Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. Journal of Algebra, 372(0):595-636, December 2012.

HYPERELLIPTIC CURVES AND THEIR INVARIANTS: GEOMETRIC, ARITHMETIC AND ALGORITHMIC ASPECTS

REYNALD LERCIER AND CHRISTOPHE RITZENTHALER

Abstract. We apply classical invariant theory of binary forms to explicitly characterize isomorphism classes of hyperelliptic curves of small genus and, conversely, propose algorithms for reconstructing hyperelliptic models from given invariants. We focus on genus 3 hyperelliptic curves. Both geometric and arithmetic aspects are considered.

Introduction

Invariant theory played a central role in 19th century algebra and geometry, yet many of its techniques and algorithms were practically forgotten by the middle of the 20th century and replaced by the abstract and powerful machinery of modern algebraic geometry. However, motivated by computational applications to cryptography, robotics, coding theory, *etc.*, the classical invariant theory has come to a renaissance. Among classical groups, the natural action of SL_2 on binary forms has received most attention. One reason is the remarkable formalism developed by Gordan in 1868 to compute a finite set of generators of invariants. The other reason is the application of hyperelliptic curves in cryptography, especially for the so-called CM methods (see [14]).

When K is an algebraically closed field of characteristic 0 or a prime $p \neq 2$, hyperelliptic curves of genus $g > 1$ are indeed naturally related to the action of $\mathrm{SL}_2(K)$ on binary forms of even degree $n = 2g+2$. Thus, isomorphisms between curves with equation $y^2 = f(x)$ and $f \in K[x]$ of degree n are globally determined by a $\mathrm{SL}_2(K)$ action on f (see Section 1.2). Thus the K-isomorphism classes of hyperelliptic curves of genus g can be represented by the values of a finite set of invariants for $\mathrm{SL}_2(K)$. In this way, exploring properties of the invariants leads to effective results on the geometry and arithmetic of the hyperelliptic moduli space.

On the geometric level, to make explicit the representation of the classes by invariants, we have to tackle a double task: compute a set of generators $\{I_i\}$ of invariants and reciprocally construct a curve from given values of these invariants. We call the latter the *reconstruction* phase. As a by-product, we also want to be able to read some geometric information, in particular the automorphism group of a curve, from the invariants.

The first issue can be addressed thanks to Gordan's method which is based on a differential operator called *transvectant*, see Section 1. Contrary to the genus 2 case which is described by 4 algebraically independent invariants, Shioda [47] gave in genus 3 a basis of 9 invariants (which we call *Shioda invariants*), the first 6 being algebraically independent and the last three related to the others by 5 explicit relations. Besides this, unlike the genus 2 case and the classical Igusa invariants [30], the discriminant is not an element of this basis. We therefore decided not to use the usual representation based on 'absolute invariants' and to switch to a weighted projective space of invariants for which we rely on some specific algorithms to test equality or to create points. Note that although we restrict to genus 3 in the present article, these algorithms apply to any weighted projective space and are therefore useful for hyperelliptic curves of higher genus too.

The main algorithm for the second issue relies on Mestre's method which he exposes for $g = 2$ in [38]. It is based on computations going back to [13, § 103] (see Section 2) and uses a generalization of invariants called *covariants* (see Definition 1.1). Roughly speaking, starting from three order 2 covariants, one constructs a

Date: January 10, 2015.

2010 *Mathematics Subject Classification.* 14Q05 ; 13A50 ; 14H10 ; 14H37.

Key words and phrases. invariant ; covariant ; binary forms ; field of moduli ; field of definition ; automorphism ; reconstruction ; genus 3 ; moduli space ; weighted projective space ; algorithm ; hyperelliptic curve.

Both authors acknowledge support by grant ANR-09-BLAN-0020-01.

plane conic $\mathcal{Q}$ and a plane degree $g+1$ curve $\mathcal{H}$ whose coefficients are invariants, hence expressible in terms of the generators $\{I_i\}$. After specialization at given values of invariants, if $\mathcal{Q}$ is not singular, the degree 2-cover of $\mathcal{Q}$ ramified at the $2(g+1) = n$ points of intersection of $\mathcal{Q}$ and $\mathcal{H}$ is a hyperelliptic curve with invariants equal to the initial values. In order to make this practical, one of the main computational difficulties is to find the expressions of the coefficients in terms of $\{I_i\}$ as the degree and number of variables are for $g = 3$ already quite large. We by-passed the difficulty using an evaluation-interpolation strategy.

For genus 2, this algorithm enabled Mestre to reconstruct hyperelliptic curves C with no *extra-automorphism*, *i.e.* $\mathrm{Aut}(C)$ is generated by the hyperelliptic involution ι. Indeed, it was proved in [4] that the 'classical' $\mathcal{Q}$ is always non-singular in this case. It is however always singular when C has extra-automorphisms and it cannot be used anymore. Cardona and Quer in [11] completed the picture by a different choice of order 2 covariants[1] which lead to another conic $\mathcal{Q}$ non-singular in the case $\mathrm{Aut}(C) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ (for bigger automorphism groups, explicit parameterizations were already known). The two authors of the present article have implemented these constructions with the computational algebra software MAGMA and generalized them to the remaining fields of small characteristics (3 and the most difficult case 5) [32]. Genus 2 can be considered as solved.

It is thus natural to turn to genus 3. Here also, the issues that we tackle are naturally stratified by the automorphism group of the curve (see Fig. 1 for the lattice of automorphism groups in genus 3). In Section 3.2, we find equations for all the strata and show how to reconstruct a curve with given invariants. These two questions are indeed intertwined.

Starting from normal models as in Fig. 1, we get necessary algebraic conditions for the invariants to define a curve with a certain automorphism group. We determine these equations by evaluations and interpolations, the same approach as the one we followed for finding the expressions of the coefficients of $\mathcal{Q}$ and $\mathcal{H}$. We were able to obtain equations for all the strata, even for the dimension 3 stratum $(\mathbb{Z}/2\mathbb{Z})^2$. In order to check that these conditions are also sufficient, we reconstruct a curve from given invariants and check that its Shioda invariants are equal to the original ones. This last step involves calculations in the quotient ring of $\mathbb{Q}[J_2, \ldots, J_{10}]$ by the ideal defined by the stratum equations. Even if modern computational algebra software can handle them, keeping polynomials reduced to normal forms modulo the ideal of relations yields several hours of computations on a powerful computer, at least for the strata of dimension 2 or 3.

The reconstruction step for most strata is carried out by 'inverting' the expressions of the invariants in terms of the parameters of normal models modulo the stratum equations. For strata of dimension less or equal to 1, we give models whose coefficients are rational expressions in terms of the invariants. For the dimension 2 stratum with automorphism group $(\mathbb{Z}/2\mathbb{Z})^3$, we can still work out these computations at the price of a 'cubic extension' (see Lemma 3.8). For the dimension 2 stratum $\mathbb{Z}/4\mathbb{Z}$, we exhibit 5 conics among which at least one is always non-singular and use Mestre's method for this stratum. The dimension 3 stratum $(\mathbb{Z}/2\mathbb{Z})^2$ is more challenging. One can show (Lemma 3.2) that *any* choice of 3 covariants in the set of the 14 fundamental covariants of order 2 (364 possibilities) leads to a singular conic, hence Cardona and Quer's patch is not possible for curves in this stratum. Our computational approach yields, in addition to a set of 24 necessary equations for the invariants to define a curve with automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$, an explicit reconstruction at the price here of a 'degree 8 extension' (Lemma 3.10). We noticed furthermore that the singularity of the 364 conics is equivalent to the nullity of only 19 determinants. Obviously, the locus where these determinants simultaneously vanish contains the stratum $(\mathbb{Z}/2\mathbb{Z})^2$. We show that it is actually *equal*. As a by-product, the reconstruction of curves with no extra-automorphisms can therefore be achieved thanks to Mestre's method by picking one of the non-singular conics $\mathcal{Q}$ among the 19 fixed ones.

So far we have avoided arithmetic issues by working over an algebraically closed field but new challenging and deep issues arrive when one considers over which 'minimal field' these constructions can be achieved. Assume for simplicity that k is a field of characteristic 0 and let C be a curve defined over k (see a more general framework in Section 4.1). One can consider the intersection of all the subfields k' of $K = \bar{k}$ over which there exists a curve K-isomorphic to C (k' is called a *field of definition*). This field is called the *field of moduli* and denoted $\mathbf{M}_C$. If it is a field of definition, it is the smallest field of definition of C. This is not always the case when the curve has non-trivial automorphism group. Therefore hyperelliptic curves are

[1] As pointed out to us by the referee, the published version of the *loc. cit.* paper uses dihedral invariants instead of a different choice of covariants. In our paper, we therefore always refer to the arXiv version.

highly concerned with this issue: when is $\mathbf{M}_C$ a field of definition? Among the first results, in characteristic 0, Shimura [46] showed that it is not the case for a generic hyperelliptic curve of even genus. On top of this, hyperelliptic curves lead to a refined question that we want to address too. Let remember that, in full generality, a hyperelliptic curve C/k is a curve with a degree 2 morphism from C to a non-singular plane conic Q. If Q has a point and, assuming the characteristic of k not 2, one can write $C/k : y^2 = f(x)$ with $f \in k[x]$. We say that C can be *hyperelliptically defined over* k or that C admits a *hyperelliptic equation over* k. This is obviously the case if k is algebraically closed or finite (and therefore people often use this property as a definition) but when k is arbitrary, there might be again an obstruction.

For even genus, Mestre showed that the two questions are equivalent. For curves C of genus 2, in the case where C has no extra-automorphism, he showed that $\mathbf{M}_C$ is a field of definition if and only if the conic $\mathcal{Q}$ constructed from the covariants has a rational point. When C has extra-automorphisms, Cardona and Quer were able to exhibit hyperelliptic equations over $\mathbf{M}_C$. We implemented and completed their results for fields of characteristic 2, 3 and 5 [32].

For $g = 3$, we address both questions, from a theoretical and computational point of view. Let us give some of the results that we have obtained according to the stratification of the moduli space by the automorphism groups (see Section 4.5).

- For dimension 0 and dimension 1 strata, since $\mathrm{Aut}(C)/\langle\iota\rangle$ is not cyclic, Huggins' results in [28] show that there is a hyperelliptic equation over $\mathbf{M}_C$. This is confirmed and made explicit by the computations we performed for the reconstruction. In theses cases we can even exhibit parameterized models over $\mathbf{M}_C$.
- The dimension 2 case $\mathrm{Aut}(C) \simeq (\mathbb{Z}/2\mathbb{Z})^3$ is theoretically covered by [28] and therefore there exists a hyperelliptic equation over $\mathbf{M}_C$ (see Remark 4.15 for the controversy on this subject). In the present article, however we only reconstruct the curve hyperelliptically over at most a cubic extension of $\mathbf{M}_C$. There is a real difficulty to perform an explicit descent over $\mathbf{M}_C$ as geometric isomorphisms between our curve and a model over $\mathbf{M}_C$ might be defined over a degree 24 extension of $\mathbf{M}_C$. In [35], we work out an algorithm based on covariants to obtain a model over $\mathbf{M}_C$.
- The dimension 2 case $\mathrm{Aut}(C) \simeq \mathbb{Z}/4\mathbb{Z}$ is not covered by the general result of [28]. However using the special form of the ramification signature, we can show that C can always be hyperelliptically defined over $\mathbf{M}_C$. To make this result explicit, we use the fact that there is always a non-singular conic $\mathcal{Q}$. Although this conic has not necessarily a rational point, we can make use of the special shapes of $\mathcal{Q}$ and $\mathcal{H}$ to perform an explicit hyperelliptic descent.
- For the dimension 3 case $\mathrm{Aut}(C) \simeq (\mathbb{Z}/2\mathbb{Z})^2$, Huggins constructed examples of genus 3 curves over $\overline{\mathbb{Q}}$ which cannot be defined over their field of moduli. Hence, we did not explore this case further in this paper and our reconstruction takes place over a degree 8 extension at most. But in a forthcoming article [34], we exhibit an easy criterion to check whether a curve can be defined over $\mathbf{M}_C$, and when this the case, we can determine the descent in an efficient way.
- Finally, for the dimension 5 case $\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z}$, we show that $\mathbf{M}_C$ is always a field of definition. This is more generally true for hyperelliptic curves with no extra-automorphisms of odd genus. However, now C has not automatically a hyperelliptic model over $\mathbf{M}_C$. In genus 3, we show that C has a hyperelliptic equation over $\mathbf{M}_C$ if and only if one (equivalently, all of the) non-singular conic $\mathcal{Q}$ has a rational point over $\mathbf{M}_C$. As we proved that such a conic always exists, the method is explicit as well. This is the same situation as for genus 2 and we wonder whether one may get a theoretical proof of such a result for any genus.

With a view to applications over finite fields, we want hyperelliptic equations over $\mathbf{M}_C$ in all cases. On one hand, the task is made easier as there is never any obstruction for the curve to have a hyperelliptic equation over its field of moduli and we propose an algorithm which makes the reconstruction over $\mathbf{M}_C$ effective. Moreover, starting from the rational parameterizations that we exhibit for most of the strata, we can state the exact number of isomorphism classes of rational curves with a given automorphism group, except for the dimension 3 stratum $\mathrm{Aut}(C) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. On the other hand, as already illustrated by the genus 2 case, strange phenomenon can happen when the characteristic p is too small. This is not so surprising as the stratification itself may be different when $p \leq 2g+1$. We took special care of denominators when computing

invariants and covariants and our results are then naturally valid for $p > 7 = 2 \cdot 3 + 1$. We wonder whether the natural bound $p > 2g + 1$ may be reached in this way for general g.

Finally, this article is only the emerged part of the iceberg. A MAGMA code[2] containing the various algorithms to check our computational assertions, calculate invariants and reconstruct curves is available on the web page of the authors. We tested it over $\mathbb{F}_p$ for $11 \leq p \leq 47$ and checked that we actually obtain the p^5 non-isomorphic curves predicted by the theory. This code includes the computation of twists to obtain a representative of each $\mathbb{F}_q$-isomorphism class, as we did for genus 2 and we checked that we obtain the number of twists predicted by Nart too [41].

Notations and conventions. In the following, the integer p is a prime or 0, k denotes any field of characteristic p and K an algebraically closed field of characteristic p. For an integer g, a *hyperelliptic curve* or a *genus g curve* C over a field k is always assumed to be smooth, projective and absolutely irreducible (if it is given by a singular equation, typically the case for hyperelliptic curves, C is the smooth model associated to this equation). However a 'curve' (like a conic) may be singular. When we speak of a morphism from C to C' we always mean a morphism *defined over k*. However the notation $\mathrm{Aut}(C)$ stands for $\mathrm{Aut}_{\bar{k}}(C)$. To shorten the article, certain equations, denoted with roman numerals instead of arabic ones, have been moved to a supplementary file available on the web page of the authors or online alongside the electronic version of this article [33].

Acknowledgments. This paper has benefit from plenty of discussions with several mathematicians. During the Huggins / Fuertes-González-Diez controversy, the authors wish to thank the help and patient listening of Nils Bruin, Pierre Dèbes, Yolanda Fuertes, Gabino González-Diez, Ruben Hidalgo, Everett Howe, Bonnie Huggins, David Kohel, Stéphane Louboutin, Enric Nart, Xavier Xarles and finally Alexey Zykin who had the sharpest eye. Proposition 4.13 has been suggested to us by Nils Bruin. We thank Jean-Marc Couveignes for indicating to us the reference [15] which leads to Proposition 4.3 and Jean-François Mestre for the precise reference to [13]. Also, we warmly thank the anonymous referee for carefully reading this work and for suggestions.

1. Invariants and symbolic computations

1.1. **Algebra of invariants and covariants.** Let k be an infinite field of characteristic p and $n > 1$ be an integer. Let $V = k^2$ be the k-vector space with basis (x, z) and let $S^n(V)$ be the $(n+1)$-dimensional vector space of homogeneous forms $\sum_{i=0}^{n} a_i x^i z^{n-i}$ of degree n in (x, z). In the sequel, we call an element of $S^n(V)$ a *(binary) form*. When $n = 0$, we let $S^0(V) = k$. Let $G \subset \mathrm{GL}_2(k)$ and let $M \in G$. If a form $f \in S^n(V)$ then $M.f$ is defined by $(M.f)(x, z) = f(M^{-1}(x, z))$, where the action of a matrix on (x, z) is the standard action on ${}^t(x, z)$.

Definition 1.1. Let $r \geq 0$ be an integer and $(n_1, \ldots, n_m)$ be positive integers. A multi-homogeneous polynomial function $C : \bigoplus S^{n_i}(V) \to S^r(V)$ of multi-degree $(d_1, \ldots, d_m)$ is a *covariant* if there exists $\omega \in \mathbb{Z}$ such that for all $M \in G$ and all $(f_1, \ldots, f_m) \in \bigoplus S^{n_i}(V)$, we have

$$C(M.f_1, \ldots, M.f_m) = \det(M)^{-\omega} \cdot M.C(f_1, \ldots, f_m)\,.$$

When $r = 0$, such a C is called a (relative) *invariant* and denoted by I.

The integer r is called the *order* of a covariant. If $nd - r$ is odd, then a covariant is necessarily zero. Otherwise the integer ω is unique and called the *weight*. It is equal to $(nd - r)/2$. In the sequel, we often identify C with $C(f)$ for a general form $f \in F(a_0, \ldots, a_n)[x, z]$ where F is the prime field of k. For instance, the identity function $S^n(V) \to S^n(V)$ is a covariant of degree 1 and of order n equal to f.

The major operation to generate new covariants from given ones is the transvectant. For i, j two distinct integers, let (x_i, z_i) and (x_j, z_j) be bases of two copies V_i and V_j of V. Let Ω_{ij} be the differential operator

$$\Omega_{ij} = \frac{\partial}{\partial x_i}\frac{\partial}{\partial z_j} - \frac{\partial}{\partial z_i}\frac{\partial}{\partial x_j}.$$

Let $r_i, r_j > 0$ be integers, $f_i \in S^{r_i}(V) = S^{r_i}(V_i)$ and $f_j \in S^{r_j}(V) = S^{r_j}(V_j)$. We define the following differential operators (where composition is denoted multiplicatively).

[2] Published under the GNU Lesser General Public License

Definition 1.2. The *h-th transvectant* $(\ ,\ )_h : S^{r_i}(V) \times S^{r_j}(V) \to S^{r_i+r_j-2h}(V)$ is defined by

$$(f_i, f_j)_h = \frac{(r_i-h)!\ (r_j-h)!}{r_i!\ r_j!} \cdot \left(\Omega_{ij}^h(f_i(x_i,z_i)\cdot f_j(x_j,z_j))\right)_{(x_i,z_i)=(x_j,z_j)=(x,z)}.$$

The h-th transvectant of two covariants of degree d_1, d_2 and of order r_1, r_2 is a covariant of degree d_1+d_2 and of order r_1+r_2-2h (see [42, Chap. 15] for a conceptual explanation).

We focus on invariants and covariants for $G = \mathrm{GL}_2(K)$ and $G = \mathrm{SL}_2(K)$. The determinant factor prevents to add covariants of different weights when $G = \mathrm{GL}_2(K)$. Hence one generally studies the graded algebra $\mathcal{C}_n$ of covariants and $\mathcal{I}_n$ of invariants under the action of $\mathrm{SL}_2(K)$. It is easy to see that the homogeneous elements of $\mathcal{C}_n$ and $\mathcal{I}_n$ are actually all the covariants or invariants under the action of $\mathrm{GL}_2(K)$. Since Gordan [24], it is known that $\mathcal{I}_n$ and $\mathcal{C}_n$ are finitely generated. Thanks to the so-called Clebsch-Gordan formula, one can even prove that $\mathcal{C}_n$ is generated by a finite number of iterations of transvectants starting from the single covariant f (see [25]). Effective computations of sets of generators when $K = \mathbb{C}$ have been worked out for n up to 10 (see [19, 49, 20, 2, 47, 16, 9, 8]). The case of octics, $n = 8$, which is the case we are interested in this article will be reviewed and developed in Section 1.4.

A classical result [39, p. 78],[19, p. 47] shows that the algebra $\mathcal{I}_n$ can separate the orbits of forms with no roots of multiplicity greater than or equal to $n/2$. In particular, two binary forms f, f' of even degree $n \geq 4$ with simple roots over K are in the same orbit under the action of $\mathrm{GL}_2(K)$ if and only if there exists $\lambda \in K$ such that for all i, $I_i(f) = \lambda^{d_i} \cdot I_i(f')$ for $\{I_i\}$ a finite set of homogeneous generators of degree d_i for $\mathcal{I}_n$.

1.2. **Hyperelliptic curves and invariants of binary forms.** Let k be a field of characteristic $p \neq 2$ and $K = \bar{k}$. A curve C of genus $g \geq 2$ defined over k is called *hyperelliptic* if C/K allows a separable degree 2 map to $\mathbb{P}^1_K$. The curve C then has a unique involution ι, called the *hyperelliptic involution*, such that $Q = C/\langle\iota\rangle$ is of genus 0. This involution is in the center of $\mathrm{Aut}(C)$. We call $\overline{\mathrm{Aut}}(C) = \mathrm{Aut}(C)/\langle\iota\rangle$ the *reduced automorphism group* of C.

If Q has a rational point, C is birationally equivalent to an affine curve of the form $y^2 = f(x)$ for a separable polynomial f of degree $2g+1$ or $2g+2$. We say that f is a *hyperelliptic polynomial* and that C has a *hyperelliptic equation* if a curve in the isomorphism class of C (over k) can be written in the form above. A hyperelliptic curve automatically has a hyperelliptic equation when k is algebraically closed or a finite field. However, as we shall see in Section 4.1 for more general fields and odd genus, it is not necessarily the case.

By homogenizing to weighted projective coordinates of weight $(1, g+1, 1)$, we obtain an equation $y^2 = f(x,z)$. Here f is seen as a form of degree $2g+2$, taking into account a 'root' at infinity when $\deg f = 2g+1$. With this convention, the roots of f are the ramification points W of the cover C/Q. We will use these conventions for the roots and degree in the sequel when we speak about a hyperelliptic polynomial or the associated form.

If f_1 and f_2 are hyperelliptic polynomials of even degree $2g+2 \geq 6$, then isomorphisms of hyperelliptic curves $y^2 = f_i(x,z)$ are represented by (M, e) with $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(k)$ and $e \in k^*$. To such a couple, one associates the isomorphism $(x, z, y) \mapsto (ax+bz, cx+dz, ey)$. The representation of an isomorphism is unique up to the equivalence $(M, e) \equiv (\lambda M, \lambda^{g+1} e)$ for $\lambda \in k^*$. If $k = K$ we can always assume $e = 1$ for the isomorphisms. Hence two hyperelliptic curves over K are isomorphic if and only if their hyperelliptic polynomials are $\mathrm{GL}_2(K)$-equivalent.

