TOPOLOGICAL TYPES OF ACTIONS ON CURVES

DIEGO CONTI, ALESSANDRO GHIGI, ROBERTO PIGNATELLI

Abstract. We describe an algorithm that constructs a list of all topological types of holomorphic actions of a finite group on a compact Riemann surface C of genus $g \geq 2$ with $C/G \cong \mathbb{P}^1$.

1. Introduction

Galois covers of the projective line often give interesting examples of algebraic curves of genus $g \geq 2$. Any such cover is a compact Riemann surface C, endowed with an action of a finite group G such that $C/G \cong \mathbb{P}^1$. Studying compact Riemann surfaces with a G-action subject to the latter condition and Galois covers of the line is equivalent.

To any G-action on a Riemann surface one can attach a topological invariant, the *topological type* (see Section 2 for the precise definitions). It turns out that for every fixed topological type there is a sort of universal family containing all the covers with the given topological type. These families are often very interesting and represent interesting loci in the moduli space of curves.

Moreover it follows from the existence and the properties of these families that two Riemann surfaces with an action of the same group are deformation equivalent (through Riemann surfaces with an action) if and only if they have the same topological type (see §2.11 for more details on this point). Thus, if one starts from a collection of Riemann surfaces and constructs new algebraic varieties out of them, the topological type controls the deformation equivalence class of the varieties one obtains.

For these reasons it is very useful to have a list of all the possibile topological types at least for reasonably small genus. This is exactly the problem we address: for a positive integer $g \geq 2$, describe explicitly the set of topological types of (faithful) actions of a finite group on a Riemann surface of genus g with quotient isomorphic to $\mathbb{P}^1$. To our knowledge a complete answer is known only for very small values of g. The papers [29, 28] give a complete classification of the topological types of group actions on Riemann surfaces of genus $g \leq 5$ without any assumption on the quotient C/G. For higher

2020 *Mathematics Subject Classification.* Primary: 14H37, Secondary: 14Q05, 57M60, 14H15, 14J10.

The authors were partially supported by INdAM (GNSAGA). The second author was partially supported also by MIUR PRIN 2017 “Moduli and Lie Theory” , by FAR 2016 (Pavia) “Varietà algebriche, calcolo algebrico, grafi orientati e topologici”, by MIUR, Programma Dipartimenti di Eccellenza (2018-2022) - Dipartimento di Matematica “F. Casorati”, Università degli Studi di Pavia. The third author was partially supported also by MIUR PRIN 2015 “Geometry of Algebraic Varieties” and by MIUR PRIN 2017 “Moduli Theory and Birational Classification”.

genus, we do not know of any classification result of this type. An important contribution in this direction is the systematic work of Paulhus [35]. She introduces a very efficient algorithm that yields a database of pairs (C, G) where C is a Riemann surface of genus among 2 and 15 and G is a finite group acting on it with quotient C/G of genus zero. Her database contains representatives for all possible topological types of groups actions in this range, but does not give a complete answer to the question (up to genus 15) since it does not indicate when two data in the database share the same topological type. For instance, Paulhus' database contains 174121 data for $g = 15$, which according to our computations correspond to 768 topological types. (Added in proof: another important work that we discovered at a very late stage, is [4]. We mention also the paper [42] where the topological classification is useful in decomposing Jacobians with group action.)

Fix $g \geq 2$, a finite group G and $r \geq 3$. It is well known that the topological types of holomorphic G-actions on a genus g surface with r branch points correspond bijectively to the points of the quotient $\mathscr{D}_g^r(G)/\mathbf{H}$ where $\mathscr{D}_g^r(G)$ is a finite (but possibly huge) set and $\mathbf{H}$ is an infinite group acting on it (this fundamental fact is recalled with some details in Section 2; see also (3.11) for the definition of $\mathbf{H}$). Therefore, the object of this paper is the description of the quotient $\mathscr{D}_g^r(G)/\mathbf{H}$ for fixed g and G. Algorithms for this kind of computation are already known and have been used in several papers, like for example [1, 18, 13, 22], just to quote the ones closer to our approach. As the genus g increases, the set $\mathscr{D}_g^r(G)$ becomes quite large, and finding an economical way of performing the computation becomes essential. In the present paper we describe an efficient algorithm that computes $\mathscr{D}_g^r(G)/\mathbf{H}$ for given g and G. The computation of $\mathscr{D}_g^r(G)$ is based on our work [13], and uses some of the ideas of [35]; the identification of the quotient is new.

We implemented the algorithm using `MAGMA` [6]; our implementation is available at [14]. Running the code over several months on a computer with 56 Intel Xeon 2.60GHz CPU and 128 GB of RAM we have been able to compute $\mathscr{D}_g(G)/\mathbf{H}$ for all groups G and $g \leq 39$, with the exception of only three cases. These exceptions share the same group, $G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$, and are respectively in genus $g = 28, 34, 37$. See Table 1 for an account of how many topological types exist for each genus. See §3.30 for some perspectives on future work related to the group G above and similar ones.

The results of our computations are collected in a database, available at

`https://mate.unipv.it/ghigi/tipitopo`.

The database also contains several other data classifying actions on surfaces of higher genus (up to $g = 100$) under some further constraints. We refer to the website for the exact indication of these constraints.

The paper is organized as follows: in §2 we recall the theoretical background, introducing the precise definitions of $\mathscr{D}_g^r(G)$, $\mathbf{H}$; in §3 we describe the algorithm, and give some details on its implementation.

Acknowledgements. The authors wish to thank Matteo Penegini, Fabio Perroni and Michael Loenne for interesting discussions, and Fabio Gennai for crucial technical help in the preparation of the website.

2. Topological types and families of G-curves

The goal of this section is to recall without proofs the mathematics behind our computation.

A *G-curve* is a smooth projective curve C over the complex numbers together with an effective algebraic action of the group G. We always assume that the genus of C is at least 2 and hence that G is finite. We also assume throughout the paper that the quotient C/G is isomorphic to the projective line $\mathbb{P}^1$, i.e. the projection $C \to C/G$ is a Galois cover of $\mathbb{P}^1$. Under this assumption it is completely equivalent to study G-curves or Galois covers of the line.

Definition 2.1. *If C and C' are two G-curves we say that they are* topologically equivalent *or that they have the same* topological type *if there exist $\eta \in \operatorname{Aut} G$ and an orientation preserving homeomorphism $f : C \to C'$ such that $f(g \cdot x) = \eta(g) \cdot f(x)$ for $x \in C$ and $g \in G$. We say that C and C' are* G-isomorphic *if moreover f is a biholomorphism.*

These concepts are sometimes called *unmarked* topological type and isomorphisms, but we will drop the 'unmarked' since we do not need to consider their marked counterparts.

For $r \geq 3$ let Γ_r denote the group

$$\Gamma_r = \langle \gamma_1, \dots, \gamma_r \,|\, \gamma_1 \cdots \gamma_r \rangle.$$

Definition 2.2. *If G is a finite group an r-datum is an epimorphism $\theta : \Gamma_r \to G$ is such that $\theta(\gamma_i) \neq 1$ for $i = 1, \dots, r$.*

The *signature* of θ, denoted $\mathbf{m}(\theta)$ or simply $\mathbf{m}$, is the vector

$$\mathbf{m} = (m_1, \dots, m_r)$$

where $m_i := \operatorname{ord} \theta(\gamma_i)$. The *genus* of θ, denoted by $g(\theta)$, is defined by the Riemann-Hurwitz formula:

$$2(g(\theta) - 1) = |G| \left(-2 + \sum_{i=1}^{r} \left(1 - \frac{1}{m_i} \right) \right) \tag{2.3}$$

By covering theory if one chooses r distinct points $x_1, \dots, x_r$ in $\mathbb{P}^1$, a base point $x_0 \in \mathbb{P}^1 - \{x_1, \dots, x_r\}$ and an isomorphism among Γ_r and $\pi_1(\mathbb{P}^1 - \{x_1, \dots, x_r\}, x_0)$, then a datum corresponds to a topological Galois covering of $C^* \to \mathbb{P}^1 - \{x_1, \dots, x_r\}$ with structure group G. By Riemann's Existence Theorem (see e.g. [32, ch. III §4] or [15]) this compactifies to a G-covering $C \to \mathbb{P}^1$, where the genus of C is $g(\theta)$.

