

# COMPUTING HERMITIAN DETERMINANTAL REPRESENTATIONS OF HYPERBOLIC CURVES

DANIEL PLAUMANN, RAINER SINN, DAVID E SPEYER, AND CYNTHIA VINZANT

## INTRODUCTION

Let  $f$  be a real homogeneous polynomial of degree  $d$  in variables  $x, y, z$ . A **Hermitian determinantal representation** of  $f$  is an expression

$$(1) \quad f = \det(xM_1 + yM_2 + zM_3),$$

where  $M_1, M_2, M_3$  are Hermitian  $d \times d$  matrices. The representation is **definite** if there is a point  $e \in \mathbb{R}^3$  for which the matrix  $e_1M_1 + e_2M_2 + e_3M_3$  is positive definite.

This imposes an immediate condition on the projective curve  $\mathcal{V}_{\mathbb{C}}(f)$ . Because the eigenvalues of a Hermitian matrix are real, every real line passing through  $e$  meets this hypersurface in only real points. A polynomial with this property is called **hyperbolic** (with respect to  $e$ ). Hyperbolicity is reflected in the topology of the real points  $\mathcal{V}_{\mathbb{R}}(f)$ . When the curve  $\mathcal{V}_{\mathbb{C}}(f)$  is smooth,  $f$  is hyperbolic if and only if  $\mathcal{V}_{\mathbb{R}}(f)$  consists of  $\lfloor \frac{d}{2} \rfloor$  nested ovals, and a pseudo-line if  $d$  is odd.

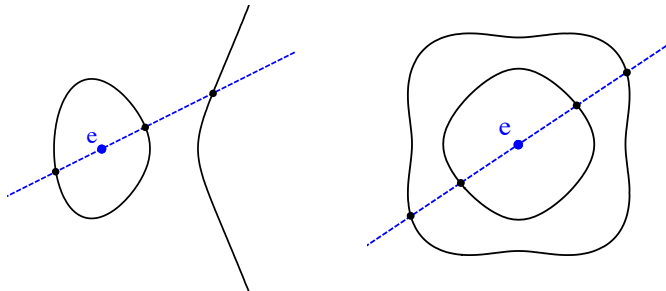


FIGURE 1. Cubic and quartic hyperbolic curves  $\mathbb{P}^2(\mathbb{R})$ .

The Helton-Vinnikov theorem [3] (previously known as the Lax conjecture) says that every hyperbolic polynomial in three variables possesses a definite determinantal representation (1) with real symmetric matrices. Thus given a hyperbolic plane curve, one can investigate the problem of computing a definite determinantal representation.

Computing symmetric determinantal representations of hyperbolic plane curves both symbolically and numerically was investigated by Sturmfels and two of the current authors in [6] and in the case of quartic curves in [5]. Recently, it was discovered [7] that looking for Hermitian matrices  $M_1, M_2, M_3$ , rather than real symmetric matrices, greatly simplifies this computational problem and the proof of Helton and Vinnikov's theorem.

The goal of this paper is to present an algorithm for computing determinantal representations (1), examine this algorithm both numerically and symbolically, and to compare it with existing methods. This construction is based heavily on [7], which generalizes a classical construction due to Dixon [1].

*Acknowledgements.* We would like to thank Arno Fehm for helpful discussions concerning Hilbert's Irreducibility Theorem.

## 1. THE ALGORITHM

The input to our algorithm will be a polynomial  $f \in \mathbb{R}[x, y, z]$  of degree  $d$  with smooth complex variety  $\mathcal{V}_{\mathbb{C}}(f)$  and a point  $e = (e_1, e_2, e_3) \in \mathbb{R}^3$  with respect to which  $f$  is hyperbolic. We will be interested in intersecting the curve  $\mathcal{V}_{\mathbb{C}}(f)$  with the degree- $(d-1)$  curve given by the directional derivative

$$(2) \quad g(x, y, z) = e_1 \frac{\partial f}{\partial x} + e_2 \frac{\partial f}{\partial y} + e_3 \frac{\partial f}{\partial z}.$$

For now, we will assume that the intersection  $\mathcal{V}_{\mathbb{C}}(f) \cap \mathcal{V}_{\mathbb{C}}(g)$  in  $\mathbb{P}^2$  is transverse. That is, the two curves  $\mathcal{V}_{\mathbb{C}}(f)$  and  $\mathcal{V}_{\mathbb{C}}(g)$  intersect in  $d(d-1)$  distinct points. In fact, this implies none of these intersection points are real [7, Lemma 2.4].