Proposition 1.3. *Let $\{I_i\}$ be a set of homogeneous generators of degree d_i for $\mathcal{I}_{2g+2}$. Two hyperelliptic curves $C : y^2 = f(x)$ and $C' : y^2 = f'(x)$ of genus g are K-isomorphic if and only if there exists $\lambda \in K^*$ such that $I_i(f') = \lambda^{d_i} \cdot I_i(f)$ for all i.*

Hence, the possible values of a set of generators for $\mathcal{I}_{2g+2}$ up to this specific equivalence are in bijection with the points of the coarse moduli space H_g of hyperelliptic curves of genus g. We therefore need algorithms to handle such 'weighted sets'.

1.3. **Algorithms in weighted projective spaces.** In the context of curves of genus 1 or 2, one usually prefers to handle absolute invariants instead of homogeneous ones, by calculating ratios of homogeneous

invariants of the same degree. In this way, one gets rid of the constant λ in Proposition 1.3. It becomes then easy to span the coarse moduli space or to check that two curves are isomorphic.

But, care has to be taken to ensure that the denominators of absolute invariants do not vanish for some hyperelliptic orbits and a common approach is to choose as denominator some powers of the discriminant invariant. We give up this strategy for higher genus curves, because the degree of the discriminant is too large (this degree is already equal to 14 for octics) and selecting invariants of smaller degree as denominators yields too many technical cases to consider. We choose instead to work with a (kind of) weighted projective space, given by m-uples $(I_1 : I_2 : \ldots : I_m)$ of weights d_1, d_2, $\ldots$, d_m.

Definition 1.4. Let k be a field and $d_1, \ldots, d_m$ positive integers wit $m \geq 2$. We call $\mathbb{W}$ a *weighted projective space* over k of dimension $m-1$ and weights $(d_1, \ldots, d_m)$ the set of elements denoted $(\iota_1 : \ldots : \iota_m)$ which are equivalence classes of m-uples $(\iota_1, \ldots, \iota_m) \in k^m \setminus (0, \ldots, 0)$ for the relation

$$(\iota_1, \ldots, \iota_m) \sim (\iota'_1, \ldots, \iota'_m) \iff \exists\, \lambda \in \bar{k}^* \text{ such that } \iota_j = \lambda^{d_j} \cdot \iota'_j \; \forall\, 1 \leq j \leq m.$$

As a first tool, we need an algorithm for testing the equality of two points in a weighted projective space.

Proposition 1.5. *Let k be a field and $\mathbb{W}$ a k-weighted projective space of dimension $m-1$ and weights $(d_1, d_2, \ldots, d_m)$, then Algorithm 1 tests if two elements of k^m are in the same class of $\mathbb{W}$.*

If k is a field which admits operations with quasi-linear complexity in time and space (multiplications, inverses, tests), then Algorithm 1 has quasi-linear complexity in time and space.

Algorithm 1: Equality in a weighted projective space.

Input : Two elements $(U_1, U_2, \ldots, U_m)$ and $(V_1, V_2, \ldots, V_m)$ in k^m and $\mathbb{W}$ a k-weighted projective space of dimension m with weights $(d_1, d_2, \ldots, d_m)$.

Output: The boolean "`true`" if $(U_1 : U_2 : \ldots : U_m) = (V_1 : V_2 : \ldots : V_m)$, "`false`" otherwise.

$\mathcal{S}_U \leftarrow \{i \in \{1, \ldots, m\}$ `s.t.` $U_i \neq 0\}$; $\mathcal{S}_V \leftarrow \{i \in \{1, \ldots, m\}$ `s.t.` $V_i \neq 0\}$;
if $\mathcal{S}_U \neq \mathcal{S}_V$ **then**
  return `false`
d, $(c_i : i \in \mathcal{S}_U) \leftarrow$ `ExtendedGCD`$(d_i : i \in \mathcal{S}_U)$;
$\Lambda \leftarrow \prod_{i \in \mathcal{S}_U} (V_i/U_i)^{c_i}$;
return `true` *if* $V_i/U_i = \Lambda^{d_i/d}$ *for all* $i \in \mathcal{S}_U$, `false` *otherwise.*

Proof. If $(U_1, U_2, \ldots, U_m)$ and $(V_1, V_2, \ldots, V_m)$ are in the same class of $\mathbb{W}$, then there exists some $\lambda \in \bar{k}^*$ such that $V_i = \lambda^{d_i} \cdot U_i$ for all i. So, Λ is equal to $\prod (V_i/U_i)^{c_i} = \lambda^{\sum c_i d_i} = \lambda^d$, and thus we have $V_i/U_i = \Lambda^{d_i/d} = \lambda^{d_i}$ for $i \in \mathcal{S}_U$. Conversely, if $\mathcal{S}_U = \mathcal{S}_V$ and $V_i/U_i = \Lambda^{d_i/d}$ for $i \in \mathcal{S}_U$, then let λ be a d-th root of Λ in $\bar{k}^*$ and we can easily check that $V_i = \lambda^{d_i} \cdot U_i$. □

We deduce from Algorithm 1 how to associate to a class $(U_1 : U_2 : \ldots : U_m)$ a unique vector of k^m representing the class. Let $\mathcal{S}_U$ be the support of U, *i.e.* $\mathcal{S}_U = \{i \in \{1, \ldots, m\}$ s.t. $U_i \neq 0\}$, let c_i be integers such that $\sum_{i \in \mathcal{S}_U} c_i d_i = d$ with $d = \gcd(d_i : i \in \mathcal{S}_U)$ and let $\Lambda = \prod_{i \in \mathcal{S}_U} U_i^{c_i}$. Set $u_i = U_i/\Lambda^{d_i/d}$ for $i \in \mathcal{S}_U$ and $u_i = 0$ otherwise. Then $(u_1, u_2, \ldots, u_m)$ is the unique representative of $(U_1 : U_2 : \ldots : U_m)$ such that $\prod_{i \in \mathcal{S}_U} u_i^{c_i} = 1$.

When k is a finite field, enumerating elements in $\mathbb{W}$ is another feature that is needed to span $\mathsf{H}_g(k)$. In weighted projective spaces, this can be easily done by enumerating representatives. Typically, for each support $\mathcal{S}_U$, considered in turn, fix, for once, integers c_i such that $\sum_{i \in \mathcal{S}_U} c_i d_i = \gcd(d_i : i \in \mathcal{S}_U)$. Then enumerate all the vectors $(u_1, u_2, \ldots, u_m)$ of k^m with support $\mathcal{S}_U$ such that $\prod_{i \in \mathcal{S}_U} u_i^{c_i} = 1$.

Example 1.6. Let $k = \mathbb{F}_7$ and $\mathbb{W}$ be a k-weighted projective space of dimension 2 and weights (5, 7). To enumerate elements in $\mathbb{W}$, we consider supports in turn. The supports $\mathcal{S} = \{1\}$ and $\mathcal{S} = \{2\}$ yield the classes $(1 : 0)$ and $(0 : 1)$. Let us now consider the support $\mathcal{S} = \{1, 2\}$. We fix $c_1 = 3$, $c_2 = -2$, so that $5c_1 + 7c_2 = \gcd(5, 7)$. This yields 6 representatives $(U_1 : U_2)$ such that $\prod_{i=1,2} U_i^{c_i} = 1$, that is $(1 : 1)$, $(1 : 6)$, $(2 : 1)$, $(2 : 6)$, $(4 : 1)$, $(4 : 6)$. Another choice of c_1 and c_2 would lead to different representatives: for instance $c_1 = 24$ and $c_2 = -17$ gives $(1 : i)$ for $1 \leq i \leq 6$.

Finally, enumerating points on a coarse moduli space can be translated into enumerating points on a variety defined inside a weighted projective space. This is much more intricate than enumerating the full space, at least for curves of genus larger than 2. A naive strategy consists in enumerating all the points in the ambient space and for each point check if it is defined on the projective moduli variety. It is often inefficient. More sophisticated methods may be possible, based on a nice description of the variety, especially when the variety is rational and one has an explicit parameterization for it. In this direction, we give in Section 1.4 an efficient method for the moduli space of genus 3 hyperelliptic curves.

1.4. **Fundamental invariants and covariants for the binary octics.** According to the syzygy theorem of Hilbert, the graded ring $\mathcal{I}_8$ of invariants of binary octics fits into a finite exact sequence of $\mathbb{C}[\mathsf{X}]$-module where $\mathbb{C}[\mathsf{X}] := \mathbb{C}[X_2, \ldots, X_{10}]$. In what Mumford called a 'tour de force', Shioda managed to find an explicit description.

Theorem 1.7 ([47], Th. 3, p. 1042)**.** *The graded ring $\mathcal{I}_8$ of invariants of binary octics is generated by 9 elements J_2, J_3, …, J_{10} of degree 2, 3, …, 10. There exist 5 generating relations, $\mathfrak{R}_i(J)$, of degree $15+i$, $(i=1,\ldots,5)$, which, in turn, are connected by 5 fundamental first syzygies $\mathfrak{T}_i(R)$ of degree $24+i$, $(i=1,\ldots,5)$. The second syzygy $\mathfrak{F}$ is unique up to constants and of degree 45. The syzygy sequence of $\mathcal{I}_8$ (as $\mathbb{C}[\mathsf{X}]$-module) is given by*

$$0 \to \mathbb{C}[\mathsf{X}]\mathfrak{F} \to \sum_{i=1}^{5} \mathbb{C}[\mathsf{X}]\mathfrak{T}_i \to \sum_{i=1}^{5} \mathbb{C}[\mathsf{X}]\mathfrak{R}_i \to \mathbb{C}[\mathsf{X}] \to \mathcal{I}_8 \to 0\,.$$

Using transvectants and the covariant f, Shioda defined the invariants J_i's of Theorem 1.7 as follows,

$$J_2 = (f,f)_8,\ J_3 = (f,\mathfrak{g})_8,\ J_4 = (\mathfrak{k},\mathfrak{k})_4,\ J_5 = (\mathfrak{m},\mathfrak{k})_4,\ J_6 = (\mathfrak{k},\mathfrak{h})_4,$$
$$J_7 = (\mathfrak{m},\mathfrak{h})_4, J_8 = (\mathfrak{p},\mathfrak{h})_4,\ J_9 = (\mathfrak{n},\mathfrak{h})_4,\ J_{10} = (\mathfrak{q},\mathfrak{h})_4$$

where

$$\mathfrak{g} = (f,f)_4,\ \mathfrak{k} = (f,f)_6,\ \mathfrak{h} = (\mathfrak{k},\mathfrak{k})_2,\ \mathfrak{m} = (f,\mathfrak{k})_4,\ \mathfrak{n} = (f,\mathfrak{h})_4,\ \mathfrak{p} = (\mathfrak{g},\mathfrak{k})_4,\ \mathfrak{q} = (\mathfrak{g},\mathfrak{h})_4\,.$$

We found for a generic form $f = a_8x^8 + a_7x^7 + \ldots + a_0$,

$$\begin{aligned} J_2 &= 1/140\,(280\,a_0\,a_8 - 35\,a_1\,a_7 + 10\,a_2\,a_6 - 5\,a_3\,a_5 + 2\,a_4^2)\,,\\ J_3 &= 1/137200\,(11760\,a_0\,a_4\,a_8 - 7350\,a_0\,a_5\,a_7 + 3150\,a_0\,a_6^2 - 7350\,a_1\,a_3\,a_8 + 2205\,a_1\,a_4\,a_7 - 525\,a_1\,a_5\,a_6 +\\ &\qquad 3150\,a_2^2a_8 - 525\,a_2\,a_3\,a_7 - 330\,a_2\,a_4\,a_6 + 225\,a_2\,a_5^2 + 225\,a_3^2a_6 - 135\,a_3\,a_4\,a_5 + 36\,a_4^3)\,, \end{aligned}$$

etc.

The invariants $J_2, \ldots, J_7$ are algebraically independent (see [47, Lemma 4, p. 1037]). We have moreover 5 relations between J_8, J_9 and J_{10}, of the form

$$\begin{array}{lcl} \mathfrak{R}_1 & : & J_8^2 + A_6\,J_{10} + A_7\,J_9 + A_8\,J_8 + A_{16} = 0\\ \mathfrak{R}_2 & : & J_8\,J_9 + B_7\,J_{10} + B_8\,J_9 + B_9\,J_8 + B_{17} = 0\\ \mathfrak{R}_3 & : & J_8\,J_{10} + C_0\,J_9^2 + C_8\,J_{10} + C_9\,J_9 + C_{10}\,J_8 + C_{18} = 0\\ \mathfrak{R}_4 & : & J_9\,J_{10} + D_9\,J_{10} + D_{10}\,J_9 + D_{11}\,J_8 + D_{19} = 0\\ \mathfrak{R}_5 & : & J_{10}^2 + E_0\,J_2\,J_9^2 + E_{10}\,J_{10} + E_{11}\,J_9 + E_{12}\,J_8 + E_{20} = 0 \end{array} \qquad (1)$$

where the A_i's, B_i's, C_i's and D_i's are invariants of degree i, that can be explicitly determined as functions of J_2, J_3, …, J_7 (see [47, Th. 1, p. 1030]).

Generically, *i.e.* when $\theta = A_6\,J_8 + A_6\,B_8 - A_7\,B_7 \neq 0$, $\mathfrak{R}_1$ and $\mathfrak{R}_2$ yield

$$\begin{aligned} J_9 &= (B_7\,J_8^2 - A_6\,B_9\,J_8 - A_6\,B_{17} + B_7\,A_8\,J_8 + A_{16}\,B_7)/\theta\,,\\ J_{10} &= -(J_8^3 + J_8^2B_8 - A_7\,B_9\,J_8 - A_7\,B_{17} + A_8\,J_8^2 + A_8\,J_8\,B_8 + A_{16}\,J_8 + A_{16}\,B_8)/\theta\,. \end{aligned}$$

Following Shioda [47, p. 1043]), we may consider $\mathfrak{R}_1$,$\mathfrak{R}_2$, $\mathfrak{R}_3$ and $(J_9 - B_9)\mathfrak{R}_2 - B_7\mathfrak{R}_4$ as linear equations in 1, J_9, J_9^2 and J_{10} and we obtain that J_8 always satisfies an equation of degree 5, denoted Eq. (II) in the sequel. Moreover, the discriminant of f is an invariant Δ of degree 14, denoted Eq. (III) in the sequel and which can be easily expressed in terms of the J_i's.

Remark 1.8. Instead of $\mathcal{I}_8$, one may look at $\mathrm{Frac}(\mathcal{I}_8)$ and consider absolute invariants. It is known that $\mathrm{Frac}(\mathcal{I}_n)$ is a rational function field (see [3]) and in the case $n = 8$, Maeda worked out 6 algebraically independent absolute invariants [36, Th. B, p. 631] which generate $\mathrm{Frac}(\mathcal{I}_8)$. Unfortunately their degrees are too large for practical computations.

As we also want to work with finite fields, we need to show that Shioda's description of $\mathcal{I}_8$ is still valid. First note that it is easy to check that the J_i's and their relations are actually defined over $\mathbb{Z}[1/2, 1/3, 1/5, 1/7]$.

Proposition 1.9. *Assume that K is an algebraically closed field of characteristic > 7. Then $\mathcal{I}_8$ is generated by the reduction of the J_i's and they satisfy the reduction of the relations $\mathfrak{R}_i$.*

Proof. We simply follow Shioda's article [47]. First note that all the algebraic computations in the article are valid over any field of characteristic $\neq 2, 3, 5, 7$. Hence, Sections 1, 2 and 4 are still valid without any change. For Section 3, we use a beautiful article of Geyer [23] who proved that the algebra of invariants $\mathcal{I}_n$ over an algebraically closed field K of characteristic p is the reduction of $\mathcal{I}_n$ in characteristic 0 as soon as $p > n$. In particular, the generating series of $\mathcal{I}_8$ used in Section 3 is still valid. The crucial Lemmas 2 and 3 in Section 3 also hold for reductive group (which is the case of SL_n) as one can see in [18, p. 60]. To check Lemmas 4 and 5, it is then enough to do the following:

(1) Prove that $J_2, \ldots, J_{10}$ are zeros if and only if f is a form with a linear factor of multiplicity > 4. With the notation of the lemma, only case 3 –where Shioda uses an argument based on Gordan's proof– does not clearly hold in positive characteristic. In this case, one needs to prove that if $J_2 = \ldots = J_{10} = 0$ and $(f, f)_6 = 0$ then f is a form with a linear factor of multiplicity > 4. First we see that the discriminant Δ is zero so f as at least a double root that we can assume is 0. Hence we can take $f = a_7x^7 + \ldots + a_2x^2$. Working out Gröbner basis computations over $\mathbb{Z}$, we see that the equations $J_2 = J_3 = (f, f)_6 = 0$ imply $a_3 = a_4 = a_5 = 0$ and ($a_2 = 0$ or $a_7 = a_6 = 0$). The claim is proved.
(2) Once this is proved, Lemma 2 implies that $\mathrm{Frac}(\mathcal{I}_8)$ is a finite extension of $K(J_2, \ldots, J_{10})$. Since the generating series of these rings are the same as in characteristic 0, we see that the degree of the extension is still 5 and that the extension is separable. We hence get Lemmas 4 and 5 and therefore Theorem 2.

□

Now, following Section 1.3, we represent the coarse moduli space of genus 3 hyperelliptic curves by the projective variety given by Eq. (1) defined in a weighted projective space of dimension 9 with weights 2, 3,. . . , 10, the points of which are of the form $(J_2 : J_3 : \ldots : J_{10})$. In this setting, enumerating points on the moduli space over a finite field can be done as follows.

(1) Enumerate representatives for all the points of the weighted projective subspace of dimension 6 defined by the algebraically independent invariants J_2, J_3, $\ldots J_7$ (*cf.* Section 1.3).
(2) For each such representative, denoted $(j_2, j_3, \ldots, j_7)$, compute the gcd δ of its support $\{d : j_d \neq 0\}$.
(3) For each representative π of the quotient $k^*/(k^*)^\delta$ (we choose $\pi = 1$ when $\delta = 1$), compute the roots in J_8 of Eq. (II) specialized at $J_d = \pi^{(d/\delta)}\, j_d$ for $2 \leq d \leq 7$.
(4) For each root j_8, solve Eq. (1) in j_9 and j_{10}.
(5) Return representatives for $\{(\pi^{(2/\delta)}\, j_2 : \pi^{(3/\delta)}\, j_3 : \ldots : \pi^{(7/\delta)}\, j_7 : j_8 : j_9 : j_{10}) : \pi \in k^*/(k^*)^\delta\}$.

We consider in this algorithm several representatives $(\pi^{(2/\delta)}\, j_2 : \pi^{(3/\delta)}\, j_3 : \ldots : \pi^{(7/\delta)}\, j_7)$ starting from the same class $(j_2 : j_3 : \ldots : j_7)$ when $\delta \neq 1$, even if we may encounter several times the same class at the very end of the enumeration. We do so because such collisions are straightforward to filter, and otherwise we may miss points on the coarse moduli space.

For instance, modulo 11, the representative $j_2 = -1$, $j_3 = j_4 = j_5 = j_6 = j_7 = 0$ yields only one point in the moduli space, *i.e* (-1 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0), while another choice of representative for the class (-1 : 0 : . . . : 0), as for instance $j_2 = 1$, $j_3 = j_4 = j_5 = j_6 = j_7 = 0$, yields two points in the moduli space, among which the (new) point (1 : 0 : 0 : 0 : 0 : 0 : 8 : 2 : 7). This is mostly due to the fact that there exists equivalent representatives, here $(-1, 0, 0, 0, 0, 0)$ and $(1, 0, 0, 0, 0, 0)$, for some classes $(j_2 : j_3 : \ldots : j_7)$, here (-1 : 0 : 0 : 0 : 0 : 0), linked by a projective constant λ which may only be defined in a non-trivial extension of

$\mathbb{F}_{11}$ of degree δ (in the example $\delta = 2$). In this situation, specializing Eq. (1) with such representatives yield solutions which are no more necessarily equivalent.

Some of the classes encountered while enumerating may be specializations of Shioda invariants at forms f which do not have simple roots. These classes are not points of the coarse moduli space. To discriminate them, we may check that the discriminant Δ is non-zero for forms in the class $(j_2 : j_3 : \ \ldots : j_{10})$.

2. Reconstruction of binary forms

Let $n > 2$ be an even positive integer, k be a field of characteristic 0 or greater than n and $K = \bar{k}$.

2.1. **Clebsch's identities.** In the following section we recall the results contained in Example 3 of [38]. They are the fundamental tools to reconstruct a generic binary form of even degree n from its invariants as it is explained in *loc. cit.* and 2.2. The classical reference for this section is [13, § 103] where beautiful proofs are given using multi-linear algebra.

Let q_1, q_2, q_3, f be four quadratic forms over k. We denote

$$\begin{aligned} q_1^* = (q_2, q_3)_1, \qquad & q_2^* = (q_3, q_1)_1, \qquad q_3^* = (q_1, q_2)_1, \\ A_{ij} = (q_i, q_j)_2 \quad & \text{for } i, j \in \{1, 2, 3\}, \\ R(q_1, q_2, q_3) \quad & \text{the determinant of } q_1, q_2, q_3 \text{ in the basis } x^2, xz, z^2. \end{aligned}$$

One has the following relations.

$$q_1 q_1^* + q_2 q_2^* + q_3 q_3^* = 0\,, \tag{4}$$

$$2 \cdot \det((A_{ij})_{i,j=1,2,3}) = R^2(q_1, q_2, q_3)\,, \tag{5}$$

$$R(q_1, q_2, q_3) \cdot f = 2\left((f, q_1)_2 \cdot q_1^* + (f, q_2)_2 \cdot q_2^* + (f, q_3)_2 \cdot q_3^*\right)\,, \tag{6}$$

$$\sum_{i,j} A_{ij} \cdot q_i^* \cdot q_j^* = 0\,. \tag{7}$$

Note also that the constants in our formulas sometimes slightly differ from Mestre's. All these formulas can be checked by a computer algebra software. However the following result needs a proof which uses the following classical lemma.

Lemma 2.1 ([42, p. 565])**.** *For $1 \le i \le 2$, let r_i be positive integers, $\alpha_i, \beta_i \in k$ and $\ell_i = (\alpha_i x + \beta_i z)$. Then $(\ell_i^{r_i}, \ell_j^{r_j})_h = [\ell_i, \ell_j]^h \cdot \ell_i^{r_i - h} \ell_j^{r_j - h}$ where $[\ell_i, \ell_j] = \alpha_i \beta_j - \alpha_j \beta_i$.*

Proposition 2.2. *Let f be a binary form of even degree n. Then*

$$R(q_1, q_2, q_3)^{n/2} \cdot f(x, z) = \frac{1}{n!} \cdot \left(\sum_{i=1}^{3} q_i^*(x, z) \delta_i \right)^{n/2} f(x_1, z_1) \tag{8}$$

where δ_i is the differential operator $\phi(x_1, z_1) \mapsto \Omega_{12}^2(\phi(x_1, z_1) \cdot q_i(x_2, z_2))$.

