



**HAL**  
open science

# Covariant reconstruction of forms from their invariants

Thomas Bouchet

► **To cite this version:**

| Thomas Bouchet. Covariant reconstruction of forms from their invariants. 2024. hal-04520832v2

**HAL Id: hal-04520832**

**<https://hal.science/hal-04520832v2>**

Preprint submitted on 26 Mar 2024

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

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



Distributed under a Creative Commons Attribution 4.0 International License

# COVARIANT RECONSTRUCTION OF FORMS FROM THEIR INVARIANTS

THOMAS BOUCHET

ABSTRACT. Let  $K$  be an algebraically closed field of characteristic 0 and  $f$  be a homogeneous polynomial. We provide an explicit algorithm, which, given the invariants of a generic  $f$  under the action of  $\mathrm{GL}_n(K)$  returns a polynomial in the orbit of  $f$ . We derive a specific algorithm for the reconstruction of a generic non-hyperelliptic curve of genus 4 from its invariants, as well as a direct reconstruction algorithm for generic non-hyperelliptic curves of genus 3 from their Dixmier-Ohno invariants.

## 1. INTRODUCTION

Invariant theory is the study of algebraic expressions that remain unchanged under various transformations, such as linear changes of variables. Covariants and contravariants stand as central concepts in this discipline, offering powerful tools for analyzing the geometric properties of algebraic structures. Invariant theory has lots of applications extending across various fields, including combinatorics, physics, and computer vision.

Historically, mathematicians interested in invariant theory were primarily concerned with generating systems of invariants of certain invariant algebras of binary or ternary forms under the action of the special linear group. More recently, people have started to become interested with the reverse question: given a point in the space of invariants, is there an explicit way to find a form in that orbit? This problem has a wide range of applications: finding rational models of curves (in particular for CM curves [BS15; Kil+18]), arithmetic statistics [LRRS14], and also mechanical physics [OKDD17].

Let  $n, d > 0$ , and let  $K$  be an algebraically closed field. For any  $(n + 1)$ -dimensional  $K$ -vector space  $W$ , we let  $\mathrm{Sym}^d(W^*)$  denote the space of  $(n + 1)$ -ary  $d$ -forms with coefficients in  $K$ , which is of dimension  $\binom{n+d}{d}$ . Let  $K[\mathrm{Sym}^d(W^*)]^{\mathrm{SL}_{n+1}}$  denote the algebra of invariant functions of  $\mathrm{Sym}^d(W^*)$  under the action of  $\mathrm{SL}_{n+1}$ . By a theorem of Nagata [Nag64], this algebra is always finitely generated. We assume that a finite set of generators  $\{I_j\}_{j \in J}$  of  $K[\mathrm{Sym}^d(W^*)]^{\mathrm{SL}_{n+1}}$  is known (see Section 2.4).

Our problem is as follows: let  $f \in \mathrm{Sym}^d(W^*)$ , and suppose given the orbit of  $f$  under the action of  $\mathrm{GL}_{n+1}$  as a set of values  $(I_j(f))_{j \in J}$ . Is it possible to explicitly find an element of  $f' \in \mathrm{Sym}^d(W^*)$  such that  $f$  is in the same orbit as  $f'$ ? Under mild conditions on  $f$ , we positively address this question by giving what we call a reconstruction algorithm.

While certain cases are treated in the literature, it seems that this problem had not been approached in its full generality. Mestre [Mes91] presented an algorithm for reconstructing binary forms of degree 6, while Noordsij [Noo22] more recently introduced an algorithm for the reconstruction of binary forms of degree 5 in his master's thesis. Their algorithms extend to generic binary forms of even and odd degrees respectively. The case of hyperelliptic curves of genus 3 (binary forms of degree 8) is covered by [LR12, Lemma 3.24] (even curves with extra automorphisms). Lercier and al. [LRS20] tackled the case of plane quartics by reducing it to the reconstruction of a space of binary forms. Notably, all these methods rely on formulas derived from Clebsch's work [Cle70].

In this paper, we present an algorithm for reconstruction based on the theory of covariants (see Definition 4), linear algebra and classical tools of algebraic geometry, instead of relying on the Clebsch formulas.

We find a way to characterize a generic form  $f$  with equations which coefficients are invariants, or fractions of invariants, in a bigger space (given by a Veronese morphism). These results are contained in Theorem 1 and its Corollary 2. They rely on an identity which ensures that any form can be recovered from its “projection” onto products of elements from a basis of smaller degree (see Corollary 1).

**Main result 1** (see Theorem 1). *Let  $k, d, n > 0$ . 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  $f \in \mathrm{Sym}^{kd}(W^*)$ , and let  $r = \dim_K(\mathrm{Sym}^d(W^*)) - 1$ . We assume that there exist  $q_0, \dots, q_r$  covariants of order  $d$  which are linearly independent at  $f$ . Let*

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

There exists an explicit  $\tilde{f} \in \text{Sym}^k(\text{Sym}^d(W^*))$  such that  $\varphi$  realizes an isomorphism

$$V(f) \simeq V(\tilde{f}) \cap \text{Im}(\varphi).$$

Moreover, equations for  $\tilde{f}$  and  $\text{Im}(\varphi)$  can be computed by specializing explicit invariants of  $\text{Sym}^{kd}(W^*)$  which depend only on  $q_0, \dots, q_r$  and the identity covariant.

From this result, we derive an explicit reconstruction algorithm.

**Main result 2** (see Proposition 5). *With the same assumptions, there exists a reconstruction algorithm that, given a generic family  $(I_j(f))_{j \in J}$  of generating invariants evaluated at  $f$ , returns  $f' \in \text{Sym}^{kd}(W^*)$  which is  $\text{GL}_{n+1}$ -equivalent to  $f$ .*

The proof of Theorem 1 relies on Equation (3), which gives a decomposition of  $f$  on products of a basis of covariants of a given degree.

The case  $d = 1$  is of great interest and is treated in Remark 3. If  $d > 1$ , there exist quadratic relations among the  $q_i(f)$ , which complicate the matter in practice.

Remains the question of seeing when the assumptions of Theorem 1 are satisfied.

**Main result 3** (see Corollary 3). *In characteristic 0, any smooth hypersurface of degree  $d > 2$  without automorphisms can be reconstructed with our algorithm.*

Note that the condition on the automorphism group is not a necessary one, as illustrated in [CQ05] by the case of binary forms of degree 6 with automorphism group  $C_2$  which can be reconstructed using Mestre's algorithm with a different set of covariants than the generic case.