We let $\mathscr{D}_g^r(G)$ denote the set of all r-data of genus g associated with the group G.

Definition 2.4. *Denote by $\operatorname{Aut}^* \Gamma_r \subset \operatorname{Aut} \Gamma_r$ the subgroup of automorphisms ν satisfying:*

(1) for $i = 1, \dots, n$ the element $\nu(\gamma_i)$ is conjugate to γ_j for some j;
(2) the automorphism of $H^2(\Gamma_r, \mathbb{Z})$ induced by ν is the identity.

The second condition means that ν is orientation-preserving: if we identify Γ_r with $\pi_1(\mathbb{P}^1 - \{x_1, \dots, x_r\})$ appropriately (using a so-called geometric basis) then ν is represented by an orientation preserving self-homeomorphism of $\mathbb{P}^1 - \{x_1, \dots, x_r\}$ (Dehn-Nielsen-Baer theorem, see e.g. [16, 26, 46]).

2.5. The group $\operatorname{Aut}^* \Gamma_r \times \operatorname{Aut} G$ acts on the set $\mathscr{D}_g^r(G)$ by the rule

$$(\nu, \eta) \cdot \theta := \eta \circ \theta \circ \nu^{-1},$$

where $(\nu, \eta) \in \operatorname{Aut}^* \Gamma_r \times \operatorname{Aut} G$ and $\theta \in \mathscr{D}_g^r(G)$ is a datum. Moreover $\operatorname{Inn} \Gamma_r \subset \operatorname{Aut}^* \Gamma_r$ and we set

$$\operatorname{Out}^* \Gamma_r := \frac{\operatorname{Aut}^* \Gamma_r}{\operatorname{Inn} \Gamma_r}.$$

This group has a presentation with generators $\sigma_1, \ldots, \sigma_{r-1}$ and relations

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{for } |i-j| \geq 2, \qquad \sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i \sigma_{i+1} \sigma_i, \tag{2.6}$$

$$\sigma_1 \cdots \sigma_{r-2} \sigma_{r-1}^2 \sigma_{r-2} \cdots \sigma_1 = 1, \qquad (\sigma_1 \cdots \sigma_{r-1})^r = 1. \tag{2.7}$$

Instead the braid group B_r is the group generated by $\sigma_1, \ldots, \sigma_{r-1}$ subject only to relations (2.6). Define $\tilde{\sigma}_i : \Gamma_r \to \Gamma_r$ as follows:

$$\begin{gathered} \tilde{\sigma}_i(\gamma_i) = \gamma_{i+1}, \quad \tilde{\sigma}_i(\gamma_{i+1}) = \gamma_{i+1}^{-1} \gamma_i \gamma_{i+1}, \\ \tilde{\sigma}_i(\gamma_j) = \gamma_j \quad \text{for } j \neq i, i+1. \end{gathered} \tag{2.8}$$

Then $\tilde{\sigma}_i$ is an automorphism of Γ_r and it is called the *i-th Hurwitz move.* The Hurwitz moves $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{r-1} \in \operatorname{Aut}^* \Gamma_r$ satisfy the relations (2.6). Thus there is a (unique) morphism $\varphi : \mathrm{B}_r \to \operatorname{Aut}^* \Gamma_r$ such that $\varphi(\sigma_i) := \tilde{\sigma}_i$. Using φ we let $\mathrm{B}_r \times \operatorname{Aut} G$ act on $\mathscr{D}_g^r$: if $(\eta, \sigma) \in \mathrm{B}_r \times \operatorname{Aut} G$ and $\theta \in \mathscr{D}_g^r$, then

$$(\eta, \sigma) \cdot \theta := \eta \circ \theta \circ \varphi(\sigma)^{-1}.$$

The composition

$$\mathrm{B}_r \xrightarrow{\varphi} \operatorname{Aut}^* \Gamma_r \longrightarrow \operatorname{Out}^* \Gamma_r$$

maps $\tilde{\sigma}_i$ to σ_i, so is surjective. It follows that $\varphi(\mathrm{B}_r) \cdot \operatorname{Inn} \Gamma_r = \operatorname{Aut}^* \Gamma_r$. For $a \in \Gamma_r$ let $\operatorname{inn}_a : \Gamma_r \to \Gamma_r$ be conjugation by a: $\operatorname{inn}_a(x) := axa^{-1}$. Then for $\theta \in \mathscr{D}_g^r$, we have

$$\theta \circ \operatorname{inn}_a = \operatorname{inn}_{\theta(a)} \circ \theta.$$

Hence the actions of $\operatorname{Aut}^* \Gamma_r \times \operatorname{Aut} G$ and of $\mathrm{B}_r \times \operatorname{Aut} G$ on $\mathscr{D}_g^r$ have the same orbits and

$$\mathscr{D}_g^r / (\operatorname{Aut}^* \Gamma_r \times \operatorname{Aut} G) = \mathscr{D}_g^r / (\mathrm{B}_r \times \operatorname{Aut} G).$$

The orbits of the $\mathrm{B}_r \times \operatorname{Aut} G$–action are called *Hurwitz equivalence classes* and elements in the same orbit are said to be *Hurwitz equivalent.*

Theorem 2.9. *Fix $g \geq 2$ and a finite group G, the topological types of G-curves C with $g(C) = g$, $g(C/G) = 0$ and r branch points are in bijection with the set*

$$\mathscr{D}_g^r(G) / \left(\mathrm{B}_r \times \operatorname{Aut} G\right). \tag{2.10}$$

A proof can be found for example in [23, Section 5].

2.11. It often happens that one is not interested in a precise G-curve, but rather in the whole family of G-curves of a given topological type. Indeed, there is a sort of universal family containing all G-curves of a given topological type. These "universal" families have been widely studied and used in the literature for several purposes in the last decades, see e.g.

[1, 8, 9, 10, 34, 18, 20, 21, 36, 38, 45]. They were first constructed by González-Díez and Harvey [24] using Teichmüller theory. There are other ways to construct it. Recently in [23] the second author and Tamborini gave a different construction of these families and corrected an inaccuracy in [24]. The precise statement is a bit long and there is no need to recall it here in full detail. At any rate, the end result is that for any topological type there is a family of G-curves whose fibres all have the given topological type, and which is universal in the following sense: every G-curve with the given topological type appears as a fibre of the family and it appears at most a finite number of times. Moreover the base of this family is an étale cover of the $\mathsf{M}_{0,r}$, so in particular it is smooth and connected. This "universal" family is not unique, but only unique up to the equivalence relation generate by finite étale pull-backs. We refer to the Introduction in [23] for full details.

An important consequence of this theorem is that topological types and deformation equivalence coincide for G-curves. Indeed if C and C' are G-curves with the same topological type, then they both appear as fibres of a common universal family and therefore they are deformation equivalent (through G-curves). The converse is obvious. This fact is very important in the applications to the construction of new deformation types of algebraic varieties as in [1, 2, 37, 36, 41, 11, 33, 17, 22, 3, 40, 39]. It follows from this discussion that the classification of *universal families* and of deformation equivalence classes of G-curves are both equivalent to the classification of topological types. Hence again these problems boil down to studying the quotient in (2.10). This is a strong additional motivation — in fact, our original motivation — for the classification of topological types.

3. The algorithm

We illustrate an algorithm to attack the following:

Problem 3.1. *Given a number $g_{\max}$ list all the topological types of G-curves with $g(C) \leq g_{\max}$ and $C/G \cong \mathbb{P}^1$.*

After fixing the genus g, the group G and the number of branch points r, this amounts to listing representatives of the quotient in (2.10).

