde{G} \to G$. For a conjugacy class C_i and a list of conjugacy classes $C = (C_1, \ldots, C_r)$ respectively, define subgroups of the Schur multiplier:

$$H_2(G)_{C_i} = \{\langle g, z\rangle : g \in C_i \text{ and } z \in Z(g)\}, \tag{4.1}$$

$$H_2(G)_C = \sum H_2(G)_{C_i}. \tag{4.2}$$

Here $Z(g)$ denotes the centralizer of g. The reduced Schur multiplier is then the corresponding quotient group. $H_2(G, C) = H_2(G)/H_2(G)_C$.

A choice of Schur cover $\tilde{G}$ determines a reduced Schur cover $\tilde{G}_C = \tilde{G}/H_2(G)_C$. The corresponding short exact sequence

$$H_2(G, C) \hookrightarrow \tilde{G}_C \twoheadrightarrow G$$

plays an essential role in our study.

In a degree d central extension $\pi : G^* \to G$, the preimage of a conjugacy class D consists of a certain number s of conjugacy classes, all of size $(d/s)|D|$. Always s divides d. If $s = d$ then D is called *split*. By construction, all the C_i are split in $\tilde{G}_C$, and $\tilde{G}_C$ is a maximal extension with this property. For more information on reduced Schur multipliers, see [11, §7, v1].

4.3. **Torsors $H_2(G, C, \nu)$.** For $i = 1, \ldots, r$, let $H_2(G, C, i)$ be the set of conjugacy classes of $\tilde{G}_C$ that lie in the preimage of the class C_i. If $\tilde{z}$ and $\tilde{g}$ are lifts to $\tilde{G}_C$ of the identity $z = 1$ and $g \in C_i$ respectively, then one can multiply $\tilde{z} \in H_2(G, C)$ and $[\tilde{g}] \in H_2(G, C, i)$ to get $[\tilde{z}\tilde{g}] \in H_2(G, C, i)$. This multiplication operator turns each $H_2(G, C, i)$ into a torsor over $H_2(G, C)$.

One can multiply torsors over an abelian group: if T_1 and T_2 are torsors over an abelian group Z, then their product is $(T_1 \times T_2)/Z$ where all $(zt_1, z^{-1}t_2)$ have been identified. In our setting, one has a torsor

$$H_h := H_2(G, C, \nu) = \prod_i H_2(G, C, i)^{\nu_i}. \tag{4.3}$$

Note that H_h is naturally identified with the trivial torsor if all ν_i are multiples of the exponent of $H_2(G, C)$. Namely the product $\prod a_i^{\nu_i}$ is independent of choices $a_i \in H_2(G, C, i)$, and gives a distinguished element of $H_2(G, C, \nu)$. In particular, this distinguished element is fixed under $\mathrm{Aut}(G, C)$ (see §4.5 for a more detailed discussion of functoriality).

4.4. **The lifting map.** Suppose given $(g_1, \ldots, g_n) \in \mathcal{G}_h$. Lift each g_i to an element of $\tilde{g}_i \in \tilde{G}_C$ arbitrarily, subject to the unique condition that the product of the $\tilde{g}_i$ is the identity:

$$\tilde{g}_1 \cdots \tilde{g}_n = 1 \in \tilde{G}_C.$$

Then each $\tilde{g}_i$ determines an element $[\tilde{g}_i] \in H_2(G, C, i)$. Their product is an element $\prod[\tilde{g}_i] \in H_2(G, C, \nu)$, independent of choices. This product is moreover unchanged if we replaced $(g_1, \ldots, g_n)$ by another element in its Br_ν-orbit, or if we replace $(g_1, \ldots, g_n)$ by a G-conjugate. Thus, keeping in mind the identification $\pi_0(\mathsf{Hur}_h) = \mathcal{F}_h/\mathrm{Br}_\nu$ from (3.5), we have defined a function

$$\mathrm{inv}_h : \pi_0(\mathsf{Hur}_h) \longrightarrow H_h. \tag{4.4}$$

We refer to inv_h as the lifting invariant. It has been extensively studied by Fried and Serre, cf. [3, 23]. When a set decomposes according to lifting invariants, we indicate this decomposition by subscripts. Thus, e.g., $\mathcal{F}_h = \coprod \mathcal{F}_{h,\ell}$ and $\mathcal{G}_h = \coprod \mathcal{G}_{h,\ell}$.

The map (4.4) is equivariant with respect to the natural actions of $\mathrm{Out}(G, C)$ and so we can pass to the quotient. Writing $H_h^* = H_h/\mathrm{Out}(G, C)$, we obtain

$$\mathrm{inv}_h^* : \pi_0(\mathsf{Hur}_h^*) \to H_h^*. \tag{4.5}$$

Again we notationally indicate lifting invariants by subscripts, so that e.g. $\mathcal{F}_{h,\ell}^* = \mathcal{F}_{h,\ell}/\mathrm{Out}(G, C)_\ell$, where $\mathrm{Out}(G, C)_\ell$ is the stabilizer of ℓ inside $\mathrm{Out}(G, C)$.

Note that algebraic structure is typically lost in the process from passing from objects to their corresponding starred objects. Namely at the unstarred level, one has a group $H_2(G, C)$ and its many torsors H_h. At the starred level, $H_2^*(G, C)$ is typically no longer a group, the sets H_h^* are no longer torsors, and the cardinality of H_h^* can depend on ν. Our main theorem makes direct reference only to H_h^*. However in the proof we systematically lift from H_h^* to H_h, to make use of the richer algebraic properties.

We finally note for later use that there are asymptotic mass formulas for $\mathcal{F}_{h,\ell}$ and $\mathcal{F}_{h,\ell}^*$ that are very similar to (3.7). Indeed, they are derived simply by applying (3.7) to $\tilde{G}_C$ together with liftings of the conjugacy classes C_i:

$$|\mathcal{F}_{h,\ell}| \sim \frac{|\mathcal{F}_h|}{|H_2(G, C)|}, \qquad |\mathcal{F}_{h,\ell}^*| \sim \frac{|\mathcal{F}_{h,\ell}|}{|\mathrm{Out}(G, C)_\ell|}. \tag{4.6}$$

4.5. **Functoriality.** Suppose given a surjection $f : G \to H$ of groups, together with conjugacy classes C_i in G; set $D_i = f(C_i)$. This clearly induces a map $H_2(G, C) \to H_2(H, D)$. The functoriality of the torsors is less obvious, because of the lack of uniqueness in a Schur cover. For this, we use a more intrinsic presentation:

Amongst central extensions $\tilde{G} \to G$ equipped with a lifting $\tilde{C}_i$ of each C_i, there is a universal one $\tilde{G}^*$, unique up to unique isomorphism [11, Theorem 7.5.1]. Now consider the central extension $G \times \mathbb{Z}^r \to G$, where we lift C_i to $C_i \times e_i$, where e_i is the ith coordinate vector. This gives a canonical map $\alpha : \tilde{G}^* \to G \times \mathbb{Z}^r$, and we define $H_2(G, C, \nu)_{\mathrm{univ}}$ to be the preimage of $e \times \nu \in G \times \mathbb{Z}^r$.

This is closely related to the previous definition. Note that if we fix lifts $C_i^* \subset \tilde{G}_C$ of each C_i, we get an induced map $\beta : \tilde{G}^* \to \tilde{G}_C$ from the universal property. This induces a bijection $H_2(G, C, \nu)_{\mathrm{univ}}$ with $H_2(G, C)$; indeed, the canonical map

$$\alpha \times_G \beta : \tilde{G}^* \to \tilde{G}_C \times_G (G \times \mathbb{Z}^r)$$

is an isomorphism (again, [11, Theorem 7.5.1]). So a choice of lifts C_i^* give a distinguished element $c_\nu \in H_2(G, C, \nu)_{\mathrm{univ}}$ – the preimage of the identity in $H_2(G, C)$.

Moreover, if we replace C_i^* by $z_i C_i^*$, where $z_i \in H_2(G,C)$, then the associated map $\tilde{G}^* \to \tilde{G}_C$ is multiplied by the composite map $\tilde{G}^* \to \mathbb{Z}^r \to \tilde{G}_C$ where the second map sends $e_i \in \mathbb{Z}^r$ to z_i. Thus, with this replacement, the identification $H_2(G,C,\nu) \xrightarrow{\sim} H_2(G,C)$ has been multiplied by z^{ν_i}; in other words, the distinguished element is replaced by $\prod z_i^{-\nu_i} c_\nu$.

This construction exhibits an identification of torsors

$$H_2(G,C,\nu)_{\text{univ}} \simeq H_2(G,C,\nu)^{-1}, \tag{4.7}$$

where we write $T_1 \simeq T_2^{-1}$ for two A-torsors if there is an identification of T_1 and T_2 transferring the A-action on T_1 to the inverse of the A-action on T_2.

In fact with respect to the identification (4.7), our lifting invariant corresponds to the lifting invariant of [11]: In [11], one takes $(g_1,\ldots,g_r)$ and associates to it the lifting invariant $\Pi = \prod \widetilde{g}_i \in H_2(G,C,\nu)_{\text{univ}}$, where $\widetilde{g}$ is the lift to a universal central extensions equipped with lifting. Fix $\tilde{G}_C$ and C_i^* and a morphism $\tilde{G}^* \to \tilde{G}_C$ as above. Choose $z_i \in H_2(G,C)$ such that the image of Π in $H_2(G,C)$ coincides with $\prod z_i^{\nu_i}$. Then $\prod \widetilde{g}_i$ is carried to $\prod z_i^{\nu_i}$ multiplied by the distinguished element of $H_2(G,C,\nu)_{\text{univ}}$. On the other hand, the lifting invariant as we have defined it above equals $[C_i^* z_i^{-1}] \in H_2(G,C,\nu)$, which equals $\prod z_i^{-\nu_i}$ times the corresponding element of $H_2(G,C,\nu)$.

Now – returning to the surjection $G \to H$ – take a universal extension $\tilde{H}^* \to H$ equipped with a lifting of the D_i, and consider $G \times_H \tilde{H}^* \to G$; it's a central extension and it is equipped with a lifting of C_i, namely, $C_i \times_H D_i^*$. There is thus a canonical map $\tilde{G}^* \to \tilde{H}^*$. Taking fibers above $\nu \in \mathbb{Z}^r$ gives the desired map

$$f_* : H_2(G,C,\nu)_{\text{univ}} \to H_2(H,D,\nu)_{\text{univ}},$$

and by inverting one obtains the desired map $H_2(G,C,\nu) \to H_2(H,D,\nu)$. In particular, one easily verifies that if $H = G$ and $G \to H$ is an inner automorphism, the induced map on $H_2(G,C,\nu)$ is trivial.