Finally, in Section 5, we revisit the reconstruction of binary forms and plane quartics, and extend this method to reconstruct non-hyperelliptic curves of genus 4. In these cases, the formulas are remarkably simple.

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, except for small values of  $d$  and  $n$ . In addition, even in these cases, the size of the intermediate computations or outputs may be a severe limitation.

We provide a MAGMA [BCP97] package for the reconstruction of non-hyperelliptic curves of genus 3 and 4 [Bou24]. 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 (see [Bou23]), the function `ReconstructionGenus4` returns a quadratic form  $Q$  and a cubic form  $E$  such that the non-hyperelliptic curve of genus 4 given by  $V(Q, E) \subset \mathbb{P}^3$  has said invariants. Both cases  $\text{rk}(Q) = 3, 4$  are covered. The author will soon update the package with a function to reconstruct generically hyperelliptic curves of genus 4.

## 2. RECONSTRUCTION

We introduce the building blocks of the paper and expose an identity which is valid in a general setting. We then move on to invariant theory, and apply the previously established results to prove the main theorem.

Let  $n, d > 0$ , 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 4).

**Definition 1.** We extend the natural pairing  $W \times W^* \rightarrow K$  to the  $K$ -bilinear map

$$\begin{aligned} D : K[w_0, \dots, w_n] \times K[x_0, \dots, x_n] &\longrightarrow K[x_0, \dots, x_n] \\ (w_0^{\alpha_0} \cdots w_n^{\alpha_n}, P) &\longmapsto \frac{\partial^\alpha P}{\partial x_0^{\alpha_0} \cdots \partial x_n^{\alpha_n}}, \end{aligned}$$

where  $\alpha = \sum_i \alpha_i$ .

One can also define  $D : K[x_0, \dots, x_n] \times K[w_0, \dots, w_n] \rightarrow K[w_0, \dots, w_n]$  in a similar way. The order of the arguments resolves any ambiguity. The bilinear map  $D$  is classically called the ‘‘apolarity bilinear form’’ [Dol12; ER93], and gives an isomorphism  $\text{Sym}^d(W^*) \simeq \text{Sym}^d(W)^*$ .

This map can be used to tackle the Waring problem for forms [ER93]. 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 [ER93, Corollary 4.3].

**Definition 2.** Let  $d > 0$ . 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 1.** 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.** 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 basis, 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  $k, d, n > 0$ . 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 how to recover a form of degree  $kd$  from its “projection” onto elements of  $\text{Sym}^k(\text{Sym}^d(W^*))$ .

**Definition 3.** Let  $d \geq 1$ , and  $\alpha_0, \dots, \alpha_n \geq 0$  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 3.** For any integers  $\alpha_0, \dots, \alpha_n \geq 0$  of sum  $kd$ , we define

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

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 1.** Let  $f \in \text{Sym}^{kd}(W^*)$ , let  $b_0, \dots, b_r$  denote the canonical basis of  $\text{Sym}^d(W^*)$ , 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 only for monomials.

Let  $f = x_0^{\alpha_0} \cdots x_n^{\alpha_n} \in \text{Sym}^{kd}(W^*)$ . We compute the right member of Equation (2):

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

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

A somewhat similar computation is carried out in [ER93, Proposition 3.2].

**Remark 1.** To avoid problems in positive characteristic, one might be tempted to use Hasse-Schmidt derivatives [SH37] instead of partial derivatives. However, things do not unfold as smoothly as one might expect, and the condition on the characteristic of  $K$  remains.

**Corollary 1.** *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 and Proposition 1 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  $d$ :

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

It is well-known that  $v_{n,d}$  realizes an isomorphism of  $\mathbb{P}^n$  onto its image, which is defined by quadratic forms [Har92, 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  $m$  (we can have  $i = j$  or  $l = m$ ). The number of such quadratic forms is

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

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

$$\varphi : \begin{array}{ccc} \mathbb{P}^n & \longrightarrow & \mathbb{P}^r \\ [x_0 : \cdots : x_n] & \longmapsto & [q_0(x_0, \dots, x_n) : \cdots : q_r(x_0, \dots, x_n)] \end{array}$$

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

**Proposition 2.** *Let  $f \in \text{Sym}^{kd}(W^*)$ , let  $q_0, \dots, q_r$  be a basis of  $\text{Sym}^d(W^*)$ , and let  $q_0^*, \dots, q_r^*$  be its dual basis. There exists an explicit  $\tilde{f} \in \text{Sym}^k(\text{Sym}^d(W^*))$  such that*

$$V(f) \simeq V(\tilde{f}) \cap \text{Im}(\varphi).$$

*Proof.* Let

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

Then by Corollary 1, we have  $V(\tilde{f}(q_0, \dots, q_r)) = V(f)$ , which concludes the proof.  $\square$

**Proposition 3.** *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  $\text{Im}(\varphi)$ .*

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

*Proof.* Since the image of  $\varphi$  is defined by the  $Q_i$ 's, there exists a parametrization  $\varphi' : \mathbb{P}^n \longrightarrow \mathbb{P}^r$  of  $\text{Im}(\varphi)$  (we know there exists one, given by  $\varphi$ ). Thus, since they have the same image,  $\varphi$  and  $\varphi'$  differ only from an automorphism of  $\text{PGL}_{n+1}$ .

Let  $q'_0(x_0, \dots, x_n), \dots, q'_r(x_0, \dots, x_n) \in \text{Sym}^d(W^*)$  be the coordinates of  $\varphi'$ . We obtain that  $\tilde{f}(q'_0(x_0, \dots, x_n), \dots, q'_r(x_0, \dots, x_n))$  is  $\text{GL}_{n+1}$ -equivalent to  $f$ .  $\square$

### 2.3. Generalization.

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 1 can be made.

**Proposition 4.** *Let  $k, d_1, \dots, d_s > 0$ . Let  $f \in \text{Sym}^{kd_1}(W_1^*) \otimes \cdots \otimes \text{Sym}^{kd_s}(W_s^*)$ , and let  $q_0, \dots, q_r$  be a basis of  $\text{Sym}^{d_1}(W_1^*) \otimes \cdots \otimes \text{Sym}^{d_s}(W_s^*)$ . 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*

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

where  $X_0, \dots, X_r$  are coordinates for  $\mathbb{P}^r$ .