Proof. As the right member is linear in f we can assume that $f = \ell^n = (\mu x_1 + \nu z_1)^n$. To make it linear in the q_i we consider $n/2$ triplets of quadratic forms (q_{1j}, q_{2j}, q_{3j}) and define accordingly

$$q_{1j}^* = (q_{2j}, q_{3j})_1, \quad q_{2j}^* = (q_{3j}, q_{1j})_1, \quad q_{3j}^* = (q_{1j}, q_{2j})_1.$$

We replace the previous operator by

$$\Psi := \frac{1}{n!} \cdot \prod_{j=1}^{n/2} \sum_{i=1}^{3} q_{ij}^*(x, z)\, \delta_{ij}$$

where $\delta_{ij}(\phi(x_1, z_1)) = \Omega_{12}^2(\phi(x_1, z_1) q_{ij}(x_2, z_2))$. As Ψ is linear in each q_{ij} we can assume that $q_{ij} = \ell_{ij}^2 = (\alpha_{ij} x + \beta_{ij} z)^2$. For $1 \le j \le n/2$, let $i_j \in \{1, 2, 3\}$. Observe that for all m

$$\delta_{i_j j}(\ell^m) = \Omega_{12}^2(\ell^m(x_1, z_1) q_{i_j j}(x_2, z_2)) = \frac{2!\ m!}{(m-2)!} \cdot [\ell, \ell_{i_j j}] \cdot \ell^{m-2}.$$

Hence

$$\frac{1}{n!}\left(\prod_{j=1}^{n/2}\delta_{i_jj}\right)(f)=\prod_{j=1}^{n/2}2[\ell,\ell_{i_jj}]^2=\prod_{j=1}^{n/2}2(\ell^2,q_{i_j,j})_2.$$

Therefore, if we develop the expression of Ψ, we can replace each product of the δ_{i_jj} operators on f by the right expression. Re-factoring the new expression, we get that

$$\Psi(f)=\prod_{j=1}^{n/2}2\sum_{i=1}^{3}q_{ij}^*\cdot(\ell^2,q_{ij})_2.$$

Using (6),

$$\Psi(f)=\prod_{j=1}^{n/2}\left(R(q_{1j},q_{2j},q_{3j})\cdot\ell^2\right)=\left(\prod_{j=1}^{n/2}R(q_{1j},q_{2j},q_{3j})\right)\cdot\ell^n.$$

To conclude, we let $q_{ij}=q_i$ for all j. □

2.2. **A generic reconstruction algorithm.** Starting from a weighted projective point $(\iota_1:\iota_2:\ldots)$ of values in k for a finite set of generators $\{I_i\}$ of $\mathcal{I}_{2g+2}$, we aim at recovering a hyperelliptic curve $C/K\ : y^2=f(x)$ such that $(\iota_1:\iota_2:\ldots)=(I_1(f):I_2(f):\ldots)$.

Inverting the polynomial system giving the invariants in terms of a generic polynomial f can be efficiently done only in very specific cases (see Section 3.2). However, Mestre explained in his Example 3 and Remark on p. 321 [38] how one can use (7) and (8) to recover a generic even degree n form f up to $\mathrm{GL}_2(K)$ equivalence from the ι's, taking advantage of the fact that the coefficients of these expressions as polynomials in the q_i^* are invariants. Practically, given values $(\iota_1:\iota_2:\ldots)$ defined in k, one proceeds as follows.

(1) Find a triple (q_1,q_2,q_3) of covariants of order 2 such that the expression of $R(q_1,q_2,q_3)$ as a polynomial in the I_i's evaluated at the ι_i's is non-zero;
(2) Compute the conic $\mathcal{Q}:\sum A_{ij}x_ix_j=0$ defined by the expression of the coefficients A_{ij} as polynomials in the I_i's evaluated at the ι_i's.
(3) Compute the degree $n/2$ curve $\mathcal{H}:\sum_I h_Ix_I=0$ defined by the expression of the coefficients h_I of the right member of (8) (seen as a polynomial in q_i^*) as polynomials in the I_i evaluated at the ι_i's.
(4) Then, the following proposition shows how to find f.

Proposition 2.3. *Let (q_1,q_2,q_3) be three covariants of order 2 of a binary form f of even degree n defined over k. If $R(q_1,q_2,q_3)\neq 0$, there is a K-isomorphism $\mathcal{Q}\to\mathbb{P}^1$ mapping the intersections points of $\mathcal{Q}\cap\mathcal{H}$ on the roots of $f(X,Z)$. Moreover, this isomorphism is defined at most over a quadratic extension of k and is defined over k as soon as $\mathcal{Q}$ has a k-rational point.*

It might happen that all possible $R(q_1,q_2,q_3)$ evaluated at the ι_i's are zero. Also, even if we know for theoretical reasons that the curve can be reconstructed over k, $\mathcal{Q}$ might have no rational point. Sections 3.2 and 4 will deal with these issues.

2.3. **Reconstruction in the hyperelliptic genus 3 case.** We have computed a system of fundamental generators for invariants and covariants of octics, using Gordan's algorithm. Results are given in Tab. 1. In this table, generators are all defined by the mean of transvectants of the form $(\prod_{d,r}C_{d,r},f)_h$ where we denote recursively by $C_{d,r}$ generators of degree d and order r given at the intersection of the row d and the column r of the table. When we have two or three generators of degree d and r, we denote them by $C'_{d,r}$ and $C''_{d,r}$. For instance, $C_{5,10}=(C_{4,8}\,,f)_3$, $C'_{5,10}=(C_{4,10}\,,f)_4$ and $C''_{5,10}=(C'_{4,10}\,,f)_4$. Covariants $C_{2,0}$, $C_{3,0}$, …, $C_{10,0}$ given in column 0 are invariants and so, they are related to Shioda invariants J_2, J_3, …, J_{10},

$$C_{2,0}=J_2\,,\ C_{3,0}=J_3\,,\ C_{4,0}=J_2^2/30-4\,J_4/35\,,\ C_{5,0}=3\,J_5/14\,,\ \textit{etc.}$$

Our main motivation for computing Tab. 1 is to determine fundamental covariants of order 2 which can be used as quadratic forms in Proposition 2.3 to reconstruct a generic binary octic from its Shioda invariants. As with Shioda invariants, we paid attention that none of the transvectant computations in Tab. 1 involves covariants of order greater than 10 (except the quadratic covariants of order 18, but it does not matter

Ord. Deg.	0	2	4	6	8	10	12	14	18	Tot
1	–	–	–	–	f	–	–	–	–	1
2	$(f,\, f)_8$	–	$(f,\, f)_6$	–	$(f,\, f)_4$	–	$(f,\, f)_2$	–	–	4
3	$(C_{2,8},\, f)_8$	–	$(C_{2,8},\, f)_6$	$(C_{2,8},\, f)_5$	$(C_{2,8},\, f)_4$	$(C_{2,8},\, f)_3$	$(C_{2,8},\, f)_2$	$(C_{2,8},\, f)_1$	$(C_{2,12},\, f)_1$	8
4	$(C_{3,8},\, f)_8$	–	$\begin{vmatrix} (C_{3,4},\, f)_4 \\ (C_{3,8},\, f)_6 \end{vmatrix}$	$(C_{3,4},\, f)_3$	$(C_{3,4},\, f)_2$	$\begin{vmatrix} (C_{3,4},\, f)_1 \\ (C_{3,8},\, f)_3 \end{vmatrix}$	$(C_{3,8},\, f)_2$	$(C_{3,8},\, f)_1$	$(C_{3,12},\, f)_1$	10
5	$(C_{4,8},\, f)_8$	$(C_{4,10},\, f)_8$	$\begin{vmatrix} (C_{4,10},\, f)_7 \\ (C_{4,8},\, f)_6 \end{vmatrix}$	$\begin{vmatrix} (C_{4,10},\, f)_6 \\ (C_{4,8},\, f)_5 \end{vmatrix}$	$(C_{4,10},\, f)_5$	$\begin{vmatrix} (C_{4,8},\, f)_3 \\ (C_{4,10},\, f)_4 \\ (C'_{4,10},\, f)_4 \end{vmatrix}$	–	$(C_{4,10},\, f)_2$	–	11
6	$(C_{3,4}\, C_{2,4},\, f)_8$	$(C_{5,8},\, f)_7$	$\begin{vmatrix} (C_{5,8},\, f)_6 \\ (C'_{5,4},\, f)_4 \end{vmatrix}$	$\begin{vmatrix} (C_{5,8},\, f)_5 \\ (C'_{5,4},\, f)_3 \\ (C'_{5,10},\, f)_6 \end{vmatrix}$	$(C'_{5,4},\, f)_2$	$(C'_{5,4},\, f)_1$	–	–	–	9
7	$(C_{2,4}\, C'_{4,4},\, f)_8$	$\begin{vmatrix} (C_{2,4}\, C_{4,6},\, f)_8 \\ (C''_{6,6},\, f)_6 \end{vmatrix}$	$\begin{vmatrix} (C_{2,4}\, C_{4,6},\, f)_7 \\ (C''_{6,6},\, f)_5 \end{vmatrix}$	$\begin{vmatrix} (C''_{6,6},\, f)_4 \\ (C_{6,2},\, f)_2 \\ (C_{2,4}\, C_{4,6},\, f)_6 \end{vmatrix}$	–	–	–	–	–	8
8	$(C_{3,4}\, C_{4,4},\, f)_8$	$\begin{vmatrix} (C_{2,8}\, C_{5,2},\, f)_8 \\ (C_{3,6}\, C_{4,4},\, f)_8 \end{vmatrix}$	$\begin{vmatrix} (C_{3,6}\, C_{4,4},\, f)_7 \\ (C_{3,4}\, C_{4,6},\, f)_7 \end{vmatrix}$	$\begin{vmatrix} (C_{3,6}\, C_{4,4},\, f)_6 \\ (C_{3,4}\, C_{4,6},\, f)_6 \end{vmatrix}$	–	–	–	–	–	7
9	$(C_{2,4}\, C_{6,4},\, f)_8$	$\begin{vmatrix} (C_{4,6}\, C'_{4,4},\, f)_8 \\ (C_{2,4}\, C_{6,4},\, f)_7 \\ (C_{2,4}\, C'_{6,6},\, f)_8 \end{vmatrix}$	$(C_{2,4}\, C_{6,4},\, f)_6$	–	–	–	–	–	–	5
10	$(C_{4,4}\, C'_{5,4},\, f)_8$	$\begin{vmatrix} (C'_{7,2}\, C_{2,4},\, f)_6 \\ (C_{4,6}\, C_{5,4},\, f)_8 \end{vmatrix}$	–	–	–	–	–	–	–	3
11	–	$\begin{vmatrix} (C'_{8,4}\, C_{2,4},\, f)_7 \\ (C'_{5,6}\, C'_{5,4},\, f)_8 \end{vmatrix}$	–	–	–	–	–	–	–	2
12	–	$(C'_{6,6}\, C'_{5,4},\, f)_8$	–	–	–	–	–	–	–	1
Tot	9	14	13	12	6	7	3	3	2	69

TABLE 1. Fundamental invariants and covariants for a binary form of degree 8

since these quadratic covariants are not useful to compute other invariants or covariants of order 2). These formulas are thus also valid, in addition to fields of characteristic 0, over any field of or characteristic greater or equal than 11.

The main computational difficulty in the reconstruction method of Section 2.2 is to write the invariants A_{ij} and h_I as polynomials in the J_i's, since their degree may be large (close to 40 in our cases). Writing them as a polynomial with 9 unknowns a_i's for a generic binary form $f = a_8x^8 + a_7x^7 + \ldots + a_0$ is hopeless. We follow instead a "black-box" approach.

Algorithm 2: Write an invariant as a polynomial in the J_i's.

Input : An invariant I of degree d (given as an evaluation program).
Output: A polynomial P in $\mathbb{Q}[J_2, \ldots, J_{10}]$ such that $I(f) = P(J_2(f), J_3(f), \ldots, J_{10}(f))$.

`// A basis for the polynomials of degree` d `in the weighted graded algebra` $\mathbb{Q}[J_2, J_3, \ldots, J_{10}]$

$\mathcal{B} \leftarrow \left[\prod_w J_w^{e_w} \text{ s.t. } \sum_w w\, e_w = d \right]$;

`// Choose at random` $\#\mathcal{B} + O(1)$ `octics over` $\mathbb{Q}$

$\mathcal{F} \leftarrow \left[a_8x^8 + \ldots + a_1x\,z^7 + a_0z^8 \text{ for } \#\mathcal{B} + O(1) \text{ random } 9\text{−uples } (a_0, a_1, \ldots, a_8) \text{ in } \mathbb{Q}^9 \right]$;

`// Evaluate the invariant` I `and the basis` $\mathcal{B}$ `at each form of` $\mathcal{F}$

for $i = 1$ **to** $\#\mathcal{F}$ **do**
    $V_i \leftarrow I(\mathcal{F}_i)$;
    for $j = 1$ **to** $\#\mathcal{B}$ **do**
        $M_{i,j} \leftarrow \mathcal{B}_j(\mathcal{F}_i)$

`// Invert the linear system defined by the matrix` M `and the vector` V

Find the vectors U such that $M \times U = V$;

return $\sum_i U_i\, \mathcal{B}_i$ for each U

More precisely, since invariants are computed through sequences of covariants which are the result of transvectant or differential operations, we represent a covariant no more by a formal expression in the a_i's but as an algorithm which performs the corresponding sequence of operations. If one inputs some generic form $f \in \mathbb{Q}[a_0, \ldots, a_8][x, z]$, such an algorithm returns the formal expression of the covariant as a multivariate homogeneous polynomial in the a_i's, x and z. But, if one inputs a form $f \in \mathbb{Q}[x, z]$, the algorithm returns the covariant as a homogeneous polynomial in $\mathbb{Q}[x, z]$, without the use of the formal expression in the a_i's. In other words, we consider that a covariant is given by an evaluation program. Note that it is immediate to determine the degree and the order of a covariant from the sequence of operations which compose its evaluation program.

Now coming back to the question of writing a homogeneous invariant as a polynomial in the J_i's, we propose to construct a basis $\mathcal{B} = \{ \prod_w J_w^{e_w} : \sum_w w\, e_w = d \}$ for the polynomials of degree d in the weighted graded algebra $\mathbb{Q}[J_2, J_3, \ldots, J_{10}]$ and we evaluate this basis (with some given evaluation programs for the J_i's), and I (given as an evaluation program too), at $\#\mathcal{B} + O(1)$ octics chosen at random over $\mathbb{Q}$. It remains to invert the corresponding linear system to find I as a polynomial in the J_i's. Algorithm 2 summarizes this method.

Remark 2.4. Working with $\mathbb{Q}[J_2, J_3, \ldots, J_{10}]$ instead of $\mathbb{Q}[a_0, a_1, \ldots, a_8]$ in Algorithm 2 makes a real difference in practice. For instance, an invariant of degree 20 yields a basis $\mathcal{B}$ with only 107 monomials. This must be compared to the 61731 monomials that otherwise we would have to deal with in the weighted projective points $(a_0 : a_1 : \ldots : a_8)$ where a_0, a_1, …, a_8 are of weight 0, 1, …, 8. Note that an invariant of degree d is of weight $4d$ in the last algebra. For instance, $J_2 = 2\,a_0\,a_8 - a_1\,a_7/4 + a_2\,a_6/14 - a_3\,a_5/28 + a_4^2/70$ is of degree 2 and weight 8.

Example 2.5. Consider the covariants of order 2 of smallest degree in Tab. 1, that is, $q_1 = C_{5,2}$, $q_2 = C_{6,2}$ and $q_3 = C_{7,2}$. A call to Algorithm 2 yields that $R = R(q_1, q_2, q_3)$ is equal, up to a constant, to

$$
\begin{aligned}
R = &-4937630140800\,J_9^2 + 6172588800000\,J_8\,J_{10} + 1016336160000\,J_6^3 - 1646487542700\,J_5\,J_6\,J_7 + 475344450\,J_5^2\,J_8 \\
&- 13778100\,J_4\,J_7^2 + 6154254741600\,J_4\,J_6\,J_8 + 2469123699840\,J_4\,J_5\,J_9 - 3175414824960\,J_4^2\,J_{10} - 1028718873000\,J_3\,J_7\,J_8 \\
&- 1555231104000\,J_3\,J_6\,J_9 + 514676332800\,J_3\,J_5\,J_{10} - 579162433500\,J_2\,J_8^2 + 231655788000\,J_2\,J_7\,J_9 + 47632860\,J_4^2\,J_5^2 \\
&- 201602675520\,J_4^3\,J_6 - 264617457390\,J_3\,J_4\,J_5\,J_6 + 529262244990\,J_3\,J_4^2\,J_7 + 4618063800\,J_3^2\,J_6^2 - 35210700\,J_3^2\,J_5\,J_7 \\
&- 228766979700\,J_3^2\,J_4\,J_8 + 38124172800\,J_3^3\,J_9 + 77149935135\,J_2\,J_5^2\,J_6 - 40603006080\,J_2\,J_4\,J_6^2 - 115812049185\,J_2\,J_4\,J_5\,J_7 \\
&- 330859026540\,J_2\,J_4^2\,J_8 + 145802916000\,J_2\,J_3\,J_6\,J_7 - 15715198800\,J_2\,J_3\,J_4\,J_9 + 42877447200\,J_2\,J_3^2\,J_{10} + 53596043550\,J_2^2\,J_7^2 \\
&- 145802916000\,J_2^2\,J_6\,J_8 - 53606606760\,J_2^2\,J_5\,J_9 + 137217628800\,J_2^2\,J_4\,J_{10} - 36737464140\,J_3^2\,J_4^3 - 7824600\,J_3^3\,J_4\,J_5 \\
&+ 11300902200\,J_3^4\,J_6 - 47249726760\,J_2\,J_4^4 - 12161979900\,J_2\,J_3\,J_4^2\,J_5 + 3344455740\,J_2\,J_3^2\,J_4\,J_6 + 1760535\,J_2^2\,J_4\,J_5^2 \\
&+ 25514097660\,J_2^2\,J_4^2\,J_6 - 153935460\,J_2^3\,J_6^2 + 1173690\,J_2^3\,J_5\,J_7 + 7625565990\,J_2^3\,J_4\,J_8 - 1270805760\,J_2^3\,J_3\,J_9 \\
&- 1429248240\,J_2^4\,J_{10} + 289800\,J_2\,J_3^4\,J_4 + 900887400\,J_2^2\,J_3^2\,J_4^2 + 2575261188\,J_2^3\,J_4^3 + 260820\,J_2^3\,J_3\,J_4\,J_5 \\
&- 753393480\,J_2^3\,J_3^2\,J_6 - 1114881858\,J_2^4\,J_4\,J_6 - 19320\,J_2^4\,J_3^2\,J_4 - 30029580\,J_2^5\,J_4^2 + 12556558\,J_2^6\,J_6 + 322\,J_2^7\,J_4\,.
\end{aligned}
$$

Similarly, we find that the equation of the conic, $\sum_{i,j} A_{ij}\,x_i x_j = 0$, is equal to

$$
\begin{aligned}
&(9217732608000\,J_{10} - 1422489600\,J_2^3\,J_4 + 1814283878400\,J_4\,J_6 - 384072192000\,J_3\,J_7 \\
&\quad + 42674688000\,J_3^2\,J_4 - 1152216576000\,J_5^2 + 212154163200\,J_2\,J_4^2 + 384072192000\,J_2\,J_8)\;x_1^2 + \\
&(-80015040000\,J_3^2\,J_5 + 2667168000\,J_2^2\,J_5 - 12002256000\,J_2^2\,J_7 + 288054144000\,J_2\,J_9 + 216040608000\,J_4\,J_7 \\
&\quad - 102019176000\,J_2\,J_4\,J_5 + 138883248000\,J_3\,J_4^2 - 48009024000\,J_5\,J_6 + 360067680000\,J_3\,J_8)\;x_1\,x_2 + \\
&(-12040358400\,J_2^2\,J_8 - 902039040\,J_2^3\,J_6 - 24768737280\,J_4^3 + 27061171200\,J_2^3\,J_6 + 18627840\,J_2^4\,J_4 - 424308326400\,J_2\,J_{10} \\
&\quad - 5482391040\,J_2^2\,J_4^2 - 43481733120\,J_2\,J_4\,J_6 + 216726451200\,J_5\,J_7 + 12040358400\,J_2\,J_3\,J_7 - 762657638400\,J_4\,J_8 \\
&\quad + 36121075200\,J_2\,J_5^2 + 135339724800\,J_3\,J_9 - 162570240000\,J_6^2 - 10516262400\,J_3\,J_4\,J_5 - 558835200\,J_2\,J_3^2\,J_4)\;x_1\,x_3 + \\
&(135025380000\,J_3\,J_9 + 55566000\,J_2^3\,J_6 - 15788682000\,J_2\,J_4\,J_6 + 2813028750\,J_2^2\,J_8 - 2813028750\,J_2\,J_3\,J_7 + 149333625\,J_2^4\,J_4 \\
&\quad + 8439086250\,J_3\,J_4\,J_5 - 151903552500\,J_4\,J_8 - 2509400250\,J_2^2\,J_4^2 \\
&\quad + 75951776250\,J_5\,J_7 - 1666980000\,J_2^3\,J_6 - 4480008750\,J_2\,J_3^2\,J_4 \\
&\quad + 92610000\,J_2^3\,J_3^2 - 1543500\,J_2^6 - 1389150000\,J_3^4 - 2893401000\,J_4^3 - 50009400000\,J_6^2 - 67512690000\,J_2\,J_{10})\;x_2^2 + \\
&(1434793500\,J_2^2\,J_4\,J_5 - 1629217800\,J_2\,J_3\,J_4^2 + 6460738200\,J_2\,J_5\,J_6 \\
&\quad + 365148000\,J_3^3\,J_4 - 41806800\,J_2^4\,J_5 - 12748654800\,J_3\,J_4\,J_6 \\
&\quad + 1254204000\,J_2\,J_3^2\,J_5 + 914457600\,J_2\,J_4\,J_7 - 12171600\,J_2^3\,J_3\,J_4 - 172254600\,J_2^3\,J_7 - 2400451200\,J_2^2\,J_9 - 714420000\,J_6\,J_7 \\
&\quad - 5643918000\,J_2\,J_3\,J_8 - 4445733600\,J_4^2\,J_5 + 14402707200\,J_4\,J_9 \\
&\quad + 10811556000\,J_3^2\,J_7 - 63440496000\,J_3\,J_{10} - 44365482000\,J_5\,J_8)\;x_2\,x_3 + \\
&(94363920\,J_2^3\,J_8 + 2592705024\,J_4^2\,J_6 - 32568480\,J_3^2\,J_4^2 + 57512\,J_2^5\,J_4 \\
&\quad - 283091760\,J_2^2\,J_5^2 + 4386130560\,J_2^2\,J_{10} - 1905120000\,J_6\,J_8 \\
&\quad - 40824000\,J_7^2 + 34895088\,J_2^3\,J_4^2 + 1886976000\,J_2\,J_6^2 - 10150479360\,J_5\,J_9 - 109801152\,J_2^2\,J_4\,J_6 + 23227223040\,J_4\,J_{10} \\
&\quad + 21819168\,J_2^4\,J_6 + 3110425920\,J_3\,J_5\,J_6 + 15630965280\,J_2\,J_4\,J_8 \\
&\quad + 164838240\,J_2\,J_3\,J_4\,J_5 + 635065920\,J_2\,J_4^3 - 3676609440\,J_3\,J_4\,J_7 \\
&\quad - 1725360\,J_2^2\,J_3^2\,J_4 - 3397101120\,J_2\,J_5\,J_7 - 2121396480\,J_2\,J_3\,J_9 - 94363920\,J_2^2\,J_3\,J_7 - 654575040\,J_2\,J_3^2\,J_6)\;x_3^2 = 0\,.
\end{aligned}
$$