Finally, suppose ν is chosen to be simultaneously divisible by the order of $H_2(G,C)$ and $H_2(H,D)$ (i.e., each ν_i is so divisible.) Then in fact the map $H_2(G,C,\nu) \to H_2(H,D,\nu)$ respects the natural identifications of both sides with $H_2(G,C)$ and $H_2(H,D)$ (see after (4.3)). In fact, one has natural identifications

$$H_2(G,C,\nu_1+\nu_2) \simeq H_2(G,C,\nu_1) \times H_2(G,C,\nu_2)/H_2(G,C),$$

where the action of $z \in H_2(G,C)$ on the right is as $z : (t_1,t_2) \mapsto (t_1 z, z^{-1} t_2)$. These identifications are easily seen to be compatible with the map $H_2(G,C,\nu) \to H_2(H,D,\nu)$. Now choose C_i^* and D_i^* as above, giving rise to corresponding elements $c_\nu \in H_2(G,C,\nu)$ and $d_\nu \in H_2(H,D,\nu)$. Write $f_* c_\nu = \gamma_\nu d_\nu$ for some $\gamma_\nu \in H_2(H,D)$; then our comments show that $\gamma_{\nu_1+\nu_2} = \gamma_{\nu_1}\gamma_{\nu_2}$, and the claim follows: if ν is divisible by the order of $H_2(H,D)$, then γ_ν will be trivial.

4.6. **The Conway-Parker theorem.** We will use a result due to Conway and Parker [6] in the important special case where $H_2(G,C)$ is trivial, and described in the paper of Fried and Völklein [12]. See also [11, 15] for further information.

Lemma 4.1. (Conway-Parker theorem) *Consider Hurwitz parameters $h = (G,C,\nu)$ for (G,C) fixed and ν varying. Suppose that all the C_i are distinct. For sufficiently large $\min_i \nu_i$, the lifting invariant map $\mathrm{inv}_h : \pi_0(\mathsf{Hur}_h) \to H_h$ is bijective.*

The Conway-Parker theorem plays a central role in this paper and a number of comments in several categories are in order.

First, the condition that $\min_i \nu_i$ is sufficiently large carries on passively to many of our later considerations. We will repeat it explicitly several times but also refer to it by the word *asymptotically.*

Second, there are a number of equivalent statements. The direct translation of the bijectivity of $\pi_0(\mathsf{Hur}_h) \to H_h$ into group theory is that each fiber of $\mathcal{F}_h \to H_h$ is a single orbit of Br_ν. Statements in the literature often compose the cover $\mathsf{Hur}_h \to \mathsf{Conf}_\nu$ with the cover $\mathsf{Conf}_\nu \to \mathsf{Conf}_n$ and state the result in terms of actions of the full braid group Br_n.

Third, quotienting by $\mathrm{Out}(G, C)$ one gets a similar statement: the resulting map $\mathrm{inv}_h^* : \pi_0(\mathsf{Hur}_h^*) \to H_h^*$ is asymptotically bijective. This is the version that our full-monodromy theorem refines for certain (G, C). Note that a complication not present in Lemma 4.1 itself appears at this level: the cardinality of $\mathcal{H}_h^*$ can be dependent on ν.

5. The full-monodromy theorem

In this section, we state the full-monodromy theorem. Involved in the statement is a homological condition. We clarify the nature of this condition by giving instances when it holds and instances when it fails.

5.1. Preliminary definitions. In this section, we define notions of *pseudosimple*, *unambiguous*, and *quasi-full*. All three of these notions figure prominently in the statement of full-monodromy theorem.

We say that a centerless finite group G is *pseudosimple* if its derived group G' is a power of a nonabelian simple group and any nontrivial quotient group of G is abelian. Thus, there is an extension

$$G' \to G \to G^{\mathrm{ab}} \tag{5.1}$$

where $G' \simeq T^w$, with T nonabelian simple, and the action of G^{ab} on T^w is transitive on the w simple factors. [Our terminology is meant to be reminiscent of similar standard terms for groups closely related to a non-abelian simple group T: *almost simple* groups are extensions $T.A$ contained in $\mathrm{Aut}(T)$ and *quasi-simple* groups are quotients $M.T$ of the Schur cover $\tilde{T}$.]

We say that a conjugacy class C_i in a group G is *ambiguous* if the G' action on C_i by conjugation has more than one orbit. If it has exactly one orbit we say that C_i is *unambiguous*. These are standard notions and for many G the division of classes into ambiguous and unambiguous can be read off from an Atlas page [5].

Essentially repeating a definition from the introduction, we say that the action of a group Γ on a set X is *full* if the image of Γ in $\mathrm{Sym}(X)$ contains the alternating group $\mathrm{Alt}(X)$. Generalizing now, we say the action is *quasi-full* if the image contains $\mathrm{Alt}(X_1) \times \cdots \times \mathrm{Alt}(X_s)$, where the X_i are the orbits of Γ on X. Again we transfer the terminology to a topological setting. Thus a covering of a connected space Y is quasi-full if for any $y \in \mathsf{Y}$, the monodromy action of $\pi_1(\mathsf{Y}, y)$ on X_y is quasi-full.

5.2. Fiber powers of Hurwitz parameters. This subsection describes how a Hurwitz parameter $h = (G, C, \nu)$ and a positive integer k gives a triple $h^k = (G^{[k]}, C^k, \nu)$. Part of this notion, in the special case $k = 2$, appears in the statement of the main theorem. The general notion plays a central role in the proof.

In general, if G is a finite group with abelianization G^{ab} we can consider its k-fold fiber power

$$G^{[k]} = G \times_{G^{\mathrm{ab}}} \cdots \times_{G^{\mathrm{ab}}} G.$$

Note that even when $G = T^w.G^{\mathrm{ab}}$ is pseudosimple, the fiber powers $G^{[k]} = T^{wk}.G^{\mathrm{ab}}$ for $k \geq 2$ are not, because G^{ab} does not act transitively on the factors.

If C_i is a conjugacy class in a group G, we can consider its Cartesian powers $C_i^k \subseteq G^{[k]}$. In general, C_i^k is only a union of conjugacy classes. However if C_i unambiguous then C_i^k is a single class.

If $C = (C_1, \ldots, C_r)$ is a list of conjugacy classes, we can consider the corresponding list $(C_1^k, \ldots, C_r^k)$. Generation of G by the C_i does not imply generation of $G^{[k]}$ by the C_i^k. However if G is pseudosimple then this implication does hold. Thus if G is pseudosimple and C consists only of unambiguous classes, the triple h^k is a Hurwitz parameter.

Suppose, then, that G is pseudosimple and C consists of unambigous classes. The natural map (§4.5)

$$H_2(G^{[k]}, C^k, \nu) \to H_2(G, C, \nu)^k$$

is surjective. This surjectivity can be seen by interpreting both sides in terms of connected components via the Conway-Parker theorem. Alternately, it follows because the map is equivariant with respect to the natural map $H_2(G^{[k]}, C^k) \to H_2(G, C)^k$, which is surjective by homological algebra, as we explain after (5.2).

5.3. **Statement.** With our various definitions in place, we can state the main result of this paper.

Theorem 5.1. (The full-monodromy theorem) *Let G be a finite centerless nonabelian group, let $C = (C_1, \ldots, C_r)$ a list of distinct nonidentity conjugacy classes generating G, and consider Hurwitz parameters $h = (G, C, \nu)$ for varying allowed $\nu \in \mathbb{Z}_{\geq 1}^r$. Then the following are equivalent:*

I:
1. *G is pseudosimple,*
2. *The classes C_i are all unambiguous, and*
3. *$|H_2(G^{[2]}, C^2)| = |H_2(G, C)|^2$.*

II: *The covers $\mathsf{Hur}_h^* \to \mathsf{Conf}_\nu$ are quasi-full whenever $\min_i \nu_i$ is sufficiently large.*

Note that Statement II can equivalently be presented in terms of fullness: for $\min_i \nu_i$ sufficiently large, the covers $\mathsf{Hur}_{h,\ell}^* \to \mathsf{Conf}_\nu$ are full and pairwise nonisomorphic as ℓ ranges over H_h^*. Note also that a pseudosimple group G is simple if and only if G^{ab} is trivial. In this case, Conditions I.2 and I.3 are trivially satisfied and the direction I $\Rightarrow$ II becomes the statement highlighted in §1.2.

For the more important direction I $\Rightarrow$ II, the condition that $\min_i \nu_i$ is sufficiently large is simply inherited from the Conway-Parker theorem. Calculations suggest that quasi-fullness tends to be obtained as soon as it is allowed by the mass formula. We are not pursuing the important question of effectivity here, but we note that effective statements of fullness are obtained for certain classical Hurwitz parameters in [13].

Given (G, C), whether or not Conditions 1 and 2 hold is immediately determinable in practice. Evaluating Condition 3 is harder in general, and the next two subsections are devoted to giving an easily checkable reformulation applicable in many cases (Proposition 5.2) and showing (Corollary 5.3) that it sometimes fails.

5.4. **The homological condition for G of split-cyclic type.** We say that a pseudosimple group G has *split* type if the canonical surjection $\pi : G \to G^{\mathrm{ab}}$ has a section $s : G^{\mathrm{ab}} \to G$. This *a priori* strong condition is actually commonly satisfied. Similarly, we say that a pseudosimple group has *cyclic* type if G^{ab} is cyclic. Again this strong-seeming condition is commonly satisfied, as indeed for a simple group T all of $\mathrm{Out}(T)$ is often cyclic [5]. When both of these conditions are satisfied, we say that G is of *split-cyclic* type.

For G of split-cyclic type, the next proposition says that Condition 3 of Theorem 5.1 is equivalent to an apparent strengthening $\hat{3}$. Moreover these two conditions are both equivalent to a more explicit condition E which makes no reference to either fiber powers or powers. For E, we modify the notions defined in §4.2 as follows:

$$\begin{aligned} H_2'(G)_{C_i} &= \{\langle g, z\rangle : g \in C_i \text{ and } z \in Z(g) \cap G'\}, \\ H_2'(G)_C &= \sum H_2'(G)_{C_i}. \end{aligned}$$

These are straightforward variants, as indeed if one removes every $'$ one recovers definitions (4.1), (4.2) of the previous notions.

Proposition 5.2. *Let G be a pseudosimple group of split-cyclic type and let $C = (C_1, \ldots, C_r)$ be a list of distinct unambiguous conjugacy classes. Then the following are equivalent:*

3: $|H_2(G^{[2]}, C^2)| = |H_2(G, C)|^2$,
$\hat{3}$: $|H_2(G^{[k]}, C^k)| = |H_2(G, C)|^k$ *for all positive integers k,*
E: $H_2(G)_C = H_2'(G)_C$.

Moreover if $|G^{\mathrm{ab}}|$ is relatively prime to $|H_2(G)|$ then all three conditions hold.

Proof. All three conditions involve the list C of conjugacy classes. We begin however with considerations involving G only. The k different coordinate projections $G^{[k]} \to G$ together induce a map $f_k : H_2(G^{[k]}) \to H_2(G)^k$. We first show that the assumption that G has split-cyclic type implies all the f_k are isomorphisms. We present this deduction in some detail because we will return to parts of it in §6.5.