This can be proven by induction on  $s$ , since  $D$  acts independently and successively on the different spaces  $W_i$ . Hence, like in the previous subsection, one can find an explicit isomorphism  $V(f) \simeq V(\tilde{f}) \cap \text{Im}(\varphi)$ , where

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

and  $\varphi$  is the morphism which associates to points of  $\prod_i \mathbb{P}^{\dim(W_i)-1}$  the  $q_j$ 's evaluated at this point.

#### 2.4. Invariant theory.

In this section, we introduce some basic notions of invariant theory, which include invariants and covariants.

Let  $n, d > 0$ , and  $K$  be an algebraically closed field. Take  $W$  as a  $(n+1)$ -dimensional  $K$  vector space with basis  $w_0, \dots, w_n$  and dual basis  $x_0, \dots, x_n$ . Let  $G = \text{SL}_{n+1}$  or  $\text{GL}_{n+1}$ . 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 induce an action of  $G$  on  $\text{Sym}^d(W)$  and  $\text{Sym}^d(W^*)$ . Moreover, we say that  $f_1, f_2 \in \text{Sym}^d(W^*)$  are  $G$ -equivalent if one can transform  $f_1$  into  $f_2$  with the action of an element of  $G$ .

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  $\text{SL}_{n+1}$ .

**Definition 4.** Let  $k > 0$  and  $r \geq 0$ . A covariant (resp. contravariant) of  $\text{Sym}^k(W^*)$  is an  $\text{SL}(W)$ -equivariant homogeneous polynomial map

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

One calls  $r$  the order of  $C$ , and its degree is the degree of  $C$  as a homogeneous polynomial map. In the special case  $r = 0$ ,  $C$  is called an invariant. Moreover, the weight of a covariant is defined to be the integer  $(kd - r)/(n + 1)$  (resp.  $(kd + r)/(n + 1)$ ).

There are multiple ways to find covariants/contravariants. Usually, one starts with a form with coefficients given as indeterminates, and then apply equivariant transformations to it. One such equivariant transformation is the  $\Omega$ -process [Olv99], which gives rise to a differential operator called the transvectant. The transvectant is traditionally used for the description of the algebra of covariants/invariants of binary forms.

However, in general, it is not possible to determine all covariants and invariants through repeated iterations of the transvectant. We refer the interested reader to [GK06], in which the authors recall several ways to construct covariants and contravariants. We now show how the apolar bilinear form  $D$  can be used to construct covariants and contravariants.

**Definition 5.** Let  $p$  be a contravariant of  $\text{Sym}^d(W^*)$  and  $q$  a covariant of  $\text{Sym}^d(W^*)$ . We define  $D(p, q)$  pointwise:  $[D(p, q)](f) = D(p(f), q(f))$  for all  $f \in \text{Sym}^d(W^*)$ . We define  $D(q, p)$  in a similar way.

**Lemma 4.** 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 order  $r_q - r_p$  (resp.  $r_p - r_q$ ) and degree  $d_p + d_q$ .

**Lemma 5.** Let  $r = \dim_K(\text{Sym}^d(W^*)) - 1$ , and  $l > 0$ . Let us assume that there exist  $q_0, \dots, q_r$  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  $(b_i)_i$  to  $(q_i)_i$ , and let  $\Delta$  be its determinant. Clearly  $\Delta$  is a non-zero invariant of  $\text{Sym}^l(W^*)$ . Moreover,  $\Delta^t S^{-1}$  is a matrix whose columns are contravariants, precisely the dual basis  $q_0^*, \dots, q_r^*$  multiplied by the invariant  $\Delta$ .

#### 2.5. Main theorem.

We have all the tools at our disposal to present the main results of this paper, Theorem 1 and its Corollary 2.

**Theorem 1.** Let  $k, d, n > 0$ . 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  $q_0, \dots, q_r$  covariants of order  $d$  which are linearly independent at  $f$ . Let

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

There exists an explicit  $\tilde{f} \in \text{Sym}^k(\text{Sym}^d(W^*))$  such that  $\varphi$  realizes an isomorphism

$$V(f) \simeq V(\tilde{f}) \cap \text{Im}(\varphi).$$

Moreover, equations for  $\tilde{f}$  and  $\text{Im}(\varphi)$  can be computed by specializing explicit invariants of  $\text{Sym}^{kd}(W^*)$  which depend only on  $q_0, \dots, q_r$  and the identity covariant.

*Proof.* Let  $\Delta q_0^*, \dots, \Delta q_r^*$  be the set of contravariants defined in Lemma 5 of  $\text{Sym}^{kd}(W^*)$ . By assumption, they are linearly independent at  $f$ .

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  $\text{Id}$  is the identity covariant of  $\text{Sym}^{kd}(W^*)$ .

We use Proposition 2, applied to the basis of covariants  $q_0(f), \dots, q_r(f)$  and its dual basis (up to  $\Delta$ )  $\Delta q_0^*(f), \dots, \Delta q_r^*(f)$ , and we obtain  $V(f) \simeq V(\tilde{f}) \cap \text{Im}(\varphi)$ .

Moreover, the coefficients of  $\tilde{f}$  are invariants of  $f$ , by Lemma 4. Remains to see how to compute quadratic forms defining the image of  $\varphi$  with invariants.

The image of  $\varphi$  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  $\text{Sym}^{2d}(W)$ , which means that 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 matrix of invariants (specialized at  $f$ )

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

which is of size  $(r+1)^2 \times (r+1)^2$ .  $\square$

**Corollary 2.** *With the same assumptions, knowing the values of a generating set of invariants at  $f$  is theoretically enough to recover a form  $f' \in \text{Sym}^{kd}(W^*)$  which is  $\text{GL}_{n+1}$ -equivalent to  $f$ .*

This follows from Proposition 3. However, it is hard to find a parametrization  $\varphi'$  of the image of  $\varphi$  in practice. We will see in the next section 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. We first give the ideas of this algorithm, and then show some possible improvements.

Let  $k, d, n > 0$ . 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  $q_0, \dots, q_r$  covariants of order  $d$  which are linearly independent at  $f$ .

#### 3.1. Algorithm.

We derive a reconstruction algorithm from Corollary 2.