The beginning of the quartic $\sum_{i,j,k,l} h_{i,j,k,l} x_i x_j x_k x_l$ (its coefficients are too large to be all written here) is then

$$
\begin{aligned}
&(20832487200\,J_7^3 - 98761420800\,J_6\,J_7\,J_8 - 14814213120\,J_6^2\,J_9 + 140619288600\,J_5\,J_8^2 \\
&\quad + 21526903440\,J_5\,J_7\,J_9 + 192584770560\,J_4\,J_8\,J_9 - 29628426240\,J_3\,J_9^2 \\
&\quad + 6351593875200000\,J_2\,J_9\,J_{10} - 231472080\,J_5^3\,J_6 + 17310682368\,J_4\,J_5\,J_6^2 - 24651776520\,J_4\,J_5^2\,J_7 \\
&\cdots \\
&+ 653457959280\,J_2^5\,J_5\,J_6 - 653460684660\,J_2^5\,J_4\,J_7 + 108909756900\,J_2^6\,J_9 + 47040\,J_2^4\,J_3^3\,J_4 + 56723695560\,J_2^5\,J_3\,J_4^2 \\
&\quad + 141120\,J_2^5\,J_3^2\,J_5 + 222264\,J_2^6\,J_4\,J_5 + 117600\,J_2^6\,J_3\,J_6 + 7056\,J_2^7\,J_7 - 784\,J_2^7\,J_3\,J_4 - 2352\,J_2^8\,J_5)\;x_1^4 + \cdots
\end{aligned}
$$

These precomputations done, let us look now for an octic f defined over $\mathbb{F}_{11}$ such that for instance $J_2 = 1$, $J_3 = J_4 = J_5 = J_6 = J_7 = 0$, $J_8 = 8$, $J_9 = 2$ and $J_{10} = 7$. We first check that $R \neq 0$ and that the conic equation is equal to

$$x_1\,x_2 + 3\,x_1\,x_3 + 6\,x_2^2 + x_2\,x_3 + 8\,x_3^2 = 0\,.$$

Then, since the point $(1:0:1)$ is on this conic, we have the parameterization

$$(x, z) \mapsto (8\,x^2 + 10\,x\,z + 6\,z^2 : 8\,x\,z + 9\,z^2 : x\,z + 6\,z^2)\,.$$

In this case, the quartic equation of $\mathcal{H}$ is equal to

$$
\begin{aligned}
&6\,x_1^4 + 5\,x_1^3\,x_2 + 9\,x_1^3\,x_3 + 5\,x_1^{*2}\,x_2^{*2} + x_1^2\,x_2\,x_3 + 7\,x_1^2\,x_3^2 + 8\,x_1\,x_2^3 \\
&\qquad + 10\,x_1\,x_2^2\,x_3 + 3\,x_1\,x_2\,x_3^2 + 3\,x_1\,x_3^3 + 7\,x_2^4 + 7\,x_2^3\,x_3 + 9\,x_2\,x_3^3 + 5\,x_3^4
\end{aligned}
$$

and we finally find that, up to a constant,

$$f(x, z) = 2\,x^8 + 7\,x^7\,z + 9\,x^6\,z^2 + 9\,x^5\,z^3 + 8\,x^4\,z^4 + 3\,x^3\,z^5 + 2\,x^2\,z^6 + 4\,x\,z^7 + 8\,z^8\,.$$

3. Automorphisms and strata of hyperelliptic genus 3 curves

In the sequel, K is an algebraically closed field of characteristic p where p is a prime or 0.

3.1. **Review on automorphism groups.** Let C be a hyperelliptic curve of genus $g \geq 2$ over K and ι be its hyperelliptic involution. We say that C has *extra-automorphism* when $\#\overline{\mathrm{Aut}}(C) > 1$. The reduced automorphism group acts on $C/\langle\iota\rangle \simeq \mathbb{P}^1$. The list of possible finite groups $\overline{\mathcal{G}}$ acting on $\mathbb{P}^1$ was given in [50, 71-74]. In his PhD thesis, Brandt [5] gave the full list of polynomial orbits under any $\overline{\mathcal{G}}$ which in turn gives the *normal models* of hyperelliptic curves whose automorphism group contains a group $\mathcal{G}$ such that $\mathcal{G}/\langle\iota\rangle = \overline{\mathcal{G}}$. The structure of $\mathcal{G}$ itself then depends on the behavior of the exact sequence

$$1 \to \langle\iota\rangle \to \mathcal{G} \to \overline{\mathcal{G}} \to 1$$

which is measured by $H^2(\overline{\mathcal{G}}, \mathbb{Z}/2\mathbb{Z})$. When $p = 0$, the structure of $\mathcal{G}$, depending on its signature, has then been worked out in [6]. Finally among the groups $\overline{\mathcal{G}}$, one has to determine the ones which appear as automorphism group of C, and not only as subgroups. When $p = 0$, this can be done using Fuchsian groups [48], Teichmüller theory [43] or Hurwitz spaces [37].

For $g = 2$, a complete list of automorphism groups and models can be found in [12] for $p \neq 2$ and in [10] for $p = 2$.

For $g = 3$ and $p = 0$, this work has been achieved explicitly in several papers. We refer to [37] (or [27]) for a historical viewpoint and we gather their results in Fig. 1 (see also Remark 3.1). Using the signature [37, Sec. 4] (or the shape of the equations), we can deduce the relations between the strata in the moduli space.

#	$\mathrm{Aut}(C)$	$\overline{\mathrm{Aut}}(C)$	signature	δ	equation $y^2 = f(x)$	Id.
1	$\mathbf{C}_2$	$\{1\}$	(2^8)	5	$x(x-1)(x^5+ax^4+bx^3+cx^2+dx+e)$	$(2,1)$
2	$\mathbf{D}_4$	$\mathbf{C}_2$	(2^6)	3	$\begin{cases} x^8+ax^6+bx^4+cx^2+1 & \text{or} \\ (x^2-1)(x^6+ax^4+bx^2+c) \end{cases}$	$(4,2)$
3	$\mathbf{C}_4$	$\mathbf{C}_2$	$(2^3,4^2)$	2	$x(x^2-1)(x^4+ax^2+b)$	$(4,1)$
4	$\mathbf{C}_2^3$	$\mathbf{D}_4$	(2^5)	2	$(x^4+ax^2+1)(x^4+bx^2+1)$	$(8,5)$
5	$\mathbf{C}_2 \times \mathbf{C}_4$	$\mathbf{D}_4$	$(2^2,4^2)$	1	$\begin{cases} (x^4-1)(x^4+ax^2+1) & \text{or} \\ x(x^2-1)(x^4+ax^2+1) \end{cases}$	$(8,2)$
6	$\mathbf{D}_{12}$	$\mathbf{D}_6$	$(2^3,6)$	1	$x(x^6+ax^3+1)$	$(12,4)$
7	$\mathbf{C}_2 \times \mathbf{D}_8$	$\mathbf{D}_8$	$(2^3,4)$	1	x^8+ax^4+1	$(16,11)$
8	$\mathbf{C}_{14}$	$\mathbf{C}_7$	$(2,7,14)$	0	x^7-1	$(14,2)$
9	$\mathbf{U}_6$	$\mathbf{D}_{12}$	$(2,4,12)$	0	$x(x^6-1)$	$(24,5)$
10	$\mathbf{V}_8$	$\mathbf{D}_{16}$	$(2,4,8)$	0	x^8-1	$(32,9)$
11	$\mathbf{C}_2 \times \mathbf{S}_4$	$\mathbf{S}_4$	$(2,4,6)$	0	x^8+14x^4+1	$(48,48)$

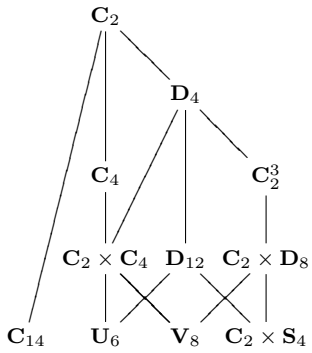

Figure 1. Automorphism groups for genus 3 hyperelliptic curves in characteristic 0 (see Remark 3.1)

For sake of completeness, we show how these results extend to all p. By [44], we know that when $p > 3+1 = 4$ and $p \neq 2\cdot 3+1 = 7$, then $C \mapsto C/\mathrm{Aut}(C)$ is tamely ramified and so by [26, XIII.2.12], it can be lifted to characteristic 0. Hence, Fig. 1 is also valid in these characteristics. When $p = 2$, the possible automorphism groups and models are in [40]. When $p = 7$, by [44] the curve $C : y^2 = x^7 - x$ which has a group of order $2^5 \cdot 3 \cdot 7$ is the only exceptional case. Finally for $p = 3$, going through the list of [5, Satz. 2.3], it seems that there is no new automorphism group and moreover the cases for which 3 divides $\#\,\mathrm{Aut}(C)$ in Fig. 1 do not appear anymore.

Remark 3.1. Some remarks on the notation and convention for Fig. 1.

- We have the following notation for the groups:
  - $\mathbf{C}_n = \mathbb{Z}/n\mathbb{Z}$;
  - $\mathbf{D}_{2n}$ is the dihedral group with $2n$ elements;

- $\mathbf{U}_6$ is a group with 24 elements defined by $\langle S, T\rangle$ with $S^{12} = T^2 = 1$ and $TST = S^5$;
- $\mathbf{V}_8$ is a group with 32 elements defined by $\langle S, T\rangle$ with $S^4 = T^8 = (ST)^2 = (S^{-1}T)^2 = 1$;
- $\mathbf{S}_n$ is the symmetric group over n letters.

- An exponent in the signature must be understood as repetition: for instance the signature (2^6) represents $(2, 2, 2, 2, 2, 2)$. The dimension δ of the stratum in H_3 is easily computed as $-3 + \#S$ where S is the signature. The column Id. refers to the GAP or MAGMA library of small groups.
- The order chosen for Fig. 1 is by decreasing dimension δ (resp. from top to bottom) then by increasing order of the automorphism group (resp. from left to right).
- The equation of the normal model is valid for the stratum: for some special values of the parameters, the curve can have more automorphisms.
- In both references [37] and [27], case 11 of Fig. 1 is wrongly written as $x^8 + 14x^2 + 1$.
- In [27, Fig. 1] and in [1, Tab. 3], the organization of the strata is wrong.

3.2. **Identification of loci and reconstruction with non-trivial automorphism groups.** Let C be a hyperelliptic curve of genus 3 defined over a field k of characteristic $p \neq 2, 3, 5, 7$ and let $K = \bar{k}$. Let $(j_2 : j_3 : \ldots : j_{10})$ be the Shioda invariants of C, our aim is to retrieve from them a K-isomorphic hyperelliptic model $y^2 = f(x)$.

The conic and quartic method presented in Section 2.3, based on Proposition 2.3 is our main tool for solving this problem, but unfortunately Lemma 3.2 shows that this method cannot work for most of the curves with a non-trivial automorphism group.

Lemma 3.2. *When the automorphism group of an hyperelliptic curve $C : y^2 = f(x)$ contains $\mathbf{D}_4$ (which are cases 2,4,5,6,7,9,10,11 of Fig. 1), then for any choice of 3 quadratic covariants $q_i = q_i(f, (x, z))$ of $f = x^8 + ax^6 + bx^4 + cx^2 + 1$, we have that $R(q_1, q_2, q_3) = 0$.*

Proof. Let d_i be the degree of the covariants q_i. Their weight is then $(8d_i - 2)/2 = 4d_i - 1$ which is always odd. Hence, for $g \in \mathrm{Aut}(C)$ acting as $g.(x, z) = (-x, z)$,

$$q_i(g.f) = q_i(f) = \det(g)^{4d_i-1} g.q_i(f) = -g.q_i(f).$$

Comparing the second and the last terms, we see that for all i, q_i has only an xz term. In particular the determinant of the q_i's in the bases x^2, xz, z^2 is zero. □

Remark 3.3. Note that this lemma actually applies to any odd genus hyperelliptic curve whose automorphism group contains $\mathbf{D}_4$.

We thus have to develop more specific methods for reconstructing models for curves in this case. Given invariants $(j_2 : j_3 : \ldots : j_{10})$, a prerequisite is to determine what is the automorphism group of the corresponding curve so that we can select the right normal model to reconstruct. To this aim, we determine for each automorphism group equations for the corresponding stratum in H_3. There are very few cases where determining some of these equations is straightforward, for instance automorphism groups which contains $\mathbf{C}_4$.

Lemma 3.4. *When the automorphism group of an hyperelliptic curve $C : y^2 = f(x)$ contains $\mathbf{C}_4$, i.e. in cases 3,5,9 and 10, then $J_i(f) = 0$ for all odd index i.*

Proof. The weight of an invariant of degree d is $8d/2 = 4d$. If $\mathrm{Aut}(C)$ contains $\mathbf{C}_4$, the curve C admits a model of the form $y^2 = f(x)$ with $f(x) = x(x^2-1)(x^4+ax^2+1)$. For $g \in \mathrm{Aut}(C)$ acting as $g.(x, z) = (-x, z)$, we get that

$$J_i(g.f) = \det(g)^{4i} J_i(f) = J_i(f).$$

On the other hand, $g.f = -f$, so if the degree of J_i is odd, then $J_i(g.f) = J_i(-f) = -J_i(f)$. Hence we get that $J_i(f) = -J_i(f)$. □

In order to exhibit necessary conditions for all the strata, we have applied Algorithm 2. We choose for I the constant invariant 0, seen as an invariant of increasing positive degree d, and choose for $\mathcal{F}$ (at line 2) a set of random octics over $\mathbb{Q}$ of the form the normal model for the automorphism group that we consider. Increasing one by one d from 0 to 30 yields generators for the ideal of relations which defines the stratum. The shape of these generators is very close to the one of a Gröbner basis for the graded reverse lexicographical

(or 'grevlex') order $J_2 < J_3 < \ldots < J_{10}$ with weights 2, 3, ..., 10. For this order, it is thus possible to deduce a reduced Gröbner basis. In the easier cases, note that it is feasible to apply a 'change of order algorithm' and to deduce a reduced Gröbner basis for the lexical order $J_2 < J_3 < \ldots < J_{10}$ too.

Now, in order to exhibit a model from given invariants, we proceed as above, except that we slightly modify Algorithm 2 to add in the basis $\mathcal{B}$ (at line 1) the coefficients a, b, *etc.* of the normal model in Fig. 1 for the considered stratum. We still choose for $\mathcal{F}$ (at line 2) a set of random octics in the shape of the normal model. The lowest degree equations found in this way are then enough to reconstruct a model.

All in all, we give below reconstruction lemmas, one for each automorphism group in Fig. 1. We precisely state the stratum equations that we have obtained and a model in terms of the j_i's for the curve C which may be defined over a non-trivial extension of k. In order to make this extension as small as possible, we introduce models which have more non-zero coefficients than the ones in Fig. 1. We refer the reader to Section 4 for the existence of a model over the field of moduli.

The proofs of these lemmas do not depend on the way we have obtained the equations. They follow essentially all the same principle.

- We check that the normal models of Fig. 1 have Shioda invariants that satisfy the stratum equations, so that we are convinced that these models are a subset of all the models which satisfy the stratum equations.
- Conversely, we check that the reconstructed model has Shioda invariants in the same weighted projective class as the 9-uple $(j_2 : j_3 : \ldots : j_{10})$ provided in input. Since these models are of normal form, we have proved that only normal models satisfy the stratum equations. If we can perform this step, we then have checked that the equations we found describe the stratum.

Most of these proofs need heavy computations, far too complex to be written down here, and so we must skip them. But a program written in the MAGMA computational algebra system is available on the web page of the authors for independent checks.

Incidentally, we succeed in parameterizing the projective variety defined by the stratum equations of dimension ≤ 2 (it is often a pencil of rational curves). As a first consequence, we give parameterized models over the field of moduli for all these strata, except the cases $\mathbf{C}_2^3$ where we have to deal with algebraic extensions. As a second consequence, we give the exact number of isomorphism classes of curves over a finite field $\mathbb{F}_q$ in these strata.

Algorithm 3: Reconstruct a hyperelliptic polynomial from its Shioda invariants

Input : Shioda invariants $(j_2 : j_3 : \ldots : j_{10})$.
Output: A hyperelliptic polynomial f

1 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (9), then reconstruct f with Lemma 3.5 (case $\mathbf{C}_2 \times \mathbf{S}_4$);
2 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (10), then reconstruct f with Lemma 3.5 (case $\mathbf{V}_8$);
3 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (11), then reconstruct f with Lemma 3.5 (case $\mathbf{U}_6$);
4 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (12), then reconstruct f with Lemma 3.5 (case $\mathbf{C}_{14}$);
5 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (XIII), then reconstruct f with Lemma 3.6 (case $\mathbf{C}_2 \times \mathbf{D}_8$);
6 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (XIV), then reconstruct f with Lemma 3.6 (case $\mathbf{D}_{12}$);
7 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (XV), then reconstruct f with Lemma 3.6 (case $\mathbf{C}_2 \times \mathbf{C}_4$);
8 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (XVII), then reconstruct f with Lemma 3.8 (case $\mathbf{C}_2^3$);
9 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (XVIII), then reconstruct f with Lemma 3.8 (case $\mathbf{C}_4$);
10 If $(j_2 : j_3 : \ldots : j_{10})$ satisfies Eq. (XXI), then reconstruct f with Lemma 3.10 (case $\mathbf{D}_4$);
11 Otherwise, reconstruct f with Lemma 3.13 (case $\mathbf{C}_2$);
12 **return** f;

Algorithm 3 summarizes how one can apply the lemmas below to reconstruct a model in any case. Actually, this algorithm returns more generally a binary form f of degree 8, even in the cases where f does not have simple roots. But, when the order of one of these roots is greater than 4, only one among all the possible orbits, is returned. Typically only $f = x^8$ is returned for $j_2 = j_3 = \ldots = j_{10} = 0$. Moreover the automorphism group of such a form may in general be bigger than the one indicated in the algorithm.

We state now, by increasing dimension, the reconstruction lemmas.

3.2.1. *Strata of dimension 0.*

Lemma 3.5. *Let C be a hyperelliptic curve of genus 3 over k, let $(j_2 : j_3 : \ldots : j_{10})$ be its Shioda invariants. Then the automorphism group of C is the one of the four strata of dimension 0 if and only if, respectively,*

$$\mathbf{C}_2 \times \mathbf{S}_4 : \quad 0 = 30\,j_3^2 - j_2^3 = j_4 = j_5 = \cdots = j_{10}\,; \tag{9}$$

$$\mathbf{V}_8 : \quad 0 = 6\,j_4 - j_2^2 = 36\,j_6 + j_2^3 = 420\,j_8 + j_2^4 = 2520\,j_{10} - j_2^5 = j_3 = j_5 = j_7 = j_9\,; \tag{10}$$

$$\mathbf{U}_6 : \quad 0 = 96\,j_4 - j_2^2 = 2304\,j_6 + j_2^3 = 17920\,j_8 - j_2^4 = 430080\,j_{10} + j_2^5 = j_3 = j_5 = j_7 = j_9\,; \tag{11}$$

$$\mathbf{C}_{14} : \quad 0 = j_2 = j_3 = j_4 = j_5 = j_6 = j_8 = j_9 = j_{10} \qquad (j_7 \neq 0)\,. \tag{12}$$

Furthermore, curves with these automorphism groups are, respectively, K-isomorphic to the curves

$$\mathbf{C}_2 \times \mathbf{S}_4 : y^2 = x^8 + 14\,x^4 + 1\,, \quad \mathbf{V}_8 : y^2 = x^8 - 1\,, \quad \mathbf{U}_6 : y^2 = x^7 - x\,, \quad \mathbf{C}_{14} : y^2 = x^7 - 1\,.$$

3.2.2. *Strata of dimension 1.*

Lemma 3.6. *Let C be a hyperelliptic curve of genus 3 over k, let $(j_2 : j_3 : \ldots : j_{10})$ be its Shioda invariants. Then the automorphism group of C is the one of the three strata of dimension 1 if and only if the invariants satisfy, respectively,*

- $\mathbf{C}_2 \times \mathbf{D}_8$: *a set of 9 equations of degrees 6, 7, 8, 8, 9, 9, 10, 10 and 12, denoted Eq. (XIII);*
- $\mathbf{D}_{12}$: *a set of 9 equations of degrees 6, 7, 8, 8, 9, 9, 10, 10 and 12, denoted Eq. (XIV);*
- $\mathbf{C}_2 \times \mathbf{C}_4$: *a set of 7 equations of degrees 3, 5, 7, 8, 9, 10 and 12, denoted Eq. (XV).*

Furthermore, curves with these automorphism groups are, respectively, K-isomorphic to the curves

- $\mathbf{C}_2 \times \mathbf{D}_8$: $y^2 = x^8 + a_4\,x^4 + a_0$ *where* $a_0 = -a_4^2/140 + j_2/2$ *and*
$$a_4 = \begin{cases} 35(j_5\,j_2 + 6\,j_4\,j_3)/(-60\,j_3^2 + 2{j_2}^3) & \text{if } -30\,j_3^2 + j_2^3 \neq 0\,, \\ 35j_5\,/\,3j_4 & \text{otherwise}\,; \end{cases}$$
- $\mathbf{D}_{12}$: $y^2 = x\,(x^6 + a_4\,x^3 + a_1)$ *where* $a_1 = 2\,a_4^2\,/\,35 - 4\,j_2$ *and*
$$a_4 = \begin{cases} 280\,(-j_5\,j_2 + 4\,j_4\,j_3)/(30\,j_3^2 - j_2^3) & \text{if } -30\,j_3^2 + j_2^3 \neq 0\,, \\ 35j_5\,/\,3j_4 & \text{otherwise}\,; \end{cases}$$
- $\mathbf{C}_2 \times \mathbf{C}_4 : y^2 = a^2x^8 + 2\,a^2x^6 + 8\,ax^2 - 16$ *with*
$$a = \begin{cases} 196/3 & \text{if } 6\,j_4 - j_2^2 = 0\,, \\ -84 & \text{if } 147\,j_4 - 2\,j_2^2 = 0\,, \\ 98\,\dfrac{36288\,j_4^2 - 3906\,j_4\,j_2^2 + 14400\,j_6\,j_2 + 43\,j_2^4}{9(96\,j_4 - j_2^2)(147\,j_4 - 2\,j_2^2)} & \text{otherwise}\,. \end{cases} \tag{16}$$

We remark that there is no difficulty to check that curves with invariants that annihilate denominators in these expressions have larger automorphism group.

