3

Symbolic-numeric methods for solving polynomial equations and applications

Mohamed Elkadi[1] and Bernard Mourrain[2]

[1] UMR 6623, UNSA, B.P. 71, Parc Valrose, 06108 Nice, France,
elkadi@math.unice.fr
[2] INRIA, GALAAD, B.P. 93, Sophia-Antipolis, 06902 France,
mourrain@sophia.inria.fr

Summary. This tutorial gives an introductory presentation of algebraic and geometric methods to solve a polynomial system $f_1 = \cdots = f_m = 0$. The algebraic methods are based on the study of the quotient algebra $\mathcal{A}$ of the polynomial ring modulo the ideal $I = (f_1, \ldots, f_m)$. We show how to deduce the geometry of solutions from the structure of $\mathcal{A}$ and in particular, how solving polynomial equations reduces to eigenvalue and eigenvector computations of multiplication operators in $\mathcal{A}$. We give two approaches for computing the normal form of elements in $\mathcal{A}$, used to obtain a representation of multiplication operators. We also present the duality theory and its application to solving systems of algebraic equations. The geometric methods are based on projection operations which are closely related to resultant theory. We present different constructions of resultants and different methods for solving systems of polynomial equations based on these formulations. Finally, we illustrate these tools on problems coming from applications in computer-aided geometric design, computer vision, robotics, computational biology and signal processing.

3.0 Introduction

Polynomial system solving is ubiquitous in many applications such as computer geometric design, geometric modelling, robotics, computer vision, computational biology, signal processing, ... Specific methods like minimization, Newton iterations, ... are often used, but do not always offer guarantees on the result. In this paper, we give an introductory presentation of algebraic methods for solving a polynomial system $f_1 = \cdots = f_m = 0$. By a reformulation of the problem in terms of matrix manipulations, we obtain a better control of the structure and the accuracy of computations. The tools that we introduce are illustrated by explicit computations. A MAPLE package implements the algorithms described hereafter and is publicly available on the Internet[3]. We encourage the reader to use it for his own experimentation on

[3] http://www.inria.fr/galaad/logiciels/multires/

the examples illustrating the presentation. For more advanced computations described in the last section, we use the C++ library SYNAPS available on the Internet[4]. Our approach is based on the study of the quotient algebra $\mathcal{A}$ of the polynomial ring by the ideal $(f_1, \ldots, f_m)$. We describe, in the first part, the well known method of Gröbner basis to compute the normal form of elements in $\mathcal{A}$ which yields the algebraic structure of this quotient. We also mention a recent generalization of this approach which allows to combine, more safely, symbolic and numeric computations.

In the second part, we show how to deduce the geometry of solutions from the structure of $\mathcal{A}$. In particular, we show how solving polynomial systems reduces to the computation of eigenvalues or eigenvectors of operators of multiplication in $\mathcal{A}$. In the real case, we also show how to recover information on the real roots from this algebra.

We also study duality theory and show how to use it for solving polynomial systems.

Another major operation in effective algebraic geometry is projection. It is related to resultant theory. We present different notions and constructions of resultants and we derive methods to solve systems of polynomial equations. In practice, according to the class of systems that we want to solve, we will have to choose the resultant construction adapted to the geometry of the problem. Finally, we illustrate these tools on problems coming from several areas of applications.

For more details on the material presented here, see [EM].

3.1 Solving polynomial systems

The problem of solving polynomial equations goes back to the ancient Greeks and Chinese. It is not surprising that a large number of methods exists to handle this problem. We divide them into the following families and we will focus essentially on the last two classes.

3.1.1 Classes of solvers

Analytic solvers

The analytic solvers exploit the value of the functional $f = (f_1, \ldots, f_m)$ and its derivatives in order to converge to a solution or all the solutions of $f = 0$. Typical examples are Newton-like methods, Minimization methods, Weierstrass' method [Dem87, SS93, Bin96, MR02].

[4] `http://www.inria.fr/galaad/logiciels/synaps/`

Homotopic solvers

The idea behind the homotopic approaches is to deform a system with known roots into the system $f = 0$ that we want to solve. Examples of such continuation methods are based on projective [MS87b], toric [Li97, VVC94] or generally flat deformations of $f = 0$. See Chapter 8 and [AG90b] for more details.

Subdivision solvers

The subdivision methods use an exclusion criterion to remove a domain if it does not contain a root of $f = 0$. These solvers are often used to isolate the real roots, if possible. Exclusion criteria are based on Taylor's exclusion function [DY93], interval arithmetic [Kea90], the Turan test [Pan96], Sturm's method [BR90, Roy96], or Descartes' rule [Usp48, RZ03, MVY02].

Algebraic solvers

This class of methods exploits the known relations between the unknowns. They are based on normal form computations in the quotient algebra [CLO97, MT00, MT02] and reduce to a univariate or eigenvalue problem [Mou98].

Geometric solvers

These solvers project the problem onto a smaller subspace and exploit geometric properties of the set of solutions. Tools such as resultant constructions [GKZ94, EM99b, BEM00, BEM01, Bus01a] are used to reduce the solutions of the polynomial system to a univariate or eigenvalue problem. This reduction to univariate polynomials is also an important ingredient of triangular set methods [Tsü94, Wan95, ALMM99].

3.1.2 Notation

We fix the notation that will be used hereafter. Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ be its algebraic closure, $R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$ be the algebra of polynomials in the variables $\mathbf{x} = (x_1, \ldots, x_n)$ with coefficients in $\mathbb{K}$. For the sake of simplicity, we will assume that $\mathbb{K}$ is of characteristic 0.

Let $f_1, \ldots, f_m \in R$ be m polynomials. Our objective is to solve the system $f_1 = 0, \ldots, f_m = 0$, also denoted by $f = 0$. If $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n, |\alpha| = \alpha_1 + \cdots + \alpha_n, \mathbf{x}^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$.

Let I be the ideal generated by $f_1, \ldots, f_m$ in R and $\mathcal{Z}(I)$ be the affine variety $\{\zeta \in \overline{\mathbb{K}}^n : f_1(\zeta) = \cdots = f_m(\zeta) = 0\}$. We will assume that $\mathcal{Z}(I) = \{\zeta_1, \ldots, \zeta_d\}$ is a non-empty and finite set. The algebraic approach to solve the system $f = 0$ is based on the study of the $\mathbb{K}$-algebra $\mathcal{A} = R/I$. The hypothesis

that $\mathcal{Z}(I)$ is finite implies that the $\mathbb{K}$-vector space $\mathcal{A}$ is of finite dimension over $\mathbb{K}$, see Theorem 2.1.2 in Chapter 2. We denote by $\widehat{R}$ (resp. $\widehat{\mathcal{A}}$) the dual of the vector space R (resp. $\mathcal{A}$).

Algebraic solvers exploit the properties of $\mathcal{A}$, which means that they must be able to compute effectively in this algebra. This can be performed by a so-called *normal form* algorithm. We are going to describe now two approaches to compute normal forms.

3.1.3 Gröbner bases

Gröbner bases are a major tool in effective algebraic geometry, which yields algorithmic answers to many question in this domain [CLO97, BW93, AL94, Eis95]. It is related to the use of a monomial ordering.

Definition 3.1.1. *A monomial ordering is a total order* $>$ *on the set of monomials of* $\mathbb{K}[\mathbf{x}]$ *such that*

i) $\forall \alpha \neq 0,\ 1 < \mathbf{x}^\alpha$,
ii) $\forall (\alpha, \beta, \gamma) \in (\mathbb{N}^n)^3$, *if* $\mathbf{x}^\alpha < \mathbf{x}^\beta$ *then* $\mathbf{x}^{\alpha+\gamma} < \mathbf{x}^{\beta+\gamma}$.

Some well known monomial orderings are defined as follows:

Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$.

– The lexicographic ordering with $x_1 > \cdots > x_n$: $\mathbf{x}^\alpha <_l \mathbf{x}^\beta$ iff there exists i such that $\alpha_1 = \beta_1, \ldots, \alpha_i = \beta_i, \alpha_{i+1} < \beta_{i+1}$.

– The graded lexicographic ordering with $x_1 > \cdots > x_n$: $\mathbf{x}^\alpha <_{gl} \mathbf{x}^\beta$ iff $|\alpha| < |\beta|$ or ($|\alpha| = |\beta|$ and $\mathbf{x}^\alpha <_l \mathbf{x}^\beta$).

Given a monomial ordering $>$, we define as in the univariate case, the leading term of $p \in R$ as the term (the coefficient times its monomial) of p whose monomial is maximal for $>$. We denote it by $\mathcal{L}_>(p)$ $\big($or simply $\mathcal{L}(p)\big)$. We write every $p \in R$ as $p = a_0\mathbf{x}^{\alpha_0} + \cdots + a_l\mathbf{x}^{\alpha_l}$, with $a_i \neq 0$ and $\alpha_0 > \cdots > \alpha_l$.

Let $f, f_1, \ldots, f_m \in R$. As in the Euclidean division there are polynomials $q_1, \ldots, q_m, r$ such that $f = q_1 f_1 + \cdots + q_m f_m + r$, where no term of r divides any of $\mathcal{L}(f_1), \ldots, \mathcal{L}(f_m)$ (in this case we say that r is reduced with respect to $f_1, \ldots, f_m$). This is the multivariate division of f by $f_1, \ldots, f_m$. The polynomials $q_1, \ldots, q_m$ are the quotients and r the remainder of this division.

If I is an ideal of $R = \mathbb{K}[\mathbf{x}]$, we define $\mathcal{L}_>(I)$ $\big($or simply $\mathcal{L}(I)\big)$ to be the ideal generated by the set of leading terms of elements of I.

By Dickson's lemma [CLO97] or by Noetherianity of $\mathbb{K}[\mathbf{x}]$, this ideal $\mathcal{L}_>(I)$ is generated by a finite set of monomials. This leads to the definition of Gröbner bases:

Definition 3.1.2. *A finite subset* $G = \{g_1, \ldots, g_t\}$ *of the ideal* I *is a Gröbner basis of* I *for a given monomial order* $>$ *iff* $\mathcal{L}_>(I) = \big(\mathcal{L}_>(g_1), \ldots, \mathcal{L}_>(g_t)\big)$.

Some interesting properties of a Gröbner basis G are:

– For any $p \in R$, the remainder of the multivariate division of p by G is unique. It is called the *normal form* of p modulo the ideal I and is denoted by $N(p)$ (see [CLO97]).

– The polynomial $p \in I$ iff its normal form $N(p) = 0$.

– A basis B of the $\mathbb{K}$-vector space $\mathcal{A} = R/I$ is given by the set of monomials *which are not in* $\mathcal{L}_>(I)$. This allows us to define the multiplication table by an element $a \in \mathcal{A}$: We multiply first the elements of B by a as usual polynomials and then normalize the products by reduction by G.

The ideal I can have several Gröbner bases but only one which is reduced (i.e. the leading coefficients of elements of G are equal to 1, and every $g \in G$ is reduced with respect to $G \setminus \{g\}$). Efficient algorithms and software have been developed over the past decades to compute reduced Gröbner bases. We mention in particular [Fau99], [GS], [GPS01], [Roba].

Example 3.1.3. Let I be the ideal of $R = \mathbb{Q}[x_1, x_2]$ generated by

$$f_1 := 13\,x_1^2 + 8\,x_1\,x_2 + 4\,x_2^2 - 8\,x_1 - 8\,x_2 + 2 \quad \text{and} \quad f_2 := x_1^2 + x_1\,x_2 - x_1 - \tfrac{1}{6}.$$

The reduced Gröbner basis `G` of I for the graded lexicographic ordering with $x_1 > x_2$ is (on Maple):

```
> with(Groebner); G:= gbasis([f1,f2],tdeg(x[1],x[2]));
```

$$(30\,x_1x_2 - 30\,x_1 - 25 - 24\,{x_2}^2 + 48\,x_2, 15\,{x_1}^2 + 12\,{x_2}^2 - 24\,x_2 + 10,$$
$$216\,{x_2}^3 - 648\,{x_2}^2 + 5\,x_1 + 632\,x_2 - 200).$$

The leading monomials of elements of `G` are $x_1\,x_2, {x_1}^2, {x_2}^3$. Then a basis of $\mathcal{A}$ is $\{1, x_1, x_2, x_2^2\}$. Using the reduction by `G`, the matrix of multiplication by x_1 in this basis is:

```
> L:= map(u->normalf(u,G,tdeg(x[1],x[2])),
>         [x[1],x[1]^2,x[1]*x[2],x[1]*x[2]^2]);
```

$$(x_1, -4/5\,{x_2}^2 + 8/5\,x_2 - 2/3, x_1 + 5/6 + 4/5\,{x_2}^2 - 8/5\,x_2, -\frac{839}{270}\,x_2 + 8/5\,{x_2}^2 + \frac{53}{54}\,x_1 + \frac{85}{54})$$

```
> matrixof(L,[[1,x[1],x[2],x[2]^2]]);
```

$$\begin{pmatrix} 0 & -2/3 & 5/6 & \frac{85}{54} \\ 1 & 0 & 1 & \frac{53}{54} \\ 0 & 8/5 & -8/5 & -\frac{839}{270} \\ 0 & -4/5 & 4/5 & 8/5 \end{pmatrix}.$$

This is the matrix of coefficients of elements of the monomial basis multiplied by x_1, expressed in this basis.

Since the variety $\mathcal{Z}(I)$ is finite, a lexicographic Gröbner basis with $x_n > \cdots > x_1$ contains elements $g_1, \ldots, g_n$ such that $g_i \in \mathbb{K}[x_1, \ldots, x_i]$ and $\mathcal{L}(g_i)$ depends only on x_i. This reduces the problem of solving $f = 0$ to solving a triangular system, hence to the problem of finding the roots of a univariate polynomial. Unfortunately the lexicographic Gröbner bases are not used in practice because of their high complexity of computation. We proceed as follows: First we compute a Gröbner basis for another monomial ordering and then we use a conversion procedure to obtain a lexicographic one. For more details see for instance [FGLM93].

3.1.4 General normal form

The construction of Gröbner bases may not be numerically stable, as shown in the following example:

Example 3.1.4. Let

```
> f1:= x[1]^2+x[2]^2-x[1]+x[2]-2; f2:= x[1]^2-x[2]^2+2*x[2]-3;
```

The Gröbner basis of (f_1, f_2) for the graded lexicographic ordering with $x_1 > x_2$ is:

```
> G:=gbasis([f1,f2],tdeg(x[1],x[2]));
```

$$(2\,{x_2}^2 - x_1 - x_2 + 1, 2\,{x_1}^2 - x_1 + 3\,x_2 - 5).$$

The leading monomials of elements of `G` are x_1^2 and x_2^2. A monomial basis of $\mathcal{A}$ is $\{1, x_1, x_2, x_1x_2\}$. Consider now a small perturbation of the system $f_1 = f_2 = 0$ and compute its Gröbner basis for the same monomial ordering:

```
> gbasis([f1,f2+1.0/10000000*x[1]*x[2]],tdeg(x[1],x[2]));
```

$$\begin{aligned}(&-2\,{x_2}^2 + x_1 + x_2 - 1 + 0.0000001\,x_1x_2, \quad {x_1}^2 + {x_2}^2 - x_1 + x_2 - 2,\\ &{x_2}^3 - 10000000.99999999999999500000000000000125\,{x_2}^2\\ &+5000000.25000001249999937499996875000156250000781250\,x_1\\ &+5000000.75000003749999312499990625001718750023437 50\,x_2\\ &-5000000.25000006249999937499984375000156250039062 50).\end{aligned}$$

The leading monomials of this Gröbner basis are $x_1\,{x_2}, {x_1}^2, {x_2}^3$ and the corresponding basis of the perturbed algebra is $\{1, x_1, x_2, x_2^2\}$. After a small perturbation, the basis of the quotient algebra may "jump" from one set of monomials to another one, though the two set of solutions are very close from a geometric point of view. Moreover, some polynomials of the Gröbner basis of the perturbed system have large coefficients.

Thus, Gröbner bases computations may introduce artificial discontinuities due to the choice of a monomial order. A recent generalization of this notion has been proposed in [Mou99, MT00]. It is based on a new criterion which gives a necessary and sufficient condition for a projection onto a vector subspace of R to be a normal form modulo the ideal I. More precisely we have:

Theorem 3.1.5. *Let B be a vector space in $R = \mathbb{K}[x_1, \ldots, x_n]$ connected to the constant polynomial* 1[5]. *If B^+ is the vector subspace generated by $B \cup x_1 B \cup \ldots \cup x_n B$, $N : B^+ \to B$ is a linear map such that N is the identity on B, we define for $i = 1, \ldots, n$, the maps*

$$\begin{aligned} M_i : B &\to B \\ b &\mapsto M_i(b) := N(x_i b). \end{aligned}$$

The two following properties are equivalent:

1. *For all $1 \leq i, j \leq n$, $M_i \circ M_j = M_j \circ M_i$.*
2. *$R = B \oplus I$, where I is the ideal generated by the kernel of N.*

If this holds, the B-reduction along $\ker(N)$ *is canonical.*

In Chapter 4, you will also find more material on this approach and a proof of Theorem 3.1.5, in the special case of 0-dimensional ideals.