**Proposition 5.** *Let  $k, d, n > 0$ . 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  $q_0, \dots, q_r$  covariants of order  $d$  which are linearly independent at  $f$ . Let  $(I_j)_{j \in J}$  be a (finite) set of generators of  $K[\text{Sym}^{kd}(W^*)]^{\text{SL}_{n+1}}$ . Then there exists a reconstruction algorithm, which, given  $(I_j(f))_{j \in J}$ , returns a form  $f' \in \text{Sym}^{kd}(W^*)$  which is  $\text{GL}_{n+1}$ -equivalent to  $f$ .*

We explain how to derive such an algorithm from Theorem 1. Here is a high-level description to clarify our point:

- (1) The first step (which is done only once for every set of covariants) consists in the precalculation of a decomposition on a generating set of invariants of all the invariants required for the computation of  $\tilde{f}$  and the matrix  $(D(\Delta q_i^* \Delta q_j^*, q_l q_m))$ .
- (2) One can then specialize these formulas to a specific  $f$  by evaluating the decomposition polynomials at the values of the generating set of invariants at  $f$ .

- (3) Finally, we can parametrize  $\text{Im}(\varphi)$  using the quadratic forms. Then, by evaluating  $\tilde{f}$  on this parametrization, we recover  $f' \in \text{Sym}^{kd}(W^*)$  which is  $\text{GL}_{n+1}$ -equivalent to  $f$ .

The first step can be done using an evaluation-interpolation strategy, and the second step is clear. At the end of the next paragraph, we discuss a strategy that we came up with to solve the problem of parametrization for small  $r$ .

### 3.2. Improvements.

In order to make this algorithm run in practice, it is necessary to improve it.

First, we remark that if we choose  $q_1, \dots, q_r$  generically linearly independent covariants of  $\text{Sym}^{kd}(W^*)$  of degrees  $d_1, \dots, d_r$ , their dual basis  $\Delta q_1^*, \dots, \Delta q_r^*$  of contravariants has high degree:  $\deg(\Delta q_i^*) = d_i + 2 \sum_{j \neq i} d_j$ . The coefficients of  $f$  are of very high degree, thus finding a decomposition of these invariants on a generating set of invariants is not doable in general.

To avoid this problem, we choose a set of covariants  $q$  and a set of contravariants  $p$ . We compute a decomposition of the invariants of smaller degrees  $D(p_{i_1} \cdots p_{i_k}, \text{Id})$  and  $D(p_i p_j, q_l q_m)$ . We use the following remark to see that it is easy to make the connection with Theorem 1.

**Remark 2.** Let  $M_{p,q} = \left( D(p_i, q_j) \right)_{i,j}$ . Then the basis  $(p_i(f)^*)_i$  can be expressed using the basis  $(q_j(f))_j$ , by the following formula:

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

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

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

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  $Q_{p,q}({}^t M_{p,q}^{-1} \otimes {}^t M_{p,q}^{-1})$ .

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).

We now turn to the problem of the quadratic forms: by computing the right kernel of the matrix  $Q_{p,q}({}^t M_{p,q}^{-1} \otimes {}^t M_{p,q}^{-1})$ , one recovers a basis in which the quadratic forms have no prescribed rank. However, it is shown in [Har92] that the canonical quadratic forms which define the Veronese embedding have rank 3 or 4. The problem of finding a quadratic form of prescribed rank as a linear combination of a set of other quadratic forms is known to be a difficult problem.

Thus, we expose an algorithmic solution that works for small  $r$ . It is based on the fact that we know a parametrization of the canonical Veronese embedding, hence we try to reduce to the case where the quadratic forms are ones defining the image of the canonical Veronese embedding. In order to do so, we consider the matrix  $Q_{b^*,b}$  where  $b$  denotes the canonical basis of  $\text{Sym}^d(W^*)$ , and  $b^*$  its dual basis. We now play with the matrix  $Q_{p(f),p(f)^*}$  to somehow change it to  $Q_{b^*,b}$ .

In fact, it is easy to see that if  $M$  is an  $(r+1) \times (r+1)$  matrix with coefficients in  $K$ , and that we have

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

Thus, our algorithmic solution is to try and find an invertible matrix  $M$  such that

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

Then by changing  $p(f)$  into  $Mp(f)$ , and  $p(f)^*$  into  ${}^t M^{-1}p(f)^*$ , the quadratic relations we obtain are the ones corresponding to the canonical embedding.

We know that Equation (5) has a solution, since  $p(f)$  and  $b^*$  are both bases of  $\text{Sym}^d(W)$ .

The problem of finding a solution to Equation (5) can be solved by considering  $M$  as a matrix of indeterminates. Then, we try to find a solution to the system of  $(r+1)^4$  quadratic equations in  $(r+1)^2$  indeterminates given by  $Q_{b^*,b}(M \otimes M) - (M \otimes M) Q_{p(f),p(f)^*} = 0$ . In our



area of application, it can be done by doing Gröbner bases, and assigning arbitrary values to some indeterminates.

Once a solution is known, one needs to update  $\tilde{f}(X)$  to  $g := \tilde{f}({}^tMX)$ . Eventually,  $g(b) = g(x_0^d, \dots, x_n^d)$  is  $\mathrm{GL}_{n+1}$ -equivalent to  $f$ .

**Remark 3.** In the case  $d = 1$ , we have  $r = n$ , so the morphism  $\varphi$  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  $\mathrm{GL}_{n+1}$ -equivalent.

This fact is used to provide a new reconstruction algorithm for smooth plane quartics in Section 5.2.

**Remark 4.** We note that in the opposite case  $k = 1$ , the situation is significantly worse: eventhough the form  $f$  itself is a covariant, the number of invariants needed explodes, and the step of parametrization of  $\mathrm{Im}(\varphi)$  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  $k, d, n > 0$ . 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  $f \in \mathrm{Sym}^{kd}(W^*)$ , there exist  $\dim_K(\mathrm{Sym}^d(W^*))$  covariants of  $\mathrm{Sym}^{kd}(W^*)$  which are linearly independent at  $f$ . We use the notion of stability defined in Mumford's GIT theory [MFK94]. One can find an exposure that suits our needs in [Dol03, Chapters 8, 9].

Let us recall an important result, written in its original form.

