



HAL
open science

DECOMPOSING JACOBIANS VIA GALOIS COVERS

Elisa Lorenzo García, Davide Lombardo, Christophe Ritzenthaler, Jeroen Sijssling

► **To cite this version:**

Elisa Lorenzo García, Davide Lombardo, Christophe Ritzenthaler, Jeroen Sijssling. DECOMPOSING JACOBIANS VIA GALOIS COVERS. *Experimental Mathematics*, 2023, 32 (1), pp.218-240. 10.1080/10586458.2021.1926008 . hal-02512858

HAL Id: hal-02512858

<https://hal.science/hal-02512858>

Submitted on 20 Mar 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

DECOMPOSING JACOBIANS VIA GALOIS COVERS

DAVIDE LOMBARDO, ELISA LORENZO GARCÍA, CHRISTOPHE RITZENTHALER,
AND JEROEN SIJSLING

ABSTRACT. Let $\phi : X \rightarrow Y$ be a (possibly ramified) cover between two algebraic curves of positive genus. We develop tools that may identify the Prym variety of ϕ , up to isogeny, as the Jacobian of a quotient curve C in the Galois closure of the composition of ϕ with a well-chosen map $Y \rightarrow \mathbb{P}^1$. This method allows us to recover all previously obtained descriptions of a Prym variety in terms of a Jacobian that are known to us, besides yielding new applications. We also find algebraic equations for some of these new cases, including one where X has genus 3, Y has genus 1 and ϕ is a degree 3 map totally ramified over 2 points.

INTRODUCTION

Let k be an algebraically closed field of characteristic 0, and let X/k be a smooth projective irreducible curve of genus $g > 0$. Already in the 19th century, complex geometers were interested in understanding the periods of X in terms of periods of curves of smaller genera. In modern terms, one would like to decompose the Jacobian $\text{Jac}(X)$ of X as a product (up to isogeny) of powers of non-trivial simple abelian sub-varieties A_i , and then interpret the A_i as Jacobians of suitable curves C_i . This is not possible for every curve X : Jacobians are generically simple, and even in those cases when $\text{Jac}(X)$ does decompose there is no reason for the simple factors A_i to be isogenous to Jacobians of curves. Indeed, while using a suitable isogeny allows us to assume that the A_i are principally polarized, such abelian varieties are generically not Jacobians if $\dim(A_i) \geq 4$.

When the automorphism group of X is non-trivial, one can often find some curves C_i as above as quotients of X by well-chosen subgroups of G , and in certain cases one even gets all of the A_i in this way. This strategy has been employed many times, frequently in combination with the Kani-Rosen formula [KR89], to get (more or less explicit) examples of Jacobians whose isogeny factors are again Jacobians. For instance, when $g = 2$ and $\#G > 2$, this strategy always gives the full decomposition of $\text{Jac } X$ [GS01], and more examples have been worked out in [Pau08, PR17, IJR19]. In Section 1 we give analogous results for $g = 3$, both for hyperelliptic and non-hyperelliptic curves X . We show that the decomposition of the Jacobian of a generic curve with a given non-trivial automorphism group can indeed be obtained in terms of quotients

Date: March 17, 2020.

2010 Mathematics Subject Classification. 14K20, 14K25, 14J15, 11F46, 14L24.

Key words and phrases. Siegel modular forms, plane quartics, invariants, generators, explicit.

We acknowledge support from the PICS JADERE (281036) from the French CNRS. The fourth author was moreover supported by a Juniorprofessurenprogramm of the Science Ministry of Baden-Württemberg. Part of the work for this paper was carried out at the workshop “Arithmetic of Curves”, held in Baskerville Hall in August 2018. We would like to thank the organisers Alexander Betts, Tim Dokchitser, Vladimir Dokchitser, Céline Maistret and Beryl Stapleton, as well as the Baskerville Hall staff, for providing a great opportunity to concentrate on this project.

of X in all cases, except when

$$g(X) = 3, X \text{ non-hyperelliptic, } \text{Aut}(X) \cong C_2 \text{ or } \text{Aut}(X) \cong C_6. \quad (\star)$$

In this scenario, the quotient X/G is an explicit genus 1 curve Y , but (even up to isogeny) the complementary abelian surface A cannot be interpreted as the Jacobian of a quotient of X . However, equations for a curve C such that $A \sim \text{Jac}(C)$ have been worked out also in this case, by a technique that we now briefly recall.

The aforementioned complementary abelian surface A is an example of a *Prym variety*. Recall that the (generalized) Prym variety of a cover $\pi : X \rightarrow Y$ is defined as the identity component $P := \text{Prym}(X/Y)$ of the kernel $\ker(\pi_*)$ of the pushforward map $\pi_* : \text{Jac } X \rightarrow \text{Jac } Y$ induced by π . There is a significant body of literature dedicated to the description of P in many special situations. The case when π is an unramified cover of degree 2 is especially beautiful and well-understood [Mum74]. In this case P inherits a principal polarization from $\text{Jac } X$, and in some circumstances it has been described as the Jacobian of an explicit curve (see [Mum74, p.346], [Lev12] or [Bru08]). In the situation (\star) , the morphism $X \rightarrow X/C_2$ is *not* étale, but it was shown in [RR18] that one could realize this map as the degeneration of a family of étale covers between curves of genera 5 and 3, and using the previously mentioned work [Bru08] it was possible to give an explicit equation for a curve C such that $P \sim \text{Jac}(C)$. This result is recalled in Section 2. It is however unclear how this idea may be extended to other types of covers.

The present paper was motivated by the desire to find an alternative proof of the previous result which could lead to generalizations. Our main sources of inspiration were Donagi's work on Prym varieties [Don92], based on Galois-theoretic considerations, and a specific construction by [Dal75] in the setting when $X \rightarrow Y$ is a cover of degree 2 of a hyperelliptic curve branched at 2 points Q_1 and Q_2 (see also [Lev12, Th.4.1]). In this latter work, P is realized as the Jacobian of a curve C obtained as a quotient of the Galois closure Z of $X \rightarrow Y \rightarrow \mathbb{P}^1$ by a well-chosen subgroup of the automorphism group of Z . Here, the cover from Y to \mathbb{P}^1 is the hyperelliptic quotient, and generically Q_1 and Q_2 are not sent to the same point of \mathbb{P}^1 . In the case (\star) however, the cover $X \rightarrow Y$ has 4 branched points, and one has to carefully choose a map from $Y \rightarrow \mathbb{P}^1$ which collapses 2 of them. With this particular choice, we show in Section 2 that P is again realized up to isogeny as the Jacobian of an explicit quotient of the Galois closure Z of the composed morphism $X \rightarrow Y \rightarrow \mathbb{P}^1$.

We then set out to see to what extent this somewhat miraculous construction could yield results for other classes of (not necessarily Galois) morphisms $X \rightarrow Y$. There are two main difficulties in carrying out this program. One is fundamental: given a cover $\pi_{X/Y} : X \rightarrow Y$, there is no a priori reason for the Prym variety to appear as the Jacobian of a quotient of a related Galois cover. In fact the general principally polarized abelian variety of dimension 4 is known to be a Prym variety, and by [Tsi12] we know that there are 4-dimensional abelian varieties over $\overline{\mathbb{Q}}$ that are not $\overline{\mathbb{Q}}$ -isogenous to a Jacobian. The second difficulty lies in the choice of the morphism $Y \rightarrow \mathbb{P}^1$: the Galois closure Z of the composition $X \rightarrow Y \rightarrow \mathbb{P}^1$ depends very strongly on this choice, and we did not find a general principle to guide us. In fact, as already mentioned, there is little previous work concerning Prym varieties when the degree of $\pi_{X/Y}$ is greater than 2, and the present project is mainly exploratory.

The existing literature seems to have focused on two main cases: (1) the consideration of Galois or étale covers $X \rightarrow Y$ [LO18, LO11] and (2) a top-down approach, which starts with

a curve Z with large automorphism group G and decomposes of $\text{Jac}(Z)$ in terms of Prym varieties of subcovers $Z/H \rightarrow Z/G$ [RR06] (see also the more complete arXiv version [RR03]). Our approach combines aspects of these previous methods, in that it starts with a completely general map $X \rightarrow Y$ and finds candidates for the Prym variety in terms of the Galois closure of a suitable composition $X \rightarrow Y \rightarrow \mathbb{P}^1$. Finding examples for which this approach yields results is by no means straightforward: it is hard to get explicit equations for the curves, and the Galois groups of the composed maps rapidly attain prohibitive size.

In order to be able to analyze complicated situations, we use powerful tools from monodromy theory, which we implemented in the computer algebra system MAGMA [BCP97] (be aware that we use version 2.25-3 and that our programs do not always work with version 2.24-5). Specifying covers $X \rightarrow Y \rightarrow \mathbb{P}^1$ by their ramification structure, we can describe all possible monodromy types for the branched cover $X \rightarrow \mathbb{P}^1$, which in turn yields complete Galois-theoretic information on the Galois closure $Z \rightarrow \mathbb{P}^1$ of this map. The enumeration of possible monodromy types is a classical problem, often used in the setting of Galois covers [Bre00, Pau15]. In Section 3 we recall the relevant theory and show how to adapt it in our cases, when the covers $X \rightarrow Y$ and $X \rightarrow \mathbb{P}^1$ need not be Galois. A crucial tool in our applications is a beautiful result by Chevalley and Weil [CWH34, Wei35], by means of which one can identify, for a given Galois quotient $\pi_{Z/C} : Z \rightarrow C$, the image of $H^0(C, \Omega_C^1)$ by $\pi_{Z/C}^*$ inside $H^0(Z, \Omega_Z^1)$. Since we can similarly describe the images under pullback of $H^0(X, \Omega_X^1)$ and $H^0(Y, \Omega_Y^1)$, intersecting these subspaces allows us to decide if $\text{Jac } C$ is isogenous to $\text{Prym}(X/Y)$. Implementation details are given in Section 4 and the code can be found at [LLGRS20].

By using this approach, we could (up to the limitations imposed by keeping the running time of our programs acceptable) recover all situations previously known in the literature, see Section 5. We also found some new cases. For example, consider a cover $X \rightarrow Y$ of degree d , where Y is an elliptic curve, totally ramified over 2 points Q_1, Q_2 of Y , and compose it with the map $Y \rightarrow \mathbb{P}^1$ which identifies Q_1 and Q_2 . For $d = 3, 4$, and for some cases with $d = 5$ (see Table 8), we have been able to check within reasonable time that the abelian variety $\text{Prym}(X/Y)$ is indeed isogenous to the Jacobian of a quotient C of the Galois closure Z of $X \rightarrow Y \rightarrow \mathbb{P}^1$. When $d = 3$ and $X \rightarrow Y$ is a non-Galois cover, it turns out that X and the corresponding Galois closure Z of genus 5 are hyperelliptic. Using this information, we were able to write down equations for X and Y , and to find an explicit equation for a curve C for which $\text{Jac}(C) \sim \text{Prym}(X/Y)$, see Section 5.3. In another direction, we were able to generalize the example of [Bru08] (a genus-5 étale cover of degree 2 of a genus 3 curve) to genus $g_X = 2g + 1$ étale covers of degree 2 of genus $g_Y = g$ curves with $g = 4, 5$ or 6, where Y is a generic trigonal curve. In particular, for $g_Y = 4$ we cover all generic non-hyperelliptic cases in this way.

Finally, we remark that our construction can also be seen through the lens of Belyi's theorem. Indeed, Belyi's result guarantees that all algebraic curves arise as covers of \mathbb{P}^1 ramified over just 3 points, and our approach usually consists in finding a morphism $Y \rightarrow \mathbb{P}^1$ such that the branch locus of $X \rightarrow Y \rightarrow \mathbb{P}^1$ is smaller than it would be for a generic choice of the map $Y \rightarrow \mathbb{P}^1$. In fact, this suggests that we are only scratching the surface, handling just the easiest of cases, and it might even be possible to *always* recover the curves C_i , if they exist, by choosing a suitable morphism $Y \rightarrow \mathbb{P}^1$. The problem of decomposing the Prym variety of $X \rightarrow Y$ then becomes that of choosing an appropriate rational function on Y , a point of view which seems to be genuinely

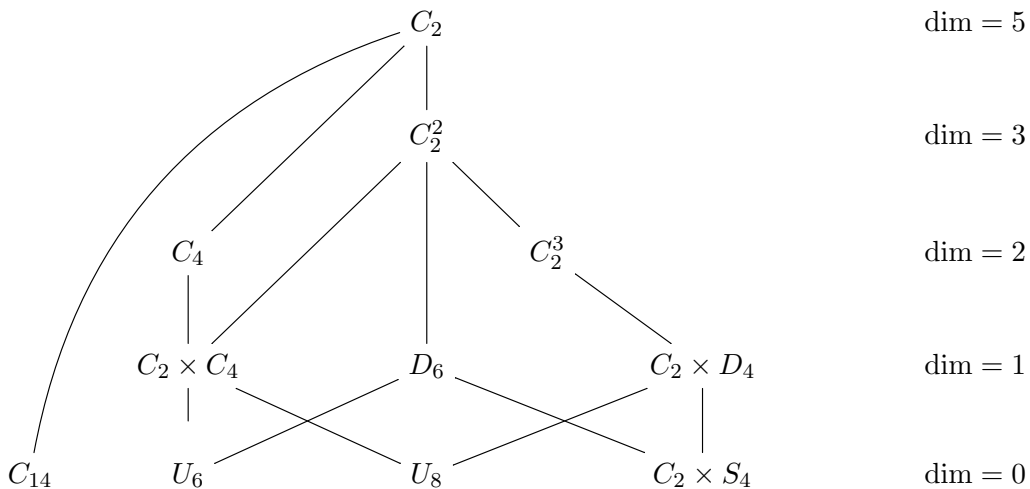
new. We think that these experiments and theoretical motivations are sufficiently intriguing for the relations between Prym varieties and Galois constructions to merit further study.

1. DECOMPOSING JACOBIANS OF CURVES OF GENUS 3 WITH NON-TRIVIAL AUTOMORPHISM GROUP

Let k be an algebraically closed field of characteristic 0. We will implicitly assume that $k = \mathbb{C}$ throughout this article, especially in Section 3 when using the theory of covers. We do note that the results thus obtained will still be valid when the characteristic of k does not divide the order of the intervening Galois groups — for example, the results in the current section continue to apply when k has finite characteristic strictly larger than 7.

In this section we consider the decomposition of Jacobians of curves of genus 3 induced by the action of their automorphism group. Most of these results are folklore. Note that this approach does not always yield the full decomposition of the Jacobian, nor can it guarantee that the higher-dimensional factors found in this way are irreducible.