The map f_k is part of a morphism of five-term exact sequences (see [9, Theorem 5.2], noting that $H_1(G') = 0$)

$$\begin{array}{ccccccccc} H_3(G^{[k]}) & \xrightarrow{\pi_3^{[k]}} & H_3(G^{\mathrm{ab}}) & \xrightarrow{\delta^{[k]}} & H_2(G'^k)_{G^{\mathrm{ab}}} & \xrightarrow{i_2^{[k]}} & H_2(G^{[k]}) & \overset{\pi_2^{[k]}}{\twoheadrightarrow} & H_2(G^{\mathrm{ab}}) \\ \downarrow & & \downarrow \Delta_3 & & \downarrow \simeq & & \downarrow f_k & & \downarrow \Delta_2 \\ H_3(G)^k & \xrightarrow{\pi_3^k} & H_3(G^{\mathrm{ab}})^k & \xrightarrow{\delta^k} & H_2(G')^k_{G^{\mathrm{ab}}} & \xrightarrow{i_2^k} & H_2(G)^k & \overset{\pi_2^k}{\twoheadrightarrow} & H_2(G^{\mathrm{ab}})^k. \end{array} \tag{5.2}$$

Each five-term sequence arises from the Hochschild-Serre spectral sequence associated to an exact sequence of groups. The top sequence comes from the k^{th} fiber power of $G' \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} G^{\mathrm{ab}}$, while the bottom sequence comes from the k^{th} ordinary Cartesian power.

We note that (5.2) actually shows that $H_2(G^{[k]}, C^k) \to H_2(G, C)^k$ is surjective whenever G is pseudosimple and C consists of unambiguous classes. The point is that $H_2(G)_C$ surjects onto $H_2(G^{\mathrm{ab}})$. That is because $H_2(G^{\mathrm{ab}})$ is generated by symbols $\langle \alpha, \beta\rangle$. But such a symbol belongs to the image of $H_2(G)_C$, since the $[C_i]$ generate G^{ab} and, for any $g \in C_i$, the centralizer $Z(g)$ surjects to G^{ab} because C_i is unambiguous.

The assumption that $\pi : G \to G^{\mathrm{ab}}$ has a splitting s drastically simplifies (5.2). From $\pi \circ s = \mathrm{Id}_{G^{\mathrm{ab}}}$ one gets that $\pi_3^{[k]} \circ s_3^{[k]}$ and $\pi_3^k \circ s_3^k$ are the identity on $H_3(G^{\mathrm{ab}})$ and $H_3(G^{\mathrm{ab}})^k$ respectively. Thus $\pi_3^{[k]}$ and π_3^k are both surjective and so the boundary maps $\delta^{[k]}$ and δ^k are both 0. Thus the part of (5.2) relevant for us becomes

$$\begin{array}{ccccc} H_2(G'^k)_{G^{\mathrm{ab}}} & \hookrightarrow & H_2(G^{[k]}) & \twoheadrightarrow & H_2(G^{\mathrm{ab}}) \\ \downarrow \simeq & & \downarrow f_k & & \downarrow \Delta_2 \\ H_2(G')^k_{G^{\mathrm{ab}}} & \hookrightarrow & H_2(G)^k & \twoheadrightarrow & H_2(G^{\mathrm{ab}})^k. \end{array} \tag{5.3}$$

We have suppressed some notation, since we have no further use for it.

The assumption that G^{ab} is cyclic is equivalent to the assumption that $H_2(G^{\mathrm{ab}})$ is the zero group. Thus exactly in this situation one gets the independent simplification of (5.2) where the last column becomes the zero map between zero groups. Applied to (5.3) it says that $f_k : H_2(G^{[k]}) \to H_2(G)^k$ is an isomorphism. We henceforth use f_k to identify $H_2(G^{[k]})$ with $H_2(G)^k$.

We now bring in the list C of conjugacy classes. We have a morphism of short exact sequences:

$$\begin{array}{ccccc} H_2(G^{[k]})_C & \hookrightarrow & H_2(G^{[k]}) & \twoheadrightarrow & H_2(G^{[k]}, C^k) \\ \cap\!\!| & & \| & & \twoheaddownarrow \\ H_2(G)^k_C & \hookrightarrow & H_2(G)^k & \twoheadrightarrow & H_2(G, C)^k. \end{array} \tag{5.4}$$

Since the map in the right column is surjective, Conditions 3 and $\hat{3}$ become that it is an isomorphism for $k = 2$ and all k respectively. So they are equivalent to the inclusion in the left column being equality, again for $k = 2$ and all k respectively. We work henceforth with these versions of Conditions 3 and $\hat{3}$.

Trivially

$$|H_2(G)_C| = |H_2'(G)_C| \cdot |H_2(G)_C / H_2'(G)_C| . \tag{5.5}$$

But also the image of $H_2(G^{[k]})_{C^k}$ in $\left(H_2(G)/H_2'(G)_C\right)^k$ is exactly the diagonal image of $H_2(G)_C/H_2'(G)_C$. To see this, note that $H_2(G^{[k]})_{C^k}$ is generated by

$$(\langle g, z_1\rangle, \ldots, \langle g, z_k\rangle)$$

where $g \in \bigcup C_i$, each $z_i \in Z(g)$, and $z_1 \equiv \cdots \equiv z_k$ modulo G'. In particular, it certainly contains the diagonal image of $H_2(G)_C$. On the other hand, the images of $\langle g, z_i\rangle$ inside $H_2(G)_C/H_2'(G)_C$ are equal to each other, since $\langle g, z_i z_j^{-1}\rangle \in H_2'(G)_C$.

Moreover, $H_2'(G)^k_C \subseteq H_2(G^{[k]})_{C^k}$. This inclusion holds because, for any $g \in C_i$ and $z \in Z(g) \cap G'$, we have

$$(\langle g, z\rangle, 0, 0, \ldots) \in H_2(G^{[k]})_{C^k},$$

since we can regard the left-hand side as $(\langle g, z\rangle, \langle g, e\rangle, \langle g, e\rangle, \ldots)$. Similarly for any other "coordinate." Therefore,

$$|H_2(G^{[k]})_{C^k}| = |H_2'(G)_C|^k \cdot |H_2(G)_C / H_2'(G)_C| . \tag{5.6}$$

Dividing the k^{th} power of (5.5) by (5.6), one gets

$$\frac{|H_2(G)_C|^k}{|H_2(G^{[k]})_{C^k}|} = |H_2(G)_C / H_2'(G)_C|^{k-1}. \tag{5.7}$$

Condition 3 says the left side is 1 for $k = 2$. Condition $\hat{3}$ says the left side is 1 for all k. Equation (5.7) says that each of these is equivalent to $H_2(G)_C = H_2'(G)_C$, which is exactly Condition E.

For the final statement, $|H_2(G)_{C_i}/H_2'(G)_{C_i}|$ clearly divides $|H_2(G)|$. It also divides $|G^{\mathrm{ab}}|$, because $Z(g)/(Z(g)\cap G')$ surjects onto $H_2(G)_{C_i}/H_2'(G)_{C_i}$ via $z \in Z(g) \mapsto \langle g, z\rangle$, for any fixed $g \in C_i$. So, if $|H_2(G)|$ and $|G^{\mathrm{ab}}|$ are relatively prime then always $H_2(G)_{C_i} = H_2'(G)_{C_i}$ and so Condition E holds. □

5.5. **The homological condition for G of split-p-p type.** For p a prime, we say that a pseudosimple group G has *split-p-p* type if $G \to G^{\mathrm{ab}}$ is split and

$$|G^{\mathrm{ab}}| = |H_2(G)| = p.$$

Even this seemingly very special case is common. For example, taking $p = 2$, it includes

- all six extensions $T.A$ of sporadic groups T with A and $H_2(T.A)$ non-trivial,
- all S_d with $d \geq 5$, and
- all $PGL_2(q)$ for odd $q \geq 5$.

To illustrate the tractability of Condition E of Proposition 5.2, we work it out explicitly for groups G of split-p-p type. Explicating Condition E for the full split-cyclic case would be similar but combinatorially more complicated.

For G of split-p-p type, we divides its unambiguous classes up into three types. Let $\tilde{G}$ be a Schur cover of G. An unambiguous class C is *split* if its preimage $\tilde{C}$ consists of p conjugacy classes in $\tilde{G}$. It is *mixed* if $\tilde{C}$ is p different $\tilde{G}'$ conjugacy classes but just one $\tilde{G}$ class. Otherwise a class C is *inert*. Mixed classes are necessarily in the derived group, but split and inert classes can lie above any element of G^{ab}.

Corollary 5.3. *Let G be a pseudosimple group of split-p-p type and let $C = (C_1, \ldots, C_r)$ be a list of unambiguous classes. Then Condition E fails exactly when the are no inert classes and at least one mixed class among the C_i.*

Proof. We are considering subgroups of the p-element Schur multiplier $H_2(G)$. The subgroups have the following form

C_i	Split	Mixed	Inert
$H_2'(G)_{C_i}$	0	0	$H_2(G)$
$H_2(G)_{C_i}$	0	$H_2(G)$	$H_2(G)$

Thus $H_2'(G)_C = \sum_i H_2'(G)_{C_i}$ is a proper subgroup of $H_2(G)_C = \sum_i H_2(G)_{C_i}$ exactly under the conditions stated in the corollary. □

For a group $T.p$, the types of classes can be determined from an Atlas-style character table, including its lifting row and fusion column. For example, for the six sporadic T mentioned above, the mixed classes in $T.2$ are exactly as follows:

Mathieu$_{12}$	Mathieu$_{22}$	Hall-Janko	Higman-Sims	Suzuki	Fischer$_{22}$
$10A$	$8A$	$8A$	$4A, 6A, 12A$	$12D, 12E, 24A$	(15 classes)

In the sequences S_d and $PGL_2(q)$, the patterns evident from character tables in the first few instances can be proved to hold in general. Namely for S_d, conjugacy classes are indexed by partitions of d. The type of a class C_λ can be read off from two features of the indexing partition λ, the number e of even parts and whether or not all parts are distinct:

	$e = 0$	$e \in \{2, 4, 6, \ldots\}$	$e \in \{1, 3, 5, \ldots\}$
All distinct	Ambiguous	Mixed	Split
Not all distinct	Split	Inert	Inert

Thus S_5 has no mixed classes while C_{42} and C_{421} are the unique mixed classes of S_6 and S_7 respectively. For $PGL_2(q)$, the division is even easier: the two classes of order the prime dividing q are ambiguous, the two classes of order 2 are inert, and all other classes are split. Thus for $PGL_2(q)$, the homological condition always holds.

6. Proof of I $\Rightarrow$ II

In this section we prove the implication I $\Rightarrow$ II of Theorem 5.1. Thus we consider Hurwitz parameters $h = (G, C, \nu)$ for fixed (G, C) satisfying Conditions 1-3 and varying ν. We then prove that the action of Br_ν on $\mathcal{F}_h^*$ is quasi-full whenever $\min_i \nu_i$ is sufficiently large. The implication I $\Rightarrow$ II is the part of Theorem 5.1 which provides theoretical support for Conjecture 1.1.

6.1. **A Goursat Lemma.** The classical Goursat lemma classifies certain subgroups of powers of a simple group. We state and prove a generalized version here. As usual, if one has groups G_1, G_2 endowed with homomorphisms π_1, π_2 to a third group Q, we say that G_1 and G_2 are isomorphic *over* Q if there is an isomorphism $i : G_1 \to G_2$ satisfying $\pi_2 i = \pi_1$.