3.2. We use a refinement of the algorithm illustrated in [13], which lists r-data forming counter-examples to the Coleman-Oort conjecture up to the action of $\operatorname{Aut} G$. This algorithm uses signature as an invariant for the classification, as was done in [1, 18]. A *spherical system of generators* of the group G is a list $(g_1, \dots, g_r)$ such that (1) $g_i \neq 1$ for any i, (2) G is generated by $g_1, \dots, g_r$ and (3) $g_1 \cdots g_r = 1$. Having fixed a finite group G, giving an r-datum θ is equivalent to giving a spherical systems of generators $(g_1, \dots, g_r)$ of G: simply define θ or g_i by the relation $\theta(\gamma_i) = g_i$. From now on we will identify data and spherical systems of generators and we will write a datum in $\mathscr{D}^r_g(G)$ as $(g_1, \dots, g_r)$. Signature defines a map

$$\mathscr{D}^r_g(G) \to \mathbb{N}^r, \quad (g_1, \dots, g_r) \mapsto (\operatorname{ord}(g_1), \dots, \operatorname{ord}(g_r)). \tag{3.3}$$

With the interpretation of $\mathscr{D}^r_g(G)$ just described, we have $\mathscr{D}^r_g(G) \subset G^r$, and the action of $\mathrm{B}_r \times \operatorname{Aut} G$ on $\mathscr{D}^r_g(G)$ described in 2.5 extends to an action on

G^r: $\operatorname{Aut} G$ acts componentwise,

$$\eta \cdot (g_1, \dots, g_r) = (\eta(g_1), \dots, \eta(g_r),$$

while the generator σ_i of B_r acts as follows

$$\sigma_i \cdot (g_1, \dots, g_r) = (g_1, \dots, \underbrace{g_i g_{i+1} g_i^{-1}}_{i}, \underbrace{g_i}_{i+1}, \dots, g_r). \tag{3.4}$$

Denote by Σ_r the symmetric group. There is a surjective morphism

$$\rho : \mathrm{B}_r \to \Sigma_r, \tag{3.5}$$

which maps the i-th Hurwitz move σ_i to the transposition $(i, i+1)$. The map (3.3) is ρ-equivariant: if ψ is in B_r and $\sigma = \rho(\psi)$ then $(\psi \cdot (g_1, \dots, g_r))$ is mapped to $(\operatorname{ord}(g_{\sigma_1}), \dots, \operatorname{ord}(g_{\sigma_r}))$.

Recall that Hurwitz equivalence in $\mathscr{D}_g^r(G)$ is defined in terms of the action of $\mathrm{B}_r \times \operatorname{Aut} G$; thus, (3.3) maps Hurwitz equivalence classes onto Σ_r-orbits in $\mathbb{Z}^r$. This shows that every Hurwitz equivalence class has a representative with signature of the form

$$\mathbf{m} = (m_1, \dots, m_r), \quad m_1 \le \cdots \le m_r,$$

and $\mathbf{m}$ is uniquely determined by the equivalence class.

3.6. As a first step we wish to determine the set of all possible signatures. We iterate over the order $d = |G|$. For fixed d, let $\mathfrak{S}_{d,g_{\max}}$ be the set of finite sequences $\mathbf{m} = (m_1, \dots, m_r)$ such that

- (S1) $3 \le r \le \frac{4(g_{\max}-1)}{d} + 4$;
- (S2) each m_i is a divisor of d;
- (S3) $2 \le m_i \le d$;
- (S4) g, determined by d and $\mathbf{m}$ as in (2.3), is an integer between 2 and $g_{\max}$.
- (S5) if $r = 3$, d satisfies the bound of [12, Appendix 1] as long as $g \le 301$.
- (S6) $m_1 \le \cdots \le m_r$;

It follows from the same arguments as in the proof of Hurwitz theorem that the signature of any G-curve satisfies (S1), see e.g. Lemma 3.2 (b) in [13]. Notice that we do not exclude $r = 3$ or cyclic groups here, unlike in [13].

Computing $\mathfrak{S}_{d,g_{\max}}$ is not difficult (see e.g. [13, Algorithm 1]). In our implementation, we found it convenient to store the resulting signatures on disk for later retrieval; this allows us to iterate through signatures with fixed genus g at a later stage, in order to compute the sets $\mathscr{D}_g(G)$. Upon retrieving signatures with fixed genus, we make use of the inequalities $d \le 84(g-1)$ (for $r = 3$) and $d \le 12(g-1)$ (for $r \ge 4$, see [13, Lemma 3.2.(c)]), which do not appear in the definition of $\mathfrak{S}_{d,g_{\max}}$ since they are consequences of (2.3).

3.7. Problem 3.1 can be addressed by iterating through the signatures in $\mathfrak{S}_{d,g_{\max}}$. For each signature, we iterate through isomorphism classes of groups G of order d. Some groups can be eliminated right away, namely:

- groups G that do not contain elements of order m_i for some m_i in the signature;
- groups G that contain elements of order greater than $4g + 2$ (for $r = 3$) or $4(g-1)$ (for $r > 3$);

- groups that cannot be generated by $r-1$ elements because their abelianization cannot.

Similar exclusions are listed in [13, Algorithm 2], with some differences due to the fact that we allow $r=3$ and cyclic groups here.

3.8. What remains to be done is, in fact, the most complicated and most novel part of our work, namely producing an algorithm to classify spherical systems of generators for fixed G and $\mathbf{m}$. The construction of this algorithm will take the rest of this section.

Fix a group G of order d and a signature $\mathbf{m}$, and let $\mathscr{D}_{G,\mathbf{m}}$ be the set of spherical systems of generators of G with signature $\mathbf{m}$. The group

$$(\mathrm{B}_r)_{\mathbf{m}} = \{g \in \mathrm{B}_r \mid \rho(g)\cdot \mathbf{m} = \mathbf{m}\}$$

acts on $\mathscr{D}_{G,\mathbf{m}}$, and so does $\operatorname{Aut} G$. We will need the following:

Proposition 3.9. *Given a group G of order d and $\mathbf{m}$ in $\mathfrak{S}_{d,g_{\max}}$, two elements θ,θ' of $\mathscr{D}_{G,\mathbf{m}}$ are Hurwitz equivalent if and only if they are in the same $(\mathrm{B}_r)_{\mathbf{m}}\times\operatorname{Aut} G$-orbit.*

Proof. If θ and θ' are in the same $(\mathrm{B}_r)_{\mathbf{m}}\times\operatorname{Aut} G$-orbit, they are obviously Hurwitz equivalent.

Conversely, suppose $\theta' = (\nu,\alpha)\cdot\theta$, with $\nu\in\mathrm{B}_r$, $\alpha\in\operatorname{Aut} G$; by equivariance of (3.3), the signature of θ' is $\mathbf{m} = \rho(\nu)\cdot\mathbf{m}$, so ν lies in $(\mathrm{B}_r)_{\mathbf{m}}$. □

3.10. Set for simplicity

$$\mathbf{H} := \mathrm{B}_r\times\operatorname{Aut} G. \tag{3.11}$$

Then $\mathbf{H}_{\mathbf{m}} = (\mathrm{B}_r)_{\mathbf{m}}\times\operatorname{Aut} G$. We are reduced to the following problem: given a group G of order d and $\mathbf{m}$ in $\mathfrak{S}_{d,g_{\max}}$, determine a *section* for the action of $\mathbf{H}_{\mathbf{m}}$ on $\mathscr{D}_{G,\mathbf{m}}$, that is to say a subset of $\mathscr{D}_{G,\mathbf{m}}$ that contains exactly one element in each $\mathbf{H}_{\mathbf{m}}$-orbit.

The approach used in [1, 18] was to iterate through lists of elements in

$$G^{\mathbf{m}} = \{(g_1,\dots,g_r)\in G^r \mid \operatorname{ord}(g_1)=m_1,\dots,\operatorname{ord}(g_r)=m_r\}$$

and identify those for which $\prod g_i = 1$ and $\langle g_1,\dots,g_r\rangle = G$. This produces a set of spherical systems of generators which can become quite large as r or $|G|$ increase; the fact that we are ultimately interested in extracting a representative for each orbit of $\mathbf{H}_{\mathbf{m}}$ suggests that an alternative approach could be more suited to our goal.