1.1. Hyperelliptic case. There is a stratification of the moduli space of hyperelliptic curves of genus 3 by their automorphism group (see [Bou98, LR12] and the references in the latter). The inclusions between the different strata are summarized in the following diagram, where we write C_n for the cyclic group of order n , D_n for the dihedral group of order $2n$, S_n for the symmetric group over n elements and U_6 and U_8 for certain groups with respectively 24 and 32 elements:



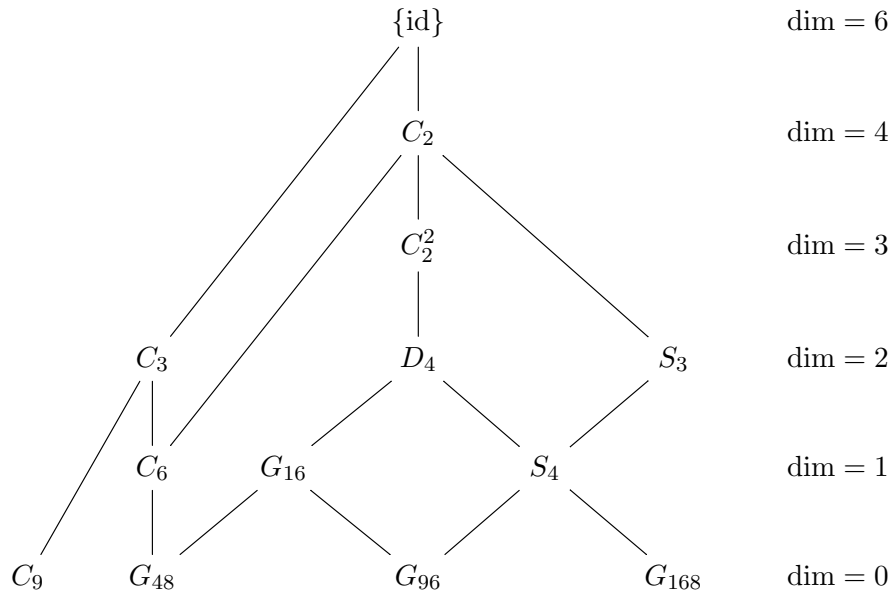
Proposition 1.1. *Suppose X is a hyperelliptic curve of genus 3 whose automorphism group contains a group G appearing in the previous diagram. Then the Jacobian of X decomposes up to isogeny as in Table 1.*

1.2. Non-hyperelliptic case. A similar analysis can be carried out in the non-hyperelliptic case, with the notable exception of the group C_2 and its specialization C_6 which shall be reviewed in Section 2. There is a stratification of the moduli space of non-hyperelliptic genus 3 curves according to their automorphism group (see [Hen76, 2.88], [Ver83, p.62], [MSSV02], [Bar06] and [Dol12]; the groups G_i are certain groups of order i). The inclusions between the different

G	$X : y^2 = f(x)$	$\text{Jac}(X) \sim \prod_{i \in I} \text{Jac}(C_i)$	Curves C_i
C_2			$\text{Jac}(X)$ generically simple
C_2^2	$x^8 + ax^6 + bx^4 + cx^2 + 1$	$I = [1, 2]$	$\begin{cases} C_1 : y^2 = x^4 + ax^3 + bx^2 + cx + 1, \\ C_2 : y^2 = x(x^4 + ax^3 + bx^2 + cx + 1) \end{cases}$
C_2^3	$x^8 + ax^6 + bx^4 + ax^2 + 1$	$I = [1, 2, 3]$	$\begin{cases} C_1 : y^2 = x^4 + ax^3 + bx^2 + ax + 1, \\ C_2 : y^2 = x^4 + (a-4)x^2 - 2a + b + 2 \\ C_3 : y^2 = x^4 + (a+4)x^2 + 2a + b + 2 \end{cases}$
C_4	$x(x^2 - 1)(x^4 + ax^2 + b)$		$\text{Jac}(X)$ generically simple with endomorphism algebra $\mathbb{Q}(i)$
$C_2 \times C_4$	$x^8 + ax^6 - ax^2 - 1 = (x^4 - 1)(x^4 + ax^2 + 1)$	$I = [1, 2]$	$\begin{cases} C_1 : y^2 = (x^2 - 1)(x^2 + ax + 1) \\ C_2 : y^2 = x(x^2 - 1)(x^2 + ax + 1) \end{cases}$
D_6	$x(x^6 + ax^3 + 1)$	$I = [1, 2, 2]$	$\begin{cases} C_1 : y^2 = x(x^2 + ax + 1) \\ C_2 : y^2 = x^3 - 3x + a \end{cases}$
$C_2 \times D_4$	$x^8 + ax^4 + 1$	$I = [1, 2, 2]$	$\begin{cases} C_1 : y^2 = x^4 + ax^2 + 1 \\ C_2 : y^2 = x^4 - 4x^2 + (a + 2) \end{cases}$
C_{14}	$x^7 - 1$		$\text{Jac}(X)$ simple with endomorphism algebra $\mathbb{Q}(\zeta_7)$
U_6	$x(x^6 + 1)$	$I = [1, 1, 1]$	$C_1 : y^2 = x^3 + x$, i.e., $j = 1728$
$C_2 \times S_4$	$x^8 + 14x^4 + 1$	$I = [1, 1, 1]$	$C_1 : y^2 = x^3 + x^2 - 4x - 4$, i.e., $j = 2^4 \cdot 3^{-2} \cdot 13^3$
U_8	$x^8 + 1$	$I = [1, 2, 2]$	$\begin{cases} C_1 : y^2 = x^4 + 1, \text{ i.e., } j = 1728 \\ C_2 : y^2 = x^4 - 4x^2 + 2, \text{ i.e., } j = 2^6 \cdot 5^3 \end{cases}$

TABLE 1. Decomposition of Jacobian: hyperelliptic case

strata are summarized in the following diagram:



Proposition 1.2. *Suppose X is a non-hyperelliptic curve of genus 3 whose automorphism group contains a group G appearing in the previous diagram. Then the Jacobian of X decomposes up to isogeny as in Table 2.*

2. PLANE QUARTICS WITH AUTOMORPHISM GROUP C_2 OR C_6

Let X/k be a non-hyperelliptic curve of genus 3 with automorphism group C_2 . The action of the automorphism induces a map $\pi : X \rightarrow Y$ of degree 2, where Y is an elliptic curve. Hence we know that $\text{Jac } X \sim Y \times A$, but A is not the Jacobian of a subcover of X . Indeed, the Riemann-Hurwitz formula shows that any morphism $X \rightarrow C$ with $g(C) = 2$ must be of degree 2, hence should come from another involution of X . The problem of describing A up to isogeny as the Jacobian of an explicit curve C of genus 2 was solved in [RR18] by relying on a suitable

G	$X : F(x, y, z) = 0$	$\text{Jac}(X) \sim \prod_{i \in I} \text{Jac}(C_i)$	Curves C_i
C_2			see Section 2
C_2^2	$x^4 + y^4 + z^4 + rx^2y^2 + sy^2z^2 + tz^2x^2$	$I = [1, 2, 3]$	$\begin{cases} C_1 : y^2 = (1/4r^2 - 1)x^4 + (1/2rs - t)x^2 + (1/4s^2 - 1), \\ C_2 : y^2 = (1/4s^2 - 1)x^4 + (1/2st - r)x^2 + (1/4t^2 - 1), \\ C_3 : y^2 = (1/4t^2 - 1)x^4 + (1/2tr - s)x^2 + (1/4r^2 - 1), \end{cases}$
C_3	$x^3z + y(y-z)(y-rz)(y-sz)$		Jac(X) generically simple with endomorphism algebra $\mathbb{Q}(\sqrt{-3})$
D_4	$x^4 + y^4 + z^4 + rx^2yz + sy^2z^2$	$I = [1, 2, 2]$	$\begin{cases} C_1 : y^2 = x^4 + (r^2/4 - s)x^2 + 1, \\ C_2 : y^2 = (-s - 2 + r^2/4)x^4 - 2rx^2 - s + 2 \end{cases}$
S_3	$x(y^3 + z^3) + y^2z^2 + rx^2yz + sx^4$	$I = [1, 1, 2]$	$\begin{cases} C_1 : y^2 = -x^3 + 9/4x^2 - 3/2rx + r^2/4 - s \\ C_2 : y^2 = x^4 + 2rx^3 + (r^2 - 4s)x^2 - sx \end{cases}$
C_6	$x^3z + y^4 + ry^2z^2 + z^4$	$I = [1, 2]$	See Section 2
G_{16}	$x^4 + y^4 + z^4 + ry^2z^2$	$I = [1, 2, 2]$	$\begin{cases} C_1 : y^2 = x^4 - rx^2 + 1 \\ C_2 : y^2 = (-r - 2)x^4 - r + 2 \end{cases}$
S_4	$x^4 + y^4 + z^4 + r(x^2y^2 + y^2z^2 + z^2x^2)$	$I = [1, 1, 1]$	$C_1 : y^2 = (1/4r^2 - 1)x^4 + (1/2r^2 - r)x^2 + (1/4r^2 - 1)$
C_9	$x^3y + y^3z + z^4$		Jac(X) simple with endomorphism algebra $\mathbb{Q}(\zeta_9)$
G_{48}	$x^4 + (y^3 - z^3)z$	$I = [1, 2, 2]$	$\begin{cases} C_1 : y^2 = x^3 + 1 \\ C_2 : y^2 = x^3 + x \end{cases}$
G_{96}	$x^4 + y^4 + z^4$	$I = [1, 1, 1]$	$C_1 : y^2 = x^3 + x$
G_{168}	$x^3y + y^3z + z^3x$	$I = [1, 1, 1]$	$C_1 : y^2 + xy + y = x^3 - x^2 - 2680x + 66322,$ i.e., $j = -3375$

TABLE 2. Decomposition of the Jacobian: non-hyperelliptic case

deformation of π to an étale cover between curves of genera 5 and 3. This result is recalled below. Since every non-hyperelliptic genus 3 curve with an involution can be written in the form (2.1), this completes the tables of Section 1.

Proposition 2.1 (Ritzenthaler-Romagny [RR18]). *Let X be a smooth, non-hyperelliptic genus 3 curve defined by*

$$X : y^4 - h(x, z)y^2 + f(x, z)g(x, z) = 0 \quad (2.1)$$

in \mathbb{P}_k^2 , where

$$f = f_2x^2 + f_1xz + f_0z^2, \quad g = p_2x^2 + g_1xz + g_0z^2, \quad h = h_2x^2 + h_1xz + h_0z^2$$

are homogeneous polynomials of degree 2 over a field k of characteristic different from 2. The involution $(x : y : z) \mapsto (x : -y : z)$ induces a cover π of degree 2 of the genus 1 curve

$$Y : y^2 - h(x, z)y + f(x, z)g(x, z) = 0$$

in the weighted projective space $\mathbb{P}(1, 2, 1)$. Let

$$M = \begin{bmatrix} f_2 & f_1 & f_0 \\ h_2 & h_1 & h_0 \\ p_2 & g_1 & g_0 \end{bmatrix}$$

and assume that M is invertible. Let

$$M^{-1} = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}.$$

Then $\text{Jac}(X) \sim \text{Jac}(Y) \times \text{Jac}(C)$ with $C : y^2 = b \cdot (b^2 - ac)$ in $\mathbb{P}(1, 3, 1)$ where

$$a = a_1 + 2a_2x + a_3x^2, \quad b = b_1 + 2b_2x + b_3x^2, \quad c = c_1 + 2c_2x + c_3x^2.$$

In the special case when the automorphism group of X is C_6 , it can be realized as a plane quartic

$$X : x^3z + y^4 + ry^2z^2 + z^4 = 0$$

for some $r \in k$, and we find $\text{Jac}(X) \sim C_1 \times \text{Jac}(C_2)$ with

$$\begin{cases} C_1 : & y^2 = -x^3 + r^2/4 - 1 \\ C_2 : & y^2 = (x^2 - 2x - 2)(x^4 - 4x^3 + (-2r^2 + 8)x - r^2 + 4) \end{cases}$$

In the next subsection we explain a different approach to handle the case of non-hyperelliptic curves with automorphism group C_2 . This will serve as motivation for the generalization discussed in Section 3.

2.1. A Galois approach. Let X be as in the previous section, that is, a non-hyperelliptic genus 3 curve with an involution. The corresponding quotient is a curve Y of genus 1, and the morphism $\pi_{X/Y} = \pi : X \rightarrow Y$ of degree 2 is branched over 4 distinct points Q_1, Q_2, Q_3 and Q_4 . Let us consider a morphism $\pi_{Y/\mathbb{P}^1} : Y \rightarrow \mathbb{P}^1$ which maps Q_1 and Q_2 to the same point $[\beta, 1] \in \mathbb{P}^1$ with $\beta \neq 0$. Choosing an origin on Y , and thereby giving it the structure of an elliptic curve, this morphism can be constructed by taking the quotient of the elliptic curve Y by the involution $P \mapsto Q_1 + Q_2 - P$. Composing with an automorphism of \mathbb{P}^1 if necessary, we can and will assume that $\pi_{Y/\mathbb{P}^1}(Q_3) = [0, 1]$. Additionally, we write $\pi_{Y/\mathbb{P}^1}(Q_4) = [\gamma, 1]$.

Remark 2.2. Consider the special case $\gamma = 0$, that is, the morphism $Y \rightarrow \mathbb{P}^1$ identifies Q_1 with Q_2 , as well as Q_3 with Q_4 . The methods developed later on in Section 3 will enable us to show that this happens if and only if the composite map $X \rightarrow \mathbb{P}^1$ is Galois, with Galois group C_2^2 (see Table 3). In this case $\text{Aut}(X)$ contains a copy of the Klein 4-group C_2^2 , and we see from Table 2 that $\text{Jac}(X)$ decomposes as the product of three elliptic curves, each of which is a quotient of X .

From now on we restrict to the case $\gamma \neq 0$. By [ER08, Lev12] we have the following equations: we may write $Y : y^2 = f(t) = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)$ and

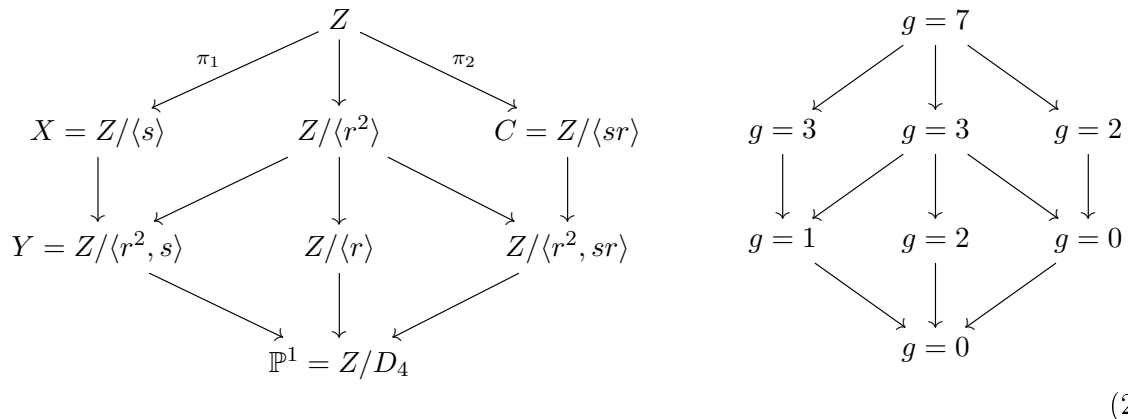
$$X = \begin{cases} y^2 = & f(t) \\ x^2 = & (t - \beta)(p_2(t) + y) \end{cases}$$

where p_2 is a polynomial of degree 2 such that $p_2(t)^2 - f(t) = t(t - \gamma)p_1(t)^2$ with $p_1(t)$ a polynomial of degree 1.

