

Reconstruction of hypersurfaces from their invariants

Thomas Bouchet

^a *Université Côte d’Azur, Campus Sciences, Parc Valrose, 28 Avenue Valrose, 06108, Nice, France*

Abstract

Let K be a field of characteristic 0. We present an explicit algorithm that, given the invariants of a generic homogeneous polynomial f under the linear action of GL_n or SL_n , returns a polynomial differing from f only by a linear change of variables with coefficients in a finite extension of K . Our approach uses the theory of covariants and the Veronese embeddings to characterize the linear equivalence class of a homogeneous polynomial through equations whose coefficients are invariants. As applications, we derive explicit formulas for reconstructing of a generic non-hyperelliptic curve of genus 4 from its invariants, as well as reconstructing generic non-hyperelliptic curves of genus 3 from their Dixmier-Ohno invariants. In both cases, the coefficients of the reconstructed curve lie in its field of moduli.

1. Introduction

Invariant theory is the study of algebraic expressions that remain unchanged under various transformations, providing powerful tools to analyze and reveal intrinsic features of mathematical structures.

In the 19th century, invariants theorists sought to classify the orbits of homogeneous polynomials in n variables under the action of $\mathrm{SL}_n(\mathbb{C})$. This naturally led to the study of invariants, which are polynomials in the coefficients of these forms that remain unchanged under the group action. Using Gordan’s algorithm (Gordan, 1868), they constructed generating systems for the algebras of invariants of binary forms ($n = 2$) of degrees $d \leq 6$ and $d = 8$ (Sylvester and Franklin, 1879). Additionally, they found generating sets of invariants for cubic ternary and quaternary forms (Clebsch, 1870). Unfortunately, due to the rapidly growing complexity of the task, only partial results were obtained at that time for larger degrees.

The field experienced a resurgence with Mumford’s Geometric Invariant Theory (GIT) (Mumford et al., 1994), which constructs geometric quotients through algebras of invariants. For instance, knowing a generating set of invariants (and their relations) for the algebra of $\mathrm{Sym}^d(K^n)$ under the action of SL_n enables the explicit construction of the geometric quotient of the subvariety of stable elements of $\mathrm{Sym}^d(K^n)$ under SL_n , and provides parameters for the corresponding coarse moduli space. Broadly speaking, a stable element can be represented by a list of invariants. We explain further in the introduction the meaning of the word stable.

In recent years, attention has turned to the reverse problem: given the invariants of a stable element of $\mathrm{Sym}^d(K^n)$ under the action of SL_n , is there an explicit and efficient method to reconstruct a representative of that orbit? Although this problem is theoretically solvable using Gröbner bases, such methods are often computationally impractical in practice, given the large number of invariants and their degrees.

Only specific cases have been addressed in the literature, and the reconstruction problem does not seem to have been approached in full generality. Mestre (1991) presented an algorithm for reconstructing binary forms of degree 6, while Noordsij (2022) later introduced an algorithm for the reconstruction of binary forms of degree 5 in his Master’s thesis. Their methods extend to generic binary forms of even and odd degrees respectively. The case of hyperelliptic curves of genus 3, which are closely related to binary forms of degree 8, is treated by Lercier and Ritzenthaler (2012), even in the presence of extra automorphisms. Lercier et al. (2020) tackled the reconstruction of plane quartics by reducing the problem to reconstructing a space of binary forms. Notably, all these methods rely on formulas derived from the work of Clebsch (1870).

In this paper, we present a solution to the reconstruction problem which is valid in a very general setting. This method holds significant potential for applications, among which the construction of curves or hypersurfaces with interesting arithmetic or geometric properties (e.g. CM curves (Bouyer and Streng, 2015; Kılçer et al., 2018)), arithmetic statistics (Lercier et al., 2014), and mechanical physics (Olive et al., 2017). Moreover, this construction could shed light on rationality questions for some moduli spaces of hypersurfaces or curves.

Let n and d be positive integers, and let K be an algebraically closed field of characteristic 0 or $p > d$. Take W as a $(n + 1)$ -dimensional K vector space with basis w_0, \dots, w_n and dual

Email address: `thomas.bouchet@univ-cotedazur.fr` (Thomas Bouchet)

basis x_0, \dots, x_n , and define $\text{Sym}^d(W^*)$ as the space of $(n+1)$ -ary d -forms with coefficients in K , which is of dimension $\binom{n+d}{d}$.

Let $G = \text{SL}_{n+1}$ or GL_{n+1} . The group G acts naturally on W by left multiplication

$$(g, v) \mapsto gv,$$

which induces a contragredient G -action on W^*

$$(g, x) \mapsto {}^t g^{-1}x,$$

where x is written in coordinates in the basis x_0, \dots, x_n .

These actions extend to $\text{Sym}^d(W)$ and $\text{Sym}^d(W^*)$, and we write

$$M \cdot f$$

for the action of $M \in G$ on $f \in \text{Sym}^d(W)$ or $\text{Sym}^d(W^*)$. Moreover, we say that $f, f' \in \text{Sym}^d(W^*)$ are G -equivalent if one can transform f into f' with the action of an element of G . We call *stabilizer* G_f of a form $f \in \text{Sym}^d(W^*)$ the subgroup of matrices $M \in G$ that satisfy

$$M \cdot f = f.$$

For $G = \text{GL}_{n+1}$, we always have

$$U_d = \{\mu I_{n+1} \mid \mu \in K, \mu^d = 1\} \subseteq G_f.$$

For $G = \text{SL}_{n+1}$, we have a similar inclusion

$$U_d = \{\mu I_{n+1} \mid \mu \in K, \mu^d = 1, \mu^{n+1} = 1\} \subseteq G_f.$$

We say that G_f/U_d is the *reduced stabilizer* of f . The reduced stabilizer does not depend on the choice of $G \in \{\text{SL}_{n+1}, \text{GL}_{n+1}\}$.

We let $K[\text{Sym}^d(W^*)]^{\text{SL}_{n+1}}$ be the algebra of invariant functions on $\text{Sym}^d(W^*)$ for the action of SL_{n+1} . Since SL_{n+1} is reductive, a celebrated theorem of Nagata (1964) states that this algebra of invariants is finitely generated. Let us assume that a finite set of generators $\{I_j\}_{j \in J}$ of $K[\text{Sym}^d(W^*)]^{\text{SL}_{n+1}}$ is known.

We define the *nullcone*

$$\mathcal{N}_{\text{Sym}^d(W^*)}^{\text{SL}_{n+1}} = \{f \in \text{Sym}^d(W^*) \mid \forall I \in K[\text{Sym}^d(W^*)]_{>0}^{\text{SL}_{n+1}}, I(f) = 0\}.$$

Morally speaking, the nullcone is composed of the degenerate orbits of the variety.

Let us define

$$\text{Sym}^d(W^*)^{ss} = \text{Sym}^d(W^*) \setminus \mathcal{N}_{\text{Sym}^d(W^*)}^{\text{SL}_{n+1}}.$$

The elements of $\text{Sym}^d(W^*)^{ss}$ are called *semistable*. Finally, we let $\text{Sym}^d(W^*)^s$ denote the subvariety of $\text{Sym}^d(W^*)^{ss}$ consisting of the semistable elements with a closed orbit and finite stabilizer. Such elements are called *stable*. For instance, homogeneous forms for $n \geq 2$ and $d \geq 3$ which define smooth hypersurfaces are stable (Dolgachev, 2003, Chapter 8).

Our problem is as follows: let $f \in \text{Sym}^d(W^*)$ be stable, and suppose we are given only its orbit under the action of GL_{n+1} or SL_{n+1} as a list of invariants $(I_j(f))_{j \in J}$. Can we explicitly find an element $f' \in \text{Sym}^d(W^*)$ with the same invariants as f ?

In this paper, we present an efficient algorithm which solves this problem generically. In some favorable cases, such as binary forms of odd degrees, or ternary forms of degrees not multiple of 3, the coefficients of the form f' are invariants (see Section 5).

Unlike previous approaches that rely on Clebsch formulas (Clebsch, 1870), our method is built upon the theory of covariants, linear algebra, and classical tools of algebraic geometry. We are able to characterize a general form f by equations whose coefficients are invariants, or quotients of invariants, in a larger space obtained through a Veronese morphism. These results are established in Theorem 2.5.1 and its Corollary 2.5.2, with the key ingredient being a Taylor-like identity (Corollary 2.2.5).

Main result 1 (see Corollary 3.2.1). *Let k and n be positive integers, and let K be an algebraically closed field of characteristic 0 or $p > d$. Let W be a K -vector space of dimension $n+1$. There exists an efficient algorithm, which, given a list of generating invariants $(I_j(f))_{j \in J}$ corresponding to the orbit of some unknown $f \in \text{Sym}^k(W^*)$ which satisfies mild assumptions, returns a form $f' \in \text{Sym}^k(W^*)$ with those invariants.*

In general, we require K to be algebraically closed because the reconstructed form f' may a priori lie in a finite extension of the base field of the invariants. However, in practice, we aim to keep these extensions as small as possible (see Remark 3.1.2). The case where the covariants have degree 1 is of great interest and is discussed in Remark 3.3.2. In this case, the reconstruction yields a polynomial whose coefficients lie in the same field as the invariants.

It remains to determine when the assumptions of Theorem 2.5.1 are satisfied.

Main result 2 (see Proposition 4.0.3). *Let n and k be positive integers. We let K be an algebraically closed field of characteristic 0, and W be a K -vector space of dimension $n + 1$. Our algorithm can reconstruct any list of invariants $(I_j(f))_{j \in J}$ corresponding to a stable $f \in \text{Sym}^k(W^*)$ with trivial reduced stabilizer.*

In particular, we get a strong result for the reconstruction of hypersurfaces.

Main result 3 (see Corollary 4.0.4). *Let $n \geq 2$ and $k \geq 3$ be integers. We let K be an algebraically closed field of characteristic 0, and W a K -vector space of dimension $n + 1$. Let $f \in \text{Sym}^k(W^*)$. Our algorithm can reconstruct any list of invariants $(I_j(f))_{j \in J}$ corresponding to a form f which defines a smooth hypersurface without automorphisms.*

Note that the condition on the stabilizer is not a necessary one, as illustrated by Cardona and Quer (2005) in the case of binary forms of degree 6 with stabilizer C_2 , which can be reconstructed using Mestre's algorithm with a different set of covariants than the generic case.

Finally, we revisit the reconstruction of binary forms and plane quartics in Section 5, and extend our algorithm to reconstruct non-hyperelliptic curves of genus 4. In these cases, the formulas are remarkably simple, and the reconstructed equations have coefficients in the field where the invariants lie, or an extension of degree at most 2 for binary forms of even degrees.

Eventhough this algorithm works in all generality, there are very few instances where it can be effectively applied. Indeed, generators of the rings of invariants $K[\text{Sym}^d(W^*)]^{\text{SL}_{n+1}}$ are not known in general, except for small values of d and n .

We provide a MAGMA (Bosma et al., 1997) package for the reconstruction of generic non-hyperelliptic curves of genus 3 and 4 (Bouchet, 2024b). To a generic tuple of Dixmier-Ohno invariants, the function `ReconstructionGenus3` returns a plane quartic with these invariants (up to some weighted projective equivalence). Similarly, to a generic tuple of invariants of non-hyperelliptic genus 4 curves (Bouchet, 2024a), the function `ReconstructionGenus4` returns a quadratic form Q and a cubic form E such that the non-hyperelliptic curve of genus 4 canonically embedded in \mathbb{P}^3 defined by Q and E has said invariants. Both cases $\text{rk}(Q) = 3, 4$ are covered, as well as the reconstruction of hyperelliptic curves of genus 4 from the 106 invariants exhibited by Brouwer and Popoviciu (2010).