This leads to a completion-like algorithm which starts with the linear subspace K_0 generated by the polynomials $f_1, \ldots, f_m$, which we wish to solve, and iterates the construction $K_{i+1} = K_i^+ \cap L$, where L is a fixed vector space. We stop when $K_{i+1} = K_i$. See [Mou99, MT00, Tré02] for more details. This approach allows us to fix first the set of monomials on which we want to do linear operations and thus to treat more safely polynomials with approximate coefficients. It can be adapted very naturally to Laurent polynomials, which is not the case for Gröbner bases computations. Moreover it can be specialized very efficiently to systems of equations for which the basis of $\mathcal{A}$ is known a priori, such as in the case of a complete projective intersection [MT00].

Example 3.1.6. For the perturbed system of the previous example, the normal forms for the monomials on the border of $B = \{1, x_1, x_2, x_1x_2\}$ are:

$$\begin{aligned} {x_1}^2 &= -0.00000005\, x_1x_2 + 1/2\, x_1 - 3/2\, x_2 + 5/2, \\ {x_2}^2 &= +0.00000005\, x_1x_2 + 1/2\, x_1 + 1/2\, x_2 - 1/2, \\ {x_1}^2x_2 &= 0.49999999\, x_1x_2 - 0.74999998\, x_1 + 1.75000003\, x_2 + 0.74999994, \\ x_1{x_2}^2 &= 0.49999999\, x_1x_2 - 0.25000004\, x_1 - 0.74999991\, x_2 + 1.25000004. \end{aligned}$$

This set of relations gives the matrices of multiplication by the variables x_1 and x_2 in $\mathcal{A}$. An implementation by Ph. Trébuchet of an algorithm computing this new type of normal form is available in the SYNAPS library (see `Solve(L,newmac<C>())`).

3.2 Structure of the quotient algebra

In this section we will see how to recover the solutions of the system $f = 0$ from the structure of the algebra $\mathcal{A}$, which we assume to be given through a normal form procedure.

[5] Any monomial $\mathbf{x}^\alpha \neq 1 \in B$ is of the form $x_i\mathbf{x}^\beta$ with $\mathbf{x}^\beta \in B$ and some i in $\{1, \ldots, n\}$.

3.2.1 Dual of the quotient algebra

First we consider the dual $\widehat{R}$ that is, the space of linear forms from R to $\mathbb{K}$. The *evaluation* $\mathbf{1}_\zeta$ *at a fixed point* ζ is an example of such linear forms: $p \in R \mapsto \mathbf{1}_\zeta(p) := p(\zeta) \in \mathbb{K}$. Another class of linear forms is obtained by differential operators, namely for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$,

$$\begin{aligned} \mathbf{d}^\alpha : \ & R \to \mathbb{K} \\ & p \mapsto \frac{1}{\prod_{i=1}^n \alpha_i!} \big((\partial_1)^{\alpha_1} \cdots (\partial_n)^{\alpha_n} p\big)(0), \end{aligned}$$

where ∂_i is the derivative with respect to the variable x_i (see also Section 2.2.2 of Chapter 2). If $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$,

$$\mathbf{d}^\alpha \left(\prod_{i=1}^n x_i^{\beta_i} \right) = \begin{cases} 1 \text{ if } \alpha_i = \beta_i \text{ for } i = 1, \ldots, n \\ 0 \text{ otherwise.} \end{cases}$$

It follows that $(\mathbf{d}^\alpha)_{\alpha \in \mathbb{N}^n}$ is the dual basis of the monomial basis $(\mathbf{x}^\alpha)_{\alpha \in \mathbb{N}^n}$ of R. Notice that $(\mathbf{d}^\alpha)_{\alpha \in \mathbb{N}^n}$ can be defined for every characteristic. We assume again that $\mathbb{K}$ is a field of arbitrary characteristic. We deduce that for every $\Lambda \in \widehat{R}$ we have $\Lambda = \sum_{\alpha \in \mathbb{N}^n} \Lambda(\mathbf{x}^\alpha)\, \mathbf{d}^\alpha$.

The vector space $\{\sum_{\alpha \in \mathbb{N}^n} c_\alpha\, \mathbf{d}_1^{\alpha_1} \ldots \mathbf{d}_n^{\alpha_n} : c_\alpha \in \mathbb{K}\}$ (where $\mathbf{d}_i^{\alpha_i}$ denotes the map $p \in R \mapsto \frac{1}{\alpha_i!}(\partial_i^{\alpha_i} p)(0)\big)$ of formal power series in $\mathbf{d}_1, \ldots, \mathbf{d}_n$ with coefficients in $\mathbb{K}$ is denoted by $\mathbb{K}[[\mathbf{d}]] = \mathbb{K}[[\mathbf{d}_1, \ldots \mathbf{d}_n]]$. The linear map

$$\Lambda \in \widehat{R} \mapsto \sum_{\alpha \in \mathbb{N}^n} \Lambda(\mathbf{x}^\alpha)\, \mathbf{d}^\alpha \in \mathbb{K}[[\mathbf{d}]]$$

defines a one-to-one correspondence. So we can identify $\widehat{R}$ with $\mathbb{K}[[\mathbf{d}]]$. Under this identification, the linear form evaluation at 0 corresponds to the constant power series 1; it is also denoted $\mathbf{d}^0$.

Example 3.2.1. Let $n = 3$. The value of the linear form $1 + \mathbf{d}_1 + 2\,\mathbf{d}_1\mathbf{d}_2 + {\mathbf{d}_3}^2$ on the polynomial $1 + x_1 + x_1x_2$ is:

$$(1 + \mathbf{d}_1 + 2\,\mathbf{d}_1\mathbf{d}_2 + {\mathbf{d}_3}^2)(1 + x_1 + x_1x_2) = 4.$$

The dual $\widehat{R}$ has a natural structure of R-module: For $(p, \Lambda) \in R \times \widehat{R}$,

$$p \cdot \Lambda : q \in R \mapsto (p \cdot \Lambda)(q) := \Lambda(p\, q) \in \mathbb{K}.$$

If $p \in R$ and $\alpha_i \in \mathbb{N}^*$, we check that $\mathbf{d}_i^{\alpha_i}(x_i\, p) = \frac{1}{(\alpha_i - 1)!}\big(\partial_i^{\alpha_i - 1} p\big)(0)$. Consequently, for $p \in R$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ with $\alpha_i \neq 0$ for a fixed i, we have

$$(x_i \cdot \mathbf{d}^\alpha)(p) = \mathbf{d}^\alpha(x_i\, p) = \mathbf{d}_1^{\alpha_1} \cdots \mathbf{d}_{i-1}^{\alpha_{i-1}} \mathbf{d}_i^{\alpha_i - 1} \mathbf{d}_{i+1}^{\alpha_{i+1}} \cdots \mathbf{d}_n^{\alpha_n}(p).$$

That is, x_i acts as the *inverse* of $\mathbf{d}_i$ in $\mathbb{K}[[\mathbf{d}]]$. This is the reason why in the literature such a representation is referred to as the *inverse system* (see for instance [Mac94]). If $\alpha_i = 0$, then $x_i \cdot \mathbf{d}^\alpha = 0$. Then we redefine the product $p \cdot \Lambda$ as follows:

Proposition 3.2.2. *(see also [MP00], [Fuh96]) For $p \in R$ and $\Lambda \in \mathbb{K}[[\mathbf{d}]]$,*

$$p \cdot \Lambda = \pi_+\big(p(\mathbf{d}_1^{-1}, \ldots, \mathbf{d}_n^{-1})\, \Lambda(\mathbf{d})\big),$$

where π_+ is the projection on the vector space generated by the monomials with positive exponents.

Example 3.2.1 (continued).

$$(1 + x_1 + x_1x_2) \cdot (1 + \mathbf{d}_1 + \mathbf{d}_1\mathbf{d}_2 + {\mathbf{d}_3}^2) = 3 + \mathbf{d}_1 + \mathbf{d}_1\mathbf{d}_2 + {\mathbf{d}_3}^2 + \mathbf{d}_2.$$

The constant term of this expansion is the value of the linear form $1 + \mathbf{d}_1 + \mathbf{d}_1\mathbf{d}_2 + {\mathbf{d}_3}^2$ at the polynomial $1 + x_1 + x_1x_2$.

3.2.2 Multiplication operators

Since the variety $\mathcal{Z}(I)$ is finite, the $\mathbb{K}$-algebra $\mathcal{A}$ has the decomposition

$$\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_d, \tag{3.1}$$

where $\mathcal{A}_i$ is the local algebra associated with the root ζ_i (see also Section 2.7, Chapter 2). So there are elements $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathcal{A}$ such that

$$\mathbf{e}_1 + \cdots + \mathbf{e}_d \equiv 1\ ,\ \mathbf{e}_i^2 \equiv \mathbf{e}_i\ ,\ \mathbf{e}_i\mathbf{e}_j \equiv 0 \text{ if } i \neq j.$$

These elements are called the fundamental *idempotents* of $\mathcal{A}$, and generalize the univariate Lagrange polynomials. They satisfy $\mathcal{A}_i = \mathbf{e}_i\,\mathcal{A}$ and $\mathbf{e}_i(\zeta_j) = 1$ if $i = j$ and 0 otherwise. The dimension of the $\mathbb{K}$-vector space $\mathcal{A}_i$ is by definition the *multiplicity* of the root ζ_i, and it is denoted by μ_{ζ_i} .

We recall that a linear form on $\mathcal{A}$ can be identified with a linear form on R which vanishes on the ideal I. Thus the evaluation $\mathbf{1}_\zeta$, which is a linear form on R, is an element of $\widehat{\mathcal{A}}$ iff $\zeta \in \mathcal{Z}(I)$.

The first operators that come naturally in the study of $\mathcal{A}$ are the operators of multiplication by elements of $\mathcal{A}$. For any $a \in \mathcal{A}$, we define

$$\begin{aligned} M_a : \mathcal{A} &\to \mathcal{A} \\ b &\mapsto M_a(b) := a\,b. \end{aligned}$$

We also consider its transpose operator

$$\begin{aligned} M_a^{\mathtt{t}} : \widehat{\mathcal{A}} &\to \widehat{\mathcal{A}} \\ \Lambda &\mapsto M_a^{\mathtt{t}}(\Lambda) = \Lambda \circ M_a. \end{aligned}$$

The matrix of $M_a^{\mathtt{t}}$ in the dual basis of a basis B of $\mathcal{A}$ is the transpose of the matrix of M_a in B.

Example 3.1.3 (continued). Consider the matrix $\mathtt{M}_{x_1}$ of multiplication by x_1 in the basis $B = \{1, x_1, x_2, x_1x_2\}$ of $\mathcal{A} = \mathbb{K}[x_1, x_2]/(f_1, f_2)$: We multiply the monomials of B by x_1 and reduce the products to the normal forms, so

$$1 \times x_1 \equiv x_1 \quad , \quad x_1 \times x_1 \equiv -x_1x_2 + x_1 + \frac{1}{6} \quad , \quad x_2 \times x_1 \equiv x_1x_2 \quad ,$$
$$x_1x_2 \times x_1 \equiv -x_1x_2 + \frac{55}{54}\,x_1 + \frac{2}{27}\,x_2 + \frac{5}{54}.$$

Then

$$\mathtt{M}_{x_1} = \begin{pmatrix} 0 & \frac{1}{6} & 0 & \frac{5}{54} \\ 1 & 1 & 0 & \frac{55}{54} \\ 0 & 0 & 0 & \frac{2}{27} \\ 0 & -1 & 1 & -1 \end{pmatrix}.$$

The multiplication operators can be computed using a normal form algorithm. This can be performed, for instance by Gröbner basis computations (see Sections 3.1.3 and 3.1.4). In Section 3.5, we will describe another way to compute implicitly these operators based on resultant matrices (see also Section 2.3, Chapter 2).

Hereafter, $\mathbf{x}^E = (\mathbf{x}^\alpha)_{\alpha\in E}$ denotes a monomial basis of $\mathcal{A}$ (for instance obtained by a Gröbner basis). Then any polynomial can be reduced modulo $(f_1, \ldots, f_m)$ to a linear combination of monomials of $\mathbf{x}^E$.

The matrix approach to solve polynomial systems is based on the following fundamental theorem:

Theorem 3.2.3. *Assume that $\mathcal{Z}(I) = \{\zeta_1, \ldots, \zeta_d\}$. We have*

1. *Let $a \in \mathcal{A}$. The eigenvalues of the operator M_a (and its transpose $M_a^{\mathtt{t}}$) are $a(\zeta_1), \ldots, a(\zeta_d)$.*
2. *The common eigenvectors of $(M_a^{\mathtt{t}})_{a\in\mathcal{A}}$ are (up to a scalar) $\mathbf{1}_{\zeta_1}, \ldots, \mathbf{1}_{\zeta_d}$.*

Proof. 1) Let $i \in \{1, \ldots, d\}$. For every $b \in \mathcal{A}$,

$$\big(M_a^{\mathtt{t}}(\mathbf{1}_{\zeta_i})\big)(b) = \mathbf{1}_{\zeta_i}(a\,b) = \big(a(\zeta_i)\,\mathbf{1}_{\zeta_i}\big)(b).$$

This shows that $a(\zeta_1), \ldots, a(\zeta_d)$ are eigenvalues of M_a and $M_a^{\mathtt{t}}$, $\mathbf{1}_{\zeta_i}$ is an eigenvector of $M_a^{\mathtt{t}}$ associated with $a(\zeta_i)$, and $\mathbf{1}_{\zeta_1}, \ldots, \mathbf{1}_{\zeta_d}$ are common eigenvectors to $M_a^{\mathtt{t}}, a \in \mathcal{A}$.

Now we will show that every eigenvalue of M_a is one $a(\zeta_i)$. For this we consider

$$p(\mathbf{x}) = \prod_{\zeta\in\mathcal{Z}(I)} \big(a(\mathbf{x}) - a(\zeta)\big) \in \mathbb{K}[\mathbf{x}].$$

This polynomial vanishes on $\mathcal{Z}(I)$. Using Hilbert's Nullstellensatz we can find an integer $m \in \mathbb{N}$ such that the operator

$$p^m(M_a) = \prod_{\zeta\in\mathcal{Z}(I)} \big(M_a - a(\zeta)\,\mathbb{I}\big)^m$$

vanishes on $\mathcal{A}$ ($\mathbb{I}$ is the identity operator). We deduce that the minimal polynomial of the operator M_a divides $\prod_{\zeta\in\mathcal{Z}(I)} \big(T - a(\zeta)\big)^m$, and that the eigenvalues of M_a belong to $\{a(\zeta) : \zeta \in \mathcal{Z}(I)\}$.

2) Let $\Lambda \in \widehat{\mathcal{A}}$ be a common eigenvector to $M_a^{\mathtt{t}}$, $a \in \mathcal{A}$, and $\gamma = (\gamma_1, \ldots, \gamma_n)$ such that $M_{x_i}^{\mathtt{t}}(\Lambda) = \gamma_i \Lambda$ for $i = 1, \ldots, n$. Then all the monomials $\mathbf{x}^\alpha$ satisfy

$$\big(M_{x_i}^{\mathtt{t}}(\Lambda)\big)(\mathbf{x}^\alpha) = \Lambda(x_i\, \mathbf{x}^\alpha) = \gamma_i \Lambda(\mathbf{x}^\alpha).$$

From this we deduce that $\Lambda = \Lambda(1)\, \mathbf{1}_\gamma$. As $\Lambda \in \widehat{\mathcal{A}} = I^\perp$, $\Lambda(p) = \Lambda(1)p(\gamma) = 0$ for every $p \in I$, and $\mathbf{1}_\gamma \in \widehat{\mathcal{A}}$.

Since $\mathbf{x}^E = (\mathbf{x}^\alpha)_{\alpha \in E}$ is a basis of $\mathcal{A}$, the coordinates of $\mathbf{1}_{\zeta_i}$ in the dual basis of $\mathbf{x}^E$ are $(\zeta_i^\alpha)_{\alpha \in E}$. Thus if $\mathbf{x}^E$ contains $1, x_1, \ldots, x_n$ (which is often the case), we deduce the following algorithm:

Algorithm 3.2.4 Solving in the case of simple roots.

