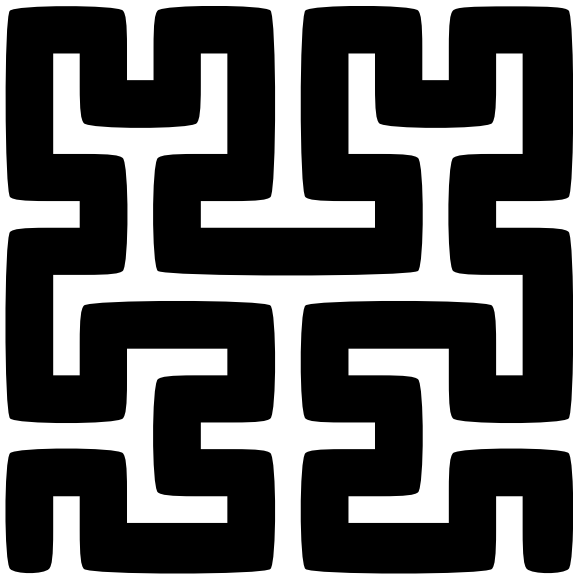

Polynesian Journal of Mathematics

Volume 3, Issue 3

Functionality for isomorphism classes of curves and hypersurfaces

Thomas Bouchet Reynald Lercier
Christophe Ritzenthaler Jeroen Sijsling

Received 6 Mar 2026
Revised 31 Aug 2026
Accepted 1 Sep 2026
Published 9 Sep 2026
Communicated by Gaetan Bisson
DOI: 10.69763/polyjmath.3.3

Polynesian Journal of Mathematics
Volume 3, Issue 3 (Sept. 2026)

Functionality for isomorphism classes of curves and hypersurfaces

Thomas Bouchet[1] Reynald Lercier[2]
Christophe Ritzenthaler[3] Jeroen Sijsling[4]

[1]Center for Systems Biology Dresden, Max-Planck Institute of Molecular Cell Biology and Genetics, Germany
[2]DGA & Université de Rennes, CNRS, IRMAR - UMR 6625, Rennes, France
[3]Université de Rennes, CNRS, IRMAR - UMR 6625, Rennes, France
[4]Institut für Algebra und Zahlentheorie, Universität Ulm, Germany

Abstract

We describe algorithms based on invariant theory to solve problems on the geometry of curves, mainly those of genus 2, 3, and 4. New theoretical results building on the first author's PhD thesis are also included.

Keywords: Plane quartic curves, hyperelliptic curves, invariants, reconstruction, descent, twists.

Introduction

This article originated in 2021 as a technical note intended to illustrate functions that complement those already available in Magma[1] as of version 2.28-27. Most of them were disseminated across previous articles; we gathered them into coherent packages for the convenience of users. These packages, together with a full description of the corresponding functions and options, can be found at [35] for the hyperelliptic case, at [36] for quartics, and at [5] for curves of genus 4.

A preliminary version of this work, authored by the last three authors, was uploaded to the arXiv but never published. In the meantime, the first author completed his PhD thesis in June 2025 and obtained results that significantly extend the previously available functionality. The present article therefore provides an updated overview of the current state of these developments. Some of the new results have been published in [6, 8], and only their algorithmic and implementation aspects are described here. However, the part of the thesis devoted to the computation of isomorphisms between hypersurfaces and its extension to handle the case of genus 4 curves have not yet appeared elsewhere; as it

[1]See: `https://magma.maths.usyd.edu.au/magma/handbook/hyperelliptic_curves`

constitutes a natural continuation of the earlier version, we include the corresponding proofs in this article. Hence, this article can be read at various levels: as a vademecum on how to use the corresponding Magma functions and their current limitations; as a research article with new theoretical or algorithmic results; as a source for open research questions. As a corollary, some sections may require more advanced knowledge than others and the sudden change of 'pace' may be troubling for the reader not familiar with the necessary concepts of invariant theory.

Our exposition begins in Section 1 with an overview of invariants and their role in classifying isomorphism classes of curves, both hyperelliptic and non-hyperelliptic, in genus 2 up to 4. Whereas the invariant theory of hyperelliptic curves was the subject of intense interest in the nineteenth century due to its relation with binary forms, methods for non-hyperelliptic curves are of more recent date, with the foundations for genus 3 (respectively 4) being laid in [14] (respectively [6]). After briefly touching upon the construction of these invariants, we turn to the problem of reconstruction.

The reconstruction of generic n-ary forms from their invariants is developed in [8]. This approach generalizes the reconstruction of hyperelliptic curves and non-hyperelliptic genus 3 curves from [34] and applies to cases that are beyond the reach of this algorithm. It also yields a complete explicit reconstruction algorithm for generic curves of genus 4. Finally, we present new tools for the efficient reconstruction of hyperelliptic curves of genus up to 4.

In Section 2, we address the explicit construction of isomorphisms between given curves. We describe new methods for computing isomorphisms between generic hypersurfaces; in particular, this yields a useful criterion for detecting when a hypersurface has trivial automorphism group (Proposition 2.3). Via the correspondence with binary forms, we also obtain a new efficient method for determining isomorphisms of hyperelliptic curves. These ideas culminate in an effective algorithm for determining isomorphisms of generic hyperelliptic or non-hyperelliptic genus 4 curves. Applications to automorphisms and twists over finite fields are discussed as well.

Appendix A contains Table 3, which illustrates the computational performance of our algorithms. Finally, Appendix B contains an unpublished theoretical result from the first author which allows to certify that the reduction of the Dixmier–Ohno invariants is still a generating set of the invariant ring of ternary quartic forms in characteristic greater than 13.

Table 1 summarizes the state of the main algorithms around rings of invariants, reconstruction, and isomorphisms, in various special cases and genera; in particular, this schematic overview pinpoints the new contributions in this article in lower genus.

Some of the new contributions in Table 1 are for now limited to the case of characteristic 0 and suitably generic curves. In practice, this genericity does allow one to deal with the vast majority of such curves. Still, many questions remain, not the least of which is the generalization of these reconstruction methods to arbitrary (not necessarily generic) curves. We have made an overview of those open problems that strike us as particularly intriguing in the following list.

	INVARIANTS	RECONSTRUCTION	ISOMORPHISMS
Hyperelliptic $g \leqslant 4$	Classical (§ 1.1)	New refinement of Mestre (§ 1.4)	New binary forms method (§ 2.2)
Non-hyp. $g = 3$	Dixmier–Ohno (§ 1.2)	New hypersurface method (§ 1.5)	New hypersurface method (§ 2.3)
Non-hyp. $g = 4$	First author [6]	First author [8]	New description (§ 2.4)

Table 1: Main algorithms around rings of invariants, reconstruction, and isomorphisms.

From generic reconstruction to all curves of a given genus (already in characteristic 0):

- In genus 3: reconstruction of all plane quartics with automorphism group either trivial, C_2 or V_4.
- In genus 4: reconstruction of all curves with trivial automorphism group.
- In genus 4, to go further one would already need to figure out models for the different automorphisms strata of genus 4 curves, and find the corresponding equations in the moduli space.
- After solving the previous problem, implement a reconstruction algorithm for curves of genus 4 with non-trivial automorphism group.

Questions in positive characteristic:

- Find separating invariants for the invariant ring of binary octic forms in characteristic 5.
- Prove that the separating invariants for the invariant ring of binary octic forms in characteristic 3 and 7 (and 5?) are generators.
- Reconstruct genus 3 hyperelliptic curves from a list of invariants (or separating invariants) in characteristic 5.
- Prove that the reductions of the Dixmier–Ohno invariants are still generators for the invariant ring if the characteristic of the residue field is 11, or 13.
- Prove the correctness of the conjectural homogeneous systems of parameters from [30] in characteristic 3.
- Determine generators for the ring of invariants of plane quartics in small characteristic.
- Work out a reconstruction process for generic plane quartics in characteristic 2 or 3.
- Find homogeneous systems of parameters in all characteristics for the ring of invariants for genus 4 curves lying on a smooth quadric.
- Find homogeneous systems of parameters in all characteristics for the ring of invariants for genus 4 curves lying on a quadric cone.

Notation

In this article, k denotes an algebraically closed field of characteristic $p \geqslant 0$, whereas K denotes any field.

1 Invariants and reconstruction

Since the nineteenth century, the isomorphism classes of certain algebraic varieties, notably hyperelliptic curves, have been studied through the theory of classical invariants, e.g. binary forms under the action of the linear group. More generally, for most hypersurfaces, isomorphisms are induced by linear maps of the ambient projective space, even in positive characteristic. Notably:

- Following the proof of [38], in any characteristic, isomorphisms between projective hypersurfaces of dimension at least 2 are linear, with the exception of some quartic surfaces.
- For plane curves, this is also the case with the exception of plane cubics using for instance [2, Exercise 18, page 56].

The ring of invariants of these objects under the action of the linear group is known to be finitely generated. However, explicit generators are known only in a small number of cases, especially when the characteristic of the base field is not zero.

Section 1.1 discusses the rings of invariants of hyperelliptic curves of genus up to 4, with some emphasis on the cases of positive characteristic. The cases of smooth non-hyperelliptic curves of genus 3 and 4 are considered in Section 1.2.

Conversely, given an isomorphism class characterized by its invariants, one can ask for an explicit representative curve, if possible defined over the field generated by these invariants. This question is called *reconstruction* (from the invariants). A general framework for addressing this question, first introduced in [8], is summarized in Section 1.3. Concrete algorithms are considered in Section 1.4 for hyperelliptic curves of small genus and in Section 1.5 for non-hyperelliptic genus 3 and 4 curves.

For background on invariant theory, including standard terminology and algorithms for the construction of invariants, we refer the reader to [42, 15, 48]. Basic definitions and properties of invariants and their generalizations (covariants and contravariants) are not recalled here.

1.1 Invariants: hyperelliptic curves of small genus

Here, we assume that the characteristic p of k is different from 2. The case $p = 2$ requires separate treatment and will be addressed when possible. Let C be a hyperelliptic curve of genus $g \geqslant 2$ over k given by an affine model $y^2 = f(x)$ where f is a separable polynomial of degree $2g + 1$ or $2g + 2$.

The isomorphism class of C corresponds to the orbit of the binary form $z^{2g+2} f(x/z)$ under the classical action of $\mathrm{GL}_2(k)$. As explained in [17, § 10.2], since the ring of polynomial functions on the space $\mathrm{Sym}^{2g+2}(k^2)$ of binary forms of degree $2g + 2$ is

described by $\bigoplus_n \mathrm{Sym}^n(\mathrm{Sym}^{2g+2}(k^2))$ as an SL_2-representation, one can characterize these orbits by the invariant space $\mathrm{Proj}(R_g(k))$, where

$$R_g(k) = \left(\bigoplus_{n\geqslant 0} \mathrm{Sym}^n\left(\mathrm{Sym}^{2g+2}(k^2)\right)\right)^{\mathrm{SL}_2(k)}.$$

Note that $\mathrm{SL}_2(k)$ is used instead of $\mathrm{GL}_2(k)$ as we only care about the action on the form up to a multiplicative scalar; indeed, since the elements λ in the center of $\mathrm{GL}_2(k)$ scale invariants by a factor $\lambda^{(2g+2)n}$, this restriction and the use of the corresponding projective space are essential for there to be a non-trivial space of invariants at all.