2. Reconstruction

In this section, we introduce the building blocks of the paper and expose a key identity (Corollary 2.2.5). We then move on to invariant theory, and apply the previously established results to prove the main Theorem 2.5.1.

Let $n, d > 0$ be integers, and let K be an algebraically closed field. Let W be a K -vector space with basis w_0, \dots, w_n , and let $x_0, \dots, x_n \in W^*$ denote its dual basis.

2.1. Preliminaries

In this section, we introduce a bilinear operator D which is equivariant in some sense. This operator can produce new covariants/contravariants from old ones (see Lemma 2.4.6).

Definition 2.1.1. We extend the natural pairing $W \times W^* \rightarrow K$ to the K -bilinear map

$$\begin{aligned} D : \text{Sym}(W) \times \text{Sym}(W^*) &\longrightarrow \text{Sym}(W^*) \\ (w_0^{\alpha_0} \cdots w_n^{\alpha_n}, P) &\longmapsto \frac{\partial^\alpha P}{\partial x_0^{\alpha_0} \cdots \partial x_n^{\alpha_n}} \end{aligned} \quad ,$$

where $\alpha = \sum_i \alpha_i$.

We also define $D : \text{Sym}(W^*) \times \text{Sym}(W) \rightarrow \text{Sym}(W)$ in a symmetric way. The order of the arguments resolves any ambiguity. The bilinear map D is classically called the *apolarity bilinear form* Ehrenborg and Rota (1993); Dolgachev (2012), and gives an isomorphism $\text{Sym}^d(W^*) \simeq \text{Sym}^d(W)^*$ over a field of characteristic 0 or $p > d$.

Remark 2.1.2. This map can be used to tackle the Waring problem for forms Ehrenborg and Rota (1993). The Waring problem consists, given a form $f \in \text{Sym}^d(W^*)$, in finding the minimal number of linear forms such that f can be written the sum of the d -th powers of these linear forms. For example, a generic ternary quintic can be written as the sum of 7 fifth powers (Ehrenborg and Rota, 1993, Corollary 4.3).

Definition 2.1.3. Let $d > 0$. We assume that $\text{char}(K)$ is either 0 or $p > d$. Let q_0, \dots, q_r be a basis of the K -vector space $\text{Sym}^d(W^*)$. We say that $q_0^*, \dots, q_r^* \in \text{Sym}^d(W)$ is a dual basis for q_0, \dots, q_r , if for any $0 \leq i, j \leq r$ we have

$$D(q_i^*, q_j) = \delta_{i,j} \ ,$$

where $\delta_{i,j}$ is the Kronecker symbol.

Lemma 2.1.4. We assume that $\text{char}(K)$ is either 0 or $p > d$. Let $p_0, \dots, p_r \in \text{Sym}^d(W)$ and $q_0, \dots, q_r \in \text{Sym}^d(W^*)$. Then the matrix

$$M_{p,q} := (D(p_i, q_j))_{i,j}$$

is invertible if and only if $(p_i)_i$ and $(q_j)_j$ are bases of their respective spaces.

Lemma 2.1.5. We assume that $\text{char}(K)$ is either 0 or $p > d$. Let q_0, \dots, q_r be a basis of $\text{Sym}^d(W^*)$, and let q_0^*, \dots, q_r^* be its dual basis. Let b_i denote the i -th element of the canonical monomial basis, in lexicographical order, for $0 \leq i \leq r$. Let S be the change of basis matrix from $(b_i)_i$ to $(q_i)_i$. Then ${}^t S^{-1}$ is the change of basis matrix from $(b_i^*)_i$ to $(q_i^*)_i$.

2.2. Main identity

Let k, d , and $n > 0$ be integers. We assume that $\text{char}(K) > kd$ or $\text{char}(K) = 0$. Now, let W be a K -vector space with basis w_0, \dots, w_n , and dual basis x_0, \dots, x_n . In this paragraph, we show an identity which allows to recover $f \in \text{Sym}^{kd}(W^*)$ from its D -pairings with the k -products of a basis of $\text{Sym}^d(W)$, identified as elements of $\text{Sym}^{kd}(W)$.

Definition 2.2.1. Let $d \geq 1$, and $\alpha_0, \dots, \alpha_n \geq 0$ be integers of sum d . We define the multinomial coefficient associated to $(\alpha_i)_i$ as

$$\binom{d}{\alpha_0, \dots, \alpha_n} = \frac{d!}{\alpha_0! \cdots \alpha_n!}.$$

Lemma 2.2.2. For any integers $\alpha_0, \dots, \alpha_n \geq 0$ of sum kd , we define

$$J_\alpha = \left\{ (\beta_{i,j})_{\substack{1 \leq i \leq k \\ 0 \leq j \leq n}} \in \mathbb{Z}_{\geq 0}^{k \times (n+1)} \mid \sum_{l=0}^n \beta_{i,l} = d, \sum_{l=1}^k \beta_{l,j} = \alpha_j \right\},$$

where $\alpha = (\alpha_i)_{0 \leq i \leq n}$. We have the following equality:

$$\sum_{(\beta_{i,j}) \in J_\alpha} \binom{d}{\beta_{1,0}, \dots, \beta_{1,n}} \cdots \binom{d}{\beta_{k,0}, \dots, \beta_{k,n}} = \binom{kd}{\alpha_0, \dots, \alpha_n}. \quad (1)$$

Proof. The coefficients of $x_0^{\alpha_0} \cdots x_n^{\alpha_n}$ in $(x_0 + \dots + x_n)^{kd}$ and in $(x_0 + \dots + x_n)^d \cdots (x_0 + \dots + x_n)^d$ are equal. By computing these numbers, we obtain Equation (1). \square

We now prove a Taylor-like identity, which is at the heart of the algorithm.

Proposition 2.2.3. Let $f \in \text{Sym}^{kd}(W^*)$, let b_0, \dots, b_r denote the canonical monomial basis of $\text{Sym}^d(W^*)$ in lexicographical order, and let b_0^*, \dots, b_r^* be its dual basis. Then we have

$$\frac{(kd)!}{d!^k} f = \sum_{0 \leq i_1, \dots, i_k \leq r} D(b_{i_1}^* \cdots b_{i_k}^*, f) b_{i_1} \cdots b_{i_k}. \quad (2)$$

Proof. Since D is bilinear, we prove that statement for monomials.

Let $f = x_0^{\alpha_0} \cdots x_n^{\alpha_n} \in \text{Sym}^{kd}(W^*)$. Further, if we write $b_i = \prod_{j=0}^n x_j^{\gamma_{i,j}}$, where $\gamma_{i,j}$ is a nonnegative integer, then for any integers $0 \leq i_1, \dots, i_k \leq r$, we have

$$b_{i_1} \cdots b_{i_k} = \prod_{j=0}^n x_j^{\sum_{l=1}^k \gamma_{i_l,j}} = \prod_{j=0}^n x_j^{\sum_{l=1}^k \beta_{l,j}},$$

where we set $\beta_{l,j} = \gamma_{i_l,j}$.

We compute the right member of Equation (2):

$$\begin{aligned}
& \sum_{0 \leq i_1, \dots, i_k \leq r} D(b_{i_1}^* \cdots b_{i_k}^*, f) b_{i_1} \cdots b_{i_k} \\
&= \sum_{0 \leq i_1, \dots, i_k \leq r} D(b_{i_1}^* \cdots b_{i_k}^*, f) b_{i_1} \cdots b_{i_k} \\
&= \sum_{\substack{(\beta_{l,j}) \in \mathbb{Z}_{\geq 0}^{k \times (n+1)} \\ \forall l, \sum_{j=0}^n \beta_{l,j} = d}} D\left(\frac{1}{\beta_{1,0}! \cdots \beta_{k,n}!} w_0^{\sum_{l=1}^k \beta_{l,0}} \cdots w_n^{\sum_{l=1}^k \beta_{l,n}}, f\right) x_0^{\sum_{l=1}^k \beta_{l,0}} \cdots x_n^{\sum_{l=1}^k \beta_{l,n}} \\
&= \sum_{(\beta_{l,j}) \in J_\alpha} \frac{\alpha_0! \cdots \alpha_n!}{\beta_{1,0}! \cdots \beta_{k,n}!} f \\
&= \frac{\alpha_0! \cdots \alpha_n!}{d!^k} \sum_{(\beta_{l,j}) \in J_\alpha} \frac{d!}{\prod_{j=0}^n \beta_{1,j}!} \cdots \frac{d!}{\prod_{j=0}^n \beta_{k,j}!} f \\
&= \frac{\alpha_0! \cdots \alpha_n!}{d!^k} \sum_{(\beta_{l,j}) \in J_\alpha} \binom{d}{\beta_{1,0}, \dots, \beta_{1,n}} \cdots \binom{d}{\beta_{k,0}, \dots, \beta_{k,n}} f \\
&= \frac{\alpha_0! \cdots \alpha_n!}{d!^k} \binom{kd}{\alpha_0, \dots, \alpha_n} f \\
&= \frac{(kd)!}{d!^k} f.
\end{aligned}$$

Since $\text{char}(K) > kd$ or $\text{char}(K) = 0$, all the operations above are well-defined. \square

A somewhat similar computation is carried out in (Ehrenborg and Rota, 1993, Proposition 3.2).

Remark 2.2.4. To avoid problems in positive characteristic, the author also tried to use Hasse-Schmidt derivatives (Schmidt and Hasse, 1937) instead of partial derivatives. However, the factorial numbers do not cancel out with the Hasse Derivative as we might expect, thus the conditions on the characteristic of K must remain.

Corollary 2.2.5. *Let $f \in \text{Sym}^{kd}(W^*)$, let q_0, \dots, q_r be a basis of $\text{Sym}^d(W^*)$, and let q_0^*, \dots, q_r^* denote its dual basis. Then we have*

$$\frac{(kd)!}{d!^k} f = \sum_{0 \leq i_1, \dots, i_k \leq r} D(q_{i_1}^* \cdots q_{i_k}^*, f) q_{i_1} \cdots q_{i_k}. \quad (3)$$

Proof. We use Lemma 2.1.5 and Proposition 2.2.3 to compute the right hand side of Equation (3). After some simplifications, we obtain the desired result. \square

Let us introduce the Veronese embedding that maps $[x_0 : \cdots : x_n]$ to all monomials of total degree d :

$$\begin{aligned}
v_{n,d} : \quad \mathbb{P}^n &\longrightarrow \mathbb{P}^r \\
[x_0 : \cdots : x_n] &\longmapsto [x_0^d : x_0^{d-1}x_1 : \cdots : x_n^d] \quad .
\end{aligned}$$

It is well-known that $v_{n,d}$ realizes an isomorphism of \mathbb{P}^n onto its image, which is defined by irreducible quadratic forms (Harris, 1992, Exercise 2.5). Let X_0, \dots, X_r denote coordinates for \mathbb{P}^r . These quadratic forms can be written as $X_i X_j - X_l X_m$ for some well-chosen i, j, l , and m , where we can have $i = j$ or $l = m$. The number of linearly independent such quadratic forms is

$$\dim(\text{Sym}^2(\text{Sym}^d(W^*))) - \dim(\text{Sym}^{2d}(W^*)).$$

Let q_0, \dots, q_r be a basis of $\text{Sym}^d(W^*)$. It is clear that the morphism

$$\begin{aligned}
\varphi : \quad \mathbb{P}^n &\longrightarrow \mathbb{P}^r \\
[x_0 : \cdots : x_n] &\longmapsto [q_0 : \cdots : q_r]
\end{aligned}$$

is also an isomorphism of \mathbb{P}^n onto its image, which is defined by irreducible quadratic forms, which reflect the relations that exist among the q_i 's.