Let $a \in \mathcal{A}$ such that $a(\zeta_i) \neq a(\zeta_j)$ for $i \neq j$ (which is generically the case) and $\mathtt{M}_a$ be the matrix of multiplication by a in the basis $\mathbf{x}^E = (1, x_1, \ldots, x_n, \ldots)$ of $\mathcal{A}$.

1. *Compute the eigenvectors $\Lambda = (\Lambda_1, \Lambda_{x_1}, \ldots, \Lambda_{x_n}, \ldots)$ of $\mathtt{M}_a^{\mathtt{t}}$.*
2. *For each eigenvector Λ with $\Lambda_1 \neq 0$, compute and output the point $\zeta = \left(\frac{\Lambda_{x_1}}{\Lambda_1}, \ldots, \frac{\Lambda_{x_n}}{\Lambda_1}\right)$.*

The set of output points ζ contains the simple roots (i.e. roots with multiplicity 1) of $f = 0$, since for such a root the eigenspace associated to the eigenvalue $a(\zeta)$ is one-dimensional and contains $\mathbf{1}_\zeta$. But as we will see in the next example, it can also yield in some cases the multiple roots.

Example 3.1.3 (continued). The eigenvalues, their multiplicities, and the corresponding normalized eigenvectors of the transpose of the matrix of multiplication by x_1 are:

```
> neigenvects(transpose(Mx1),1);
```

$$\left\{-\frac{1}{3}, 2, V_1 = \big(1, -\frac{1}{3}, \frac{5}{6}, -\frac{5}{18}\big)\right\} \quad , \quad \left\{\frac{1}{3}, 2, V_2 = \big(1, \frac{1}{3}, \frac{7}{6}, \frac{7}{18}\big)\right\}.$$

As the basis of $\mathcal{A}$ is $(1, x_1, x_2, x_1x_2)$, we deduce from Theorem 3.2.3 that the solutions of the system $f_1 = f_2 = 0$ can be read off from the 2^{nd} and the 3^{rd} coordinates of the normalized eigenvectors: So $\mathcal{Z}(I) = \{(-\frac{1}{3}, \frac{5}{6}), (\frac{1}{3}, \frac{7}{6})\}$. Moreover, the 4^{th} coordinates of V_1 and V_2 are the products of the 2^{nd} by the 3^{rd} coordinates. In this example the multiplicity 2 of the two eigenvalues is exactly the multiplicity of roots ζ_1 and ζ_2 (see Chapter 2, Proposition 2.1.14).

In order to compute exactly the set of roots counted with their multiplicity, we use the following result. It is based on the fact that commuting matrices share common eigenspaces and the decomposition (3.1) of the algebra $\mathcal{A}$.

Theorem 3.2.5. *[Mou98, MP00, CGT97] There exists a basis of $\mathcal{A}$ such that for all $a \in \mathcal{A}$, the matrix of M_a in this basis is of the form*

$$\mathtt{M}_a = \begin{pmatrix} \mathtt{N}_a^1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \mathtt{N}_a^d \end{pmatrix} \quad \text{with} \quad \mathtt{N}_a^i = \begin{pmatrix} a(\zeta_i) & & \star \\ & \ddots & \\ \mathbf{0} & & a(\zeta_i) \end{pmatrix}.$$

Proof. For every $i \in \{1, \ldots, d\}$, the multiplication operators in $\mathcal{A}_i$ by elements of $\mathcal{A}$ commute. Then using (3.1) it is possible to choose a basis of $\mathcal{A}_i$ such that the multiplication matrices $\mathtt{N}_a^i$ by $a \in \mathcal{A}$ in $\mathcal{A}_i$ in this basis are upper-triangular. By theorem 3.2.3, $\mathtt{N}_a^i$ has one eigenvalue, namely $a(\zeta_i)$.

We deduce the algorithm:

Algorithm 3.2.6 Solving by simultaneous triangulation.

INPUT: *Matrices of multiplication* $\mathtt{M}_{x_i}, i = 1, \ldots, n$, *in a basis of* $\mathcal{A}$.

1. *Compute a (Schur) decomposition* $\mathtt{P}$ *such that the matrices* $\mathtt{T}_i = \mathtt{P}\mathtt{M}_{x_i}\mathtt{P}^{-1}$, $i = 1, \ldots, n$, *are upper-triangular.*
2. *Compute and output the diagonal vectors* $\mathbf{t}_i = (t_{i,i}^1, \ldots, t_{i,i}^n)$ *of triangular matrices* $\mathtt{T}_k = (t_{i,j}^k)_{i,j}$.

OUTPUT: $\mathcal{Z}(I) = \{\mathbf{t}_i : i = 1, \ldots, \dim_{\mathbb{K}}(\mathcal{A})\}$.

The first step in this algorithm is performed by computing a Schur decomposition of M_l (where l is a generic linear form) which yields a change of basis matrix $\mathtt{P}$. Then we compute the triangular matrices $\mathtt{T}_i = \mathtt{P}\mathtt{M}_{x_i}\mathtt{P}^{-1}$, $i = 1, \ldots, n$, since they commute with M_l.

3.2.3 Chow form and rational univariate representation

In some problems it is important to have an exact representation of the roots of the system $f = 0$. We will represent these roots in terms of solutions of a univariate polynomial. More precisely, they will be the image of these solutions by a rational map. The aim of the foregoing developments is to show how to construct explicitly such a representation.

Definition 3.2.7. *The Chow form of the ideal* I *is the homogeneous polynomial in* $\mathbf{u} = (u_0, \ldots, u_n)$ *defined by*

$$\mathcal{C}_I(\mathbf{u}) = \det(u_0 + u_1 \mathtt{M}_{x_1} + \cdots + u_n \mathtt{M}_{x_n}) \in \mathbb{K}[\mathbf{u}].$$

According to Theorem 3.2.5, we have:

Proposition 3.2.8. *The Chow form*

$$\mathcal{C}_I(\mathbf{u}) = \prod_{\zeta \in \mathcal{Z}(I)} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{\mu_\zeta}.$$

Example 3.1.3 (continued). The Chow form of $I = (f_1, f_2)$ using the matrices of multiplication by x_1 and x_2 is:

```
> factor(det(u[0]+ u[1]*Mx1+ u[2]*Mx2));
```

$$\left(u_0 + \frac{1}{3}\,u_1 + \frac{7}{6}\,u_2\right)^2 \left(u_0 - \frac{1}{3}\,u_1 + \frac{5}{6}\,u_2\right)^2.$$

It is a product of linear forms whose coefficients yield the roots $\zeta_1 = (-\frac{1}{3}, \frac{5}{6})$ and $\zeta_2 = (\frac{1}{3}, \frac{7}{6})$ of $f_1 = f_2 = 0$. The exponents are the multiplicities of the roots (here 2). When the points of $\mathcal{Z}(I)$ are rational (as in this example) we can easily factorize $\mathcal{C}_I(\mathbf{u})$ as a product of linear forms and get the solutions of the system $f = 0$. But usually, this factorization is possible only on an algebraic extension of the field of coefficients (see Chapter 9 for more details on this task).

From the Chow form, it is possible to deduce a rational univariate representation of $\mathcal{Z}(I)$:

Theorem 3.2.9. *(see [Ren92, ABRW96, Rou99, EM99a, Lec00]) Let $\Delta(\mathbf{u})$ be a multiple of the Chow form $\mathcal{C}_I(\mathbf{u})$. For a generic vector $\mathbf{t} \in \mathbb{K}^{n+1}$ we write*

$$\frac{\Delta}{\gcd\left(\Delta, \frac{\partial \Delta}{\partial u_0}\right)}(\mathbf{t} + \mathbf{u}) = d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + R(u)\ ,$$

where $d_i(u_0) \in \mathbb{K}[u_0], R(u) \in (u_1, \ldots, u_n)^2$, $\gcd\big(d_0(u_0), {d_0}'(u_0)\big) = 1$. Then for all $\zeta \in \mathcal{Z}(I)$, there exists a root ζ_0 of $d_0(u_0)$ such that

$$\zeta = \left(\frac{d_1(\zeta_0)}{d_0'(\zeta_0)}, \ldots, \frac{d_n(\zeta_0)}{d_0'(\zeta_0)}\right).$$

Proof. We decompose $\Delta(\mathbf{u})$ as

$$\Delta(\mathbf{u}) = \left(\prod_{\zeta=(\zeta_1,\ldots,\zeta_n)\in\mathcal{Z}(I)} (u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n)^{n_\zeta}\right) H(\mathbf{u})\ ,$$

with $n_\zeta \in \mathbb{N}^*$, where $\prod_{\zeta\in\mathcal{Z}(I)}(u_0+\zeta_1 u_1+\cdots+\zeta_n u_n)^{n_\zeta}$ and $H(\mathbf{u})$ are relatively prime. Let

$$d(\mathbf{u}) = \frac{\Delta(\mathbf{u})}{\gcd\left(\Delta(\mathbf{u}), \frac{\partial \Delta}{\partial u_0}(\mathbf{u})\right)} = \left(\prod_{\zeta\in\mathcal{Z}(I)} (u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n)\right) h(\mathbf{u})\ ,$$

where $\prod_{\zeta\in\mathcal{Z}(I)}(u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n)$ and $h(\mathbf{u})$ are relatively prime. If $t = (t_1, \ldots, t_n) \in \mathbb{K}^n$ and $\mathbf{t} = (0, t_1, \ldots, t_n) \in \mathbb{K}^{n+1}$, we have

$$\begin{aligned} d(\mathbf{t} + \mathbf{u}) &= \left(\prod_{\zeta\in\mathcal{Z}(I)} \big((t, \zeta) + u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n\big)\right) h(\mathbf{t} + \mathbf{u}) \\ &= d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + r(\mathbf{u})\ , \end{aligned}$$

with $(t,\zeta) = t_1\zeta_1 + \cdots + t_n\zeta_n$, $d_0, \ldots, d_n \in \mathbb{K}[u_0]$, $r(\mathbf{u}) \in (u_1, \ldots, u_n)^2$, and

$$h(\mathbf{t}+\mathbf{u}) = h_0(u_0) + u_1 h_1(u_0) + \cdots + u_n h_n(u_0) + s(\mathbf{u}) \ ,$$

with $h_0, \ldots, h_n \in \mathbb{K}[u_0]$ and $s(\mathbf{u}) \in (u_1, \ldots, u_n)^2$. By identification

$$d_0(u_0) = \Big(\prod_{\zeta \in \mathcal{Z}(I)} \big((t,\zeta) + u_0\big) \Big) h_0(u_0) \quad , \qquad \text{and for i} = 1, \ldots, \text{n},$$

$$d_i(u_0) = \Big(\sum_{\zeta \in \mathcal{Z}(I)} \zeta_i \prod_{\xi \neq \zeta} \big((t,\xi) + u_0\big) \Big) h_0(u_0) + \Big(\prod_{\zeta \in \mathcal{Z}(I)} \big((t,\zeta) + u_0\big) \Big) h_i(u_0).$$

If $t \in \mathbb{K}^n$ is generic, $\prod_{\zeta \in \mathcal{Z}(I)} \big((t,\zeta) + u_0\big)$ and $h_0(u_0)$ are relatively prime. Let $\zeta_0 = -(t,\zeta)$ be a root of $d_0(u_0)$, then $h_0(\zeta_0) \neq 0$ and

$$d_0{}'(\zeta_0) = \Big(\prod_{\xi \neq \zeta} \big((t,\xi) - (t,\zeta)\big) \Big) h_0(\zeta_0) \quad ,$$

$$d_i(\zeta_0) = \zeta_i \Big(\prod_{\xi \neq \zeta} \big((t,\xi) - (t,\zeta)\big) \Big) h_0(\zeta_0) \qquad , \text{for} \quad i = 1, \ldots, n.$$

Moreover we can assume that the generic vector t is such that $(t,\zeta) \neq (t,\xi)$ for $(\zeta,\xi) \in \mathcal{Z}(I)^2$ and $\zeta \neq \xi$. Then

$$\zeta_i = \frac{d_i(\zeta_0)}{d_0{}'(\zeta_0)}, \qquad \text{for } i = 1, \ldots, n.$$

This result describes the coordinates of solutions of $f = 0$ as the image by a rational map of some roots of $d_0(u_0)$. It does not imply that any root of $d_0(u_0)$ yields a point in $\mathcal{Z}(I)$, so that this representation may be redundant. However the "bad" prime factors in $d_0(u_0)$ can be removed by substituting the rational representation back into the equations $f_1, \ldots, f_m$.

In Proposition 3.5.4 we will see how to obtain a multiple of $\mathcal{C}_I(\mathbf{u})$ without the knowledge of a basis of $\mathcal{A}$.

Algorithm 3.2.10 RATIONAL UNIVARIATE REPRESENTATION.

INPUT: *A* multiple $\Delta(\mathbf{u})$ *of the Chow form of the ideal* $I = (f_1, \ldots, f_m)$.

1. *Compute the square-free part* $d(\mathbf{u})$ *of* $\Delta(\mathbf{u})$.
2. *Choose a generic* $t \in \mathbb{K}^n$ *and compute the first terms of*

$$d(\mathbf{t} + \mathbf{u}) = d_0(u_0) + u_1\, d_1(u_0) + \cdots + u_n\, d_n(u_0) + \cdots$$

3. *Compute the redundant rational representation*

$$d_0(u_0) = 0 \quad , \quad \Big(\frac{d_1(u_0)}{{d_0}'(u_0)}, \ldots, \frac{d_n(u_0)}{{d_0}'(u_0)}\Big).$$

4. *Factorize* $d_0(u_0)$*, keep the "good" prime factors and output the rational univariate representation of* $\mathcal{Z}(I)$.

Example 3.1.3 (continued). From the Chow form, we deduce the univariate representation of $\mathcal{Z}(I)$:

$$\left(u_0 + \frac{3}{2}\right)\left(u_0 + \frac{1}{2}\right) = 0 \quad , \quad \zeta(u_0) = \left(-\frac{1}{6\,(1+u_0)},\ \frac{11 + 12\,u_0}{12\,(1+u_0)}\right).$$

This gives the solutions

$$u_0 = -\tfrac{3}{2}, \zeta_1 = \zeta(-\tfrac{3}{2}) = \big(\tfrac{1}{3}, \tfrac{7}{6}\big) \ \text{ and } \ u_0 = -\tfrac{1}{2}, \zeta_2 = \zeta(-\tfrac{1}{2}) = \big(-\tfrac{1}{3}, \tfrac{5}{6}\big)$$

of $f_1 = f_2 = 0$.

3.2.4 Real roots

Now we assume that the polynomials $f_1, \ldots, f_m$ have real coefficients: $\mathbb{K} = \mathbb{R}$. A natural question which arises in many practical problems is *how many real solutions does the system* $f = 0$ *have ?* We will use properties of the linear form trace to answer this question.

Definition 3.2.11. *The linear form trace, denoted by* Tr*, is defined by*

$$\begin{aligned} \mathrm{Tr} : \mathcal{A} &\to \mathbb{R} \\ a &\mapsto \mathrm{Tr}(a) := tr(M_a), \end{aligned}$$

where $tr(M_a)$ *is the trace of the linear operator* M_a.

According to Theorem 3.2.5, we have

$$\mathrm{Tr} = \sum_{\zeta \in \mathcal{Z}(I)} \mu_\zeta\, \mathbf{1}_\zeta.$$

We associate to Tr and to any $h \in \mathcal{A}$ the *quadratic form*:

$$Q_h : (a,b) \in \mathcal{A} \times \mathcal{A} \mapsto Q_h(a,b) := \mathrm{Tr}(hab) \in \mathbb{R},$$

which gives the following generalization of a result due to Hermite for counting the number of real roots.

Theorem 3.2.12. *(See [PRS93, GVRR99]) Let $h \in \mathbb{R}[\mathbf{x}]$. We have:*

1. *The rank of the quadratic form Q_h is the number of distinct complex roots ζ of $f = 0$ such that $h(\zeta) \neq 0$.*
2. *The signature of Q_h is equal to*

$\#\{\zeta \in \mathbb{R}^n : f_1(\zeta) = \cdots = f_m(\zeta) = 0, h(\zeta) > 0\} - \#\{\zeta \in \mathbb{R}^n : f_1(\zeta) = \cdots = f_m(\zeta) = 0, h(\zeta) < 0\}$, where # denotes the cardinality of a set.