The output of the algorithm will be three Hermitian  $d \times d$  matrices  $M_1, M_2, M_3$  such that  $f = c \cdot \det(xM_1 + yM_2 + zM_3)$  where  $c \in \mathbb{R}_{>0}$  and  $e_1M_1 + e_2M_2 + e_3M_3$  is positive definite. Also,  $g$  will be one of the diagonal minors of the resulting matrix  $M = xM_1 + yM_2 + zM_3$ , namely the minor of  $M$  obtained by removing the first row and first column from  $M$ .

The construction below is based on the idea that if the Hermitian matrix  $M$  is a determinantal representation of  $f = \det(M)$ , then its adjugate matrix  $M^{\text{adj}}$  satisfies

$$M^{\text{adj}} \cdot M = \det(M) \cdot I = f \cdot I.$$

Let  $a$  denote the top row of  $M^{\text{adj}}$ . Then, taking the top row of this matrix equation, we obtain the relation  $a(xM_1 + yM_2 + zM_3) = (f, 0, \dots, 0)$ . Similar arguments give  $(xM_1 + yM_2 + zM_3)\bar{a}^T = (f, 0, \dots, 0)^T$ . We introduce a suitable vector  $a = (a_{11}, a_{12}, \dots, a_{1d})$  and solve these linear equations in the entries of the  $M_i$ . This finds  $(M_1, M_2, M_3)$  without ever explicitly computing  $M^{\text{adj}}$ .

The algorithm proceeds as follows:

- (A1) Compute the  $d(d-1)$  points  $\mathcal{V}_{\mathbb{C}}(f) \cap \mathcal{V}_{\mathbb{C}}(g)$ .
- (A2) Split the points into two disjoint, conjugate sets  $\mathcal{V}_{\mathbb{C}}(f, g) = S \cup \bar{S}$ .
- (A3) Let  $a_{11}$  equal  $g$ .
- (A4) Extend  $a_{11}$  to a basis  $a = (a_{11}, \dots, a_{1d})$  of the vector space of polynomials in  $\mathbb{C}[x, y, z]_{d-1}$  that vanish on the points  $S$ .
- (A5) In the  $3d^2$  variables  $(M_1)_{i,j}, (M_2)_{i,j}, (M_3)_{i,j}$ , solve the  $2d \binom{d+2}{2} = (d+2)(d+1)d$  affine linear equations coming from the polynomial vector equations

$$\begin{aligned} a(xM_1 + yM_2 + zM_3) &= (f, 0 \dots 0) \\ (xM_1 + yM_2 + zM_3)\bar{a}^T &= (f, 0 \dots 0)^T. \end{aligned}$$

- (A6) Output the *unique* solution  $M_1, M_2, M_3$ .

We need to argue that such a solution  $M_1, M_2, M_3$  exists, is unique, and has the desired properties, which we do below. Numerical implementation of this algorithm and surrounding computational issues will be discussed in Section 2. In Section 3, we discuss the field extensions necessary for symbolic implementation.

**Theorem 1.** *Let  $f \in \mathbb{R}[x, y, z]$  be hyperbolic with respect to a point  $e \in \mathbb{R}^3$  with  $f(e) > 0$ . Suppose that  $\mathcal{V}_{\mathbb{C}}(f)$  is smooth and that all the intersection points of  $\mathcal{V}_{\mathbb{C}}(f)$  and  $\mathcal{V}_{\mathbb{C}}(g)$  are transverse, where  $g = e_1 \frac{\partial f}{\partial x} + e_2 \frac{\partial f}{\partial y} + e_3 \frac{\partial f}{\partial z}$ . Then the system of equations in (A5) has a unique solution  $M_1, M_2, M_3$ , which are Hermitian matrices satisfying*

$$f = c \cdot \det(xM_1 + yM_2 + zM_3) \quad \text{and} \quad e_1M_1 + e_2M_2 + e_3M_3 \succ 0,$$

where  $c \in \mathbb{R}_{>0}$ .