Lemma 6.1. (Generalized Goursat lemma) *Suppose that G is pseudosimple, and $H \subseteq G^{[k]}$ is a "Goursat subgroup" in the sense that it surjects onto each coordinate factor. Then*

1: *H is itself isomorphic over G^{ab} to $G^{[w]}$ for some $w \leq k$.*
2: *There is a surjection $f : [1, k] \to [1, w]$ and automorphisms $\varphi_1, \ldots, \varphi_k$ of G over G^{ab} such that H is the image of $G^{[w]}$ under*

$$(g_1, \ldots, g_w) \mapsto (\varphi_1(g_{f(1)}), \ldots, \varphi_k(g_{f(k)})).$$

Proof. We first prove Statement 1 by induction, the base case $k = 1$ being trivial. Note that the projection $\bar{H} = \pi_2(H)$ of H to the second factor in

$$G^{[k]} = G \times_{G^{\mathrm{ab}}} G^{[k-1]}$$

is also a Goursat subgroup. By induction, it is G^{ab}-isomorphic to $G^{[v]}$ for suitable v. The kernel $K = \ker(\pi_2)$ of the projection $H \to \bar{H}$ maps, under the first projection π_1, to a subgroup $\bar{K} \subseteq G'$ that is invariant under conjugation by G. In particular, either $\bar{K}$ is trivial, and we're done by induction, or $\bar{K} = G'$. In the latter case, we will show that $H = G \times_{G^{\mathrm{ab}}} \bar{H}$: Take any element $(m^*, \mu) \in G \times_{G^{\mathrm{ab}}} \bar{H}$. By assumption there exists m in G such that $(m, \mu) \in H$; but then m and m^* have the same projection to G^{ab}, and so

$$(m^*, \mu) = (m^* m^{-1}, 1) \cdot (m, \mu)$$

lies in H also. This concludes the proof of the first assertion: H is isomorphic to $G^{[w]}$ over G^{ab} for some w.

Now we deduce Statement 2 from Statement 1. Let $\Theta = G^{[w]} \to H$ be any isomorphism and write $\Theta(g) = (\theta_1(g), \ldots, \theta_k(g))$. We need to show that for each i, one can express $\theta_i(g)$ in the form $\varphi_i(g_{f(i)})$ as in Statement 2. In other words, letting $\pi_j : G^{[w]} \to G$ be the j^{th} projection, we need to show that any surjective morphism $\theta : G^{[w]} \to G$ over G^{ab} factors as $\varphi \pi_j$ for some $j \in \{1, \ldots, w\}$ and some automorphism $\varphi : G \to G$ over G^{ab}.

So let $\theta : G^{[w]} \to G$ be any surjective morphism over G^{ab}. Its kernel K is a normal subgroup of $(G')^w$, invariant under $G^{[w]}$, and with index $|G'|$. Now, via $G' \simeq T^u$ for some nonabelian simple group T, the normal subgroups of $(G')^w \simeq T^{uw}$ are of the form $T_I = \prod_{(i,j)\in I} T_{(i,j)}$, where I is a subset of $P = \{1, \ldots, u\} \times \{1, \ldots, w\}$. The normal subgroups which are invariant under G^w are those for which the indexing set I is invariant under the natural action of G^{ab}. The orbits of G^{ab} on P are the sets $P_j = \{1, \ldots, u\} \times \{j\}$. So the kernel K of θ necessarily has the form T_{P-P_j}. Thus K is also the kernel of the coordinate projection π_j. The unique bijection $\varphi : G \to G$ satisfying $\theta = \varphi\pi_j$ is then an automorphism of G over G^{ab}. $\square$

6.2. **Identifying braid orbits.** For F a set and k a positive integer we let

$$F^{\underline{k}} = \{(x_1, \ldots, x_k) : \text{all } x_i \text{ are different}\}.$$

If F has cardinality N then $F^{\underline{k}}$ has cardinality $N^{\underline{k}} := N(N-1)\cdots(N-k+1)$. In this subsection we assume Conditions 1 and 2 and identify the quotient set $(\mathcal{F}_h^*)^{\underline{k}}/\mathrm{Br}_\nu$ asymptotically.

Begin with $x_1, \ldots, x_k \in \mathcal{F}_h^*$. Choose a set of representatives $\underline{g}_1, \ldots, \underline{g}_k \in \mathcal{G}_h$. Writing each $\underline{g}_i$ as a column vector, we get a matrix

$$(\underline{g}_1, \ldots, \underline{g}_k) = \begin{pmatrix} g_{11} & g_{21} & \cdots & g_{k1} \\ g_{12} & g_{22} & \cdots & g_{k2} \\ g_{13} & g_{23} & \cdots & g_{k3} \\ \vdots & \vdots & \vdots & \vdots \\ g_{1n} & g_{2n} & \cdots & g_{kn} \end{pmatrix}. \tag{6.1}$$

So, simply recalling our context:

- All the g_{ij} in in a given row are in the same conjugacy class of G.
- These conjugacy classes are $\overbrace{C_1, \ldots, C_1}^{\nu_1}; \ldots; \overbrace{C_r, \ldots, C_r}^{\nu_r}$ as one goes down the rows, so that a given row is in some C_i^k.
- Each column in its given order multiplies to 1.
- Each column generates all of G.

All entries in a given row certainly have the same projection to G^{ab} and so each row defines an element of $G^{[k]}$. Consider now the subgroup H of $G^{[k]}$ generated by the rows of this matrix. We are going to show that

$$H = G^{[k]} \iff (\text{all } x_i \text{ are different}). \tag{6.2}$$

First of all, note that the condition that $H = G^{[k]}$ is independent of the choice of lifting from $\mathcal{F}_h^*$ to $\mathcal{G}_h$. For example, if we modify the $\underline{g}_1$, the first column of (6.1), by an element $\alpha \in \mathrm{Aut}(G, C)$, then the subgroup generated by the rows simply changes by the automorphism $(\alpha, 1, 1, 1 \ldots, 1)$ of $G^{[k]}$. Note that α is automatically an isomorphism of G over G^{ab} because it preserves each C_i and they generate G^{ab}.

Now direction $\Longrightarrow$ of (6.2) is easy: if $x_i = x_j$ for some $i \neq j$ then we could lift so that $\underline{g}_i = \underline{g}_j$, and then certainly $H \subsetneq G^{[k]}$.

Now suppose that $x_i \neq x_j$ for all $i \neq j$; we'll show that $H = G^{[k]}$. Since each column generates G, the subgroup H is a Goursat subgroup of $G^{[k]}$. Accordingly we may apply Lemma 6.1, and see that H can be constructed from a surjective function $f : [1, k] \to [1, w]$ together with a system of isomorphisms $\varphi_j : G \to G$ over G^{ab}, for $1 \leq j \leq k$. In particular, we may find $(y_1, \ldots, y_w) \in G^{[w]}$ which maps to the first row $(g_{11}, g_{21}, \ldots, g_{k1})$, so that

$$\varphi_j(y_{f(j)}) = g_{j1}, \quad 1 \leq j \leq k.$$

In particular, whenever $f(j) = f(j')$, the map

$$\varphi_{j'}\varphi_j^{-1}$$

carries g_{j1} to $g_{j'1}$ and so preserves C_1. By similar reasoning, applied to the second row, third row and so on, this map preserves *every* conjugacy class, so

$$\varphi_{j'}\varphi_j^{-1} \in \mathrm{Aut}(G, C)$$

whenever $f(j) = f(j')$. But $\varphi_{j'}\varphi_j^{-1}$ carries g_{ji} to $g_{j'i}$; that means that actually $x_j = x'_j$, and so $j = j'$. In other words, f is injective, and so $H \simeq G^{[k]}$ as desired.

Each matrix (6.1) with H all of $G^{[k]}$ defines an element of $\mathcal{G}_{h^k}$. Now, the group $\mathrm{Aut}(G, C)^k$ acts on $G^{[k]}$; its image in the outer automorphism group will be called $\mathrm{Out}(G, C)^{[k]}$. This latter group maps onto $\mathrm{Out}(G, C)^k$, with kernel isomorphic to $(G^{\mathrm{ab}})^{k-1}$. Our considerations have given a bijective map

$$\mathcal{F}_{h^k}/\mathrm{Out}(G, C)^{[k]} \xrightarrow{\sim} \mathcal{F}_h^{*\underline{k}}. \tag{6.3}$$

This bijection is purely algebraic in nature and valid for all ν.

Lifting invariants give a map $\mathcal{F}_{h^k}/\mathrm{Br}_\nu \to H_2(G^{[k]}, C^k, \nu)$. For any fixed k, the Conway-Parker theorem says that this map is asymptotically a bijection. Taking the quotient by $\mathrm{Out}(G, C)^{[k]}$ and incorporating the Goursat conclusion (6.3) we get the desired description of braid orbits:

$$\mathcal{F}_h^{*\underline{k}}/\mathrm{Br}_\nu \xrightarrow{a\sim} H_2(G^{[k]}, C^k, \nu)/\mathrm{Out}(G, C)^{[k]}. \tag{6.4}$$

The map of (6.4) is defined for all allowed ν and, as indicated by the notation $a\sim$, is asymptotically a bijection.

There is, of course, a map $\mathcal{F}_h^{*\underline{k}}/\mathrm{Br}_\nu \to (\mathcal{F}_h^*/\mathrm{Br}_\nu)^k$; on the right-hand side of (6.4), this corresponds to the natural map

$$H_2(G^{[k]}, C^k, \nu)/\mathrm{Out}(G, C)^{[k]} \to \left(H_2(G, C, \nu)/\mathrm{Out}(G, C)\right)^k. \tag{6.5}$$

Note that the action of $\mathrm{Out}(G, C)^{[k]}$ on $H_2(G^{[k]}, C^k, \nu)$ factors, under the coordinate projection $H_2(G^{[k]}, C^k, \nu) \to H_2(G, C, \nu)$, through the corresponding coordinate projection $\mathrm{Out}(G, C)^{[k]} \to \mathrm{Out}(G, C)$.

6.3. **End of the proof of I $\Rightarrow$ II in the split-cyclic case.** We now assume not only Conditions 1 and 2 of I, but also Condition 3. In this subsection, we complete the proof of I $\Rightarrow$ II under the auxiliary assumption that the surjection $G \to G^{\mathrm{ab}}$ is split and G^{ab} is cyclic. Some of the notions introduced here are used again in the §6.5, where we complete the proof without auxiliary assumptions.

Consider the canonical surjections $H_2(G^{[k]}, C^k, \nu) \twoheadrightarrow H_2(G, C, \nu)^k$. Under our auxiliary assumption that G has split-cyclic type, Condition 3 and Proposition 5.2 show that

$$|H_2(G^{[k]}, C^k)| = |H_2(G, C)|^k$$

for all k. Thus, since cardinality does not change when one passes from groups to torsors, the surjections are bijections. Moreover, because inner automorphisms act trivially on $H_2(G, C, \nu)$, the action of $\mathrm{Out}(G, C)^{[k]}$ on $H_2(G, C, \nu)^k$ actually factors through $\mathrm{Out}(G, C)^k$.