- When $-30\,j_3^2 + j_2^3$ and j_4 are both equal to 0 in $\mathbf{C}_2 \times \mathbf{D}_8$ or $\mathbf{D}_{12}$ cases, Eq. (XIII) or Eq. (XIV) can be reduced to Eq. (9). This means that the automorphism group of C contains $\mathbf{C}_2 \times \mathbf{S}_4$. So Lemma 3.5 can be used, instead, for reconstructing a model.
- In $\mathbf{C}_2 \times \mathbf{C}_4$ case:
  - When $6\,j_4 - j_2^2$ and $36\,j_6 + j_2^3$ are both equal to 0, Eq. (XV) can be reduced to Eq. (10) and Lemma 3.5 can be used, instead, for reconstructing a model. Otherwise, *i.e.* when $6\,j_4 - j_2^2 = 0$ but $36\,j_6 + j_2^3 \neq 0$, then now $576\,j_6 - 65\,j_2^3 = 0$ but this lemma can still be applied.
  - When $96\,j_4 - j_2^2 = 0$, Eq. (XV) can be reduced to Eq. (11) and Lemma 3.5 can now be used for reconstructing a model.
  - When $147\,j_4 - 2\,j_2^2 = 0$ and $3087\,j_6 - 2\,j_2^3 = 0$, we can choose $f(x) = x(x-1)(x+1)(x^2+1)^2$. Its discriminant is obviously equal to zero and no hyperelliptic curve exists with such invariants. Otherwise, *i.e.* when $147\,j_4 - 2\,j_2^2 = 0$ but $3087\,j_6 - 2\,j_2^3 \neq 0$, then now $197568\,j_6 - 47\,j_2^3 = 0$ but this lemma can still be applied.

Actually the quotient field of $\mathcal{I}_8$ modulo the ideal defined by Eq. (XIII) or Eq. (XIV) is in both cases obtained by adjoining j_4 to $k[j_2, j_3]$ and j_4 satisfies an irreducible monic equation of degree 3. The invariants j_5, j_6, …, j_{10} are then rational in j_2, j_3 and j_4. Similarly, the quotient field of $\mathcal{I}_8$ modulo the ideal defined by Eq. (XV) is obtained by adjoining j_6 to $k[j_2, j_4]$ and j_6 satisfies an irreducible monic equation of degree 2. The invariants j_8 and j_{10} are then rational in j_2, j_4 and j_6 (the invariants j_3, j_5, j_7 and j_9 are trivial).

More geometrically, the projective varieties defined by Eq. (XIII), Eq. (XIV) or Eq. (XV) have singularities at the curves with larger automorphism group. They are all birationally equivalent to a non-degenerate conic. We can parameterize them and reconstruction formulas of Lemma 3.6 yield families of models for all the curves with such automorphism groups. All in all, we found what follows.

$$\begin{aligned}
\mathbf{C}_2\times\mathbf{D}_8:\quad & y^2 = x^8 + 7/6\,x^4 + 1/2\,t + 1/144\,,\\
& \qquad t \neq -1/72, 2/3 \quad (\mathbf{C}_2\times\mathbf{S}_4 \text{ and } \mathbf{V}_8 \text{ reached with } t = 0,\infty)\,;\\
\mathbf{D}_{12}:\quad & y^2 = x\,(x^6 - 7/9\,x^3 - 48\,t - 8/81)\,,\\
& \qquad t \neq -1/(2\cdot 3^5), -1/(2^6\cdot 3) \quad (\mathbf{C}_2\times\mathbf{S}_4 \text{ and } \mathbf{U}_6 \text{ reached with } t = 0,\infty)\,;\\
\mathbf{C}_2\times\mathbf{C}_4:\quad & y^2 = (x^4 + 2\,x^2 + 5/147\,t - 1/7)(x^4 - 5/147\,t + 1/7)\,,\\
& \qquad t \neq 21/5, 168/5 \quad (\mathbf{U}_6 \text{ and } \mathbf{V}_8 \text{ reached with } t = 24/5,\infty)\,.
\end{aligned}$$

We deduce from this the following result.

Proposition 3.7. *The strata of hyperelliptic curves of genus 3 whose automorphism group contains* $\mathbf{C}_2\times\mathbf{D}_8$, $\mathbf{D}_{12}$ *or* $\mathbf{C}_2\times\mathbf{C}_4$ *are rational of dimension one.*

Incidentally, the parameterizations show that over a finite field $\mathbb{F}_q$ of characteristic at least 11 there are $q-3$ isomorphism classes of curves with each of these automorphism groups.

3.2.3. *Strata of dimension 2.*

Lemma 3.8. *Let C be a hyperelliptic curve of genus 3 over k, let $(j_2 : j_3 : \ldots : j_{10})$ be its Shioda invariants. Then the automorphism group of C is the one of the two strata of dimension 2 if and only if the invariants satisfy, respectively,*

- $\mathbf{C}_2^3$: *a set of 14 equations of degrees 8, 9, 10, 10, 11, 12, 12, 13, 14, 14, 15, 16, 18 and 20, denoted Eq. (XVII);*
- $\mathbf{C}_4$: *a set of 8 equations of degrees 3, 5, 7, 9, 16, 18, 20 and 24, denoted Eq. (XVIII).*

Furthermore, curves with these automorphism groups are, respectively, K-isomorphic to

- $\mathbf{C}_2^3$: $y^2 = a_8\,x^8 + a_6\,x^6 + a_4\,x^4 + \lambda a_6\,x^2 + \lambda^2 a_8$ *where a_4 is any root of the degree 3 equation*

$$\begin{aligned}
0 = {} & 192\,(-60\,j_3^2 + 2\,j_2^3 + 18\,j_6 - 9\,j_4\,j_2)\,x^3 - 90720\,(3\,j_4\,j_3 + 3\,j_7 - j_5\,j_2)\,x^2\\
& + 294\,(765\,j_4\,j_2^2 + 1440\,j_6\,j_2 - 5940\,j_5\,j_3 - 1782\,j_4^2 + 1140\,j_3^2 j_2 - 38\,j_2^4)\,x + 6637050\,j_6\,j_3\\
& + 1250235\,j_5\,j_4 - 833490\,j_5\,j_2^2 + 2932650\,j_4\,j_3\,j_2 + 2881200\,j_3^3 - 96040\,j_3\,j_2^3
\end{aligned} \tag{19}$$

and $a_6 = -28\,\nu^2 - a_4^2/5 + 14\,j_2$, $a_8 = \nu\,a_6$ and $\lambda = 1/a_6$ with

$$\nu = \frac{18\,j_6\,a_4 - 9\,a_4\,j_4\,j_2 - 60\,a_4\,j_3^2 + 2\,a_4\,j_2^3 - 810\,j_7 + 270\,j_5\,j_2 - 810\,j_4\,j_3}{10\,(-18\,j_6 + 9\,j_4\,j_2 + 60\,j_3^2 - 2\,j_2^3)}\,.$$

- $\mathbf{C}_4$: *a curve constructed with the method of Proposition 8 for which one (at least) of the five discriminants*

$$R(C_{5,2}, C_{6,2}, C_{7,2}),\ R(C_{5,2}, C_{6,2}, C'_{7,2}),\ R(C_{5,2}, C_{7,2}, C'_{8,2}),\ R(C_{5,2}, C_{8,2}, C_{9,2}) \text{ or } R(C_{5,2}, C_{6,2}, C''_{9,2}) \tag{20}$$

is non-zero.

In $\mathbf{C}_2^3$ case, we remark that Eq. (19) may not have a root in the base field k too. Lemma 3.8 then yields a model over an extension k' of degree 3 (see Section 4 for the rationality issue). When $-18\,j_6 + 9\,j_4\,j_2 + 60\,j_3^2 - 2\,j_2^3 = 0$, Eq. (XVII) can be reduced to Eq. (XIII) and Lemma 3.6 can be used, instead, for reconstructing a model.

$f(x) = x\,(x^2-1)\,(x^4 + a\,x^2 + b)$		$\mathrm{Aut}(C)$
$a = 0$	$b = 0$	$\mathbf{U}_6, \mathbf{V}_8, \mathbf{C}_2 \times \mathbf{S}_4 \subset \mathrm{Aut}(C)$
any a	$b = 1$	$\mathbf{C}_2 \times \mathbf{C}_4 \subset \mathrm{Aut}(C)$
any a	$b^2 + (-3\,a + 1)\,b + a^3 = 0$	$\mathbf{C}_2 \times \mathbf{C}_4 \subset \mathrm{Aut}(C)$
$a = -6$	$b = -27$	$\mathbf{U}_6 \subset \mathrm{Aut}(C)$
$a = 10/3$	$b = 1$	$\mathbf{U}_6 \subset \mathrm{Aut}(C)$
$a = 2/9$	$b = -1/27$	$\mathbf{U}_6 \subset \mathrm{Aut}(C)$
$a = -6$	$b = 1$	$\mathbf{V}_8 \subset \mathrm{Aut}(C)$
$a^2 + 40\,a + 8 = 0$	$b = -5\,a - 1$	$\mathbf{V}_8 \subset \mathrm{Aut}(C)$

TABLE 2. $\mathbf{C}_4$-hyperelliptic polynomials that cancel all the determinants of Eq. (20)

Unlike the previous strata, curves with automorphism group $\mathbf{C}_4$ can be reconstructed with the conic and quartic method of Section 2.3. To check that at least one among the five determinants of Eq. (20) is non-zero for a curve with automorphism group $\mathbf{C}_4$, we solve in a and b (over the integers to ensure that the result is still true modulo any positive prime p) the system obtained by evaluating these determinants at normal forms $x\,(x^2-1)\,(x^4 + a\,x^2 + b)$. We found a finite number of irreducible components, possibly defined in a k-extension, but all with an automorphism group larger than $\mathbf{C}_4$ (*cf.* Tab. 2). In fields of characteristic 0, we can conclude with only 4 determinants,

$$R(C_{5,2}, C_{6,2}, C_{7,2}),\ R(C_{5,2}, C_{7,2}, C'_{8,2}),\quad R(C_{5,2}, C_{8,2}, C_{9,2}) \text{ and } R(C_{5,2}, C_{6,2}, C''_{9,2}).$$

These four determinants are enough in positive characteristic p too, except for a finite number of primes the smallest of which is $p = 47$ (modulo 47, the point $(1\ :0\ :1:0:3:0:43:0:18)$ cancel all the determinants of Eq. (20) except $R(C_{5,2}, C_{6,2}, C'_{7,2})$). It may happen that none of the five conics has a k-rational point. Rationality issues will be handled in Section 4.

Now, the quotient field of $\mathcal{I}_8$ modulo the ideal defined by Eq. (XVII) is obtained by adjoining j_5 to $k[j_2, j_3, j_4]$ and j_5 satisfies an irreducible monic equation of degree 4. The invariants j_6, j_7, ..., j_{10} are then rational in j_2, j_3, j_4 and j_5. Similarly, the quotient field of $\mathcal{I}_8$ modulo the ideal defined by Eq. (XVIII) is obtained by adjoining j_8 to $k[j_2, j_4, j_6]$ and j_8 satisfies an irreducible monic equation of degree 3. The invariant j_{10} is then rational in j_2, j_4, j_6 and j_8 (the invariants j_3, j_5, j_7 and j_9 are trivial).

More geometrically, the projective varieties defined by Eq. (XVII) or Eq. (XVIII) have singularities at the curves with larger automorphism group, *i.e* respectively $\mathbf{C}_2 \times \mathbf{D}_8$ and $\mathbf{C}_2 \times \mathbf{C}_4$. They are both birationally equivalent to a pencil of rational curves. Similarly to Section 3.2.2, we can parameterize them and reconstruction formulas of Lemma 3.8 yield families of models for all the curves with such automorphism groups.

For curves with automorphism group $\mathbf{C}_2^3$ and rational Shioda invariants, we found in this way the following generic parameterization,

$$\begin{aligned} y^2 = {} & (-\frac{14}{5}\,u\alpha^2 + (-\frac{7}{20}\,t + \frac{1029}{2}\,u^2)\alpha + \frac{3185}{32}\,tu + \frac{343}{32}\,t - \frac{156065}{4}\,u^3)x^8 + \\ & (-\frac{12}{25}\,\alpha^2 + \frac{392}{5}\,u\alpha + 14\,t - 5488\,u^2)x^6 + \alpha x^4 + x^2 + (\frac{61}{700}\,tu - \frac{3}{100}\,t - \frac{14}{5}\,u^3)\frac{\alpha^2}{\delta} + \\ & (-\frac{1}{35}\,t^2 - \frac{133}{20}\,tu^2 + \frac{133}{20}\,tu - 686\,u^4)\frac{\alpha}{\delta} + (\frac{95}{32}\,t^2u - \frac{7}{32}\,t^2 - \frac{2597}{16}\,tu^3 - \frac{14749}{48}\,tu^2 + \frac{156065}{2}\,u^5)\frac{1}{\delta} \end{aligned}$$

with α any root of $192\,x^3 - 47040\,ux^2 + (-4200\,t + 4527600\,u^2)\,x + 385875\,tu - 42875\,t - 151263000\,u^3$ and

$$\delta = t^3 - 16709\,t^2u^2/32 + 1029\,t^2u/16 - 1029\,t^2/32 + 132055\,tu^4/2 + 84035\,tu^3/6 - 5882450\,u^6\,.$$

The curves that are not reached by this parameterization are as follows.

$$\underline{J_2=0 \text{ and } J_3,\, J_4\neq 0}: y^2=(\frac{7}{5}\,\alpha^2+\frac{1029}{8}\,\alpha+\frac{108045}{8}\,t+\frac{12005}{2})x^8+(-\frac{12}{25}\,\alpha^2-\frac{196}{5}\,\alpha-1372)x^6+$$
$$\alpha x^4+x^2+(\frac{2}{2701125}\,t+\frac{4}{72930375})\frac{\alpha^2}{\delta}+(\frac{19}{231525}\,t+\frac{16}{2083725})\frac{\alpha}{\delta}+(\frac{43}{22680}\,t+\frac{1}{4860})\frac{1}{\delta}$$
$$\text{with here } \delta=t^2+17\,t/81+1/81 \text{ and } 16\,\alpha^3+1960\,\alpha^2+94325\,\alpha-4501875\,t+1200500=0\,;$$

$$\underline{J_3=0 \text{ and } J_2,\, J_5\neq 0}: y^2=\frac{1}{240}\,(96\,\alpha^2+280\,(367\,t+430)\alpha+15925\,(59+52\,t)(17\,t+29))(59+52\,t)x^8+$$
$$(-\frac{12}{25}\,\alpha^2-\frac{56}{5}\,(59+52\,t)\alpha-\frac{196}{3}\,(59+52\,t)(17\,t+29))x^6+x^4\alpha+x^2+36\,(791\,t+779)\frac{\alpha^2}{\delta}+$$
$$420\,(124717+114964\,t^2+239429\,t)\frac{\alpha}{\delta}+3675\,(107671\,t^2+220001\,t+112798)(59+52\,t)\frac{1}{\delta}$$
$$\text{with now } \delta=300125\,(17\,t+29)(9844\,t^2+19487\,t+9679)(59+52\,t) \text{ and}$$
$$96\,\alpha^3+3360\,(59+52\,t)\alpha^2+9800\,(173\,t+206)(59+52\,t)\alpha+128625\,(17\,t+29)(59+52\,t)^2=0\,;$$

$$\underline{\text{Isolated point}}: y^2=(4/5\,a^2+\frac{2569}{78}\,a+\frac{4165}{24})x^8+(-\frac{12}{25}\,\alpha^2-\frac{112}{5}\,\alpha-\frac{3332}{39})x^6+$$
$$x^4\alpha+x^2+\frac{343746}{1793761375}\,\alpha^2+\frac{4483596}{358752275}\,\alpha+\frac{4199169}{20500130}$$
$$\text{where } 624\,\alpha^3+43680\,\alpha^2+847700\,\alpha+2186625=0\,.$$

Modulo 101, the latter degenerates to only one projective point. In this case, we can consider

$$\underline{J_3=0 \text{ and } J_2,\, J_5\neq 0}: y^2=89\,(\alpha^2+(45\,t+11)\alpha+78\,(12+t)(t+84))(12+t)x^8+$$
$$(48\,\alpha^2+(33\,t+93)\alpha+42\,(12+t)(t+84))x^6+x^4\alpha+x^2+$$
$$63\,((t+17)\alpha^2+(11\,t^2+26\,t+66)\alpha+7\,(12+t)(t^2+57\,t+11))/\delta$$
$$\text{for } \delta=(t+84)(t^2+14\,t+87)(12+t) \text{ and } \alpha^3+61\,(12+t)\alpha^2+44\,(12+t)(t+63)\alpha+88\,(12+t)^2(t+84)=0\,;$$
$$\underline{\text{Isolated point}}: y^2=x^8+41\,x^7+100\,x^6+59\,x^5+75\,x^4+75\,x^3+67\,x^2+78\,x+67\,.$$

We are also able to deduce explicit models for $\mathbf{C}_4$ over the field of moduli (see Section 4.5), but such expressions are far too large to be written down here. We thus restrict here parameterizations for Shioda invariants, $(t,u)\mapsto(j_2(t,u):0:j_4(t,u):0:j_6(t,u):0:j_8(t,u):0:j_{10}(t,u))\,,$

$$\begin{cases}
j_2=t\,,\ \ j_4=\frac{1}{96}\,(t+1)t^2\,,\\
j_6=-\frac{1}{124416000}\,(720\,u+63\,t-25)(-518400\,u^2+(-90720\,t+36000)u+2700\,t^3-1269\,t^2+3150\,t-625)\,,\\
j_8=\frac{8}{3}\,u^4+(2/3\,t-\frac{10}{27})u^3+(-\frac{1}{360}\,t^3+\frac{139}{3600}\,t^2-\frac{5}{72}\,t+\frac{25}{1296})u^2+(-\frac{17}{14400}\,t^4+\frac{241}{432000}\,t^3-\frac{139}{51840}\,t^2+\frac{25}{10368}\,t\\
\quad -\frac{125}{279936})u-\frac{1}{483840}\,t^6-\frac{9707}{145152000}\,t^5+\frac{82091}{967680000}\,t^4-\frac{299}{18662400}\,t^3+\frac{139}{2985984}\,t^2-\frac{125}{4478976}\,t+\frac{625}{161243136}\,,\\
j_{10}=-\frac{5}{3}\,u^5+(-\frac{31}{48}\,t+\frac{125}{432})u^4+(-\frac{23}{3360}\,t^3-\frac{3349}{40320}\,t^2+\frac{155}{1728}\,t-\frac{625}{31104})u^3\\
\quad +(-\frac{1}{345600}\,t^4-\frac{94723}{29030400}\,t^3+\frac{3349}{387072}\,t^2-\frac{775}{165888}\,t+\frac{3125}{4478976})u^2\\
\quad +(\frac{61}{3870720}\,t^6+\frac{86893}{580608000}\,t^5-\frac{735179}{13934592000}\,t^4+\frac{105073}{418037760}\,t^3-\frac{16745}{55738368}\,t^2+\frac{3875}{35831808}\,t-\frac{15625}{1289945088})u\\
\quad +\frac{1}{44236800}\,t^7+\frac{734581}{139345920000}\,t^6-\frac{23681183}{3344302080000}\,t^5+\frac{736579}{401316249600}\,t^4\\
\quad -\frac{108523}{24078974976}\,t^3+\frac{83725}{24078974976}\,t^2-\frac{19375}{20639121408}\,t+\frac{15625}{185752092672}\,.
\end{cases}$$

The curves that are not reached by this parameterization are as follows.

$$\underline{J_4 = J_2^2/96}: \quad \begin{cases} j_2 = t\,,\ j_4 = \dfrac{1}{96}\,t^2\,,\ j_6 = \dfrac{1}{7776000}\,(71\,t+2)(2183\,t^2+142\,t+2)\,, \\ j_{10} = \dfrac{16012139}{8817984000}\,t^4 + \dfrac{51401}{196830000}\,t^3 + \dfrac{7301}{524880000}\,t^2 + \dfrac{31}{98415000}\,t \\ \qquad + \dfrac{1}{393660000}, 0, -\dfrac{905961157}{3174474240000}\,t^5 - \dfrac{672811}{14171760000}\,t^4 - \dfrac{2449033}{793618560000}\,t^3 \\ \qquad - \dfrac{77179}{793618560000}\,t^2 - \dfrac{337}{226748160000}\,t - \dfrac{1}{113374080000} \end{cases}$$

$$\underline{J_2 = 0 \text{ and } J_6 = J_4}: \quad \begin{cases} j_2 = 0\,,\ j_4 = \dfrac{4}{3969}\,(t-9)(11\,t+6)\,,\ j_6 = \dfrac{4}{3969}\,(t+1)(11\,t+6)^2\,, \\ j_8 = \dfrac{32}{36756909}\,(373\,t^2+440\,t+127)(11\,t+6)^2\,,\ j_{10} = -\dfrac{8}{992436543}\,(835\,t^2+646\,t+51)(11\,t+6)^3 \end{cases}$$

$$\underline{\text{Isolated points}}: \quad \begin{cases} \left(1:0:\dfrac{1}{96}:0:\dfrac{154993}{7776000}:0:\dfrac{16012139}{8817984000}:0:-\dfrac{905961157}{3174474240000}\right), \\ \left(0:0:\dfrac{4}{43659}:0:\dfrac{4}{43659}:0:\dfrac{11936}{4447585989}:0:-\dfrac{6680}{120084821703}\right), \qquad \text{when defined.} \end{cases}$$

In both cases, we can check that the rational projective points defined on these two varieties are none other than the ones given by these parameterizations. We deduce the following result.

Proposition 3.9. *The strata of hyperelliptic curves of genus 3 whose automorphism group contains* $\mathbf{C}_2^3$ *or* $\mathbf{C}_4$ *are rational of dimension* 2.

Incidentally, this shows that over a finite field $\mathbb{F}_q$ of characteristic at least 11 there are $q^2-2\,q+2$ isomorphism classes of curves with each of these automorphism groups.

3.2.4. *Stratum of dimension 3.* The stratum of dimension 3 corresponds to curves with automorphism group $\mathbf{D}_4$. Contrary to the other strata, we consider generators for the grevlex order $J_2 < J_3 < \ldots < J_{10}$ with weights 2, 3, ..., 10 (since generators for a lexical order are too huge).