Let $Z \rightarrow \mathbb{P}^1$ be the Galois closure of $X \rightarrow \mathbb{P}^1$. The Galois group of Z/\mathbb{P}^1 is isomorphic to D_4 , the dihedral group on 4 elements. We write $D_4 = \langle r, s \mid r^4 = s^2 = 1, sr = r^3s \rangle$, assuming (as we may) that s is the non-central element of order 2 such that $Z/\langle s \rangle \cong X$. Let \bar{x} be any root of $\bar{x}^2 = (t - \beta)(p_2(t) - y)$. We then see that Z is the smooth projective curve an affine part of which is given by

$$\begin{cases} y^2 = & f(t), \\ x^2 = & (t - \beta)(p_2(t) + y), \\ \bar{x}^2 = & (t - \beta)(p_2(t) - y). \end{cases}$$

Since X corresponds to the quotient of Z by s , we know that s sends (x, \bar{x}, y) to $(x, -\bar{x}, y)$. We can choose r to be $(x, \bar{x}, y) \mapsto (\bar{x}, -x, -y)$. Direct inspection of the subgroup lattice of D_4 implies that the maps $Z \rightarrow X \rightarrow Y \rightarrow \mathbb{P}^1$ fit into a larger diagram of maps of degree 2:



Knowing the action of s and r explicitly allows us to work out equations for the various quotients in the previous diagram and to compute their genera using the Riemann-Hurwitz formula. We will be mainly interested in $C = Z/\langle sr \rangle$. Consider the sr -invariant functions $v = x + \bar{x}$ and $w = \frac{x\bar{x}}{(t - \beta)p_1(t)}$. Note that the invariant function $z := y(x - \bar{x})$ also lies in the function field $k(v, w, t)$, since $vz = y(x^2 - \bar{x}^2) = 2f(t)(t - \beta)$. The relations between v , w and t describe the quotient curve

$$C = \begin{cases} v^2 = & 2(t - \beta)(p_2(t) + wp_1(t)), \\ w^2 = & t(t - \gamma) \end{cases} \quad (2.3)$$

which is indeed a cover of \mathbb{P}^1 of degree 4, as it is a cover of degree 2 of a conic that is in turn a cover of degree 2 of \mathbb{P}^1 .

The second equation in (2.3) describes a conic with a rational point, which may be parametrized as $(t, w) = \left(\frac{\gamma}{1-u^2}, \frac{\gamma u}{1-u^2}\right)$. Replacing this parametrization in the first equation and setting $s := (1 - u^2)^3 v$ we then get the hyperelliptic model

$$s^2 = 2(\gamma - \beta(1 - u^2)) \left((1 - u^2)^2 p_2\left(\frac{\gamma}{1 - u^2}\right) + \gamma u(1 - u^2) p_1\left(\frac{\gamma}{1 - u^2}\right) \right). \quad (2.4)$$

Remark 2.3. The model (2.4) is smooth and defines a curve of genus 2. Indeed, one may check that (under our assumptions $\beta \neq 0, \gamma \neq 0, \beta \neq \gamma$) the irreducible factors of the discriminant of the polynomial on the right hand side are also factors of either $\text{disc}(f)$ or $\text{Res}_t(f(t), (t - \beta)p_2(t))$. This shows that (2.4) is smooth, because $\text{disc}(f) = 0$ (resp. $\text{Res}_t(f(t), (t - \beta)p_2(t)) = 0$) would imply that Y (resp. X) is not smooth.

We now aim to show that the Prym variety of the cover $X \rightarrow Y$ is isogenous to $\text{Jac}(C)$ (Theorem 2.6). In order to do so, we begin by investigating the action of $D_4 \subset \text{Aut}(Z)$ on the space of regular differentials $H^0(Z, \Omega_Z^1)$. We will freely use some results that will be discussed in general in Section 3, see in particular Theorem 3.25. Recall that the character table of D_4 is as follows:

	{id}	{r ² }	{s, sr ² }	{sr, sr ³ }	{r, r ³ }
(1)	1	1	1	1	1
V ₁	1	1	-1	-1	1
V ₂	1	1	1	-1	-1
V ₃	1	1	-1	1	-1
(2)	2	-2	0	0	0

Note in particular that r^2 acts trivially on the 1-dimensional representations V_1, V_2, V_3 and -1 on (2), while the fixed subspace in (2) of each of the symmetries s, sr, sr^2, sr^3 is 1-dimensional.

Lemma 2.4. *We have $H^0(Z, \Omega_Z^1) \cong V_1^{\oplus 2} \oplus V_2 \oplus (2)^{\oplus 2}$ as representations of D_4 .*

Proof. Write $H^0(Z, \Omega_Z^1) \cong (1)^{\oplus e_0} \oplus V_1^{\oplus e_1} \oplus V_2^{\oplus e_2} \oplus V_3^{\oplus e_3} \oplus (2)^{\oplus e_4}$ as representations of D_4 . Let H be any subgroup of G . One has

$$H^0(Z, \Omega_Z)^H \cong H^0(Z/H, \Omega_{Z/H}), \quad (2.5)$$

which implies that the dimension of the subspace of $H^0(Z, \Omega_Z^1)$ fixed by H is the genus of Z/H . Applying this to $H = G$, and observing that $Z/G \cong \mathbb{P}^1$ has genus 0, we obtain that $H^0(Z, \Omega_Z^1)$ does not contain any copy of the trivial representation, i.e., $e_0 = 0$. Applying the same argument with $H = \langle r^2 \rangle$ one obtains $g(Z/H) = 3 = \dim H^0(Z, \Omega_Z^1)^H$, and since r^2 acts trivially on V_1, V_2, V_3 and without fixed points on (2) this implies $3 = e_1 + e_2 + e_3$. We also have the condition $e_1 + e_2 + e_3 + 2e_4 = \dim H^0(Z, \Omega_Z^1) = 7$, so – combining the last two equations – we obtain $e_4 = 2$. Finally, the conditions

$$3 = g(Z/\langle s \rangle) = \dim H^0(Z, \Omega_Z^1)^{\langle s \rangle} = e_2 + e_4 \quad (2.6)$$

and

$$2 = g(Z/\langle sr \rangle) = \dim H^0(Z, \Omega_Z^1)^{\langle sr \rangle} = e_3 + e_4 \quad (2.7)$$

imply $e_2 = 1, e_3 = 0$ and therefore $e_1 = 2$. \square

Lemma 2.5. *The correspondence*

$$\begin{array}{ccc}
 & Z & \\
 \pi_1 \swarrow & & \searrow \pi_2 \\
 X = Z/\langle s \rangle & & C = Z/\langle sr \rangle
 \end{array}
 \quad
 \begin{array}{ccc}
 & g = 7 & \\
 \swarrow & & \searrow \\
 g = 3 & & g = 2
 \end{array}
 \quad (2.8)$$

induces a homomorphism of abelian varieties $\text{Jac}(Z/\langle sr \rangle) \rightarrow \text{Jac}(X)$ with finite kernel. In particular, $\text{Jac}(Z/\langle sr \rangle)$ is a factor of $\text{Jac}(X)$ in the category of abelian varieties up to isogeny.

Proof. We consider the action of this correspondence on regular differentials and determine the image of

$$\pi_{1*}\pi_2^* : H^0(C, \Omega_C^1) \rightarrow H^0(X, \Omega_X^1). \quad (2.9)$$

The image of π_2^* is the sr -invariant subspace of $H^0(Z, \Omega_Z^1)$; given our description of $H^0(Z, \Omega_Z^1)$ as a D_4 -representation, we see that this is precisely the sr -invariant subspace in $(2)^{\oplus 2}$. Identifying $H^0(X, \Omega_X^1)$ with $H^0(Z, \Omega_Z^1)^{\langle s \rangle}$, the map

$$\pi_{1*} : H^0(Z, \Omega_Z^1) \rightarrow H^0(X, \Omega_X^1) \cong H^0(Z, \Omega_Z^1)^{\langle s \rangle} \quad (2.10)$$

is given by $\omega \mapsto \omega + s^*\omega$. Since the structure of the 2-dimensional representation (2) shows that the map $(1 + s)$ is injective on its sr -invariant subspace, we obtain that π_{1*} is injective on the

image of π_2^* . This implies that the image of $\pi_{1*}\pi_2^*$ is 2-dimensional, which in turn means that the image of $\text{Jac}(Z/\langle sr \rangle) \rightarrow \text{Jac}(X)$ is 2-dimensional as claimed. \square

Theorem 2.6. *The Jacobian of X decomposes up to isogeny as*

$$\text{Jac}(X) \sim Y \times \text{Jac}(Z/\langle sr \rangle). \quad (2.11)$$

As a consequence, $\text{Jac}(Z/\langle sr \rangle)$ is isogenous to the Prym variety of $\pi : X \rightarrow Y$, and a nontrivial map $\text{Jac}(Z/\langle sr \rangle) \rightarrow \text{Jac}(X)$ is induced by the correspondence Z in (3.2).

Proof. In the light of Lemma 2.5 it suffices to prove that the subspaces $\pi_{X/Y}^*H^0(Y, \Omega_Y^1)$ and $\pi_{1*}\pi_2^*H^0(C, \Omega_C^1)$ of $H^0(X, \Omega_X^1)$ generate this vector space, or equivalently (by dimension considerations) that they intersect trivially. Since $\pi_1^* : H^0(X, \Omega_X^1) \rightarrow H^0(Z, \Omega_Z^1)$ is injective, it suffices to prove that they intersect trivially after pullback to $H^0(Z, \Omega_Z^1)$. One can describe the subspaces $\pi_1^*\pi_{X/Y}^*H^0(Y, \Omega_Y^1)$ and $\pi_1^*\pi_{1*}\pi_2^*H^0(C, \Omega_C^1)$ in terms of the action of D_4 : according to Diagram (2.2) and Lemma 2.4, $\pi_1^*\pi_{X/Y}^*H^0(Y, \Omega_Y^1) = H^0(Z, \Omega_Z^1)^{\langle r^2, s \rangle} = V_2$, while

$$\pi_1^*\pi_{1*}\pi_2^*H^0(C, \Omega_C^1) = (1+s)H^0(Z, \Omega_Z^1)^{\langle sr \rangle}.$$

It now suffices to note that sr has no nonzero fixed points in $V_1^{\oplus 2} \oplus V_2$, so $H^0(Z, \Omega_Z^1)^{\langle sr \rangle}$ is contained in $(2)^{\oplus 2}$. Since $(2)^{\oplus 2}$ is a subrepresentation of $H^0(Z, \Omega_Z^1)$ it follows that also $(1+s)H^0(Z, \Omega_Z^1)^{\langle sr \rangle}$ is contained in $(2)^{\oplus 2}$, hence it does not intersect $H^0(Z, \Omega_Z^1)^{\langle r^2, s \rangle}$ as claimed. We conclude as desired that $\pi_1^*\pi_{X/Y}^*H^0(Y, \Omega_Y^1)$ and $\pi_2^*(C, \Omega_C^1)$ together generate $H^0(Z, \Omega_Z^1)^{\langle s \rangle} = H^0(X, \Omega_X^1)$. \square

Theorem 2.6 recovers Proposition 2.1 and also clarifies the nature of a correspondence between C and X . In addition, notice that the curve C described in Proposition 2.1 depends on the choice of a factorization $f(x, z)g(x, z)$ of a certain polynomial of degree 4 as the product of two quadratics. Note that the zero locus of $f(x, z)g(x, z)$ on Y describes precisely the branch locus of $X \rightarrow Y$. In our new approach, the choice of factorization can be reinterpreted as the choice of the two points Q_1, Q_2 that are contracted by the morphism π_{Y/\mathbb{P}^1} .

Remark 2.7. In [RR18], the aforementioned choice of a partition of 4 points into 2 pairs is clearly symmetric in the pairs. By contrast, in this new approach the choice is highly asymmetric since 2 points are contracted and the other 2 are not.

3. AN ALGORITHMIC APPROACH VIA GROUP THEORY

Our purpose in this section is to generalize the previous discussion to more complicated cases, for which explicit equations are not available. The proof of Lemma 2.4 relied strongly on the fact that we could compute the genus of any quotient of Z by direct inspection of the equations of the curves and of the action of automorphisms. In general it is more difficult to get such information explicitly, so in this section we explain how we may reverse the process: we first describe the action of $\text{Aut}(Z \rightarrow \mathbb{P}^1)$ on $H^0(Z, \Omega_Z^1)$ (Paragraph 3.4.3), and subsequently rely on this information to completely describe the morphisms between Jacobians of curves obtained as quotients of Z (Paragraph 3.4.4). The method has its roots in the theory of monodromy actions for branched covers of curves. While developing the main notions of this theory below, we show how it can be combined with the description of the aforementioned action, and also give some explicit references for useful statements in this context, in particular Theorem 3.10.

3.1. Preliminaries on ramification and monodromy. In this section we fix our notation and conventions for describing the ramification of a morphism between smooth projective curves over \mathbb{C} . We will freely use without further mention the fact that the category of such curves is equivalent to the category of Riemann surfaces, and assume that all our curves are connected. We will find it useful to introduce the following definition:

Definition 3.1. Let $\varphi : X \rightarrow Y$ be a morphism of smooth projective curves over \mathbb{C} and let $B = (b_1, \dots, b_n)$ be a fixed ordered subset of Y which contains the branch locus of φ . For $b \in Y$, let $\varphi^{-1}(b) = \{a_1, \dots, a_k\}$ be the fiber of φ above b and suppose that this set contains m_i points of ramification index e_i , with the e_i distinct and with i running from 1 to r , say. Then the *ramification structure of φ at b* is the set $R_b := \{(e_1, m_1), \dots, (e_r, m_r)\}$. The *ramification structure of φ* is the ordered vector $R := (R_{b_i} : i = 1, \dots, n)$.

Remark 3.2. The ramification structure R depends on B and on the ordering of the points in B — even though this is not emphasized by our notation, the choice of b_1, \dots, b_n should always be clear from the context. Note furthermore that the definition above allows one to include the ramification structure at b for points in the complement of the branch locus. In this case, the ramification structure at b is $R_b = \{(1, \deg \varphi)\}$: all $\deg \varphi$ points in the fiber over b have ramification index 1.