*Proof. (Existence.)* First, let us show that the affine linear equations (A5) have some solution  $M_1, M_2, M_3$ . By Construction 4.5 and Theorem 4.6 of [7], there exists a Hermitian linear matrix  $M' = xM'_1 + yM'_2 + zM'_3$  such that for some  $c \neq 0$ , the determinant  $\det(M')$  equals  $c^{d-1}f$ , the matrix  $M'(e) = e_1M'_1 + e_2M'_2 + e_3M'_3$  is either positive or negative definite, and the first row of the adjugate matrix  $A = (1/c^{d-2})(M')^{\text{adj}}$  is precisely  $a = (a_{11}, a_{12}, \dots, a_{1d})$ . Since the matrices  $M'$  and  $(M')^{\text{adj}}$  are Hermitian, it follows that the first column of  $(1/c^{d-2})(M')^{\text{adj}}$  is  $\bar{a}^T = (\bar{a}_{11}, \bar{a}_{12}, \dots, \bar{a}_{1d})^T$ .

In fact, the constant  $c$  must be positive. We can see this from examining our matrices at the point  $e$ . Since  $M'(e)$  is definite, both  $(M')^{\text{adj}}(e)$  and  $A(e)$  must be definite as well. Furthermore, because the  $(1, 1)$  entry of  $A(e)$ , namely  $a_{11}(e) = g(e)$ , is positive we see that the matrix  $A(e)$  is positive definite. Then the equation

$$\det(A) = (1/c^{d-2})^d \det((M')^{\text{adj}}) = (1/c^{d-2})^d \cdot (c^{d-1}f)^{d-1} = c \cdot f^{d-1}$$

evaluated in the point  $e$  shows that  $c$  is positive. To find a solution to the equations (A5), let  $M = (1/c)M'$ . Then

$$\det(M) = (1/c)^d \det(M') = (1/c)f.$$

Furthermore  $M^{\text{adj}}$  equals  $(1/c)^{d-1}(M')^{\text{adj}}$ , which is  $(1/c) \cdot A$ . We know that both  $M^{\text{adj}} \cdot M$  and  $M \cdot M^{\text{adj}}$  equal  $\det(M)I$ . Dividing these identities by  $(1/c)$  we see that  $A \cdot M = f \cdot I$  and  $M \cdot A = f \cdot I$ . From taking the first row of the first equation and the first column of the second equation, we see that  $M$  satisfies the equations

$$aM = (f, 0 \dots 0) \quad \text{and} \quad M\bar{a}^T = (f, 0 \dots 0)^T.$$

Since  $c \cdot f = \det(M)$  and  $M(e)$  is positive definite, in order to finish the proof, it suffices to show that this is the unique solution to these equations.

*(Uniqueness.)* Suppose  $M' = xM'_1 + yM'_2 + zM'_3$  is a matrix satisfying the equations (A5). We immediately see that at any point  $(x, y, z)$  in  $\mathcal{V}_{\mathbb{C}}(f)$  the matrix  $M'$  does not have full rank. Since  $\det(M')$  has degree  $d$  and  $f$  is irreducible, we can conclude that  $\det(M') = \alpha f$  for some constant  $\alpha \neq 0$ .

Again we use the identity  $M' \cdot (M')^{\text{adj}} = \det(M')I = \alpha fI$ . For generic  $(x, y, z)$  in  $\mathbb{C}^3$ , the matrix  $M'$  is invertible. These identities then show that the first row of  $(M')^{\text{adj}}$  is  $\alpha a$  and the first column of  $(M')^{\text{adj}}$  is  $\alpha \bar{a}^T$ .

Let  $A$  be the matrix from above whose first row is  $a$  and first column  $\bar{a}^T$ . Because both  $A$  and  $(M')^{\text{adj}}$  have rank one along the curve  $\mathcal{V}_{\mathbb{C}}(f)$ , the entries of  $\alpha A$  and  $(M')^{\text{adj}}$  must differ by a multiple of  $f$ . However, the entries of these matrices have degree  $d - 1$  whereas  $f$  has degree  $d$ , so we see that  $(M')^{\text{adj}}$  must equal  $\alpha A$ . In particular,  $(M')^{\text{adj}}$  is a constant multiple of  $M^{\text{adj}}$ . It follows that  $M'$  is a constant multiple of the original solution  $M$ . Because our affine linear equations (A5) are not homogenous, we see that the solution  $M$  is unique.  $\square$

**Remark 2.** In fact, in our algorithm we can replace  $g$  in (2) by any polynomial  $g \in \mathbb{R}[x, y, z]_{d-1}$  where  $g(e) > 0$  and  $g$  **interlaces  $f$  with respect to  $e$** . By this, we mean that for every point  $p \in \mathbb{R}^3$  the roots of the univariate polynomial  $g(te + p)$  interlace those of  $f(te + p)$ .