This paper relies heavily on the following key result.

Proposition 2.2.6. *Let*

$$\tilde{f} = \sum_{0 \leq i_1, \dots, i_k \leq r} D(q_{i_1}^* \cdots q_{i_k}^*, f) X_{i_1} \cdots X_{i_k},$$

and let Q_0, \dots, Q_s be a set of quadratic forms which define $\text{Im}(\varphi)$.

Then, the knowledge of \tilde{f} and the Q_i 's is enough to recover $f' \in \text{Sym}^{kd}(W^*)$ which is GL_{n+1} -equivalent to f .

Proof. We assume that φ and f are not known, otherwise the statement becomes trivial.

We know that there exists a parametrization of $\text{Im}(\varphi)$, because φ is one of them. Let $\varphi' : \mathbb{P}^n \rightarrow \mathbb{P}^r$ be any such parametrization. Since φ and φ' have the same image, we can consider the automorphism $\varphi^{-1} \circ \varphi'$ of \mathbb{P}^n , and it is known that the group of automorphisms of \mathbb{P}^n is PGL_{n+1} (Harris, 1992, Exercise 18.7). Thus, the parametrizations φ and φ' differ only by an element of PGL_{n+1} .

If we let $q'_0, \dots, q'_r \in \text{Sym}^d(W^*)$ be coordinates of φ' , then $\tilde{f}(q'_0, \dots, q'_r)$ is GL_{n+1} -equivalent to f by the previous analysis. \square

Remark 2.2.7. The parametrization step in that proof is not constructive. To develop an effective and efficient algorithm, we require a constructive approach. Section 3.1 addresses this in detail.

It remains to see how we can write the coefficients of \tilde{f} and the quadratic relations Q_i as invariants. The use of a linear basis of covariants of a given degree will be primordial to achieve that goal.

2.3. Generalization to tensor spaces

Equation (3) can be extended to tensor spaces. Let W_1, \dots, W_s be finite-dimensional K -vector spaces. Let D_s denote the composition of the operators D for W_1, \dots, W_s . In that situation, a similar statement as Corollary 2.2.5 can be made.

Proposition 2.3.1. *Let $k, d_1, \dots, d_s > 0$. Let $f \in \text{Sym}^{kd_1}(W_1^*) \otimes \dots \otimes \text{Sym}^{kd_s}(W_s^*)$, and let q_0, \dots, q_r be a basis of $\text{Sym}^{d_1}(W_1^*) \otimes \dots \otimes \text{Sym}^{d_s}(W_s^*)$. Let q_0^*, \dots, q_r^* denote its dual basis with respect to D_s (such a basis exists, and is unique). Then we have*

$$\frac{(kd_1)!}{d_1!^k} \dots \frac{(kd_s)!}{d_s!^k} f = \sum_{0 \leq i_1, \dots, i_k \leq r} D_s(q_{i_1}^* \dots q_{i_k}^*, f) q_{i_1} \dots q_{i_k}. \quad (4)$$

This can be proven by induction on s , since D acts independently and successively on the different spaces W_i .

Let us define a morphism φ , which associates to a point of $\prod_i \mathbb{P}^{\dim(W_i)-1}$ the q_j 's evaluated at this point. Its image is a Segre-Veronese variety, and φ realizes an isomorphism of the projective variety $\prod_i \mathbb{P}^{\dim(W_i)-1}$ onto its image. The algorithmic solution for the parametrization presented in Section 3.1 extends naturally to that case.

2.4. Invariant theory

In this section, we introduce some notions of invariant theory.

Let n and d be positive integers, and let K be an algebraically closed field. Take W as a $(n+1)$ -dimensional K vector space.

Definition 2.4.1. Let $k > 0$ and $r \geq 0$ be integers. A *covariant* (resp. *contravariant*) of $\text{Sym}^k(W^*)$ of order r is an $\text{SL}(W)$ -equivariant homogeneous polynomial map

$$C : \text{Sym}^k(W^*) \rightarrow \text{Sym}^r(W^*)$$

(resp. $C : \text{Sym}^k(W^*) \rightarrow \text{Sym}^r(W)$).

The *degree* d of C is its degree as a homogeneous polynomial map. In the special case $r = 0$, C is called an *invariant*. Moreover, the *weight* (or index) of a covariant the number $(kd - r)/(n+1)$ (resp. $(kd + r)/(n+1)$).

Remark 2.4.2. In fact, when a covariant is transformed by a matrix $A \in \text{GL}_{n+1}$, we have

$$C(A \cdot f) = \det(A)^{-\frac{kd-r}{n+1}} (A \cdot C(f)),$$

for any $f \in \text{Sym}^k(W^*)$. In order for this expression to be well-defined, the weight must be an integer.

Thus, we note that given a value of k and n , not all values of d and r give an integer. For instance, the case of binary forms of even degrees, corresponding to $k = 2k'$ and $n = 1$, implies that r must be even. Thus there exist no covariants of odd degree for binary forms of even degree.

Definition 2.4.3. Let $f \in \text{Sym}^k(W^*)$. We say that the covariants (or contravariants) q_1, \dots, q_r of order d of $\text{Sym}^k(W^*)$ are *linearly independent at f* if the forms $q_i(f)$ are linearly independent.

We say that the q_i 's are *generically linearly independent* if there exists a dense open subvariety

$$U \subseteq \text{Sym}^k(W^*)/\text{SL}_{n+1} = \text{Spec}(K[\text{Sym}^k(W^*)]^{\text{SL}_{n+1}})$$

such that for every $f \in U$, the q_i 's are linearly independent at f .

Remark 2.4.4. Since the quotient variety $\text{Sym}^k(W^*)/\text{SL}_{n+1} = \text{Spec}(K[\text{Sym}^k(W^*)]^{\text{SL}_{n+1}})$ is affine by definition, and its coordinate ring is a domain, the variety $\text{Sym}^k(W^*)/\text{SL}_{n+1}$ is irreducible. Therefore, if there exists one $f \in \text{Sym}^k(W^*)$ such that the q_i 's are linearly independent at f , it means that the q_i 's are generically linearly independent.

To construct covariants and contravariants, one usually starts with a form whose coefficients are indeterminates, and then applies equivariant transformations. The apolarity bilinear operator D turns out to be equivariant in a sense that we will explore (see Lemma 2.4.6). Another valuable tool is the transvectant (Olver, 1999), which is traditionally used for the description of the algebra of covariants and invariants of binary forms.

However, in general, it is not possible to construct all covariants and invariants through repeated iterations of the transvectant. We refer the interested reader to Girard and Kohel (2006), in which the authors recall several ways to construct covariants and contravariants. We now show how the apolar bilinear form D defined in Definition 2.1.1 can be used to construct covariants and contravariants.

Definition 2.4.5. Let p be a contravariant of order r_p of $\text{Sym}^d(W^*)$, and let q be a covariant of order r_q of $\text{Sym}^d(W^*)$. We define $D(p, q)$ pointwise:

$$[D(p, q)](f) = D(p(f), q(f)) \in \text{Sym}^{r_q - r_p}(W^*)$$

for all $f \in \text{Sym}^d(W^*)$, with the convention that $\text{Sym}^{-r}(W^*) = \{0\}$ for any positive integer r . We define symmetrically $D(p, q)$ by

$$[D(q, p)](f) = D(q(f), p(f)) \in \text{Sym}^{r_p - r_q}(W^*)$$

for all $f \in \text{Sym}^d(W^*)$.

Lemma 2.4.6. Let p be a contravariant of $\text{Sym}^d(W^*)$ and q a covariant of $\text{Sym}^d(W^*)$ of respective orders r_p, r_q and degrees d_p, d_q . Then $D(p, q)$ (resp. $D(q, p)$) is a covariant (resp. contravariant) of $\text{Sym}^d(W^*)$ of degree $d_p + d_q$.

Lemma 2.4.7. Let $r = \dim_K(\text{Sym}^d(W^*)) - 1$, and let l be a positive integer. Let q_0, \dots, q_r be covariants of order d of $\text{Sym}^l(W^*)$, which are generically linearly independent. Let S be the change of basis matrix from the canonical basis $(b_i)_i$ of $\text{Sym}^d(W^*)$ to $(q_i)_i$, and let Δ be its determinant. Then Δ is a non-zero invariant of $\text{Sym}^l(W^*)$, and $\Delta^t S^{-1}$ is a matrix whose columns are contravariants, precisely the dual basis q_0^*, \dots, q_r^* multiplied by the invariant Δ .

2.5. Main theorem

We have all the tools at our disposal to present the main results of this paper, Theorem 2.5.1 and its Corollary 2.5.2.

Theorem 2.5.1. Let k, d , and n be positive integers. Let K be an algebraically closed field of characteristic 0 or $p > kd$. Let W be a K -vector space with basis w_0, \dots, w_n and dual basis x_0, \dots, x_n . Let $f \in \text{Sym}^{kd}(W^*)$, and let $r = \dim_K(\text{Sym}^d(W^*)) - 1$. We assume that there exist $r + 1$ covariants of order d of $\text{Sym}^{kd}(W^*)$ which are linearly independent at f . Let q_0, \dots, q_r be such covariants. Let us define

$$\begin{aligned} \varphi : \quad \mathbb{P}^n &\longrightarrow \mathbb{P}^r \\ [x_0 : \dots : x_n] &\longmapsto [q_0(f) : \dots : q_r(f)] \end{aligned} .$$

Let X_0, \dots, X_r be coordinates for \mathbb{P}^r . We define

$$\tilde{f} = \sum_{0 \leq i_1, \dots, i_k \leq r} D(\Delta q_{i_1}^* \cdots \Delta q_{i_k}^*, \text{Id})(f) X_{i_1} \cdots X_{i_k},$$

where Id is the identity covariant of $\text{Sym}^{kd}(W^*)$, and we let Q_0, \dots, Q_s be a set of quadratic forms in the X_i 's which define $\text{Im}(\varphi)$.

The coefficients of \tilde{f} are invariants of $\text{Sym}^{kd}(W^*)$, and the coefficients of the Q_i 's can be chosen to have coefficients which can be computed in terms of invariants of $\text{Sym}^{kd}(W^*)$.

Moreover, the knowledge of \tilde{f} and the Q_i 's is enough to recover $f' \in \text{Sym}^{kd}(W^*)$ which is GL_{n+1} -equivalent to f .

Proof. Let us further assume that φ and f are unknown (otherwise the statement is trivial). Let $\Delta q_0^*, \dots, \Delta q_r^*$ be the set of contravariants defined in Lemma 2.4.7 of $\text{Sym}^{kd}(W^*)$. By assumption, they are linearly independent at f .

It is clear by Lemma 2.4.6 that the coefficients of \tilde{f} are invariants of $\text{Sym}^{kd}(W^*)$. Remains to see how we can compute quadratic forms defining the image of φ with invariants.