Taking the quotient by $\mathrm{Out}(G, C)^{[k]}$, we can rewrite (6.4) as

$$\mathcal{F}_h^{*\underline{k}}/\mathrm{Br}_\nu \xrightarrow{a\sim} H_2^*(G, C, \nu)^k. \tag{6.6}$$

Then standard group theory shows that the action of Br_ν on $\mathcal{F}_h^*$ is quasi-full for sufficiently large $\min_i \nu_i$:

In general, consider a permutation group $B \subseteq \mathrm{Sym}(F)$ with orbit decomposition $F = \coprod_{i=1}^s F_i$. Suppose each orbit F_i has size at least k. Then the induced action of B on $F^{\underline{k}}$ has at least s^k orbits. If equality holds, then the images $B_i \subseteq \mathrm{Sym}(F_i)$ of B are each individually k-transitive. If $k \geq 6$, then the classification of finite simple groups says that B_i contains $\mathrm{Alt}(F_i)$. Still assuming that B has exactly s^k orbits on $F^{\underline{k}}$, it is then elementary that B contains $\mathrm{Alt}(F_1) \times \cdots \times \mathrm{Alt}(F_s)$.

6.4. **A lemma on 2-transitive groups.** For the general case, Condition 3 gives us control over Br_ν-orbits only on pairs (x_1, x_2) of distinct elements in $\mathcal{F}_h^*$, not tuples of larger length. To deal with this problem, we replace the classification of multiply-transitive groups by a statement derived from the classification of 2-transitive groups. The exact formulation of our lemma is inessential; its import is that full groups are clearly separated out from other 2-transitive groups in a way sufficient for our purpose.

Lemma 6.2. *Fix an odd integer $j \geq 5$. Suppose a 2-transitive group $\Gamma \subseteq \mathrm{Sym}(X)$ satisfies $|X^{\underline{2j}}/\Gamma| \leq 2^{j^2-4j}$. If $|X|$ is sufficiently large, then Γ is full.*

Proof. To prove the statement, we use the classification of non-full 2-transitive groups, as presented in [7, §7.7], thereby breaking into a finite number of cases. For fixed j, we discard in each case a finite number of Γ and otherwise establish $|X^{\underline{2j}}/\Gamma| > 2^{j^2-4j}$.

It suffices to restrict attention to maximal non-full 2-transitive groups Γ. Besides a small number of examples involving seven of the sporadic groups [7, p.252-253], every such maximal Γ occurs on the following table.

#	Type	Γ	Degree N	Order $\lvert\Gamma\rvert$
1	Affine	$AGL_d(p)$	p^d	
2	Projective	$P\Gamma L_d(q)$	$(q^d-1)/(q-1)$	
3	OS2	$O_{2d+1}(2)$	$2^d(2^d \pm 1)/2$	
4	Unitary	$U_3(q)$	q^3+1	$q^3(q^2-1)(q^3+1)$
5	Suzuki	$Sz(q)$	q^2+1	$(q^2+1)q^2(q-1)$
6	Ree	$R(q)$	q^3+1	$(q^3+1)q^3(q-1)$

The six series are listed in the order they are treated in [7, p.244-252]. Throughout, p is a prime number and $q = p^e$ is a prime power. These numbers are arbitrary, except in Cases 5 and 6 where the base is $p = 2$ and $p = 3$ respectively and the exponent e is odd. The orders $|\Gamma|$ in Cases 1-3 are not needed in our argument and so are omitted from the table.

Cases 4-6. In these cases, the order $|\Gamma|$ grows only polynomially in the degree N, with $|\Gamma| < N^3$ holding always. One has

$$|X^{\underline{2j}}/\Gamma| \geq N^{\underline{2j}}/|\Gamma| > N^{\underline{2j}}/N^3.$$

For $j \geq 5$ fixed and $N \to \infty$, the right side tends to ∞. So, with finitely many exceptions, $|X^{\underline{2j}}/\Gamma| > 2^{j^2-4j}$.

Case 1. In this case, the affine general linear group $AGL_d(\mathbb{F}_p)$ acts on the affine space $\mathbb{F}_p^d$. Let $w = \min(j, d+1)$. Fix $x_1, \ldots, x_w$ in $\mathbb{F}_p^d$ spanning an affine subspace A of dimension $w-1$. The set $A - \{x_1, \ldots, x_w\}$ has $p^{w-1} - w$ elements. There are $(p^{w-1} - w)^{\underline{2j-w}}$ ways to successively choose $x_{w+1}, \ldots, x_{2j}$ in A so that all the x_i are distinct. The tuples $(x_1, \ldots, x_{2j}) \in (\mathbb{F}_p^d)^{\underline{2j}}$ so obtained are in different $AGL_d(\mathbb{F}_p)$ orbits. Thus

$$|(\mathbb{F}_p^d)^{\underline{2j}}/AGL_d(\mathbb{F}_p)| \geq \left(p^{w-1} - w\right)^{\underline{2j-w}}.$$

For fixed $d < j$, so that $w = d+1$, the right side tends to ∞ with p, and so with finitely many exceptions, $|(\mathbb{F}_p^d)^{\underline{2j}}/AGL_d(\mathbb{F}_p)| > 2^{j^2-4j}$. For $d \geq j$, so that $w = j$, one gets no exceptions, as

$$\left(p^{w-1} - w\right)^{\underline{2j-w}} = \left(p^{j-1} - j\right)^{\underline{j}} \geq \left(2^{j-1} - j\right)^{\underline{j}} \geq \left(2^{j-1} - 2j + 1\right)^{j} > 2^{j^2-4j}.$$

[Case 1 is the only case where there is a complicated list of non-maximal 2-transitive groups. Some large ones are $AGL_{d/e}(\mathbb{F}_{p^e}) \subset A\Gamma L_{d/e}(\mathbb{F}_{p^e}) \subset AGL_d(p)$, for any e properly dividing d.]

Cases 2 and 3 are very similar to Case 1, but sufficiently different to require separate treatments.

Case 2. Here $\Gamma = P\Gamma L_d(\mathbb{F}_q) = PGL_d(\mathbb{F}_q).\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acts on the projective space $X = \mathbb{P}^{d-1}(\mathbb{F}_q)$. Again let $w = \min(j, d+1)$. Fix $x_1, \ldots, x_w$ in $\mathbb{P}^{d-1}(\mathbb{F}_q)$ spanning a projective subspace P of dimension $w-1$. Similarly to Case 1, there are $((q^w-1)/(q-1) - w)^{\underline{2j-w}}$ ways to successively choose $x_{w+1}, \ldots, x_{2j}$ in P so that all the x_i are distinct. The tuples $(x_1, \ldots, x_{2j}) \in \mathbb{P}^{d-1}(\mathbb{F}_q)^{\underline{2j}}$ so obtained are in different $PGL_d(\mathbb{F}_q)$ orbits. However one $P\Gamma L_d(\mathbb{F}_q)$ orbit can consist of up to e different $PGL_d(\mathbb{F}_q)$ orbits. Thus our lower bound in this case is

$$|\mathbb{P}^{d-1}(\mathbb{F}_q)^{\underline{2j}}/P\Gamma L_d(\mathbb{F}_q)| \geq \frac{1}{e}\left(\frac{q^w-1}{q-1} - w\right)^{\underline{2j-w}}.$$

Again the subcase $d < j$, where $w = d+1$, is simple: the right side tends to ∞ with q and so $|\mathbb{P}^{d-1}(\mathbb{F}_q)^{\underline{2j}}/P\Gamma L_d(\mathbb{F}_q)| > 2^{j^2-4j}$ holds with only finitely many exceptions. For $d \geq j$, so that $w = j$ again, one has no further exceptions as

$$\frac{1}{e}\left(\frac{q^w-1}{q-1} - w\right)^{\underline{2j-w}} > \frac{1}{e}\left(q^{j-1} - 2j + 1\right)^{j} > \left(2^{j-1} - 2j + 1\right)^{j} > 2^{j^2-4j}.$$

Case 3. Here the group in question in its most familiar guise is $\Gamma = Sp_{2d}(\mathbb{F}_2)$ for $d \geq 2$. It is better in our context to view $\Gamma = O_{2d+1}(\mathbb{F}_2)$, as from this point of view the 2-transitive actions appear most naturally. In fact the orbit decomposition of the natural action of $O_{2d+1}(\mathbb{F}_2)$ is

$$\mathbb{F}_2^{2d+1} - \{0\} = X_{-1} \coprod X_1 \coprod X_0.$$

Here X_0 is the set of isotropic vectors. The pair $(O_{2d+1}(\mathbb{F}_2), X_0)$ is a copy of the more standard pair $(Sp_{2d}(\mathbb{F}_2), \mathbb{F}_2^{2d} - \{0\})$ and so in particular $|X_0| = 2^{2d} - 1$. A non-isotropic vector is in X_1 if its stabilizer is the split orthogonal group $O_{2d}^+(\mathbb{F}_2)$ and is in X_{-1} if its stabilizer is the non-split orthogonal group $O_{2d}^-(\mathbb{F}_2)$. From the order of the stabilizers one gets that $|X_\epsilon| = 2^{d-1}(2^d + \epsilon)$. While the action of Γ on $X_0^{\underline{2}}$ has two orbits, the actions on the other two X_ϵ are 2-transitive. [Familiar examples for $O_{2d+1}(\mathbb{F}_2) = Sp_{2d}(\mathbb{F}_2)$ come from $d = 2$, and $d = 3$. Here the groups respectively are S_6, and $W(E_7)$. The orbit sizes on (X_{-1}, X_1, X_0) are $(6, 10, 15)$ and $(28, 36, 63)$ respectively.]

By discarding a finite number of Γ, we can assume $d \geq j$. Fix $x_1, \ldots, x_j$ in X_ϵ spanning a j-dimensional vector space $V \subset \mathbb{F}_2^{2d+1}$ on which the quadratic form remains non-degenerate and each x_i has type ϵ in this smaller space. Let

$V_\epsilon = V \cap X_\epsilon$. Writing $j = 2u+1$, one has $|V_\epsilon| = 2^{u-1}(2^u+\epsilon)$. There are $(|V_\epsilon| - j)^{\underline{j}}$ ways to successively choose $x_{j+1}, \ldots, x_{2j}$ in V_ϵ so that all the x_i are distinct. One has

$$|X_\epsilon^{\underline{2j}}/O_{2d+1}(\mathbb{F}_2)| \geq \left(2^{u-1}(2^u+\epsilon) - j\right)^{\underline{j}} \geq \left(2^{u-1}(2^u+\epsilon) - 2j + 1\right)^j > 2^{j^2-4j}.$$

Thus there are no further exceptional Γ from this case. $\square$

6.5. **End of the proof if I $\Rightarrow$ II in general.** We now end the proof without the split-cyclicity assumption, by modifying the standard argument of §6.3.

Consider again the diagram (5.2) relating two five-term exact sequences. The last three terms of the top sequence and the last four terms of the bottom sequence give respectively

$$\begin{aligned} |H_2(G^{[k]})| &\leq |H_2(G')_{G^{\mathrm{ab}}}|^k |H_2(G^{\mathrm{ab}})|, \\ |H_2(G')_{G^{\mathrm{ab}}}|^k &\leq \frac{|H_3(G^{\mathrm{ab}})|^k |H_2(G)|^k}{|H_2(G^{\mathrm{ab}})|^k}. \end{aligned}$$

Combining these inequalities and replacing $H_2(G^{[k]})$ by its quotient $H_2(G^{[k]}, C^k)$ yields

$$|H_2(G^{[k]}, C^k)| \leq |H_2(G) \times H_3(G^{\mathrm{ab}})|^k. \tag{6.7}$$

As described in §6.3, Condition 3 implies that for $\min \nu_i$ sufficiently large, the action of Br_ν on $\mathcal{F}_h^*$ is 2-transitive when restricted to each orbit. We will use this 2-transitivity and the exponential bound (6.7) to conclude that the action of Br_ν on $\mathcal{F}_h^*$ is asymptotically quasi-full.