**Example 3.** To illustrate our algorithm, we apply it to the quartic

$$(3) \quad f(x, y, z) = x^4 - 4x^2y^2 + y^4 - 4x^2z^2 - 2y^2z^2 + z^4,$$

which is hyperbolic with respect to the point  $e = [1 : 0 : 0]$ , and appears as Example 4.12 in [7]. This curve has two nodes,  $[0 : 1 : 1]$  and  $[0 : -1 : 1]$ , but done carefully, our algorithm still works. Figure 2 shows the real curves  $\mathcal{V}_{\mathbb{R}}(f)$  and  $\mathcal{V}_{\mathbb{R}}(g)$  in different affine planes.

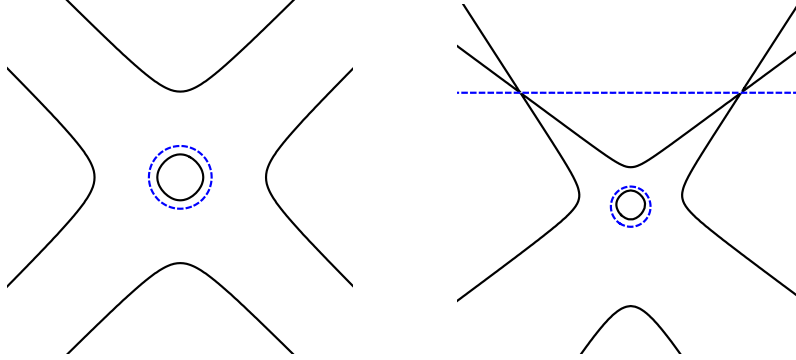


FIGURE 2. The hyperbolic quartic (3) and its directional derivative.

First we define  $a_{11}$  to be the directional derivative  $\frac{1}{4}D_e f = x^3 - 2xy^2 - 2xz^2$ . The intersection of  $f$  and  $a_{11}$  consists of the eight points  $[2 : \pm\sqrt{3} : \pm i]$ ,  $[2 : \pm i : \pm\sqrt{3}]$  and the two nodes,  $[0 : \pm 1 : 1]$ , each with multiplicity 2. We divide these points into two conjugate sets  $S \cup \bar{S}$  where

$$S = \left\{ [0 : 1 : 1], [0 : -1 : 1], [2 : \sqrt{3} : i], [2 : -\sqrt{3} : i], [2 : i : \sqrt{3}], [2 : i : -\sqrt{3}] \right\}.$$

The vector space of cubics in  $\mathbb{C}[x, y, z]$  vanishing on these six points is four dimensional and we extend  $a_{11}$  to a basis  $\{a_{11}, a_{12}, a_{13}, a_{14}\}$  for this space, where

$$\begin{aligned} a_{12} &= ix^3 + 4ixy^2 - 4x^2z - 4y^2z + 4z^3, \\ a_{13} &= -3ix^3 + 4x^2y + 4ixy^2 - 4y^3 + 4yz^2, \\ a_{14} &= -x^3 - 2ix^2y - 2ix^2z + 4xyz. \end{aligned}$$

Let  $M = xA + yB + zC$ . The two  $4 \times 4$  polynomial matrix equations  $aM = (f, 0)$  and  $M\bar{a}^T = (f, 0)^T$  give us 120 affine linear equations in the 48 variables  $A_{ij}, B_{ij}, C_{ij}$ . For example, the first entry of the vector  $aM$  is