Working out generators for the invariant algebra $R_g(\mathbb{C})$ was a major topic of interest among nineteenth-century mathematicians. For $g = 2$, corresponding to binary sextics, such generators already appear in the work of Clebsch [10], whereas for $g = 3$, that is, binary octics, they go back to [44, 50]. More recently, the case $g = 4$ was settled by Brouwer and Popoviciu [9], although substantial progress had already been made during the nineteenth century [44].

When the characteristic p is positive, the situation becomes more delicate. In order to obtain a set of generators for $R_g(k)$, a good starting point is often to reduce a set of well-normalized generators of $R_g(\mathbb{C})$ modulo p. Here, well-normalized means that the invariants are primitive $\mathbb{Z}$-integral polynomials in the coefficients of a generic form; such a normalization is always possible by [46, Lemma 5.8.1]. Unfortunately, there is currently no general criterion to ensure that the reduced invariants still generate the full invariant ring. In fact, counterexamples are known: for instance $g = 3$ and $p = 5$ [3].

Let us give some details on the implementations available in Magma for the cases $g = 2$, 3, and 4. In all cases, the output invariants should be interpreted as points in a weighted projective space. They can be normalized and compared using the option `normalize := true`, which relies on the techniques of [31, Section 1.4].

Genus 2. The algebra $R_2(\mathbb{C})$ is generated by invariants I_2, I_4, I_6, I_{10} which are algebraically independent, together with an invariant I_{15} such that $I_{15}^2 \in \mathbb{Z}[I_2, I_4, I_6, I_{10}]$. While I_{15} is useful for classifying binary sextic forms up to SL_2-equivalence, it becomes irrelevant in the classification of genus 2 curves, which considers such forms up to a scalar instead. Algebraically, this is reflected in the fact that $\mathrm{Proj}\, R_2$ remains identical when restricting to invariants of even degree; also see the discussion before Example 1.3.

Igusa [27] managed to give a "universal set of invariants" for genus 2 curves that works in all characteristics, including 2. This set $\{I_2, I_4, I_6, I_8, I_{10}\}$ (with I_8 being superfluous beyond characteristic 2) is integrated in Magma via the function `IgusaInvariants()`.[2] The invariant I_{15} is not computed unless the option `extend` is set to `true`.

Genus 3. Using the work of Geyer [22], it was shown in [31] that the reductions modulo p of Shioda generators for $R_3(\mathbb{C})$ remain generators[3] for $R_3(k)$ whenever $p > 7$.

[2] There are also other sets of invariants (`IgusaClebschInvariants()`, `ClebschInvariants()`) and absolute invariants (`G2Invariants()`), which are used for historical or practical reasons.

[3] Note that [31, Proposition 1.9] should have included a different proof of [45, Lemma 1] to be complete, as the one in *loc. cit.* is only valid in characteristic 0. The missing argument can be found in [47, Proposition 5.5.2].

For characteristics $p = 2$, 3, and 7, Basson [3] constructed sets of *separating invariants* (i.e. invariants that need not generate the full invariant ring but still separate the orbits of the binary forms, and therefore characterize the isomorphism classes). This list depends on the characteristic and for $p = 2$ on the type defined in [40] or [3, Appendix]. For $p = 5$, the algorithms return a minimal list of invariants that generates the largest subring of invariants currently known to us.

All these variants are accessed in Magma through the function `ShiodaInvariants()`. When the option `PrimaryOnly := true` is used, the output restricts to a homogeneous system of parameters (HSOP) in any characteristic different from 2 (in characteristic 2, we only conjecture that the result is a HSOP).

Genus 4. Brouwer and Popoviciu [9] showed that $R_4(\mathbb{C})$ admits a minimal set of generators of size 106. These invariants are available in Magma via the function `BrouwerPopoviciuInvariants()`, from the GitHub repository [5]. To the authors' knowledge, no systematic study of the invariant ring of genus-4 hyperelliptic curves in positive characteristic was carried out so far.

1.2 Invariants: non-hyperelliptic curves of genus 3 and 4

Isomorphisms of non-hyperelliptic curves of genus 3 over an algebraically closed field k, represented by smooth plane quartics, are induced by linear transformations of the ambient projective plane $\mathbb{P}^2$. Accordingly, isomorphism classes are characterized by the space $\mathrm{Proj}(R(k))$, where

$$R(k) = \bigoplus_{n \geqslant 0} \left(\mathrm{Sym}^n \left(\mathrm{Sym}^4(k^3) \right) \right)^{\mathrm{SL}_3(k)}$$

is a graded ring of invariants under the classical action of $\mathrm{SL}_3(k)$, this time of the graded vector space of polynomial functions on the space $\mathrm{Sym}^4(k^3)$ of ternary quartic forms, the degree-n component of the latter being $\mathrm{Sym}^n(\mathrm{Sym}^4(k^3))$.

When k is of characteristic 0, Dixmier [14] gave a list of 7 invariants which form a homogeneous system of parameters for $R(k)$. It was completed by Ohno [41], who provided a full set of 13 generators for the invariant ring. These invariants are polynomials in the 15 coefficients of a ternary quartic form, with coefficients in $\mathbb{Z}[1/6]$.

They can be viewed in a weighted projective space with weights 3, 6, 9, 9, 12, 12, 15, 15, 18, 18, 21, 21, and 27. The corresponding functionality was implemented in Magma for the first time in [23]. The current function is called `DixmierOhnoInvariants()`, and differs from the earlier implementations only by normalization constants. The original normalization from [23] can be recovered by setting the option `IntegralNormalization := true`. Normalized representatives, for which equality suffices to test geometric isomorphism, can be obtained using the option `normalize := true`.

Remark 1.1. Among the Dixmier–Ohno invariants of a ternary quartic form $f(x, y, z)$, the invariant I_{27} of degree 27 plays a distinguished role. One checks that $(1/2^{40})I_{27}$ has integral coefficients and that, over any field, its vanishing locus coincides with the locus of singular plane quartics.

Unlike for Igusa's invariant I_{10}, which has similar properties, it is foolhardy to try and store an explicit expression of the Dixmier–Ohno invariant I_{27}. Instead, it is calculated separately for any concrete given plane quartic, classically as the resultant of the three partial derivatives of f, following [24, page 426]. This approach fails in characteristic 2 for intrinsic reasons, and may have additional issues in characteristic 3. In these cases, we instead compute the resultant of the partial derivatives of f with respect to two variables and of the polynomial f itself. This method is based on ideas and programs kindly provided by Laurent Busé and relies on the techniques developed in [4, Definition 4.6, Proposition 4.7] or [13, Proposition 11] and [28, Section 3.11.19.25].

This computation introduces an extraneous factor corresponding to the discriminant of the binary form $f|_{z=0}$. To eliminate this factor, we deform f to $f + \varepsilon(x^4 + y^4)$ in characteristic different from 2 and to $f + \varepsilon(x^4 + xy^3 + y^4)$ in characteristic 2. The discriminant of this family is then computed and specialized at $\varepsilon = 0$.

In his thesis [7], the first author proved that, when k is of characteristic $p > 13$, the reductions modulo p of the Dixmier–Ohno invariants remain generators of $R(k)$. The proof relies on the theory of *good modules* [19, 16], together with the results of [30], where homogeneous systems of parameters are determined in all characteristics except 3 (for which only a conjectural HSOP involving an invariant of degree 81 is proposed). The proof of this result is given in the Appendix B. We conjecture that the Dixmier–Ohno invariants also generate $R(k)$ after reduction modulo primes in the range $7 < p \leqslant 13$. As in the case of Shioda invariants in characteristic 5, a call to `DixmierOhnoInvariants()` in arbitrary characteristic returns a minimal set of invariants generating the largest subring of invariants currently known.

Invariants that classify non-hyperelliptic curves of genus 4 were worked out by the first author [6]. Such curves lie on a quadric, and depending on whether that quadric is smooth or a cone, one gets either a set of 65 invariants (in the smooth case) or 60 invariants. An implementation is available in the package [5]. In particular, a call to the function `InvariantsGenus4Curves()` on a smooth canonically embedded curve of genus 4 returns its associated invariants.

1.3 Reconstruction: general philosophy

Let V be a finite-dimensional vector space over an algebraically closed field k, and let $G \subset \mathrm{GL}(V)$ be a reductive algebraic group acting linearly on V. Denote by R the ring of invariant polynomial functions on V. Since invariants in R enable one to classify elements in V up to the action of G, they allow us to distinguish different orbits in V but do not, in general, provide a canonical representative of each orbit. This leads to the converse question, called *reconstruction from invariants*: given a point in the space of G-orbits in V, can we find a concrete element of V that corresponds to it, up to G-equivalence?

In his thesis [7], the first author generalizes earlier reconstruction algorithms for hyperelliptic and non-hyperelliptic curves, and includes them as special cases of reconstruction for hypersurfaces. This is explained in detail in [8]. Here, we summarize the general strategy and discuss its consequences for some families of curves. It draws inspi-

ration from Mestre's work on binary forms of even degree [37], itself based on formulae given in [10, § 103]. The method uses the notion of contravariant, a natural extension of invariants, and consists in constructing suitable linear bases of contravariants combined with a Taylor-like formula, to produce a collection of polynomials in a larger ambient space, given by the Veronese embedding of the hypersurface. The coefficients of the polynomials defining this embedding are expressed in terms of SL_n-invariants, and one can generically[4] recover from this collection a single polynomial in the GL_n-equivalence class characterized by the initial invariants. By varying the basis of contravariants, one can cover new cases and reduce the remaining ones to small-dimensional families for which *ad hoc* methods may be applied.

When the arity and degree of the form are coprime, the reconstruction simplifies considerably: a single polynomial is produced, which is GL_n-equivalent to the original one. In this situation, the coefficients of the reconstructed polynomial are invariants, and therefore belong to the field of moduli[5] of the corresponding geometric object. This yields an explicit birational inverse to the quotient map that sends a closed orbit to its invariants. Note that this inverse is defined on an open set, which excludes the locus of curves that are not defined over their field of moduli.

Example 1.2 ([8, Corollary 6.4.3]). As an illustration, we give an explicit expression for all smooth cubic surfaces with trivial automorphism group in terms of their Clebsch–Salmon invariants $(I_8, I_{16}, I_{24}, I_{32}, I_{40})$. The presence of automorphisms is detected by a unique invariant of degree 100, which also appears (up to a constant) as the vanishing of the determinant associated with the four generically linearly independent contravariants of order 1. Using the reconstruction process described above, one obtains the polynomial of Figure 1.