Consider S_m in its standard full action on $Y_m = \{1, \ldots, m\}$. The induced action on $X_m = Y_m \coprod Y_m$ is not quasi-full. Let $a_{k,m}$ be the number of orbits of S_m on $Y_m^{\underline{k}}$. As m increases the sequence $a_{k,m}$ stabilizes at a number a_k. The sequence a_k appears in [17] as A000898. There are several explicit formulas and combinatorial interpretations. The only important thing for us is that a_k grows superexponentially, as indeed $a_k/a_{k-1} \sim \sqrt{2k}$.

From (6.7) we know that there exists an odd number j with

$$|H_2(G^{[2j]}, C^{2j}, \nu)/\mathrm{Out}(G,C)^{[2j]}| \leq |H_2(G^{[2j]}, C^{2j})| < \min(2^{j^2-4j}, a_{2j}).$$

By (6.4), the left-hand set is identified with $|\mathcal{F}_h^{*\underline{2j}}/\mathrm{Br}_\nu|$ for sufficiently large $\min_i \nu_i$. Lemma 6.2 above says that, at the possible expense of making $\min_i \nu_i$ even larger, each orbit of the action of Br_ν on $\mathcal{F}_h^*$ is full. Our discussion of the action of S_m on Y_m says that the constituents are pairwise non-isomorphic, again for sufficiently large $\min_i \nu_i$. The classical Goursat lemma then says the action is quasi-full. $\square$

A consequence of the results of the section is that in fact the equivalence $3 \Leftrightarrow \hat{3}$ of Proposition 5.2 holds without the assumption of split-cyclicity. Condition E is also meaningful in general, and it would be interesting to identify the class of (G,C) for which the equivalence extends to include E.

7. Proof of II $\Rightarrow$ I

In this section, we complete the proof of Theorem 5.1 by proving that (not I) implies (not II). Accordingly, we fix a centerless group G and a list $C = (C_1, \ldots, C_r)$ of conjugacy classes and consider consequences of the failure of Conditions 1, 2, and 3 in turn. In all three cases, we show more than is needed for Theorem 5.1.

7.1. **Failure of Condition 1.** The failure of the first condition requires a somewhat lengthy analysis, because it breaks into two quite different cases. The conclusion of the following lemma shows more than asymptotic quasi-fullness of $\mathsf{Hur}_h^* \to \mathsf{Conf}_\nu$ fails; it shows that asymptotically each individual component $\mathsf{Hur}_{h,\ell}^* \to \mathsf{Conf}_\nu$ fails to be full.

Lemma 7.1. *Let G be a centerless group which is not pseudosimple. Let $C = (C_1, \ldots, C_r)$ be a list of conjugacy classes. Consider varying allowed $\nu \in \mathbb{Z}_{\geq 1}^r$ and thus varying Hurwitz parameters $h = (G, C, \nu)$. Then for $\min_i \nu_i$ sufficiently large and any $\ell \in H_h^*$, the action of Br_ν on $\mathcal{F}_{h,\ell}^*$ is not full.*

Proof. A group is pseudosimple exactly when it satisfies two conditions: A, it has no proper nonabelian quotients; B, its derived group is nonabelian. We assume first that A fails. Then we assume that A holds but B fails.

Assume A fails. Let $\overline{G}$ be a proper nonabelian quotient. Let $\bar{h} = (\overline{G}, (\overline{C}_1, \ldots, \overline{C}_r), \nu)$ be the corresponding quotient Hurwitz parameter. Consider the natural map $H_h \to H_{\bar{h}}$ from §4.5 and let $\bar{\ell}$ be the image of ℓ.

By the definition of Hurwitz parameter, the classes C_i generate G. At least one of the surjections $C_i \to \overline{C}_i$ has to be non-injective, as otherwise the kernel of $G \to \overline{G}$ would be central in G and G is centerless. So $|C_i| \geq 2|\overline{C}_i|$ for at least one i. Similarly, since $\overline{G}$ is nonabelian and generated by the $\overline{C}_i$, one has $|\overline{C}_i| \geq 2$ for at least one i.

We now examine the induced map $\mathcal{G}_{h,\ell} \to \mathcal{G}_{\bar{h},\bar{\ell}}$. Let $\mathcal{I}_{h,\ell}$ be its image and $\phi_{h,\ell}$ be the size of its largest fiber. We will use the two inequalities of the previous paragraph to show that both $\phi_{h,\ell}$ and $|\mathcal{I}_{h,\ell}|$ grow without bound with $\min_i \nu_i$.

From $|C_i| \geq 2|\overline{C}_i|$ and two applications of the asymptotic mass formula (3.7), one gets $|\mathcal{G}_{h,\ell}| \geq 1.5^{\min_i \nu_i} |\mathcal{G}_{\bar{h},\bar{\ell}}|$ and hence $\phi_{h,\ell} \geq 1.5^{\min_i \nu_i}$.

To show the growth of $|\mathcal{I}_{h,\ell}|$, we assume without loss of generality that $|\overline{C}_1| \geq 2$ and choose $y_1 \neq y_2 \in \overline{C}_1$. Let M be the exponent of a reduced Schur cover $\tilde{G}_C$ of G. Let k be a positive integer and let $a_1, \ldots, a_k$ be a sequence with $a_i \in \{1, 2\}$. Then for $\min_i \nu_i$ large enough, we claim that $\mathcal{I}_{h,\ell}$ contains an element of the form

$$(\underbrace{y_{a_1}, \ldots, y_{a_1}}_{M}, \ldots, \underbrace{y_{a_k}, \ldots, y_{a_k}}_{M}, \underbrace{x_1, \ldots, x_{\nu_1 - Mk}}_{\text{all in } \overline{C}_1}, \ldots, \underbrace{x_{n-kM-\nu_r+1}, \ldots, x_{n-kM}}_{\text{all in } \overline{C}_r}). \tag{7.1}$$

To see the existence of such an element, fix a lift C_i^* of the conjugacy class C_i to $\tilde{G}_C$ and choose $\tilde{y}_1, \tilde{y}_2 \in C_1^*$ mapping (under $\tilde{G}_C \to G \to \bar{G}$) to $y_1, y_2 \in \overline{C}_1$ respectively.

Let $z \in H_2(G, C)$ be chosen so that $z^{-1} \cdot \prod_i [C_i]^{\nu_i} = \ell$ inside $H_2(G, C, \nu)$. Consider the equation

$$(\tilde{y}_{a_1}^M \cdots \tilde{y}_{a_k}^M) \underbrace{\tilde{x}_1 \cdots \tilde{x}_{\nu_1 - kM}}_{\text{all in } C_1^*} \cdots \underbrace{\tilde{x}_{n-kM-\nu_r+1} \cdots \tilde{x}_{n-kM}}_{\text{all in } C_r^*} = z, \tag{7.2}$$

where $\tilde{x}_i \in C_i^*$. By our choice of M, the powers $\tilde{y}_{a_i}^M$ are all the identity in $\tilde{G}_C$. One has $[C_1^*]^{\nu_1 - kM} \cdots [C_r^*]^{\nu_r} = [z]$ in $\tilde{G}_C^{\mathrm{ab}} = G^{\mathrm{ab}}$, both sides being the identity. The asymptotic mass formula then applies to say that (7.2) in fact has many solutions $(\tilde{x}_1, \ldots, \tilde{x}_{n-kM})$ where moreover $\tilde{x}_i$ generate $\tilde{G}_C$. Now, the image of $(\tilde{y}_{a_1}, \ldots, \tilde{y}_{a_k}, \tilde{x}_1, \ldots, \tilde{x}_{n-kM})$ actually defines an element of $\mathcal{G}_{h,\ell}$, and its image in $\bar{G}$ is an element of $\mathcal{I}_{h,\ell}$ of the form (7.1). Varying $(a_1, \ldots, a_k)$ now, always taking $\min_i \nu_i$ sufficiently large, we conclude $|\mathcal{I}_{h,\ell}| \geq 2^k$.

For large enough $\min_i \nu_i$ the action of Br_ν on $\mathcal{G}_{h,\ell}$ is transitive, by the Conway–Parker theorem. This action preserves a partition of $\mathcal{G}_{h,\ell}$ into $b = |\mathcal{I}_{h,\ell}|$ blocks, each of size $f = \phi_{h,\ell}$. Thus the image of Br_ν on $\mathcal{G}_{h,\ell}$ is contained in the wreath product $S_f \wr S_b$. Hence the image of Br_ν on $\mathcal{F}^*_{h,\ell}$ is contained in a subquotient of $S_f \wr S_b$. But we have established that f and b increase indefinitely with $\min_i \nu_i$. Let $a = |\mathrm{Aut}(G,C)_\ell|$ and $m = |\mathcal{F}^*_{h,\ell}|$ so that $|\mathcal{G}_{h,\ell}| = ma = fb$. As soon as $\min(f,b) > a$, one has $m > \max(f,b)$ and the alternating group A_m is not a subquotient of $S_f \wr S_b$. So the action of Br_ν on $\mathcal{F}^*_{h,\ell}$ is not full.

Assume A holds but B fails. The assumptions force G' to be isomorphic to the additive group of $\mathbb{F}_p^w$ for some prime p and some power w. Moreover, consider the action of G^{ab} on G'. Now G', considered as an $\mathbb{F}_p$-vector space, is an irreducible representation of $\mathbb{F}_p[G^{\mathrm{ab}}]$. G^{ab} must have order coprime to p, as otherwise the fixed subspace for the p-primary part of G^{ab} would be a proper subrepresentation. So $\mathbb{F}_p[G^{\mathrm{ab}}]$ is isomorphic to a sum of finite fields and the action on $G' = \mathbb{F}_p^w$ is through a single summand $\mathbb{F}_q$. We can thus identify G' with the additive group of a finite field $\mathbb{F}_q$ and G^{ab} with a subgroup of $\mathbb{F}_q^\times$ in such a way that G itself is a subgroup of the affine group $\mathbb{F}_q.\mathbb{F}_q^\times$. Moreover, $G^{\mathrm{ab}} \subseteq \mathbb{F}_q^\times$ acts irreducibly on $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space.

We think of elements of G as affine transformations $x \mapsto mx + b$. Since braid groups act on the right in (3.2), we compose these affine transformation from left to right, so that the group law is $\binom{m_1}{b_1}\binom{m_2}{b_2} = \binom{m_1 m_2}{m_2 b_1 + b_2}$.

We think of elements $(g_1, \ldots, g_n) \in \mathcal{G}_h$ with $g_i = \binom{m_i}{b_i}$ in terms of the following matrix:

$$\begin{bmatrix} m_1 & \cdots & m_i & m_{i+1} & \cdots & m_n \\ b_1 & \cdots & b_i & b_{i+1} & \cdots & b_n \end{bmatrix} \tag{7.3}$$

The top row is determined by C, via $m_i = [C_i]$. Thus, via the bottom row, we have realized $\mathcal{G}_h$ as a subset of $\mathbb{F}_q^n$. We can assume without loss of generality that none of the C_i are the identity class. Then the requirement $g_i \in C_i$ for membership in $\mathcal{G}_h$ gives $|G^{\mathrm{ab}}|$ choices for b_i if $m_i = 1$. If $m_i \neq 1$ then $g_i \in C_i$ allows all q choices for b_i.