The image of φ is defined by quadratic forms that reflect the relations between the $q_i(f)$'s. We note that the family $(\Delta q_i^*(f)\Delta q_j^*(f))_{0 \leq i,j \leq r}$ generates the space $\text{Sym}^{2d}(W)$, and D is non-degenerate. Therefore for any $Q \in \text{Sym}^{2d}(W^*)$ we have

$$(\forall 0 \leq i, j \leq r, D(\Delta q_i^*(f)\Delta q_j^*(f), Q) = 0) \iff Q = 0.$$

Thus, one way to find a basis of quadratic relations for the $q_i(f)$'s is to compute the right kernel of the $(r+1)^2 \times (r+1)^2$ matrix of invariants

$$(D(\Delta q_i^* \Delta q_j^*, q_l q_m)(f))_{\substack{0 \leq i,j \leq r \\ 0 \leq l,m \leq r}}.$$

Finally, the last part of the result is a direct consequence of Proposition 2.2.6, applied to the basis of covariants $q_0(f), \dots, q_r(f)$ and its dual basis (up to Δ) $\Delta q_0^*(f), \dots, \Delta q_r^*(f)$. \square

Corollary 2.5.2. *For a general $f \in \text{Sym}^{kd}(W^*)$, knowing only the values of the invariants*

$$D(\Delta q_{i_1}^* \cdots \Delta q_{i_k}^*, \text{Id})(f)$$

for $0 \leq i_1, \dots, i_k \leq r$ and

$$(D(\Delta q_i^* \Delta q_j^*, q_l q_m)(f))_{\substack{0 \leq i,j \leq r \\ 0 \leq l,m \leq r}},$$

is theoretically enough to recover a form $f' \in \text{Sym}^{kd}(W^*)$ which is GL_{n+1} -equivalent to f .

In practice, it is hard to find a parametrization φ' from the Q_i 's in practice. We will see an algorithmic solution to this problem for small values of r .

3. Reconstruction algorithm

In this section, we present a reconstruction algorithm, which, given a set of specialized generating invariants of $K[\text{Sym}^{kd}(W^*)]^{\text{SL}_{n+1}}$, returns an element of $\text{Sym}^{kd}(W^*)$ with said invariants. It relies on Theorem 2.5.1, and a parametrization algorithm.

Let k, d , and n be positive integers. Let W be a K -vector space with basis w_0, \dots, w_n and dual basis x_0, \dots, x_n . Let $r = \dim_K(\text{Sym}^d(W^*)) - 1$. Let us assume that there exist $r+1$ covariants of order d of $\text{Sym}^{kd}(W^*)$ which are generically linearly independent, and we take q_0, \dots, q_r to be such covariants.

3.1. Finding a parametrization

We turn to the problem of finding a parametrization of φ from a set of quadratic forms defining its image, which is a special instance of a challenging problem, concerned with the parametrization of a projective variety from its implicit representation. Notably, the reverse problem of finding an implicit representation from a parametrization is an equally interesting question which is also hard to solve efficiently.

Our approach leverages the particular geometry of our problem to give an algorithmic solution. The central idea is that we know a parametrization of the canonical Veronese embedding. By performing a suitable change of basis, we can reduce the problem to the case where the quadratic forms correspond to those defining the image of the canonical Veronese embedding.

Let $q = (q_i)$ be a basis of $\text{Sym}^d(W^*)$, and let $q^* = (q_i^*)$ denote its dual basis. We define

$$Q_{q^*,q} = (D(q_i^* q_j^*, q_l q_m))_{\substack{0 \leq i,j \leq r \\ 0 \leq l,m \leq r}}.$$

Let $f \in \text{Sym}^{kd}(W^*)$ such that there exist $r+1$ covariants of $\text{Sym}^d(W^*)$ which are linearly independent at f , which we take to be q_0, \dots, q_r . We can form the matrix $Q_{q(f)^*,q(f)}$, and the matrix $Q_{b^*,b}$, where $b = (b_i)$ denotes the canonical monomial basis of $\text{Sym}^d(W^*)$ in lexicographic order, and b^* its dual basis. Our aim is to find a change of basis to transform $Q_{q(f)^*,q(f)}$ into $Q_{b^*,b}$, in a way which is given by the next lemma.

Lemma 3.1.1. *For any $M \in \text{GL}_{r+1}$, we have*

$$Q_{Mq(f)^*, {}^t M^{-1}q(f)} = (M \otimes M) Q_{q(f)^*,q(f)} (M \otimes M)^{-1}.$$

Thus, our algorithmic solution is to try and find a matrix $M \in \text{GL}_{r+1}$ such that

$$Q_{b^*,b} = (M \otimes M) Q_{q(f)^*,q(f)} (M \otimes M)^{-1},$$

or equivalently

$$Q_{b^*,b}(M \otimes M) = (M \otimes M) Q_{q(f)^*,q(f)}. \quad (5)$$

We know that there exists a matrix M satisfying these equations, which is the change of basis from the basis $q(f)$ to b . Unfortunately $\varphi(f) = q(f)$ is not known, thus we need to understand how to obtain a solution to Equation (5). Let us consider $M = (m_{i,j})$ as a matrix of $(r+1)^2$ indeterminates.

Then by changing $p(f)$ into $Mp(f)$, and $p(f)^*$ into ${}^tM^{-1}p(f)^*$, the quadratic relations we obtain are the ones corresponding to the canonical embedding. Equation (5) becomes a system of $(r+1)^4$ quadratic equations in $(r+1)^2$ indeterminates. In our area of application, we can solve that system by computing a Noether normalization (Derksen and Kemper, 2015, Lemma 2.5.7). This yields a linear combination of variables which are algebraically independent $(m_l)_{l \in L}$, where $L \subseteq \{(i, j) \mid 0 \leq i, j \leq r\}$. Moreover, any other variable m_l for $l \notin L$ satisfies an integral relation on $K[m_l \mid l \in L]$.

Therefore we can for instance assign arbitrary values to the indeterminates m_l for $l \in L$, and finding the rest of the indeterminates then amounts to taking some field extensions.

Once a solution is known, we update $\tilde{f}(X)$ to $g := \tilde{f}({}^tMX)$, and the form

$$g(b) = g(x_0^d, x_0^{d-1}x_1, x_0^{d-1}x_2, \dots, x_n^d) \in \text{Sym}^{kd}(W^*)$$

is GL_{n+1} -equivalent to f .

Remark 3.1.2. The author does not know how to control the size of the field extensions over which the parametrization is computed. There might exist an approach to this specific instance of the parametrization problem which would always compute a parametrization over the smallest possible field, but the author is not aware of it.

In practice, one should try as much as possible to use covariants of small orders to reduce the degrees of the fields extensions.

The most favorable case is when the covariants are of degree 1. Then \tilde{f} belongs to $\text{Sym}^{kd}(W^*)$, and is directly GL_{n+1} -equivalent to f . In addition, the coefficients of \tilde{f} lie in the field where the invariants of f live.

Unfortunately sometimes covariants of order 1 do not exist. For instance, binary forms of even degree only have covariants of degree 2. The image of φ is always a conic, and can be parametrized if it has a rational point. Otherwise, the parametrization is defined over a quadratic extension of the field in which the invariants lie.

For other higher degrees or greater number of variables, there exist several quadratic relations, and the algorithm can be quite impractical.

3.2. Main algorithm

We derive a reconstruction algorithm from Corollary 2.5.2.

Corollary 3.2.1. *Let k, d , and n be positive integers. Let K be an algebraically closed field of characteristic 0 or $p > kd$. Let W be a K -vector space with basis w_0, \dots, w_n and dual basis x_0, \dots, x_n , and let $r = \dim_K(\text{Sym}^d(W^*)) - 1$. We assume that there exist q_0, \dots, q_r covariants of order d which are generically linearly independent. Let $(I_j)_{j \in J}$ be a (finite) set of generators of $K[\text{Sym}^{kd}(W^*)]^{\text{SL}_{n+1}}$.*

There exists an algorithm, which, given $(I_j(f))_{j \in J}$ corresponding to $f \in \text{Sym}^{kd}(W^)$ such that q_0, \dots, q_r are linearly independent at f , returns a form $f' \in \text{Sym}^{kd}(W^*)$ with the same invariants as f .*

We explain how to derive such an algorithm from Theorem 2.5.1. Here is a high-level description of this algorithm:

1. The first step (which is done only once for every set of covariants) consists in the pre-calculation of a decomposition on a generating set of invariants of all the invariants required for the computation of \tilde{f} , of the matrix $(D(\Delta q_i^* \Delta q_j^*, q_l q_m))$, and of the invariant $\det(q_0, \dots, q_r)$. That step can be done using an evaluation-interpolation strategy.
2. We can then specialize these formulas to an f represented by a list of invariants $(I_j(f))_{j \in J}$ by evaluating the decomposition polynomials at the values of the generating set of invariants at f . We check the condition of linear independance at f by specializing the invariant $\det(q_0, \dots, q_r)$ at f .
3. If the determinant is not 0, we can parametrize $\text{Im}(\varphi)$ from the quadratic forms by using Section 3.1. Then, we evaluate \tilde{f} on this parametrization, and we recover a form $f' \in \text{Sym}^{kd}(W^*)$ which is GL_{n+1} -equivalent to f .

3.3. Improving the algorithm

In order to be able to use this algorithm in practice, we need to reduce the degrees of the invariants used. Indeed, the degrees of the invariants involved in the formulas in Theorem 2.5.1 can be high, rendering our technique very much not effective.

For instance, if we choose q_1, \dots, q_r generically linearly independent covariants of $\text{Sym}^{kd}(W^*)$ of respective degrees d_1, \dots, d_r , their dual basis $\Delta q_1^*, \dots, \Delta q_r^*$ of contravariants has high degree: $\deg(\Delta q_i^*) = d_i + 2 \sum_{j \neq i} d_j$. Thus the coefficients of f are invariants of very high degrees, hence they are not effectively decomposable on a generating set of invariants.

To remedy this problem, we can choose a set of covariants $q = (q_i)$ and a set of contravariants $p = (p_i)$ of the same order, which generically form a basis of their respective spaces. Then, computing a dual basis $p(f)^*$ of $p(f)$ in terms of $q(f)$ (or the reverse) is just a task of linear algebra, as established in the following lemma.

Lemma 3.3.1. *Let $M_{p,q} = (D(p_i, q_j))_{i,j}$. Then the basis $(p_i(f)^*)_i$ can be expressed using the basis $(q_j(f))_j$. We have in particular*

$$(p_i(f)^*)_i = M_{p,q}^{-1}(q_j(f))_j.$$

Hence, if we let

$$\tilde{f}_{p,q} = \sum_{0 \leq i_1, \dots, i_k \leq r} D(p_{i_1} \cdots p_{i_k}, f) X_{i_1} \cdots X_{i_k},$$

and

$$Q_{p,q} = (D(p_i p_j, q_l q_m)(f))_{\substack{0 \leq i, j \leq r \\ 0 \leq l, m \leq r}},$$

we have

$$\tilde{f}_{p,q}(p_0(f)^*, \dots, p_r(f)^*) = \frac{(kd)!}{d!^k} f,$$

and the quadratic relations between the $p_i(f)^*$ can be known by computing a basis of the right kernel of $Q_{p,q}^t M_{p,q}^{-1}$.

To summarize, here is what need to be precomputed:

1. The decomposition of $D(p_i, q_j)$ for all $0 \leq i, j \leq r$ for the computation of the dual basis of p by inverting $M_{p,q}$.
2. The decomposition of $D(p_i p_j, q_l q_m)$ for all $0 \leq i, j, l, m \leq r$ for the computation of the quadratic forms.
3. The decomposition of $D(p_{i_1} \cdots p_{i_k}, f)$ for all $0 \leq i_1, \dots, i_k \leq r$ for the computation of \tilde{f} .

It consists in a total of $(r+1)^k + (r+1)^4 + (r+1)^2$ invariants, of degrees at most $\max(d_p^2 d_q^2, d_p^k + 1)$, where d_p (resp. d_q) is the maximal degree of the contravariants (resp. covariants).