Lemma 3.10. *Let* C *be a hyperelliptic curve of genus 3 over* k*, let* $(j_2, j_3, \ldots, j_{10})$ *be its Shioda invariants. Then the automorphism group of* C *is* $\mathbf{D}_4$ *if and only if* j_2*,* j_3*, ...,* j_{10} *satisfy a set of 24 equations, from degree 16 up to degree 24, denoted Eq.* (XXI) *.*
Furthermore, a curve C *with automorphism group* $\mathbf{D}_4$ *is* K*-isomorphic to the curve* $y^2 = a_0\,x^8 + a_6\,x^6 + a_4\,x^4 + a_2\,x^2 + a_0$ *where* a_4 *is the solution of the linear equation*

$$\begin{aligned} 0 = {} & (-11022480 j_5 j_4 j_3 + 2933280 j_4 j_3^2 j_2 + 784 j_2^6 + 55339200 j_6^2 + 4408992 j_4^3 + 705600 j_3^4 - 36741600 j_9 j_3 - 4286520 j_5^2 j_2 \\ & + 32315760 j_6 j_4 j_2 + 36741600 j_{10} j_2 - 64297800 j_7 j_5 + 10054800 j_6 j_3^2 - 335160 j_6 j_2^3 - 47040 j_3^2 j_2^3 + 2812320 j_4^2 j_2^2 \\ & - 97776 j_4 j_2^4)X - 410791500 j_7 j_6 - 10716300 j_9 j_2^2 + 4365900 j_7 j_2^3 + 150793650 j_6 j_4 j_3 + 39590775 j_6 j_5 j_2 \\ & - 196465500 j_7 j_4 j_2 + 10716300 j_4^2 j_3 j_2 + 1205583750 j_8 j_5 - 1157360400 j_9 j_4 + 254435580 j_5 j_4^2 + 321489000 j_{10} j_3 \\ & - 75014100 j_5^2 j_3 - 130977000 j_7 j_3^2 + 7144200 j_4 j_3^3 + 5120010 j_5 j_4 j_2^2 - 238140 j_4 j_3 j_2^3 - 185220 j_5 j_2^4 + 5556600 j_5 j_3^2 j_2 \\ & \text{if this equation is non-trivial,} \end{aligned} \tag{22}$$

$$\begin{aligned} 0 = {} & (-483840 j_4 j_3^2 j_2 + 2449440 j_5 j_4 j_3 - 112 j_2^6 - 9072000 j_6^2 - 629856 j_4^3 - 100800 j_3^4 + 612360 j_5^2 j_2 - 6713280 j_6 j_4 j_2 \\ & + 9185400 j_7 j_5 - 2797200 j_6 j_3^2 + 93240 j_6 j_2^3 + 6720 j_3^2 j_2^3 - 498960 j_4^2 j_2^2 + 16128 j_4 j_2^4 + 18370800 j_8 j_4)X \\ & + 89302500 j_7 j_6 + 26460 j_5 j_2^4 - 2381400 j_4^2 j_3 j_2 - 22027950 j_6 j_4 j_3 - 11013975 j_6 j_5 j_2 + 41079150 j_7 j_4 j_2 \\ & + 10716300 j_5^2 j_3 - 241116750 j_8 j_5 + 257191200 j_9 j_4 - 56030940 j_5 j_4^2 + 23814000 j_7 j_3^2 \\ & - 1587600 j_4 j_3^3 - 793800 j_7 j_2^3 - 793800 j_5 j_3^2 j_2 - 476280 j_5 j_4 j_2^2 + 52920 j_4 j_3 j_2^3 \quad \text{otherwise;} \end{aligned} \tag{23}$$

a_0 is any root of the quadratic equation

$$\begin{aligned} 0 = {} & (-529079040 j_5 j_4 j_3 + 1551156480 j_6 j_4 j_2 + 140797440 j_4 j_3^2 j_2 - 2257920 j_3^2 j_2^3 - 4693248 j_4 j_2^4 - 1763596800 j_9 j_3 \\ & + 1763596800 j_{10} j_2 + 2656281600 j_6^2 + 33868800 j_3^4 + 37632 j_2^6 + 211631616 j_4^3 + 134991360 j_4^2 j_2^2 - 16087680 j_6 j_2^3 \\ & - 205752960 j_5^2 j_2 + 482630400 j_6 j_3^2 - 3086294400 j_7 j_5)X^2 - 14647500 j_4 j_3^2 j_2^2 - 307355310 j_6 j_4 j_2^2 - 140277690 j_6 j_3^2 j_2 \\ & - 382571910 j_7 j_4 j_3 + 1130212440 j_6 j_5 j_3 - 105019740 j_8 j_4 j_2 + 555660 j_5 j_3 j_2^3 + 206671500 j_9 j_3 j_2 + 36996750 j_5 j_4 j_3 j_2 \\ & + 3472081200 j_7^2 - 3724 j_2^7 + 507952620 j_7 j_5 j_2 + 8024365440 j_{10} j_4 + 530456850 j_5^2 j_4 - 472252032 j_6 j_4^2 - 4089340080 j_9 j_5 \\ & + 39293100 j_4^2 j_3^2 - 16669800 j_5 j_3^3 - 400029840 j_6^2 j_2 - 114388848 j_4^3 j_2 - 3351600 j_3^4 j_2 - 206671500 j_{10} j_2^2 + 27862380 j_5^2 j_2^2 \\ & + 10835370 j_8 j_2^3 - 15739920 j_4^2 j_2^3 + 4675923 j_6 j_2^4 + 223440 j_3^2 j_2^4 + 488250 j_4 j_2^5 - 325061100 j_8 j_3^2 - 13974055200 j_8 j_6 \\ & \text{if this equation is non-trivial,} \end{aligned} \tag{24}$$

$$
\begin{aligned}
0 = (&117573120 j_5 j_4 j_3 - 322237440 j_6 j_4 j_2 - 23224320 j_4 j_3^2 j_2 + 322560 j_3^2 j_2^3 + 774144 j_4 j_2^4 + 881798400 j_8 j_4 - 435456000 j_6^2 \\
&- 4838400 j_3^4 - 5376 j_2^6 - 30233088 j_4^3 - 23950080 j_4^2 j_2^2 + 4475520 j_6 j_2^3 + 29393280 j_5^2 j_2 - 134265600 j_6 j_3^2 \\
&+ 440899200 j_7 j_5) X^2 + 151099830 j_7 j_4 j_3 + 2457000 j_4 j_3^2 j_2^2 \\
&+ 34838370 j_6 j_3^2 j_2 - 257905620 j_6 j_5 j_3 - 184779630 j_8 j_4 j_2 - 79380 j_5 j_3 j_2^3 - 72564660 j_7 j_5 j_2 - 10206000 j_5 j_4 j_3 j_2 \\
&- 868020300 j_7^2 + 532 j_2^7 - 2469035520 j_{10} j_4 - 96446700 j_5^2 j_4 + 62215776 j_6 j_4^2 + 1080203040 j_9 j_5 + 66418380 j_6 j_4 j_2^2 \\
&+ 2381400 j_5 j_3^3 + 20230560 j_6^2 j_2 + 15422724 j_4^3 j_2 + 478800 j_3^4 j_2 - 3980340 j_5^2 j_2^2 - 1547910 j_8 j_2^3 + 2999430 j_4^2 j_2^3 \\
&- 1161279 j_6 j_2^4 - 31920 j_3^2 j_2^4 - 81900 j_4 j_2^5 + 46437300 j_8 j_3^2 + 3815002800 j_8 j_6 - 11736900 j_4^2 j_3^2 \quad \text{otherwise;}
\end{aligned}
\tag{25}
$$

a_2 is any root of

$$
\begin{aligned}
0 &= 15750\, a_0\, X^4 + (105000\, a_0^2\, a_4 + 510\, a_4^3 - 23100\, a_4\, j_2 - 686000\, j_3)\, X^2 + 705600\, a_0^3\, a_4^2 - 10804500\, a_0^3\, j_2 \\
&\quad + 3024\, a_0\, a_4^4 - 244755\, a_0\, a_4^2\, j_2 - 1440600\, a_0\, a_4\, j_3 + 15126300\, a_0\, j_4 + 2881200\, a_0\, j_2^2 \quad \textit{if } a_0 \neq 0, \\
0 &= X - 1 \quad \textit{otherwise;}
\end{aligned}
$$

and a_6 is any root of

$$
\begin{aligned}
0 &= 5\, a_2\, X + 140\, a_0^2 + a_4^2 - 70\, j_2 \quad \textit{if } a_2 \neq 0, \\
0 &= 1575\, a_0\, X^2 - 24\, a_4^3 + 2940\, a_4\, j_2 - 68600\, j_3 \quad \textit{otherwise.}
\end{aligned}
$$

Similarly to the automorphism group $\mathbf{C}_2^3$, Lemma 3.10 yields most of the time a model over an extension of k (of degree at most 8, see Section 4 for the rationality issue).

In case the j_i's correspond to polynomials with multiple roots, it may happen that some of equations in Lemma 3.10 for a_4, a_0, a_2 or a_6 are inconsistent (typically '$0 = 1$'). It means that none of the polynomials $a_0\, x^8 + a_6\, x^6 + a_4\, x^4 + a_2\, x^2 + a_0$ have such invariants. Instead, we construct polynomials of the form $f(x) = a_8\, x^8 + a_6\, x^6 + a_4\, x^4 + a_2\, x^2$ where a_4 is the root of

$$
\begin{aligned}
0 &= (11741206932\, j_7 + 7172848242\, j_4\, j_3 - 407219400\, j_3\, j_2^2 - 340313967\, j_5\, j_2) X - 770798216160\, j_8 + 48652305408\, j_6\, j_2 \\
&\quad - 21652069824\, j_4^2 - 15830753400\, j_5\, j_3 + 1196327160\, j_4\, j_2^2 - 77421296\, j_2^4 - 6442857120\, j_3^2 j_2 \quad \text{if this equation is non-trivial,} \\
0 &= (488750830848\, j_4^2 + 19912489511040\, j_8 + 11982595926 0\, j_3^2 j_2 + 272672590848\, j_4\, j_2^2 - 11523989242\, j_2^4) X \\
&\quad + 663046656007680\, j_9 + 29540232087660\, j_7\, j_2 - 147027580680960\, j_5\, j_4 - 238603106730240\, j_6\, j_3 \\
&\quad - 32453930490450\, j_4\, j_3\, j_2 + 5621022644895\, j_5\, j_2^2 + 590440221000\, j_3\, j_2^3 j_2 \quad \text{otherwise, if this equation is non-trivial,} \\
0 &= (7023805824\, j_6\, j_2 - 83616540\, j_3^2 j_2 + 1090412288\, j_4\, j_2^2 + 1936166400\, j_4^2 - 40257382\, j_2^4) X + 231759118080\, j_9 \\
&\quad - 96001584000\, j_5\, j_4 - 23998355150\, j_4\, j_3\, j_2 - 191099623680\, j_6\, j_3 - 32526010860\, j_7\, j_2 + 310611000\, j_3\, j_2^3 - 617600655\, j_5\, j_2^2 \\
&\quad \text{otherwise, if this equation is non-trivial,} \\
0 &= X \quad \text{otherwise;}
\end{aligned}
$$

and

$$
a_2 = 1\,,\ a_6 = -\,(a_4^2 - 70\, j_2)/5a_2\,,\ a_8 = -17\, a_4^3/525 + 22\, a_4\, j_2/15 + 392\, j_3/9\,.
$$

Remark 3.11. It may happen that a curve C annihilates both Eqs. (22) and (23), so that we cannot determine a_4. But, when it happens, the automorphism group is larger than $\mathbf{D}_4$ (see Tab. 3) and so, lemmas for larger automorphism group apply.

Curves $C : y^2 = a_0\, x^8 + a_6\, x^6 + a_4\, x^4 + a_2\, x^2 + a_0$	Singular	Aut C
$a_0 = 0$	Yes	$\mathbf{C}_2^3 \subset \operatorname{Aut} C$
$a_6 + a_2 = 0$	No	$\mathbf{C}_2^3 \subset \operatorname{Aut} C$
$a_6 - a_2 = 0$	No	$\mathbf{C}_2^3 \subset \operatorname{Aut} C$
$\begin{cases} 308 a_0 a_2 a_6 a_4 - 224 a_0 a_4^3 + 3 a_2^3 a_6 + 15 a_2^2 a_4^2 + 3 a_2 a_6^3 + 15 a_6^2 a_4^2 = 0 \\ 21 a_0 a_2^2 + 21 a_0 a_6^2 + 11 a_2 a_6 a_4 - 8 a_4^3 = 0 \\ 196 a_0^2 - a_2 a_6 - 5 a_4^2 = 0 \end{cases}$	No	$\mathbf{D}_{12} \subset \operatorname{Aut} C$

TABLE 3. Automorphism groups of curves C which cancel both Eqs. (22) and (23)

Remark 3.12. It may happen that a curve C cancels both Eqs. (24) and (25), so that we cannot determine a_0. But again, when it happens, the automorphism group is larger than $\mathbf{D}_4$ (see Tab. 4) and so, lemmas for larger automorphism group apply.

Curves $C : y^2 = a_0\,x^8 + a_6\,x^6 + a_4\,x^4 + a_2\,x^2 + a_0$	Singular	$\mathbf{C}_2^3 \subset \mathrm{Aut}\,C$
$a_0 = 0$	Yes	$\mathbf{C}_2^3 \subset \mathrm{Aut}\,C$
$a_6 + a_2 = 0$	No	$\mathbf{C}_2^3 \subset \mathrm{Aut}\,C$
$a_6 - a_2 = 0$	No	$\mathbf{C}_2^3 \subset \mathrm{Aut}\,C$
$\begin{cases} 308a_0a_2a_6a_4 - 224a_0a_4^3 + 3a_2^3a_6 + 15a_2^2a_4^2 + 3a_2a_6^3 + 15a_6^2a_4^2 = 0 \\ 21a_0a_2^2 + 21a_0a_6^2 + 11a_2a_6a_4 - 8a_4^3 = 0 \\ 196a_0^2 - a_2a_6 - 5a_4^2 = 0 \end{cases}$	No	$\mathbf{D}_{12} \subset \mathrm{Aut}\,C$
$\begin{cases} 14a_0 + 2a_6 - a_4 = 0 \\ 14a_0 + 2a_2 - a_4 = 0 \end{cases}$	No	$\mathbf{C}_2 \times \mathbf{D}_8 \subset \mathrm{Aut}\,C$
$\begin{cases} 14a_0 - 2a_6 - a_4 = 0 \\ 14a_0 - 2a_2 - a_4 = 0 \end{cases}$	No	$\mathbf{C}_2 \times \mathbf{D}_8 \subset \mathrm{Aut}\,C$

TABLE 4. Automorphism groups of curves C which cancel both Eqs. (24) and (25)

Here, the quotient field of $\mathcal{I}_8$ modulo the ideal defined by Eq. (XXI) is obtained by adjoining j_6 to $k[j_2, j_3, j_4, j_5]$ and j_6 satisfies an irreducible monic equation of degree 10. The invariants j_7, j_8, j_9 and j_{10} are then rational in j_2, j_3, j_4 and j_5.

Geometrically and contrary to the other strata, we did not find any rational intersection with trivial hyperplane of the projective variety defined by Eq. (XXI). For instance, intersecting with $j_2 = j_3 = 0$ is geometrically birationally equivalent to the elliptic curve $y^2 = x^3 - x$, of j-invariant 1728 (the curve with complex multiplication by $\sqrt{-1}$). Nevertheless, it is straightforward to adapt the enumeration algorithm at the end of Section 1.4 to the case of a field of degree 10 over $k[j_2, j_3, j_4, j_5]$ (instead of a field of degree 5 over $k[j_2, j_3, j_4, j_5, j_6, j_7]$ for the full $\mathcal{I}_8$), in order to find non-trivial curves with automorphism group contained in $\mathbf{D}_4$.

At last, we emphasize that we have encountered unexpected computational difficulties to check that a reconstructed model for $\mathbf{D}_4$ has the same weighted projective class as the 9-uple $(j_2 : \ldots : j_{10})$ provided in input. Our first MAGMA implementations took about one week only to define the degree 8 extensions needed for the reconstructed model (due to some unexpected internal Gröbner basis computations) that we had to design a more optimized version. We perform by 'hand', *i.e.* directly over the quotient field of $\mathcal{I}_8$ modulo the ideal defined by Eq. (XXI), the calculation of the Shioda invariants of the reconstructed model. This requires explicit expressions for each coordinate of the Shioda invariants in the basis 1, a_0, a_2, $a_0\,a_2$, a_2^2,..., $a_0a_2^3$. Moreover, we only check the equality of j_2, ..., j_6 since j_7, j_8, j_9 and j_{10} are rational in j_2, j_3, j_4, j_5 and j_6. The corresponding routine took about half a day on a computer to check finally that everything is fine.

3.2.5. *Generic stratum.* Our main tool for reconstructing curves C with automorphism group $\mathbf{C}_2$ is the conic and quartic method developed in Proposition. 2.3. It requires that C does not cancel all the 364 fundamental conic determinants $R(q_1, q_2, q_3)$ (or equivalently Eq. (XXI)), otherwise Algorithm 3 fails. To check that this cannot happen, we have computed a Gröbner basis (for the grevlex order $J_2 < J_3 < \ldots < J_{10}$ with weights 2, 3, ..., 10) of a polynomial system which concatenates relations (1) and the *fundamental determinants* $R(q_1, q_2, q_3)$ with $\{q_1, q_2, q_3\}$ any subset of size 3 of the set of 14 covariants of order 2 given in Tab. 1. From Lemma 3.2, these 364 fundamental determinants all vanish for curves with automorphism group containing $\mathbf{D}_4$. Surprisingly, the Gröbner basis that we obtain is equal to the system of 24 polynomials (XXI) of Lemma 3.10.

After some further computations, still for the 'grevlex' order $J_2 < J_3 < \ldots < J_{10}$ with weights 2, 3, ..., 10, we observe that we can reduce the set of 364 fundamental conic determinants $R(q_1, q_2, q_3)$ to a subset of only 19 elements, since the determinants of these 19 conics generate the same ideal as the one defined by Eq. (XXI).

Lemma 3.13. *Let C be a hyperelliptic curve of genus 3 over k, let $(j_2 : j_3 : \ldots : j_{10})$ be its Shioda invariants. If j_2, j_3, ... j_{10} do not cancel Eq. (XXI), nor Eq. (XVIII) and Eq. (12), then its automorphism group is $\mathbf{C}_2$. Some of the 364 fundamental determinants are non-zero among which at least one of the following 19*

determinants,

$$\begin{array}{lllll} R(C_{5,2},C_{6,2},C_{7,2}), & R(C_{5,2},C_{8,2},C_{9,2}), & R(C_{5,2},C_{7,2},C'_{8,2}), & R(C_{5,2},C_{6,2},C''_{9,2}), & R(C_{5,2},C'_{7,2},C'_{9,2}),\\ R(C_{5,2},C_{6,2},C'_{7,2}), & R(C_{5,2},C'_{8,2},C_{11,2}), & R(C_{5,2},C_{7,2},C_{11,2}), & R(C_{5,2},C_{7,2},C'_{11,2}), & R(C_{5,2},C'_{7,2},C'_{10,2}),\\ R(C_{6,2},C'_{7,2},C_{9,2}), & R(C_{5,2},C_{7,2},C_{10,2}), & R(C_{5,2},C_{7,2},C_{9,2}), & R(C_{5,2},C_{6,2},C'_{10,2}), & R(C_{5,2},C_{6,2},C_{10,2}),\\ R(C_{5,2},C'_{7,2},C'_{8,2}), & R(C_{5,2},C_{6,2},C'_{9,2}), & R(C_{5,2},C_{6,2},C'_{8,2}), & R(C_{5,2},C_{6,2},C_{8,2}). & \end{array}$$

With one of the corresponding non-singular conics, we can use Proposition. 2.3 to reconstruct the curve.

There are examples of curves with automorphism group $\mathbf{C}_2$ for which many determinants R are zero.

- The curve defined over $\mathbb{Q}$ by
$$\begin{aligned} y^2 = {} & 2581381040\,x^8 + 7704021083264\,x^7 + 101567018399840\,x^6 - 96172789044745280\,x^5 \\ & - 1962596803409291000\,x^4 - 15122894980514300000\,x^3 + 266225999081701799000\,x^2 \\ & + 3116782046067938990000\,x + 191614097302577354466875 \end{aligned}$$
has Shioda invariants in the class $(0:1:0:1:0:0:0:0:0)$ for which the only non-zero determinants in the list of Lemma 3.13 are $R(C_{5,2},C_{6,2},C'_{9,2})$ and $R(C_{5,2},C_{6,2},C''_{9,2})$. These two discriminants are zero modulo 19 and 113 too, but then the automorphism group is larger than $\mathbf{C}_2$.
- Similarly, the singular form $8\,x^5z^3 - 125z^8$ has Shioda invariants in the class
$$(0:0:0:1:0:0:0:0:0)$$
(resp. $16\,x^7z - 35\,x^2z^6$, in the class $(0:0:0:1:0:0:0:0:3/32)$) for which 18 determinants in the list are zero in fields of characteristic 17 (resp. characteristic 13). Note that over $\mathbb{Q}$, these two forms already have 17 determinants in the list which are zero.

4. Field of moduli and field of definition

4.1. **Field of definition and field of moduli: general facts.** Let K be an algebraically closed field and let $k \subset K$ be a subfield. Let C be a curve defined over K of genus $g \geq 2$.

Definition 4.1. The *field of moduli* of C, denoted $\mathbf{M}_C$, is the subfield of K fixed by the set $\{\sigma \in \mathrm{Aut}(K),\ C \simeq {}^\sigma C\}$. We say that k is a *field of definition* of C if there exists a curve $\mathcal{C}/k$ such that $\mathcal{C}$ is K-isomorphic to C. The curve $\mathcal{C}/k$ is a model of C over k.

As shown in [31] (or [28, Th. 1.5.8]), $\mathbf{M}_C$ is a purely inseparable extension of the intersection of all the fields of definition of C.

A classical problem is to know whether $\mathbf{M}_C$ is a field of definition or if there is an obstruction. One finds several sufficient conditions in the literature. For instance, the moduli field $\mathbf{M}_C$ is a field of definition when C has no automorphism [17, Cor. 4.3]) or when K is the algebraic closure of a finite field [29, Cor. 2.11]. Another very useful criterion is the following construction from [17]. Assume now that $K/\mathbf{M}_C$ is a Galois extension and let $\Gamma = \mathrm{Gal}(K/\mathbf{M}_C)$. By definition of the field of moduli, for all $\sigma \in \Gamma$, there exists a K-isomorphism $F_\sigma : C \to {}^\sigma C$. Consider the curve $B = C/\mathrm{Aut}(C)$. The isomorphism F_σ induces an isomorphism $f_\sigma : B \to {}^\sigma C/\mathrm{Aut}({}^\sigma C) = {}^\sigma B$ and the diagram

$$\begin{array}{ccc} C & \xrightarrow{F_\sigma} & {}^\sigma C \\ \downarrow & & \downarrow \\ B & \xrightarrow{f_\sigma} & {}^\sigma B \end{array}$$

is commutative. Weil cocyle relations as in [51, proof of Th.1] imply that the curve B admits a model $\mathcal{B}$ over $\mathbf{M}_C$ and a K-isomorphism $\phi : B \to \mathcal{B}$ such that for all $\sigma \in \Gamma$, $f_\sigma = (\phi^{-1})^\sigma \circ \phi$.