A preliminary observation is that, whilst the group $\mathbf{H}_{\mathbf{m}}$ is infinite, it can be replaced by its image in $\operatorname{Perm}(\mathscr{D}_{G,\mathbf{m}})$, the symmetric group over $\mathscr{D}_{G,\mathbf{m}}$, which is finite. In prior algorithms, precisely first in the paper [1] and then in [2, 18, 19, 17, 3, 22, 13], the orbit of an element is calculated by a heavy recursive procedure that builds an increasing chain of sets by the action of a fixed set of generators of $\mathbf{H}$ and stops when the chain stabilizes. By contrast, here we build first the image of $\mathbf{H}_{\mathbf{m}}$ as subgroup of $\operatorname{Perm}(\mathscr{D}_{G,\mathbf{m}})$, then compute directly all orbits without any recursion.

After this first step, the problem boils down to extracting a section for the action of a finite group on a finite set. This can be achieved efficiently in `MAGMA` using `GSets`. It is then the size of the finite group and of the finite set $\mathscr{D}_{G,\mathbf{m}}$ that determine memory use and execution time.

The basic idea to reduce both is to split the action of $\mathbf{H_m}$ on $G^{\mathbf{m}}$ into a large number of actions, each one by a much smaller group acting on a much smaller set. The key observation is the following. Consider the set $\mathcal{C}_G$ of conjugacy classes in G, and consider the commutative diagram

$$\begin{tikzcd} G^r \arrow[r, "p"] \arrow[dr, "\pi"'] & (\mathcal{C}_G)^r \arrow[d] \\ & (\mathcal{C}_G)^r/\Sigma_r \end{tikzcd} \tag{3.12}$$

where $p(g_1, \ldots, g_r) = ([g_1], \ldots, [g_r])$. Setting $\mathcal{C}_G^{\mathbf{m}} := p(G^{\mathbf{m}})$, we obtain a commutative diagram

$$\begin{tikzcd} G^{\mathbf{m}} \arrow[r, "p"] \arrow[dr, "\pi"'] & \mathcal{C}_G^{\mathbf{m}} \arrow[d] \\ & \mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}} \end{tikzcd} \tag{3.13}$$

with $(\Sigma_r)_{\mathbf{m}}$ denoting the stabiliser of $\mathbf{m}$ in Σ_r. The group $\mathbf{H}$ acts also on $(\mathcal{C}_G)^r$ in the following way:

$$\eta \cdot ([g_1], \ldots, [g_r]) = (\eta([g_1]), \ldots, \eta([g_r]), \qquad \eta \in \operatorname{Aut} G$$
$$\sigma_i \cdot ([g_1], \ldots, [g_r]) = ([g_1], \ldots, \underbrace{[g_{i+1}]}_{i}, \underbrace{[g_i]}_{i+1}, \ldots, [g_r]).$$

This means that if $(\eta, \psi) \in \mathbf{H}$ and $\sigma = \rho(\nu)$, then

$$(\eta, \nu) \cdot ([g_1], \ldots, [g_r]) = ([\eta(g_{\sigma_1})], \ldots, [\eta(g_{\sigma_r})]). \tag{3.14}$$

For $\tilde{c} \in (\mathcal{C}_G)^r$, let $\mathbf{H}_{\tilde{c}}$ denotes the stabilizer for this action.

Since $(\mathcal{C}_G)^r/\Sigma_r$ is the quotient of $(\mathcal{C}_G)^r$ by B_r, it has an induced action of $\mathbf{H}$ with the factor B_r acting trivially. In other words $\operatorname{Aut} G$ acts naturally on $(\mathcal{C}_G)^r/\Sigma_r$ and we let B_r act trivially on this set. With this understood the map p and the whole Diagram (3.12) is $\mathbf{H}$-equivariant, while (3.13) is $\mathbf{H_m}$-equivariant.

Notice that a section S for the action of $\operatorname{Aut} G$ on $\mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$ can be constructed adapting [13, Algorithm 4]. From this, we recover a section for the action of $\mathbf{H_m}$ on $G^{\mathbf{m}}$ as follows:

Proposition 3.15. *Let $S \subset \mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$ be a section for the action of* $\operatorname{Aut} G$*, and let $\tilde{S}$ be a subset of $\mathcal{C}_G^{\mathbf{m}}$ that projects one-to-one onto S. Let $S' \subset G^{\mathbf{m}}$ be the union of sections for the action of $\mathbf{H}_{\tilde{c}}$ on $p^{-1}(\tilde{c})$, as $\tilde{c}$ varies in $\tilde{S}$. Then S' is a section for the action of $\mathbf{H_m}$ on $G^{\mathbf{m}}$.*

Proof. We need to show that $\mathbf{H_m} \cdot S' = G^{\mathbf{m}}$ and that two elements $X, Y \in S'$ that belong to the same $\mathbf{H_m}$-orbit coincide.

To see that $\mathbf{H_m} \cdot S' = G^{\mathbf{m}}$, pick $X = (g_1, \ldots, g_r)$ in $G^{\mathbf{m}}$. Up to the action of $\operatorname{Aut} G$, we can assume that $\pi(X) \in S$. Then $p(X) = \sigma \cdot \tilde{c}$ for some $\sigma \in (\Sigma_r)_{\mathbf{m}}$ and some $\tilde{c} \in \tilde{S}$. If $\sigma = \rho(\nu)$, where ρ is the map in (3.5), then ν is in $(\mathrm{B}_r)_{\mathbf{m}}$ and $\nu^{-1} \cdot X = \nu^{-1} \cdot (g_1, \ldots, g_r)$ is in $p^{-1}(\tilde{c})$, so its $\mathbf{H}_{\tilde{c}}$-orbit intersects S'. As $\mathbf{H}_{\tilde{c}} \subset \mathbf{H}_{\mathbf{m}}$ we conclude that the $\mathbf{H}_{\mathbf{m}}$-orbit of X intersects S', as desired.

Next assume that X, Y are elements of S' that belong to the same $\mathbf{H}_{\mathbf{m}}$-orbit. By equivariance $\pi(X)$ and $\pi(Y)$ are in the same $\mathbf{H}_{\mathbf{m}}$-orbit. But $(\mathrm{B}_r)_{\mathbf{m}}$ acts trivially on $\mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$. Hence $\pi(X)$ and $\pi(Y)$ are in the same $\operatorname{Aut} G$-orbit. By construction they also belong to S; therefore, they coincide. Since $\tilde{c} = p(X)$ and $p(Y)$ are elements of $\tilde{S}$ that lie over the same element of $\mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$, they also coincide. By equivariance, X and Y are in the same $\mathbf{H}_{\mathbf{m}}$-orbit only if they are in the same $\mathbf{H}_{\tilde{c}}$-orbit, which forces them to be the same. □

A first advantage of this approach is that for some G and $\mathbf{m}$, $p^{-1}(\tilde{c})$ can be considerably smaller than the whole $G^{\mathbf{m}}$, leading to a reduced memory usage. In addition, $\mathbf{H}_{\tilde{c}}$ has index

$$[\mathbf{H}_{\mathbf{m}} : \mathbf{H}_{\tilde{c}}] = [(\mathrm{B}_r)_{\mathbf{m}} : (\mathrm{B}_r)_{\tilde{c}}] \cdot [\operatorname{Aut} G : (\operatorname{Aut} G)_{\tilde{c}}].$$

This means that $\mathbf{H}_{\tilde{c}}$ is typically smaller than $\mathbf{H}_{\mathbf{m}}$ and the image of $\mathbf{H}_{\tilde{c}}$ in $\operatorname{Perm}(p^{-1}(\tilde{c}))$ is smaller than the image of $\mathbf{H}_{\mathbf{m}}$ in $\operatorname{Perm}(G^{\mathbf{m}})$, in a way that more than compensates for the fact that one has to iterate through elements of S.