1.4 Reconstruction: hyperelliptic curves of genus 2, 3, and 4

In the case of hyperelliptic curves defined over a field k of characteristic $p \neq 2$, the reconstruction strategy specializes to Mestre's method which we summarize here.

Given the values $\underline{I}$ of a set of generators for the invariants of a hyperelliptic curve C of genus g, the reconstruction algorithm produces a conic and a plane curve of degree $g+1$, both defined over the field K generated over the prime field by the invariants. Their intersection points are precisely the Weierstrass points of C and therefore determine its geometric isomorphism class. By parametrizing the conic, possibly over a quadratic extension of K, one can recover a model of C in the usual form $y^2 = f(x)$.

In order to obtain such a model defined over K itself, one needs to find a K-rational point on the conic.[6] In the sequel, we refer to fields for which Magma can perform this step as *computable fields*.

[4] Precisely when the specialization of the basis of contravariants at the set of invariants remains linearly independent.

[5] There are several possible definitions of the field of moduli. They coincide when the base field is perfect; see [31, Section 4].

[6] Note that if such a point exists, then K is a field of definition of C, but the converse does not hold in general; see [31, Section 4].

$$
\begin{aligned}
f = {} & \big(- I_8^3 I_{16} + I_8^2 I_{24} + 200 I_{16} I_{24} + 35 I_8 I_{32} + 100 I_{40}\big) X^3 \\
& + \big(24 I_8^2 I_{16}^2 - 6 I_8 I_{16} I_{24} + 90 I_{24}^2 - 6 I_8^2 I_{32} - 180 I_{16} I_{32} - 30 I_8 I_{40}\big) X^2 Y \\
& + \big(- 12 I_8^2 I_{16} I_{24} + 18 I_8 I_{24}^2 + 240 I_{24} I_{32} + 45 I_8^2 I_{40} - 2400 I_{16} I_{40}\big) X^2 Z \\
& + \big(- 18 I_8^2 I_{24}^2 + 1200 I_{16} I_{24}^2 + 36 I_8^2 I_{16} I_{32} - 24 I_8 I_{24} I_{32} - 720 I_{32}^2 + 9 I_8^3 I_{40} \\
& \qquad - 360 I_8 I_{16} I_{40} + 960 I_{24} I_{40}\big) X^2 T \\
& + \big(- 192 I_8 I_{16}^3 - 216 I_{16}^2 I_{24} - 9 I_8 I_{24}^2 + 66 I_8 I_{16} I_{32} + 60 I_{24} I_{32} + 9/2 I_8^2 I_{40} - 60 I_{16} I_{40}\big) X Y^2 \\
& + \big(192 I_8 I_{16}^2 I_{24} + 96 I_{16} I_{24}^2 - 48 I_8 I_{24} I_{32} - 120 I_8 I_{16} I_{40} - 600 I_{24} I_{40}\big) X Y Z \\
& + \big(48 I_8 I_{16} I_{24}^2 + 360 I_{24}^3 - 576 I_8 I_{16}^2 I_{32} - 528 I_{16} I_{24} I_{32} + 144 I_8 I_{32}^2 - 24 I_8^2 I_{16} I_{40} \\
& \qquad - 1920 I_{16}^2 I_{40} - 372 I_8 I_{24} I_{40}\big) X Y T \\
& + \big(- 48 I_8 I_{16} I_{24}^2 - 144 I_{24}^3 + 480 I_8 I_{24} I_{40} + 1800 I_{32} I_{40}\big) X Z^2 \\
& + \big(- 144 I_8 I_{24}^3 + 288 I_8 I_{16} I_{24} I_{32} + 384 I_{24}^2 I_{32} + 72 I_8^2 I_{24} I_{40} - 8640 I_{16} I_{24} I_{40} \\
& \qquad - 480 I_8 I_{32} I_{40} - 2400 I_{40}^2\big) X Z T \\
& + \big(2400 I_{16} I_{24}^3 + 312 I_8 I_{24}^2 I_{32} - 432 I_8 I_{16} I_{32}^2 - 1056 I_{24} I_{32}^2 - 2640 I_8 I_{16} I_{24} I_{40} \\
& \qquad + 2640 I_{24}^2 I_{40} - 156 I_8^2 I_{32} I_{40} - 5280 I_{16} I_{32} I_{40} - 600 I_8 I_{40}^2\big) X T^2 \\
& + \big(512 I_{16}^4 + 22 I_{16} I_{24}^2 - 244 I_{16}^2 I_{32} + 20 I_{32}^2 - 11 I_8 I_{16} I_{40} - 16 I_{24} I_{40}\big) Y^3 \\
& + \big(- 768 I_{16}^3 I_{24} - 36 I_{24}^3 + 264 I_{16} I_{24} I_{32} + 480 I_{16}^2 I_{40} + 18 I_8 I_{24} I_{40} - 120 I_{32} I_{40}\big) Y^2 Z \\
& + \big(- 432 I_{16}^2 I_{24}^2 + 2304 I_{16}^3 I_{32} + 228 I_{24}^2 I_{32} - 792 I_{16} I_{32}^2 + 216 I_8 I_{16}^2 I_{40} - 144 I_{16} I_{24} I_{40} \\
& \qquad - 114 I_8 I_{32} I_{40} - 120 I_{40}^2\big) Y^2 T \\
& + \big(384 I_{16}^2 I_{24}^2 - 96 I_{24}^2 I_{32} - 240 I_{16} I_{24} I_{40} + 600 I_{40}^2\big) Y Z^2 \\
& + \big(192 I_{16} I_{24}^3 - 2304 I_{16}^2 I_{24} I_{32} + 576 I_{24} I_{32}^2 - 96 I_8 I_{16} I_{24} I_{40} - 1488 I_{24}^2 I_{40} \\
& \qquad + 1440 I_{16} I_{32} I_{40} + 360 I_8 I_{40}^2\big) Y Z T \\
& + \big(360 I_{24}^4 - 816 I_{16} I_{24}^2 I_{32} + 3456 I_{16}^2 I_{32}^2 - 864 I_{32}^3 - 2880 I_{16}^2 I_{24} I_{40} - 360 I_8 I_{24}^2 I_{40} \\
& \qquad + 408 I_8 I_{16} I_{32} I_{40} + 1344 I_{24} I_{32} I_{40} + 90 I_8^2 I_{40}^2 - 2400 I_{16} I_{40}^2\big) Y T^2 \\
& + \big(- 64 I_{16} I_{24}^3 + 400 I_{24}^2 I_{40} + 200 I_8 I_{40}^2\big) Z^3 \\
& + \big(- 288 I_{24}^4 + 576 I_{16} I_{24}^2 I_{32} + 144 I_8 I_{24}^2 I_{40} - 960 I_{24} I_{32} I_{40} + 9600 I_{16} I_{40}^2\big) Z^2 T \\
& + \big(1248 I_{24}^3 I_{32} - 1728 I_{16} I_{24} I_{32}^2 - 10560 I_{16} I_{24}^2 I_{40} - 624 I_8 I_{24} I_{32} I_{40} + 2880 I_{32}^2 I_{40} \\
& \qquad + 2400 I_8 I_{16} I_{40}^2 - 4800 I_{24} I_{40}^2\big) Z T^2 \\
& + \big(1600 I_{16} I_{24}^4 - 1952 I_{24}^2 I_{32}^2 + 1728 I_{16} I_{32}^3 - 1600 I_8 I_{16} I_{24}^2 I_{40} + 2240 I_{24}^3 I_{40} \\
& \qquad + 1280 I_{16} I_{24} I_{32} I_{40} + 976 I_8 I_{32}^2 I_{40} + 400 I_8^2 I_{16} I_{40}^2 - 12800 I_{16}^2 I_{40}^2 \\
& \qquad - 1120 I_8 I_{24} I_{40}^2 + 320 I_{32} I_{40}^2\big) T^3 .
\end{aligned}
$$

Figure 1: Reconstructed polynomial for all smooth cubic surfaces with trivial automorphism group in terms of their Clebsch–Salmon invariants $(I_8, I_{16}, I_{24}, I_{32}, I_{40})$.

Genus 2. For $g = 2$, using the work of [12, 11], reconstruction is available over any computable field, including characteristic 2, and applies to all hyperelliptic curves of genus 2. The corresponding functionality is implemented in Magma under the name `HyperellipticCurveFromIgusaInvariants()`.

Genus 3. Reconstruction over computable fields of characteristic $p > 7$ was implemented in [31] and applies to *all* hyperelliptic curves of genus 3. Thanks to the work of Basson [3], reconstruction from separating invariants is also available over any computable field of characteristic different from 5. The corresponding function is called `HyperellipticCurveFromShiodaInvariants()`.

Genus 4. Reconstruction has been worked out by the first author for generic curves in characteristic 0, using three generically linearly independent covariants of order 2. The corresponding function is called `HyperellipticCurveFromBrouwerPopoviciuInvariants()`. This function works over fields of characteristic $p > 6263$, although this bound could be largely improved.

Over $\mathbb{Q}$, the size of the coefficients in the output of the reconstruction can be significantly reduced using methods developed by Stoll [21], implemented in the function `MinRedBinaryForm`. Additionally, for the cases $g = 2$ and $g = 3$, we speed-up the reconstruction itself. This optimization was first introduced for $g = 3$ in [29, Section 3.1], using a technique based on a so-called "variation of conics", which accelerates the search for a rational point on the conic arising in the reconstruction procedure. Developing an analogous technique for $g = 2$ turns out to be more subtle, and we briefly explain the necessary adjustments as they have not been written anywhere else.

For the usual choices of order 2 covariants used in the reconstruction, the variation of conics involves the invariant I_{15} which does not belong to the usual set of Igusa invariants. However, there exists a relation of degree 30 that gives I_{15}^2 as a polynomial function of I_2, I_4, I_6, and I_{10}. If this relation is not a square over $\mathbb{Q}$, we can substitute λI_2, $\lambda^2 I_4$, $\lambda^3 I_6$ and $\lambda^5 I_{10}$ for $I_2, I_4, I_6, \ldots I_{10}$ for a suitable constant λ, chosen so that $\lambda^{15} I_{15}^2$ becomes a square. This yields I_{15} up to sign, which is sufficient for our purposes. (Indeed, the genus 2 curves $y^2 = f(x)$ and $y^2 = -f(x)$ are quadratic twists of each other and have the same even-degree Igusa invariants, even though $I_{15}(f) = -I_{15}(-f)$.)