Remark 3.3. We will connect ramification structures with the cycle type of certain permutations. We therefore agree to also write cycle types in the previous way: if the permutation σ contains m_i cycles of length e_i , with the e_i distinct and with i running from 1 to r , say, then we write its cycle type as $\{(e_1, m_1), \dots, (e_r, m_r)\}$.

Example 3.4. Let X be a smooth projective curve of genus 3, Y be an elliptic curve, and $\varphi : X \rightarrow Y$ be a morphism of degree 2. The Riemann-Hurwitz formula immediately implies that φ is ramified at exactly 4 points, each with ramification index 2. If we take B to be the branch locus of φ (consisting of 4 points, ordered arbitrarily), then the ramification structure of φ is $(\{(2, 1)\}, \{(2, 1)\}, \{(2, 1)\}, \{(2, 1)\})$.

We now recall some basic facts about monodromy. Consider a morphism $\varphi : X \rightarrow Y$ between smooth projective curves over \mathbb{C} . Let $B = (b_1, \dots, b_n)$ be a finite ordered subset of Y which contains the branch locus of φ , and fix a base point $q \in Y - B$. Also fix loops $\gamma_1, \dots, \gamma_n$, based at q , with the property that γ_i is nontrivial in $\pi_1(Y - B, q)$ but trivial in $\pi_1(Y - (B - \{b_i\}), q)$, and that winds precisely once in the counter-clockwise direction around b_i . We will call such a loop a *small loop* based at q around b_i . The classes $[\gamma_1], \dots, [\gamma_n]$ then generate the fundamental group of $Y - B$. One can classify all maps φ with branch locus contained in B and of fixed degree in terms of representations of the fundamental group $\pi_1(Y - B, q)$. More precisely, we have

Theorem 3.5 ([Mir95, Proposition 4.9]). *Let Y be a compact Riemann surface, B be a finite subset of Y , and let q be a base point of $Y - B$. There is a bijection*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{holomorphic maps } \varphi : X \rightarrow Y \\ \text{of degree } d \\ \text{whose branch points} \\ \text{lie in } B \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{group homomorphisms} \\ \rho : \pi_1(Y - B, q) \rightarrow S_d \\ \text{with transitive image} \\ \text{up to conjugacy in } S_d \end{array} \right\}$$

denoted by $\varphi_\rho \leftrightarrow \rho$ and $\varphi \leftrightarrow \rho_\varphi$. If γ_i is a small loop based at q around $b_i \in B$, the ramification structure of φ_ρ at b_i is the cycle type of $\sigma_i := \rho([\gamma_i])$.

As an immediate consequence of the previous theorem we have:

Corollary 3.6. *With the same notation as in the theorem, the ramification structure of $\varphi_\rho : X \rightarrow Y$ is determined by the conjugacy classes in S_d of $\rho([\gamma_i])$ for $i = 1, \dots, n$.*

Definition 3.7. In the situation of the previous theorem, we will call the vector $\Sigma = (\sigma_1, \dots, \sigma_n) = (\rho([\gamma_1]), \dots, \rho([\gamma_n]))$ the *monodromy datum* associated with φ .

Remark 3.8. While the monodromy datum Σ alone does not uniquely identify a map $\varphi : X \rightarrow Y$ (even up to isomorphism), because one also needs to specify the ordered set of points (b_1, \dots, b_n) , any choice of such an ordered set will lead to a map φ with the same ramification structure. Recall from [MSSV02, §3] that the dimension of the moduli space of covers of \mathbb{P}^1 branched over n points has dimension $n - 3$, so by letting the branch locus vary we get $(n - 3)$ -dimensional families of curves with fixed monodromy.

We now specialize this discussion to the case $Y = \mathbb{P}^1$. The fundamental group of $\mathbb{P}^1 - B$ is generated by $[\gamma_1], \dots, [\gamma_n]$, subject to the only relation $\prod_{i=1}^n [\gamma_i] = 1$. Thus, given $\sigma_1, \dots, \sigma_n \in S_d$ that satisfy $\prod_{i=1}^n \sigma_i = 1$, we can define a homomorphism

$$\rho : \pi_1(\mathbb{P}^1 - B, q) \rightarrow S_d$$

by sending $[\gamma_i]$ to σ_i , and every homomorphism arises in this way for some $(\sigma_1, \dots, \sigma_n)$. Thus we obtain the following special important case of Theorem 3.5:

Theorem 3.9 ([Mir95, Corollary 4.10]). *There is a bijective correspondence*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{holomorphic maps } \varphi : C \rightarrow \mathbb{P}^1 \\ \text{of degree } d \\ \text{whose branch points} \\ \text{lie in } B \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{conjugacy classes of } n\text{-tuples} \\ (\sigma_1, \dots, \sigma_n) \text{ of permutations in } S_d \\ \text{such that } \sigma_1 \cdots \sigma_n = 1 \\ \text{and the subgroup generated by the } \sigma_i \\ \text{is transitive} \end{array} \right\}$$

which enjoys the following additional property: the ramification structure at b_i of the map φ corresponding to $(\sigma_1, \dots, \sigma_n)$ is the cycle type of σ_i .

3.2. Galois closure of a morphism of curves. Given a non-constant morphism $\varphi : X \rightarrow Y$ of smooth projective curves over \mathbb{C} , it makes sense to consider the corresponding (finite, separable) field extension $\varphi^*\mathbb{C}(Y) \subseteq \mathbb{C}(X)$. As with any such extension, we can then consider the Galois closure of $\mathbb{C}(X)$ over $\varphi^*\mathbb{C}(Y)$, which by the equivalence between smooth projective curves over \mathbb{C} and extensions of \mathbb{C} of transcendence degree 1 corresponds to some curve \tilde{C} equipped with a canonical morphism $\tilde{C} \rightarrow X$. We call \tilde{C} (equipped with its maps $\tilde{C} \rightarrow X \rightarrow Y$) the Galois closure of $X \rightarrow Y$, and we say that \tilde{C}/Y has Galois group G if this is true for the corresponding extension of function fields. There is a natural action of G on \tilde{C} , and for a subgroup H of G we write \tilde{C}/H for the curve corresponding to the subfield of $\mathbb{C}(\tilde{C})$ fixed by H .

We now recall a description of the Galois closure in terms of the monodromy datum. Suppose the map $\varphi : X \rightarrow Y$ corresponds, as in Theorem 3.5, to $B = (b_1, \dots, b_n)$ and to the representation ρ . As in the statement of the theorem, let γ_i be a small loop based at q around b_i . Finally, let $\sigma_i = \rho([\gamma_i])$. Then we have the following description of the Galois closure of φ :

Theorem 3.10. *Let $\tilde{\varphi} : \tilde{C} \rightarrow X \rightarrow Y$ be the Galois closure of $\varphi : X \rightarrow Y$. Then:*

- (i) *the Galois group of \tilde{C}/Y is the subgroup G of S_d generated by the σ_i , and the degree of $\tilde{\varphi}$ is $|G|$;*
- (ii) *the branch locus of $\tilde{\varphi}$ is contained in B ;*
- (iii) *the corresponding representation $\rho_{\tilde{\varphi}}$ is obtained as follows: identifying $S_{|G|}$ with the group of permutations of the elements of G , the class $[\gamma_i]$ is sent to the permutation of G induced by left-multiplication by σ_i .*

This is all explained in [Ber13], which, however, does not contain a separate statement that comprises all three items above. We therefore include a short proof with more detailed references:

Proof. Part (i) is in [Ber13, §4.3.1]. Part (ii) follows from the equivalence between curves and function fields: a point $b \in Y$ is a branch point for $\varphi : X \rightarrow Y$ precisely when the corresponding place of $\mathbb{C}(Y)$ ramifies in $\mathbb{C}(X)$. Moreover, because a compositum of unramified extensions of local fields is unramified [Neu99, II.7.3], the branched places of the extension $\mathbb{C}(X)/\varphi^*\mathbb{C}(Y)$ coincide with those of its Galois closure. Finally, (iii) is part of the theory of G -sets [Mas91, Chapter V], [Len08, Chapter 1]. More generally, if H is any subgroup of G , then the fiber of $\tilde{C}/H \rightarrow \tilde{C}/G = Y$ is identified with G/H , and the monodromy action is the natural multiplication action of G on G/H . Applying this to $H = \{1\}$ yields the result. \square

Remark 3.11. If $\varphi : X \rightarrow Y$ corresponds to the monodromy datum $\Sigma = (\sigma_1, \dots, \sigma_n)$, we will denote by $\tilde{\sigma}_i$ the permutation $\rho_{\tilde{\varphi}}([\gamma_i])$ and by $\tilde{\Sigma}$ the vector $(\tilde{\sigma}_1, \dots, \tilde{\sigma}_n)$.

3.3. Statement of the problem. We begin by describing the objects of interest:

Definition 3.12. Consider a 5-tuple (g_X, g_Y, d_X, d_Y, R) , where g_X, g_Y are non-negative integers, d_X, d_Y are positive integers, and $R = (R_1, \dots, R_n)$ is a ramification structure, that is, a collection of pairs $R_i = (e_i, m_i)$ of positive integers. A *diagram of type (g_X, g_Y, d_X, d_Y, R)* is a diagram of maps of smooth projective curves

$$Z \longrightarrow X \xrightarrow{\pi_{X/Y}} Y \xrightarrow{\pi_{Y/\mathbb{P}^1}} \mathbb{P}^1 \quad (3.1)$$

that satisfies the following properties:

- (i) the genera of X and Y are g_X, g_Y respectively;
- (ii) $\pi_{X/Y}$ is of degree d_X and π_{Y/\mathbb{P}^1} is of degree d_Y ;
- (iii) the branch locus of $X \rightarrow \mathbb{P}^1$ is contained in an ordered set $B = (b_1, \dots, b_n)$ with n elements;
- (iv) the ramification structure of $X \rightarrow \mathbb{P}^1$, computed with respect to B , is equal to R ;
- (v) $Z \rightarrow \mathbb{P}^1$ is the Galois closure of $X \rightarrow \mathbb{P}^1$.

Remark 3.13. Note that the number of branching points of $X \rightarrow \mathbb{P}^1$ is precisely n if and only if none of the R_i is equal to $\{(1, d_X d_Y)\}$. Indeed, this ramification structure denotes a point whose fiber contains $d_X d_Y$ points, none of which is ramified.

The map $X \rightarrow \mathbb{P}^1$ corresponds to a monodromy datum Σ as in Theorem 3.9. Let G be the Galois group of Z/\mathbb{P}^1 , and let $\tilde{\Sigma}$ be the corresponding monodromy datum. On the function fields side we have corresponding inclusions $\mathbb{C}(\mathbb{P}^1) \subseteq \mathbb{C}(Y) \subseteq \mathbb{C}(X) \subseteq \mathbb{C}(Z)$, and by Galois correspondence we obtain subgroups H_X, H_Y of G with the property that $Z/H_X = X$ and

$Z/H_Y = Y$. In what follows we will be interested in 4-tuples (G, H_X, H_Y, Σ) that arise from this construction.

Remark 3.14. Let $d = d_X d_Y$. The construction of $Z \rightarrow \mathbb{P}^1$ as the Galois closure of $X \rightarrow \mathbb{P}^1$ amounts to fixing a distinguished embedding of the Galois group G into S_d , for which H_X is conjugate to the stabilizer of 1. This leads to a corresponding notion of isomorphism, which is that of simultaneous conjugation of the 4-tuple (G, H_X, H_Y, Σ) in S_d . That is, if g is any element of S_d , and $\Sigma = (\sigma_1, \dots, \sigma_n)$, then we write $g\Sigma g^{-1}$ for the vector $(g\sigma_i g^{-1})_{i=1, \dots, n}$ and say that the 4-tuples (G, H_X, H_Y, Σ) and $(gGg^{-1}, gH_Xg^{-1}, gH_Yg^{-1}, g\Sigma g^{-1})$ are isomorphic.

The problem we will solve is the following. Fix a 5-tuple (g_X, g_Y, d_X, d_Y, R) as in Definition 3.12 and let $X \rightarrow Y \rightarrow \mathbb{P}^1$ be a diagram of type (g_X, g_Y, d_X, d_Y, R) . Let (G, H_X, H_Y, Σ) be the corresponding 4-tuple constructed above. Up to isomorphism there are only finitely many possibilities for (G, H_X, H_Y, Σ) , and our first algorithmic task is the following:

Problem 3.15. Given (g_X, g_Y, d_X, d_Y, R) as in Definition 3.12, output a list $\mathcal{L}(g_X, g_Y, d_X, d_Y, R)$ of all isomorphism classes of 4-tuples (G, H_X, H_Y, Σ) that can be obtained from a diagram $X \rightarrow Y \rightarrow \mathbb{P}^1$ of type (g_X, g_Y, d_X, d_Y, R) .

Note that a list $\mathcal{L}(g_X, g_Y, d_X, d_Y, R)$ as in the statement of Problem 3.15 gives a complete set of representatives of isomorphism classes of diagrams of type (g_X, g_Y, d_X, d_Y, R) , in the following precise sense. Suppose we have a diagram of type (g_X, g_Y, d_X, d_Y, R) : then one of the 4-tuples (G, H_X, H_Y, Σ) in $\mathcal{L}(g_X, g_Y, d_X, d_Y, R)$ enjoys the following properties. Consider the unique (up to isomorphism) cover X' of \mathbb{P}^1 of degree $d_X d_Y$, branched at most over B , and corresponding to the monodromy datum Σ . Also let Z' be the Galois closure of $X' \rightarrow \mathbb{P}^1$. The following holds:

- (i) we have $\text{Aut}(Z/\mathbb{P}^1) \cong \text{Aut}(Z'/\mathbb{P}^1) \cong G$;
- (ii) there is a canonical identification $X' = Z'/H_X$;
- (iii) the map $Z' \rightarrow \mathbb{P}^1$ is isomorphic to $Z \rightarrow \mathbb{P}^1$ as a G -cover;
- (iv) the G -isomorphism $Z' \cong Z$ can be chosen in such a way that Z'/H_X is carried to X and Z'/H_Y is carried to Y ;
- (v) in particular, the monodromy datum attached to $X \rightarrow \mathbb{P}^1$ is equivalent to Σ (up to conjugacy in the symmetric group).

Remark 3.16. Informally, this means that a diagram of type (g_X, g_Y, d_X, d_Y, R) arises from one of the monodromy data Σ found in $\mathcal{L}(g_X, g_Y, d_X, d_Y, R)$, the only information missing being the ordered set of branch points.