Example 3.16. For example, take $G = \Sigma_4$ and $\mathbf{m} = (\underbrace{2, \dots, 2}_{r})$. Then G has nine elements of order two, namely the conjugacy class of $(1,2)$ and the conjugacy class of $(1,2)(3,4)$, call them C_1 and C_2. Then $|C_1| = 6$, $|C_2| = 3$ and

$$G^{\mathbf{m}} = (C_1 \cup C_2)^r$$

has 9^r elements.

However, if

$$\tilde{c} = (\underbrace{C_1, \dots, C_1}_{k}, \underbrace{C_2, \dots, C_2}_{r-k}), \tag{3.17}$$

up to the order, then $p^{-1}(\tilde{c})$ has $6^k 3^{r-k}$ elements, which is considerably less. It follows from (3.14) that $(\mathrm{B}_r)_{\tilde{c}} = \rho^{-1}((\Sigma_r)_{\tilde{c}})$, so $\mathrm{B}_r / (\mathrm{B}_r)_{\tilde{c}} \cong \Sigma_r/(\Sigma_r)_{\tilde{c}}$. By (3.17) $(\Sigma_r)_{\tilde{c}} \cong \Sigma_k \times \Sigma_{r-k}$, so $[\mathrm{B}_r : (\mathrm{B}_r)_{\tilde{c}}] = \binom{r}{k}$. Moreover in this special case $\operatorname{Aut} G$ fixes every conjugacy class, as every automorphism of $G = \Sigma_4$ is inner [25, vol. 1 Satz 5.5 p. 175] or [43, Cor. 7.7 p. 159]. Hence $\operatorname{Aut} G$ fixes $\tilde{c}$, and $\mathbf{H}_{\tilde{c}} = (\mathrm{B}_r)_{\tilde{c}} \times \operatorname{Aut} G$ has index $\binom{r}{k}$ in $\mathbf{H}_{\mathbf{m}}$. Furthermore, $\mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$ has $r+1$ elements indexed by k as above and $\operatorname{Aut} G$ acts trivially. We have split the action into $r+1$ actions of much smaller size.

3.18. In order to apply Proposition 3.15, one needs to compute the stabilizer $\mathbf{H}_{\tilde{c}}$ of an element $\tilde{c}$ in $\mathcal{C}_G^{\mathbf{m}}$.

In the above example $\mathbf{H}_{\tilde{c}}$ splits as a product of $(\mathrm{B}_r)_{\tilde{c}}$ and $(\operatorname{Aut} G)_{\tilde{c}}$. In general $(\mathrm{B}_r)_{\tilde{c}} \times (\operatorname{Aut} G)_{\tilde{c}}$ is only a subgroup of $\mathbf{H}_{\tilde{c}}$. In fact an element of B_r can move the conjugacy classes and element of $\operatorname{Aut} G$ can restore them to their original order. The situation in the general case is described by the exact sequence

$$1 \to (\mathrm{B}_r)_{\tilde{c}} \xrightarrow{\alpha} \mathbf{H}_{\tilde{c}} \xrightarrow{\beta} (\operatorname{Aut} G)_c \to 1, \tag{3.19}$$

where α is the inclusion: $\alpha(\psi) = (\psi, 1)$, β is the projection $\beta(\psi, \eta) = \eta$, and c is the image of $\tilde{c}$ in the quotient $\mathcal{C}_G^{\mathbf{m}} \big/ (\Sigma_r)_{\mathbf{m}}$. Indeed if $(\psi, \eta) \in \mathbf{H}_{\tilde{c}}$ and $\rho(\psi) = \sigma$, then by (3.14) we have

$$(\psi, \eta) \cdot (\tilde{c}_1, \ldots, \tilde{c}_r) = (\eta(\tilde{c}_{\sigma(1)}), \ldots, \eta(\tilde{c}_{\sigma(r)})) = (\tilde{c}_1, \ldots, \tilde{c}_r).$$

Thus η permutes the elements $\tilde{c}_i$ i.e. it fixes c. This shows that β lands in $(\operatorname{Aut} G)_c$. Obviously $\beta\alpha = 1$. If $(\psi, \eta) \in \ker \beta$, then $\eta = \mathrm{id}_G$ hence $\sigma = 1$ and $\psi \in (\mathrm{B}_r)_{\tilde{c}}$. If $\eta \in (\operatorname{Aut} G)_c$, then $\eta(c_i) = c_{\sigma(i)}$. Since ρ is surjective there is $\psi \in \mathrm{B}_r$ such that $\rho(\psi) = \sigma^{-1}$ and then $(\psi, \eta) \in \mathbf{H}_{\tilde{c}}$. Thus β is onto.

In particular, one can obtain a set of generators for $\mathbf{H}_{\tilde{c}}$ by choosing elements $\gamma_1, \ldots, \gamma_k$ such that $\beta(\gamma_1), \ldots, \beta(\gamma_k)$ generate $(\operatorname{Aut} G)_c$ and adding a set of generators of $(\mathrm{B}_r)_{\tilde{c}}$.

So we need to find a set of generators of $(\mathrm{B}_r)_{\tilde{c}}$. We start with the following observation. An element of $(\mathcal{C}_G)^r/\Sigma_r$ (or of $\mathcal{C}_G^{\mathbf{m}}/\Sigma_{\mathbf{m}}$) is represented in our implementation as a *multiset*, i.e. $(C_1^{r_1}, \ldots, C_s^{r_s})$ where $C_i \in \mathcal{C}_G$ and $r_i \geq 1$. To each multiset of conjugacy classes c there correspond several ordered sequences of conjugacy classes $\tilde{c}$. We fix a total ordering on the set of conjugacy classes $\mathcal{C}_G$. Then, among all sequences $\tilde{c}$ corresponding to the same c there is a minimal one with respect to the induced lexicographic order on $\mathcal{C}_G^r$, i.e. the only nondecreasing one:

$$\tilde{c} = (C_1, \ldots, C_r) \quad \text{with} \quad C_1 \leq \cdots \leq C_r. \tag{3.20}$$

For ease of notation, multisets will be represented by the associated nondecreasing sequence in the following.

In order to find generators of $(\mathrm{B}_r)_{\tilde{c}}$ one can consider the exact sequence

$$0 \to \mathcal{P}\,\mathrm{B}_r \to \mathrm{B}_r \xrightarrow{\rho} \Sigma_r \to 0,$$

where $\mathcal{P}\,\mathrm{B}_r$ denote the group of pure braids, i.e. $\ker \rho$. We also have the following exact sequence obtained by restriction:

$$0 \to \mathcal{P}\,\mathrm{B}_r \to (\mathrm{B}_r)_{\tilde{c}} \to (\Sigma_r)_{\tilde{c}} \to 0.$$

Recall from [5, p. 20] that $\mathcal{P}\,\mathrm{B}_r$ is generated by the elements

$$A_{ij} = \sigma_{j-1}\sigma_{j-2}\cdots\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}\cdots\sigma_{j-2}^{-1}\sigma_{j-1}^{-1}, \quad 1 \leq i < j \leq r.$$

Since we chose $\tilde{c}$ with $C_1 \leq \cdots \leq C_r$, the subgroup $(\Sigma_r)_{\tilde{c}}$ is generated by transpositions $(i\ i+1)$ where i is such that $C_i = C_{i+1}$. It follows that $(\mathrm{B}_r)_{\tilde{c}}$ is generated by

$$\{A_{ij} \mid 1 \leq i < j \leq r\} \cup \{\sigma_i \mid 1 \leq i \leq r-1, C_i = C_{i+1}\};$$

notice however that when $C_i = C_j$, then $C_i = C_{i+1} = \cdots = C_j$, so A_{ij} belongs to the group generated by $\sigma_i, \ldots, \sigma_{j-1}$, and it is redundant as a generator of $(\mathrm{B}_r)_{\tilde{c}}$. This gives Algorithm 1.

3.21. The problem considered in this paper is to compute effectively a section for the action of $\mathbf{H}$ on $\mathscr{D}^r(G)$. Logically, the problem can be split in two parts: first computing a section for the action of $\mathbf{H}$ on G^r, next checking which elements of the section are spherical systems of generators of G. For reasons of efficiency, our algorithm does not attack the two problems one after another, but simultaneously.