Example 1.3. We reconstruct a curve of genus 3 from its invariants.

```
> P<x> := PolynomialRing(Rationals());
> f := x^8 + x^3 + 1;
> f2 := P ! (Evaluate(f, (x+1001)/(3*x+5))*(3*x+5)^8);
> f2;
6805*x^8 + 827242*x^7 + 765112882*x^6 + 306007035874*x^5 + 72331829214220*x^4 +
    5628736468095180 6*x^3 + 28168431872398529278*x^2 + 805616828969271682 4758*x
    + 10080280560731904127767 51
> I := ShiodaInvariants(f2);
> HyperellipticCurveFromShiodaInvariants(I);
```

```
Hyperelliptic Curve defined by y^2 = x^8 + x^3 + 1 over Rational Field
Symmetric group acting on a set of cardinality 2
Order = 2
```

1.5 Reconstruction: non-hyperelliptic curves of genus 3 and 4

We begin with the case of a generic non-hyperelliptic curve of genus 3 over a field k. The input consists of a set $\underline{I}$ of Dixmier–Ohno invariants. Depending on the characteristic p of k, different instances of the general reconstruction strategy described in Section 1.3 are applied. This leads to a generic reconstruction algorithm in characteristic different from 2 and 3; see [8] for details[7].

- If $p = 0$ or $p > 7$ with $p \neq 17, 37$, one uses a set of three generically linearly independent contravariants of order 1 and respective degrees 14, 17, and 17. It yields an explicit plane quartic whose coefficients are rational functions in the Dixmier–Ohno invariants. Explicit expressions can be found in [36]. Over $\mathbb{Q}$, the denominators of the coefficients involve only the primes 5, 7, 17, and 37.
- When $p = 17$ or 37, the same contravariants remain generically linearly independent, and we give alternative valid reconstruction formulas.
- If $p = 5$ or 7, one of the contravariants always vanishes. In this situation, we replace it by a contravariant of degree 20, which again leads to valid reconstruction formulas. Using the notation of [8, Table A.1], this contravariant can be defined as $(\rho, \rho, c_{12,3})_2$.

When this first method fails for a given set $\underline{I}$, we switch to an earlier algorithm developed in [34]. This method allows one to reconstruct a model whenever the invariant $I_{12} \neq 0$.[8] If all the above methods fail because of a lack of linear independence, alternative systems of covariants or contravariants can in principle be used to perform the reconstruction. Such systems have not been implemented, and there exist smooth plane quartics for which no such system exists at all. This is for example the case for the Klein quartic, the reason being that a calculation shows that the corresponding ambient representation V of its automorphism group $\mathrm{PSL}_2(\mathbb{F}_7)$ has the property that the character of $\mathrm{Sym}^2(V^*)$ has norm 1, precluding the existence of any invariant subspace, and therefore of any non-trivial quadratic covariant. Nevertheless, for all non-trivial automorphism strata except for the largest ones, namely the cyclic group $\mathbb{Z}/2\mathbb{Z}$, as well as $(\mathbb{Z}/2\mathbb{Z})^2$ when $I_{12} = 0$, an *ad hoc* reconstruction is performed and implemented using the models with few coefficients described in [32]. These algorithms are implemented, although they may fail in positive characteristic as large as 41762629.

[7] There is a typo in the definition of p_0 in Table A.1 of [8]: p_0 should be $\mathrm{D}(C_{4,4}, c_{10,5})$, otherwise it vanishes identically.

[8] The algorithm is only proven to work in characteristic 0. In practice, it can be executed in positive characteristic as long as the Dixmier–Ohno invariants exist and characterize the isomorphism class, but failures may occur in characteristics as large as 89.

Over $\mathbb{Q}$, the variation of conics together with the algorithms of [20] reconstruct quartics with small coefficients, as in [29]. All the methods described above are implemented in the function `PlaneQuarticFromDixmierOhnoInvariants(I)`.

The case of non-hyperelliptic curves of genus 4 constitutes the main result of [8]. At present, reconstruction is available for generic curves in characteristic $p = 0$ and $p > 3$. The corresponding functionality is implemented under the name `Genus4CurveFromInvariants()` in the package [5].

2 Isomorphisms, automorphisms, and twists

This section deals with the computation of isomorphisms, automorphisms, and twists. It is divided into three cases. We first explain a new strategy to determine (linear) isomorphisms of generic hypersurfaces. We then give an overview of what can be achieved for hyperelliptic curves, before finishing with non-hyperelliptic curves of genus 3 and 4.

The computation of automorphisms is a special case of the one of isomorphisms. Automorphism groups may be described as abstract groups or by explicit linear matrices, defined either over the ground field or over a suitable extension.

To compute twists of a quasi-projective algebraic variety X, one uses the bijection between the set of twists and the cohomology set $H^1(\mathrm{Gal}(\bar{K}/K), \mathrm{Aut}(X_{\bar{K}}))$ [43, page 131]. Over a finite field, this set and the bijection can be computed when the elements of $\mathrm{Aut}(X_{\bar{K}})$ are linear; see for instance [39]. Since our methods allow us to compute $\mathrm{Aut}(X_{\bar{K}})$ and its Galois structure explicitly, this leads to a function `Twists(C, H)`, which takes as input any projective curve C (not necessarily plane or non-singular), together with a finite linear subgroup H of the geometric automorphism group of C; its output yields the corresponding set of twists. We give some additional details for certain families of curves below.

2.1 A generic strategy for hypersurfaces

By further developing the idea of linear bases of covariants and contravariants introduced in Section 1.3, we obtain a method to compute linear isomorphisms between generic hypersurfaces. Let $n \geqslant 2$, $d \geqslant 1$, and $\ell \geqslant 1$ be integers, where d denotes the order of the covariants that we use, ℓd is the total degree of the polynomial considered, and $n+1$ the number of variables. Let V be a k-vector space with basis $v_0, \ldots, v_n$, and dual basis $x_0, \ldots, x_n$. The group SL_{n+1} acts on V by $g.v = gv$, identifying v with its coordinate vector in the basis (v_i). The induced action on V^* is given by $g.x = {}^t g^{-1} x$, where x is identified with its coordinate vector in the basis (x_i). These actions extend naturally to $\mathrm{Sym}^d(V)$ and $\mathrm{Sym}^d(V^*)$. In what follows, we often write $\mathrm{Sym}^d(k^{n+1})$ for $\mathrm{Sym}^d(V^*)$.

Let $f, g \in \mathrm{Sym}^{\ell d}(k^{n+1})$ be the defining polynomials of two projective hypersurfaces of degree ℓd and dimension n. Let $c_1, \ldots, c_r$ be covariants of order d and degree α of $\mathrm{Sym}^{\ell d}(k^{n+1})$ (later, we explain how to construct them). We assume that their evaluations at f form a basis of $\mathrm{Sym}^d(k^{n+1})$; this holds for a generic f when the covariants are

chosen appropriately. If the same covariants evaluated at g are linearly dependent, then f and g are not equivalent and we are done. We now assume that this is not the case.

For every $M \in \mathrm{GL}_{n+1}(k)$, we have

$$c_i(M.f) = \det(M)^{\frac{\alpha \ell d - d}{n+1}} M.c_i(f) \quad \text{for all } i.$$

Let $C_f := \big(c_1(f)|\cdots|c_r(f)\big)$ be the matrix whose columns are the coordinate vectors of the $c_i(f)$ with respect to a fixed basis $\mathcal{B}$ of $\mathrm{Sym}^d(k^{n+1})$. Define C_g similarly. For $M \in \mathrm{GL}_{n+1}(k)$, let $\widehat{M} = \rho_d(M)$, where $\rho_d : \mathrm{GL}_{n+1}(k) \longrightarrow \mathrm{GL}(\mathrm{Sym}^d(k^{n+1}))$ is the induced representation on $\mathrm{Sym}^d(k^{n+1})$, and the matrices in the image are written with respect to the basis $\mathcal{B}$.

The following crucial lemma immediately follows from these definitions.

Lemma 2.1. *If $M.f = g$, then there exists a scalar $\lambda \in k^\times$ such that $\widehat{M}.C_f = \lambda C_g$. In particular, $\widehat{M} = 1/\lambda \cdot {}^t(C_f C_g^{-1})$.*

Using Lemma 2.1, we first compute $\widehat{M}$. Recovering a preimage M amounts to solving a system of monomial equations obtained from suitable entries of $\widehat{M}$. We illustrate this with the following example.

Example 2.2. Let $n = 2$, $d = 2$, and write $M = (m_{i,j})_{1 \leqslant i,j \leqslant 3}$. In the ordered basis $\mathcal{B} = \{x^2, xy, xz, y^2, yz, z^2\}$ of $\mathrm{Sym}^2(k^3)$, the induced matrix $\widehat{M} = \rho_2(M)$ is

$$\widehat{M} = \begin{pmatrix} m_{1,1}^2 & m_{1,1}m_{1,2} & m_{1,1}m_{1,3} & m_{1,2}^2 & m_{1,2}m_{1,3} & m_{1,3}^2 \\ 2m_{1,1}m_{2,1} & \cdot & \cdot & 2m_{1,2}m_{2,2} & \cdot & 2m_{1,3}m_{2,3} \\ 2m_{1,1}m_{3,1} & \cdot & \cdot & 2m_{1,2}m_{3,2} & \cdot & 2m_{1,3}m_{3,3} \\ m_{2,1}^2 & m_{2,1}m_{2,2} & m_{2,1}m_{2,3} & m_{2,2}^2 & m_{2,2}m_{2,3} & m_{2,3}^2 \\ 2m_{2,1}m_{3,1} & \cdot & \cdot & 2m_{2,2}m_{3,2} & \cdot & 2m_{2,3}m_{3,3} \\ m_{3,1}^2 & m_{3,1}m_{3,2} & m_{3,1}m_{3,3} & m_{3,2}^2 & m_{3,2}m_{3,3} & m_{3,3}^2 \end{pmatrix},$$

where the dots "$\cdot$" indicate non-monomial entries.

Suppose, in the image of ρ_2, we are given the matrix

$$\widehat{M}_0 = \begin{pmatrix} 0 & 0 & 0 & 5 & -5 & 5 \\ 0 & \cdot & \cdot & 20 & \cdot & -10 \\ 0 & \cdot & \cdot & 10 & \cdot & -10 \\ 5 & -10 & -5 & 20 & 10 & 5 \\ -20 & \cdot & \cdot & 20 & \cdot & 10 \\ 20 & 10 & 10 & 5 & 5 & 5 \end{pmatrix}.$$

To avoid introducing an unnecessary field extension, we first normalize one of the nonzero square terms to 1, for instance the entry corresponding to $m_{1,2}^2$. We obtain

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 1 \\ 0 & \cdot & \cdot & 4 & \cdot & -2 \\ 0 & \cdot & \cdot & 2 & \cdot & -2 \\ 1 & -2 & -1 & 4 & 2 & 1 \\ -4 & \cdot & \cdot & 4 & \cdot & 2 \\ 4 & 2 & 2 & 1 & 1 & 1 \end{pmatrix}.$$

Assuming $m_{1,2} = 1$ (note that -1 yields the same matrix), the fourth column gives $2m_{2,2} = 4$, $2m_{3,2} = 2$, while the first row yields $m_{1,3} = -1$. The remaining monomial relations then allow us to recover the entire matrix, leading to

$$M_0 = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}.$$

In general, we can always choose $\mathcal{B}$ to be the standard monomial basis. The monomial entries then appear precisely in the rows and columns corresponding to pure d^{th} powers, and the same procedure allows one to reconstruct M by solving only monomial equations.