$$\begin{aligned} & (A_{11} + iA_{21} - 3iA_{31} - A_{41})x^4 + (4A_{31} - 2iA_{41} + B_{11} + iB_{21} - 3iB_{31} - B_{41})x^3y \\ & + (-2A_{11} + 4iA_{21} + 4iA_{31} + 4B_{31} - 2iB_{41})x^2y^2 + (-4A_{31} - 2B_{11} + 4iB_{21} + 4iB_{31})xy^3 \\ & - 4B_{31}y^4 + (-4A_{21} - 2iA_{41} + C_{11} + iC_{21} - 3iC_{31} - C_{41})x^3z \\ & + (4A_{41} - 4B_{21} - 2iB_{41} + 4C_{31} - 2iC_{41})x^2yz + (-4A_{21} + 4B_{41} - 2C_{11} + 4iC_{21} + 4iC_{31})xy^2z \\ & + (-4B_{21} - 4C_{31})y^3z + (-2A_{11} - 4C_{21} - 2iC_{41})x^2z^2 + (4A_{31} - 2B_{11} + 4C_{41})xyz^2 \\ & + (4B_{31} - 4C_{21})y^2z^2 + (4A_{21} - 2C_{11})xz^3 + (4B_{21} + 4C_{31})yz^3 + 4C_{21}z^4. \end{aligned}$$

Identifying this polynomial with  $f$  gives us 15 affine linear equations. For example, from the monomial  $x^4$ , we see that  $A_{11} + iA_{21} - 3iA_{31} - A_{41} = 1$ . Similarly, from each of the other entries of  $aM - (f, 0)$  and  $M\bar{a}^T - (f, 0)^T$  we get 15 affine linear equations in the  $3 \cdot 4^2$  variables  $A_{ij}, B_{ij}, C_{ij}$ , for a total of  $2 \cdot 4 \cdot 15 = 120$ . The unique solution to these 120 equations gives the Hermitian matrix representation

$$xA + yB + zC = \frac{1}{8} \begin{pmatrix} 14x & 2z & 2ix - 2y & 2i(y - z) \\ 2z & x & 0 & -ix + 2y \\ -2ix - 2y & 0 & x & ix - 2z \\ -2i(y - z) & ix + 2y & -ix - 2z & 4x \end{pmatrix},$$

whose determinant is  $(1/256) \cdot f$ .

## 2. NUMERICAL IMPLEMENTATION

Here we discuss the numerical implementation of this algorithm in `Mathematica`. Below we give some preliminary computation times. Overall, this method results in very fast computations, although the accuracy becomes poor for large  $d$ .

One major issue with numerical computations is that the affine linear equations in (A5) are overdetermined – there are  $d^3 + 3d^2 + 2d$  equations in  $3d^2$  variables. With small numerical errors, these equations no longer have a solution. We solve this by taking a least squares solution to the system.

The steps that take a significant amount of computation time are the following.

- Computing the points  $\mathcal{V}(f, g)$ .
- Computing the basis  $(a_{11}, \dots, a_{1d})$ .
- Translating the polynomial equations (A5) into a system of linear equations.
- Solving the resulting least squares problem.

Extracting the affine equations from the polynomial identities  $aM = (f, 0 \dots 0)$  and  $M\bar{a}^T = (f, 0 \dots 0)^T$  is a step that takes surprisingly long in our `Mathematica` implementation, even longer than solving the least squares problem.

None the less, this method finds (approximate) determinantal representations surprisingly fast. To test our code, we generated hyperbolic polynomials of degree  $d$  by taking the determinant of  $xI + y(B + B^T) + z(C + C^T)$  where  $B$  and  $C$  are random  $d \times d$  matrices with normally distributed entries. Any such determinant will be hyperbolic with respect to the point  $[1 : 0 : 0]$ . Averaging test times for 10 examples in each degree gave the following computation times:

degree	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>15</b>
time (sec)	0.4	0.8	1.7	3.2	6.1	10.7	110
error	$1 \cdot 10^{-9}$	$7 \cdot 10^{-9}$	$1 \cdot 10^{-7}$	$1 \cdot 10^{-5}$	$2 \cdot 10^{-5}$	$1 \cdot 10^{-4}$	500
relative error	$1 \cdot 10^{-11}$	$1 \cdot 10^{-11}$	$9 \cdot 10^{-11}$	$2 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	$5 \cdot 10^{-9}$	$1 \cdot 10^{-5}$

Here by “error” we mean the maximum over the absolute values of the coefficients of the difference between the original polynomial  $f$  and the appropriately scaled determinant  $c \cdot \det(M)$ . We also found it useful to look at the “relative error”, by which we mean the error divided by the largest coefficient of  $f$ .