In particular, if $h = 1$, the rank of Q_1 is the number of distinct complex roots of $f = 0$ and its signature is the number of real roots of this system. This allows us to analyze the geometry of the real roots as illustrated in the following example:

Example 3.1.3 (continued). By direct computations, we have

$$\mathrm{Tr}(1) = 4\ ,\ \mathrm{Tr}(x_1) = 0\ ,\ \mathrm{Tr}(x_2) = 4\ ,\ \mathrm{Tr}(x_1x_2) = \frac{2}{9}.$$

We deduce the value of the linear form Tr on the other interesting monomials by using the transpose operators $\mathtt{M}^{\mathtt{t}}_{x_i}$ as follows:

```
> T0  := evalm([4,0,4,2/9]):
> T1  := evalm(transpose(Mx1)&*T0):  T2:= evalm(transpose(Mx2)&*T0):
> T11 := evalm(transpose(Mx1)&*T1): T12:= evalm(transpose(Mx2)&*T1):
> T112:= evalm(transpose(Mx2)&*T11):
> Q1  := matrix(4,4,[T0,T1,T2,T12]);
> Qx1 := matrix(4,4,[T1,T11,T12,T112]);
```

So we obtain

$$Q_1 = \begin{pmatrix} 4 & 0 & 4 & \frac{2}{9} \\ 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ 4 & \frac{2}{9} & \frac{37}{9} & \frac{4}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \end{pmatrix},\quad Q_{x_1} = \begin{pmatrix} 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ \frac{4}{9} & 0 & \frac{4}{9} & \frac{2}{81} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \\ \frac{4}{9} & \frac{2}{81} & \frac{37}{81} & \frac{4}{81} \end{pmatrix}.$$

The rank and the signatures of the quadratic forms Q_1 and Q_{x_1} are

```
> rank(Q1), signature(Q1), rank(Qx1), signature(Qx1);
```

$$2\ ,\quad (2,0)\ ,\quad 2\ ,\quad (1,1)\ ,$$

which tells us (without computing these roots) that there are 2 real roots, one with $x_1 < 0$ and another with $x_1 > 0$.

3.3 Duality

In this section $m = n$. Let us define the notion of Bezoutian matrix that will be useful in the following.

Definition 3.3.1. The Bezoutian $\Theta_{f_0,\ldots,f_n}$ of $f_0, \ldots, f_n \in R$ is the polynomial

$$\Theta_{f_0,\ldots,f_n}(\mathbf{x},\mathbf{y}) = \begin{vmatrix} f_0(\mathbf{x}) & \theta_1(f_0)(\mathbf{x},\mathbf{y}) & \cdots & \theta_n(f_0)(\mathbf{x},\mathbf{y}) \\ \vdots & \vdots & \vdots & \vdots \\ f_n(\mathbf{x}) & \theta_1(f_n)(\mathbf{x},\mathbf{y}) & \cdots & \theta_n(f_n)(\mathbf{x},\mathbf{y}) \end{vmatrix} \in \mathbb{K}[\mathbf{x},\mathbf{y}],$$

where

$$\theta_i(f_j)(\mathbf{x},\mathbf{y}) = \frac{f_j(y_1,\ldots,y_{i-1},x_i,\ldots,x_n) - f_j(y_1,\ldots,y_i,x_{i+1},\ldots,x_n)}{x_i - y_i}.$$

Set $\Theta_{f_0,\ldots,f_n}(\mathbf{x},\mathbf{y}) = \sum_{\alpha,\beta} a_{\alpha,\beta}\mathbf{x}^\alpha\mathbf{y}^\beta$ with $a_{\alpha,\beta} \in \mathbb{K}$, we order the monomials $\mathbf{x}^\alpha\mathbf{y}^\beta$, then the matrix $B_{f_0,\ldots,f_n} := (a_{\alpha,\beta})_{\alpha,\beta}$ is called the Bezoutian matrix of $f_0, \ldots, f_n$.

The Bezoutian was initially used by E. Bézout to construct the resultant of two polynomials in one variable [Béz64].

When f_0 is the constant 1 and f is the polynomial map $(f_1, \ldots, f_n)$, the Bezoutian $\Theta_{1,f_1,\ldots,f_n}$ will be denoted by Δ_f.

We will define the residue τ_f associated to $f = (f_1, \ldots, f_n)$ and we will give some of its important properties (for more details see [SS75], [Kun86], [EM96], [BCRS96], also Chapter 1 of this book).

The dual $\widehat{\mathcal{A}}$ of the vector space $\mathcal{A}$ has a natural structure of $\mathcal{A}$-module: If $(a, \Lambda) \in \mathcal{A} \times \widehat{\mathcal{A}}$, the linear form $a.\Lambda : b \in \mathcal{A} \mapsto (a.\Lambda)(b) := \Lambda(ab)$.

Definition 3.3.2. *The finite $\mathbb{K}$-algebra $\mathcal{A}$ is called Gorenstein if the $\mathcal{A}$-modules $\widehat{\mathcal{A}}$ and $\mathcal{A}$ are isomorphic.*

Set $\Delta_f = \sum_{\alpha,\beta} a_{\alpha,\beta}\ \mathbf{x}^\alpha\mathbf{y}^\beta$ with $a_{\alpha,\beta} \in \mathbb{K}$, we define the linear map

$$\begin{aligned} {\Delta_f}^\triangleright : \widehat{R} &\to R \\ \Lambda &\mapsto {\Delta_f}^\triangleright(\Lambda) := \sum_\alpha \left(\sum_\beta\ a_{\alpha,\beta}\ \Lambda(\mathbf{y}^\beta) \right) \mathbf{x}^\alpha. \end{aligned}$$

This map induces naturally a linear one also denoted by ${\Delta_f}^\triangleright : \widehat{\mathcal{A}} \to \mathcal{A}$. Since the number of polynomials m is equal to the number n of variables and the affine variety $\mathcal{Z}(I)$ is finite, one can prove that ${\Delta_f}^\triangleright$ is an isomorphism of $\mathcal{A}$-modules (see [SS75], [Kun86], [EM96], [BCRS96]). Then $\mathcal{A}$ is a Gorenstein algebra. Thus we can state the following definition:

Definition 3.3.3. The residue τ_f of $f = (f_1, \ldots, f_n)$ is the linear form on R such that

1. $\tau_f(h) = 0, \forall\, h \in I$,
2. $\Delta_f{}^{\triangleright}(\tau_f) - 1 \in I$.

In the univariate case, let $f = f_d\, x^d + \cdots + f_0$ be a polynomial of degree d. For $h \in R$ let $r = r_{d-1}x^{d-1} + \cdots + r_0$ be the remainder in the Euclidean division of h by f, then

$$\tau_f(h) = \frac{r_{d-1}}{f_d}. \tag{3.2}$$

In the multivariate case, if for each $i = 1, \ldots, n$, f_i depends only on x_i, then

$$\tau_f(x_1^{\alpha_1} \ldots x_n^{\alpha_n}) = \tau_{f_1}(x_1^{\alpha_1}) \ldots \tau_{f_n}(x_n^{\alpha_n}). \tag{3.3}$$

If the roots of $f_1 = \cdots = f_n = 0$ are simple (this is equivalent to the fact that the Jacobian of f, denoted by $\mathrm{Jac}(f)$, does not vanish on $\mathcal{Z}(I)\big)$, then $\tau_f = \sum_{\zeta \in \mathcal{Z}(I)} \frac{\mathbf{1}_\zeta}{\mathrm{Jac}(f)(\zeta)}$.

But in the general multivariate setting the situation is more complicated. We will show how to compute effectively τ_f for an arbitrary map f.

An important tool in the duality theory is the transformation law.

Proposition 3.3.4. *(Classical transformation law)*

Let $g = (g_1, \ldots, g_n)$ be another polynomial map such that the variety defined by $g_1, \ldots, g_n$ is finite and

$$\forall\, i = 1, \ldots, n \quad , \quad g_i = \sum_{j=1}^{n} a_{i,j} f_j \quad \text{with} \quad a_{i,j} \in \mathbb{K}[x].$$

Then $\tau_f = \det(a_{i,j}) \cdot \tau_g$.

Proposition 3.3.5. *(Generalized transformation law [BY99, EM96]).*

Let $(f_0, \ldots, f_n)$ and $(g_0, \ldots, g_n)$ be two maps of $\mathbb{K}[x_0, \mathbf{x}] = \mathbb{K}[x_0, x_1, \ldots, x_n]$ which define finite affine varieties. We assume that $f_0 = g_0$ and there are positive integers m_i and polynomials $a_{i,j}$ such that

$$\forall\, i = 1, \ldots, n \quad , \quad f_0^{m_i} g_i = \sum_{j=1}^{n} a_{i,j} f_j.$$

Then $\tau_{(f_0,\ldots,f_n)} = \det(a_{i,j}) \cdot \tau_{(g_0^{m_1+\cdots+m_n+1}, g_1 \ldots, g_n)}$.

If $f_0 = x_0$ and $m_1 = \cdots = m_n = 0$, the generalized transformation law reduces to the classical one.

Another important fact in this theory is the following formula:

$$\mathrm{Jac}(f) \cdot \tau_f = \mathrm{Tr}\ , \tag{3.4}$$

where $\mathrm{Tr} : a \in R \mapsto \mathrm{Tr}(a) \in \mathbb{K}$ ($\mathrm{Tr}(a)$ is the trace of the endomorphism of multiplication by a in the vector space $\mathcal{A}$). If the characteristic of $\mathbb{K}$ is 0, we deduce from this formula that $\dim_{\mathbb{K}}(\mathcal{A}) = \tau_f\big(\mathrm{Jac}(f)\big)$.

3.3.1 Residue calculus

The effective construction of the residue of the polynomial map $f = (f_1, \ldots, f_n)$ is based on the computation of algebraic relations between $f_1, \ldots, f_n$ and the coordinate functions x_i (see also Section 1.5.4 of Chapter 1). We give here a method using Bezoutian matrices to get them.

Let $f_0, \ldots, f_n$ be $n+1$ elements of R such that the n polynomials $f_1, \ldots, f_n$ are algebraically independent over $\mathbb{K}$. For algebraic dimension reasons there is a nonzero polynomial P such that $P(f_0, \ldots, f_n) = 0$. We will show how to find such a P by means of the Bezoutian matrix.

Proposition 3.3.6. *(see [EM00]) Let $u = (u_0, \ldots, u_n)$ be new parameters. Then every nonzero maximal minor $P(u_0, \ldots, u_n)$ of the Bezoutian matrix of the elements $f_0 - u_0, \ldots, f_n - u_n$ in $\mathbb{K}[u_0, \ldots, u_n][\mathbf{x}]$ satisfies the identity $P(f_0, \ldots, f_n) = 0$.*

This proposition comes from the fact that we can write the Bezoutian matrix of $f_0 - u_0, \ldots, f_n - u_n$ (up to invertible matrices with coefficients in $\mathbb{K}(u_1, \ldots, u_n)$) as

$$\left(\begin{array}{c|c} \mathtt{M}_{f_0} - u_0\mathbb{I} & \mathbf{0} \\ \hline \mathbf{0} & * \end{array}\right) \tag{3.5}$$

where $\mathbb{I}$ is the identity matrix, $\mathtt{M}_{f_0}$ is the matrix of multiplication by f_0 in the vector space $\mathbb{K}(u_1, \ldots, u_n)[\mathbf{x}]/(f_1 - u_1, \ldots, f_n - u_n)$. By Cayley-Hamilton's theorem every maximal minor of this Bezoutian matrix gives an algebraic relation between $f_0, \ldots, f_n$ (for more details see [EM00]).

In practice, we use a fraction free Gaussian elimination (Bareiss method) in order to find a nonzero maximal minor of the Bezoutian matrix (see the implementation of the function `melim` in the MULTIRES package).

We will see now how to compute effectively the residue τ_f.

Proposition 3.3.7. *For $i \in \{1, \ldots, n\}$, let*

$$P_i(u_0, \ldots, u_n) = a_{i,0}(u_1, \ldots, u_n)\, u_0^{m_i} + \cdots + a_{i,m_i}(u_1, \ldots, u_n)$$

be an algebraic relation between $x_i, f_1, \ldots, f_n$. If for each i there is $k_i \in \{0, \ldots, m_i - 1\}$ such that $a_{i,k_i}(0) \neq 0$, then for $h \in R$ the computation of the multivariate residue $\tau_f(h)$ reduces to univariate residue calculus.

Proof. If $j_i = \min\{k : a_{i,k}(0) \neq 0\}$, we have

$$g_i(x_i) = a_{i,j_i}(0)x_i^{m_i - j_i} + \cdots + a_{i,m_i}(0) = \sum_{j=1}^{n} A_{i,j} f_j \ , \quad A_{i,j} \in \mathbb{K}[x].$$

By the transformation law and (3.3) there are scalars c_α such that

$$\tau_f(h) = \tau_{(g_1,\dots,g_n)}\big(h\det(A_{i,j})\big) = \sum_{\alpha=(\alpha_1,\dots,\alpha_n)} c_\alpha\ \tau_{g_1}(x_1^{\alpha_1})\dots\tau_{g_n}(x_n^{\alpha_n}).$$

If w are formal parameters, similarly for every $h \in R$, $\tau_{f-w}(h)$ is a rational function in w whose denominator is the product of powers of $a_{1,0}(w),\dots,a_{n,0}(w)$. But it is not clear how to recover $\tau_f(h)$ from this function. For an arbitrary map f, $\tau_f(h)$ can be computed using the generalized transformation law.

For $(\alpha_1,\dots,\alpha_n) \in \mathbb{K}^n$ and a new variable x_0, we define the multi-index $m = (m_1,\dots,m_n)$ and the polynomials R_i, S_i as follows: If $P_i(u_0,\dots,u_n)$ is an algebraic relation between $x_i, f_1,\dots,f_n$, then there are $B_{i,j} \in \mathbb{K}[x_0,\dots,x_n]$ such that

$$P_i(x_i,\alpha_1x_0,\dots,\alpha_nx_0) = \sum_{j=1}^{n}(f_j-\alpha_jx_0)B_{i,j} \tag{3.6}$$

$$= x_0^{m_i}\big(R_i(x_i) - x_0S_i(x_i,x_0)\big). \tag{3.7}$$

From the transformation laws we deduce the following result:

Proposition 3.3.8. *If for each $i = 1\dots n$, the univariate polynomial R_i does not vanish identically, then for $h \in R$ we have*

$$\tau_f(h) = \sum_{k\in\mathbb{N}^n:|k|\le|m|} \tau_{(x_0^{|m|+1-|k|},R_1^{k_1+1},\dots,R_n^{k_n+1})}\big(S_1^{k_1}\dots S_n^{k_n}\,h\det(B_{i,j})\big).$$

Proof. From (3.6) and Proposition 3.3.5, we have

$$\tau_f(h) = \tau_{(x_0,f_1-\alpha_1x_0,\dots,f_n-\alpha_nx_0)}(h) = \tau_{(x_0^{|m|+1},R_1-x_0S_1,\dots,R_n-x_0S_n)}\big(h\det(B_{i,j})\big).$$

Using the identities

$$R_i^{|m|+1} - (x_0S_i)^{|m|+1} = (R_i-x_0S_i)\sum_{k_i=0}^{|m|} R_i^{|m|-k_i}(x_0S_i)^{k_i}, i = 1\dots n,$$

and Proposition 3.3.4 we deduce the formula in Proposition 3.3.8.

Propositions 3.3.6 and 3.3.8 give an effective algorithm to compute the residue of a map in the multivariate setting. They reduce the multivariate residue calculus to the univariate one.

We will show how to use the residue for solving polynomial systems. Let $\zeta_1,\dots,\zeta_D$ be the solutions of the system $f = 0$ (each solution appears as many times as its multiplicity). Let us fix $i \in \{1,\dots,n\}$. Using formula (3.4) and Theorem 3.2.5, we can compute the Newton sums

$$S_j = \tau_f\big(x_i{}^j \mathrm{Jac}(f)\big) = \mathrm{Tr}(x_i{}^j) = \zeta_{1,i}{}^j + \cdots + \zeta_{D,i}{}^j,$$

where $\zeta_{1,i}, \ldots, \zeta_{D,i}$ are the i-th coordinates of $\zeta_1, \ldots, \zeta_D$. If $\sigma_1, \ldots, \sigma_D$ are the elementary symmetric functions of $\zeta_{1,i}, \ldots, \zeta_{D,i}$ (i.e. $\sigma_j = \sum_{1 \le i_1 < \cdots < i_j \le D} \zeta_{1,i_1} \ldots \zeta_{D,i_j}$), we can obtain the univariate polynomial

$$A_i(T) = (T - \zeta_{1,i}) \ldots (T - \zeta_{D,i}) = T^D + \sigma_1 T^{D-1} + \cdots + \sigma_D$$

by means of the Newton identities:

$$k\sigma_k = -S_k - \sigma_1 S_{k-1} - \cdots - \sigma_{k-1} S_1 \ , \ 1 \le k \le D. \tag{3.8}$$

The residue τ_f allows us to find the univariate polynomials $A_i(T), 1 \le i \le n$, and then to deduce the i-th coordinates of the roots of the system $f_1 = \cdots = f_n = 0$.