The following proposition shows that this method applies only to hypersurfaces with trivial automorphism group.

Proposition 2.3. *Let $c_1, \dots, c_r$ be covariants of $\mathrm{Sym}^{\ell d}(k^{n+1})$ of order d and equal degree, whose evaluations at f form a basis of $\mathrm{Sym}^d(k^{n+1})$. Then the stabilizer of f in $\mathrm{PGL}_{n+1}(k)$ is trivial. Equivalently, the hypersurface $f = 0$ has no nontrivial automorphisms.*

Proof. Let M be in the stabilizer of f, i.e. $M \cdot f = f$. By Lemma 2.1, we have $\widehat{M} = \lambda^t (C_f C_f^{-1}) = \lambda I_r$ for some $\lambda \in k^\times$. This implies that M is diagonal, with diagonal entries $(\delta_0, \dots, \delta_n)$. Since the diagonal entries of $\widehat{M}$ are of the form $\delta_0^{d-1}\delta_i$, they must all equal λ. This forces $\delta_0 = \cdots = \delta_n$, so M is a scalar multiple of the identity matrix. Therefore the stabilizer of f in $\mathrm{PGL}_{n+1}(k)$ is trivial. □

Remark 2.4. If the hypersurfaces defined by f and g have trivial automorphism groups, the linear equivalence matrix M is unique up to scalars. Its coefficients lie in the compositum of the fields of definition of f and g, so no field extension is required to compute the isomorphism.

It remains to explain how to construct such a basis of covariants. Let $m \geqslant 3$ be an integer and let d be the smallest divisor of m for which covariants of order d of $\mathrm{Sym}^m(k^{n+1})$ exist or, equivalently, the smallest integer such that $\gcd\big(m/d, (n+1)/\gcd(d, n+1)\big) = 1$. Write $m = \ell d$.

ARITY	DEGREE m	ORDER d'	BASIS ORDER d
$n = 1$ (binary)	$2 \mid m$	8	2
	$2 \nmid m$	5	1
$n = 2$ (ternary)	$3 \mid m$	6	3
	$3 \nmid m$	4	1
$n = 3$ (quaternary)	$4 \mid m$	4	4
	$2 \mid m, 4 \nmid m$	6	2
	$2 \nmid m$	3	1

Table 2: Covariant orders for generic degree-m hypersurfaces in n variables.

We first fix an order $d' \leqslant \ell d$ (the smaller, the more convenient) satisfying the following technical conditions:

- the stabilizer in PGL_{n+1} of a generic $f \in \mathrm{Sym}^{d'}(k^{n+1})$ is trivial; this holds for $d' > 4$ when $n = 1$, $d' > 3$ when $n = 2$ and $d' > 2$ when $n > 2$,
- d divides d' and $\gcd\left(d'/d, (n+1)/\gcd(d, n+1)\right) = 1$.

These conditions ensure the existence of covariants of order d in $\mathrm{Sym}^{d'}(k^{n+1})$ that form a basis of $\mathrm{Sym}^{d}(k^{n+1})$ generically [8, Proposition 5.0.3].

We also require d' to satisfy:

- the existence is constructive, providing a collection (b_i) of covariants of order d in $\mathrm{Sym}^{d'}(k^{n+1})$ that forms a basis generically. We obtain them using transvectant operations [42, Section 5] and possibly the Clebsch transfer principle [18, Section 3.4.2].
- there exists a covariant c of order d' for $\mathrm{Sym}^{m}(k^{n+1})$ such that, the specialization of the (b_i) at c forms a basis of the k-vector space $\mathrm{Sym}^{d}(k^{n+1})$. In practice, this condition is satisfied on the first try.

This procedure yields a collection of covariants of $\mathrm{Sym}^{m}(k^{n+1})$ that is generically a linear basis of $\mathrm{Sym}^{d}(k^{n+1})$; see Table 2.

Technical remark 2.5. The main computational bottleneck is the symbolic computation of transvectant. Computing a level k transvectant in $n+1$ variables involves a polynomial in $(n+1)^2$ variables with approximately $\binom{(n+1)^2+k-1}{k}$ terms, which grows very quickly with n. Faster methods for computing covariants would allow this approach to scale to higher arity.

2.2 The hyperelliptic case

Unlike the previous section, which dealt with isomorphisms in the absence of non-trivial automorphisms, here, we are interested in more global methods. As a consequence,

isomorphisms are not necessarily defined over the field of definition of the curves. For both practical and theoretical reasons, we consider possibly non-algebraically closed fields K, call *isomorphisms* those defined over K, and *geometric isomorphisms* those defined over $k = \bar{K}$.

Throughout this section, we consider hyperelliptic curves of genus $g \geqslant 2$ over a base field K of characteristic different from 2, given by explicit equations

$$y^2 = f(x), \quad f \in K[x] \text{ separable of degree } 2g+1 \text{ or } 2g+2.$$

Given two such curves $C_i \colon y^2 = f_i(x)$, isomorphisms $C_1 \longrightarrow C_2$ are of the form

$$(x, y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{g+1}} \right), \tag{1}$$

with $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(K)$ and $e \in K^\times$. If K is algebraically closed, one can impose $e = 1$ and return to the setting of Section 1.1, but we do not insist on this here. The set of isomorphisms is a principal homogeneous space over the automorphism group of either curve C_1 or C_2. Determining whether C_1 and C_2 are (resp. geometrically) isomorphic, and returning the set of (resp. geometric) isomorphisms if they are, boils down to computing the elements of $\mathrm{GL}_2(K)$ (resp. $\mathrm{GL}_2(k)$) whose right action transforms f_1 into a scalar multiple of f_2. The quotient of the automorphism group by the hyperelliptic involution is called the group of *reduced automorphisms*.

The first step is to try the fast and generic method from Section 2.1, which may succeed if the reduced geometric automorphism group of the curve is trivial. If this is not the case, another approach for determining these (geometric) isomorphisms is to apply Gröbner bases after a formal coefficient comparison, see for instance [25]. In [33], the last three authors gave alternative algorithms that speed up this computation when p does not divide $2g+2$. The function `IsIsomorphicHyperellipticCurves()` determines both the full set of isomorphisms $C_1 \longrightarrow C_2$ over K itself and those over the algebraic closure of K using the option `geometric`. Over a number field, this option can be computationally costly. The function `AutomorphismGroupOfHyperellipticCurve()` returns the automorphism group of a curve as a permutation group; if the option `explicit` is enabled, it additionally provides an isomorphism from this abstract group to the actual group of automorphisms.

Twists of hyperelliptic curves over finite fields of characteristic different from 2 can be computed following the general strategy outlined above.

Example 2.6. We determine the twists of the hyperelliptic curve $C \colon y^2 = x^{12} - 1$ over the finite field $\mathbb{F}_{11}$.

```
> P<x> := PolynomialRing(GF(11));
> C := HyperellipticCurve(x^12 - 1);
> Ts, Aut := Twists(C : AutomorphismGroup := true);
> Ts;
[
    Hyperelliptic Curve defined by y^2 = x^12 + 10 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 5*x^11 + 8*x + 9 over GF(11),
```

```
    Hyperelliptic Curve defined by y^2 = x^12 + 6*x^11 + 10*x + 4 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 2*x + 3 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 3*x^11 + 9*x + 3 over GF(11),
    Hyperelliptic Curve defined by y^2 = 2*x^12 + 6*x^11 + 7*x + 6 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + x^11 + 3*x + 1 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^11 + 10*x over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 7*x^11 + 10*x + 2 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 5*x + 1 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 9*x^11 + 3*x + 7 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 6*x^11 + 3*x + 6 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 8*x^11 + 2*x + 4 over GF(11),
    Hyperelliptic Curve defined by y^2 = x^12 + 5 over GF(11)
]
> Aut;
Permutation group Aut acting on a set of cardinality 12
Order = 1320 = 2^3 * 3 * 5 * 11
    (3, 4, 7, 5, 9)(6, 10, 8, 11, 12)
    (3, 6, 5, 11, 4, 10, 9, 12, 7, 8)
    (2, 3)(4, 5)(7, 12)(8, 10)(9, 11)
    (1, 2)(4, 9)(5, 7)(6, 8)(11, 12)
> GroupName(Aut);
PSL(2,11).C2
```

For curves of genus 2 or 3, the computation of twists has been thoroughly implemented in all cases, even in characteristic 2. For curves with small geometric automorphism groups, the generic method, recalled in the introduction of this section, is used; in the case of large automorphism groups special models are reconstructed from invariants (as in Sections 1.1 and 1.2), after which explicit representatives can be more easily obtained. In all cases, the corresponding function is `Twists()`.

2.3 The case of plane quartics

Let C_1 and C_2 be two plane quartic curves over a field K.

As for hyperelliptic curves, the algorithm first tries to find isomorphisms $C_1 \to C_2$ using the ideas of Section 2.1. This method is quite efficient, regardless of the base field chosen, but it applies only when the chosen covariants are linearly independent, which in particular excludes curves with non-trivial automorphism groups. Should this fail, we then check whether $I_{12} \neq 0$. In this case, [51] shows that the use of a suitable covariant reduces the computation of isomorphisms to the problem of finding transformations between certain binary forms associated to C_1 and C_2. This leads to the same computation of elements of $\mathrm{GL}_2(K)$ that was considered in Section 2.2.

In the remaining cases, we use a direct Gröbner basis method first implemented by Michael Stoll, in which one transforms the homogeneous defining equation F_1 of C_1 by a matrix with formal coefficients and imposes that the result be equal to a nonzero scalar multiple of the defining equation F_2 of C_2. Note that, in principle, this method

could be sped up by considering this equality together with those for certain covariants of F_1 and F_2 of small order. The corresponding function is called `AutomorphismGroupOfPlaneQuartic()`.

Once again, the algorithm admits both a version over the base field and a geometric version, with the latter finding the isomorphisms over the algebraic closure of K. Both versions are very efficient over finite fields, and the version over the base field is also reasonably fast for $K = \mathbb{Q}$. By contrast, finding geometric isomorphisms between plane quartic curves over $\mathbb{Q}$ can still take a significant amount of time. For more general fields, the implementation remains too slow, and our functions therefore restrict consideration to the cases where K is either finite or equal to $\mathbb{Q}$.