In addition, for each (G, H_X, H_Y, Σ) we would like to extract some additional information:

Problem 3.17. Given (G, H_X, H_Y, Σ) , determine:

- (i) for every pair of subgroups $H_1 < H_2 < G$, the degree and ramification structure of the corresponding map $Z/H_1 \rightarrow Z/H_2$;
- (ii) for every subgroup H of G , the genus of the curve Z/H ;
- (iii) the action of G on the vector space $H^0(Z, \Omega_Z^1)$ induced by the natural action of G on Z ;

- (iv) for every pair of subgroups H_1, H_2 of G , the dimension of the image of the map on Jacobians $\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2)$ induced by the correspondence

$$\begin{array}{ccc}
 & Z & \\
 \pi_1 \swarrow & & \searrow \pi_2 \\
 Z/H_1 & & Z/H_2
 \end{array} \tag{3.2}$$

3.4. Theory. We now review the theoretical tools necessary to solve Problem 3.17. Our input data is a 4-tuple (G, H_X, H_Y, Σ) , corresponding to a diagram of type (g_X, g_Y, d_X, d_Y, R) .

3.4.1. *Degree and ramification structure of $Z/H_1 \rightarrow Z/H_2$.* Galois theory immediately shows that the degree of the natural projection $Z/H_1 \rightarrow Z/H_2$ is equal to $[H_2 : H_1]$.

As for the ramification structure, we begin with the special case $H_2 = G$ and H_1 arbitrary. The quotient Z/H_2 is therefore equal to \mathbb{P}^1 , the curve Z/H_1 is a branched cover of it, and we may rely on Theorem 3.9 to describe its ramification. In fact, the theorem shows that it suffices to understand the monodromy representation corresponding to $\pi : Z/H_1 \rightarrow \mathbb{P}^1$. Let B be the set (containing the branch locus) that defines the cover $Z \rightarrow \mathbb{P}^1$ and let B_Z (resp. B_{Z/H_1}) be the inverse images of B in Z (resp. Z/H_1). Let $Z^0 := Z - B_Z$ and observe that Z^0/H_1 coincides with $Z/H_1 - B_{Z/H_1}$. We have a diagram of étale maps

$$Z^0 \rightarrow Z^0/H_1 \rightarrow \mathbb{P}^1 - B$$

which we may study via the usual topological interpretation of coverings as π_1 -sets. In particular, fixing a base point $q \in \mathbb{P}^1 - B$, one may identify the fiber of Z^0 over q with G and the fiber of $(Z/H_1)^0$ with G/H_1 . In this language, the monodromy datum Σ gives rise to a representation

$$\rho : \pi_1(\mathbb{P}^1 - B, q) \rightarrow G :$$

the π_1 -structure of G is then $\gamma \cdot g := \rho(\gamma)g$ for $\gamma \in \pi_1(\mathbb{P}^1 - B, q)$. The π_1 -set corresponding to Z^0/H_1 is then the set G/H_1 , equipped with the action $\gamma \cdot gH_1 := \rho(\gamma)gH_1$. We can now translate back to the language of monodromy datum: for each $i = 1, \dots, n$ we have a permutation of the set G/H_1 , defined by left-multiplication by the element σ_i . We may then use Theorem 3.9 to describe the ramification structure of $Z/H_1 \rightarrow \mathbb{P}^1$, and we obtain:

Proposition 3.18. *Let H_1 be a subgroup of G . The branched cover $Z/H_1 \rightarrow \mathbb{P}^1$ is ramified at most over the points in $B = (b_1, \dots, b_n)$. The ramification over b_i can be determined as follows: consider the left multiplication of σ_i on the quotient set G/H_1 . This induces a permutation of G/H_1 , with cycle type $((e_1, m_1), \dots, (e_k, m_k))$. Then for all $1 \leq j \leq k$, the fiber over b_i contains exactly m_j points with multiplicity e_j , and no other points beyond these.*

Remark 3.19. The last statement in the previous proposition shows that the fiber of $Z/H_1 \rightarrow \mathbb{P}^1$ over a point $b_i \in B$ is in natural bijection with the double coset space $\langle \sigma_i \rangle \backslash G/H_1$.

We will also need the following straightforward generalization of Proposition 3.18, which follows upon replacing Theorem 3.9 with Theorem 3.5:

Proposition 3.20. *Let Z be a smooth projective curve over \mathbb{C} with an action of a group G , and let H be a subgroup of G . Let $B = (b_1, \dots, b_n) \subseteq Z/H$ be a finite ordered subset containing the branch locus of $\pi_H : Z \rightarrow Z/H$ and let ρ be the corresponding representation $\pi_1(Z/G - B, q) \rightarrow S_d$ as in Theorem 3.5. Finally, let γ_i be small loops based at q around each b_i and let $\sigma_i = \rho([\gamma_i])$.*

Recall from Theorem 3.10 that G is identified with the subgroup of S_d generated by the σ_i . The ramification of π_H over b_i can be determined as follows. Consider the left multiplication by σ_i on the quotient set G/H : it induces a permutation of the set G/H , with cycle type (e_1, \dots, e_k) . The fiber over b_i consists of k points, of multiplicities e_1, \dots, e_k .

Second, we treat the case of a Galois cover $\pi_H : Z \rightarrow Z/H$. This is discussed for example in [BR11, Proposition 2.2.2] and in [MSSV02, §4], so we only recall the result. Let as before Z^0 be the complement in Z of the inverse image of B , and observe that we have a tower of topological covers

$$Z^0 \xrightarrow{\pi_H} Z^0/H \xrightarrow{\varphi} \mathbb{P}^1 - B :$$

in particular, π_H is unramified outside of the inverse image of B in Z/H . Thus the branch locus of π_H is contained in $\varphi^{-1}(B)$, and we have a description of this set by the special case we treated above: by Remark 3.19, the set $\varphi^{-1}(B)$ can be parametrized by pairs $(b_i, \langle \sigma_i \rangle gH)$, where the second coordinate is an element in the double coset space $\langle \sigma_i \rangle \backslash G/H$. The monodromy operator given by a small loop around the point corresponding to $\langle \sigma_i \rangle gH$ is obtained as follows: letting $m_{g,i}$ be the smallest positive integer for which $g^{-1} \sigma_i^{m_{g,i}} g \in H$, the monodromy operator is precisely $g^{-1} \sigma_i^{m_{g,i}} g$.

The case of a general intermediate cover $\pi : Z/H_1 \rightarrow Z/H_2$ follows upon combining the previous two special cases: we first obtain the monodromy datum of $Z \rightarrow Z/H_2$ in the way just described, and then deduce that of $Z/H_1 \rightarrow Z/H_2$ by applying Proposition 3.20. This leads to the following algorithmic procedure to express the monodromy of $Z/H_1 \rightarrow Z/H_2$ in terms of (G, H_1, H_2, Σ) :

Algorithm 3.21. *Input:* (G, H_1, H_2, Σ) with $H_1 < H_2$ and $\Sigma = (\sigma_1, \dots, \sigma_n)$.

Output: the ramification structure of $Z/H_1 \rightarrow Z/H_2$.

Procedure:

- (i) for every $i = 1, \dots, n$:
 - (a) compute representatives $\langle \sigma_i \rangle g_{ij} H_2$ for the double coset space $\langle \sigma_i \rangle \backslash G/H_2$.
 - (b) for each g_{ij} :
 - (i) let m_{ij} be the least positive integer for which $g_{ij}^{-1} \sigma_i^{m_{ij}} g_{ij}$ lies in H_2 . Set $\sigma_{ij} = g_{ij}^{-1} \sigma_i^{m_{ij}} g_{ij}$.
 - (ii) compute the permutation of G/H_1 induced by left multiplication by σ_{ij} . Let R_{ij} be the cycle type of this permutation.
- (ii) The ramification structure of $Z/H_1 \rightarrow Z/H_2$ is the vector $(R_{ij} \mid i = 1, \dots, n, \langle \sigma_i \rangle g_{ij} H_2 \in \langle \sigma_i \rangle \backslash G/H_2)$.

3.4.2. *The genera of the curves Z/H .* By the previous paragraph we know how to read off our data the ramification structure of the map $\varphi : Z/H \rightarrow Z/G = \mathbb{P}^1$. In particular, we know the multiplicity of each ramification point $y_i \in Z/H$, and since we also know $\deg \varphi = [G : H]$ we can simply apply the Riemann-Hurwitz formula to obtain

$$g(Z/H) = \frac{1}{2} \left(2 - 2[G : H] + \sum_{y \in Z/H} (e(y) - 1) \right). \quad (3.3)$$

3.4.3. *G -module structure of $H^0(Z, \Omega_Z^1)$.* To extract this information from (G, H_X, H_Y, Σ) we use a beautiful theorem due to Chevalley and Weil [CWH34, Wei35] that we now recall.

We need some preliminary notation. Let $B = (b_1, \dots, b_n)$ be the ordered branch locus of $Z \rightarrow \mathbb{P}^1$ and consider one of the branch points $b_i \in B$. As part of our data we have access to a permutation $\sigma_i \in G$ corresponding to the branch point b_i . Let e_i be the order of the permutation σ_i , or equivalently (by Theorem 3.10) the ramification index of any point of Z lying over b_i . Fix once and for all a primitive $|G|$ -th root of unity $\zeta \in \mathbb{C}$, and, for any divisor e of $|G|$, denote by ζ_e the complex number $\zeta^{|G|/e}$.

Observe that $V := H^0(Z, \Omega_Z^1)$ is a $\mathbb{C}[G]$ -module in a natural way, and it is automatically semisimple since \mathbb{C} is of characteristic 0. In order to describe the $\mathbb{C}[G]$ -module structure of V , therefore, it suffices to give the multiplicity of each irreducible representation of G in V . For a fixed linear representation τ of G , denote by $N_{i,\alpha} = N_{i,\alpha}(\tau)$ the multiplicity of $\zeta_{e_i}^\alpha$ as eigenvalue of $\tau(\tilde{\sigma}_i)$, where $\tilde{\sigma}_i$ is the monodromy operator corresponding to the cover $Z \rightarrow \mathbb{P}^1$ and the point b_i . With this notation, and in the special case of covers of \mathbb{P}^1 , the Chevalley-Weil formula reads as follows:

Theorem 3.22 (Chevalley-Weil). *Let $\varphi : Z \rightarrow \mathbb{P}^1$ be a branched Galois cover of smooth projective complex algebraic curves, let B be its branch locus, and let G be the corresponding Galois group. Let τ_χ be an irreducible linear complex representation of G with character $\chi : G \rightarrow \mathbb{C}$ and define e_i and $N_{i,\alpha} := N_{i,\alpha}(\tau_\chi)$ as above. The multiplicity ν_χ of τ_χ in the G -representation $H^0(Z, \Omega_Z^1)$ is given by*

$$\nu_\chi = -d_\chi + \sum_{i=1}^p \sum_{\alpha=0}^{e_i-1} N_{i,\alpha} \left\langle -\frac{\alpha}{e_i} \right\rangle + \sigma, \quad (3.4)$$

where $d_\chi = \chi(1)$ is the dimension of τ_χ and

$$\sigma = \begin{cases} 1 & \text{if } \chi \text{ is the trivial character} \\ 0 & \text{otherwise.} \end{cases}$$

Finally, $\langle x \rangle = x - [x] \in [0, 1)$ denotes the fractional part of the real number x .

Note that the multiplicity ν_χ is determined by (G, H_X, H_Y, Σ) and χ : we have already observed that e_i is the order of σ_i , and explained how to obtain the monodromy datum $\tilde{\Sigma}$ (see Theorem 3.10). Finally, the number $N_{i,\alpha}$ is the multiplicity of $\zeta_{e_i}^\alpha$ (which is a known complex number) as an eigenvalue of $\tau_\chi(\tilde{\sigma}_i)$, and a basic result in representation theory shows that τ_χ is in turn determined by χ , so that ν_χ is indeed determined by (G, H_X, H_Y, Σ) . The upshot of this discussion is that we have an isomorphism of $\mathbb{C}[G]$ -modules $V \cong \bigoplus_\chi \tau_\chi^{\oplus \nu_\chi}$, where all the objects on the right hand side are determined by (G, H_X, H_Y, Σ) as desired.

3.4.4. The maps $\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2)$. Our last objective is to understand the image of the maps $\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2)$ induced by the correspondence (3.2). Note that the complex vector space $V = H^0(Z, \Omega_Z^1)$ provides the natural analytic uniformization of $\text{Jac}(Z)$, and that the maps $\text{Jac}(Z/H_i) \rightarrow \text{Jac}(Z)$ are induced by the pullback $\pi_i^* : H^0(Z/H_i, \Omega_{Z/H_i}^1) \rightarrow H^0(Z, \Omega_Z^1)$. Thus it suffices to study the map $\pi_{2*} \circ \pi_1^* : H^0(Z/H_1, \Omega_{Z/H_1}^1) \rightarrow H^0(Z/H_2, \Omega_{Z/H_2}^1)$. Note that the pushforward π_{2*} makes sense since $Z \rightarrow Z/H_2$ is a finite (albeit ramified) cover. We will need a result from representation theory:

Theorem 3.23 ([Ser78, Théorème 2.6.8]). *Let $\tau : G \rightarrow \text{GL}(V)$ be a finite-dimensional linear complex representation of the finite group G and let H be a subgroup of G . Define $p_H :=$*

$\frac{1}{\#H} \sum_{h \in H} \tau(h) \in \text{End}(V)$. Then p_H is a projector, that is, $p_H^2 = p_H$, and its image is precisely the H -invariant subspace of V .

Remark 3.24. We will only work with the representation of G afforded by $V = H^0(Z, \Omega_Z^1)$, so, for the sake of simplicity, given a subgroup H of G we will simply write $p_H = \frac{1}{\#H} \sum_{h \in H} h$, omitting the representation τ .

In order to connect the maps π_{i*} and π_i^* with representation theory we will make use of the following result:

Theorem 3.25. *Let H be a subgroup of G and let $\pi : Z \rightarrow Z/H$ be the corresponding quotient map. Then:*

- (i) $\pi^* : H^0(Z/H, \Omega_{Z/H}^1) \rightarrow H^0(Z, \Omega_Z^1)$ is injective, and its image is the H -invariant subspace of $H^0(Z, \Omega_Z^1)$;
- (ii) $\pi^* \pi_* : H^0(Z, \Omega_Z^1) \rightarrow H^0(Z, \Omega_Z^1)$ coincides with the operator $\#H \cdot p_H$.