For other applications of residue theory see [EM98, EM].

3.4 Resultant constructions

Projection is one of the most used operations in effective algebraic geometry [Eis95, CLO98]. It reduces the dimension of the problem that we have to solve and often simplifies it. The resultant is a tool to perform such a projection and has many applications in this domain. It leads to efficient methods for solving polynomial equations based on matrix formulations [EM99b]. We present here different notions of resultants (see also Chapter 1).

We recall that a resultant of a polynomial system $\mathbf{f_c}$ on a complete variety X is a polynomial $\mathrm{Res}_X(\mathbf{f_c})$ on the coefficients $\mathbf{c}$ of this system (considered as variables) such that the vanishing of $\mathrm{Res}_X(\mathbf{f_c})$ is a necessary and sufficient condition for $\mathbf{f_c}$ to have a solution in the variety X. The best known formulation of the resultant is in the case of two univariate polynomials. It is given by the Sylvester matrix. Another classical one is the projective resultant of n homogeneous polynomials in n variables. It can be computed using Macaulay matrices (see Chapter 2, Section 2.3, or [DD01]). Recently a refined notion of resultants (on toric varieties) has been studied. It takes into account the actual monomials appearing in the polynomials. Its construction follows the same process as in the projective case except that the notion of degree is replaced by the support of a polynomial (for more details see Chapter 7). Here we will focus on an even more recent generalization of these resultant notions.

3.4.1 Resultant over a unirational variety

A natural extension of the toric resultant is to replace the monomial parameterization by a rational one. The polynomial system $\mathbf{f_c}$ is defined on an open subset of $\mathbb{K}^n$ and is of the form

$$\mathbf{f_c} := \begin{cases} f_0(\mathbf{t}) = \sum_{j=0}^{k_0} c_{0,j}\, \kappa_{0,j}(\mathbf{t}) \\ \quad\vdots \\ f_n(\mathbf{t}) = \sum_{j=0}^{k_n} c_{n,j}\, \kappa_{n,j}(\mathbf{t}) \end{cases} \tag{3.9}$$

where $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{K}^n$ and the $\kappa_{i,j}$ are nonzero rational functions, which we can assume to be polynomials by reduction to the same denominator.

Let $\mathcal{K}_i = (\kappa_{i,j})_{j=0,\ldots,k_i}$ and U be the open subset of $\mathbb{K}^n$ such that $\mathcal{K}_i(\mathbf{t}) \neq 0$ on U for $i = 0, \ldots, n$. Assume that there exists $\sigma_0, \ldots, \sigma_N \in R$ defining a map

$$\begin{aligned} \sigma : U &\to \mathbb{P}^N \\ \mathbf{t} &\mapsto \big(\sigma_0(\mathbf{t}) : \cdots : \sigma_N(\mathbf{t})\big), \end{aligned}$$

and homogeneous polynomials $\psi_{i,j}(x_0, \ldots, x_N)$, $i = 0, \ldots, n$, $j = 0, \ldots, k_i$, satisfying

$$\kappa_{i,j}(\mathbf{t}) = \psi_{i,j}\big(\sigma_0(\mathbf{t}), \ldots, \sigma_N(\mathbf{t})\big) \text{ and } \deg(\psi_{i,j}) = \deg(\psi_{i,0}) \geq 1.$$

Let X^o be the image of σ and X be its closure in $\mathbb{P}^N$. In order to construct the resultant associated to the system (3.9) on the variety X we assume the following conditions (**D**):

$$\begin{cases} (\mathbf{D1}) \text{ The Jacobian matrix of } \sigma = (\sigma_i)_{i=0,\ldots,N} \text{ is of rank } n \text{ at one point of } U, \\ (\mathbf{D2}) \text{ For generic } \mathbf{c},\ f_1 = \cdots = f_n = 0 \text{ has a finite number of solutions in } U. \end{cases}$$

We will show that these conditions are sufficient to define the resultant. Let $U^o = \{\mathbf{t} \in U : \kappa_{i,0}(\mathbf{t}) \neq 0 \text{ for } i = 0, \ldots, n\}$ be the dense open subset of U and consider the parameterization

$$\begin{aligned} \tau : \mathbb{P}^{k_0-1} \times \cdots \times \mathbb{P}^{k_n-1} \times U^o &\to \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n} \times \mathbb{P}^N \\ (\tilde{\mathbf{c}}_0, \ldots, \tilde{\mathbf{c}}_n, \mathbf{t}) &\mapsto \big(\mathbf{c}_0, \ldots, \mathbf{c}_n, \sigma(\mathbf{t})\big) \end{aligned}$$

with $\mathbf{c}_i = (c_{i,0}, \tilde{\mathbf{c}}_i)$ and $c_{i,0} = -\frac{1}{\kappa_{i,0}(\mathbf{t})} \sum_{j=1}^{k_i} c_{i,j}\kappa_{i,j}(\mathbf{t})$. We denote by W^o the image of τ, W its closure in $\mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n} \times \mathbb{P}^N$, $\pi_1 : \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n} \times \mathbb{P}^N \to \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n}$, and $\pi_2 : \mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n} \times \mathbb{P}^N \to \mathbb{P}^N$ the canonical projections.

Theorem 3.4.1. *Under the conditions* **(D)**, *the variety W is irreducible and projects onto a hypersurface $Z = \pi_1(W)$. Moreover if $\mathrm{Res}_X(\mathbf{f_c})$ is one equation of Z, for any specialization of the parameters $\mathbf{c} = (c_{i,j})$, $\mathrm{Res}_X(\mathbf{f_c}) = 0$ if and only if there exists $(\mathbf{c}, x) \in W$ such that $\tilde{f}_i(x) := \sum_{j=0}^{k_i} c_{i,j}\, \psi_{i,j}(x) = 0$ for $i = 0, \ldots, n$.*

Proof. The variety W is the closure of a parameterized variety, so it is irreducible and its projection Z is also irreducible.

According to **(D1)**, the Jacobian of σ is of rank n on an open subset of U. This implies that the dimension of the variety X is n. The fibers of the projection $\pi_2 : W^o \to X^o$ are linear spaces of dimension $\sum_{i=0}^{n} k_i - n - 1$, for

we have $\mathcal{K}_i(\mathbf{t}) \neq 0$ when $\mathbf{t} \in U$. By the fiber theorem ([Sha77] or [Har95]), we deduce that W is of dimension $\sum_{i=0}^{n} k_i - 1$.

Consider now the restriction of π_1 to W^o. According to **(D2)**, there exists an open subset of $\mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n}$ on which the number of solutions of the system $f_1 = \cdots = f_n = 0$ is finite. The fibers of π_1 on this open subset is therefore of dimension 0. This shows that the projection $\pi_1(W^o)$, and thus Z, is of the same dimension as W, that is a hypersurface of $\mathbb{P}^{k_0} \times \cdots \times \mathbb{P}^{k_n}$ defined (up to a scalar) by one equation $\mathrm{Res}_X(\mathbf{f_c})$.

As the fibers of π_2 above X^o are of dimension $\sum_{i=0}^{n} k_i - n - 1$ and W is of dimension $\sum_{i=0}^{n} k_i - 1$, $\pi_2(W)$ is an irreducible variety of dimension n containing X^o. This shows that $X = \pi_2(W)$. Consequently for a specialization of the coefficients $\mathbf{c}$, $\mathrm{Res}_X(\mathbf{f_c}) = 0$ iff there exists $x \in X$ such that $(\mathbf{c}, x) \in W$, i.e. $\tilde{f}_i(x) = 0$ for $i = 0, \ldots, n$.

The degree of the resultant $\mathrm{Res}_X(\mathbf{f_c})$ in the coefficients $c_{i,j}$ of f_i is bounded by (but not necessarily equal to) the generic number of points of $V_i = \mathcal{Z}(\tilde{f}_0, \ldots, \tilde{f}_{i-1}, \tilde{f}_{i+1}, \ldots, \tilde{f}_n) \cap X$. In the case where the linear forms $\tilde{f}_i(\zeta)$, $\zeta \in V_i$, in $c_{i,j}$, are all distinct, the degree of $\mathrm{Res}_X(\mathbf{f_c})$ in the coefficients of f_i is exactly the number of generic roots of V_i. This is the case when $t_1, \ldots, t_n$ appear among the $\kappa_{i,j}, j = 0, \ldots, k_i$, as it is illustrated below.

We can compute a non-trivial multiple of $\mathrm{Res}_X(\mathbf{f_c})$ using the Bezoutian matrix.

Theorem 3.4.2. *Assume that the conditions* **(D)** *are satisfied. Then any maximal minor of the Bezoutian matrix* $B_{f_0,\ldots,f_n}$ *is divisible by* $\mathrm{Res}_X(\mathbf{f_c})$.

This theorem is a consequence of hypotheses **(D)** and the fact that if the variety defined by $f_1, \ldots, f_n$ is finite then the Bezoutian of $f_0, \ldots, f_n$ admits a block decomposition of the form (3.5), for more details see [BEM00].

Example 3.4.3. Consider the three following polynomials:

$$\begin{cases} f_0 = c_{0,0} + c_{0,1}t_1 + c_{0,2}t_2 + c_{0,3}({t_1}^2 + {t_2}^2) \\ f_1 = c_{1,0} + c_{1,1}t_1 + c_{1,2}t_2 + c_{1,3}({t_1}^2 + {t_2}^2) + c_{1,4}({t_1}^2 + {t_2}^2)^2 \\ f_2 = c_{2,0} + c_{2,1}t_1 + c_{2,2}t_2 + c_{2,3}({t_1}^2 + {t_2}^2) + c_{2,4}({t_1}^2 + {t_2}^2)^2. \end{cases}$$

We are looking for conditions on the coefficients $c_{i,j}$ such that these three elements have a common "root". The projective resultant of these polynomials in $\mathbb{P}^2$ is zero (for all the values of parameters $c_{i,j}$), because the corresponding homogenized polynomials vanish at the points $(0 : 1 : \mathbf{i})$ and $(0 : 1 : -\mathbf{i})$). The toric resultant also vanishes (these polynomials have common roots in the associated toric variety). Now we consider the map

$$\begin{aligned} \sigma : \mathbb{K}^2 &\to \mathbb{P}^3 \\ (t_1, t_2) &\mapsto (1 : t_1 : t_2 : t_1^2 + t_2^2). \end{aligned}$$

The rank of the Jacobian matrix of σ is 2 and

$$\psi_0 = (x_0, x_1, x_2, x_3) \quad , \quad \psi_1 = \psi_2 = (x_0^2, x_0x_1, x_0x_2, x_0x_3, x_3^2) \quad ,$$

where $(x_0 : x_1 : x_2 : x_3)$ are the homogeneous coordinates in $\mathbb{P}^3$. We have $f_i = \sum c_{i,j}\psi_{i,j} \circ \sigma$ for $i = 0, 1, 2$. For generic values of the coefficients $c_{i,j}$, the system $f_1 = f_2 = 0$ has a finite number of solutions in $\mathbb{K}^2$. By Theorem 3.4.2, any nonzero maximal minor of B_{f_0,f_1,f_2} is divisible by $\mathrm{Res}_X(f_0, f_1, f_2)$.

```
> mbezout([f1,f2,f3],[t1,t2]);
```

The Bezoutian matrix of f_1, f_2, f_3 is of size 12×12 and has rank 10. A maximal minor is a huge polynomial in $(c_{i,j})$ containing 207805 monomials. It can be factored as $q_1q_2(q_3)^2\rho$, with

$$\begin{aligned}
q_1 &= -c_{0,2}c_{1,3}c_{2,4} + c_{0,2}c_{1,4}c_{2,3} + c_{1,2}c_{0,3}c_{2,4} - c_{2,2}c_{0,3}c_{1,4}\\
q_2 &= c_{0,1}c_{1,3}c_{2,4} - c_{0,1}c_{1,4}c_{2,3} - c_{1,1}c_{0,3}c_{2,4} + c_{2,1}c_{0,3}c_{1,4}\\
q_3 &= {c_{0,3}}^2{c_{1,1}}^2{c_{2,4}}^2 - 2{c_{0,3}}^2c_{1,1}c_{2,1}c_{2,4}c_{1,4} + {c_{0,3}}^2{c_{2,4}}^2{c_{1,2}}^2 + \cdots\\
\rho &= {c_{2,0}}^4{c_{1,4}}^4{c_{0,2}}^4 + {c_{2,0}}^4c_{1,4}{}^4{c_{0,1}}^4 + {c_{1,0}}^4{c_{2,4}}^4{c_{0,2}}^4 + {c_{1,0}}^4{c_{2,4}}^4{c_{0,1}}^4 + \cdots
\end{aligned}$$

The polynomials q_3 and ρ contain respectively 20 and 2495 monomials. As for generic equations f_0, f_1, f_2, the number of points in the varieties $\mathcal{Z}(f_0, f_1)$, $\mathcal{Z}(f_0, f_2)$, $\mathcal{Z}(f_1, f_2)$ is 4 (see for instance [Mou96]), the resultant $\mathrm{Res}_X(f_0, f_1, f_2)$ is homogeneous of degree 4 in the coefficients of each f_i. Thus, $\mathrm{Res}_X(f_0, f_1, f_2)$ is equal to the factor ρ.

3.4.2 Residual resultant

In practical situations the equations have common zeroes which are independent of the parameters of the problem. These "degenerate" zeroes are not interesting for the resolution of this problem. We present here a resultant construction which allows us to remove these degenerate solutions when they form a complete intersection [BEM01] (for more details see [BEM01], [BKM90, CU02, Bus01a]).

We denote by S (resp. S_ν for $\nu \in \mathbb{N}$) the set of homogeneous polynomials (resp. of degree ν) in the variables $x_0, \ldots, x_n$ with coefficients in $\mathbb{K}$.

Let $g_1, \ldots, g_r$ be r (with $r \leq n+1$) homogeneous polynomials in S of degree $k_1 \geq \cdots \geq k_r$, and let $d_0 \geq \cdots \geq d_n$ be $n+1$ integers such that $d_n \geq \max(k_1, k_r + 1)$. We assume that $G = (g_1, \ldots, g_r)$ is a complete intersection and we consider the system

$$\mathbf{f_c} := \begin{cases} f_0(\mathbf{x}) = \sum_{i=1}^r h_{i,0}(\mathbf{x})\, g_i(\mathbf{x}) \\ \quad\vdots \\ f_n(\mathbf{x}) = \sum_{i=1}^r h_{i,n}(\mathbf{x})\, g_i(\mathbf{x}) \end{cases}$$

where $h_{i,j}(\mathbf{x}) = \sum_{|\alpha|=d_j-k_i} c_\alpha^{i,j}\, \mathbf{x}^\alpha$ is the generic homogeneous polynomial of degree $d_j - k_i$. We look for a condition on the coefficients $\mathbf{c} = (c_\alpha^{i,j})$ such that $\mathbf{f_c}$ has a solution "outside" the variety defined by G. Such a condition is given

by the residual resultant defined in [BEM01]. This resultant is constructed as a resultant over the blow-up $\pi : \tilde{X} \to X = \mathbb{P}^n$ of $\mathbb{P}^n$ along the coherent sheaf of ideals $\mathcal{G}$ associated to G ([Har83]).