Note that some of these routines may overlap with routines included natively in Magma. As in the hyperelliptic case, the new ones are generally much faster.

Example 2.7. We compare timings for our automorphism routine and the native one included in version 2.29-3 of Magma.

```
> P<x,y,z> := ProjectiveSpace(Rationals(),2);
> C := Curve(P, x^4+y^4+z^4);
> time aut, phi := AutomorphismGroupOfPlaneQuartic(C : geometric := true,
explicit := true);
Time: 0.140
> GroupName(aut);
C4^2:C3:C2
> // to get all automorphisms, we base change to Q(zeta_8)
> K := CyclotomicField(8);
> C1 := BaseChange(C,K);
> time G := AutomorphismGroup(C1);
Time: 3.200
> Gp,rep := MatrixRepresentation(G);
> GroupName(Gp);
C4^2:C3:C2
```

As for twists, we have implemented a function `Twists()` that computes a list of representatives of all twists of a smooth plane quartic over a finite field using the general method presented in the introduction of this section.

2.4 The case of non-hyperelliptic curves of genus 4

Here, we assume that the characteristic of K is different from 2, 3, and 5. Non-hyperelliptic curves of genus 4 are defined as the intersection of a quadric Q and a cubic surface E. Although they are not hypersurfaces, a covariant-based approach similar to the plane quartic case can be applied.

In the generic situation, the quadric surface Q is of rank 4. In this case, there is an extra ambiguity: E can be modified by adding a linear form times Q, in addition to the classical action of $\mathrm{GL}_4(K)$. The following lemma and proposition allow us to eliminate this extra action and reduce to the standard situation without extending the field of definition.

Let $V = K^4$ with basis $\{v_0, v_1, v_2, v_3\}$ and dual basis $\{x_0, x_1, x_2, x_3\}$, equipped with the standard action of $\mathrm{GL}_4(K)$ as in Section 2.1.

Lemma 2.8. *Let Q and E be homogeneous polynomials of degrees 2 and 3 over a field K, with* $\mathrm{rank}(Q) = 4$. *Define*

$$\widetilde{E} = (Q, Q, Q, Q)_2 E - \frac{3}{2}(Q, Q, Q, E)_2 Q,$$

where $(\cdot,\cdot,\cdot,\cdot)_l$ denotes the classical transvectant of level l [42, Section 5]. Then

$$\widetilde{\ }\colon (Q, E) \longmapsto (Q, \widetilde{E}) \in \mathrm{Sym}^2(V^*) \times \mathrm{Sym}^3(V^*)$$

is $\mathrm{GL}_4(K)$-equivariant and, for any linear form ℓ, we have

$$\widetilde{E + \ell Q} = \widetilde{E}.$$

Proof. A direct computation shows $(Q, Q, Q, Q)_2 \ell = (3/2)(Q, Q, Q, \ell Q)_2$. Equivariance of all operators then implies the lemma. □

Proposition 2.9. *Let C and C' be two genus 4 curves over K defined by (Q, E) and (Q', E'), respectively. We assume that Q and Q' are of rank 4. Then*

$$C \simeq C' \iff \exists M \in \mathrm{GL}_4(K), \exists \alpha \in K^\times, \begin{cases} M.Q = Q', \\ M.\widetilde{E} = \alpha \widetilde{E'}. \end{cases}$$

Proof. By definition, $C \simeq C'$ if and only if there exist $M \in \mathrm{GL}_4(K)$, $\alpha \in K^\times$, and a linear form ℓ such that $M.Q = Q'$, and $M.E = \alpha E' + \ell Q'$. Applying Lemma 2.8 gives $M.\widetilde{E} = \widetilde{M.E} = \widetilde{\alpha E' + \ell Q'} = \alpha \widetilde{E'}$ which proves one direction. Conversely, $(Q, \widetilde{E})$ and (Q, E) define the same curve, as do $(Q', \widetilde{E'})$ and (Q', E'). □

As we have seen, we know how to compute linear transformations between generic cubic surfaces using covariants. Proposition 2.9 shows that we can compute the isomorphisms between the curves C and C' by first computing the isomorphisms between $\widetilde{E}$ and $\widetilde{E'}$ and then retaining the ones mapping Q onto Q'.

This approach fails when the cubic surface defined by $\widetilde{E}$ admits non-trivial automorphisms (which is always the case if C does). In that case, one instead solves a system of polynomial equations to determine the coefficients of the transformation, imposing compatibility conditions on the images of Q, $\widetilde{E}$, and the order 1 covariants of $\widetilde{E}$. The function `IsIsomorphicGenus4()` implements this strategy, combining the covariant-based method with a Gröbner basis approach when necessary.

For curves supported on a quadric Q of rank 3, the situation is more subtle. We introduce two linear forms derived from Q and E that transform covariantly and contravariantly, respectively, under the action of $\mathrm{GL}_4(K)$. These forms are invariant under the transformation $E \mapsto E + \ell Q$. By normalizing these quantities and applying a similar argument as in the rank 4 case, we eliminate the residual action $E \mapsto E + \ell Q$, and apply a strategy similar to the one presented before.

Let $\mathrm{H}(Q)$ denote the Hessian matrix of Q. By definition, the rank of the quadric surface is the rank of $\mathrm{H}(Q)$.

Lemma 2.10. *Let $Q \in K[x_0, x_1, x_2, x_3]_2$ be of rank 3, and let v_Q be a nonzero element of the right kernel of $\mathrm{H}(Q)$ canonically identified to an element in V. Then for any $M \in \mathrm{GL}_4(K)$, $(M^{-1})^t.v_Q$ lies in the right kernel of $\mathrm{H}(M \cdot Q)$.*

Proof. A direct calculation gives $\mathrm{H}(M.Q) = M^{-1}\,\mathrm{H}(Q)(M^{-1})^t$ and $(M^{-1})^t.v_Q = M^t v_Q$. The lemma follows. □

Remark 2.11. The vector v_Q can be interpreted as a contravariant of order 1 of $\mathrm{Sym}^2(K^4)$, even though it is defined only up to multiplication by a scalar.

Finding a transformation that sets $v_Q = v_3$ forces Q to have no term in x_3, so that $Q \in K[x_0, x_1, x_2]_2$. From now on, we assume Q has been normalized in this way and that $v_Q = v_3$.

Now, let $E \in \mathrm{Sym}^3(V^*)$ be such that the intersection of the quadric defined by Q and the cubic defined by E is a smooth non-hyperelliptic curve C of genus 4. Since C is smooth, the coefficient of x_3^3 in E is nonzero. A direct computation also shows that the coefficient of x_3 in $(Q, Q, Q, E)_2$ is nonzero. Moreover, $(Q, Q, Q, E)_2$ is a GL_4-covariant of $\mathrm{Sym}^2(K^4) \times \mathrm{Sym}^3(K^4)$, and it is invariant under the action $E \mapsto E + \ell Q$. Compare this, where $(Q, Q, Q, E + \ell Q)_2 = (Q, Q, Q, E)_2$, to the rank 4 case, where

$$(Q, Q, Q, E + \ell Q)_2 = (Q, Q, Q, E)_2 + \frac{2}{3}(Q, Q, Q, Q)_2 \ell.$$

Transforming $(Q, Q, Q, E)_2$ into αx_3 for some $\alpha \in K^\times$ amounts to using a matrix of the form

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \star & \star & \star & 1 \end{pmatrix}, \quad {}^tM^{-1} = \mathrm{Com}(M) = \begin{pmatrix} 1 & 0 & 0 & \star \\ 0 & 1 & 0 & \star \\ 0 & 0 & 1 & \star \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

so that ${}^tM^{-1}.v_Q = v_3$ remains unchanged.

After dividing E by the coefficient of x_3^3, we can write $E = x_3^3 + x_3 f_2(x_0, x_1, x_2) + f_3(x_0, x_1, x_2)$. To eliminate the action $E \mapsto E + \ell Q$, we define

$$\widetilde{f_2} = (Q, Q, Q)_2 f_2 - \frac{3}{5}(Q, Q, f_2)Q, \quad \widetilde{f_3} = (Q, Q, Q)_2 f_3 - \frac{3}{5}(Q, Q, f_3)Q,$$

where Q is now seen as a polynomial in $K[x_0, x_1, x_2]$, and set $\widetilde{E} = (Q, Q, Q)_2 x_3^3 + x_3\widetilde{f_2} + \widetilde{f_3}$. Isomorphisms between two genus 4 curves in this normal form are characterized by the following proposition.

Proposition 2.12. *Let $Q, Q' \in K[x_0, x_1, x_2]_2$ of rank 3, and let $\widetilde{E}, \widetilde{E'}$ be in the normal form described above, defining non-hyperelliptic curves C and C' of genus 4. Then C and C' are isomorphic if and only if there exist $M \in \mathrm{GL}_3(K)$ and $\alpha, \lambda, \mu \in K^\times$ such that the diagonal by block matrix $M' \in \mathrm{GL}_4(K)$ given by $\mathrm{Diag}(M, \alpha)$ satisfies $M'.\widetilde{E} = \lambda\widetilde{E'}$ and $M'.Q = \mu Q'$.*

Now that $\widetilde{E}$ and $\widetilde{E'}$ are normalized for the residual action $\widetilde{E} \to \widetilde{E} + \ell Q$, we reduce to the previous case and compute 4 covariants of order 1 of $\widetilde{E}$.

TYPE	FIELD	INVARIANTS	RECONSTRUCTION	ISOMORPHISMS	AUTOMORPHISMS	TWISTS
Genus 2	$\mathbb{Q}$	0.00	0.05	0.07	0.00	—
	$\mathbb{F}_p$	0.00	0.00	0.01	0.00	0.00
	$\mathbb{F}_q$	0.01	0.01	0.15	0.01	0.00
Genus 3 hyp.	$\mathbb{Q}$	0.00	0.13	0.39	0.01	—
	$\mathbb{F}_p$	0.00	0.01	0.00	0.00	0.01
	$\mathbb{F}_q$	0.00	0.03	0.05	0.01	0.03
Genus 3 non-hyp.	$\mathbb{Q}$	0.00	0.36	0.22	0.05	—
	$\mathbb{F}_p$	0.00	0.06	0.06	0.03	0.16
	$\mathbb{F}_q$	0.05	0.27	0.14	0.14	0.73
Genus 4 hyp.	$\mathbb{Q}$	0.38	1.33	0.21	0.00	—
	$\mathbb{F}_p$	0.16	0.06	0.00	0.00	0.01
	$\mathbb{F}_q$	0.47	0.14	0.20	0.00	0.24
Genus 4 non-hyp.	$\mathbb{Q}$	0.59	0.00	3.13	0.12	—
	$\mathbb{F}_p$	0.03	0.00	0.18	0.05	—
	$\mathbb{F}_q$	0.09	0.00	0.56	0.28	—
Cubic surface	$\mathbb{Q}$	0.03	0.07	4.55	—	—
	$\mathbb{F}_p$	0.06	0.00	0.15	—	—
	$\mathbb{F}_q$	0.11	0.01	0.52	—	—

Table 3: Running times (in seconds) of the different algorithms.