One additional source of numerical errors is the computation of the determinant of the output of our algorithm. Because of the size of this matrix, a symbolic computation of the determinant is infeasible and instead we compute it by interpolation. Then we use the interpolated polynomial to compute the errors in the coefficients.

For comparison, the only other known methods for computing definite determinantal representations are discussed in [6]. Here, finding definite determinantal representations is already extremely time consuming for quintics ( $d = 5$ ) and practically infeasible for larger degrees ( $d \geq 6$ ). Thus the method described above provides a great improvement in computation ability.

We intend to explore many other aspects of these computations. Our goals include running significantly more trials, understanding the trade off between accuracy and computation time, extending our code to work with nodal curves (like Example 3), and investigating other methods of generating random hyperbolic polynomials. We are also considering computational methods for finding the polynomials  $(a_{11}, \dots, a_{1d})$  without computing the intersection points  $\mathcal{V}_{\mathbb{C}}(f) \cap \mathcal{V}_{\mathbb{C}}(g)$ .

### 3. SYMBOLIC ASPECTS

Ideally we would like to carry out our algorithm symbolically, but most of the time the required field extensions will be too large. Given a hyperbolic polynomial  $f \in \mathbb{Q}[x, y, z]_d$ , one can ask: What is the field extension necessary to carry through the construction above symbolically?

In fact, after computing the points  $\mathcal{V}(f, g)$  and splitting them as  $S \cup \overline{S}$ , all of the remaining steps in the algorithm only require linear algebra, and thus can be done with rational arithmetic. Thus we are interested in the smallest number field  $K$  such that the set of points  $S$  can be defined over  $K$ . For fixed  $f$ , it seems very hard to say anything about the smallest such field for the best possible choice of the interlacing polynomial  $g$ . But at least we can say what happens in the generic case.

**Definition 4.** Let  $K$  be a field of characteristic 0 and let  $f, g \in K[x, y]$  be polynomials such that the intersection  $\mathcal{V}(f, g)$  in  $\mathbb{A}_K^2$  is 0-dimensional. By the **Galois group of the intersection**  $\mathcal{V}(f, g)$ , we mean the Galois group of the field  $L$  generated by the coordinates of the intersection points over  $K$ ,

$$L = K(a_i, b_i : (a_i, b_i) \in \mathcal{V}(f, g)).$$

Note that  $L$  as in the preceding definition is a Galois extension, because any  $K$ -automorphism of  $\overline{K}$  maps a common zero  $(a, b)$  of  $f$  and  $g$  to another one. This argument also shows, that the degree of this field extension  $L/K$  is at most  $(d \cdot e)!$ , where  $\deg(f) = d$  and  $\deg(g) = e$ , since it gives an embedding of  $\text{Gal}(L/K)$  into the symmetric group over the common roots of  $f$  and  $g$ .

**Lemma 5.** Let  $d$  and  $e$  be positive integers and let  $K = \mathbb{Q}(f_{ij}, g_{kl})$  be the rational function field in the variables  $f_{ij}$  for  $i + j \leq d$  and  $g_{kl}$  for  $k + l \leq e$ . Let  $f = \sum_{i+j \leq d} f_{ij} x^i y^j$  and  $g = \sum_{i+j \leq e} g_{ij} x^i y^j$  in  $K[x, y]$ . The variety  $\mathcal{V}(f, g)$  in  $\mathbb{A}_K^2$  consists of  $d \cdot e$  distinct points and has Galois group  $S_{de}$ .

*Proof.* Let  $R \in K[x]$  be the resultant of  $f$  and  $g$  as elements of  $K[x][y]$ . Then  $R$  has degree  $d \cdot e$  and non-zero discriminant since the coefficients of  $f$  and  $g$  are algebraically independent. It follows that the field extension  $L$  of  $K$  by the coordinates of the common zeros of  $f$  and  $g$  is the splitting field of  $R$  over  $K$ .