Remark 3.3.2. When $d = 1$, we have $r = n$, so the morphism φ introduced in Section 2 is just an automorphism of \mathbb{P}^n . Hence, by choosing $n + 1$ contravariants of order d which are linearly independent at f , we obtain

$$\tilde{f} = \sum_{0 \leq i_1, \dots, i_k \leq r} D(p_{i_1}(f) \cdots p_{i_k}(f), f) X_{i_1} \cdots X_{i_k}.$$

Since

$$\tilde{f}(p_0(f)^*, \dots, p_r(f)^*) = \frac{(kd)!}{d!^k} f,$$

it is clear that \tilde{f} and f are GL_{n+1} -equivalent. Moreover, the field over which \tilde{f} is defined is the field in which the invariants lie.

Building on that remark, we provide a new reconstruction algorithm for smooth plane quartics in Section 5.2.

Remark 3.3.3. We note that in the opposite case $k = 1$, the situation is significantly worse: even though the form f itself is a covariant, the number of invariants needed explodes, and the step of parametrization of $\text{Im}(\varphi)$ becomes unmanageable. As a result, in practice, we use $d = 1, 2$ whenever possible.

4. Reconstruction of smooth hypersurfaces

Let K be an algebraically closed field of characteristic 0. Let k, d , and n be positive integers. Let W be a $(n+1)$ -dimensional K -vector space, and let W^* denote its dual. In this paragraph, we show that under mild assumptions on $f \in \text{Sym}^{kd}(W^*)$, there exist $\dim_K(\text{Sym}^d(W^*))$ covariants of $\text{Sym}^{kd}(W^*)$ which are linearly independent at f . We use the notion of stability defined in Mumford's GIT (Mumford et al., 1994). One can find an exposure that suits our needs in (Dolgachev, 2003, Chapters 8,9).

Let us recall an important result.

Proposition 4.0.1 ((Domokos, 2008, Prop 3.1)). *Let G be a linearly reductive group, X an affine G -variety, and W a G -module. If for some $x \in X$ having closed orbit the stabilizer G_x acts trivially on W , then there exist $s = \dim_K(W)$ covariants $F_1, \dots, F_s \in \text{Cov}_G(X, W)$ such that $F_1(x), \dots, F_s(x)$ are linearly independent over K .*

Remark 4.0.2. The linearly reductive condition on G implies that we work over a field of characteristic 0, since GL_{n+1} and SL_{n+1} are not linearly reductive in positive characteristic (Derksen and Kemper, 2015, Theorem 2.2.19). The authors wonders whether the linear reductivity condition can be weakened to work in positive characteristic as well, for example by using the theory of good filtrations (Andersen and Jantzen, 1984; Derksen and Makam, 2021).

Proposition 4.0.3. *For every stable $f \in \text{Sym}^{kd}(W^*)$ with trivial reduced stabilizer, the following statements are equivalent:*

1. *There exist q_0, \dots, q_r covariants of order d which are linearly independent at f ,*
2. $\gcd\left(k, \frac{(n+1)}{\gcd(n+1, d)}\right) = 1$.

Proof. Since the existence of covariants of order d of $\text{Sym}^{kd}(W^*)$ implies the second statement, we only need to prove the converse.

We apply Proposition 4.0.1 with $G = \text{SL}_{n+1}$, $X = \text{Sym}^{kd}(W^*)$, and $W = \text{Sym}^d(W^*)$. Since $\text{char}(K) = 0$, we know that G is linearly reductive Haboush (1975).

It is known that the elements of the stable locus have closed orbit (Dolgachev, 2003, Chapter 8). Now, if let $f \in X$ with trivial reduced stabilizer, we have

$$G_f = \{\lambda \text{Id} \mid \lambda^{kd} = \lambda^{n+1} = 1\}.$$

We derive from this equality that G_f acts trivially on $W = \text{Sym}^d(W^*)$ if and only if for all $\lambda \in G_f$, we have $\lambda^d = 1$. This is the case if and only if $\gcd(kd, n+1) = \gcd(d, n+1)$, and this condition can be rewritten as

$$\gcd\left(k, \frac{n+1}{\gcd(d, n+1)}\right) = 1.$$

In addition, we have

$$\frac{kd\alpha - d}{n+1} = \frac{d}{\gcd(d, n+1)} \cdot \frac{k\alpha - 1}{\frac{n+1}{\gcd(d, n+1)}}.$$

In other words, for any order d for which covariants of $\text{Sym}^{kd}(W^*)$ might exist (meaning for which the weight $\frac{kd\alpha - d}{n+1}$ is an integer), there must exist at least $\dim_K(\text{Sym}^d(W^*))$ generically linearly independent covariants of $\text{Sym}^{kd}(W^*)$.

In that case, we apply Proposition 4.0.1, which implies the existence of the desired covariants. \square

Corollary 4.0.4. *Let us assume that $kd \geq 3$, and that $\gcd\left(k, \frac{(n+1)}{\gcd(n+1, d)}\right) = 1$. For any form $f \in \text{Sym}^{kd}(W^*)$ such that which defines a smooth hypersurface with trivial automorphism group, the reconstruction algorithm (Corollary 3.2.1) applies.*

Proof. According to (Dolgachev, 2003, Theorem 10.1), any non-singular element of $\text{Sym}^{kd}(W^*)$ is stable. Hence, by Proposition 4.0.3, there exist covariants that can be used to meet the requirements of Corollary 3.2.1. \square

Remark 4.0.5. Let C_d be the $K[\text{Sym}^{kd}(W^*)]^{\text{SL}_{n+1}}$ -module of covariants of order d . Since the space of covariants is finitely generated, so is C_d . Let q_0, \dots, q_l be a generating family of C_d . Now let $f \in \text{Sym}^{kd}(W^*)$ be stable such that f has trivial reduced stabilizer. Then there exist $r = \dim_K(\text{Sym}^d(W^*))$ covariants of order d which are linearly independent at f . Hence, there must be r covariants in the set q_0, \dots, q_l which are linearly independent at f .

Therefore, if we have at our disposal a generating set of covariants of a given degree, then we know that any stable $f \in \text{Sym}^{kd}(W^*)$ such that f has trivial reduced stabilizer can be covariantly reconstructed by using only a subset of these generating covariants. Unfortunately, determining such a set of covariants is usually out of reach.

5. Examples

5.1. Binary forms

We turn to the case of binary forms, for which reconstruction algorithms have been found by Mestre (1991) and Noordsij (2022). Let W be a 2-dimensional K -vector space with basis w_0, w_1 and dual basis x_0, x_1 . They used bases of covariants of order 2 and 1 respectively, which enabled them to solve the reconstruction problem for binary forms of even degrees and odd degrees respectively.

Definition 5.1.1. Let $f \in \text{Sym}^d(W^*)$, $g \in \text{Sym}^e(W^*)$ for some positive integers d and e . For any positive integer l , we define the *transvectant* of level l of f and g to be

$$(f, g)_l = \sum_{i=0}^l (-1)^i \binom{l}{i} \frac{\partial^l f}{\partial^i x_0 \partial^{l-i} x_1} \frac{\partial^l g}{\partial^{l-i} x_0 \partial^i x_1} \in \text{Sym}^{d+e-2l}(W^*).$$

Proposition 5.1.2. Let r be a positive integer, and let K be an algebraically closed field of characteristic 0 or $p > r$. If we define the linear function

$$\begin{aligned} \tau_r : \text{Sym}^r(W^*) &\longrightarrow \text{Sym}^r(W) \\ x_0^i x_1^j &\longmapsto r! (-1)^i w_0^j w_1^i, \end{aligned}$$

then for all $C \in \text{Sym}^r(W^*)$, $C' \in \text{Sym}^{r'}(W^*)$, we have:

$$D(\tau_r(C), C') = (C, C')_r.$$

Remark 5.1.3. We note that if C is a covariant of $\text{Sym}^d(W^*)$ of order r , then $\tau_r(C)$ is a contravariant of the same space. Thus for binary forms, the notions of covariants and contravariants are essentially the same notion, and we typically speak only in terms of covariants.

However, the theory of covariants and contravariants is distinct for polynomials in more than 2 variables, thus the map τ_r does not generalize.

A similar statement holds for its inverse map τ_r^{-1} , which maps contravariants to covariants. These functions make the connection between the transvectant operator for binary forms and the operator D . Hence, if $(q_i)_i$ is a family of covariants of order d of $\text{Sym}^{kd}(W^*)$ which are generically linearly independent, then $(p_i := \tau(q_i))_i$ is a family of contravariants of order d of $\text{Sym}^{kd}(W^*)$ which are generically linearly independent. Thus, one can use the families p_i and q_j to reconstruct a generic element of $\text{Sym}^{kd}(W^*)$.

Lemma 5.1.4. We assume that K is of characteristic 0 or $p > kd$, and let $q_1, \dots, q_k \in \text{Sym}^d(W^*)$. Then we have

$$\tau_d(q_1) \cdots \tau_d(q_k) = \frac{d!^k}{(kd)!} \tau_{kd}(q_1 \cdots q_k). \quad (6)$$

We now detail the cases $d = 1, 2$.

For odd k , the condition on the gcd of Proposition 4.0.3 can be satisfied with $d = 1$.

Corollary 5.1.5. Let f be a stable binary form of odd degree $k \geq 5$ with trivial reduced stabilizer, which is generically the case. Then there exist covariants q_0 and q_1 of order 1 which are linearly independent at f . If we let

$$\tilde{f} = \sum_{i=0}^k \binom{k}{i} \left(q_0^i(f) q_1^{k-i}(f), f \right)_k X_0^i X_1^{k-i},$$

then \tilde{f} is GL_2 -equivalent to f . Moreover, the coefficients of \tilde{f} lie in the base field of the invariants.

Proof. This result is a corollary of Theorem 2.5.1. Indeed, if $p_0(f)^*, \dots, p_r(f)^*$ is the dual basis of $p_0(f), \dots, p_r(f)$, then $\tilde{f}(p_0(f)^*, \dots, p_r(f)^*) = f$. We observe that the constant $\frac{(kd)!}{d!^k}$ of Equation (3) cancels with the constant $\frac{d!^k}{(kd)!}$ of Equation (6). \square

Remark 5.1.6. This statement is established in (Noordsij, 2022, Theorem 3.10), except for the coefficients of \tilde{f} , which are not written with transvectants. Moreover, binary forms of degree 5 with automorphisms are covered in Noordsij (2022), as well as positive characteristic. These cases are not treated here.

However, for binary forms of even degree k , we have $\gcd\left(k, \frac{2}{\gcd(1, 2)}\right) = 2 \neq 1$. Thus, binary forms of even degree cannot have covariants of order 1, so we must turn to covariants of order 2.

Corollary 5.1.7. Let f be a stable binary form of even degree $k \geq 6$ with trivial reduced stabilizer, which is generically the case. Then there exist 3 covariants q_0, q_1, q_2 of order 2 which are linearly independent at f . If we let

$$\begin{aligned} \tilde{f} &= \sum_{\substack{0 \leq i, j \leq k \\ i+j \leq k}} \binom{k}{i, j} \left(q_0^i(f) q_1^j(f) q_2^{k-i-j}(f), f \right)_{2k} X_0^i X_1^j X_2^{k-i-j}, \text{ and} \\ Q &= \sum_{0 \leq i, j \leq 2} (q_i(f), q_j(f))_2 X_i X_j, \end{aligned}$$

then one can recover $f' \in \text{Sym}^{2k}(W^*)$ from Q and \tilde{f} , such that f' is GL_2 -equivalent to f . Moreover, the coefficients of f' lie in at most a quadratic extension of the base field of the invariants, depending on whether the conic defined by Q has a rational point.

Remark 5.1.8. This is essentially Mestre's approach (Mestre, 1991). He argues from Clebsch's formulas (Clebsch, 1870) that the dual basis $(q_0(f)^*, q_1(f)^*, q_2(f)^*)$ must satisfy the quadratic relation $Q = 0$. Then, by finding a point on the conic $Q = 0$, he parametrizes it, and by reinjecting in \tilde{f} , he obtains an element $f' \in \text{Sym}^k(W^*)$ which is GL_2 -equivalent to f .