Algorithm 1: Computing $\mathbf{H}_{\tilde{c}}$

input : A group G and an element $\tilde{c} = (C_1, \dots, C_r) \in \mathcal{C}_G^r$, $C_1 \leq \cdots \leq C_r$

output: A set of generators for $\mathbf{H}_{\tilde{c}}$

1 $\Gamma \leftarrow \{A_{ij} \mid 1 \leq i < j \leq r, C_i \neq C_j\} \cup \{\sigma_i \mid 1 \leq i \leq r-1, C_i = C_{i+1}\}$;

2 **for** φ *in a set of generators for* $(\operatorname{Aut} G)_c$ **do**

3 $\quad \sigma \leftarrow$ a permutation such that $\varphi \cdot \tilde{c} = \sigma \cdot \tilde{c}$;

4 $\quad \alpha_{i_1} \cdots \alpha_{i_k} \leftarrow$ a decomposition of σ as a product of transpositions $\alpha_j = (j\, j+1)$;

5 $\quad \psi \leftarrow \sigma_{i_1} \cdots \sigma_{i_k}$;

6 $\quad$ add $(\psi^{-1}, \varphi) \in \mathrm{B}_r \times \operatorname{Aut} G$ to Γ

7 **return** Γ

Proposition 3.15 reduces the first problem to determining a section for the action of $\mathbf{H}_{\tilde{c}}$ on each $p^{-1}(\tilde{c})$. In view of the second part, two more optimizations are important, already used by Breuer [7] and Paulhus [35]. Indeed, for some elements c, one can ascertain *a priori* that $\pi^{-1}(c) = p^{-1}(\tilde{c})$ does not contain any system of generators at all!

This is based on a theorem of Frobenius, see [30, p. 406] for a proof and also [27] for a generalization to higher genus.

Theorem 3.22 (Frobenius's formula)**.** *Given a finite group G and conjugacy classes $C_1, \dots, C_r$, the number of r-ples $(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r$ such that $\prod g_i = 1$ is*

$$\frac{|C_1| \cdots |C_r|}{|G|} \sum_{\chi} \frac{\chi(C_1) \cdots \chi(C_r)}{\chi(1)^{r-2}},$$

where the sum is over characters of irreducible representations of G.

Thus, $p^{-1}(C_1, \dots, C_r)$ can only contain a system of spherical generators if $\sum_\chi \frac{\chi(C_1)\cdots\chi(C_r)}{\chi(1)^{r-2}}$ is nonzero; in this case, we will say that $(C_1, \dots, C_r)$ passes Frobenius' test. Notice that this condition is independent of the order of the conjugacy classes $C_1, \dots, C_r$.

Example 3.23. In the setting of Example 3.16 it is easy to check, by looking at the character table of Σ_4, that Frobenius formula evaluates to zero for k odd in (3.17). This eliminates half of the elements of S. Notice that in this particular case, the same conclusion can be reached by observing that when elements $g_1, \dots, g_r$ of Σ_4 satisfy $\prod g_i = 1$, then the product of their signs must be 1.

A second condition is based on a theorem of Scott [44, Theorem 1]:

Theorem 3.24 (Scott)**.** *Let G be a group generated by $g_1, \dots, g_n$ with $g_1 \cdots g_n = 1$ and let V be a finite-dimensional representation of G over any field. Then*

$$\sum_{i=1}^{n} v(g_i) \geq v(G) + v(G^*),$$

where $v(g_i) = \operatorname{codim} V^{g_i}$, $v(G) = \operatorname{codim} V^G$, $v(G^*) = \operatorname{codim}(V^*)^G$.

Since $v(g_i)$ only depends on the conjugacy class of g_i, and the order of the g_i is irrelevant for the condition, we see that Scott's theorem determines a test to identify the $c \in \mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$ which can potentially have a system of generators in their preimage. We will say that c passes Scott's test over $\mathbb{K}$ if the condition of Theorem 3.24 is satisfied for every finite-dimensional irreducible representation of G over $\mathbb{K}$.

For any field $\mathbb{K}$, we define

$$\mathcal{C}_G^{\mathbf{m},\mathbb{K}} = \{\tilde{c} \in \mathcal{C}_G^{\mathbf{m}} \mid \tilde{c} \text{ passes Frobenius' test and Scott's test over } \mathbb{K}\}.$$

Our implementation runs the test on a field $\mathbb{F}_q$, with q a fixed prime number greater than the group order. Since $\mathcal{C}_G^{\mathbf{m},\mathbb{F}_q}$ is invariant under $(\Sigma_r)_{\mathrm{m}}$ and $\operatorname{Aut} G$, this allows us to replace $\mathcal{C}_G^{\mathbf{m}}$ with $\mathcal{C}_G^{\mathbf{m},\mathbb{F}_q}$ in §3.10.

Example 3.25. In Example 3.16, consider the two-dimensional representation of Σ_4 obtained by pulling back the two-dimensional irreducible representation of Σ_3 (the morphism $\Sigma_4 \to \Sigma_3$ being given by the quotient by the group generated by C_2). Then

$$v(C_1) = 1, v(C_2) = 0, v(\Sigma_4) = 2 = v(\Sigma_4^*).$$

Thus, Scott's test eliminates all $\tilde{c}$ of the form (3.17) such that $k < 4$.

3.26. We also employed a technical optimization which deserves to be mentioned.

The condition $\langle g_1, \dots, g_{r-1}\rangle = G$ only depends on the set $\{g_1, \dots, g_{r-1}\}$, call it the *underlying set* of the r-ple $(g_1, \dots, g_r)$. Different elements in $G^{\mathbf{m}}$ can have the same underlying set; indeed, when $c, c' \in \mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$ contain the same conjugacy classes, possibly with different multiplicities, elements in $\pi^{-1}(c)$ and elements in $\pi^{-1}(c')$ can have the same underlying set.

Thus, when iterating over the sets $p^{-1}(\tilde{c})$ of potential spherical systems of generators, it makes sense to store in memory a list of underlying sets that are known to either generate G or not, and look up each underlying set in the list before actually performing the (costly) test to see whether a given r-ple actually generates the group. Since these lists can become quite large, one can save memory by observing that an element of $C_1 \times \cdots \times C_r$ cannot have the same underlying set as an element of $C'_1 \times \cdots \times C'_r$ unless $\{C_1, \dots, C_{r-1}\} = \{C'_1, \dots, C'_{r-1}\}$. Therefore, given a section F of $\mathcal{C}_G^{\mathbf{m},\mathbb{F}_q}$, we work separately on each component F_A of the partition

$$F = \bigsqcup_{A \subset \mathcal{C}_G} F_A, \quad F_A = \{(C_1, \dots, C_r) \in F \mid \{C_1, \dots, C_{r-1}\} = A\}.$$

The partition is computed with Algorithm 2.

Algorithm 2: Computing the section

input : A group G, a signature $\mathbf{m}$, a prime $q \geq |G|$
output: A section F of $\mathcal{C}_G^{\mathbf{m},\mathbb{F}_q}$, partitioned as in (3.26)

$F_A \leftarrow \emptyset$ for all $A \subset \mathcal{C}_G$;
$K \leftarrow \{(C_1, \ldots, C_r) \in \mathcal{C}_G^r \mid$
  $C_1 \leq \cdots \leq C_r$ and some permutation $(C_{\sigma_1}, \ldots, C_{\sigma_r})$ is in $\mathcal{C}_G^{\mathbf{m}}\}$;
/* $K = \mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$, represented as in (3.20)) */
$S \leftarrow$ a section for the action of $\operatorname{Aut} G$ on K
for $(C_1, \ldots, C_r)$ *in* S **do**
  if $(C_1, \ldots, C_r)$ *passes Frobenius' test and Scott's test over* $\mathbb{F}_q$ **then**
    add the sequence $(C_1, \ldots, C_r)$ to the set $F_{\{C_1,\ldots,C_{r-1}\}}$
return $F = \bigcup F_A$

3.27. In theory, a section in $\mathscr{D}_{G,\mathbf{m}} := \mathscr{D}^r(G) \cap G^{\mathbf{m}} \subset G^{\mathbf{m}}$ can be obtained by computing S' as in Proposition 3.15, then verifying for each element $(g_1, \ldots, g_r)$ whether it is a spherical system of generators. A bit of experimenting shows that it is better to identify the subset of $p^{-1}(\tilde{c})$ consisting of generators, before applying the action of $\mathbf{H}_{\tilde{c}}$ to extract a section.