Theorem 4.2 ([17, Cor. 4.3(c)],[29, Cor. 2.12])**.** *If $\mathcal{B}(\mathbf{M}_C) \neq \emptyset$ then $\mathbf{M}_C$ is a field of definition of C.*

The following result which is implicitly contained in [15] gives a sufficient condition for $\mathcal{B}(\mathbf{M}_C)$ to be non-empty.

Proposition 4.3. *With the same convention as for Fig. 1, let $S = (e_1^{n_1}, \ldots, e_t^{n_t})$ be the signature of the cover $C \to C/\mathrm{Aut}(C)$ where $e_1 < e_2 < \ldots < e_t$ are the ramification indices and n_i their multiplicity. If B is a genus 0 curve and at least one of the n_i is odd then the field of moduli is a field of definition.*

Proof. Let e_i be one of the ramification index with odd signature exponent n_i. Let $Z = \sum_{j=1}^{n_i} P_j \in \mathrm{div}(\mathcal{B})$ where P_j are the images of the n_i ramification points of $C \to C/\operatorname{Aut}(C)$ with index e_i. Since Galois action of Γ respect the ramification index, Z is a rational divisor of odd degree n_i. Therefore $D = Z + \lfloor n_i/2 \rfloor \mathcal{K}_{\mathcal{B}}$ (where $\mathcal{K}_{\mathcal{B}}$ is the canonical divisor of degree -2) is a rational degree one divisor, hence linearly equivalent to a rational point $P \in \mathcal{B}(\mathbf{M}_C)$. □

4.2. **The hyperelliptic case.** From now on, let K be an algebraically closed field of characteristic $p \neq 2$. Let $g \geq 2$ be an integer, $n = 2g + 2$ and let $f \in K[x]$ be a hyperelliptic polynomial of degree n. Let C be the hyperelliptic curve of genus g defined by the equation $y^2 = f(x)$. In the sequel we assume that K is a Galois extension of $\mathbf{M}_C$ and we denote $\Gamma := \mathrm{Gal}(K/\mathbf{M}_C)$.

The problem to know if the field of moduli is a field of definition has been first addressed by Mestre in [38] under the conditions that the the genus is even. Note that in this case, he showed [38, p. 322], that if C is defined over a field k, it has a hyperelliptic equation (in the sense of Section 1.2) over k. However, in general, this is not true and we will have to distinguish two problems: is the field of moduli a field of definition? And if so, has the model over the field of moduli a hyperelliptic equation? This motivates the following terminology.

Definition 4.4. A hyperelliptic curve C over a field k can be *hyperelliptically defined* over a subfield $k \subset K$ if there exists a model of C over k which has a hyperelliptic equation.

From the form of the isomorphisms between hyperelliptic equations and Weil cocycle relations, we get the following result.

Lemma 4.5. *C has a model over k if and only if there exists an open normal subgroup $H \subset \Gamma$ and for all $\sigma \in \Gamma$ $(M_\sigma, e_\sigma) \in (\mathrm{GL}_2(k'), k'^*)$ where $k' = K^H$ such that*

- *for $\sigma \in H$, $(M_\sigma, e_\sigma) \equiv (id, 1)$;*
- *for $\sigma \in \Gamma$, (M_σ, e_σ) is an isomorphism between C and ${}^\sigma C$;*
- *for all $\sigma, \tau \in \Gamma$, there exists $\lambda \in k'^*$ such that*

$$M_{\tau\sigma} = \lambda M_\tau^\sigma M_\sigma, \quad e_{\tau\sigma} = \lambda^{g+1} e_\tau^\sigma e_\sigma.$$

If we wish to obtain a model with a hyperelliptic equation, we get the following version of the lemma.

Lemma 4.6. *$C : y^2 = f(x)$ can be hyperelliptically defined over k if and only if there exists an open normal subgroup $H \subset \Gamma$ and for all $\sigma \in \Gamma$, a matrix $M_\sigma \in \mathrm{GL}_2(k')$ where $k' = K^H$ such that*

- *for all $\sigma \in H$, $M_\sigma = id$;*
- *for all $\sigma \in \Gamma$, there exists $\lambda_\sigma \in K^*$ such that $M_\sigma.f = \lambda_\sigma \cdot f^\sigma$.*
- *for all $\sigma, \tau \in \Gamma$,*

$$M_{\tau\sigma} = M_\tau^\sigma M_\sigma.$$

Proof. If C can be hyperelliptically defined over k, there exists a curve $\mathcal{C} : y^2 = \tilde{f}(x)$ with $\tilde{f} \in k[x]$, a finite Galois extension $k' = K^H$ over k and $(A, a) \in (\mathrm{GL}_2(k'), k'^*)$ such that (A, a) is a k'-isomorphism between C and $\mathcal{C}$. Define then $M_\sigma = (A^\sigma)^{-1} A$ and $e_\sigma = a/a^\sigma$. One can check that the (M_σ, e_σ) satisfy the hypotheses. Conversely, we can assume that H is such that the finite Galois extension $k' = K^H$ over k contains a splitting field of f. We denote by r_i the roots of f. Thanks to our hypotheses, we get that for $\sigma \in \Gamma$ and $h \in H$, $M_{\sigma h} = M_\sigma^h M_h = M_\sigma$. Hence the cocyle relations induce cocycle relations for $G = \Gamma/H$. Following the proof of Hilbert 90 as in [45, p. 159, Prop.3], we can then find a matrix $P \in M_2(k')$ such that the matrix

$$A = \sum_{\tau \in G} P^\tau M_\tau$$

is invertible. Now for any $\sigma \in G$ we get

$$A^\sigma = \sum_{\tau \in G} P^{\tau\sigma} M_\tau^\sigma = \left(\sum_{\tau \in G} P^{\tau\sigma} M_{\tau\sigma} \right) M_\sigma^{-1} = A M_\sigma^{-1}.$$

Let us denote $\tilde{r}_i = A.r_i$. For all $\sigma \in G$, letting $\sigma(\infty) = \infty$, since M_σ maps the set $\{r_i\}$ on $\{r_i^\sigma\}$ we get

$$\{\tilde{r}_i^\sigma\} = \{A^\sigma.r_i^\sigma\} = \{A M_\sigma^{-1}.r_i^\sigma\} = \{A.r_i\} = \{\tilde{r}_i\}.$$

Hence the polynomial $\tilde{f} = \prod(x - \tilde{r}_i) \in k[x]$ and the curve $\mathcal{C}/k : y^2 = \tilde{f}(x)$ is a model of C. □

Remark 4.7. The previous lemmas give an easy proof that for g even, C can be defined over k if and only if C can be hyperelliptically defined over k. Indeed, assuming the cocycle condition of Lemma 4.5 we can write

$$\det M_{\tau\sigma} = \lambda^2 (\det M_\tau)^\sigma (\det M_\sigma), \quad e_{\tau\sigma} = \lambda(\lambda^2)^{g/2} e_\tau^\sigma e_\sigma.$$

Hence we can obtain a good representative satisfying the cocycle condition of Lemma 4.6 letting

$$M'_\sigma = e_\sigma^{-1} \cdot (\det M_\sigma)^{g/2} \cdot M_\sigma.$$

Let now I_1 and I_2 be two homogeneous invariants of the same degree, of degree $2g+2$ binary forms, defined over the prime field of K and $I_2(f) \neq 0$. Their quotient $\iota = I_1/I_2$ satisfies for all $\sigma \in \Gamma$

$$\iota(f)^\sigma = \iota(f^\sigma) = \iota(M_\sigma.f) = \iota(f).$$

Hence $\iota(f) \in \mathbf{M}_C$. More specifically, we can prove the following result.

Proposition 4.8. *Let $\mathcal{J} = (I_1 : \ldots : I_m)$ be an m-uple of invariants of degree d_i, of degree n binary forms, and suppose each I_i is defined over the prime field of K. Then, there exists $\lambda \in K^*$ such that for $1 \leq i \leq m$, $I_i(f)/\lambda^{d_i} \in \mathbf{M}_C$.*

Proof. Let d be the gcd of the degree d_i of the invariants I_i which value at f is not zero. Then there exists $c_i \in \mathbb{Z}$ with $c_i = 0$ if $I_i(f) = 0$ such that $\sum c_i d_i = d$. We then define $I = \prod_i I_i^{c_i}$. From what we said above, the value $\mu_i = I_i(f)/I(f)^{d_i/d} \in \mathbf{M}_C$. If we let $\lambda = I(f)^{1/d}$ for any choice of a d-th root of $I(f)$ we get the result. □

Note that the corresponding representative $(I_1(f)/\lambda^{d_1}, \ldots, I_m(f)/\lambda^{d_m})$ for the m-uple of invariants is the one constructed in Section 1.3 and used in our algorithms.

Corollary 4.9. *With the notation of Section 2.2, there exists $\lambda \in K^*$ such that the change of variables $x_i = \lambda^{e_i} \cdot x'_i$ for some integers e_1, e_2, e_3 makes the conic $\mathcal{Q}$ and the curve $\mathcal{H}$ defined over $\mathbf{M}_C$.*

Proof. Thanks to Proposition 4.8 we can find $\lambda \in K^*$ for the uple of all the A_{ij} and h_I. Let d_1, d_2, d_3 be the degree of q_1, q_2 and q_3. From the formula for the coefficients A_{ij} and h_I, one sees easily that

$$\deg(A_{ij}) + \deg(x_i^*) + \deg(x_j^*) = 2(d_1 + d_2 + d_3)$$

is a constant c and

$$\deg(h_I) + \sum_{i \in I} \deg(x_i^*) = 1 + n/2 \cdot d_1 \cdot d_2 \cdot d_3$$

is a constant c'. Hence, if we make the change of variables $x_i = \lambda^{e_i} \cdot x'_i$ where $e_i = \deg(x_i^*)$, we get that

$$\sum A_{ij} \lambda^{\deg(x_i^*) + \deg(x_j^*)} x'_i x'_j = \lambda^c \cdot \sum \left[A_{ij} / \lambda^{\deg(A_{ij})} \right] x_i x_j$$

and similarly

$$\sum_I h_I x_I = \lambda^{c'} \cdot \sum \left[h_I / \lambda^{\deg(h_I)} \right] x'_I.$$

This gives the result. □

We then find a refinement of Proposition 2.3.

Proposition 4.10. *Let (q_1, q_2, q_3) be three covariants of order 2 for degree n binary forms and assume they are defined over the prime field of K. If $R(q_1, q_2, q_3)$ evaluated at a form f in non-zero, there exists a non-singular conic $\mathcal{Q}$ and a plane curve $\mathcal{H}$ of degree $n/2$ defined over $\mathbf{M}_C$ such that there is a K-isomorphism $\mathcal{Q} \to \mathbb{P}^1$ mapping the intersection points of $\mathcal{Q} \cap \mathcal{H}$ on the roots of $f(x, z)$. In particular the field of moduli is a field of definition if $\mathcal{Q}$ has an $\mathbf{M}_C$-rational point and in this case C can be hyperelliptically defined over $\mathbf{M}_C$.*

4.3. **The hyperelliptic case with no extra-automorphism.** Besides the hypotheses of Section 4.2, we assume that $\mathrm{Aut}(C) = \langle \iota \rangle$. In particular $C/\langle \iota \rangle = B$ is the genus 0 curve Q defined in Section 1.2.
Let D be the image of the ramification divisor W of C by the map $\phi \circ \rho : C \to B \to \mathcal{B}$. The divisor D is defined over $\mathbf{M}_C$. Indeed for any $\sigma \in \Gamma$

$$^{\sigma}D = \phi^{\sigma} \circ \rho^{\sigma}(^{\sigma}W) = \phi^{\sigma} \circ \rho^{\sigma}(F_{\sigma}(W)) = \phi^{\sigma} \circ f_{\sigma} \circ \rho(W) = \phi \circ \rho(W) = D.$$

Assume now that there exists $\Phi : C \to C'$ an isomorphism onto a model $C'/\mathbf{M}_C$ of C. Let Q' be the quotient of C' by the hyperelliptic involution and D' the image of the ramification divisor W' on C'. The induced K-isomorphism $\tilde{\Phi} : \mathcal{B} \to Q'$ maps the divisor D onto D'. Now for any $\sigma \in \Gamma$, we have $\tilde{\Phi}^{-1} \circ \tilde{\Phi}^{\sigma}(D) = D$. Since C has no extra-automorphism, this means that $\tilde{\Phi}^{-1} \circ \tilde{\Phi}^{\sigma} = \mathrm{id}$ hence $\tilde{\Phi}$ is defined over $\mathbf{M}_C$. Hence we get

Proposition 4.11. *The curve $\mathcal{B}$ has a rational point if and only if C can be hyperelliptically defined over $\mathbf{M}_C$.*

With the notation and hypotheses of Proposition 4.10, using $Q' = \mathcal{Q}$, we get a sufficient and necessary condition.

Corollary 4.12. *Let (q_1, q_2, q_3) be three covariants of order 2 for degree n binary forms and assume they are defined over the prime field of K. If $R(q_1, q_2, q_3)$ evaluated at a form f is non-zero, there exists a non-singular conic $\mathcal{Q}$ and a plane curve $\mathcal{H}$ of degree $n/2$ defined over $\mathbf{M}_C$ such that there is a K-isomorphism $\mathcal{Q} \to \mathbb{P}^1$ mapping the intersection points of $\mathcal{Q} \cap \mathcal{H}$ on the roots of $f(x, z)$. In particular the field of moduli is a field of definition if and only if $\mathcal{Q}$ has an $\mathbf{M}_C$-rational point and in this case C can be hyperelliptically defined over $\mathbf{M}_C$.*

Note that the equivalence does not hold if C has extra-automorphism (see Remark 4.21).

If 'to be defined' and 'to be hyperelliptically defined' over $\mathbf{M}_C$ are the same problem when g is even, it is not the case for odd genus. Indeed,

Proposition 4.13. *Let g be odd. Then $\mathbf{M}_C$ is a field of definition for C.*

Proof. Consider the rational canonical divisor κ on $\mathcal{B}$ of degree -2. It is the negative of the intersection of a line with a place model of $\mathcal{B}$. If $\mathbf{M}_C$ is finite, we get the result directly from Section 4.1. Hence we assume that $\mathbf{M}_C$ is infinite. We can find a line such that $\mathrm{Supp}(-\kappa) \cap \mathrm{Supp}(D) = \emptyset$. Since $\deg D = 2g + 2$, $D - 2 \cdot \frac{g+1}{2}(-\kappa)$ is a divisor of degree 0, it is the divisor of a function $u \in \mathbf{M}_C(\tilde{Q})$. If we consider the degree 2 extension of the form $z^2 = u$, this defines a hyperelliptic curve over $\mathbf{M}_C$ with the same ramification as C, hence C admits a model over $\mathbf{M}_C$ (note that the crucial fact is that each point in the divisor $2 \cdot \frac{g+1}{2}(-\kappa)$ has even multiplicity and hence does not contribute to the ramification). □

On the other hand, it is easy to exhibit examples for which $\mathbb{Q}$ is a field of moduli of a genus 3 curve C with no extra automorphism but C cannot be hyperelliptically defined over $\mathbb{Q}$. Indeed, consider the hyperelliptic genus 3 curve over $\mathbb{Q}$ which is a degree 2 cover of the conic

$$Q : x_1^2 + x_2^2 + x_3^2 = 0$$

ramified over the intersection points of Q and

$$H : x_2^4 + x_1 x_2^3 - (x_1^4 + x_1^3 x_3 + x_1^2 x_3^2 + x_1 x_3^3 + 2x_3^4) = 0.$$

The curve C has a hyperelliptic equation

$$y^2 = -x^8 + (2i + 2)x^7 - 8x^6 + (-2i - 6)x^5 - 14x^4 + (-2i + 6)x^3 - 8x^2 + (2i - 2)x - 1$$

over $\mathbb{Q}(i)$ and we can check using our programs that C has no extra-automorphism. Since $Q \simeq \mathcal{B}$ and $Q(\mathbb{Q}) = \emptyset$, Proposition 4.11 shows that C cannot be hyperelliptically defined over $\mathbb{Q}$.

4.4. **The hyperelliptic case with extra-automorphisms.** Besides the hypotheses of Section 4.2, we assume now that C has extra-automorphisms. In [29] and [28], the following results are proved.

Proposition 4.14 ([29, Th. 5.4], [28, Prop. 4.2.2])**.** *If* $\overline{\mathrm{Aut}}(C)$ *is not cyclic or is cyclic and of order divisible by* p *then* C *can be hyperelliptically defined over its field of moduli.*

Remark 4.15. In [21] and [22], one can find a family of hyperelliptic curves, among which the genus 5 curve

$$C : y^2 = (x^4 - 2\,(1 - 2\,\frac{r_3 - r_1}{r_3 - r_2}\,\frac{q_4 - r_2}{q_4 - r_1})\,x^2 + 1)\cdot \\ (x^4 - 2\,(1 - 2\,\frac{r_3 - r_1}{r_3 - r_2}\,\frac{q_5 - r_2}{q_5 - r_1})\,x^2 + 1)\cdot(x^4 - 2\,(1 - 2\,\frac{r_3 - r_1}{r_3 - r_2}\,\frac{q_6 - r_2}{q_6 - r_1})\,x^2 + 1)\,,$$

with $q_4 = 3, q_5 = -1, q_6 = 7$ and r_1, r_2, r_3 the conjugate roots of $X^3 - 3X + 1 = 0$ (these values of q_i are only to fix ideas). This curve was claimed to be a curve with automorphism group $(\mathbb{Z}/2\mathbb{Z})^3$, field of moduli $\mathbb{Q}$ but with no hyperelliptic equation over $\mathbb{Q}$, contradicting Huggins' general result without the respective authors being aware of it. It took us a long month of discussions to realize that there was a subtle gap on page 406 point d) of [21]: it is claimed there that a certain extension is Galois which is not always the case. It took us even longer to find an explicit hyperelliptic model of the curve over $\mathbb{Q}$ because, although the curve is defined over a cubic Galois extension of $\mathbb{Q}$, the $\overline{\mathbb{Q}}$-isomorphism we found between C and a model over $\mathbb{Q}$ is defined over a 12 degree extension of $\mathbb{Q}$. More recently, a faster and more systematic way to derive a hyperelliptic equation over the field of moduli is worked out in [35].

4.5. **The hyperelliptic case of genus 3.** Let now C be a genus 3 hyperelliptic curve. In this section, we want to address several issues which will be cut out according to the automorphism groups reviewed in Fig. 1.

Issue I.: Can we compute the automorphism group from the invariants?

Issue II.: Is the field of moduli automatically a field of definition?

Issue III.: Can the curve be always hyperelliptically defined over the field of moduli?

Issue IV.: Can we hyperelliptically reconstruct the curve from the invariants over K?

Issue V.: Can we reconstruct a model over the field of moduli when there is no obstruction?

Issue VI: Can we hyperelliptically reconstruct a model over the field of moduli when there is no obstruction?

Issue VII.: What is the number of $\overline{\mathbb{F}}_q$-isomorphism classes of hyperelliptic genus 3 curves with given automorphism group over a finite field $\mathbb{F}_q$?

The following table gather our state of knowledge (we **emphasize** what is proved in the present article). Note that the practical results are valid for $p = 0$ or $p \geq 11$.

#	Dim. 0	Dim. 1	$\mathbf{C}_2^3$	$\mathbf{C}_4$	$\mathbf{D}_4$	$\mathbf{C}_2$
I	yes	**yes**	**yes**	**yes**	**yes**	**yes**
II	yes	yes	yes	**yes**	no (counterex. exist)	**yes**
III	yes	yes	yes	**yes**	no	**computable** (possible theo. obstruction)
IV	yes	**yes**	**yes**	**yes**	**yes**	**yes**
V	yes	**yes**	yes (*see* [35])	**yes**	yes (*see* [34])	**yes**
VI	yes	**yes**	yes (*see* [35])	**yes**	yes (*see* [34])	**yes** **(if no theo. obstruction)**
VII	1	$\mathbf{q-3}$	$\mathbf{q^2-2q+2}$	$\mathbf{q^2-2q+2}$	q^3-2q^2+3 (unproven)	q^5-q^3+q-2 (unproven)

TABLE 5. Issues addressed in the present paper.

Curves in the strata of dimension 0 (cases 8,9,10 and 11 in Fig. 1) and of dimension 1 (by Proposition 4.14) are hyperelliptically defined over their field of moduli and we have explicit hyperelliptic equations over the field of moduli (see Lemmas 3.5 and 3.6). We thus focus on the strata $\mathbf{C}_2^3$, $\mathbf{C}_4$, $\mathbf{D}_4$ and $\mathbf{C}_2$.

Remark 4.16. Similar issues for genus 2 are completely solved by [11] (see also [10, Th. 5] for $p = 2$). In particular if the curve has extra-automorphism, then $\mathbf{M}_C$ is always a field of definition and moreover C can be hyperelliptically defined over $\mathbf{M}_C$. Actually, in [11] for the case of automorphism group $\mathbf{D}_4$, the authors assumed that $p \neq 2, 3, 5$. A careful analysis and some improvements made during the implementation of their work in MAGMA by the two authors removed this restriction (see [32]).

4.5.1. *Stratum* $\mathbf{C}_2^3$. By Proposition 4.14, we know that this case is hyperelliptically defined over its field of moduli. In Lemma 3.8, explicit equations for the stratum are given. Moreover an explicit hyperelliptic equation over an extension at most cubic of the field of moduli is given. To write a hyperelliptic equation over the field of moduli can be efficiently done following [35], as mentioned in the introduction.

Remark 4.17. Lemma 10 iv) of [27] pretends to give an equation of a model of C over the field of moduli when $\mathrm{Aut}(C) = \mathbf{C}_2^3$. Their method does not work in general as it can be easily checked on the genus 3 curve $y^2 = x^8 + ax^6 + bx^4 + ax^2 + 1$ where

$$a = (32\alpha^5 + 112\alpha^4 + 40\alpha^3 - 112\alpha^2 + 32\alpha + 92)/17, \quad b = (-304\alpha^5 - 752\alpha^4 + 160\alpha^3 + 1040\alpha^2 - 752\alpha - 554)/17$$

and α a root of $x^6 + 3x^5 + x^4 - 3x^3 + x^2 + 3x + 1 = 0$ in $\overline{\mathbb{Q}}$. This curve has Shioda invariants defined over $\mathbb{Q}$

$$j_2 = 0, j_3 = 0, j_4 = -25/98, j_5 = j_4, j_6 = -225/2744, j_7 = -25/1372, j_8 = -225/134456$$

but the equation given by Lemma 10 iv) is not defined over $\mathbb{Q}$.