If $\tilde{\mathcal{G}}$ is the sheaf on $\tilde{X}$ inverse image of $\mathcal{G}$ by π and $\tilde{\mathcal{G}}_{d_i} = \tilde{\mathcal{G}} \otimes \pi^*\big(\mathcal{O}_X(d_i)\big)$, the degree of the residual resultant in the coefficients of each f_i is $N_i = \int_{\tilde{X}} \prod_{j \neq i} c_1(\tilde{\mathcal{G}}_{d_j})$, with $c_1(\tilde{\mathcal{G}}_{d_j})$ is the first Chern class of $\tilde{\mathcal{G}}_{d_j}$. Using intersection theory [Ful98], we can give an explicit formula for N_i if G is a complete intersection. More precisely we have:

Theorem 3.4.4. *[BEM01] There exists an irreducible and homogeneous polynomial* $\mathrm{Res}_{G,d_0,\ldots,d_n}$ *in* $\mathbb{K}[\mathbf{c}]$ *which satisfies*

$$\mathrm{Res}_{G,d_0,\ldots,d_n}(f_0,\ldots,f_n) = 0 \Leftrightarrow \mathcal{Z}(F:G) \neq \emptyset.$$

Moreover, if for a fixed $j \in \{0,\ldots,n\}$ *we denote by* $\mathbf{d}$ *the* n*-tuple* $\mathbf{d} = (d_0,\ldots,d_{j-1},d_{j+1},\ldots,d_n)$, $\sigma_0(\mathbf{d}) = (-1)^n$, $\sigma_1(\mathbf{d}) = (-1)^{n-1}\sum_{l\neq j} d_l$, $\sigma_2(\mathbf{d}) = (-1)^{n-2}\sum_{j_1\neq j, j_2\neq j, j_1<j_2} d_{j_1}d_{j_2}$, $\ldots$, $\sigma_n(\mathbf{d}) = \prod_{l\neq j} d_l, r_j(T) = \sigma_n(\mathbf{d}) + \sum_{l=r}^{n} \sigma_{n-l}(\mathbf{d})\,T^l$, *and*

$$P_{r_j}(y_1,\ldots,y_r) = \det \begin{pmatrix} r_j(y_1) & \cdots & r_j(y_r) \\ y_1 & \cdots & y_r \\ \vdots & & \vdots \\ y_1^{r-1} & \cdots & y_r^{r-1} \end{pmatrix}.$$

The degree of $\mathrm{Res}_{G,d_0,\ldots,d_n}$ *in the coefficients of each polynomial* f_j *is*

$$N_j = \frac{P_{r_j}}{P_1}(k_1,\ldots,k_r).$$

The polynomial $\mathrm{Res}_{G,d_0,\ldots,d_n}$ is called the residual resultant. In order to compute it, let $\Delta_{i_1\ldots i_r}$ be the $r \times r$ minor of the matrix $(h_{i,j})_{1\leq i\leq r, 0\leq j\leq n}$ corresponding to the columns $i_1,\ldots,i_r$, $(e_0,\ldots,e_n)$ and $(\tilde{e_0},\ldots,\tilde{e_n})$ be two bases of the S-module S^{n+1}. A matrix whose determinant is a non-trivial multiple of $\mathrm{Res}_{G,d_0,\ldots,d_n}$ can be constructed using the following result:

Theorem 3.4.5. *[BEM01] For* $\nu \geq \nu_{\mathbf{d},\mathbf{k}} = \sum_{i=0}^{n} d_i - n - (n-r+2)k_r$, *the map*

$$\partial_\nu : \left(\bigoplus_{0\leq i_1<\ldots<i_r\leq n} S_{\nu-d_{i_1}-\cdots-d_{i_r}+\sum_{i=1}^{r} k_i} e_{i_1} \wedge \ldots \wedge e_{i_r} \right) \bigoplus \left(\bigoplus_{i=0}^{i=n} S_{\nu-d_i}\tilde{e_i} \right) \longrightarrow S_\nu$$

$$e_{i_1} \wedge \ldots \wedge e_{i_r} \longrightarrow \Delta_{i_1\ldots i_r}$$

$$\tilde{e_i} \longrightarrow f_i$$

is surjective if and only if $\mathcal{Z}(F:G) = \emptyset$. *In this case, every nonzero maximal minors of size* $\dim_{\mathbb{K}}(S_\nu)$ *of the matrix of* ∂_ν *is a multiple of* $\mathrm{Res}_{G,d_0,\ldots,d_n}$, *and the gcd of all these minors is exactly the residual resultant.*

This result is based on the resolution of the ideal $\big((f_0,\ldots,f_n):G\big)$ given in [BKM90].

Example 3.4.6. (The residual of two points in $\mathbb{P}^2$). We consider the following system in $\mathbb{P}^2$:

$$\begin{cases} f_0 = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3(x_1^2+x_2^2) \\ f_1 = b_0x_0^2 + b_1x_0x_1 + b_2x_0x_2 + b_3(x_1^2+x_2^2) \\ f_2 = c_0x_0^2 + c_1x_0x_1 + c_2x_0x_2 + c_3(x_1^2+x_2^2). \end{cases}$$

If $G=(x_0,x_1^2+x_2^2)$, $\nu_{\mathbf{d},\mathbf{k}}=2$ and a nonzero maximal minor of the matrix of ∂_ν is

$$\begin{vmatrix} a_0 & b_0 & c_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -b_1c_3+c_1b_3 & -b_2c_3+c_2b_3 & -c_1a_3+a_1c_3 \\ a_1 & b_1 & c_1 & 0 & -c_3b_0+b_3c_0 & 0 \\ c_2 & b_2 & c_2 & -c_3b_0+b_3c_0 & 0 & a_0c_3-c_0a_3 \\ a_3 & b_3 & c_3 & 0 & -b_1c_3+c_1b_3 & 0 \\ a_3 & b_3 & c_3 & -b_2c_3+c_2b_3 & 0 & -c_2a_3+a_2c_3 \end{vmatrix}.$$

The formula for the degrees gives $N_0=N_1=N_2=2$ and we check that this minor is the residual resultant times $c_3(c_1b_3-c_3b_1)$. It has the minimal degree N_0 in the coefficients of f_0. In this example the projective and toric resultants vanish identically.

Example 3.4.7. (The residual of a curve in $\mathbb{P}^3$). We consider the following system of cubics in $\mathbb{P}^3$ containing the umbilic:

$$\begin{cases} f_0 = (a_0x_0+a_1x_1+a_2x_2+a_3x_3)(x_0^2+x_1^2+x_2^2) + (a_4x_0^2+a_5x_1^2+a_6x_2^2+a_7x_3^2+ \\ \quad a_8x_0x_1+a_9x_0x_2+a_{10}x_0x_3+a_{11}x_1x_2+a_{12}x_1x_3+a_{13}x_2x_3)x_3 \\ f_1 = (b_0x_0+b_1x_1+b_2x_2+b_3x_3)(x_0^2+x_1^2+x_2^2) + (b_4x_0^2+b_5x_1^2+b_6x_2^2+b_7x_3^2+ \\ \quad b_8x_0x_1+b_9x_0x_2+b_{10}x_0x_3+b_{11}x_1x_2+b_{12}x_1x_3+b_{13}x_2x_3)x_3 \\ f_2 = (c_0x_0+c_1x_1+c_2x_2+c_3x_3)(x_0^2+x_1^2+x_2^2) + (c_4x_0^2+c_5x_1^2+c_6x_2^2+c_7x_3^2+ \\ \quad c_8x_0x_1+c_9x_0x_2+c_{10}x_0x_3+c_{11}x_1x_2+c_{12}x_1x_3+c_{13}x_2x_3)x_3 \\ f_3 = (d_0x_0+d_1x_1+d_2x_2+d_3x_3)(x_0^2+x_1^2+x_2^2) + (d_4x_0^2+d_5x_1^2+d_6x_2^2+d_7x_3^2+ \\ \quad d_8x_0x_1+d_9x_0x_2+d_{10}x_0x_3+d_{11}x_1x_2+d_{12}x_1x_3+d_{13}x_2x_3)x_3 \end{cases}$$

Let $G=(x_3,x_0^2+x_1^2+x_2^2)$. The previous construction gives $N_0=N_1=N_2=N_3=15$. The size of the matrix $\mathtt{M}_\nu$ of ∂_ν is a 84×200. A maximal minor of rank 84 whose determinant has degree 15 in the coefficients of f_0 has been constructed as follows. We extract from $\mathtt{M}_\nu$ 69 independent columns (by considering a random specialization). We add to this submatrix the columns of $\mathtt{M}_\nu$ depending on the coefficients of f_0 and independent of the 69 columns, in order to get a 84×84 matrix with a nonzero determinant. It yields a nonzero multiple of the residual resultant. Notice that the projective and toric resultants are identically 0 in this example.

3.5 Geometric solvers

Let us describe now how to exploit the resultant constructions to solve polynomial systems.

3.5.1 Multiplicative structure

Let $f_0, \ldots, f_n \in R$ and $\mathtt{M}_0 = \left(\begin{array}{c|c} \mathtt{M}_{00} & \mathtt{M}_{01} \\ \hline \mathtt{M}_{10} & \mathtt{M}_{11} \end{array}\right)$ be the transpose of the matrix defined in Section 2.3 of Chapter 2. Here, we use the natural convention that the columns of the resultant matrices represent multivariate polynomials.

Theorem 3.5.1. *[PS96, ER94, MP00, CLO98] For generic systems $f_1, \ldots, f_n$, the matrix of multiplication by f_0 in the basis*

$$\mathbf{x}^{E_0} = \{x_0^{\alpha_0} \ldots x_n^{\alpha_n} : 0 \leq \alpha_i < \deg f_i, i = 1, \ldots, n\}$$

of $\mathcal{A} = R/(f_1, \ldots, f_n)$ is the Schur complement of $\mathtt{M}_{1,1}$ in $\mathtt{M}_0$, namely $\mathtt{M}_{f_0} = \mathtt{M}_{00} - \mathtt{M}_{01}{\mathtt{M}_{11}}^{-1}\mathtt{M}_{10}$.

Proof. (see also proof of Theorem 2.3.2 of Chapter 2) Since $\mathbf{x}^{E_0}$ is a basis of the quotient by the polynomials $x_1^{d_1}, \ldots, x_n^{d_n}$, it remains a basis for generic polynomials $f_1, \ldots, f_n$ of degree $d_1, \ldots, d_n$.

In order to compute the matrix of M_{f_0} in this basis, we have first to multiply the elements of the basis by f_0. This is represented in a matrix form by the block $\mathtt{C}_0 := \begin{pmatrix} \mathtt{M}_{00} \\ \mathtt{M}_{10} \end{pmatrix}$. Then we have to reduce these polynomials in terms of the basis $\mathbf{x}^{E_0}$ by multiples of polynomials $f_1, \ldots, f_n$. The multiples that we use are represented by the coefficient matrix $\mathtt{C}_1 := \begin{pmatrix} \mathtt{M}_{01} \\ \mathtt{M}_{11} \end{pmatrix}$. The reduction corresponds to the matrix operation $\mathtt{C}_0 - \mathtt{C}_1\,\mathtt{M}_{11}^{-1}\mathtt{M}_{10}$ which yields the block

$$\mathtt{M}_{f_0} := \mathtt{M}_{00} - \mathtt{M}_{01}{\mathtt{M}_{11}}^{-1}\mathtt{M}_{10}.$$

Example 3.1.3 (continued). The matrix $\mathtt{M}_0$ associated to the polynomials f_1, f_2 of example 3.1.3, and a generic linear form $f_0 = u_0 + u_1x_1 + u_2x_2$ is:

```
> M_0 := mresultant([u[0]+u[1]*x[1]+u[2]*x[2],f1,f2],[x[1],x[2]]);
```

$$\mathtt{M}_0 := \left(\begin{array}{cccc|ccc|ccc} u_0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & -\frac{1}{6} \\ ub_2 & u_0 & 0 & 0 & 2 & 0 & -8 & 0 & -\frac{1}{6} & 0 \\ ub_1 & 0 & u_0 & 0 & 0 & 2 & -8 & -\frac{1}{6} & 0 & -1 \\ 0 & u_1 & u_2 & u_0 & -8 & -8 & 8 & 0 & -1 & 1 \\ \hline 0 & 0 & u_1 & 0 & 0 & -8 & 13 & -1 & 0 & 1 \\ 0 & u_2 & 0 & 0 & -8 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 13 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u_1 & 13 & 8 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & u_2 & 8 & 4 & 0 & 0 & 1 & 0 \end{array}\right).$$

In this example a basis of $\mathcal{A}$ is $S_0 = \{1, x_1, x_2, x_1x_2\}$. The Schur complement $\mathtt{M_{00}} - \mathtt{M_{01}}\mathtt{M_{11}}^{-1}\mathtt{M_{10}}$ of $\mathtt{M_{11}}$ in $\mathtt{M_0}$ is the 4×4 matrix:

```
> M(u):= uschur(M_0,4);
```

$$\mathtt{M}(u) := \begin{pmatrix} u_0 & -\frac{25}{24}\,u_2 & \frac{1}{6}\,u_1 & \frac{5}{54}\,u_1 - \frac{5}{54}\,u_2 \\ u_2 & u_0 + 2\,u_2 & 0 & \frac{2}{27}\,u_1 + \frac{5}{54}\,u_2 \\ u_1 & -\frac{5}{4}\,u_2 & u_0 + u_1 & \frac{55}{54}\,u_1 - \frac{55}{54}\,u_2 \\ 0 & u_1 + \frac{5}{4}\,u_2 & u_2 - u_1 & u_0 - u_1 + 2\,u_2 \end{pmatrix}.$$

By Theorem 3.5.1, the coefficient of u_i in $\mathtt{M}(u)$ is the matrix of the operator M_{x_i}.

An advantage of this approach is that we have a direct matrix representation of the multiplication operator without using an algorithm to compute a normal form in $\mathcal{A}$. This formula is a continuous function of the coefficients of input polynomials in the open set of systems such that $\mathtt{M_{11}}$ is invertible. Thus it can be used with approximated coefficients, which is useful in many practical applications. However the main drawback is that the size of the matrix $\mathtt{M_0}$ increases very quickly with the number of variables. One way to tackle this problem consists in exploiting the structure of the matrices (i.e. their sparsity and quasi-Toeplitz structure) as described in [MP00, BMP00]. Another way to handle it and to keep a continuous representation of the matrix of multiplication has been proposed in [MT00]. In some sense, it combines the previous resultant approach with the normal form method proposed in section 3.1.4, replacing the computation of a big Schur complement $\mathtt{M_{00}} - \mathtt{M_{01}}\mathtt{M_{11}}^{-1}\mathtt{M_{10}}$ by the inversion of much smaller systems.

In the next table, we compare the size of different systems to invert (first lines) with the size m of the matrix $\mathtt{M_{11}}$ to invert in Macaulay's formulation, in the case of projective resultants of quadrics ($d_i = 2$) in $\mathbb{P}^n$. Here D is the Bézout bound or the dimension of the $\mathbb{K}$-vector space $\mathcal{A}$.

n	5	6	7	8	9	10	11
	5	6	7	8	9	10	11
	20	30	42	56	72	90	110
	30	**60**	105	168	252	360	495
	20	**60**	**140**	**280**	504	840	1320
	5	30	105	**280**	**630**	**1260**	2310
		6	42	168	504	**1260**	**2772**
			7	56	252	840	2310
				8	72	360	1320
					9	90	495
						10	110
							11
Σ	80	192	448	1024	2304	5120	11264
m	**430**	**1652**	**6307**	**24054**	**91866**	**351692**	**1350030**
D	32	64	128	256	512	1024	2048

3.5.2 Solving by hiding a variable

Another approach to solve a system of polynomial equations consists in *hiding* a variable (that is, in considering one of the variables as a *parameter*), and in searching the values of this hidden variable for which the system has a solution. Typically, if we have n equations $f_1 = 0, \ldots, f_n = 0$ in n variables, we "hide" a variable, say x_n, and apply one of resultant constructions described before to the overdetermined system $f_1 = 0, \ldots, f_n = 0$ in the $n-1$ variables $x_1, \ldots, x_{n-1}$ and a parameter x_n. This leads to a resultant matrix $\mathtt{S}(x_n)$ with polynomial entries in x_n. It can be decomposed as

$$\mathtt{S}(x_n) = \mathtt{S}_d\, x_n^d + \mathtt{S}_{d-1} x_n^{d-1} + \cdots + \mathtt{S}_0,$$

where $\mathtt{S}_i$ has coefficients in $\mathbb{K}$ and the same size than $\mathtt{S}(x_n)$. We look for the values ζ_n of x_n for which the system has a *solution* $\zeta' = (\zeta_1, \ldots, \zeta_{n-1})$ in the corresponding variety X' (of dimension $n-1$) associated with the resultant formulation. This implies that

$$\mathbf{v}(\zeta')^{\mathtt{t}}\, \mathtt{S}(\zeta_n) = \mathbf{0}, \tag{3.10}$$

where $\mathbf{v}(\zeta')$ is the vector of monomials indexing the rows of $\mathtt{S}$ evaluated at ζ'. Conversely, for generic systems of the corresponding resultant formulation there is only one point ζ' above the value ζ_n. Thus the vectors $\mathbf{v}$ satisfying $\mathtt{S}(\zeta_n)^{\mathtt{t}}\, \mathbf{v} = \mathbf{0}$ are scalar multiples of $\mathbf{v}(\zeta')$. From the entries of these vectors, we can deduce the other coordinates of the point ζ'. This will be assumed hereafter[6].