Part (i) is well-known; we include a short proof of (ii):

Proof of (ii). Since a curve and its Jacobian share the same space of regular differentials, it suffices to prove the same statement with $Z, Z/H$ replaced by their Jacobians. We prove the stronger statement that the required relation is true for the divisor groups. Let $D = \sum_i n_i P_i$ be a divisor on Z . By definition, $\pi_* D = \sum_i n_i \pi(P_i)$. Since the fiber over $\pi(P_i)$ is the divisor given by the sum of all the points that map to $\pi(P_i)$, namely, $\sum_{h \in H} h \cdot P_i$, we obtain $\pi^* \pi_* D = \sum_i n_i \sum_{h \in H} h \cdot P_i = \#H \cdot p_H(D)$ as desired. \square

We wish to determine the dimension of $\text{Im}(\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2))$, or equivalently the dimension of $\pi_{2*} \circ \pi_1^*(H^0(Z/H_1, \Omega_{Z/H_1}^1))$. Since π_2^* is injective, we may as well study the dimension of $\pi_2^* \circ \pi_{2*} \circ \pi_1^*(H^0(Z/H_1, \Omega_{Z/H_1}^1))$. By Theorem 3.25, $\pi_1^*(H^0(Z/H_1, \Omega_{Z/H_1}^1))$ is precisely the H_1 -invariant subspace of V , hence (by Theorem 3.23) it is the image of p_{H_1} . We may easily identify this subspace, because we have already shown how to write down a representation isomorphic to V . It follows that

$$\pi_2^* \circ \pi_{2*} \circ \pi_1^*(H^0(Z/H_1, \Omega_{Z/H_1}^1)) = \#H_2 \cdot p_{H_2} \pi_1^*(H^0(Z/H_1, \Omega_{Z/H_1}^1)) = \#H_2 \cdot p_{H_2} \cdot p_{H_1}(V)$$

has dimension equal to the rank of the operator $p_{H_2} \cdot p_{H_1}$. We have obtained:

Proposition 3.26. *The dimension of the image of the map $\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2)$ induced by the correspondence Z is equal to the rank of*

$$\left(\sum_{h_2 \in H_2} h_2 \right) \left(\sum_{h_1 \in H_1} h_1 \right) : V \rightarrow V. \quad (3.5)$$

Since we have already shown that the action of G on V is completely determined by the monodromy datum Σ , this allows us to express the dimension of $\text{Im}(\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2))$ in terms of (G, H_X, H_Y, Σ) .

Note furthermore that the same machinery allows us to also answer a slightly different question: for example, in our application we consider diagrams of curves of the form

$$\begin{array}{ccc}
 & Z & \\
 \pi_2 \swarrow & & \searrow \pi_1 \\
 X & & C \\
 \pi_3 \downarrow & & \\
 Y & &
 \end{array}$$

and we need to understand whether or not the image of the map $\text{Jac}(C) \rightarrow \text{Jac}(X)$ induced by the correspondence Z intersects the image of the map $\text{Jac}(Y) \rightarrow \text{Jac}(X)$ induced by pulling back divisors from Y to X . Passing to analytic uniformizations, the question is whether the subspaces $\pi_{2*} \circ \pi_1^*(H^0(C, \Omega_C^1))$ and $\pi_3^*(H^0(Y, \Omega_Y^1))$ of $H^0(X, \Omega_X^1)$ intersect nontrivially. However, since $\pi_1^*, \pi_2^*, \pi_3^*$ are all injective, it suffices to know whether

$$\pi_2^* \circ \pi_{2*} \circ \pi_1^*(H^0(C, \Omega_C^1)) \text{ and } \pi_2^* \circ \pi_3^*(H^0(Y, \Omega_Y^1)) = (\pi_3 \circ \pi_2)^*(H^0(Y, \Omega_Y^1))$$

intersect nontrivially inside V . Proceeding as above, and letting H_X, H_Y, H_C be the subgroups of G corresponding via Galois theory to X, Y, C respectively, we conclude that the image of the map $\text{Jac}(C) \rightarrow \text{Jac}(X)$ induced by Z intersects the image of $\text{Jac}(Y) \rightarrow \text{Jac}(X)$ if and only if the operator $p_{H_Y} p_{H_C}$ is nonzero.

3.4.5. *Conclusion.* Putting together the results of the previous paragraphs we obtain:

Proposition 3.27. *Let $Z \rightarrow \mathbb{P}^1$ be a Galois branched cover with group G . The monodromy datum of $Z \rightarrow \mathbb{P}^1$ determines the following (in an effectively computable way): For every subgroup $H < G$, the genus of Z/H , and for every pair of subgroups H_1, H_2 of G , the dimension of the image of the induced map $\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2)$.*

4. IMPLEMENTATION

We now turn to details and optimizations concerning the implementation of Problems 3.15 and 3.17 in practice. Since our solution to Problem 3.15 actually relies on being able to handle Part (i) of Problem 3.17, we begin with the latter.

4.1. **Solving Problem 3.17.** This is a direct application of the theory explained in Section 3:

Algorithm 4.1. *Input: a 4-tuple (G, H_X, H_Y, Σ) as in Problem 3.17.*

Output: the structure of $H^0(Z, \Omega_Z^1)$ as a G -representation; for each pair of subgroups $H_1 < H_2 < G$, the ramification structure of $Z/H_1 \rightarrow Z/H_2$, the genus of Z/H_1 , and the dimension of the image of the map $\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2)$ induced by Z as in (3.2).

Procedure:

- (i) *Compute the genera of $Z \rightarrow Z/H_1$ and the intermediate ramification of $Z/H_1 \rightarrow Z/H_2$ using (3.3) and Algorithm 3.21.*
- (ii) *Compute the G -module structure of $H^0(Z, \Omega_Z^1)$ as explained in Section 3.4.3.*
- (iii) *Compute the dimension of $\text{Im}(\text{Jac}(Z/H_1) \rightarrow \text{Jac}(Z/H_2))$ using Theorem 3.22 and Proposition 3.27.*

The theory behind each of these steps has been laid out in Section 3.4. These computations do not require the computation of curve equations and depend only on the specified ramification structure Σ over the branch locus B of $X \rightarrow \mathbb{P}^1$, and not on this branch locus itself. This independence of B implies that all our calculations may be performed abstractly, and will be valid for any choice of B . This means that we actually consider families of examples of dimension $-3 + r$, where r is the number of branch points of $X \rightarrow \mathbb{P}^1$, see Remark 3.8.

Finally, note that as long as the degree of the composed map $X \rightarrow \mathbb{P}^1$ is small, the computations involved in 4.1(i), which are described in Algorithm 3.21 and Section 3.4.2, take place in a symmetric group on a small set, and therefore terminate quickly. We discuss speedups for Parts (ii) and (iii) in the next section.

4.2. Solving Problem 3.15. Let (g_X, g_Y, d_X, d_Y, R) be given. We want to find the corresponding tuples (G, H_X, H_Y, Σ) . Recall that for $d = d_X d_Y$, the group G is the subgroup of S_d generated by the monodromy Σ . Moreover, we want that the corresponding Galois cover is the Galois closure of the cover of degree d corresponding to H_X . We can ensure this by fixing an embedding of G into S_d and letting H_X be the stabilizer of 1. In other words, given G , determining the possible pairs (G, H_X) comes down to realizing G as a conjugacy class of subgroups of S_d . Moreover, when the group G is not specified, we can find all pairs (G, H_X) up to equivalence by running through the conjugacy classes of subgroups of S_d . For this latter problem, efficient algorithms exist when d is small.

Remark 4.2. Note that at the very least G has to act transitively to correspond to a connected cover of \mathbb{P}^1 . Moreover, we may restrict to subgroups H_X with the property that H_X has a normal subgroup of index at most $(d_Y - 1)!$, since only such subgroups can give rise to a diagram (3.1) with the requested properties. (Indeed, the core of H_X in H_Y is a normal subgroup of H_Y that is contained in H_X and that is of index at most $d_Y!$ in H_Y .)

It now remains to find all the possible extensions of a given pair (G, H_X) to quadruples (G, H_X, H_Y, Σ) . Once (G, H_X) , or alternatively (by the above) an embedding of G into S_d , is given, the remaining isomorphisms on the level of covers translate into conjugation by the normalizer N_G of G in S_d . We accordingly determine the subgroups K_Y of G of index d_Y up to conjugacy by N_G . Having found this, we find representatives for triples (G, H_X, H_Y) as follows:

Proposition 4.3. *The simultaneous N_G -conjugacy classes of triples (G, K_X, K_Y) such that K_X (resp. K_Y) is N_G -conjugate to a given subgroup H_X (resp. H_Y) of G are in bijection with the double coset space $N_Y \backslash N_G / N_X$. Here N_Y (resp. N_X) is the normalizer of H_Y (resp. H_X) in N_G , and to a double coset $N_Y g N_X$ there corresponds the triple $(G, H_X, g^{-1} H_Y g)$.*

Proof. The indicated map is well-defined, and it is surjective since after conjugating by a suitable element of N_G if necessary we may assume that $K_X = H_X$. Conversely, if two pairs $(G, H_X, n_1^{-1} H_Y n_1)$ and $(G, H_X, n_2^{-1} H_Y n_2)$ are simultaneously N_G -conjugate, then $n_1^{-1} H_Y n_1 = g n_2^{-1} H_Y n_2 g$ for some element g of N_X , which implies that $n_2 g = h n_1$ for $h \in N_Y$. \square

Applying Proposition 4.3, we find the possible triples (G, H_X, H_Y) such that moreover $H_X < H_Y < G$, all up to simultaneous conjugacy by N_G . If so desired, we can impose that H_X be maximal in H_Y , to reflect that the corresponding map $X \rightarrow Y$ is indecomposable, and a similar remark applies to H_Y and G .

It then remains to find the possible monodromy data Σ starting from (G, H_X, H_Y) . For this, we have used fast and efficient code by Paulhus [Pau15] based on work of Breuer [Bre00]. This finds the possible Σ up to conjugation by elements of G once conjugacy classes in G are given. While we do not have these conjugacy classes at our disposal, we do have imposed ramification data R , which above any point determines the cycle structure of the corresponding conjugacy classes (recall that our data furnish a conjugacy class of embeddings of G into S_d , so that this is well-defined). This gives a finite number of explicit possibilities for the conjugacy classes above a given point. Combining the outcomes of Breuer's algorithms for all possible choices, we obtain the possible covers Σ . If so desired, we can still reduce the set of possible Σ further under common N_G -conjugacy to prevent duplicates. While we usually do this, it can occasionally cost some time if there are lots of covers involved, in which case our algorithms allow this step to be skipped.

Finally, given an element Σ , we append it to one of the triples obtained before to obtain a quadruple (G, H_X, H_Y, Σ) . If this quadruple has the correct ramification, as can be checked using Algorithm 4.1(i), then we retain this quadruple.

The above discussion motivates the following algorithm:

Algorithm 4.4. *Input:* (g_X, g_Y, d_X, d_Y, R) as in Definition 3.12.

Output: a list of 4-tuples (G, H_X, H_Y, Σ) .

Procedure:

- (i) Initialize $d := d_X d_Y$ and let \mathcal{L}_1 and \mathcal{L}_2 be the empty lists.
- (ii) Loop over representatives G of conjugacy classes of subgroups of S_d . For each representative do:
 - (a) If G is not transitive, discard G and continue with the next subgroup;
 - (b) Set H_X to be the stabilizer of 1 in G ;
 - (c) Append to \mathcal{L}_1 all triples (G, H_X, H_Y) obtained using Proposition 4.3.
- (iii) Using Breuer's algorithm as implemented by Paulhus, find all possible isomorphism classes of monodromy data Σ , up to N_G -conjugacy if desired. Loop over these Σ , and for a fixed such element do:
 - (a) Loop over the triples (G, H_X, H_Y) in \mathcal{L}_1 ;
 - (b) Using Algorithm 4.1, compute the genera of Z/H_X and of Z/H_Y . If $g(Z/H_X) \neq g_X$ or $g(Z/H_Y) \neq g_Y$, return to the beginning of the loop;
 - (c) Using Algorithm 4.1, compute the ramification structure of $X \rightarrow \mathbb{P}^1$. If it is different from R , return to the beginning of the loop;
 - (d) Add (G, H_X, H_Y, Σ) to \mathcal{L}_2 .
- (iv) Return \mathcal{L}_2 .

4.2.1. *Action of G on $H^0(Z, \Omega_Z^1)$ and calculation of image dimensions.* Given a finite group G , one can compute its character table, for example by using the Dixon–Schneider algorithm, or the LLL-based induce/reduce algorithm of Unger [Ung06]. Once the character table of G is known, in order to fully describe the G -representation V we simply need to determine the multiplicity with which each character χ of G appears in V . Such multiplicities can be obtained by applying Theorem 3.22 to the map $Z \rightarrow \mathbb{P}^1$. Indeed, given a character χ corresponding to a representation τ_χ , the only information we need to determine ν_χ are the numbers e_i and $N_{i,\alpha}$. We have already observed that e_i is the order of σ_i . Furthermore, by definition, $N_{i,\alpha}$ is the multiplicity of ζ_{e_i} as

an eigenvalue of $\tau_\chi(\sigma_i)$. This multiplicity can be read off the characteristic polynomial of $\tau_\chi(\sigma_i)$, whose coefficients are the elementary symmetric functions in the eigenvalues of $\tau_\chi(\sigma_i)$. As we are in characteristic zero, the symmetric functions of $\lambda_1, \dots, \lambda_k$ are determined by the Newton sums

$$\sum_{i=1}^k \lambda_i = \text{tr } \tau_\chi(\sigma_i) = \chi(\sigma_i), \quad \sum_{i=1}^k \lambda_i^2 = \text{tr } \tau_\chi(\sigma_i^2) = \chi(\sigma_i^2), \quad \dots, \quad \sum_{i=1}^k \lambda_i^k = \text{tr } \tau_\chi(\sigma_i^k) = \chi(\sigma_i^k).$$

This shows that the knowledge of the character χ is enough to determine the characteristic polynomial of $\tau_\chi(\sigma_i)$, hence we may compute the numbers $N_{i,\alpha}$ from the knowledge of χ without even having to describe the G -module τ_χ . This solves Part (ii) of Algorithm 4.1. Part (iii) can then be obtained by calculating the relevant irreducible representations τ_χ explicitly (there is functionality available to this end in our computer algebra system of choice MAGMA) and summing the dimensions of the images of the maps obtained in Proposition 3.26, multiplied by the relevant multiplicities. In our application, we often use the following more specific procedure:

Algorithm 4.5. *Input: a 4-tuple (G, H_X, H_Y, Σ) as in Problem 3.17.*

Output: A subgroup H_C of G (if it exists) for which the corresponding curve $C = Z/H_C$ has the following properties:

- $0 < g_C \leq g_X - g_Y$;
- The map $\text{Jac}(C) \rightarrow \text{Jac}(X)$ induced by $X \leftarrow Z \rightarrow C$ is injective;
- The image of $\text{Jac}(C) \rightarrow \text{Jac}(X)$ does not intersect the image of $\text{Jac}(Y) \rightarrow \text{Jac}(X)$.

Procedure:

- (i) Run through the subgroups of H of G ;
- (ii) Compute the genus g_C of the curve $C := Z/H$. If we do not have that $0 < g_C \leq g_X - g_Y$, then move on to the next H , otherwise proceed to (iii);
- (iii) Compute the dimension of the image of the induced map $\text{Jac}(C) \rightarrow \text{Jac}(Y)$ using the G -module $H^0(Z, \Omega_Z^1)$ and Proposition 3.26. If it is non-zero, then move on to the next H , otherwise proceed to (iv);
- (iv) Using similar methods, compute the dimension of the image of the induced map $\text{Jac}(C) \rightarrow \text{Jac}(X)$. If its dimension does not equal g_C , then move on to the next H , otherwise return H .