Any specialization of  $f_{ij}, g_{kl}$  to rational numbers induces a place  $K \rightarrow \mathbb{Q}$ , which extends to a place  $L \rightarrow F$ , where  $F$  is a finite field extension of  $\mathbb{Q}$  such that the Galois group  $\text{Gal}(F/\mathbb{Q})$  embeds into  $\text{Gal}(L/K)$  (see [2, §2.3 and Lemma 16.1.1]). By the example below, there is such a specialization with  $\text{Gal}(F/\mathbb{Q}) = S_{de}$ , hence  $\text{Gal}(L/K) = S_{de}$ .  $\square$

**Example 6.** The resultant of the polynomials  $y - x^d$  and  $y^e - x - 1$  with respect to the variable  $y$  is the polynomial  $R = x^{de} - x - 1$ . The splitting field of  $R$  over  $\mathbb{Q}$  is known to have Galois group  $S_{de}$ , cf. [8, p. 42].

**Theorem 7.** *For almost all polynomials  $f, g \in \mathbb{Q}[x, y]$  of degree  $d$  and  $e$  respectively, the Galois group of the intersection  $\mathcal{V}(f, g)$  is  $S_{de}$ .*

Here, by “almost all” we mean all pairs of polynomials with coefficients outside a thin set in the sense of Serre, cf. [8, §3.3]. Suitably interpreted, this means that for random  $f$  and  $g$ , the Galois group of  $\mathcal{V}(f, g)$  is  $S_{de}$  with probability one.

*Proof.* Let  $L$  and  $K$  be as in the proof of the preceding lemma and let  $p \in K[x]$  be the minimal polynomial of a primitive element of  $L/K$ . For any specialization of  $f_{ij}$  and  $g_{kl}$  to rational numbers for which  $p$  remains irreducible, the resulting extension  $F/\mathbb{Q}$  has Galois group  $S_{de}$  by [2, Lemma 16.1.1(b)].

By Hilbert’s Irreducibility Theorem, the set of all points in  $\mathbb{A}_{\mathbb{Q}}^N$ , where  $N = \text{trdeg}(K/\mathbb{Q})$ , for which  $p$  becomes reducible, is thin, cf. [8, Proposition 3.3.5].  $\square$

**Corollary 8.** *For almost all hyperbolic polynomials  $f \in \mathbb{Q}[x, y, z]_d$  and almost all interlacing curves  $g \in \mathbb{Q}[x, y, z]_{d-1}$ , the smallest Galois extension  $K/\mathbb{Q}$  over which a splitting  $\mathcal{V}_{\mathbb{C}}(f, g) = S \cup \bar{S}$  is defined, has Galois group  $S_{d(d-1)}$ .*

*Proof.* First note that the set of all hyperbolic polynomials of degree  $d$  has non-empty interior in the vector space of polynomials of degree  $d$  and that the set of all interlacing curves for a smooth hyperbolic curve of degree  $d$  has non-empty interior in the vector space of all polynomials of degree  $d - 1$ , cf. [4]. Given such  $f, g$ , let  $F$  be the splitting field of  $\mathcal{V}(f, g)$  and let  $F' \subset F$  be a Galois extension of  $\mathbb{Q}$  over which  $S$  is defined. Then the Galois group of  $F'$  is a normal subgroup of  $\text{Gal}(F/\mathbb{Q})$  that leaves  $S$  invariant. If  $\text{Gal}(F/\mathbb{Q}) = S_{d(d-1)}$ , there is no non-trivial such subgroup.  $\square$

## REFERENCES

- [1] Alfred Cardew Dixon. Note on the reduction of a ternary quantic to a symmetrical determinant. *Math. Proc. Cambridge Phil. Society*, 11:350–351, 1902.
- [2] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.
- [3] J. William Helton and Victor Vinnikov. Linear matrix inequality representation of sets. *Comm. Pure Appl. Math.*, 60(5):654–674, 2007.
- [4] Wim Nuij. A note on hyperbolic polynomials. *Math. Scand.*, 23:69–72 (1969), 1968.
- [5] Daniel Plaumann, Bernd Sturmfels, and Cynthia Vinzant. Quartic curves and their bitangents. *J. Symbolic Comput.*, 46(6):712–733, 2011.
- [6] Daniel Plaumann, Bernd Sturmfels, and Cynthia Vinzant. Computing linear matrix representations of Helton-Vinnikov curves. In *Mathematical methods in systems, optimization, and control*, volume 222 of *Oper. Theory Adv. Appl.*, pages 259–277. Birkhäuser/Springer Basel AG, Basel, 2012.
- [7] Daniel Plaumann and Cynthia Vinzant. Determinantal representations of hyperbolic plane curves: An elementary approach. *ArXiv e-prints*.
- [8] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.