The relation (3.10) implies that $\mathbf{v}(\zeta')$ is a generalized eigenvector of $\mathtt{S}^t(x_n)$. Computing such vectors can be transformed into the following linear generalized eigenproblem

$$\left(\begin{bmatrix} \mathbf{0} & \mathbb{I} & \cdots & \mathbf{0} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbb{I} \\ \mathtt{S}_0^t & \mathtt{S}_1^t & \ldots & \mathtt{S}_{d-1}^t \end{bmatrix} - \zeta_n \begin{bmatrix} \mathbb{I} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \mathbb{I} & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & -\mathtt{S}_d^t \end{bmatrix} \right) \mathbf{w} = 0. \tag{3.11}$$

The set of eigenvalues of (3.11) contains the values of ζ_n for which (3.10) has a solution. The corresponding eigenvectors $\mathbf{w}$ are decomposed as $\mathbf{w} = (\mathbf{w}_0, \ldots, \mathbf{w}_{d-1})$ so that the solution vector $\mathbf{v}(\zeta')$ of (3.10) is

$$\mathbf{v}(\zeta') = \mathbf{w}_0 + \zeta_n \mathbf{w}_1 + \cdots + \zeta_n^{d-1} \mathbf{w}_{d-1}.$$

This yields the following algorithm:

[6] Notice however that this genericity condition can be relaxed by using duality, in order to compute the points ζ' above ζ_n (when they form a zero-dimensional fiber) from the eigenspace of $\mathtt{S}(\zeta_n)$.

Algorithm 3.5.2 SOLVING BY HIDING A VARIABLE.

INPUT: $f_1, \ldots, f_n \in R$.

1. *Construct the resultant matrix* $\mathtt{S}(x_n)$ *of* $f_1, \ldots, f_n$ *(as polynomials in* $x_1, \ldots, x_{n-1}$*, with coefficients in* $\mathbb{K}[x_n]$*) adapted to the geometry of the problem.*
2. *Solve the generalized eigenproblem* $\mathtt{S}(x_n)\,\mathbf{v} = \mathbf{0}$.
3. *Deduce the coordinates of roots* $\zeta = (\zeta_1, \ldots, \zeta_n)$ *of* $f_1 = \cdots = f_n = 0$.

OUTPUT: *The roots of* $f_1 = \cdots = f_n = 0$.

Here again, we reduce the resolution of $f_1 = 0, \ldots, f_n = 0$ to an eigenvector problem.

Example 3.5.3. We illustrate this algorithm on the system

$$\begin{cases} f_1 = x_1\,x_2 + x_3 - 2 \\ f_2 = {x_1}^2 x_3 + 2\,x_2\,x_3 - 3 \\ f_3 = x_1\,x_2 + {x_2}^2 + x_2\,x_3 - x_1\,x_3 - 2. \end{cases}$$

We hide x_3 and use the projective resultant formulation (see Section 2.3 in Chapter 2). We obtain a 15×15 matrix $\mathtt{S}(x_3)$, and compute its determinant:

```
> S:=mresultant([f1,f2,f3],[t1,t2]):det(S);
```

$$\det(\mathtt{S}) := {x_3}^4\,(x_3 - 1)\left(2\,{x_3}^5 - 11\,{x_3}^4 + 20\,{x_3}^3 - 10\,{x_3}^2 + 10\,x_3 - 27\right).$$

The root $x_3 = 0$ does not yield an affine root of the system $f_1 = f_2 = f_3 = 0$ (the corresponding point is at infinity). Substituting $x_3 = 1$ in $\mathtt{S}(x_3)$, we get a matrix of rank 14. The kernel of $\mathtt{S}(1)^{\mathtt{t}}$ is generated by

$$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1).$$

This implies that the corresponding root is $(1, 1, 1)$. For the other eigenvalues (which are the roots of the last factor in $\det(\mathtt{S})$), we proceed similarly in order to obtain the 5 other (simple) roots of $f_1 = f_2 = f_3 = 0$. Here are numerical approximation of these roots:

$$(0.511793 - 1.27671\,\mathbf{i}, 0.037441 + 1.92488\,\mathbf{i}, -0.476671 - 0.937337\,\mathbf{i}),$$
$$(0.511793 + 1.27671\,\mathbf{i}, 0.037441 - 1.92488\,\mathbf{i}, -0.476671 + 0.937337\,\mathbf{i}),$$
$$(-1.38186 + 0.699017\,\mathbf{i}, -0.171994 + 0.704698\,\mathbf{i}, 2.25492 + 1.09402\,\mathbf{i}),$$
$$(-1.38186 - 0.699017\,\mathbf{i}, -0.171994 - 0.704698\,\mathbf{i}, 2.25492 - 1.09402\,\mathbf{i}),$$
$$(0.0734678, 0.769107, 1.9435).$$

3.5.3 Isolated points from resultant matrices

In this section, we consider n equations $f_1, \ldots, f_n$ in n unknowns, but we do not assume necessarily that they define a finite affine variety $\mathcal{Z}(f_1, \ldots, f_n)$.

We are interested in computing a rational univariate representation of the isolated points of this variety. We denote by I_0 the intersection of the primary components of $I = (f_1, \ldots, f_n)$ corresponding to isolated points of $\mathcal{Z}(I)$ and $\mathcal{Z}_0 = \mathcal{Z}(I_0)$. We denote by $\mathcal{C}_0(\mathbf{u})$ the Chow form associated to the ideal I_0 (see Section 3.2.3).

First we consider that $I = I_0$. Let $f_0 = u_0 + u_1x_1 + \cdots + u_nx_n$ be a generic affine form (the u_i are considered as variables). We choose one of the previous resultant constructions for $f_0, \ldots, f_n$ which yields a matrix

$$\mathtt{M}_0 = \begin{pmatrix} \mathtt{M}_{00} & \mathtt{M}_{01} \\ \mathtt{M}_{10} & \mathtt{M}_{11} \end{pmatrix}$$

such that $\mathtt{M}_{11}$ is invertible (if it exists). The blocks $\mathtt{M}_{00}, \mathtt{M}_{10}$ depend only on the coefficients of f_0. From Section 3.5.1 and according to the relation

$$\begin{pmatrix} \mathtt{M}_{00} & \mathtt{M}_{01} \\ \mathtt{M}_{10} & \mathtt{M}_{11} \end{pmatrix} \begin{pmatrix} \mathbb{I} & \mathbf{0} \\ -\mathtt{M}_{11}^{-1}\mathtt{M}_{10} & \mathbb{I} \end{pmatrix} = \begin{pmatrix} \mathtt{M}_{00} - \mathtt{M}_{01}\mathtt{M}_{11}^{-1}\mathtt{M}_{10} & \mathtt{M}_{01} \\ \mathbf{0} & \mathtt{M}_{11} \end{pmatrix}$$

we deduce that $\det(\mathtt{M}_0) = \det(\mathtt{M}_{f_0}) \det(\mathtt{M}_{11})$. This means that $\det(\mathtt{M}_0)$ is a scalar multiple of the Chow form of the ideal I. Such a construction applies for a system which is generic for one of the mentioned resultant formulations. We can obtain a rational univariate representation of $\mathcal{Z}(I)$ applying Algorithm 3.2.10.

If the affine variety $\mathcal{Z}(I)$ is not finite, we can still deduce a rational univariate representation of the isolated points from the previous resultant construction in (at least) two ways.

When the system is not generic for a given construction, a perturbation technique can be used. Introducing a new parameter ϵ and considering a perturbed system f_ϵ (for instance $f_\epsilon = f + \epsilon f_0$), we obtain a resultant matrix $\mathtt{S}_\epsilon(\mathbf{u})$ whose determinant is of the form

$$\Delta(\mathbf{u}, \epsilon) = \epsilon^k \Delta_k(\mathbf{u}) + \epsilon^{k+1}\Delta_{k+1}(\mathbf{u}) + \cdots \quad \text{with} \quad \Delta_k \neq 0.$$

It can be shown that $\Delta_k(\mathbf{u})$ is a multiple of the Chow form of I_0. Applying Algorithm 3.2.10 to this multiple of the Chow form yields a rational univariate representation of $\mathcal{Z}_0$ (see [Gri86, Chi86, Can90, GH91, LL91] for more details).

The use of a new parameter ϵ has a cost that we want to remove. This can be done by exploiting the properties of the Bezoutian matrix.

Proposition 3.5.4. *[EM99a, BEM00] Any nonzero maximal minor $\Delta(\mathbf{u})$ of the Bezoutian matrix of polynomials $f_0 = u_0 + u_1x_1 + \cdots + u_nx_n, f_1, \ldots, f_n$ is divisible by the Chow form $\mathcal{C}_0(\mathbf{u})$ of the isolated points of $I = (f_1, \ldots, f_n)$.*

The interesting point here is that we get directly the Chow form of the isolated points of $\mathcal{Z}(I)$ even if this variety is not finite. In other words, we do not need to perturb the system for computing a multiple of $\mathcal{C}_0(\mathbf{u})$. Another advantage of this approach is that it yields an "explicit" formulation for $\Delta(\mathbf{u})$, and its

structure can be handled more carefully (for instance, by working directly on the matrix form instead of dealing with the expansion of minors). So we have the following algorithm:

Algorithm 3.5.5 Rational univariate representation of the isolated points.

Input : $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$

1. *Compute a nonzero multiple* $\Delta(\mathbf{u})$ *of the Chow form of* $f_1, \ldots, f_n$*, from an adapted resultant formulation of* $f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n, f_1, \ldots, f_n$ *(for instance using the Bezoutian matrix).*
2. *Get a rational univariate representation of the isolated (and maybe some embedded) roots of* $f_1 = \cdots = f_n = 0$ *by applying Algorithm 3.2.10.*

In practice, instead of expanding completely the polynomial $d(\mathbf{t}+\mathbf{u})$ in Algorithm 3.2.10, it would be advantageous to consider $u_1, \ldots, u_n$ as *infinitesimal numbers* (i.e. $u_i^2 = u_i u_j = 0$ for $i, j = 1, \ldots, n$) in order to get only the first terms $d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0)$ of the expansion of $d(\mathbf{t}+\mathbf{u})$. Moreover, we can describe these terms as sums of determinants of matrices deduced from resultant matrices. This allows us to use fast interpolation methods to compute efficiently $d_0(u_0), \ldots, d_n(u_0)$.

3.5.4 Solving overdetermined systems

In many problems (such as in reconstruction in computer vision, autocalibration in robotics, identification of sources in signal processing, ...), each observation yields an equation. Thus, we can generate as many (approximated) equations as we want but usually only one solution is of (physical) interest. Thus we are dealing with overconstrained systems which have approximate coefficients (due to measurement errors for instance).

Here again we are interested in matrix methods which allow us to handle systems with approximate coefficients. The methods of the previous sections for the construction of resultant matrices $\mathtt{M}_0$ admit natural generalizations [Laz77] to overconstrained systems, that is, to systems of equations $f_1 = \ldots = f_m = 0$, with $m > n$, defining a finite number of roots. We consider a map of the form

$$\begin{aligned} \mathcal{S} : \mathcal{V}_1 \times \cdots \times \mathcal{V}_m &\to \mathcal{V} \\ (q_1, \ldots, q_m) &\mapsto \sum_{i=1}^{m} f_i \, q_i \end{aligned}$$

where $\mathcal{V}$ and $\mathcal{V}_i$ are linear subspaces generated by monomials of R. This yields a rectangular matrix $\mathtt{S}$.

A case of special interest is when this matrix is of rank $N-1$, where N is the number of rows of $\mathtt{S}$. In this case, it can be proved [EM] that $\mathcal{Z}(f_1, \ldots, f_m)$

is reduced to one point $\zeta \in \mathbb{K}^n$, and if $\mathbf{x}^F = (\mathbf{x}^\alpha)_{\alpha \in F}$ is the set of monomials indexing the rows of $\mathtt{S}$ that

$$(\zeta^\alpha)_{\alpha \in F}\, \mathtt{S} = \mathbf{0}.$$

Using Cramer's rule, we see that ζ^α/ζ^β $(\alpha, \beta \in F,\ \zeta^\beta \neq 0)$ can be expressed as the ratio of two maximal minors of $\mathtt{S}$. If $1, x_1, \ldots, x_n \in \mathbf{x}^F$ (which is the case most of the time), we obtain ζ as a rational function of maximal minors of $\mathtt{S}$, and thus of input coefficients of $f_1, \ldots, f_m$.

Algorithm 3.5.6 Solving an overconstrained system defining a single root

Input: *A system* $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *(with* $m > n$*) defining a single solution.*

1. *Compute the resultant matrix* $\mathtt{S}$ *for one of the proposed resultant formulations.*
2. *Compute the kernel of* $\mathtt{S}$ *and check that it is generated by one vector* $\mathbf{w} = (\mathbf{w}_1, \mathbf{w}_{x_1}, \ldots, \mathbf{w}_{x_n}, \ldots)$.

Output: $\zeta = (\frac{\mathbf{w}_{x_1}}{\mathbf{w}_1}, \ldots, \frac{\mathbf{w}_{x_n}}{\mathbf{w}_1})$.

Let us illustrate this algorithm, with a projective resultant construction.

Example 3.5.7. We consider the case of 3 conics:

```
> f1:= x1^2-x1*x2+x2^2-3;
> f2:= x1^2-2*x1*x2+x2^2+x1-x2;
> f3:= x1*x2+x2^2-x1+2*x2-9;
> S:=mresultant([f1,f2,f3],[x1,x2]);
```

$$\mathtt{S} := \begin{pmatrix}
-3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -9 & 0 & 0 & 0 \\
0 & -3 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -9 & 2 & 0 & 0 & 0 \\
0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -9 \\
-1 & 0 & 0 & -3 & 0 & -1 & -2 & 0 & 1 & 0 & -1 & 1 & -9 & 0 & 2 \\
0 & 1 & -1 & 0 & -1 & -2 & 0 & 1 & 1 & 0 & 0 & 0 & -1 & 2 & 1 \\
0 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & -2 & -1 & 1 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 1 & -2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1 & 1 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -9 & -1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & -9 & 2 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

The rows of $\mathtt{S}$ are indexed by

$$(1, x_2, x_1, x_1x_2, {x_1}^2x_2, x_1{x_2}^2, {x_1}^3x_2, {x_1}^2{x_2}^2, x_1{x_2}^3, {x_1}^2, {x_2}^2, {x_1}^3, {x_2}^3, {x_1}^4, {x_2}^4).$$

We compute the kernel of $\mathtt{S}^t$ in order to check its rank and to deduce the common root ζ of the system:

```
> kernel(transpose(S));
```

$$\{(1,2,1,2,2,4,2,4,8,1,4,1,8,1,16)\}.$$

Considering the list of monomials which index the rows of S we deduce that $\zeta = (1,2)$.

In case that the overdetermined system has more than one root, we can follow the same approach. We chose a subset E of F (if possible containing the monomials $1, x_1, \ldots, x_n$) such that the rank of the matrix indexed by the monomials $\mathbf{x}^{F\setminus E}$ is the rank $r = N - D$ of S. The set $\mathbf{x}^E$ will be the basis of $\mathcal{A}$. Assuming that the monomials $x_i\,\mathbf{x}^E$, $i = 1, \ldots, n$, are also in $\mathbf{x}^F$, we complete the matrix S with the block of coefficients of $f_0\,\mathbf{x}^{E_0}$, where $f_0 = u_0 + u_1\,x_1 + \cdots + u_n\,x_n$. By a Schur complement computation, we deduce the matrix of multiplication by f_0 in the basis $\mathbf{x}^E$ of $\mathcal{A}$. Now, by applying the algorithms of Section 3.2.2, we deduce the roots of the overdetermined system $f_1, \ldots, f_m$ (see [EM99b] for more details on this approach).

3.6 Applications

We will use the tools and methods developed above to solve some problems coming from several areas of applications.

3.6.1 Implicitization of a rational surface

A rational surface (S) in $\mathbb{K}^3$ may be represented by a parametric representation:

$$(S) : x = \frac{f(s,t)}{d_1(s,t)} \quad , \quad y = \frac{g(s,t)}{d_2(s,t)} \quad , \quad z = \frac{h(s,t)}{d_3(s,t)} \ ,$$

where $f, g, h, d_1, d_2, d_3 \in \mathbb{K}[s,t]$ or by an implicit equation (i.e. $F \in \mathbb{K}[x,y,z]$ of minimal degree satisfying $F(a,b,c) = 0$ for all $(a,b,c) \in (S)\big)$. These two representations are important for different reasons. For instance, the first one is useful for drawing (S) and the second one to intersect surfaces or to decide whether a point is in (S) or not.

We will investigate the implicitization problem, that is the problem of converting a parametric representation of a rational surface into an implicit one.