Remark 4.6. Algorithm 4.5 insists on the injectivity of the map $\text{Jac}(C) \rightarrow \text{Jac}(X)$ because otherwise we would have to deal with another decomposition problem in order to describe the part of the Prym variety thus obtained as a Jacobian.

If the algorithm returns a group H_C for which moreover $g_C = g_X - g_Y$, then $\text{Jac}(X) \sim \text{Jac}(C) \times \text{Jac}(Y)$, so that (up to isogeny) we have realized the Prym variety of the cover $X \rightarrow Y$ as the Jacobian of the curve C . If for all (G, H_X, H_Y, Σ) that we consider we can find a group H_C and a corresponding curve C as above, then we know that for every diagram $X \rightarrow Y \rightarrow \mathbb{P}^1$ of type (g_X, g_Y, d_X, d_Y, R) , the abelian variety $\text{Prym}(X \rightarrow Y)$ is isogenous to the Jacobian of a quotient C of the Galois closure of $X \rightarrow \mathbb{P}^1$. Even if this does not happen, it is still possible that we are successful for, say, all quadruples for which G is in a certain specified isomorphism class. To our surprise, we have discovered several types (g_X, g_Y, d_X, d_Y, R) for which this construction gives non-trivial information on the Prym variety, and we report on these findings in Section 5.3 below.

Even if there is no single quotient C in Algorithm 4.5 such that $\text{Jac}(C)$ is isogenous to $\text{Prym}(X \rightarrow Y)$, it may still happen that the latter Prym variety is isogenous to a product of Jacobians obtained in this fashion, as can be ascertained by determining the sum of the corresponding subspaces in $\text{Jac}(X)$. An example of this is given in the entry **rr-spec** of Table 3, as explained in Section 5.

4.2.2. Some fine print and speedups. This final section contains a smattering of more detailed remarks on our implementation, calculations, and results. To start, we note that the calculation in Algorithm 4.5(ii) is possible from the knowledge of the modules τ_χ and their multiplicities n_χ , which we need only calculate once given G and Σ . As we run through the possible Σ , we store the different intervening representations τ_χ so that we do not have to recalculate them later for different Σ . (We do have to calculate new multiplicities n_χ , but this is fortunately far less laborious.) This is worthwhile because our implementation works with the Chevalley-Weil decomposition throughout: All dimension calculations involving Proposition 3.26 are done for the irreducible representation τ_χ , after which the corresponding results are summed with the relevant multiplicities n_χ .

When looking for a single curve C to furnish the complement of $\text{Jac}(Y)$ in $\text{Jac}(X)$, we can in fact do better than running over all possible H . Indeed, we still have the ambient isomorphism group N_G to consider, and reasoning as in Proposition 4.3 shows that it suffices to consider candidate subgroups K up to conjugacy at first. Whether the condition in Algorithm 4.5(ii) holds depends only on the G -conjugacy class of H . Given a representative K of such a conjugacy class, the argument from Proposition 4.3 then shows that we only need consider the possibilities $(G, H_X, H_Y, \Sigma, n^{-1}Kn)$ where n runs through the double coset $N_C \backslash G / (N_X \cap N_Y)$ for N_C (resp. N_X, N_Y) the normalizer of K (resp. H_X, H_Y) in G . Since the pairs (H_X, H_Y) in our quadruples (G, H_X, H_Y, Σ) stem from a fixed list, we can store these double coset representatives on the fly so as not to have to recalculate them.

This same uniformity then ensures that only a relatively small number of triples (H_X, H_Y, H) is encountered for a fixed group G , albeit for many different Σ and with many different multiplicities. This makes it very worthwhile to store all the ranks and projectors in Proposition 3.26 that are calculated when working with a fixed representation τ_χ in a hash table, as considerable time is gained when using a lookup instead of a recalculation. In fact, in practice our calculations show that most time is spent constructing the explicit projectors in Proposition 3.26 on the larger irreducible subrepresentations of $H^0(Z, \Omega_Z^1)$. Similarly, we can ensure that the rank of composition of these projectors does not need be calculated for τ_χ when we encounter a previously stored triple (H_X, H_Y, H) , which is very often the case in practice.

5. RESULTS

5.1. Presentation of the tables. The tables in the appendix describe results obtained by running our algorithms. We recover *all* classical results from the literature (up to time limitations of our codes), as we will discuss later on. First we explain how to read an entry in these tables, illustrated by the concrete case **total4**:

“ g_X, g_Y, d_X ” For the case **total4**, the genus g_X of X equals 4, the genus g_Y of Y equals 1 and the degree d_X of the cover $X \rightarrow Y$ equals 4.

“Ramification” This describes the ramification structure of the composition $X \rightarrow Y \rightarrow \mathbb{P}^1$. The degree of $Y \rightarrow \mathbb{P}^1$ usually equals 2. If not, the name of the case starts with the degree $\deg(Y/\mathbb{P}^1)$ (for instance **3-orig** in Table 6). A thin line represents an unramified point. A thick line without a number on its side a totally ramified point; for a thick line with a number on its side, this number specifies the ramification index. For all ramification types thus displayed, the number over them represents the number of copies in the total ramification structure. In the case **total4**, we see that the map $Y \rightarrow \mathbb{P}^1$ has 4 ramification points, all of which split totally in the cover $X \rightarrow Y$. Moreover, the 2 total ramification points of $X \rightarrow Y$ are merged under the map $X \rightarrow \mathbb{P}^1$.

“ $\#G, g_Z$ ” This lists the different possible pairs $\#G, g_Z$, where $\#G = \deg(Z \rightarrow \mathbb{P}^1)$ is the cardinality of the monodromy group G and where g_Z is the genus of Z . In the case **total4** there turns out to be only one such pair.

“ X nhyp/hyp” Running through the possible cases from the previous item, we consider the isomorphism classes of curves X for which an automorphism of the Galois closure induces a hyperelliptic involution. Given such a class, we use our algorithms to check whether a piece of the Prym variety of $X \rightarrow Y$ is given by the Jacobian of a quotient of Z . The number of curves for which this happens (resp. does not happen) is the second bracket entry of the case listed in this column. The first entry does the same, but instead for those isomorphism class of curves X for which no hyperelliptic involution is induced by the Galois closure. In the case **total4**, we obtain 48 possibly non-hyperelliptic and 16 hyperelliptic curves in this way for the single possible pair $\#G, g_Z$, for all of which we can indeed generate a piece of the Prym variety as the Jacobian of a quotient of Z .

“Prym dims” For the entries above, we give the dimensions of the disjoint pieces of the Prym variety that we found as Jacobians of quotients of Z , separated between non-hyperelliptic and hyperelliptic case (if one, or both, of these cases never yields a piece of the Prym, it does simply not appear). In the case **total4**, we always find a curve C of genus 3 such that $\text{Jac } C \sim P(X/Y)$ in the non-hyperelliptic case. By contrast, in the hyperelliptic case, we find two curves C_1 and C_2 of genus 1 and 2 such that $\text{Jac } C_1 \times \text{Jac } C_2 \sim P(X/Y)$. It is possible that there are multiple cases with different resulting dimensions. This is illustrated in the case **total5**.

“ $\deg Z \rightarrow C_i$ ” The last column gives the degrees of the maps $Z \rightarrow C_i$ obtained in the previous entry, separated into the non-hyperelliptic and hyperelliptic case as before.

Remark 5.1. Our implementation allows the determination of more information, like the ramification of intermediate covers.

Remark 5.2. Given a certain ramification structure, our programs can equally well calculate results for “specializations” of it, for instance those obtained by collapsing two ramification points of the cover $Y \rightarrow \mathbb{P}^1$. We did not try to do this systematically, but we did often observe that if one recovers the Prym as the Jacobian of a quotient of Z in the generic initial case, this continues to hold for the specializations. A notable example of this is furnished by Table 6.

5.2. Comments on the tables. Let us start with examples that already appear in the existing literature and that we could recover and extend.

- Table 3 recovers the [RR18] case we looked at in Section 2 and which was the starting point of this article.

- Table 4 gathers covers of genus 2 of curves genus 1 by a map of degree d_X with $2 \leq d_X \leq 7$. In all these cases the Prym (which is a curve of genus 1) appears as a quotient of the Galois closure Z . Note that when $2 \leq d_X \leq 11$, there are direct construction of the Prym as an explicit curve of genus 1: The case $d_X = 2$ goes back to the work of Jacobi on abelian integrals, (see the references in [Bak95, p.395] or [HLP00]), $d_X = 3$ (see [Gou85], [Kuh88] or the appendix of [BHLS15]), $d_X = 4$ (see [Bol87] and [BD11]), $d_X = 5$ (see [MSV09]) and more generally when $d_X \leq 11$ (see [Kum15]).
- Table 5 gathers degree 2-covers of hyperelliptic curves ramified over exactly 2 points. We recover the results of [Dal75] and [Lev12, Th.4.1].
- Table 6 gathers étale covers of degree 2 of curves of genus $g_Y \geq 3$. Bruin's result [Bru08] for $g_X = 5$ is the first configuration and we see that it seems to generalize well to higher genus. In this case, we have not determined all covers, as there are tens of millions of these, but have instead taken a sample of several hundreds of such covers by generating these randomly. Note that here, the map to \mathbb{P}^1 is of degree 3, which for $g_Y = 3$ and $g_Y = 4$ is actually the smallest degree that is generically possible.

Here are some new ramification patterns:

- Table 7 gathers étale covers of curves of genus 2 by maps of degree 3, 4 and 5. The situation is more chequered, since certain cases give positive results and other do not, even for the same ramification structure.
- Table 8 is a new situation which does not appear in the literature. One sees that when the degree of the cover from X to the curve Y of genus 1 is 3 or 4 we only get positive cases (that is, cases in which our strategy can describe the Prym as a Jacobian up to isogeny), but as soon as the degree is 5, we only get very few favorable situations.
- Table 9 gathers some miscellaneous cases.

5.3. Some explicit equations. As an application of our programs, we consider the first case of Table 8: $g_X = 3$, $g_Y = 1$, $d_X = 3$ and $d_Y = 2$ with the ramification data

$$R = (\{(3, 2)\}, \{(2, 3)\}, \{(2, 3)\}, \{(2, 3)\}, \{(2, 3)\}).$$

The cover $X \rightarrow \mathbb{P}^1$ may be Galois with $G \simeq S_3$: in this case, X is non-hyperelliptic, and the result already appears in Table 2. We therefore concentrate on the second case where X is hyperelliptic. The programs show in the same way that Z is also hyperelliptic, is equipped with an action of $C_2 \times S_3$, and admits both X (of genus 3) and C (of genus 2) as quotients by involutions. Since the action of S_3 commutes with that of the hyperelliptic involution, we may assume that the automorphism group is generated by $\sigma : (x, y) \mapsto (\zeta_3 x, y)$, $\tau : (x, y) \mapsto (1/x, y/x^6)$ and $\iota : (x, y) \mapsto (x, -y)$. This means that the hyperelliptic curve Z , of genus 5, is given by

$$y^2 = x^{12} + ax^9 + bx^6 + ax^3 + 1,$$

with discriminant $3^{12} (a^2 - 4b + 8)^6 ((b + 2)^2 - 4a^2)^3 \neq 0$. The quotient $Z/\langle \iota\tau \rangle$ is the genus 3 curve X , and by taking the fixed functions $u = x + 1/x$ and $v = y(x - 1/x)$ we obtain:

$$X : v^2 = (u^6 - 6u^4 + au^3 + 9u^2 - 3au + (b - 2))(u^2 - 4),$$

with discriminant $-2^4 \cdot 3^6 \cdot (a^2 - 4b + 8)^3 (4a^2 - (b + 2)^2)^3 \neq 0$. The map $X \rightarrow Y$ can then be recovered by considering the quotient $Z/\langle \iota\tau, \sigma \rangle$: we then obtain $Y : t^2 = (s^2 - 4)(s^2 + as + (b - 2))$

and a 3-to-1 map

$$\begin{aligned} X &\rightarrow Y \\ (u, v) &\mapsto (u^3 - 3u, v(u^2 - 1)). \end{aligned}$$

The Prym variety of $X \rightarrow Y$ is isogenous to the Jacobian of $C = Y/\langle \tau \rangle$. By taking the fixed functions $u = x + 1/x$ and $v' = y/x^3$ we obtain:

$$C : v'^2 = (u^6 - 6u^4 + au^3 + 9u^2 - 3au + (b - 2)).$$

The discriminant is $-729(a^2 - 4b + 8)^3(4a^2 - (b + 2)^2) \neq 0$, so this is indeed a smooth curve of genus 2.