We also point out that in a spherical system of generators $(g_1, \ldots, g_r)$, the last element is determined by the others; thus, given $\tilde{c} = (C_1, \ldots, C_r) \in \mathcal{C}_G^{\mathbf{m}}$, spherical generators in $p^{-1}(\tilde{c})$ can be determined by iterating in $C_1 \times \cdots \times C_{r-1}$, and testing for each element if the inverse of the product is in C_r.

The number of iterations can therefore be reduced by choosing $\tilde{c} = (C_1, \ldots, C_r)$ in such a way that the last conjugacy class is the biggest. Since we have $C_1 \leq \cdots \leq C_r$ relative to the fixed ordering of $\mathcal{C}_G$, it suffices to choose the latter in such a way that conjugacy classes with more elements come after.

This leads to Algorithm 3.

3.28. For dihedral groups of order $4k + 2$, our problem is the object of one of the main results in [8]: Theorem 2 of that paper shows that given $\tilde{c}$ in $\mathcal{C}_G^{\mathbf{m}}$ there is at most one orbit of systems of spherical generators in $p^{-1}(\tilde{c})$. Indeed, if the order is of the form $4k + 2$, the *numerical type* defined in [8, Definition 2] corresponds exactly to the class of c modulo the action of $\operatorname{Aut} G$.

Therefore, instead of computing the whole set of systems of generators mapping to $\tilde{c}$ as in Algorithm 3, it is sufficient to iterate through $p^{-1}(\tilde{c})$ and stop as soon as a system of generators is found.

3.29. For abelian groups G, conjugacy classes contain a single element and the map p of Diagram 3.12 is injective, with the action of B_r reducing to an action of Σ_r. Therefore, having computed a section S for the action of $\operatorname{Aut} G$ on $\mathcal{C}_G^{\mathbf{m}}/(\Sigma_r)_{\mathbf{m}}$ exactly as in the nonabelian case, one only needs to determine for each element of S whether its preimage in $G^{\mathbf{m}}$ is a spherical system of generators. The tests of Scott and Frobenius become redundant

Algorithm 3: Classifying spherical systems of generators for fixed G, $\mathbf{m}$

input : A group G of order d; a signature $\mathbf{m} \in \mathfrak{S}_{d,g_{\max}}$
output: One representative in each Hurwitz equivalence class of spherical systems of generators of G with signature $\mathbf{m}$

$q \leftarrow$ the smallest prime number greater than d;
$F \leftarrow$ a section of $\mathcal{C}_G^{\mathbf{m},\mathbb{F}_q}$, partitioned as in (3.26);
for $A \subset \mathcal{C}_G$ **do**
  generating $\leftarrow \{\}$;
  notgenerating $\leftarrow \{\}$;
  for $(C_1, \dots, C_r)$ *in* F_A **do**
    $X \leftarrow \{\}$;
    for $(g_1, \dots, g_{r-1})$ *in* $C_1 \times \cdots \times C_{r-1}$ **do**
      $g_r \leftarrow (g_1 \cdots g_{r-1})^{-1}$;
      if $g_r \in C_r$ *and* $\{g_1, \dots, g_{r-1}\} \notin$ *notgenerating* **then**
        if $\{g_1, \dots, g_{r-1}\} \in$ *generating or* $\langle g_1, \dots, g_{r-1} \rangle = G$ **then**
          add $\{g_1, \dots, g_{r-1}\}$ to generating;
          add $(g_1, \dots, g_r)$ to X;
        else
          add $\{g_1, \dots, g_{r-1}\}$ to notgenerating;
    if X *not empty* **then**
      $\mathbf{H}_{\tilde{c}} \leftarrow$ stabilizer of $(C_1, \dots, C_r)$ in $\mathbf{H}_{\mathbf{m}}$;
      append to output a section of X for the action of $\mathbf{H}_{\tilde{c}}$

here, since for fixed elements $(g_1, \dots, g_r)$ it is more efficient to check the conditions $\prod g_i = 1$ and $\langle g_1, \dots, g_r \rangle = G$ directly.

3.30. Running our implementation [14] of the above-illustrated algorithms, we have been able to classify topological types of holomorphic actions on Riemann surfaces (equivalently of orientation-preserving actions on orientable topological surfaces) of genus $g \leq 39$ with genus 0 quotient, with only three exceptions:

$$
\begin{aligned}
G &= (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2, & \mathbf{m} &= \{2,2,2,2,2,2,2,2,2,2\}, & g &= 28;\\
G &= (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2, & \mathbf{m} &= \{2,2,2,2,2,2,2,2,2,2,3\}, & g &= 34;\\
G &= (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2, & \mathbf{m} &= \{2,2,2,2,2,2,2,2,2,2,2,2\}, & g &= 37.
\end{aligned}
$$

In these cases, the number of spherical systems of generators is too large to fit into the memory of the computer at our disposal.

The number of topological types by genus is summarized in Table 1. A strict inequality such as > 3580 for $g = 28$ refers to the fact that the program classifies 3580 topological types with groups and signatures distinct from the offending group and signature, which gives rise to at least one more topological type.

TABLE 1. Number of topological types of Galois covers of the line with genus g

g	# types	g	# types	g	# types
2	19	15	768	28	> 3580
3	46	16	687	29	8169
4	65	17	1473	30	3992
5	92	18	711	31	8506
6	95	19	1689	32	4336
7	160	20	881	33	16007
8	129	21	2790	34	> 6983
9	343	22	1546	35	11827
10	289	23	2178	36	8753
11	342	24	1852	37	> 26712
12	317	25	5955	38	8486
13	741	26	1881	39	19099
14	323	27	4351		

The three exceptions above, for which we were not able to finish the computation, all share the same group, i.e. $G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$. This is the semidirect product of $A := \mathbb{Z}_3 \times \mathbb{Z}_3$ with $\mathbb{Z}_2$ defined by the morphism $[1]_2 \mapsto \varphi \in \operatorname{Aut} A$, where $\varphi(a) = -a$; it is denoted by `Smallgroup(18,4)` in the `MAGMA` database. This group belongs to the family of so-called *generalized dihedral groups*, i.e. groups of the form $G = A \rtimes \mathbb{Z}_2$, with A abelian and morphism $[1]_2 \mapsto \varphi$ as above. When the order of A is odd, these groups are naturally challenging for our algorithm, since they have a very big conjugacy class, the complement of the index 2 subgroup A. For A cyclic, i.e. for G a "standard" dihedral group, we were able to avoid heavy computations by applying the results of [8], as explained in §3.28. We suspect that a more complicated analysis could yield a similar result also for more general groups of the form $A \rtimes \mathbb{Z}_2$. Apart from the theoretical importance, this would allow to reach the classification of topological types up to 39 or 40 without need of more computations. More precisely the invariant in [9] might give results analogous to those in [8] for a wider class of generalized dihedral groups. We hope to be able to give some results in this direction in a forthcoming paper.

References

[1] I. Bauer, F. Catanese, F. Grunewald, R. Pignatelli. Quotients of products of curves, new surfaces with $p_g = 0$ and their fundamental groups, *American J. of Math.* **134**, (2012), 993–1049.

[2] I. Bauer, R. Pignatelli. The classification of minimal product-quotient surfaces with $p_g = 0$, *Math. Comp* **81** (2012), no. 280, 2389–2418.

[3] I. Bauer, R. Pignatelli. Product-quotient surfaces: new invariants and algorithms, *Groups Geom. Dyn.* **10** (2016), no. 1, 319–363.