**Proposition 6** ([Dom08, Prop 3.1]). *Let  $G$  be a linearly reductive group,  $X$  an affine  $G$ -variety, and  $V$  a  $G$ -module. If for some  $x \in X$  having closed orbit the stabilizer  $G_x$  acts trivially on  $V$ , then there exist  $s = \dim_K(V)$  covariants  $F_1, \dots, F_s \in \mathrm{Cov}_G(X, V)$  such that  $F_1(x), \dots, F_s(x)$  are linearly independent over  $K$ .*

**Proposition 7.** *For every stable  $f \in \mathrm{Sym}^{kd}(W^*)$  such that  $V(f)$  has trivial automorphism group, the following statements are equivalent:*

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

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

We are going to apply Proposition 6 with  $G = \mathrm{SL}_{n+1}$ ,  $X = \mathrm{Sym}^{kd}(W^*)$ , and  $V = \mathrm{Sym}^d(W^*)$ . Since  $\mathrm{char}(K) = 0$ ,  $G$  is linearly reductive. However, this result does not apply to positive characteristic: in that case  $\mathrm{SL}_{n+1}$  is still reductive, but not linearly reductive.

It is known that the elements of the stable locus have closed orbit [Dol03, Chapter 8]. Now, let  $f \in X$  such that  $V(f)$  has trivial automorphism group. It may happen that the subgroup  $G_f$  of  $\mathrm{SL}_{n+1}$  that fixes  $f$  is non trivial. In fact, it is easy to prove that

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

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

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

In addition, we have

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

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

In that case, we can apply Proposition 6, which implies the existence of the desired covariants.  $\square$

**Corollary 3.** *We 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  $V(f)$  is a smooth hypersurface with trivial automorphism group, the reconstruction algorithm (Corollary 5) applies.*

*Proof.* According to [Dol03, Theorem 10.1], any non-singular element of  $\text{Sym}^{kd}(W^*)$  is stable. Hence, by Proposition 7, there exist covariants that can be used to meet the requirements of Corollary 5.  $\square$

**Remark 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  $V(f)$  has no automorphisms. 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  $f$ .

The point is that once we have at our disposal a generating set of covariants of a given degree, any stable  $f \in \text{Sym}^{kd}(W^*)$  such that  $V(f)$  has no automorphisms can be covariantly reconstructed by using only a subset of these generating covariants. In practice, determining such a set of covariants may be computationally hard, even infeasible. Their degrees are not known, and depend on  $k, d$  and  $n$ . If the degrees of some of them are too high, the precomputation part of the algorithm might prove impossible to do.

## 5. EXAMPLES

### 5.1. Binary forms.

We turn to the case of binary forms, for which reconstruction algorithms have been found by Mestre [Mes91] and Noordsij [Noo22]. Let  $W$  be a 2-dimensional  $K$ -vector space with basis  $w_0, w_1$  and dual basis  $x_0, x_1$ .

**Definition 6.** Let  $f \in \text{Sym}^d(W^*), g \in \text{Sym}^e(W^*)$  for some  $d, e > 0$ . For all  $l > 0$ , we define the  $l$ -th transvectant of  $f, g$  to be

$$(f, g)_l = \sum_{i=0}^l (-1)^i \binom{l}{i} \frac{\partial^l f}{\partial^i x_0 \partial^{l-i} x_1} \frac{\partial^l g}{\partial^{l-i} x_0 \partial^i x_1}.$$

**Proposition 8.** *We define the linear function*

$$\begin{aligned} \tau : K[x_0, x_1] &\longrightarrow K[w_0, w_1] \\ x_0^i x_1^j &\longmapsto (i+j)! (-1)^i w_0^j w_1^i. \end{aligned}$$

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

$$D(\tau(C), C') = (C, C')_d.$$

*Moreover, if  $C$  is a covariant of  $\text{Sym}^r(W^*)$ , then  $\tau(C)$  is a contravariant of the same space.*

A similar statement holds for its inverse map  $\tau^{-1}$ , 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,  $(p_i := \tau(q_i))_i$  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  $\text{Sym}^{kd}(W^*)$ .

**Remark 6.** We note that  $\tau$  is not exactly multiplicative. In fact, if  $q_1, \dots, q_k \in K[x_0, x_1]_d$ , we have

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

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

For odd  $k$ , the condition on the gcd of Proposition 7 can be satisfied with  $d = 1$ .

**Corollary 4.** *Let  $f$  be a binary form of odd degree  $k \geq 5$  such that  $V(f)$  is smooth and has no automorphisms (it is generically the case). Then there exist  $q_0, q_1$  covariants of order 1 which are linearly independent at  $f$ . Moreover, if we let*

$$\tilde{f} = \sum_{i=0}^k \binom{k}{i} q_0^i q_1^{k-i} X_0^i X_1^{k-i},$$

*we obtain that  $\tilde{f}$  is  $\text{GL}_2$ -equivalent to  $f$ .*

*Proof.* This result is implied by Theorem 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).  $\square$

This statement is very similar to [Noo22, Theorem 3.10]. The only difference is that his formula for  $\tilde{f}$  is not written with transvectants. In addition, his theorem includes binary forms of degree 5 with automorphisms, which are not all covered 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 do not have covariants of order 1, so we naturally turn to covariants of order 2.

**Corollary 5.** *Let  $f$  be a smooth binary form of even degree  $k \geq 6$  such that  $V(f)$  has no automorphisms (it is generically the case). Then there exist 3 covariants  $q_0, q_1, q_2$  of order 2 which are linearly independent at  $f$ . Moreover, we have*

$$V(f) \simeq V(Q, \tilde{f}),$$

where

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

From  $Q$  and  $\tilde{f}$ , one can recover  $f' \in \text{Sym}^{2k}(W^*)$  which is  $\text{GL}_2$ -equivalent to  $f$ .

This is essentially Mestre's approach. He exhibits an equation for this quadratic form  $Q$  (this equation). Then, by finding a point on  $V(Q)$ , he parametrizes it, and by reinjecting in  $\tilde{f}$ , he obtains an element  $f' \in \text{Sym}^k(W^*)$  which is  $\text{GL}_2$ -equivalent to  $f$ .