We remark that once this example, and similar ones in higher genus, were brought to our attention by the output of our programs, we were able to spot a generalisation, which allowed us to recover some of the hyperelliptic cases in Table 8. Fix an integer $k \geq 2$ and consider the hyperelliptic curve $Z : y^2 = f(x)$, where $f(x) = x^{4k} + ax^{3k} + bx^{2k} + ax^k + 1$ for generic a and b . Factor $f(x) = (x^k - \alpha_1^k)(x^k - \alpha_2^k)(x^k - \frac{1}{\alpha_1^k})(x^k - \frac{1}{\alpha_2^k})$. The automorphism group of Z contains the hyperelliptic involution $\iota(x, y) = (x, -y)$ and the elements $\sigma(x, y) = (\zeta_k x, y)$ and $\tau(x, y) = (\frac{1}{x}, \frac{y}{x^{2k}})$. The quotient $\pi_{Z/X} : Z \rightarrow X := Z/\langle \iota\tau \rangle$ can be described thanks to the invariant functions $u = x + \frac{1}{x}$ and $v = \frac{y}{x^k}(x - \frac{1}{x})$, which lead to the equation

$$X : v^2 = (u^2 - 4)(g^2(u) + ag(u) + b - 2).$$

The polynomial $(u^2 - 4)(g^2(u) + ag(u) + b - 2)$ has $2k + 2$ different roots, and X is a smooth hyperelliptic curve of genus k . Similarly, we consider the quotient $\pi_{Z/C} : Z \rightarrow C := Z/\langle \tau \rangle$, and to get an equation for C we consider the invariant functions $u = x + \frac{1}{x}$ and $w = \frac{y}{x^k}$. We write first $f(x) = x^{2k}((x^k + \frac{1}{x^k})^2 + a(x^k + \frac{1}{x^k}) + b - 2)$, and note that there exists a polynomial g of degree k such that $g(x + \frac{1}{x}) = x^k + \frac{1}{x^k}$. We get then $C : w^2 = g^2(u) + ag(u) + b - 2$. The roots of $g^2(u) + ag(u) + b - 2$ are $\zeta_k^i \alpha_j + \frac{1}{\zeta_k^i \alpha_j}$ with $i = 0, 1, \dots, k - 1$ and $j = 1, 2$. This yields a smooth hyperelliptic curve C of genus $g(C) = k - 1$. Furthermore, we consider the quotient $\pi_{X/Y} : X \rightarrow Y = Z/\langle \iota\tau, \sigma \rangle$: we take the invariant functions $U = x^k + \frac{1}{x^k} = g(u)$ and $V = \frac{y}{x^k}(x^k - \frac{1}{x^k}) = vh(u)$, where h is a degree $k - 1$ polynomial such that $h(x + \frac{1}{x}) = \frac{x^k - \frac{1}{x^k}}{x - \frac{1}{x}}$. We get then the equation $Y : V^2 = (U^2 - 4)(U^2 + aU + b - 2)$. The roots of $(U^2 - 4)(U^2 + aU + b - 2)$ are all different, and Y is a smooth curve genus 1. Computing the pullbacks to Z of the regular differentials of X, Y and C leads to the following proposition:

Proposition 5.3. *With the notation above, the Prym variety $\text{Prym}(X/Y)$ is isogenous to the Jacobian of the curve C .*

REFERENCES

- [Bak95] H. F. Baker. *Abelian functions*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1995. Abel's theorem and the allied theory of theta functions, Reprint of the 1897 original, With a foreword by Igor Krichever. 25
- [Bar06] F. Bars. Automorphism groups of genus 3 curves. Notes del seminari Corbes de Gèneres 3, 2006. 4
- [BCP97] W. Bosma, J. Cannon, and 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). 3
- [BD11] N. Bruin and K. Doerksen. The arithmetic of genus two curves with $(4, 4)$ -split Jacobians. *Canad. J. Math.*, 63(5):992–1024, 2011. 25

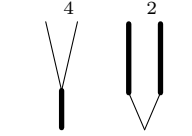
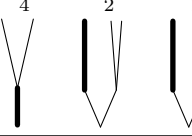
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \rightarrow C_i$
rr-spec	3, 1, 2		4, 3	[3, 0], [0, 0]	[1, 1]	[2]
rr-gen	3, 1, 2		8, 7	[8, 0], [0, 0]	[2]	[2]

TABLE 3. Recovering Ritzenthaler–Romagny

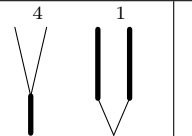
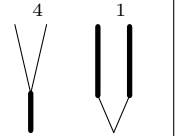
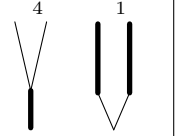
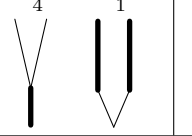
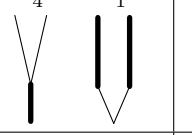
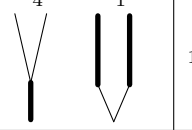
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \rightarrow C_i$
g2-2	2, 1, 2		4, 2	[0,0],[4,0]	[1]	[2]
g2-3	2, 1, 3		12, 4	[0,0],[16,0]	[1]	[2]
g2-4	2, 1, 4		48, 13	[0,0],[48,0]	[1]	[4]
g2-5	2, 1, 5		240, 61	[0,0],[160,0]	[1]	[12]
g2-6	2, 1, 6		1440, 361	[0,0],[240,0]	[1]	[48]
g2-7	2, 1, 7		10080, 2521	[0,0],[672,0]	[1]	[240]

TABLE 4. Genus 2 to genus 1

- [Ber13] J. Bertin. Algebraic stacks with a view toward moduli stacks of covers. In *Arithmetic and geometry around Galois theory*, volume 304 of *Progr. Math.*, pages 1–148. Birkhäuser/Springer, Basel, 2013. [13](#)
- [BHLS15] R. Bröker, E. W. Howe, K. E. Lauter, and P. Stevenhagen. Genus-2 curves and Jacobians with a given number of points. *LMS J. Comput. Math.*, 18(1):170–197, 2015. [25](#)
- [Bol87] O. Bolza. Über die Reduction hyperelliptischer Integrale erster Ordnung und erster Gattung auf elliptische durch eine Transformation vierten Grades. *Math. Ann.*, 28:447–456, 1887. [25](#)
- [Bou98] I. I. Bouw. *Tame covers of curves: p-ranks and fundamental groups*. PhD thesis, Utrecht University, 1998. [4](#)
- [BR11] J. Bertin and M. Romagny. Champs de Hurwitz. *Mém. Soc. Math. Fr. (N.S.)*, (125-126):219, 2011. [16](#)

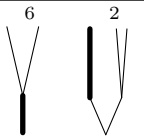
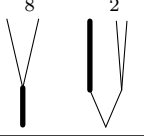
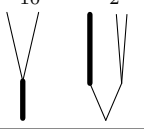
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \rightarrow C_i$
g2	4, 2, 2		8, 9	[32, 0], [0, 0]	[2]	[2]
g3	6, 3, 2		8, 13	[128, 0], [0, 0]	[3]	[2]
g4	8, 4, 2		8, 17	[512, 0], [0, 0]	[4]	[2]

TABLE 5. Testing Dalaljan's results



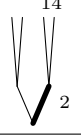
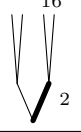
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \rightarrow C_i$
3-orig	5, 3, 2		24, 37	[?, 0], [0, 0]	[2]	[6]
3-g7	7, 4, 2		24, 49	[?, 0], [0, 0]	[2]	[6]
3-g9	9, 5, 2		24, 61	[?, 0], [0, 0]	[2]	[6]
3-g11	11, 6, 2		24, 73	[?, 0], [0, 0]	[2]	[6]

TABLE 6. Generalizing Bruin's results


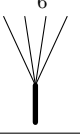
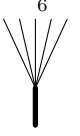
Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \rightarrow C_i$
etale-3	4, 2, 3		6, 4 12, 5	[40, 0], [0, 0] [0, 0], [60, 0]	[1, 1] [2]	[2, 2] [2]
etale-4	5, 2, 4		24, 13 48, 23 96, 49	[0, 0], [0, 120] [540, 0], [360, 0] [240, 0], [0, 0]	[3], [3] [3]	[8], [4] [6]
etale-5	6, 2, 5		10, 6 20, 11 120, 61 200, 101 240, 121 14400, 7201	[156, 0], [0, 0] [0, 0], [180, 0] [4032, 0], [0, 0] [0, 2785], [0, 0] [0, 10080], [0, 6000] no good	[2, 2] [4] [2] or [1]	[2, 2] [2] [24] or [8]

TABLE 7. Postcomposing étale covers of curves of genus 2

Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \rightarrow C_i$
total-3	3, 1, 3		6, 3 12, 5	[9, 0], [0, 0] [0, 0], [6, 0]	[2] [2]	[2] [2]
total-4	4, 1, 4		48, 19	[48, 0], [16, 0]	[3], [3]	[8], [4]
total-5	5, 1, 5		10, 5 20, 9 100, 41 120, 49 120, 49 200, 81 240, 97 7200, 2881 14400, 5761	[25, 0], [0, 0] [0, 0], [12, 0] [0, 12], [0, 0] [380, 0], [0, 0] [0, 0], [0, 25] [0, 96], [0, 0] [0, 450], [0, 60] [0, 90], [0, 0] [0, 360], [0, 0]	[4] [2] [2] or [1]	[2] [2] [24] or [8]

TABLE 8. Merging total ramification above two points

Case	g_X, g_Y, d_X	Ramification	$\#G, g_Z$	X nhyp/hyp	Prym dims	$\deg Z \rightarrow C_i$
3131	3, 1, 4		24, 9 48, 17 96, 33	[0, 0], [0, 27] [54, 0], [36, 0] [54, 0], [0, 0]	[2], [1, 1] [2]	[8], [4, 6] [6]
4211	3, 1, 4		192, 73	[64, 0], [0, 0]	[2]	[16]

TABLE 9. Genus 3 to genus 1, degree 4

- [Bre00] T. Breuer. *Characters and automorphism groups of compact Riemann surfaces*, volume 280 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. [3](#), [21](#)
- [Bru08] N. Bruin. The arithmetic of Prym varieties in genus 3. *Compos. Math.*, 144(2):317–338, 2008. [2](#), [3](#), [25](#)
- [CWH34] C. Chevalley, A. Weil, and E. Hecke. Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers. *Abh. Math. Sem. Univ. Hamburg*, 10(1):358–361, 1934. [3](#), [16](#)
- [Dal75] S. G. Dalaljan. The Prym variety of a two-sheeted covering of a hyperelliptic curve with two branch points. *Mat. Sb. (N.S.)*, 98(140)(2 (10)), 1975. [2](#), [25](#)
- [Dol12] I. V. Dolgachev. *Classical algebraic geometry*. Cambridge University Press, Cambridge, 2012. A modern view. [4](#)
- [Don92] R. Donagi. The fibers of the Prym map. In *Curves, Jacobians, and abelian varieties (Amherst, MA, 1990)*, volume 136 of *Contemp. Math.*, pages 55–125. Amer. Math. Soc., Providence, RI, 1992. [2](#)
- [ER08] V. Enolskii and P. Richter. Periods of hyperelliptic integrals expressed in terms of θ -constants by means of Thomae formulae. *Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.*, 366(1867):1005–1024, 2008. [7](#)
- [Gou85] E. Goursat. Sur la réduction des intégrales hyperelliptiques. *Bull. Soc. Math. France*, 13:143–162, 1885. [25](#)
- [GS01] P. Gaudry and E. Schost. On the invariants of the quotients of the Jacobian of a curve of genus 2. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 373–386. Springer, Berlin, 2001. [1](#)
- [Hen76] P.-G. Henn. *Die Automorphismengruppen der algebraischen Funktionenkörper vom Geschlecht 3*. PhD thesis, Heidelberg, 1976. [4](#)

- [HLP00] E. W. Howe, F. Leprévost, and B. Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000. [25](#)
- [IJR19] M. Izquierdo, L. Jiménez, and A. Rojas. Decomposition of Jacobian varieties of curves with dihedral actions via equisymmetric stratification. *Rev. Mat. Iberoam.*, 35(4):1259–1279, 2019. [1](#)
- [KR89] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989. [1](#)
- [Kuh88] R. M. Kuhn. Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc.*, 307(1):41–49, 1988. [25](#)
- [Kum15] A. Kumar. Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields. *Res. Math. Sci.*, 2:Art. 24, 46, 2015. [25](#)
- [Len08] H. Lenstra, Jr. Galois theory for schemes. Manuscript at <http://websites.math.leidenuniv.nl/algebra/>, 2008. [13](#)
- [Lev12] A. Levin. Siegel’s theorem and the Shafarevich conjecture. *J. Théor. Nombres Bordeaux*, 24(3):705–727, 2012. [2](#), [7](#), [25](#)
- [LLGRS20] D. Lombardo, E. Lorenzo García, C. Ritzenthaler, and J. Sijsling. `prym_decomposition`, a MAGMA package for realizing Prym varieties as Jacobians. https://github.com/JRSijsling/prym_decomposition, 2020. [3](#)
- [LO11] H. Lange and A. Ortega. Prym varieties of triple coverings. *Int. Math. Res. Not. IMRN*, (22):5045–5075, 2011. [2](#)
- [LO18] H. Lange and A. Ortega. Prym varieties of étale covers of hyperelliptic curves. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 18(2):467–482, 2018. [2](#)
- [LR12] R. Lercier and C. Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012. [4](#)
- [Mas91] W. S. Massey. *A basic course in algebraic topology*, volume 127 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. [13](#)
- [Mir95] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995. [11](#), [12](#)
- [MSSV02] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein. The locus of curves with prescribed automorphism group. *Sūrikaiseikikenkyūsho Kōkyūroku*, (1267):112–141, 2002. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). [4](#), [12](#), [16](#)
- [MSV09] K. Magaard, T. Shaska, and H. Völklein. Genus 2 curves that admit a degree 5 map to an elliptic curve. *Forum Math.*, 21(3):547–566, 2009. [25](#)
- [Mum74] D. Mumford. Prym varieties. I. In *Contributions to analysis (a collection of papers dedicated to Lipman Bers)*, pages 325–350. 1974. [2](#)
- [Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. [13](#)
- [Pau08] J. Paulhus. Decomposing Jacobians of curves with extra automorphisms. *Acta Arith.*, 132(3):231–244, 2008. [1](#)
- [Pau15] J. Paulhus. Branching data for curves up to genus 48. Preprint and code, 2015. [3](#), [21](#)
- [PR17] J. Paulhus and A. M. Rojas. Completely decomposable Jacobian varieties in new genera. *Exp. Math.*, 26(4):430–445, 2017. [1](#)
- [RR03] S. Recillas and R. Rodríguez. Prym varieties and fourfold covers, 2003. [3](#)
- [RR06] S. Recillas and R. E. Rodríguez. Prym varieties and fourfold covers. II. The dihedral case. In *The geometry of Riemann surfaces and abelian varieties*, volume 397 of *Contemp. Math.*, pages 177–191. Amer. Math. Soc., Providence, RI, 2006. [3](#)
- [RR18] C. Ritzenthaler and M. Romagny. On the Prym variety of genus 3 covers of genus 1 curves. *Épjournal Geom. Algébrique*, 2:Art. 2, 8, 2018. [2](#), [5](#), [6](#), [10](#), [24](#)
- [Ser78] J.-P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978. [17](#)
- [Tsi12] J. Tsimerman. The existence of an abelian variety over $\overline{\mathbb{Q}}$ isogenous to no Jacobian. *Ann. of Math. (2)*, 176(1):637–650, 2012. [2](#)

- [Ung06] W. R. Unger. Computing the character table of a finite group. *J. Symbolic Comput.*, 41(8):847–862, 2006. [21](#)
- [Ver83] A. Vermeulen. *Weierstrass points of weight two on curves of genus three*. PhD thesis, university of Amsterdam, Amsterdam, 1983. [4](#)
- [Wei35] A. Weil. Über Matrizenringe auf Riemannschen Flächen und den Riemann - Rochsehen Satz. *Abh. Math. Sem. Univ. Hamburg*, 11(1):110–115, 1935. [3](#), [16](#)

DAVIDE LOMBARDO, DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI PISA, LARGO BRUNO PONTECORVO 5, 56127 PISA, ITALIA

E-mail address: `davide.lombardo@unipi.it`

ELISA LORENZO GARCÍA, UNIV RENNES, CNRS, IRMAR - UMR 6625, F-35000 RENNES, FRANCE.

E-mail address: `elisa.lorenzogarcia@univ-rennes1.fr`

CHRISTOPHE RITZENTHALER, UNIV RENNES, CNRS, IRMAR - UMR 6625, F-35000 RENNES, FRANCE.

E-mail address: `christophe.ritzenthaler@univ-rennes1.fr`

JEROEN SIJSLING, INSTITUT FÜR REINE MATHEMATIK, UNIVERSITÄT ULM, HELMHOLTZSTRASSE 18, 89081 ULM, GERMANY

E-mail address: `jeroen.sijsling@uni-ulm.de`