While the covariant-based step may fail in non-generic cases, Proposition 2.12 remains valid in full generality. In that case, one instead solves a system of polynomial equations to determine the coefficients of the transformation, imposing compatibility conditions on the images of Q, $\widetilde{E}$, and the order 1 covariants of $\widetilde{E}$. A call to the function `IsIsomorphicGenus4()` applies the generic covariant strategy first, and resorts to a Gröbner basis when necessary.

It should in principle be possible to use the output of the previous function to compute twists via `Twist(C,H)`.

A Performance

Table 3 reports the running times of the different functions discussed in this article, applied to a smooth curve or surface with randomly chosen coefficients (over $\mathbb{Q}$, the coefficients were chosen to have absolute value smaller than 10^5). We let $p = 97$ and $q = p^{20}$.

The isomorphism function was applied to the reconstructed curve or surface and the corresponding original model. We also note that the function for computing twists of curves is currently implemented only for hyperelliptic curves and plane quartics, and only over finite fields.

B Dixmier–Ohno invariants in positive characteristic

This appendix is drawn from the first author's thesis [7, Chapter 5]. We refer the reader to [15] for background on representation theory, in particular the theory of roots and weights. We first briefly present the theory of good filtrations, tailored to our needs.

B.1 Good filtrations

Let $n, d > 1$, and let p be a prime number. Let k be an algebraically closed field of characteristic p. We are mainly interested in the invariant algebra of $V_{n,d}(k) = \mathrm{Sym}^d(k^n)$, acted upon in the usual way by $\Gamma_k = \mathrm{SL}_n(k)$. Most, if not all, of the properties listed below extend to connected reductive groups. Let T be the maximal torus of Γ_k consisting of diagonal matrices of determinant 1, and let B be the Borel subgroup of Γ_k whose elements are the upper triangular matrices with determinant 1. Let $U \subseteq B$ be the unipotent subgroup of Γ_k composed of upper triangular matrices with 1's on the diagonal. Let Λ^+ denote the set of dominant weights associated to U.

Definition B.1. *Let $\lambda \in \Lambda^+$. A* dual Weyl module $\nabla(\lambda)$ *is an irreducible rational representation of Γ_K with highest weight λ.*

Remark B.2. We assume that $p > d$. It is shown in [16, Corollary 2.5] (as a direct consequence of [49, Theorems 2 and 3]) that, for all $\lambda \vdash d$, the Schur modules $S_\lambda(k^n)$ are irreducible representations of GL_n. Therefore, when $p > d$, Schur modules are dual Weyl modules.

Definition B.3 ([16, Definition 4])**.** *A rational representation V of Γ_k is said to have a* good filtration *if there exist finite-dimensional subrepresentations $(V_i)_i$ of V such that*

$$0 = V_0 \subseteq V_1 \subseteq V_2 \subseteq \cdots \quad \text{and} \quad V = \bigcup_i V_i$$

and each subquotient V_i/V_{i-1} is a dual Weyl module.

Remark B.4 ([16, Remark 5.2]). When the group Γ can be defined over $\mathbb{Z}$, dual Weyl modules can also be defined over $\mathbb{Z}$, as $\mathbb{Z}$-modules (instead of vector spaces). For instance, the group $\Gamma = \mathrm{SL}_n$ can be defined over $\mathbb{Z}$ and, for every algebraically closed field k, we have an isomorphism of algebraic groups

$$\mathrm{SL}_n(k) \simeq \Gamma \otimes_{\mathbb{Z}} k.$$

The dual Weyl modules can also be defined over $\mathbb{Z}$: for any $\lambda \in \Lambda^+$, there exists a free Γ-module $\nabla_{\mathbb{Z}}(\lambda)$ such that for every algebraically closed field k we have an isomorphism of $\mathrm{SL}_n(k)$-representations

$$\nabla_{\mathbb{Z}}(\lambda) \otimes_{\mathbb{Z}} k \simeq \nabla_k(\lambda).$$

For $\Gamma = \mathrm{SL}_n$, these are the Schur modules defined over $\mathbb{Z}$.

Lemma B.5 ([16, Corollary 22])**.** *Let V be a rational representation of a connected reductive group over k, such that V is of dimension n and admits a good filtration. If $p = \mathrm{char}(k) > n$, then $k[V]$ admits a good filtration.*

Corollary B.6. *If $p > \binom{n+d-1}{d}$, then $k[V_{n,d}(k)]$ admits a good filtration.*

Proof. Let λ_1 be the fundamental weight associated to the simple root

$$\varepsilon_1 - \varepsilon_2 \colon \operatorname{Diag}(t_1, \dots, t_n) \in \mathrm{SL}_n(k) \longmapsto t_1/t_2.$$

We know that $V_{n,d}(k) = S_{(d)}(k^n) = \nabla(d\lambda_1)$, and since $p > \binom{n+d-1}{d} > d$, this Schur module is irreducible by Remark B.2. Thus $V_{n,d}(k)$ is a dual Weyl module. Moreover, $p > \binom{n+d-1}{d} = \dim(V_{n,d}(k))$, therefore by Lemma B.5, $k[V_{n,d}(k)]$ admits a good filtration. □

Modules with good filtrations have many interesting properties, and we refer the reader to [1] for further details. Here, we focus on two consequences: one concerning Cohen–Macaulayness and the other the Hilbert series.

Proposition B.7 ([26, Theorem 6])**.** *Let k be an algebraically closed field of characteristic $p > 0$, and Γ a connected reductive group over k. Let V be a finite-dimensional rational representation of Γ, and set $S = k[V]$. If S has a good filtration, then $k[V]^\Gamma$ is Cohen–Macaulay.*

In particular, in characteristic greater than the dimension of the rational representation considered, the algebra of invariants is Cohen–Macaulay, just as in characteristic 0. We obtain a similar result for the Hilbert series.

Proposition B.8 ([16, Proposition 8.7])**.** *Let V be a rational representation of dimension n of a connected reductive group Γ defined over $\mathbb{Z}$ which admits a good filtration. Let k be an algebraically closed field such that $k[V]$ admits a good filtration. Then the Hilbert series of $k[V]^\Gamma$ is the same as the Hilbert series of $\mathbb{C}[V]^\Gamma$.*

Corollary B.9. *If $p > \binom{n+d-1}{d}$, then*

$$\operatorname{Hilb}\left(k[V_{n,d}(k)]^{\mathrm{SL}_n(k)}, t\right) = \operatorname{Hilb}\left(\mathbb{C}[V_{n,d}(\mathbb{C})]^{\mathrm{SL}_n(\mathbb{C})}, t\right).$$

Proof. We follow [16, Section 5]. The algebraic group SL_n is connected, reductive, and defined over $\mathbb{Z}$. The representation $V_{n,d}$ is a dual Weyl module, hence admits a good filtration. If $p > \binom{n+d-1}{d}$, then $k[V_{n,d}(k)]$ admits a good filtration. Proposition B.8 then yields the result. □

B.2 Application to the invariant ring of ternary quartics

Proposition B.10 ([45])**.** *The Hilbert series of the algebra of invariants of ternary quartics over an algebraically closed field of characteristic 0 is*

$$\operatorname{Hilb}\left(\mathbb{C}[V_{3,4}(\mathbb{C})]^{\mathrm{SL}_3(\mathbb{C})}, t\right) = \frac{P(t)}{(1-t^3)(1-t^6)(1-t^9)(1-t^{12})(1-t^{15})(1-t^{18})(1-t^{27})},$$

where

$$\begin{aligned} P(t) = 1 &+ t^9 + t^{12} + t^{15} + 2t^{18} + 3t^{21} + 2t^{24} + 3t^{27} + 4t^{30} + 3t^{33} + 4t^{36} \\ &+ 4t^{39} + 3t^{42} + 4t^{45} + 3t^{48} + 2t^{51} + 3t^{54} + 2t^{57} + t^{60} + t^{63} + t^{66} + t^{75}. \end{aligned}$$

Theorem B.11. *Let k be an algebraically closed field of characteristic p. When $p > 13$, the algebra of invariants $k[V_{3,4}(k)]^{\mathrm{SL}_3(k)}$ is generated by the Dixmier–Ohno invariants.*

Proof. By Corollary B.9, we have

$$\mathrm{Hilb}\left(k[V_{3,4}(k)]^{\mathrm{SL}_3(k)}, t\right) = \mathrm{Hilb}\left(\mathbb{C}[V_{3,4}(\mathbb{C})]^{\mathrm{SL}_3(\mathbb{C})}, t\right).$$

Furthermore, a primary system of invariants of $k[V_{3,4}]^{\mathrm{SL}_3(k)}$ was established for every p greater than 7 in [30]. For $p \notin \{19, 47, 277, 523\}$, the Dixmier invariants still form a primary system of invariants. For the exceptional primes $p \in \{19, 47, 277, 523\}$, a different homogeneous system of parameters (of the same degrees) is obtained by replacing the degree-9 invariant I_9 with $I_9 + J_9$, where J_9 is the degree-9 Ohno invariant.

Since for each characteristic $p > 7$ we know a primary system of invariants of degrees matching those of the denominator of the Hilbert series, checking that the Dixmier–Ohno invariants DO generate the algebra of invariants reduces to verifying that, for every degree $d \leqslant 75$ (the degree of the numerator of the Hilbert series), we have

$$\dim(k[\mathrm{DO}]_d) = \dim\left(k[V_{3,4}(k)]_d^{\mathrm{SL}_3(k)}\right).$$

Since it is impossible to check this property directly for every $p > 13$, we perform the verification over $\mathbb{Z}\left[\frac{1}{13!}\right]$. Specifically, we evaluate a conjectured basis of invariants for each degree $d \leqslant 75$ on a set of ternary quartics with small integer coefficients, in a number exceeding the expected dimension. Computing the Smith normal form of the resulting matrix then identifies, at least, the primes for which the rank is not what is expected.

For larger degrees, computing the full Smith normal form is computationally intensive, so we compute the greatest common divisor of several maximal minors of the matrix instead. This gcd is a multiple of the last diagonal element of the Smith normal form, and hence also of every diagonal element. Computing the gcd of three maximal minors reveals that the divisors are contained in $\{2, 3, 5, 7\}$ for all degree up to 75.

For $p \in \{19, 47, 277, 523\}$, one checks separately that the algebra generated by the Dixmier–Ohno invariants has the correct dimension for all degrees between 0 and 75, using the Hilbert series and a similar evaluation/rank strategy, but this time over a finite field (which is much faster).