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

**Proposition 9.** *Let  $s > 1$ ,  $k_1, \dots, k_s > 0$  and  $d = 1$  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 the intersection of the automorphism groups of the  $V(f_i)$  (inside  $\text{PGL}_2$ ) for all  $i$  is trivial. There are 2 cases:*

- (1) *If  $d = 2$ , there exist 3 covariants  $q_0, q_1, q_2$  of order 2 of  $W'$  which are linearly independent at  $f$ . For all  $1 \leq i \leq s$ , let*

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

and

$$Q = \sum_{0 \leq l, m \leq 2} (q_l, q_m)_2 X_l X_m.$$

*Then the coefficients of  $Q$  and  $\tilde{f}_i$  are invariants of  $W'$  for all  $i$ , and one can recover  $f' = (f'_1, \dots, f'_s) \in W'$  which is  $\text{GL}_2$ -equivalent to  $f$  only from the data of  $Q$  and all the  $\tilde{f}_i$ .*

- (2) *If  $d = 1$ , there exist 2 covariants  $q_0, q_1$  of order 1 of  $W'$  which are linearly independent at  $f$ . For all  $1 \leq i \leq s$ , let*

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

*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  $\text{GL}_2$ -equivalent to  $f$*

With this proposition and Corollaries 4 and 5, one can 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 Groebner bases and the mixed conditions on the invariants (see for example [LRS20]).

**Example 1.** Let  $W$  be a 2-dimensional  $K$ -vector space. Let  $W' := \text{Sym}^6(W^*) \oplus \text{Sym}^4(W^*)$ , 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  $f$ :

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

We define

$$\begin{aligned} \tilde{f}_6 &= \sum_{\substack{0 \leq i, j \leq 3 \\ i+j \leq 3}} (q_0^i q_1^j q_2^{3-i-j}, f_6)_6 X_0^i X_1^j X_2^{3-i-j} \\ \tilde{f}_4 &= \sum_{\substack{0 \leq i, j \leq 2 \\ i+j \leq 2}} (q_0^i q_1^j q_2^{2-i-j}, f_4)_4 X_0^i X_1^j X_2^{2-i-j} \\ Q &= \sum_{0 \leq i, j \leq k} (q_i, q_j)_2 X_i X_j. \end{aligned}$$

Now let  $\varphi$  denote the Veronese embedding  $[x : y] \mapsto [\tau(q_0(f))^* : \tau(q_1(f))^* : \tau(q_2(f))^*]$ . Its image is defined by  $Q$ , and we find that  $f_6 = \tilde{f}_6(\tau(q_0(f))^*, \tau(q_1(f))^*, \tau(q_2(f))^*)$  (resp.  $f_4 = \tilde{f}_4(\tau(q_0(f))^*, \tau(q_1(f))^*, \tau(q_2(f))^*)$ ).

Finding a point on  $V(Q)$  allows us to parametrize it. The evaluation of  $\tilde{f}_6$  and  $\tilde{f}_4$  on this parametrization gives  $(f'_6, f'_4) \in W'$  which is  $\text{GL}_2$ -equivalent to  $f$ .

Moreover, Olive [Oli17, Theorem 8.3] 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. Hence, if the automorphism group of  $V(f_6)$  intersected with the automorphism group of  $V(f_4)$  is trivial, and  $f$  belongs to the stable locus of  $W'$ , there exist 3 covariants of order 2 of  $W'$  which are linearly independent at  $f$  by Proposition 6. These covariants can be taken in the generating set of 68 covariants, by Remark 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. The isomorphism classes of these curves are completely determined by a set of invariants, called the Dixmier-Ohno invariants [Dix87; Ohn07]. In [LRS20], 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  $\text{SO}_3$  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 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.

**Theorem 2.** *Let  $W$  be a 3-dimensional  $K$ -vector space, and let  $f \in \text{Sym}^4(W^*)$  such that  $V(f)$  is smooth and has no automorphisms. Then there exist 3 covariants of order 1 of  $\text{Sym}^4(W^*)$ ,  $q_0, q_1$ , and  $q_2$  such that  $f$  can be covariantly reconstructed from  $q_0, q_1$  and  $q_2$ .*

By Remark 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.

The transvectant of ternary forms is defined as the determinant of the  $\Omega$ -process [Olv99] for ternary forms. It takes 3 arguments, and is denoted  $(\cdot, \cdot, \cdot)_l$ . Let  $'$  be the operator defined in [GK06, End of page 6]. This operator allows to change covariants into contravariants, and vice-versa. We now construct contravariants  $p_0, p_1, p_2$  by considering the covariants and contravariants in Table 1.

By Remark 3,

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

is  $\text{GL}_3$ -equivalent to  $f$ .

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 [Bou24, Decomposition\_genus3.m]. After this step of decomposition, the actual reconstruction algorithm consists in specializing the invariants  $D(p_{i_1} \cdots p_{i_4}, \text{Id})$  to  $f$ . This step is very fast, around 0.2 seconds in practice for reasonably sized entries.

**Example 2.** Let

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

be a ternary quartic whose Dixmier-Ohno invariant  $I_{12}$  is 0 (this case is not covered by the existing algorithm of [LRS20]). It defines a smooth non-hyperelliptic curve of genus 3, since  $I_{27} \neq 0$ . This equation was established using a work of Shioda [Shi93].

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

$$p_0 = -36028900960739935302662w_0 + 2546868783781471003910w_1 \\ - 207634621252481717745w_2, \\ p_1 = -167266167826007043607549539758w_0 + 11957094310556682023883659540w_1 \\ - 996728625589442333471190105w_2, \\ p_2 = -2137425487531362504044770w_0 + 192739452116090004098632w_1 \\ - 4823065036939209106179w_2.$$

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. This model is improvable: we use Elsenhans and Stoll's minimization algorithm of ternary forms [ES23], and obtain the minimized model

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

A simple computation shows that the Dixmier-Ohno invariants of  $f'$  are the same as those of  $f$ . Hence  $f'$  and  $f$  are  $\mathrm{GL}_3$ -equivalent.

### 5.3. Reconstruction of non-hyperelliptic curves of genus 4.

Let  $K$  be an algebraically closed field of characteristic 0. Let  $W$  be a 2-dimension  $K$ -vector space. 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  $Q \in K[X, Y, Z, T]$  be a homogeneous irreducible quadratic form, and  $E \in K[X, Y, Z, T]$  be a homogeneous irreducible cubic form such that they define  $\mathcal{C}$ .

Since  $Q$  is irreducible, it must be of rank 3 or 4. We will here only treat the generic case, which is the case of rank 4. 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 [Bou23]), and this case is treated in Example 1.

From now on, we assume that  $Q$  is in normal form  $Q = XT - YZ$ . Let  $\psi : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3$  be the Segre embedding, defined by  $\psi([x : y], [u : v]) = [xu : xv : yu : yv]$ . The pullback of the cubic form  $E$  via  $\psi$  is  $E(xu, xv, yu, yv)$ . It is a bicubic form  $f$  in the variables  $x, y$  and  $u, v$ .