Now briefly view $(g_1, \ldots, g_n)$ as part of the larger catch-all set G^n of §3.3, on which the standard braid operators σ_i act. The braiding rule (3.2) in our current setting becomes

$$\left(\ldots, \begin{pmatrix} m_i \\ b_i \end{pmatrix}, \begin{pmatrix} m_{i+1} \\ b_{i+1} \end{pmatrix}, \ldots\right)^{\sigma_i} = \left(\ldots, \begin{pmatrix} m_{i+1} \\ b_{i+1} \end{pmatrix}, \begin{pmatrix} m_i \\ b_{i+1} + m_{i+1} b_i - m_i b_{i+1} \end{pmatrix}, \ldots\right).$$

Thus the action of σ_i corresponds to the the bottom row of (7.3), viewed as row vector of length n, being multiplied on the right by an n-by-n matrix in $GL_n(\mathbb{F}_q)$.

Returning now to the set $\mathcal{G}_h$ itself, any element of Br_ν can be written as a product of the σ_i and their inverses. Accordingly, image of the Br_ν in $\mathrm{Sym}(\mathcal{G}_h)$ lies in $GL_n(\mathbb{F}_q)$.

To prove non-fullness, it suffices to bound the sizes of groups. On the one hand,

$$|\text{Image of } \mathrm{Br}_\nu \text{ in } \mathrm{Sym}(\mathcal{F}^*_{h,\ell})| \leq |\text{Image of } \mathrm{Br}_\nu \text{ in } \mathrm{Sym}(\mathcal{G}_h)| \leq |GL_n(\mathbb{F}_q)| < q^{n^2}.$$

On the other hand, let $b = |H_2(G,C)||\mathrm{Out}(G,C)|+1$. Then, using (3.7), (4.6) and the fact that $|C_i| \in \{|G^{\mathrm{ab}}|, q\}$, one has

$$|\mathcal{F}^*_{h,\ell}| > \frac{\prod_i |C_i|^{\nu_i}}{|G||G'|b} \geq \frac{|G^{\mathrm{ab}}|^{n-3}}{q^2 b},$$

for all sufficiently large n. Certainly $q^{n^2} < \frac{1}{2}\left(\frac{a^{n-3}}{q^2b}\right)!$ for any fixed a, b, $q > 1$ and sufficiently large n. Thus the image of Br_ν in $\mathrm{Sym}(\mathcal{F}^*_{h,\ell})$ cannot contain $\mathrm{Alt}(\mathcal{F}^*_{h,\ell})$. □

The paper [10] calculates monodromy in cases with $G = S_3$ and $G = S_4$, providing worked out examples. Another illustration of the case with affine monodromy is [15, Prop. 10.4].

7.2. **Failure of Condition 2.** Our next lemma has the same conclusion as the previous lemma.

Lemma 7.2. *Let G be a centerless group. Let $C = (C_1, \ldots, C_r)$ be a list of conjugacy classes with at least one C_i ambiguous. Consider varying allowed $\nu \in \mathbb{Z}^r_{\geq 1}$ and thus varying Hurwitz parameters $h = (G, C, \nu)$. Then for $\min_i \nu_i$ sufficiently large and any $\ell \in H^*_h$, the action of Br_ν on $\mathcal{F}^*_{h,\ell}$ is not full.*

Proof. Introduce indexing sets B_i by writing

$$C_i = \coprod_{b \in B_i} C_{ib},$$

where each C_{ib} is a single G' orbit. Our hypothesis says that at least one of the B_i – without loss of generality, B_1 – has size larger than 1. On the other hand, at least one of the B_i has size strictly less than C_i; otherwise G' would centralize each element of each C_i, and then all of G, which is impossible for G center-free.

Define

$$\mathcal{G}^{\mathrm{amb}}_h = \overbrace{B_1 \times \cdots \times B_1}^{\nu_1} \times \cdots \times \overbrace{B_r \times \cdots \times B_r}^{\nu_r}.$$

The group G acts transitively through its abelianization G^{ab} on each B_i. For a lifting invariant $\ell \in H_h$, consider the natural map $\mathcal{G}_{h,\ell} \to \mathcal{G}^{\mathrm{amb}}_h$. The action of the braid group Br_ν on $\mathcal{G}_{h,\ell}$ descends to an action on $\mathcal{G}^{\mathrm{amb}}_h$.

Now we let $\min_i \nu_i \to \infty$ and get the following consequences, by arguments very closely paralleling those for the first case of Lemma 7.1. First, the image of the map $\mathcal{G}_{h,\ell} \to \mathcal{G}^{\mathrm{amb}}_h$, has size that goes to ∞. Second, the mass formula again shows that $\frac{|\mathcal{G}_{h,\ell}|}{|\mathcal{G}^{\mathrm{amb}}_h|} \to \infty$ with $\min_i \nu_i$. By the last paragraph of the first case of the proof of Lemma 7.1, the action of Br_ν on each orbit of $\mathcal{F}^*_{h,\ell}$ is forced to be imprimitive, and hence not full. □

For a contrasting pair of examples, consider $h = (S_5, (C_{2111}, C_{311}, C_5), \nu)$ for $\nu = (2,2,1)$ and $\nu = (2,1,2)$. The monodromy group for the former is all of S_{125}, despite the presence of the ambiguous class C_5. The monodromy group for the latter is $S_{85} \wr S_2$ and represents the asymptotically-forced non-fullness.

7.3. **Failure of Condition 3.** The last lemma of this section is different in structure from the previous two, and its proof is essentially a collection of some of our previous arguments. From the discussion of surjectivity after (5.2), one always has

$$|H_2(G^{[2]}, C^2)| = a|H_2(G,C)|^2 \tag{7.4}$$

for some positive integer a. Condition 3 is that $a = 1$. The number a reappears as the cardinality of every fiber of the maps of torsors

$$H_2(G^{[2]}, C^2, \nu) \overset{\pi}{\twoheadrightarrow} H_2(G, C, \nu)^2$$

considered in §4.5.

Now suppose that ν is such that all ν_i are divisible by both the exponent of $H_2(G, C)$ and the exponent of $H_2(G^{[2]}, C^2)$. In that case, we have identifications

$$\begin{array}{ccc} H_2(G^{[2]}, C^2, \nu) & \overset{\pi}{\to} & H_2(G, C, \nu)^2 \\ f\downarrow & & g\downarrow \\ H_2(G^{[2]}, C^2) & \to & H_2(G, C)^2 \end{array} \tag{7.5}$$

where the vertical bijections f, g come from §4.3, and the fact that the diagram commutes is also explained there.

Then $E = \pi^{-1}g^{-1}(0) \subseteq H_2(G^{[2]}, C^2, \nu)$ is a fiber of π. It has size ≥ 2 and $f(E) \subseteq H_2(G^{[2]}, C^2)$ is a subgroup.

The group $\mathrm{Out}(G, C)^{[2]}$, defined before (6.3), acts on $H_2(G^{[2]}, C^2, \nu)$ and also (compatibly) on $H_2(G^{[2]}, C^2)$. It preserves E and acts on it with at least two orbits, because it fixes the zero element of $f(E)$. Under the bijection (6.4), these two orbits correspond to two different braid orbits O, O' on $(\mathcal{F}_h^*)^{\underline{2}}$ which project (in both coordinates) to the same braid orbit on $\mathcal{F}_h^*$.

To summarize, we have proved:

Lemma 7.3. *Let G be a pseudosimple group, let $C = (C_1, \ldots, C_r)$ be a list of unambiguous conjugacy classes, and suppose $a > 1$ in (7.4).*

Consider ν with all ν_i a multiple of the exponent of both $H_2(G, C)$ and $H_2(G^{[2]}, C^2)$. Identify $H_2(G, C, \nu) = H_2(G, C)$ as in §4.3, writing $0 \in H_2(G, C, \nu)$ for the element corresponding to 0. Similarly identify $H_2(G^{[2]}, C^2, \nu) = H_2(G^{[2]}, C^2)$.

Then for $\min_i \nu_i$ sufficiently large, the action of Br_ν on $\mathcal{F}_{h,0}^*$ is not 2-transitive and hence not full.

8. Full number fields

Theorem 5.1 guarantees the existence of infinitely many quasi-full covers $\pi_h^* : \mathsf{Hur}_h^* \to \mathsf{Conf}_\nu$ associated to each simple group T. As discussed in §2.4, if all the C_i are different and conjugate classes C_i occur with equal multiplicity, then π_h^* canonically descends to a covering of $\mathbb{Q}$-varieties,

$$\pi_h^* : \mathrm{H{\scriptsize UR}}_h^* \to \mathrm{C{\scriptsize ONF}}_\nu^\rho. \tag{8.1}$$

This final section explains why we expect specializations of these covers to give enough fields for Conjecture 1.1.

Our object here is to give an overview only, as we defer a more detailed treatment to [22]. In particular, we return to the setting of §1.3, considering only h where all C_i are individually rational. Then the twisting ρ is trivial and the base of (8.1) is just $\mathrm{C{\scriptsize ONF}}_\nu$, as defined in §2.1.

8.1. **Specialization.** First, we give a few more details on the specialization process. The $\mathbb{Q}$-variety $\mathrm{C{\scriptsize ONF}}_\nu$ has a natural structure of scheme over $\mathbb{Z}$. In particular, one says that a point $u \in \mathrm{C{\scriptsize ONF}}_\nu(\mathbb{Q})$ is $\mathcal{P}$-integral if it belongs to $\mathrm{C{\scriptsize ONF}}_\nu(\mathbb{Z}[\frac{1}{\mathcal{P}}])$.

Concretely, a $\mathcal{P}$-integral point u can be specified by giving binary homogeneous forms $(q_1, \ldots, q_r)$, where

$$q_i \in \mathbb{Z}[x, y] \text{ and } \operatorname{disc}(\textstyle\prod q_i) \text{ is divisible only by primes in } \mathcal{P}. \tag{8.2}$$

To avoid obtaining duplicate fields in the specialization process, one can normalize in various ways to take one point from each $PGL_2(\mathbb{Q})$ orbit intersecting $\mathrm{Conf}_\nu(\mathbb{Z}[\frac{1}{\mathcal{P}}])$. This is done systematically in [21] and these sets of representatives are arbitrarily large for any given non-empty $\mathcal{P}$.

8.2. **Rationality of components.** For h to be useful in supporting Conjecture 1.1, it is essential that the subcover $\mathsf{Hur}^*_{h,\ell} \to \mathsf{Conf}_\nu$ is defined over $\mathbb{Q}$ for at least one lifting invariant $\ell \in H^*_h$. In this subsection, we explain that for fixed (G, C), many $h = (G, C, \nu)$ may not have such a rational ℓ, but infinitely many do.