Our method extends the existing reconstruction algorithms to direct sums of binary spaces.

Proposition 5.1.9. *Let $s > 1$, $k_1, \dots, k_s > 0$ be integers, and let $d = 1$ or 2 such that if $2 \mid \gcd(k_1, \dots, k_s)$, then $d = 2$. Let K be an algebraically closed field of characteristic 0 or $p > d \max(k_i)$. Let W be a 2-dimensional K -vector space. Let*

$$W' = \text{Sym}^{dk_1}(W^*) \oplus \dots \oplus \text{Sym}^{dk_s}(W^*),$$

and let $f = (f_1, \dots, f_s) \in W'$ such that f is stable in W' , and with trivial reduced stabilizer. There are 2 cases:

1. If $d = 2$, then there exist 3 covariants of order 2 of W' which are linearly independent at f , where a covariant here means a SL_2 -equivariant map $W' \rightarrow \text{Sym}^r(W^*)$ for some nonnegative integer r . Let q_0, q_1 , and q_2 be such covariants. For all $1 \leq i \leq s$, we let

$$\tilde{f}_i = \sum_{\substack{0 \leq l, m \leq k_i \\ l+m \leq k_i}} \binom{k_i}{l, m} \left(q_0^l(f) q_1^m(f) q_2^{k_i-l-m}(f), f \right)_{2k_i} X_0^l X_1^m X_2^{k_i-l-m},$$

and

$$Q = \sum_{0 \leq i, j \leq 2} (q_i(f), q_j(f))_2 X_i X_j.$$

Then the coefficients of Q and the \tilde{f}_i 's are invariants of W' , and we can recover $f' = (f'_1, \dots, f'_s) \in W'$ which is GL_2 -equivalent to f only from the data of Q and all the \tilde{f}_i .

2. If $d = 1$, then there exist 2 covariants of order 1 of W' which are linearly independent at f , which we take to be q_0 and q_1 . For all $1 \leq i \leq s$, we let

$$\tilde{f}_i = \sum_{0 \leq l \leq k_i} \binom{k_i}{l} \left(q_0^l(f) q_1^{k_i-l}(f), f \right)_{k_i} X_0^l X_1^{k_i-l}.$$

Then the coefficients of the \tilde{f}_i 's are invariants of W' , and $f' = (\tilde{f}_1, \dots, \tilde{f}_s) \in W'$ is GL_2 -equivalent to f .

With Proposition 5.1.9, and Corollaries 5.1.5 and 5.1.7, we derive a reconstruction algorithm for direct sums of binary spaces. The author is not aware of the existence of such an algorithm in the literature. Until now, the reconstruction algorithms of direct sums of binary spaces first reconstructed a form of highest degree $\max(dk_i)$, and were able to reconstruct the other forms using Gröbner bases and the mixed conditions on the invariants (see e.g. Lercier et al. (2020)).

Example 5.1.10. Let W be a 2-dimensional K -vector space, and define

$$W' := \text{Sym}^6(W^*) \oplus \text{Sym}^4(W^*).$$

We pick 3 covariants of W of order 2 which are generically linearly independent:

$$\begin{aligned} q_0(f) &= (f_6, f_4)_4, \\ q_1(f) &= (f_6, f_4^2)_6, \text{ and} \\ q_2(f) &= (f_6^2, f_4^3)_{11}, \end{aligned}$$

where $f = (f_6, f_4) \in W'$. We define

$$\begin{aligned} \tilde{f}_6 &= \sum_{0 \leq i, j, k \leq 2} (q_i(f) q_j(f) q_k(f), f_6)_6 X_i X_j X_k \\ \tilde{f}_4 &= \sum_{\substack{0 \leq i, j \leq 2 \\ i+j \leq 2}} (q_i(f) q_j(f), f_4)_4 X_i X_j \\ Q &= \sum_{0 \leq i, j \leq 2} (q_i(f), q_j(f))_2 X_i X_j, \end{aligned}$$

and we let φ denote the Veronese embedding

$$[x : y] \mapsto [q_0(f) : q_1(f) : q_2(f)].$$

Its image is defined by Q , and we know that

$$\begin{aligned} f_6 &= \tilde{f}_6(\tau_2(q_0(f))^*, \tau_2(q_1(f))^*, \tau_2(q_2(f))^*) \\ f_4 &= \tilde{f}_4(\tau_2(q_0(f))^*, \tau_2(q_1(f))^*, \tau_2(q_2(f))^*). \end{aligned}$$

Finding a point on the conic defined by Q allows us to parametrize it. The evaluation of \tilde{f}_6 and \tilde{f}_4 on this parametrization gives $f' = (f'_6, f'_4) \in W'$, which is GL_2 -equivalent to f .

Remark 5.1.11. Olive proved that a minimal set of generating covariants of order 2 of W' (as a $K[W']^{\text{SL}_2}$ -module) is generated by 68 elements (Olive, 2017, Theorem 8.3). Hence, if f belongs to the stable locus of W' and has trivial reduced stabilizer, there exist 3 covariants of order 2 of W' which are linearly independent at f by Proposition 4.0.1. These covariants can be taken in the generating set of 68 covariants, by Remark 4.0.5.

5.2. Reconstruction of non-hyperelliptic curves of genus 3

The canonical embedding of a non-hyperelliptic curve of genus 3 is given by a smooth, irreducible plane quartic, i.e. defined by a ternary form of degree 4. The isomorphism classes of these curves are completely determined by the 13 Dixmier-Ohno invariants Dixmier (1987); Ohno (2007). In Lercier et al. (2020), the authors give an algorithm to reconstruct a generic plane quartic from the data of the Dixmier-Ohno invariants. They use an exceptional isomorphism between SO_3 and $\text{SL}_2/\{\pm 1\}$ to reduce to the known case of binary forms.

Their algorithm involves a construction over a quadratic extension of the field of definition of the invariants. In addition, the authors make the generic assumption that $I_{12} \neq 0$.

We present an algorithm that theoretically solves the problem of reconstruction of plane quartics from the Dixmier-Ohno invariants in more generality. Indeed, the set of smooth plane quartics with non-trivial automorphism group is of codimension 2, compared to codimension 1 for the hypersurface defined by I_{12} .

Theorem 5.2.1. *Let W be a 3-dimensional K -vector space, and let $f \in \text{Sym}^4(W^*)$ such that f is stable and has trivial reduced stabilizer. Then there exist 3 contravariants of order 1 of $\text{Sym}^4(W^*)$, which are linearly independent at f . Let p_0 , p_1 , and p_2 be such contravariants. Then*

$$\tilde{f} = \sum_{0 \leq i_1, \dots, i_4 \leq 2} D(p_{i_1} \cdots p_{i_4}, f) X_{i_1} \cdots X_{i_4}$$

is GL_3 -equivalent to f .

The transvectant of ternary forms is defined as the determinant of the Ω -process (Olver, 1999) for ternary forms. It takes 3 arguments, and is denoted $(\cdot, \cdot, \cdot)_l$, where l is a nonnegative integer. Let $'$ be the operator defined in (Girard and Kohel, 2006, End of page 6). This operator allows to change covariants into contravariants, and vice-versa. We now construct contravariants p_0 , p_1 , and p_2 by considering the covariants and contravariants in Table A.1.

By Remark 3.3.2,

$$\tilde{f} = \sum_{0 \leq i_1, \dots, i_4 \leq 2} D(p_{i_1}(f) \cdots p_{i_4}(f), f) X_{i_1} \cdots X_{i_4}$$

is GL_3 -equivalent to f .

Remark 5.2.2. By Remark 4.0.5, finding a generating set of order 1 contravariants of $\text{Sym}^4(W^*)$ is enough to reconstruct all smooth non-hyperelliptic curves of genus 3 with no automorphisms. Presently, the author does not know such a generating set. However, we give 3 contravariants of order 1 which are generically linearly independent, and allow to reconstruct generically, except on a hypersurface given by the vanishing of the determinant of the three contravariants.

For the precomputation phase, we need the decomposition of the invariants $D(p_{i_1} \cdots p_{i_4}, \text{Id})$ for all $0 \leq i_1 \leq \dots \leq i_4 \leq 2$, for a total of 15 invariants. The degrees of the invariants vary from 57 to 69, and their decomposition (calculated using a method of evaluation-interpolation) took at most 1 day of computation. These decompositions are stored in (Bouchet, 2024b, `Decomposition_genus3.m`).

After this precomputation step, the actual reconstruction algorithm which takes a list of Dixmier-Ohno invariants and returns a ternary quartic takes around 0.2 seconds in practice for reasonably sized entries.

Let us illustrate the computation with an example. For clarity, we first compute the contravariants and then derive \tilde{f} even though, the user does not have access to the contravariants. In practice, since the coefficients of \tilde{f} are known polynomials in the Dixmier-Ohno invariants, they can be directly evaluated from the invariants of a given example.

Example 5.2.3. Let

$$\begin{aligned} f = & -745x_0^3x_2 - 6705x_0^2x_1x_2 - 75990x_0^2x_2^2 - 1788x_0x_1^3 - 36207x_0x_1^2x_2 - 571266x_0x_1x_2^2 \\ & - 1827336x_0x_2^3 - 7152x_1^4 - 123819x_1^3x_2 - 1834488x_1^2x_2^2 + 950004x_1x_2^3 - 631522x_2^4 \end{aligned}$$

be a ternary quartic form whose Dixmier-Ohno invariant I_{12} is 0 (this case is not covered by the existing algorithm of Lercier et al. (2020)). It defines a smooth non-hyperelliptic curve of genus 3, since $I_{27} \neq 0$. This equation was established using a work of Shioda Shioda (1993).

We compute its contravariants p_0 , p_1 , and p_2 as in Table A.1. Up to scaling, we find

$$\begin{aligned} p_0 &= -36028900960739935302662w_0 + 2546868783781471003910w_1 \\ &\quad - 207634621252481717745w_2, \\ p_1 &= -167266167826007043607549539758w_0 + 11957094310556682023883659540w_1 \\ &\quad - 996728625589442333471190105w_2, \\ p_2 &= -2137425487531362504044770w_0 + 192739452116090004098632w_1 \\ &\quad - 4823065036939209106179w_2. \end{aligned}$$

We compute \tilde{f} : its expression is too large to be displayed here, but its coefficient in x_0^4 is $-151647765305065905238548582432828758523321832584926229590543175552953534711319971363994226800$.

The other coefficients have similar sizes. The coefficients of this model can be reduced: we use Elsenhans and Stoll's minimization algorithm of ternary forms Elsenhans and Stoll (2023), and obtain the minimized model

$$\begin{aligned} f' &= 1428254x_0^4 + 1615140x_0^3x_1 - 747384x_0^3x_2 + 1802304x_0^2x_1^2 + 222606x_0^2x_1x_2 + 4470x_0^2x_2^2 \\ &\quad + 1489404x_0x_1^3 + 337932x_0x_1^2x_2 + 26820x_0x_1x_2^2 + 745x_0x_2^3 + 19668x_1^4 + 1788x_1^3x_2. \end{aligned}$$

A simple computation shows that the Dixmier-Ohno invariants of f' are the same as those of f . Hence f' and f are GL_3 -equivalent.