In a previous article [Bou23], the author proved that two bicubic forms define 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  $\mathrm{GL}_2$  act on their respective sets of variables, and  $\mathbb{Z}/2\mathbb{Z}$  exchanges them.

**Definition 7.** Let  $r_1, r_2 \geq 1$  and  $l_1, l_2 \geq 0$ . We define a covariant of  $\mathrm{Sym}^{r_1}(W^*) \otimes \mathrm{Sym}^{r_2}(W^*)$  to be a  $\mathrm{SL}_2 \times \mathrm{SL}_2$ -equivariant homogeneous polynomial map

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

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  $r = 0$ ,  $C$  is called an invariant.

There exist covariants of  $\mathrm{Sym}^3(W^*) \otimes \mathrm{Sym}^3(W^*)$  of bi-order  $(1, 1)$ , which we can define using a transvectant (for more details, see [Bou23]). This operator is  $\mathrm{SL}_2 \times \mathrm{SL}_2$ -equivariant. In addition, in our computations, it will also be  $\mathbb{Z}/2\mathbb{Z}$ -equivariant [Bou23, Proposition 4].

We shall denote the transvectant by  $(\cdot, \cdot)_{l,m}$ , or even  $(\cdot, \cdot)_l$  if  $l = m$ . 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 10.** Let  $\tau_2$  be the linear function defined by

$$\tau_2 : K[x, y] \otimes K[u, v] \rightarrow K[x, y] \otimes K[u, v] \\ x^i y^j u^l v^m \mapsto (-1)^{i+l} (i+j)! (l+m)! x^j y^i u^m v^l.$$

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

$$D_2(\tau_2(C), C') = (C, C')_{d_1, e_1}.$$

Moreover, if  $C$  is a covariant of  $\mathrm{Sym}^{l_1}(W^*) \otimes \mathrm{Sym}^{l_2}(W^*)$ , then  $\tau_2(C)$  is a contravariant of the same space.

Hence, the functions  $\tau_2$  and  $\tau_2^{-1}$  make the connection between the transvectant operator and the operator  $D_2$  in the case of binary forms. In the spirit of Mestre, we choose to speak only of covariants.

**Theorem 3.** *Let  $f \in \text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$  such that the corresponding genus 4 curve is smooth and has no automorphisms. There exist 4 covariants  $q_0, q_1, q_2$  and  $q_3$  of  $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$  of bi-order  $(1, 1)$  which are linearly independent at  $f$ .*

Now let

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

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

Then  $V(Q(f), E(f))$  is isomorphic to  $V(f)$ , and 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 [Dom08, 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 7, we obtain the existence of covariants  $q_0, q_1, q_2$  and  $q_3$  linearly independent at  $f$ . It is easy to see that these covariants are also  $\mathbb{Z}/2\mathbb{Z}$ -equivariant.

The second part is similar to Theorem 1, but written with the transvectant instead of  $D_2$ . The statement for  $D_2$  is treated in Section 2.3, and we obtain that

$$E(\tau_2(q_0(f))^*, \tau_2(q_1(f))^*, \tau_2(q_2(f))^*, \tau_2(q_3(f))^*) = f.$$

Now let us turn to  $Q$ . 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 between  $\tau_2(q_0(f))^*, \tau_2(q_1(f))^*, \tau_2(q_2(f))^*$  and  $\tau_2(q_3(f))^*$ . It is easy to check that  $Q(\tau_2(q_0(f))^*, \dots, \tau_2(q_3(f))^*) = 0$ , thus the quadratic relation is given by the quadratic form  $Q$ .

We conclude that the morphism

$$\varphi : \begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \longrightarrow & \mathbb{P}^3 \\ [x : y], [u : v] & \longmapsto & [\tau_2(q_0(f))^* : \tau_2(q_1(f))^* : \tau_2(q_2(f))^* : \tau_2(q_3(f))^*] \end{array}$$

is an isomorphism from  $\mathbb{P}^1 \times \mathbb{P}^1$  to  $V(Q)$ . Finally, we find that

$$V(f) \simeq V(Q(f), E(f)).$$

In addition, the coefficients of  $Q$  and  $E$  are specializations of invariants of  $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$  for the action of  $\text{SL}_2 \times \text{SL}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ .  $\square$

By Remark 5, finding a generating set of bi-order  $(1, 1)$  covariants of  $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$  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 2 a set of 4 covariants which allow to reconstruct generically. Other potential covariants can be found in [Bou23, Table 1].

The covariants  $c_{31}, c_{51,1}, c_{51,2}, c_{51,3}$  of Table 2 are generically linearly independent. The degrees of the invariants involved in the coefficients of  $Q$  and  $E$  range between 6 and 16. The author included all but one of these invariants in the basis of 65 invariants, so the phase of precomputation is nearly trivial. The only one which does not belong to the basis is the degree 8 invariant  $(c_{31}, c_{51,3})_1$ , and its decomposition is easy to find.

Hence this reconstruction algorithm takes very little time to run.

**Example 3.** Let  $\mathcal{C}$  be the non-hyperelliptic genus 4 curve defined in  $\mathbb{P}^3$  by the locus of

$$Q = XT - YZ,$$

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

$Q$  is of rank 4, thus we pullback  $E$  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 now compute the equations of  $Q$  and  $E$ :

$$\begin{aligned} Q &= 646X^2 - 6536XY - 130084XZ - 1923144XT - 19264Y^2 - 549500YZ - 6275840YT \\ &\quad - 4598186Z^2 - 78659100ZT - 143255872T^2, \\ E &= -87337008X^3 + 69815520X^2Y - 3596033232X^2Z + 178527014496X^2T - 629045568XY^2 \\ &\quad - 13790445696XYZ - 435571233408XYT - 147774846096XZ^2 + 586163101824XZT \\ &\quad - 162711651196224XT^2 + 489595536Y^3 + 31071365856Y^2Z + 625393402416Y^2T \\ &\quad + 676666128096YZ^2 + 20257026499008YZT + 246651902537904YT^2 + 4187892749328Z^3 \\ &\quad + 229585773241440Z^2T + 1868504372517600ZT^2 + 47848070690492688T^3. \end{aligned}$$

The minimization of the coefficients of non-hyperelliptic curves of genus 4 with integer coefficients is a joint work in progress with Andreas Pieper. 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 is much nicer than the previous one.