4.5.2. *Stratum* $\mathbf{C}_4$. In Lemma 3.8 explicit equations for the stratum are exhibited. Moreover since the signature is $(2^3, 4^2)$, the following result is a consequence of Proposition 4.3.

Proposition 4.18. *Let C/k be a hyperelliptic curve of genus 3 with $\mathrm{Aut}(C) \simeq \mathbf{C}_4$. Then C can be defined over its field of moduli.*

Remark 4.19. Proposition 4.18 has no analogue for even genus greater than 3, since there can be an obstruction as shown in [28, Chap. 5].

Thanks to Lemma 3.8, the procedure is effective when $p \geq 11$ or $p = 0$. Indeed let $\{j_i\}$ be the Shioda invariants of such a curve C/k. In Lemma 3.8, it is proved that we can find three order 2 covariants q_i, such that $R(q_1, q_2, q_3)$ is non-zero. Now, we can use the first part of Proposition 4.10 to construct a conic $\mathcal{Q}$ and a quartic $\mathcal{H}$ over $\mathbf{M}_C$ such that there exists a K-isomorphism $\mathcal{Q} \to \mathbb{P}^1$ mapping the intersection divisor of $\mathcal{Q} \cap \mathcal{H}$ on the ramification divisor of C. Since $g = 3$ is odd, we can moreover proceed as in the proof of Proposition 4.13 and get a curve over $\mathbf{M}_C$, K-isomorphic to C. Hence C can be defined over its field of moduli. Moreover we can effectively construct a hyperelliptic equation over at most a quadratic extension of the field of moduli. Actually one can do better.

Proposition 4.20. *Let C/k be a hyperelliptic curve of genus 3 with $\mathrm{Aut}(C) \simeq \mathbf{C}_4$. Then C can be hyperelliptically defined over its field of moduli.*

Proof. By Proposition 4.18, we know that there is a model $\mathcal{C}$ of C over $\mathbf{M}_C$. Let $\mathcal{B} = \mathcal{C}/\langle\iota\rangle$ be seen as a plane non-singular conic. The signature of C singles out on $\mathcal{B}$ a degree 2 effective rational divisor Z. If the points of Z are rational then we are done since then $\mathcal{B} \simeq \mathbb{P}^1$. Otherwise, after a quadratic extension F of $\mathbf{M}_C$, there is a map $\phi : \mathcal{B} \to \mathbb{P}^1$ sending one of this point to 0 and the other to ∞. Since these points were branches of $\mathcal{C}/\mathcal{B}$, there exists a K-isomorphism Φ lifting ϕ such that the curve $D = \Phi(\mathcal{C})$ is of the form $y^2 = xg(x)$ with $g \in F[x]$ of degree 6. Moreover since there is an involution which fixes 0 and ∞ and which is then $x \mapsto -x$, the polynomial g has only even power monomials. Let σ be the Galois involution of $F/\mathbf{M}_C$. Since D has a model over $\mathbf{M}_C$, there exists a K-isomorphism $(M_\sigma, e_\sigma) : D \to {}^\sigma D$ and M_σ is actually given by $\phi^\sigma \circ \phi^{-1}$ and hence is defined over F. Since the isomorphism preserves the ramification indexes, M_σ maps $\{0, \infty\}$ onto $\{0, \infty\}$. It is then easy to see that M_σ is either the map $x \mapsto ax$ or $x \mapsto a/x$ for some $a \in F$. By Lemma 4.5, since there exists $\lambda \in F^*$ such that $M_\sigma^\sigma M_\sigma = \lambda \cdot \mathrm{id}$, we get in the first case $a = \lambda = 1$ (and we are done) and $a = a^\sigma$ in the later case and so $a \in \mathbf{M}_C$.

If $b=\sqrt{a}\notin F$, let $F'=F(b)$ and σ' and τ be the two generators of the $\mathbf{C}_2\times\mathbf{C}_2$ Galois extension $F'/\mathbf{M}_C$ defined by $\sigma'_{|F}=\sigma$, $b^{\sigma'}=b$ and $\tau_{|F}=\mathrm{id}$ and $b^\tau=-b$. We define

$$M'_{\sigma'}=\frac{1}{b}\cdot M_\sigma=\begin{bmatrix}0 & b\\ \frac{1}{b} & 0\end{bmatrix}\text{ and }M'_\tau=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}.$$

One can check that the conditions of 4.6 are satisfied.
If $b\in F$, then we define

$$M'_\sigma=\frac{1}{b}\cdot M_\sigma\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}0 & b\\ -\frac{1}{b} & 0\end{bmatrix}.$$

One can again check that the conditions of Lemma 4.6 are satisfied. □

The previous proof can be turned out into an effective method. Let assume that among the five determinants of Lemma 3.8, $R(C_{5,2},C_{6,2},C_{7,2})$ is not zero (the other cases are obtained by permutation). Then, due to the degree of the covariants and the action of $\mathbf{C}_4$, the conic and quartic have the following forms

$$\begin{aligned}\mathcal{Q} &: A_{11}x_1^2+A_{13}x_1x_3-A_{22}x_2^2-A_{33}x_3^2=0\,,\\ \mathcal{H} &: x_2\cdot(h_{11}x_1^3+h_{13}x_1^2x_3+h_{31}x_3^2x_1+h_{33}x_3^3+h_{12}x_1x_2^2+h_{32}x_2^2x_3)=0\,.\end{aligned}$$

By a linear change of variables in x_1 and x_3 we can assume that $A_{13}=0$ and $A_{11}=1$ and we write

$$\mathcal{Q}: x_1^2-ax_2^2+cx_3^2=0.$$

The conic and the quartic have the involution $(x_1:x_2:x_3)\mapsto(x_1:-x_2:x_3)$ which hence stabilizes the ramification divisor of C and is the involution of $\overline{\mathrm{Aut}}(C)$. The divisor $\{x_2=0\}\cap\mathcal{Q}$ is the fixed divisor Z of the proof. The points of Z are $(\pm\alpha:0:1)$ where α is a root of $X^2=c$. The isomorphism $\phi^{-1}:\mathbb{P}^1\to\mathcal{Q}$ is given by

$$(t:u)\mapsto(\alpha(at^2+u^2):2\alpha tu:u^2-at^2).$$

From this, we see that

$$M_\sigma=\phi^\sigma\circ\phi^{-1}=\begin{bmatrix}0 & a\\ 1 & 0\end{bmatrix}.$$

We can then apply the formula in the proof of Lemma 4.6 to get the result. As alternative, we have noticed that there is another choice of parameterization which only requires a quadratic extension and that we implemented. We normalize $\mathcal{Q}: ax_1^2-x_2^2+cx_3^2$ and parameterize the conic $\mathcal{Q}$ with respect to the point $(0:\sqrt{c}:1)$ by

$$(t:u)\mapsto(2\sqrt{c}tu:\sqrt{c}(at^2+u^2):at^2-u^2).$$

Plugging these expressions in $\mathcal{H}$ leads to a polynomial $g\in\mathbf{M}_C[x]$ times $\sqrt{c}$, which is what we need.

Remark 4.21. Note that contrary to the case with no extra-automorphism, it might happen that none of the conics $\mathcal{Q}$ contains arithmetic information, *i.e.* that all of them have no points over $\mathbf{M}_C$. In this way, for instance, we noticed that none of the non-degenerate conics among the 19 conics of Lemma 3.13 have a $\mathbb{Q}$-rational point for $(j_2:j_3:\ldots:j_9)=(1:0:6:0:6:0:2963/2835:0:2963/2835)$.

4.5.3. *Stratum* $\mathbf{D}_4$. In [28, Chap. 5], Huggins constructs curves

$$C: y^2=(x^2-a_1)(x^2+\frac{1}{\bar{a_1}})(x^2-a_2)(x^2+\frac{1}{\bar{a_2}})$$

with $a_1,a_2\in\mathbb{Q}(i)\setminus(\mathbb{Q}\cup i\mathbb{Q})$, $|a_i|>1$ and $|a_1/a_2|\neq 1$, which are defined over $\mathbb{Q}(i)$ with geometric group of automorphism $(\mathbb{Z}/2\mathbb{Z})^2$. By [29, Prop. 5.0.5], C has field of moduli $\mathbb{Q}(i)\cap\mathbb{R}=\mathbb{Q}$ but cannot be defined over $\mathbb{Q}$. Hence the field of moduli is not always a field of definition and there is not always a hyperelliptic equation over the field of moduli. However Lemma 3.10 gives explicit equations for the stratum and shows how to construct a hyperelliptic equation over an extension of the field of moduli of degree at most 8. Following [35], we even know how to descend this equation over some quadratic extension of the field of moduli thanks to some covariants. In a forthcoming article [34], we give a precise criterion to determine whether it is possible or not to finally descent over the field of moduli, and give an efficient descend algorithm when this is the case.

Remark 4.22. In [27, Cor. 11], it is asserted that as soon as $\#\,\mathrm{Aut}(C)>2$, the field of moduli of C is a field of definition which is obviously incorrect since it does not apply to Huggins' examples.

4.5.4. *Stratum* $\mathbf{C}_2$. This is the generic case for which we can apply the results of Section 4.3. Note that as we can always find a non-singular conic $\mathcal{Q}$ in this case, we can compute the obstruction using Corollary 4.12. When the obstruction is trivial, we apply Mestre's method to obtain a model with a hyperelliptic equation over the field of moduli.

4.6. **The case of curves over finite fields.**

Proposition 4.23. *Let C be a (hyperelliptic) curve of genus $g \geq 2$ defined over a finite field $k = \mathbb{F}_q$, such that all the $\bar{k}$-automorphisms of C are defined over k. Let k' be the extension of k of degree equal to the exponent e of* $\mathrm{Aut}(C)$. *Then there exists a k'-isomorphism from C to a curve defined over $\mathbf{M}_C$.*

Proof. Let $\mathcal{C}$ be a model of C over $\mathbf{M}_C$ and $\Phi : C \to \mathcal{C}$. We want to show that for the Frobenius automorphism $(x \mapsto x^{q^e}) = \tau \in \mathrm{Gal}(\bar{k}'/k')$ we have $\Phi^\tau = \Phi$. If $\gamma = x \mapsto x^q$, we have that $(\Phi^\gamma)^{-1} \circ \Phi = f \in \mathrm{Aut}(C)$. Since γ acts trivially on the automorphism group, we get

$$(\Phi^\tau)^{-1} \circ \Phi = ((\Phi^{\gamma^e})^{-1} \circ \Phi^{\gamma^{e-1}}) \circ \cdots \circ ((\Phi^\gamma)^{-1} \circ \Phi) = ((\Phi^\gamma)^{-1} \circ \Phi)^{\gamma^{e-1}} \circ \cdots \circ ((\Phi^\gamma)^{-1} \circ \Phi) = f \circ \cdots \circ f = 1.$$

□

Let us focus on the hyperelliptic case. Assume one knows how to compute a k'-isomorphism $F_\sigma : C \to {}^\sigma C$ for σ a generator of $\mathrm{Gal}(k'/\mathbf{M}_C)$ and that we know the automorphism of C explicitly. Two different F_σ differ by an automorphism of C, hence we have a finite explicit set $\mathcal{F}$ of k'-isomorphisms. If C is given by a hyperelliptic equation, we can represent all these morphisms by couple (M_σ, e_σ) and we will actually only care about the matrix M_σ.

Now pick one of the M_σ in $\mathcal{F}$. Let $m = \deg(k'/\mathbf{M}_C)$. If $M_\sigma^{\sigma^{m-1}} \cdots M_\sigma^\sigma \cdot M_\sigma \neq \lambda \cdot \mathrm{id}$ for $\lambda \in \mathbf{M}_C$ then pick another $M_\sigma \in \mathcal{F}$. Since there exists a k'-isomorphism from C to a model over $\mathbf{M}_C$, we know that there is at least one solution to the previous equation and the procedure produces a good M_σ and λ after a finite number of trials (less than $\#\overline{\mathrm{Aut}}(C)$). We let $M'_\sigma = \frac{1}{a} \cdot M_\sigma$ for a a solution of $\mathrm{Norm}_{k'/\mathbf{M}_C}(a) = \lambda$ (which always exists in a finite field). We can then apply the formula in the proof of Lemma 4.6

$$A = P + \sum_{i=1}^{m-1} P^{\sigma^i} \cdot M^{\sigma^i} \cdots M^\sigma \cdot M$$

for a random matrix $P \in M_2(k')$. We repeat this last part until we find A invertible. We can then apply A to the hyperelliptic polynomial of C to get a hyperelliptic equation defined over $\mathbf{M}_C$.

Remark 4.24. If C is non-hyperelliptic, we can assume that it is canonically embedded. Then, isomorphisms and automorphisms are given by $g \times g$-matrices and the same strategy can be applied.

As an application, we use the algorithms developed in this article to exhibit a hyperelliptic equation over $\mathbb{F}_p$, $p = 11, 13, \ldots, 47$, for all the $\overline{\mathbb{F}}_p$-isomorphism classes of hyperelliptic curves of genus 3.

As expected (*cf.* Tab. 5), we have obtained one model for each stratum of dimension 0, $p-3$ models for each stratum of dimension 1, $p^2 - 2p + 2$ models for each stratum of dimension 2, $p^3 - 2p^2 + 3$ models for the stratum $\mathbf{D}_4$, $p^5 - p^3 + p - 2$ models for the stratum $\mathbf{C}_2$, that is a total number of p^5 non-$\overline{\mathbb{F}}_p$-isomorphic curves as predicted in [7].

p	$\mathbf{C}_2 \times \mathbf{S}_4$	$\mathbf{V}_8$	$\mathbf{U}_6$	$\mathbf{C}_{14}$	$\mathbf{C}_2 \times \mathbf{D}_8$	$\mathbf{D}_{12}$	$\mathbf{C}_2 \times \mathbf{C}_4$	$\mathbf{C}_2^3$	$\mathbf{C}_4$	$\mathbf{D}_4$	$\mathbf{C}_2$	Total
11	10	8	6	2	60	48	32	368	202	4368	319458	324562
13	10	10	12	2	76	60	56	536	580	7448	738214	747004
17	10	14	12	2	108	84	80	968	1028	17352	2829918	2849576
19	10	8	6	2	124	96	64	1232	650	24560	4938514	4965266

TABLE 6. Number of $\mathbb{F}_p$-isomorphism classes of hyperelliptic curves of genus 3

Additionally, we have computed twists of these representatives and have obtained in this way hyperelliptic equation over $\mathbb{F}_p$ for all the $\mathbb{F}_p$-isomorphism classes of hyperelliptic curves of genus 3. We give the results

in Tab. 6 for $p = 11$, 13, 17, and 19. We can check that as predicted in [41], the total number of classes is equal to

$$2\,p^5 + 2\,p^3 - 2 - 2[p^2 - p]_{4|p+1} + 2[p-1]_{p>3} + [4]_{8|p-1} + [12]_{7|p-1} + [2]_{p=7} + [2]_{p\equiv 1,5 \bmod 12}$$

where the "$+[a]_{\text{ condition}}$" notation means add a if the "condition" is true.

References

[1] H. Babu and P. Venkataraman. Group action on genus 3 curves and their Weierstrass points. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 264–272. World Sci. Publ., Hackensack, NJ, 2005.

[2] Leonid Bedratyuk. On complete system of invariants for the binary form of degree 7. *Journal of Symbolic Computation*, 42:935, 2007.

[3] F. A. Bogomolov and P. I. Katsylo. Rationality of some quotient varieties. *Mathematics of the USSR-Sbornik*, 54:571–576, 1986.

[4] Oskar Bolza. On Binary Sextics with Linear Transformations into Themselves. *Amer. J. Math.*, 10(1):47–70, 1887.

[5] Rolf Brandt. *Über die Automorphismengruppen von algebraischen Funktionenkörpern*. PhD thesis, Universität Essen, 1988.

[6] Rolf Brandt and Henning Stichtenoth. Die Automorphismengruppen hyperelliptischer Kurven. *Manuscripta Math.*, 55(1):83–92, 1986.

[7] Bradley W. Brock and Andrew Granville. More points than expected on curves over finite field extensions. *Finite Fields Appl.*, 7(1):70–91, 2001. Dedicated to Professor Chao Ko on the occasion of his 90th birthday.

[8] A.E. Brouwer and M. Popoviciu. The invariants of the binary decimic, 2010. available on http://arxiv.org/abs/1002.1008.

[9] A.E. Brouwer and M. Popoviciu. The invariants of the binary nonic, 2010. available on http://arxiv.org/abs/1002.0761.

[10] G. Cardona, E. Nart, and J. Pujolàs. Curves of genus two over fields of even characteristic. *Math. Zeitschrift*, 250:177–201, 2005.

[11] G. Cardona and J. Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of aglebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83, Hackensack, NJ,, 2005. World Sci. Publ.

[12] Gabriel Cardona. On the number of curves of genus 2 over a finite field. *Finite Fields Appl.*, 9(4):505–526, 2003.

[13] A Clebsch. *Theorie der binären algebraischen formen*. Verlag von B.G. Teubner, Leipzig, 1872.

[14] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[15] Jean-Marc Couveignes. Calcul et rationalité de fonctions de Belyĭ en genre 0. *Ann. Inst. Fourier (Grenoble)*, 44(1):1–38, 1994.

[16] H. Croeni. *Zur Berechnung von Kovarianten von Quantiken*. PhD thesis, Univ. des Saarlandes, Saarbrücken, 2002.

[17] Pierre Dèbes and Michel Emsalem. On fields of moduli of curves. *J. Algebra*, 211(1):42–56, 1999.

[18] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[19] J. Dixmier. Quelques aspects de la théorie des invariants. *Gaz. Math., Soc. Math. Fr.*, 43:39–64, 1990.

[20] J. Dixmier and D. Lazard. Le nombre minimum d'invariants fondamentaux pour les formes binaires de degré 7. *Portugal. Math.*, 43(3):377–392, 1985/86.

[21] Y. Fuertes and G. González-Diez. Fields of moduli and definition of hyperelliptic covers. *Arch. Math. (Basel)*, 86(5):398–408, 2006.

[22] Yolanda Fuertes. Fields of moduli and definition of hyperelliptic curves of odd genus. *Arch. Math. (Basel)*, 95(1):15–81, 2010.

[23] W. D. Geyer. Invarianten binärer Formen. In *Classification of algebraic varieties and compact complex manifolds*, pages 36–69. Lecture Notes in Math., Vol. 412. Springer, Berlin, 1974.

[24] Paul Gordan. Beweis, dass jede Covariante und Invariante einer binren Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist. *Journal fr die reine und angewandte Mathematik*, (69):323–354, 1868.

[25] J.H. Grace and A. Young. *The algebra of invariants*. Chelsea publishing company, New-York, 1903.

[26] A. Grothendieck. *Revêtements étales et géométrie algébrique (SGA 1)*, volume 224 of *Lecture Notes in Math.* Springer-Verlag, Heidelberg, 1971.

[27] Jaime Gutierrez, D. Sevilla, and T. Shaska. Hyperelliptic curves of genus 3 with prescribed automorphism group. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 109–123. World Sci. Publ., Hackensack, NJ, 2005.

[28] B. Huggins. *Fields of moduli and fields of definition of curves*. PhD thesis, University of California, Berkeley, Berkeley, California, 2005. http://arxiv.org/abs/math.NT/0610247.

[29] B. Huggins. Fields of moduli of hyperelliptic curves. *Math. Res. Lett.*, 14(2):249–262, 2007.

[30] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. Math*, 72:612–649, 1960.

[31] Shoji Koizumi. The fields of moduli for polarized abelian varieties and for curves. *Nagoya Math. J.*, 48:37–55, 1972.

[32] R. Lercier and C. Ritzenthaler. Invariants and reconstructions for genus 2 curves in any characteristic, 2008. Available in MAGMA 2.15 and later, http://magma.maths.usyd.edu.au/magma/handbook/text/1367.

[33] R. Lercier and C. Ritzenthaler. Equations for the automorphism group stratification of the coarse moduli space of genus 3 hyperelliptic curves. *Journal of Algebra*, 2012. Available on http://www.journals.elsevier.com/journal-of-algebra/.
[34] R. Lercier, C. Ritzenthaler, and J. Sijsling. Explicit descent obstruction for genus 3 hyperelliptic curves. Preprint, August 2012.
[35] R. Lercier, C. Ritzenthaler, and J. Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit descent. In K. Kedlaya, editor, *Proceedings of the tenth Algorithmic Number Theory Symposium ANTS-X*. Mathematical Sciences Publishers, July 2012. To appear.
[36] Takashi Maeda. On the invariant field of binary octavics. *Hiroshima Mathematical Journal*, 20(3):619–632, 1990.
[37] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein. The locus of curves with prescribed automorphism group. *Sūrikaisekikenkyūsho Kōkyūroku*, (1267):112–141, 2002. Communications in arithmetic fundamental groups (Kyoto, 1999/2001).
[38] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry*, volume 94 of *Prog. Math.*, pages 313–334, Boston, 1991. Birkäuser.
[39] David Mumford and John Fogarty. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]*. Springer-Verlag, Berlin, second edition, 1982.
[40] E. Nart and D. Sadornil. Hyperelliptic curves of genus three over finite fields of characteristic two. *Finite Fields and Their Applications*, 10:198–220, 2004.
[41] Enric Nart. Counting hyperelliptic curves. *Adv. Math.*, 221(3):774–787, 2009.
[42] Claudio Procesi. *Lie groups*. Universitext. Springer, New York, 2007. An approach through invariants and representations.
[43] John F. X. Ries. Subvarieties of moduli space determined by finite groups acting on surfaces. *Trans. Amer. Math. Soc.*, 335(1):385–406, 1993.
[44] P. Roquette. Abschätzung der Automorphismenanzahl von Funktionenkörpern. *Math. Z.*, 117:157–163, 1970.
[45] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.
[46] Goro Shimura. On the field of rationality for an abelian variety. *Nagoya Math. J.*, 45:167–178, 1972.
[47] T. Shioda. On the graded ring of invariants of binary octavics. *American J. of Math.*, 89(4):1022–1046, 1967.
[48] David Singerman. Finitely maximal Fuchsian groups. *J. London Math. Soc. (2)*, 6:29–38, 1972.
[49] F. Von Gall. Das vollständige Formensystem der binären Form 7ter Ordnung. *Math. Ann.*, 31:318–336, 1888.
[50] Heinrich Weber. *Lehrbuch der Algebra, second ed., vol II*. Vieweg, Braunshweig, 1899.
[51] A. Weil. The field of definition of a variety. *American Journal of Mathematics*, 78:509–524, 1956.

DGA MI, La Roche Marguerite, 35174 Bruz, France.

Institut de recherche mathématique de Rennes, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France.
E-mail address: reynald.lercier@m4x.org

Institut de Mathématiques de Luminy, UMR 6206 du CNRS, Luminy, Case 907, 13288 Marseille, France.
E-mail address: ritzenth@iml.univ-mrs.fr