We conclude that in characteristic p greater than 13, the dimension of the homogeneous components of $k[V_{3,4}(k)]^{\mathrm{SL}_3(k)}$ coincides with that of the algebra generated by the Dixmier–Ohno invariants. By inclusion, this implies equality. □

Remark B.12. We proved that, for every algebraically closed field k of characteristic $p > 13$,

$$k[V_{3,4}(k)]^{\mathrm{SL}_3(k)} = \mathbb{Z}[\mathrm{DO}] \otimes_{\mathbb{Z}} k.$$

Since we only observed possible dimension drops for $p \leqslant 7$, one may hope that the Hilbert series remains unchanged for $p = 11$ or 13, in which case Theorem B.11 would extend immediately to $p > 7$.

This observation naturally leads to the question of whether the bound $p > \binom{n+d-1}{d}$ is sharp, a question we hope will receive a negative answer in the future.

Question B.13. *Is the bound $p > \binom{n+d-1}{d}$ in Corollary B.6 sharp for ensuring that $k[V_{n,d}(k)]$ admits a good filtration?*

References

[1] Henning Haahr Andersen and Jens Carsten Jantzen. Cohomology of induced representations for algebraic groups. *Mathematische Annalen*, 269:487–525, 1984. DOI: 10.1007/BF01450762.

[2] Enrico Arbarello, Maurizio Cornalba, Phillip A. Griffiths, and Joseph D. Harris. *Geometry of Algebraic Curves, I.* Volume 267 of *Grundlehren der mathematischen Wissenschaften*, Springer, 1984. DOI: 10.1007/978-1-4757-5323-3.

[3] Romain Basson. *Arithmétique des espaces de modules des courbes hyperelliptiques de genre 3 en caractéristique positive.* PhD thesis, Université de Rennes 1, 2015. DOI: 10.70675/811a757ez585dz4599z9fe8zf2e4b0f972ed.

[4] Laurent Busé and Jean-Pierre Jouanolou. On the discriminant scheme of homogeneous polynomials. *Mathematics in Computer Science*, 8(2):175–234, 2014. DOI: 10.1007/s11786-014-0188-7.

[5] Thomas Bouchet. Genus-4, a Magma repository for computations with genus-4 curves. https://github.com/Thittho/Genus-4.

[6] Thomas Bouchet. Invariants of genus 4 curves. *Journal of Algebra*, 660:619–644, 2024. DOI: 10.1016/j.jalgebra.2024.07.016.

[7] Thomas Bouchet. *Géométrie des courbes : une approche explicite par les invariants.* PhD thesis, Université Côte d'Azur, 2025. DOI: 10.70675/a1ee35cbz9a54z40-16za5fdze5d630752b25.

[8] Thomas Bouchet. Reconstruction of hypersurfaces from their invariants. *Journal of Pure and Applied Algebra*, 229(11):108109, 2025. DOI: 10.1016/j.jpaa.2025.108109.

[9] Andries E. Brouwer and Mihaela Popoviciu. The invariants of the binary decimic. *Journal of Symbolic Computation*, 45(8):837–843, 2010. DOI: 10.1016/j.jsc.2010.03.002.

[10] Alfred Clebsch. *Theorie der binären algebraischen Formen.* Teubner, 1872.

[11] Gabriel Cardona, Enric Nart, and Jordi Pujolàs. Curves of genus two over fields of even characteristic. *Mathematische Zeitschrift*, 250:177–201, 2005. DOI: 10.1007/s00209-004-0750-0.

[12] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational Aspects of Algebraic Curves*, volume 13 of *Lecture Notes Series on Computing*, pages 71–83. World Scientific, 2005. DOI: 10.1142/9789812701640_0006.

[13] Michel Demazure. Résultant, discriminant. *L'Enseignement Mathématique*, 58(3/4):333–373, 2012. DOI: 10.4171/lem/58-3-5.

[14] Jacques Dixmier. On the projective invariants of quartic plane curves. *Advances in Mathematics*, 64:279–304, 1987. DOI: 10.1016/0001-8708(87)90010-7.

[15] Harm Derksen and Gregor Kemper. *Computational Invariant Theory*. Volume 130 of *Encyclopaedia of Mathematical Sciences*, Springer, 2015. DOI: 10.1007/978-3-662-48422-7.

[16] Harm Derksen and Visu Makam. Weyl's polarization theorem in positive characteristic. *Transformation Groups*, 26(4):1241–1260, 2021. DOI: 10.1007/s00031-020-09559-3.

[17] Igor V. Dolgachev. *Lectures on Invariant Theory*. Volume 296 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, 2003. DOI: 10.1017/CBO9780511615436.

[18] Igor V. Dolgachev. *Classical Algebraic Geometry, a modern view*. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139084437.

[19] Stephen Donkin. *Rational Representations of Algebraic Groups, tensor products and filtrations*. Volume 1140 of *Lecture Notes in Mathematics*, Springer, 1985. DOI: 10.1007/BFb0074637.

[20] Andreas-Stephan Elsenhans. Good models for cubic surfaces. Preprint, 2009. https://math.uni-paderborn.de/fileadmin-eim/mathematik/AG-Computeralgebra/Preprints-elsenhans/red_5.pdf.

[21] Andreas-Stephan Elsenhans and Michael Stoll. Minimization of hypersurfaces. *Mathematics of Computation*, 93(349):2513–2555, 2024. DOI: 10.1090/mcom/3924.

[22] Wulf-Dieter Geyer. Invarianten binärer Formen. In *Classification of Algebraic Varieties and Compact Complex Manifolds*, volume 412 of *Lecture Notes in Mathematics*, pages 36–69. Springer, 1974. DOI: 10.1007/BFb0066153.

[23] Martine Girard and David R. Kohel. Classification of genus 3 curves in special strata of the moduli space. In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Computer Science*, pages 346-360. Springer, 2006. DOI: 10.1007/11792086_25.

[24] Israel M. Gelfand, Mikhail M. Kapranov, Andrei V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Volume of *Modern Birkhäuser Classics*, Springer, 1994. DOI: 10.1007/978-0-8176-4771-1.

[25] Norbert Goeb. Computing the automorphism groups of hyperelliptic function fields. Preprint, 2003. DOI: 10.48550/arXiv.math/0305284.

[26] Mitsuyasu Hashimoto. Good filtrations of symmetric algebras and strong F-regularity of invariant subrings. *Mathematische Zeitschrift*, 236(3):605–623, 2001. DOI: 10.1007/s00209-005-0932-4.

[27] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960. DOI: 10.2307/1970233.

[28] Jean-Pierre Jouanolou. Formes d'inertie et résultant : un formulaire. *Advances in Mathematics*, 126(2):119–250, 1997. DOI: 10.1006/aima.1996.1609.

[29] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Acta Arithmetica*, 185(2):127–156, 2018. DOI: 10.4064/aa170227-16-3.

[30] Reynald Lercier, Qing Liu, Elisa Lorenzo García, and Christophe Ritzenthaler. Reduction type of smooth plane quartics. *Algebra & Number Theory*, 15(6):1429–1468, 2021. DOI: 10.2140/ant.2021.15.1429.

[31] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *Journal of Algebra*, 372:595–636, 2012. DOI: 10.1016/j.jalgebra.2012.07.054.

[32] Reynald Lercier, Christophe Ritzenthaler, Florent Rovetta, and Jeroen Sijsling. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS Journal of Computation and Mathematics*, 17(A):128–147, 2014. DOI: 10.1112/S146115701400031X.

[33] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit descent. In *Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *The Open Book Series*, pages 463–486. Mathematical Sciences Publishers, 2012. DOI: 10.2140/obs.2013.1.463.

[34] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Reconstructing plane quartics from their invariants. *Discrete & Computational Geometry*, 63:73–113, 2020. DOI: 10.1007/s00454-018-0047-4.

[35] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Hyperelliptic, a Magma repository for reconstruction and isomorphisms of hyperelliptic curves. https://github.com/JRSijsling/hyperelliptic.

[36] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Quartic, a Magma repository for calculating with plane quartic curves. https://github.com/JRSijsling/quartic.

[37] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 313–334. Birkhäuser, 1991. DOI: 10.1007/978-1-4612-0441-1_21.

[38] Hideyuki Matsumura and Paul Monsky. On the automorphisms of hypersurfaces. *Journal of Mathematics of Kyoto University*, 3(3):347–361, 1964. DOI: 10.1215/kjm/1250524785.

[39] Stephen Meagher and Jaap Top. Twists of genus three curves over finite fields. *Finite Fields and Their Applications*, 16(5):347–368, 2010. DOI: 10.1016/j.ffa.2010.06.001.

[40] Enric Nart and Daniel Sadornil. Hyperelliptic curves of genus three over finite fields of characteristic two. *Finite Fields and Their Applications*, 10(2):198–220, 2004. DOI: 10.1016/j.ffa.2003.08.002.

[41] Toshiaki Ohno. The graded ring of invariants of ternary quartics I. Preprint, 2007. https://aeb.win.tue.nl/math/ohno-preprint.2007.05.15.pdf.

[42] Peter J. Olver. *Classical Invariant Theory*. Volume 44 of *London Mathematical Society Student Texts*, Cambridge University Press, 1999. DOI: 10.1017/CBO9780511623660.

[43] Jean-Pierre Serre. *Cohomologie Galoisienne*. Volume 5 of *Lecture Notes in Mathematics*, Springer, 1994. DOI: 10.1007/BFb0108758.

[44] James Joseph Sylvester and Fabian Franklin. Tables of the generating functions and groundforms for the binary quantics of the first ten orders. *American Journal of Mathematics*, 2(3):223–251, 1879. DOI: 10.2307/2369240.

[45] Tetsuji Shioda. On the graded ring of invariants of binary octavics. *American Journal of Mathematics*, 89(4):1022–1046, 1967. DOI: 10.2307/2373415.

[46] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Volume 106 of *Graduate Texts in Mathematics*. Springer, 2009. DOI: 10.1007/978-0-387-09494-6.

[47] Larry Smith. *Polynomial invariants of finite groups*. Volume 6 of *Research Notes in Mathematics*. CRC Press, 1995. ISBN: 9780367449131.

[48] Bernd Sturmfels. *Algorithms in Invariant Theory*. Volume of *Texts & Monographs in Symbolic Computation*, Springer, 2008. DOI: 10.1007/978-3-211-77417-5.

[49] Burt Totaro. Projective resolutions of representations of GL(n). *Journal für die reine und angewandte Mathematik*, 482:1–13, 1997. DOI: 10.1515/crll.1997.482.1.

[50] August Johann Ludwig Karl Wilhelm von Gall. Das vollständige Formensystem der binären Form 7^{ter} Ordnung. *Mathematische Annalen*, 31:318–336, 1888. DOI: 10.1007/BF01206218.

[51] Sander M. van Rijnswou. *Testing the Equivalence of Planar Curves*. PhD thesis, Technische Universiteit Eindhoven, 2001. DOI: 10.6100/IR543172.