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

**Remark 7.** There are instances where the algorithm fails, because the automorphism group of the curve is too big. For example, 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  $V(Q, E)$  is a non-hyperelliptic curve of genus 4 (of rank 4), whose automorphism group is  $S_5$ , 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 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 2. Several covariants of  $\text{Sym}^3(W^*) \otimes \text{Sym}^3(W^*)$ 

## REFERENCES

- [BCP97] W. Bosma, J. Cannon, and C. Playoust. “The Magma algebra system. I. The user language”. In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265 (cit. on p. 2).
- [Bou24] T. Bouchet. *Reconstruction*. <https://github.com/Thittho/Reconstruction>. 2024 (cit. on pp. 2, 11).
- [Bou23] T. Bouchet. *Invariants of genus 4 curves*. 2023. arXiv: 2310.01158 [math.AC] (cit. on pp. 2, 12, 13).
- [BS15] F. Bouyer and M. Streng. “Examples of CM curves of genus two defined over the reflex field”. In: *LMS Journal of Computation and Mathematics* 18.1 (2015), pp. 507–538 (cit. on p. 1).
- [CQ05] G. Cardona and J. Quer. “Field of moduli and field of definition for curves of genus 2”. English. In: *Computational aspects of algebraic curves. Papers from the conference, University of Idaho, Moscow, ID, USA, May 26–28, 2005*. Hackensack, NJ: World Scientific, 2005, pp. 71–83 (cit. on p. 2).
- [Cle70] A. Clebsch. “Zur Theorie der binären algebraischen Formen.” German. In: *Gött. Nachr.* 1870 (1870), pp. 405–409 (cit. on p. 1).
- [Dix87] J. Dixmier. “On the projective invariants of quartic plane curves”. English. In: *Adv. Math.* 64 (1987), pp. 279–304 (cit. on p. 11).
- [Dol03] I. Dolgachev. *Lectures on invariant theory*. English. Vol. 296. Cambridge: Cambridge University Press, 2003 (cit. on pp. 8, 9).
- [Dol12] I. V. Dolgachev. *Classical algebraic geometry. A modern view*. English. Cambridge: Cambridge University Press, 2012 (cit. on p. 2).
- [Dom08] M. Domokos. “Covariants and the no-name Lemma”. In: *J. Lie Theory* 18.4 (2008), pp. 839–849 (cit. on pp. 8, 13).
- [ER93] R. Ehrenborg and G.-C. Rota. “Apolarity and canonical forms for homogeneous polynomials”. English. In: *Eur. J. Comb.* 14.3 (1993), pp. 157–181 (cit. on pp. 2, 3).



- [ES23] A.-S. Elsenhans and M. Stoll. *Minimization of hypersurfaces*. 2023. arXiv: [2110.04625](https://arxiv.org/abs/2110.04625) [[math.NT](#)] (cit. on p. [12](#)).
- [GK06] M. Girard and D. R. Kohel. “Classification of genus 3 curves in special strata of the moduli space”. English. In: *Algorithmic number theory. 7th international symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006. Proceedings*. Berlin: Springer, 2006, pp. 346–360 (cit. on pp. [5](#), [11](#)).
- [Har92] J. Harris. *Algebraic geometry. A first course*. English. Vol. 133. Berlin etc.: Springer-Verlag, 1992 (cit. on pp. [4](#), [7](#)).
- [Kıl+18] P. Kılçer, H. Labrande, R. Lercier, C. Ritzenthaler, J. Sijsling, and M. Streng. “Plane quartics over  $\mathbb{Q}$  with complex multiplication”. In: *Acta Arith.* 185.2 (2018), pp. 127–156 (cit. on p. [1](#)).
- [LR12] R. Lercier and C. Ritzenthaler. “Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects”. English. In: *J. Algebra* 372 (2012), pp. 595–636 (cit. on p. [1](#)).
- [LRRS14] R. Lercier, C. Ritzenthaler, F. Rovetta, and J. Sijsling. “Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields”. English. In: *LMS J. Comput. Math.* 17A (2014), pp. 128–147 (cit. on p. [1](#)).
- [LRS20] R. Lercier, C. Ritzenthaler, and J. Sijsling. “Reconstructing plane quartics from their invariants”. English. In: *Discrete Comput. Geom.* 63.1 (2020), pp. 73–113 (cit. on pp. [1](#), [10–12](#)).
- [Mes91] J.-F. Mestre. “Construction de courbes de genre 2 à partir de leurs modules”. In: *Effective Methods in Algebraic Geometry*. Ed. by T. Mora and C. Traverso. Boston, MA: Birkhäuser Boston, 1991, pp. 313–334 (cit. on pp. [1](#), [9](#)).
- [MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. English. 3rd enl. ed. Vol. 34. Berlin: Springer-Verlag, 1994 (cit. on p. [8](#)).
- [Nag64] M. Nagata. “Invariants of a group in an affine ring”. English. In: *J. Math. Kyoto Univ.* 3 (1964), pp. 369–377 (cit. on p. [1](#)).
- [Noo22] J. Noordsij. “Reconstruction of binary quintics.” MA thesis. Leiden University, 2022 (cit. on pp. [1](#), [9](#), [10](#)).
- [Ohn07] T. Ohno. “The graded ring of invariants of ternary quartics I”. 2007 (cit. on p. [11](#)).
- [Oli17] M. Olive. “About Gordan’s algorithm for binary forms”. English. In: *Found. Comput. Math.* 17.6 (2017), pp. 1407–1466 (cit. on p. [11](#)).
- [OKDD17] M. Olive, B. Kolev, R. Desmorat, and B. Desmorat. “Harmonic factorization and reconstruction of the elasticity tensor”. In: *CFM 2017 - 23ème Congrès Français de Mécanique*. 2017 (cit. on p. [1](#)).
- [Olv99] P. J. Olver. *Classical invariant theory*. English. Vol. 44. Cambridge: Cambridge University Press, 1999 (cit. on pp. [5](#), [11](#)).
- [SH37] F. Schmidt and H. Hasse. “Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. (Nach einer brieflichen Mitteilung von F.K. Schmidt in Jena).” In: *Journal für die reine und angewandte Mathematik* 1937.177 (1937), pp. 215–237 (cit. on p. [4](#)).
- [Shi93] T. Shioda. “Plane quartics and Mordell-Weil lattices of type  $E_7$ ”. English. In: *Comment. Math. Univ. St. Pauli* 42.1 (1993), pp. 61–79 (cit. on p. [12](#)).