Consider the lifting invariant map,

$$\operatorname{inv}^*_h : \pi_0(\mathsf{Hur}^*_h) \to H^*_h.$$

Since $\mathsf{Hur}^*_h = \mathrm{Hur}^*_h(\mathbb{C})$ is the set of complex points of a $\mathbb{Q}$-variety, there is a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\pi_0(\mathsf{Hur}^*_h)$. Likewise, via its standard action on conjugacy classes of groups, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on H^*_h. This latter action is through the abelianization $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$ and can be calculated via character tables. With these two actions, the lifting invariant map is equivariant up to sign (i.e., the action of $\sigma \in \mathrm{Gal}$ on one side corresponds to $\sigma^{\pm 1}$ on the other; we didn't compute the sign) – see [11, v1, §8].

To make the issue at hand more explicit, suppose $|H^*_h| = 2$. Then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$ acts on H^*_h the same way it acts on the complex numbers $\{-\sqrt{d}, \sqrt{d}\}$ for some square-free integer d. The case $d \neq 1$ is common, and then any specialized field $K^*_{h,u}$ contains $\mathbb{Q}(\sqrt{d})$ and hence—outside of the trivial case $K^*_{h,u} = \mathbb{Q}(\sqrt{d})$—is not full. The case $d = 1$ is more favorable to us, as commonly $K^*_{h,u}$ factors into two full fields. Explicit examples of both $d \neq 1$ and $d = 1$ can be easily built [22].

To see in general that for infinitely many ν, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$ on $H^*_h = H^*_{G,C,\nu}$ has at least one fixed point, we apply the simple remark from §4.3. Namely suppose that all ν_i are multiples of the exponent of $H_2(G, C)$. Then, the torsor H_h can be canonically identified with $H_2(G, C)$ itself. Then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$ fixes the identity element of H_h, and so also fixes the image of the identity in H^*_h.

8.3. **A sample cover.** To illustrate the ease of producing full fields, we summarize here the introductory example of [22]. For this example, we take $h = (S_5, (C_{2111}, C_5), (4, 1))$. Then $\mathsf{Hur}^*_h = \mathsf{Hur}_h$ is a full cover of $\mathsf{Conf}_{4,1}$ of degree 25. The fiber of $\mathsf{Hur}_h \to \mathsf{Conf}_{4,1}$ over the configuration $u = (D_1, D_2) = (\{a_1, a_2, a_3, a_4\}, \{\infty\})$ consists of all equivalence classes of quintic polynomials

$$g(y) = y^5 + by^3 + cy^2 + dy + e \tag{8.3}$$

whose critical values are a_1, a_2, a_3, a_4. Here the equivalence class of $g(y)$ consists of the five polynomials $g(\zeta y)$ where ζ runs over fifth roots of unity.

Explicitly, consider the resultant $r(t)$ of $g(y) - t$ and $g'(y)$. Then $r(t)$ equals

$$\begin{aligned}
&3125t^4 + 1250(3bc - 10e)t^3 \\
&+ \left(108b^5 - 900b^3d + 825b^2c^2 - 11250bce + 2000bd^2 + 2250c^2d + 18750e^2\right) t^2 \\
&-2 \left(108b^5e - 36b^4cd + 8b^3c^3 - 900b^3de + 825b^2c^2e + 280b^2cd^2\right. \\
&\qquad \left. -315bc^3d - 5625bce^2 + 2000bd^2e + 54c^5 + 2250c^2de - 800cd^3 + 6250e^3\right) t
\end{aligned}$$

$$+\big(108b^5e^2 - 72b^4cde + 16b^4d^3 + 16b^3c^3e - 4b^3c^2d^2 - 900b^3de^2 + 825b^2c^2e^2$$
$$+560b^2cd^2e - 128b^2d^4 - 630bc^3de + 144bc^2d^3 - 3750bce^3$$
$$+2000bd^2e^2 + 108c^5e - 27c^4d^2 + 2250c^2de^2 - 1600cd^3e + 256d^5 + 3125e^4\big)\,.$$

For fixed $\{a_1, a_2, a_3, a_4\}$, there are generically 125 different solutions (b, c, d, e) to the equation $r(t) = 3125(t - a_1)\cdots(t - a_4)$. Two solutions are equivalent exactly if they have the same e. Whenever D_1 is rational, i.e. $\prod(t - a_i) \in \mathbb{Q}[t]$, the set of e arising forms the set of roots of a degree 25 polynomial with rational coefficients. By taking $u \in \mathrm{Conf}_{4,1}(\mathbb{Z}[\frac{1}{30}])$ one gets more than 10000 different fields with Galois group A_{25} or S_{25} and discriminant of the form $\pm 2^a 3^b 5^c$.

8.4. **Support for Conjecture 1.1.** Let $F_{\mathcal{P}}(m)$ be the number of full fields ramified within $\mathcal{P}$ of degree m. The mass heuristic [1] gives an expected value $\mu_{\mathcal{P}}(m)$ for $F_{\mathcal{P}}(m)$ as an easily computed product of local masses. This heuristic has had clear success in the setting of fixed degree and large discriminant, being for example exactly right on average for $m = 5$ [2].

The numerical support for Conjecture 1.1 presented in [22] gives evidence that specialization of the covers (8.1) does indeed behave generically. General computations for fixed $\mathcal{P}$ in arbitrarily large degree do not seem possible. However our numerical support at least shows that specialization of Hurwitz covers produces many fields in degrees larger than would be expected from the mass heuristic.

For instance, one of many examples in [22] comes from the Hurwitz parameter $h = (S_6, (C_{321}, C_{2111}, C_{3111}, C_{411}), (2, 1, 1, 1))$. The covering $\mathrm{Hur}_h \to \mathrm{Conf}_{2,1,1,1}$ is full of degree 202. The specialization set $\mathrm{Conf}_{2,1,1,1}(\mathbb{Z}[\frac{1}{30}])$ intersects exactly 2947 different $\mathrm{PGL}_2(\mathbb{Q})$ orbits on the set $\mathrm{Conf}_{2,1,1,1}(\mathbb{Q})$ [21]. The mass heuristic predicts $\sum_{m=202}^{\infty} \mu_{\{2,3,5\}}(m) < 10^{-16}$ full fields in degree ≥ 202. However specialization is as generic as it could be, as the 2947 algebras $K_{h,u}$ are pairwise non-isomorphic and all full.

Even sharper contradictions to the mass heuristic are obtained in [20] from fields ramified at just two primes. However the construction there is very special, and does not give fields in arbitrarily large degree for a given $\mathcal{P}$. Here we have not just the large supply of full covers studied in this paper, but also very large specialization sets [21] giving many opportunities for full fields. Specialization in large degrees would have to behave extremely non-generically for Conjecture 1.1 to be false. Our belief is that Conjecture 1.1 still holds with the conclusion strengthened to $F_{\mathcal{P}}(m)$ being unbounded.

8.5. **Concluding discussion.** There are other aspects of the sequences $F_{\mathcal{P}}(m)$ that are not addressed by our Conjecture 1.1. Most notably, the fields arising from full fibers of Hurwitz covers occur only in degrees for which there is a cover. By the mass formula, these degrees form a sequence of density zero.

A fundamental question is thus the support of the sequences $F_{\mathcal{P}}(m)$, meaning the set of degrees m for which $F_{\mathcal{P}}(m)$ is positive. One extreme possibility, giving as much credence to the mass heuristic as is still reasonable, is that $F_{\mathcal{P}}(m)$ has support on a sequence of density zero in general and is eventually zero unless $\mathcal{P}$ contains the set of prime divisors of the order of a finite simple group. This would imply that the classification of finite simple groups has an unexpected governing influence on a part of algebraic number theory seemingly quite removed from general group theory. If one is not in this extreme possibility, then there would have to be a broad and as yet unknown new class of number fields which is also exceptional from the point of view of the mass heuristic.

References

[1] Manjul Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. Int. Math. Res. Not. IMRN 2007, no. 17, Art. ID rnm052, 20 pp.

[2] ——— The density of discriminants of quintic rings and fields. Annals of Math, 172, No. 3 (2010), 1559–1591.

[3] Paul Bailey and Michael D. Fried. Hurwitz monodromy, spin separation and higher levels of a modular tower. Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 79–220, Proc. Sympos. Pure Math., 70, Amer. Math. Soc., Providence, RI, 2002.

[4] José Bertin and Matthieu Romagny. Champs de Hurwitz. Mém. Soc. Math. Fr. (N.S.) No. 125–126 (2011), 219 pp.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. and Wilson. Atlas of finite groups. Oxford University Press, 1985.

[6] J. H. Conway and R. A. Parker. On the Hurwitz number of arrays of group elements, unpublished preprint, September 1988.

[7] John D. Dixon and Brian Mortimer. Permutation groups. Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996. xii+346 pp. ISBN: 0-387-94599-7

[8] N. Dunfield and W. Thurston. Finite covers of random 3-manifolds. Inventiones Math 166 (2006), 457–521.

[9] Beno Eckmann and Urs Stammbach. On exact sequences in the homology of groups and algebras. Illinois Journal of Math 14 (1970), 183–362.

[10] David Eisenbud, Noam Elkies, Joe Harris and Robert Speiser. On the Hurwitz scheme and its monodromy. Composito Math 77 (1991), 95–117.

[11] Jordan Ellenberg, Akshay Venkatesh and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, II. `http://arxiv.org/abs/1212.0923`

[12] Michael Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. Mathematische Annalen 290 (1991), 771-800.

[13] Paul Kluitmann. Hurwitz action and finite quotients of braid groups. Braids (Santa Cruz, CA, 1986), 299–325, Contemp. Math., 78, Amer. Math. Soc., Providence, RI, 1988.

[14] Kay Magaard, Sergey Shpectorov, and Helmut Völklein. A GAP package for braid orbit computation and applications. Experiment. Math. 12 (2003), no. 4, 385–393.

[15] Gunter Malle and Heinrich B. Matzat. Inverse Galois theory. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999. xvi+436 pp. ISBN: 3-540-62890-8

[16] Gunter Malle and David P. Roberts. Number fields with discriminant $\pm 2^a 3^b$ and Galois group A_n or S_n. LMS J. Comput. Math. 8 (2005), 80–101.

[17] OEIS Foundation. The On-Line Encyclopedia of Integer Sequences, http://oeis.org.

[18] Matthieu Romagny and Stefan Wewers. Hurwitz spaces. Séminaires et Congrès 13, SMF 2006, p.313–341.

[19] David P. Roberts. Wild partitions and number theory. J. Integer Seq. 10 (2007), no. 6, Article 07.6.6, 34 pp.

[20] ——— Chebyshev covers and exceptional number fields. Preprint, DPR's homepage.

[21] ——— Polynomials with prescribed bad primes. Submitted preprint, DPR's homepage.

[22] ——— Hurwitz number algebras. In preparation.

[23] Jean-Pierre Serre. Relèvements dans $\tilde{A}_n$. C. R. Acad. Sci. Paris Sér. I Math. 311 (1990), no. 8, 477–482.

[24] ——— with Henri Darmon. Topics in Galois theory. Second edition. Research Notes in Mathematics, 1. A K Peters, Ltd., Wellesley, MA, 2008. xvi+120 pp.

Division of Science and Mathematics, University of Minnesota Morris, Morris, MN 56267, USA
E-mail address: roberts@morris.umn.edu

Department of Mathematics, Building 380, Stanford University, Stanford, CA 94305, USA
E-mail address: akshay@math.stanford.edu