5.3. Reconstruction of non-hyperelliptic curves of genus 4

Let K be an algebraically closed field of characteristic 0. Let \mathcal{C} be the canonical embedding in \mathbb{P}^3 of a (smooth, irreducible) non-hyperelliptic curve of genus 4 defined over K . Then \mathcal{C} is the complete intersection of a quadric and a cubic. Let $Q, E \in K[X, Y, Z, T]$ be homogeneous irreducible forms of degree 2 and 3 respectively, which define \mathcal{C} .

Since Q is irreducible, it must be of rank 3 or 4 as a quadratic form. The case of rank 3 reduces to the reconstruction of elements from $\mathrm{Sym}^6(W^*) \oplus \mathrm{Sym}^4(W^*)$ (for more details, we refer the reader to Bouchet (2024a)). In fact, any smooth non-hyperelliptic genus 4 curve C lying on a singular quadric can be defined as the vanishing locus of $F = w^3 + wf_4(s, t) + f_6(s, t)$ in the weighted space $\mathbb{P}(1, 1, 2)$, where w is of weight 2.

Proposition 5.3.1 (Example 5.1.10). *Let W be a 2-dimensional K -vector space. Let $W' := \mathrm{Sym}^6(W^*) \oplus \mathrm{Sym}^4(W^*)$, and let $f = (f_6, f_4) \in W'$.*

We pick 3 covariants of W of order 2, and assume that they are linearly independent at f , which is generically the case:

$$\begin{aligned} q_0(f) &= (f_6, f_4)_4, \\ q_1(f) &= (f_6, f_4^2)_6, \text{ and} \\ q_2(f) &= (f_6^2, f_4^3)_{11}. \end{aligned}$$

If we define

$$\begin{aligned} Q &= \sum_{0 \leq i, j \leq 2} (q_i(f), q_j(f))_2 X_i X_j, \\ E &= X_3^3 + X_3 \left(\sum_{0 \leq i, j \leq 2} (q_i(f)q_j(f), f_4)_4 X_i X_j \right) + \sum_{0 \leq i, j, k \leq 2} (q_i(f)q_j(f)q_k(f), f_6)_6 X_i X_j X_k, \end{aligned}$$

then the vanishing locus of Q and E is a non-hyperelliptic genus 4 curve of rank 3 which is isomorphic to F .

We now treat the generic case, which is the case of rank 4. Without loss of generality, we can assume that Q is in normal form $Q = XT - YZ$, which comes from the fact that Q and $XT - YZ$, as quadratic forms, are both of rank 4, and therefore are GL_4 -equivalent. Let

$$\psi : \mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3$$

be the Segre embedding, defined by $\psi([x : y], [u : v]) = [xu : xv : yu : yv]$. The pullback of the cubic form E via ψ is $E(xu, xv, yu, yv)$, which is a bicubic form in the variables x, y and u, v that we call f .

In a previous article (Bouchet, 2024a), the author proved that two bicubic forms define geometrically isomorphic curves if and only if they are $\mathrm{GL}_2 \times \mathrm{GL}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ -equivalent, where the groups GL_2 act on their respective sets of variables, and $\mathbb{Z}/2\mathbb{Z}$ exchanges them.

Definition 5.3.2. Let $r_1, r_2 \geq 1$ and $l_1, l_2 \geq 0$ be integers. Let W be a 2-dimension K -vector space. We define a covariant of $\text{Sym}^{r_1}(W^*) \otimes \text{Sym}^{r_2}(W^*)$ to be a $\text{SL}_2 \times \text{SL}_2$ -equivariant homogeneous polynomial map

$$C : \text{Sym}^{r_1}(W^*) \otimes \text{Sym}^{r_2}(W^*) \rightarrow \text{Sym}^{l_1}(W^*) \otimes \text{Sym}^{l_2}(W^*)$$

We call (l_1, l_2) the bi-order of C , and d its degree as a homogeneous polynomial map. As before, in the case $l_1 = l_2 = 0$, C is called an invariant.

There exist covariants of $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$ of bi-order $(1, 1)$, which we can define using a transvectant (Bouchet, 2024a, Proposition 4).

We shall denote the transvectant of bi-level (l, m) by $(f, g)_{l, m}$, or even $(f, g)_l$ when $l = m$. Let D_2 denote the differential operator defined in Section 2.3 for $s = 2$. Like in the case of binary forms, there is a link between D_2 and the transvectant.

Proposition 5.3.3. *Let us assume that $\text{char}(K)$ is either 0 or $p > \max(d, e)$. Let $\tau_{d, e}$ be the linear function defined by*

$$\begin{aligned} \tau_{d, e} : \text{Sym}^d(W^*) \otimes \text{Sym}^e(W^*) &\longrightarrow \text{Sym}^d(W) \otimes \text{Sym}^e(W) \\ x^i y^j u^l v^m &\longmapsto (-1)^{i+l} d! e! x^j y^i u^m v^l \end{aligned}$$

Then for any, $C \in \text{Sym}^{d_1}(W^*) \otimes \text{Sym}^{e_1}(W^*)$ and $C' \in \text{Sym}^{d_2}(W^*) \otimes \text{Sym}^{e_2}(W^*)$, we have:

$$D_2(\tau_{d_1, e_1}(C), C') = (C, C')_{d_1, e_1}.$$

Moreover, if C is a covariant of $\text{Sym}^{l_1}(W^*) \otimes \text{Sym}^{l_2}(W^*)$, then $\tau_{d_1, e_1}(C)$ is a contravariant of the same space.

Hence, in characteristic 0 or $p > \max(d, e)$, the functions $\tau_{d, e}$ and $\tau_{d, e}^{-1}$ establish the connection between the transvectant operator and the operator D_2 , as well as between covariants and contravariants in the context of double binary forms. In the spirit of Mestre, we choose to speak only of covariants.

Theorem 5.3.4. *Let $f \in \text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$ be a stable form, with trivial reduced stabilizer (in $\text{GL}_2 \times \text{GL}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$). There exist 4 covariants of $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$ of bi-order $(1, 1)$ which are linearly independent at f . Let us denote them by q_0, q_1, q_2 and q_3 .*

Now let us define

$$Q(f) = \sum_{0 \leq i, j \leq 3} (q_i(f), q_j(f))_1 X_i X_j, \text{ and} \quad (7)$$

$$E(f) = \sum_{0 \leq i, j, l \leq 3} (q_i(f) q_j(f) q_l(f), f)_3 X_i X_j X_l. \quad (8)$$

$$(9)$$

Then the genus 4 curve defined by $Q(f)$ and $E(f)$ is isomorphic to the genus 4 curve defined by the bicubic form f . Moreover, the coefficients of Q and E are invariants for the action of $\text{SL}_2 \times \text{SL}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

Proof. The first part of the statement is an application of (Domokos, 2008, Prop 3.1): $\text{SL}_2 \times \text{SL}_2$ is a linearly reductive group, $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$ and $\text{Sym}^1(W^*) \otimes \text{Sym}^1(W^*)$ are irreducible $\text{SL}_2 \times \text{SL}_2$ -modules. With a proof similar to Proposition 4.0.3, we obtain the existence of linearly independent covariants q_0, q_1, q_2 and q_3 . It is easy to see that these covariants are also $\mathbb{Z}/2\mathbb{Z}$ -equivariant.

The second part is similar to Theorem 2.5.1, but written with the transvectant instead of the apolar pairing. In fact, the statement for D_2 is treated in Section 2.3, and we obtain that

$$E(\tau_{1,1}(q_0(f))^*, \tau_{1,1}(q_1(f))^*, \tau_{1,1}(q_2(f))^*, \tau_{1,1}(q_3(f))^*) = f.$$

Moreover, we know that

$$\dim(\text{Sym}^2(W^*) \otimes \text{Sym}^2(W^*)) = 9,$$

and

$$\dim(\text{Sym}^2(\text{Sym}^1(W^*) \otimes \text{Sym}^1(W^*))) = 10.$$

Hence there is exactly one quadratic relation, up to scaling, between $\tau_{1,1}(q_0(f))^*, \tau_{1,1}(q_1(f))^*, \tau_{1,1}(q_2(f))^*$ and $\tau_{1,1}(q_3(f))^*$. It is easy to check that

$$Q(\tau_{1,1}(q_0(f))^*, \dots, \tau_{1,1}(q_3(f))^*) = 0,$$

thus the quadratic relation must be given by the quadratic form Q .

We conclude that the morphism $\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3$, which sends $[x : y], [u : v]$ to

$$[\tau_{1,1}(q_0(f))^* : \tau_{1,1}(q_1(f))^* : \tau_{1,1}(q_2(f))^* : \tau_{1,1}(q_3(f))^*],$$

is an isomorphism from $\mathbb{P}^1 \times \mathbb{P}^1$ to the vanishing locus of Q .

It is possible to find such an isomorphism by putting Q in normal form $XT - YZ$ for example. Then, we pullback E via the Segre isomorphism, and the bicubic form obtained is $\mathrm{GL}_2 \times \mathrm{GL}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ -equivalent to f . As a consequence, the genus 4 curve defined by $Q(f)$ and $E(f)$ is isomorphic to the genus 4 curve defined by the bicubic form f .

Finally, the coefficients of $Q(f)$ and $E(f)$ are specializations of invariants of $\mathrm{Sym}^3(W^*) \otimes \mathrm{Sym}^3(W^*)$ for the action of $\mathrm{SL}_2 \times \mathrm{SL}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$, which concludes the proof. \square

By Remark 4.0.5, finding a generating set of bi-order (1,1) covariants of $\mathrm{Sym}^3(W^*) \otimes \mathrm{Sym}^3(W^*)$ is enough to reconstruct all smooth non-hyperelliptic curves of genus 4 and rank 4 with no automorphisms. Presently, the author does not know such a generating set.

However, we give in Table A.2 a set of 4 covariants which allow to reconstruct generically. Other potential covariants can be found in (Bouchet, 2024a, Table 1).

The covariants c_{31} , $c_{51,1}$, $c_{51,2}$, and $c_{51,3}$ of Table A.2 are generically linearly independent. The degrees of the invariants of $\mathrm{Sym}^3(W^*) \otimes \mathrm{Sym}^3(W^*)$ involved range between 6 and 16. These invariants have a very nice decomposition on the basis of 65 invariants, as all but one of these invariants are already included in the basis chosen by the author. Hence the reconstruction algorithm for non-hyperelliptic curves of genus 4 is extremely fast.

Let us illustrate the computation with an example. For clarity, we first compute the covariants and then derive Q and E even though, the user does not have access to the covariants. In practice, since the coefficients of Q and E are known polynomials in the basis of 65 invariants for non-hyperelliptic genus 4 curves of rank 4, they can be directly evaluated from the invariants of a given example.

Example 5.3.5. Let \mathcal{C} be the projective non-hyperelliptic genus 4 curve canonically embedded in \mathbb{P}^3 , defined by the vanishing locus of

$$Q = XT - YZ,$$

and

$$E = X^2Y + X^2Z + X^2T + XY^2 + XYZ + XZ^2 + XZT + XT^2 + Y^2Z + YZ^2 + YZT + YT^2 + T^3.$$

The quadratic form Q is of rank 4, thus we pullback through the Segre morphism the cubic form E to a bicubic form f in x, y and u, v . Then, we compute its covariants c_{31} , $c_{51,1}$, $c_{51,2}$ and $c_{51,3}$.

$$\begin{aligned} c_{31} &= -44xu - 17xv - 25yu - 17yv, \\ c_{51,1} &= 9xu - 107xv - 88yu - 24yv, \\ c_{51,2} &= -620xu - 1937xv - 1129yu + 181yv, \\ c_{51,3} &= 25889xu - 5563xv - 19056yu + 1328yv. \end{aligned}$$

We can now compute the equations of Q and E given by Equation 7. We obtain

$$\begin{aligned} Q &= 646X^2 - 6536XY - 130084XZ - 1923144XT - 19264Y^2 - 549500YZ - 6275840YT \\ &\quad - 4598186Z^2 - 78659100ZT - 143255872T^2, \end{aligned}$$

$$\begin{aligned} E &= -87337008X^3 + 69815520X^2Y - 3596033232X^2Z + 178527014496X^2T - 629045568XY^2 \\ &\quad - 13790445696XYZ - 435571233408XYT - 147774846096XZ^2 + 586163101824XZT \\ &\quad - 162711651196224XT^2 + 489595536Y^3 + 31071365856Y^2Z + 625393402416Y^2T \\ &\quad + 676666128096YZ^2 + 20257026499008YZT + 246651902537904YT^2 + 4187892749328Z^3 \\ &\quad + 229585773241440Z^2T + 1868504372517600ZT^2 + 47848070690492688T^3. \end{aligned}$$

The minimization of the coefficients of non-hyperelliptic curves of genus 4 with integer coefficients is a joint work in progress with Andreas Pieper, it is a variation on the algorithm of Elsenhans and Stoll (2023).