[4] A. Behm, A.M. Rojas, M. Tello-Carrera, A SAGE Package for n-Gonal Equisymmetric Stratification of $\mathcal{M}_g$. *Experimental Mathematics.* 2020. To appear `https://doi.org/10.1080/10586458.2020.1763872`.

[5] J. S. Birman. Braids, links, and mapping class groups. Princeton University Press, Princeton, N.J., 1974. Annals of Mathematics Studies, No. 82.
[6] W. Bosma, J. Cannon, C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. *Computational algebra and number theory* (London, 1993).
[7] T. Breuer. Characters and automorphism groups of compact Riemann surfaces, volume 280 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000.
[8] F. Catanese, M. Lönne, F. Perroni. Irreducibility of the space of dihedral covers of the projective line of a given numerical type. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 22(3):291–309, 2011.
[9] F. Catanese, M. Lönne, F. Perroni. The irreducible components of the moduli space of dihedral covers of algebraic curves. *Groups Geom. Dyn.*, 9(4):1185–1229, 2015.
[10] F. Catanese, M. Lönne, F. Perroni. Genus stabilization for the components of moduli spaces of curves with symmetries. *Algebr. Geom.*, 3(1):23–49, 2016.
[11] G. Carnovale, F. Polizzi. The classification of surfaces with $p_g = q = 1$ isogenous to a product of curves *Adv. Geom.* 9 (2009), no. 2, 233–256.
[12] M.D.E. Conder. Large group actions on surfaces. In *Riemann and Klein surfaces, Automorphisms, Symmetries and Moduli Spaces*, Contemporary Mathematics, 629, pages 77–97, AMS, 2014.
[13] D. Conti, A.C. Ghigi, R. Pignatelli. Some evidence for the Coleman-Oort conjecture. *Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Mat. RACSAM*, 116(1):50, 2022.
[14] D. Conti, A. Ghigi, R. Pignatelli. *Gullinbursti*, a `MAGMA` program to classify topological types of Galois covers of the projective line. `https://github.com/diego-conti/gullinbursti`.
[15] P. Dèbes. Revêtements topologiques. In *Arithmétique de revêtements algébriques (Saint-Étienne, 2000)*, volume 5 of *Sémin. Congr.*, pages 163–214. Soc. Math. France, Paris, 2001.
[16] B. Farb, D. Margalit. A Primer on Mapping Class Groups, Princeton University Press, Princeton and Oxford, 2012.
[17] D. Frapporti, R. Pignatelli. Mixed quasi-étale quotients with arbitrary singularities, *Glasg. Math. J.* **57** (2015), no. 1, 143–165.
[18] P. Frediani, A. Ghigi, M. Penegini. Shimura varieties in the Torelli locus via Galois coverings. *Int. Math. Res. Not.* 2015, no. 20, 10595-10623.
[19] P. Frediani, M. Penegini and P. Porru. Shimura varieties in the Torelli locus via Galois coverings of elliptic curves. *Geometriae Dedicata* 181 (2016) 177-192.
[20] P. Frediani and F. Neumann, Étale homotopy types of moduli stacks of algebraic curves with symmetries. *K-Theory* 30 (2003), no. 4, 315-340.
[21] M.D. Fried, H. Völklein. The inverse Galois problem and rational points on moduli spaces, *Mathematische Annalen*, 290 (1991), 771-800.
[22] Ch. Gleißner. Threefolds Isogenous to a Product and Product quotient Threefolds with Canonical Singularities. PhD Dissertation. Bayreuth, 2016. `https://epub.uni-bayreuth.de/2981`.
[23] A. Ghigi, C. Tamborini. A topological construction of families of Galois covers of the line. Preprint.*ArXiv: 2204.07817.* 2022.
[24] G. González Díez, W. J. Harvey. Moduli of Riemann surfaces with symmetry. In *Discrete groups and geometry (Birmingham, 1991)*, volume 173 of *London Math. Soc. Lecture Note Ser.*, pages 75–93. Cambridge Univ. Press, Cambridge, 1992.
[25] B. Huppert. Endliche Gruppen. I. Springer-Verlag, Berlin-New York, 1967.
[26] N.V. Ivanov. Mapping class groups, In R.J. Daverman and R.B. Sher, *Handbook of geometric topology*, pages 523–633, North-Holland, Amsterdam, 2002.
[27] G.A. Jones. Enumeration of homomorphisms and surface-coverings. *Quart. J. Math. Oxford* (2) 46 (1995), 485–507.
[28] A. Kuribayashi, H. Kimura. Automorphism groups of compact Riemann surfaces of genus five. *J. Algebra*, 134(1):80–103, 1990.
[29] I. Kuribayashi, A. Kuribayashi. Automorphism groups of compact Riemann surfaces of genera three and four. *J. Pure Appl. Algebra*, 65(3):277–292, 1990.

[30] S. K. Lando, A. K. Zvonkin, Graphs on Surfaces and Their Applications, volume 141 of *Encyclopaedia of Mathematical Sciences*. Springer, 2004.

[31] K. Magaard, T. Shaska, S. Shpectorov, H. Völklein. The locus of curves with prescribed automorphism group. *Sūrikaisekikenkyūsho Kōkyūroku*, (1267):112–141, 2002. Communications in arithmetic fundamental groups (Kyoto, 1999/2001).

[32] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[33] E. Mistretta, F. Polizzi. Standard isotrivial fibrations with $p_g = q = 1$. II. *J. Pure Appl. Algebra* 214 (2010), no. 4, 344–369.

[34] B. Moonen. Special subvarieties arising from families of cyclic covers of the projective line. *Doc. Math.*, 15:793–819, 2010.

[35] J. Paulhus. A database of group actions on Riemann surfaces. 2017. In: I. Cheltsov, X. Chen, L.Kadzarkov, J.Park (editors), *Birational Geometry, Kähler-Einstein Matrices and Degeneration*, volume 409 of *Springer Proceedings in Mathematics and Statistics*. To appear. https://link.springer.com/book/9783031178580.

[36] M. Penegini. Surfaces isogenous to a product of curves, braid groups and mapping class groups. In *Beauville surfaces and groups*, volume 123 of *Springer Proc. in Mathe. Stat.*, pages 129-148.

[37] M. Penegini. The classification of isotrivially fibred surfaces with $p_g = q = 2$. With an appendix by Sönke Rollenske. *Collect. Math.* 62 (2011), no. 3, 239–274.

[38] F. Perroni. Smooth covers of moduli stacks of Riemann surfaces with symmetries, . *Boll. Unione Mat. Ital.* 15 (2022), no. 1-2, 333-342.

[39] R. Pignatelli. Quotients of the square of a curve by a mixed action, further quotients and Albanese morphisms. *Rev. Mat. Complut.* 33 (2020), no. 3, 911–931.

[40] R. Pignatelli, F. Polizzi. A family of surfaces with $p_g = q = 2$, $K^2 = 7$ and Albanese map of degree 3. *Math. Nachr.* 290 (2017), no. 16, 2684–2695.

[41] F. Polizzi. Standard isotrivial fibrations with $p_g = q = 1$, *J. Algebra* 321 (2009), no. 6, 1600–1631

[42] S. Reyes-Carocca, A. Rojas. On large prime actions on Riemann surfaces. *Journal of Group Theory*, 2022, 25(5), 887-940. https://doi.org/10.1515/jgth-2020-0140

[43] J.J. Rotman. An Introduction to the Theory of Groups. 4th edn. Springer-Verlag, New York, 1995.

[44] L.L. Scott. Matrices and cohomology. *Ann. Math.* 105 (1977), 473–492.

[45] H. Völklein. Moduli spaces for covers of the Riemann sphere. *Israel J. Math.* 85 (1994), no. 1-3, 407-430.

[46] H. Zieschang, E. Vogt, H.-D. Coldewey. Surfaces and planar discontinuous groups, volume 835 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

Università di Pisa
Email address: diego.conti@unipi.it

Università di Pavia
Email address: alessandro.ghigi@unipv.it

Università di Trento
Email address: Roberto.Pignatelli@unitn.it