For this curve, our minimization algorithm returns in half a second the model

$$\begin{aligned} Q &= X^2 - XZ - 2YZ + 2Z^2 - XT - YT - T^2 \\ E &= -XY^2 - X^2Z + 3XYZ - 2Y^2Z + 2XZ^2 + Z^3 + X^2T \\ &\quad + 4XZT - 3YZT - 2Z^2T + 3XT^2 - 6ZT^2 - 2T^3, \end{aligned}$$

which has much smaller coefficients.

As expected, the computation of the invariants of the reconstructed curve are equal, up to weighted projective equivalence, to the original ones.

Remark 5.3.6. There are some instances where the reconstruction algorithm fails, because the automorphism group of the curve is too big. Let

$$Q = X^2 + Y^2 + Z^2 + T^2 + (X + Y + Z + T)^2,$$

and

$$E = X^3 + Y^3 + Z^3 + T^3 - (X + Y + Z + T)^3.$$

Then the non-hyperelliptic curve of genus 4 (of rank 4) defined by Q and E , has automorphism group S_5 , the biggest possible for a curve defined over \mathbb{C} . The reconstruction algorithm fails, since most of its invariants vanish. The author was not able to find a non-hyperelliptic curve of genus 4 (of rank 4) with automorphisms which could be reconstructed using the 4 covariants above.

Appendix A. Covariant tables

Covariants	Contravariants
$\mathbf{H} = (\mathbf{F}, \mathbf{F}, \mathbf{F})_2$ $\mathbf{C}_{4,4} = x_2^4[(\sigma', \sigma')_4](x_0/x_2, x_1/x_2)$ $\mathbf{C}_{5,2} = D(\sigma, \mathbf{H})$ $\mathbf{C}_{8,5} = (\mathbf{F}, \mathbf{H}, \mathbf{C}_{4,4})_3$ $\mathbf{C}_{12,3} = D(\rho, \mathbf{C}_{8,5})$	$\sigma = w_2^4[(\mathbf{F}', \mathbf{F}')_4](w_0/w_2, w_1/w_2)$ $\psi = w_2^6[(\mathbf{F}', \mathbf{F}')_2, \mathbf{F}')_4](w_0/w_2, w_1/w_2)$ $\rho = D(\mathbf{F}, \psi)$ $c_{5,4} = D(\mathbf{F}, \sigma^2)$ $c_{10,5} = (\sigma, \psi, c_{5,4})_3$ $c_{12,3} = D(\mathbf{C}_{8,5}, \sigma^2)$ $p_0 = D(\mathbf{C}_{12,3}, \rho)$ $p_1 = D(\mathbf{C}_{12,3}, c_{5,4})$ $p_2 = D(\mathbf{C}_{5,2}, c_{12,3})$

Table A.1: Covariants (bold) and contravariants used to compute p_0, p_1 and p_2

order degree	1	2	3	4
1			f	
2		$h = (f, f)_2$		$j = (f, f)_1$
3	$c_{31} = (h, f)_2$		$c_{33,1} = (j, f)_2$ $c_{33,2} = (h, f)_1$	
4		$c_{42,1} = (h, h)_1$ $c_{42,2} = (c_{31}, f)_1$ $c_{42,3} = (c_{33,2}, f)_2$		$c_{44,1} = (c_{33,2}, f)_1$ $c_{44,2} = ((j, f)_1, f)_2$
5	$c_{51,1} = (c_{42,2}, f)_2$ $c_{51,2} = (c_{44,1}, f)_3$ $c_{51,3} = (c_{44,2}, f)_3$			

Table A.2: Several covariants of $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$

References

Andersen, H.H., Jantzen, J.C., 1984. Cohomology of induced representations for algebraic groups. *Math. Ann.* 269, 487–525. doi:10.1007/BF01450762.

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24, 235–265. URL: <http://dx.doi.org/10.1006/jsc.1996.0125>, doi:10.1006/jsc.1996.0125. computational algebra and number theory (London, 1993).

Bouchet, T., 2024a. Invariants of genus 4 curves. *Journal of Algebra* 660, 619–644. URL: <https://www.sciencedirect.com/science/article/pii/S0021869324004009>, doi:<https://doi.org/10.1016/j.jalgebra.2024.07.016>.

Bouchet, T., 2024b. Reconstruction. <https://github.com/Thittho/Reconstruction>.

Bouyer, F., Streng, M., 2015. Examples of cm curves of genus two defined over the reflex field. *LMS Journal of Computation and Mathematics* 18, 507–538. doi:10.1112/S1461157015000121.

Brouwer, A.E., Popoviciu, M., 2010. The invariants of the binary decimic. *J. Symb. Comput.* 45, 837–843. doi:10.1016/j.jsc.2010.03.002.

Cardona, G., Quer, J., 2005. Field of moduli and field of definition for curves of genus 2, in: Computational aspects of algebraic curves. Papers from the conference, University of Idaho, Moscow, ID, USA, May 26–28, 2005. Hackensack, NJ: World Scientific, pp. 71–83.

Clebsch, A., 1870. Zur Theorie der binären algebraischen Formen. *Gött. Nachr.* 1870, 405–409.

Derksen, H., Kemper, G., 2015. Computational invariant theory. With two appendices by Vladimir L. Popov and an addendum by Nobert A. Campo and Vladimir L. Popov. volume 130 of *Encycl. Math. Sci.* 2nd enlarged edition ed., Berlin: Springer. doi:10.1007/978-3-662-48422-7.

- Derksen, H., Makam, V., 2021. Weyl’s polarization theorem in positive characteristic. *Transform. Groups* 26, 1241–1260. doi:10.1007/s00031-020-09559-3.
- Dixmier, J., 1987. On the projective invariants of quartic plane curves. *Adv. Math.* 64, 279–304. doi:10.1016/0001-8708(87)90010-7.
- Dolgachev, I., 2003. Lectures on invariant theory. volume 296 of *Lond. Math. Soc. Lect. Note Ser.* Cambridge: Cambridge University Press.
- Dolgachev, I.V., 2012. Classical algebraic geometry. A modern view. Cambridge: Cambridge University Press. doi:10.1017/CB09781139084437.
- Domokos, M., 2008. Covariants and the no-name Lemma. *J. Lie Theory* 18, 839–849. URL: www.heldermann.de/JLT/JLT18/JLT184/jlt18051.htm.
- Ehrenborg, R., Rota, G.C., 1993. Apolarity and canonical forms for homogeneous polynomials. *Eur. J. Comb.* 14, 157–181. doi:10.1006/eujc.1993.1022.
- Elsenhans, A.S., Stoll, M., 2023. Minimization of hypersurfaces. [arXiv:2110.04625](https://arxiv.org/abs/2110.04625).
- Girard, M., Kohel, D.R., 2006. Classification of genus 3 curves in special strata of the moduli space, in: Algorithmic number theory. 7th international symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006. Proceedings.. Berlin: Springer, pp. 346–360. doi:10.1007/11792086.
- Gordan, 1868. Proof that each covariant and each invariant of a binary form is an entire function, with numerical coefficients, of finitely many such forms. *J. Reine Angew. Math.* 69, 323–354. doi:10.1515/crll.1868.69.323.
- Haboush, W.J., 1975. Reductive groups are geometrically reductive. *Ann. Math. (2)* 102, 67–83. doi:10.2307/1970974.
- Harris, J., 1992. Algebraic geometry. A first course. volume 133 of *Grad. Texts Math.* Berlin etc.: Springer-Verlag.
- Kılıçer, P., Labrande, H., Lercier, R., Ritzenthaler, C., Sijsling, J., Streng, M., 2018. Plane quartics over \mathbb{Q} with complex multiplication. *Acta Arith.* 185, 127–156. URL: <https://doi.org/10.4064/aa170227-16-3>, doi:10.4064/aa170227-16-3.
- Lercier, R., Ritzenthaler, C., 2012. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra* 372, 595–636. doi:10.1016/j.jalgebra.2012.07.054.
- Lercier, R., Ritzenthaler, C., Rovetta, F., Sijsling, J., 2014. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS J. Comput. Math.* 17A, 128–147. doi:10.1112/S146115701400031X.
- Lercier, R., Ritzenthaler, C., Sijsling, J., 2020. Reconstructing plane quartics from their invariants. *Discrete Comput. Geom.* 63, 73–113. doi:10.1007/s00454-018-0047-4.
- Mestre, J.F., 1991. Construction de courbes de genre 2 à partir de leurs modules. Birkhäuser Boston, Boston, MA. pp. 313–334. URL: https://doi.org/10.1007/978-1-4612-0441-1_21, doi:10.1007/978-1-4612-0441-1_21.
- Mumford, D., Fogarty, J., Kirwan, F., 1994. Geometric invariant theory.. volume 34 of *Ergeb. Math. Grenzgeb.* 3rd enl. ed. ed., Berlin: Springer-Verlag. URL: hdl.handle.net/2433/102881, doi:10.1007/978-3-319-65907-7.
- Nagata, M., 1964. Invariants of a group in an affine ring. *J. Math. Kyoto Univ.* 3, 369–377. doi:10.1215/kjm/1250524787.
- Noordsij, J., 2022. Reconstruction of binary quintics. Master’s thesis. Leiden University.
- Ohno, T., 2007. The graded ring of invariants of ternary quartics i.
- Olive, M., 2017. About Gordan’s algorithm for binary forms. *Found. Comput. Math.* 17, 1407–1466. doi:10.1007/s10208-016-9324-x.
- Olive, M., Kolev, B., Desmorat, R., Desmorat, B., 2017. Harmonic factorization and reconstruction of the elasticity tensor, in: CFM 2017 - 23ème Congrès Français de Mécanique. URL: <https://hal.science/hal-03465304>.
- Olver, P.J., 1999. Classical invariant theory. volume 44 of *Lond. Math. Soc. Stud. Texts.* Cambridge: Cambridge University Press.

- Schmidt, F., Hasse, H., 1937. Noch eine begründung der theorie der höheren differentialquotienten in einem algebraischen funktionenkörper einer unbestimmten. (nach einer brieflichen mitteilung von f.k. schmidt in jena). Journal für die reine und angewandte Mathematik 1937, 215–237. URL: <https://doi.org/10.1515/crll.1937.177.215>, doi:doi:10.1515/crll.1937.177.215.
- Shioda, T., 1993. Plane quartics and Mordell-Weil lattices of type E_7 . Comment. Math. Univ. St. Pauli 42, 61–79.
- Sylvester, J.J., Franklin, F., 1879. Tables of the generating functions and groundforms for the binary quantic of the first ten orders. Am. J. Math. 2, 223–251. doi:10.2307/2369240.