These last decades have witnessed a renewal of this problem motived by applications in computer-aided geometric design and geometric modelling ([SAG84], [Buc88a], [Hof89], [Kal91], [CM92], [AGR95], [CGZ00], [AS01], [CGKW01]). Its solution is given by resultants, Gröbner bases, moving surfaces (see [SC95], [BCD03], [D'A01]). The techniques based on resultants and

moving surfaces fail in the presence of base points (i.e. common roots of f, g, h, d_1, d_2, d_2). The Gröbner bases methods are fairly expensive in practice even if the dimension is small. Recently, methods using residual resultants and approximation complexes have been proposed but only under some restrictive geometric hypotheses on the zero-locus of base points which are difficult to verify ([Bus01b], [BJ03], [BC]). We propose an approach based on the residue calculus extending [GV97]. This method works in the presence of base points and no geometric hypotheses on the zero-locus of base points are needed.

In order to find an implicit equation of (S), as in Proposition 3.3.6 we can compute a nonzero maximal minor of the Bezoutian matrix of polynomials $xd_1 - f, yd_2 - g, zd_3 - h$ with respect to s, t. In general, this yields a multiple of the implicit equation as shown below.

Example 3.6.1. Let (S) be the surface parameterized by

$$x = s \quad , \quad y = \frac{t^2 s + 2t + s}{t^2} \quad , \quad z = \frac{t^2 - 2st - 1}{t^2}.$$

The Bezoutian matrix of $x - s, yt^2 - t^2 s - 2t - s, zt^2 - t^2 + 2ts + 1$ in $(\mathbb{K}[x, y, z])[s, t]$ is a 4×4 matrix.

```
> melim([x*d1-f,y*d2-g,z*d3-h],[s,t]);
```

$$(z-1)^2(4x^4 - 4x^3 y + x^2 z^2 - 8x^2 z + 2xyz + 4x^2 + y^2 + 4z - 4).$$

The second factor in this expression is the expected implicit equation.

The use of the Bezoutian matrix produces an extraneous term along with the implicit equation. We will see how to use the residue calculus in order to remove it from this equation.

Let us consider the polynomials in $(\mathbb{K}[x, y, z])[s, t]$

$$\begin{cases} F(s,t) = x\ d_1(s,t) - f(s,t) \\ G(s,t) = y\ d_2(s,t) - g(s,t) \\ H(s,t) = z\ d_3(s,t) - h(s,t). \end{cases}$$

Let $\mathcal{Z}_0 = \{\zeta \in \overline{\mathbb{K}(y,z)}^2 : G(\zeta) = H(\zeta) = 0\} = \mathcal{Z}_1 \cup \mathcal{Z}_2$, where $\mathcal{Z}_1$ is the algebraic variety $\mathcal{Z}_0 \cap \mathcal{Z}(d_1 d_2 d_3) = \{\zeta \in \overline{\mathbb{K}(y,z)}^2 : G(\zeta) = H(\zeta) = d_1 d_2 d_3(\zeta) = 0\}$ and $\mathcal{Z}_2 = \mathcal{Z}_0 \setminus \mathcal{Z}_1$. If $\mathcal{Z}_2$ is finite, let $Q(x, y, z)$ be the following nonzero element

$$Q(x,y,z) = \prod_{\zeta \in \mathcal{Z}_2} F(\zeta) = \left(\prod_{\zeta \in \mathcal{Z}_2} d_1(\zeta) \right) \left(x^m + \sigma_1(y,z) x^{m-1} + \cdots + \sigma_m(y,z) \right)$$

where m is the number of points (counting their multiplicities) in $\mathcal{Z}_2$ and $\sigma_i(y, z)$ is the i-th elementary symmetric function of $\left\{ \frac{f(\zeta)}{d_1(\zeta)} : \zeta \in \mathcal{Z}_2 \right\}$.

Theorem 3.6.2. *The implicit equation of the surface (S) is the square-free part of the numerator of*

$$E(x,y,z) := x^m + \sigma_1(y,z)x^{m-1} + \cdots + \sigma_m(y,z) \in \mathbb{K}(y,z)[x].$$

Proof. Let us choose a point (y_0, z_0) in the open subset U of $\overline{\mathbb{K}}^2$ such that the specialization $\tilde{\mathcal{Z}}_2$ of $\mathcal{Z}_2$ is finite in $\overline{\mathbb{K}}^2$ and the denominators of $\sigma_1, \ldots, \sigma_m$ do not vanish. Then we have $Q(x_0, y_0, z_0) = 0$ if and only if

$$x_0^m + \sigma_1(y_0,z_0)x_0^{m-1} + \cdots + \sigma_m(y_0,z_0) = 0\ ,$$

which is equivalent to the existence of an element $\zeta_0 \in \tilde{\mathcal{Z}}_2$ such that $x_0 = \frac{f(\zeta_0)}{d_1(\zeta_0)}$. In other words, the numerator of $E(x,y,z)$ vanishes on a point $(x_0, y_0, z_0) \in U$ if and only if it belongs to (S), which implies that the square-free part of the numerator of $E(x,y,z)$ is up to a scalar the implicit equation of the surface (S).

The coefficients $\sigma_i(y,z)$ in Theorem 3.6.2 can be computed using the Newton identities (3.8). So we need to compute the Newton sums $S_i(y,z) = \sum_{\zeta\in\mathcal{Z}_2}\big(\frac{f(\zeta)}{d_1(\zeta)}\big), i = 0, \ldots, m$. By adding a variable we can assume that $d_1 = 1$.

Algorithm 3.6.3 IMPLICITIZATION OF A RATIONAL SURFACE

INPUT: *Polynomials f, g, h, d_1, d_2, d_3 in $\mathbb{K}[s,t]$.*

1. *Compute an algebraic relation $A_s(u_0,u_1,u_2)$ (resp. $A_t(u_0,u_1,u_2)$) between s, $G = y\,d_2 - g$, $H = z\,d_3 - h$ (resp. t, G, H) in $\mathbb{K}[y,z][s,t]$.*
   - *If the univariate polynomials $R_s = A_s(s,0,0)$, $R_t = A_t(t,0,0)$ do not vanish identically (which is often the case), let M be the 2×2 matrix such that $\begin{pmatrix} R_s \\ R_t \end{pmatrix} = M \begin{pmatrix} G \\ H \end{pmatrix}$.*
     – *Compute the degree*

     $$m = \tau_{(G,H)}\big(\mathrm{Jac}(G,H)\big) = \tau_{(R_s,R_t)}\big(\mathrm{Jac}(G,H)\det(M)\big)$$

     in x of the polynomial $E(x,y,z) \in \mathbb{K}(y,z)[x]$ in Theorem 3.6.2.
     – *For i from 1 to m, compute*

     $$S_i(y,z) = \tau_{(G,H)}\big(\mathrm{Jac}(G,H)f^i\big) = \tau_{(R_s,R_t)}\big(\mathrm{Jac}(G,H)\det(M)f^i\big).$$

   - *If the polynomial $R_sR_t \equiv 0$, the power sums $S_i(y,z)$, for $i = 0, \ldots, m$, are computed using the algebraic relations $A_s(u_0,u_1,u_2)$, $A_t(u_0,u_1,u_2)$ and the formula in Proposition 3.3.8.*
2. *Use the Newton identities (3.8) to obtain the elementary symmetric functions $\sigma_i(y,z)$ from the Newton sums $S_i(y,z)$, $i = 1, \ldots, m$.*

OUTPUT: *The numerator of $x^m + \sigma_1(y,z)x^{m-1} + \cdots + \sigma_m(y,z) \in \mathbb{K}(y,z)[x]$.*

Example 3.6.1 (continued). In this case, the univariate polynomials R_s and R_t are equal to

$$\begin{aligned} R_s &= -4 + 4z^3 + 4s^4 + 4s^2 + 21s^2z^2 - 16s^2z - 4s^3y - 12z^2 - 10z^3s^2 \\ &\quad + z^4s^2 - 8zs^4 + 4z^2s^4 + 2yz^3s + 8ys^3z - 4ys^3z^2 - 4z^2ys \\ &\quad + 2zsy + y^2 - 2y^2z + z^2y^2 + 12z, \\ R_t &= 4z - 4 - 8t^3y + 8t^3yz + 16t^2 - 20t^2z + 4z^2t^2 + 4t^4z^2 - 8t^4z + 4t^4. \end{aligned}$$

The computation of the Newton sums gives

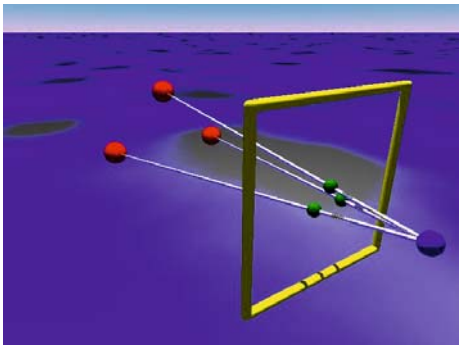
$$S_0 = 4, S_1 = y, S_2 = -\frac{1}{2}z + 4z + y - 2, \quad S_3 = \frac{1}{4}y(-3z^2 + 18z - 12 + 4y^2)$$
$$S_4 = \frac{1}{8}z^4 - 2z^3 - z^2y^2 + 9z^2 - 12z + 6y^2z + y^4 - 5y^2 + 6.$$

And the implicit equation of (S) is

$$x^4 - x^3y + \frac{1}{4}x^2z^2 - 2x^2z + x^2 + \frac{1}{2}zxy + z + \frac{1}{4}y^2 - 1.$$

3.6.2 The position of a camera

We consider a camera which is observing a scene. In this scene, three points A, B, C are identified. The center of the camera is denoted by X. We assume that the camera is calibrated, that is, we know the focal distance, the projection of the center of the camera, ... Then, we easily deduce the angles between the rays XA, XB, XC from the images of the points A, B, C.



We denote by α the angle between XB and XC, β the angle between XA and XC, γ between XA and XB. These angles are deduced from the measurements in the image. We also assume that the distances a between B and C, b

between A and C, c between A and B are known. This leads to the following system of polynomial constraints:

$$\begin{cases} x_1^2 + x_2^2 - 2\cos(\gamma)x_1x_2 - c^2 = 0 \\ x_1^2 + x_3^2 - 2\cos(\beta)x_1x_3 - b^2 = 0 \\ x_2^2 + x_3^2 - 2\cos(\alpha)x_2x_3 - a^2 = 0 \end{cases} \tag{3.12}$$

where $x_1 = |XA|$, $x_2 = |XB|$, $x_3 = |XC|$. Once we know the distances x_1, x_2, x_3, the two symmetric positions of the center X are easily deduced. The system (3.12) can be solved by direct polynomial manipulations, expressing x_2 and x_3 in terms of x_1 from the two first equations and substituting in the last one. After removing the square roots, we obtain a polynomial of degree 8 in x_1, which implies at most 16 positions of the center X in this problem. Another simple way to get this equation is to eliminate the variables x_2, x_3, using the Bezoutian construction (from the MULTIRES package), and we obtain

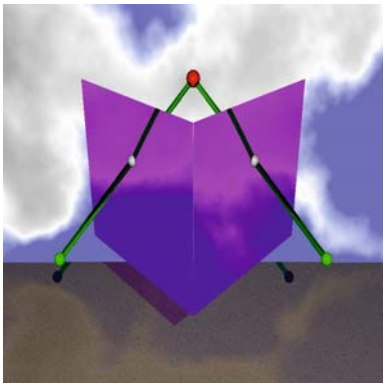
```
> melim([f1,f2,f3], [x2,x3]);
```

$$\begin{aligned} &2\cos(\alpha)\left(64\cos(\beta)^2\cos(\alpha)^2\cos(\gamma)^2 - 64\cos(\beta)^3\cos(\alpha)\cos(\gamma) - 64\cos(\beta)\cos(\alpha)^3\cos(\gamma) + 16\cos(\gamma)^4\right. \\ &-64\cos(\beta)\cos(\alpha)\cos(\gamma)^3 + 16\cos(\beta)^4 + 32\cos(\beta)^2\cos(\alpha)^2 + 32\cos(\beta)^2\cos(\gamma)^2 + 16\cos(\alpha)^4 \\ &\left.+32\cos(\alpha)^2\cos(\gamma)^2 + 64\cos(\beta)\cos(\alpha)\cos(\gamma) - 32\cos(\beta)^2 - 32\cos(\alpha)^2 - 32\cos(\gamma)^2 + 16\right) x_1^8 + \cdots \end{aligned}$$

Once this equation of degree 8 in x_1 is known, the numerical solving is easy.

3.6.3 Autocalibration of a camera

We consider here the problem of computing the intrinsic parameters of a camera from observations and measurements in 3 images of the same scene. Following the approach described in [Fau93], the camera is modeled by a pine hole projection. From the 3 images, we suppose that we are able to compute the fundamental matrices relating a pair of points in correspondence in two images. If **m, m'** are the images of a point $M \in \mathbb{R}^3$ in two photos, we have $\mathbf{m}\ F\mathbf{m'}$=0, where F is the fundamental matrix.



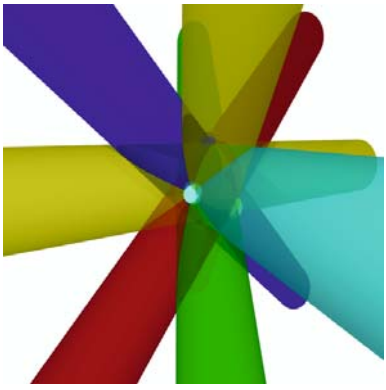
From 3 images and the 3 corresponding fundamental matrices, we deduce the so-called Kruppa equations on the 6 intrinsic parameters of the camera. See [Kru13], [Fau93] for more details. This is a system of 6 quadratic homogeneous equations in 6 variables. We solve this overdetermined system by choosing 5 equations among the six, solving the corresponding affine system and choosing the best solutions for the last equation among the 32 solutions. This took $0.38s$ on a Alpha 500Mhz workstation for the following experimentation:

Exact root	Computed root
1.049401330318981	1.049378730793354
4.884653820635368	4.884757558650871
6.011985256613766	6.011985146332036
.1726009605860270	.1725610425715577
1.727887086410446	1.727898150468536

The solver used for this computation has been developed by Ph. Trébuchet [Tré02] and is available in the library SYNAPS [DRMRT02] (see `Solve(L, newmac<C>())`.

3.6.4 Cylinders through 4 and 5 points

We consider the problem of finding cylinders through 4 or 5 points. The system that we use is described in [DMPT03].



The number of solutions for the problems that we consider are the following:

- Cylinders through 5 points: $6 = 3 \times 3 - 3$ solutions.
- Cylinders through 4 points and fixed radius: $12 = 3 \times 4$ solutions.
- Lines tangent to 4 unit balls: 12 solutions.
- Cylinders through 4 points and extremal radius: $18 = 3 \times 10 - 3 \times 4$ solutions.

Here are experimental results also performed with the solver developed by Ph. Trébuchet:

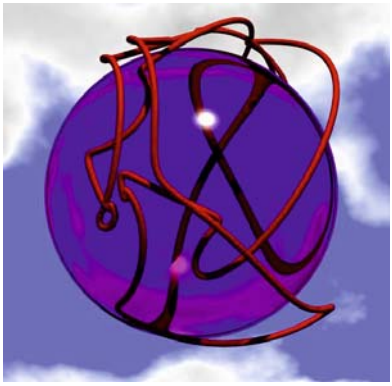
Problem	*time*	$max(\|f_i\|)$
Cylinders through 5 points	$0.03s$	$5 \cdot 10^{-9}$
Parallel cylinders through 2×4 points	$0.03s$	$5 \cdot 10^{-9}$
Cylinders through 4 points, extremal radius	$2.9s$	10^{-6}

The computation was performed on an Intel PII 400 128 MB of RAM. $max(|f_i|)$ is the maximum of the norm of the defining polynomials f_i evaluated at the approximated roots. The relatively huge time spent in the last problem is due to the treatment of multiple roots.

3.6.5 Position of a parallel robot

Consider a parallel robot, which is a platform controlled by 6 arms:

From the measurements of the length of the arms, we would like to know the position of the platform. This problem is a classical benchmark in polynomial system solving. We know from [RV95, Laz93, Mou93] that this problem has at most 40 solutions and that this bound is reached [Die98]. Here is the 40 degree curve that we obtain when we remove an arm of the mechanism:



The geometric constraints describing the position of the platform are transformed into a system of 6 polynomial equations:

$$\|R\,Y_i + T - X_i\|^2 - d_i^2 = 0 \quad , \quad i = 1, \ldots, 6,$$

where R equals

$$\frac{1}{a^2+b^2+c^2+d^2}\begin{pmatrix} a^2-b^2-c^2+d^2 & 2\,ab-2\,cd & 2\,ac+2\,bd \\ 2\,ab+2\,cd & -a^2+b^2-c^2+d^2 & 2\,bc-2\,ad \\ 2\,ac-2\,bd & 2\,ad+2\,bc & -a^2-b^2+c^2+d^2 \end{pmatrix}$$

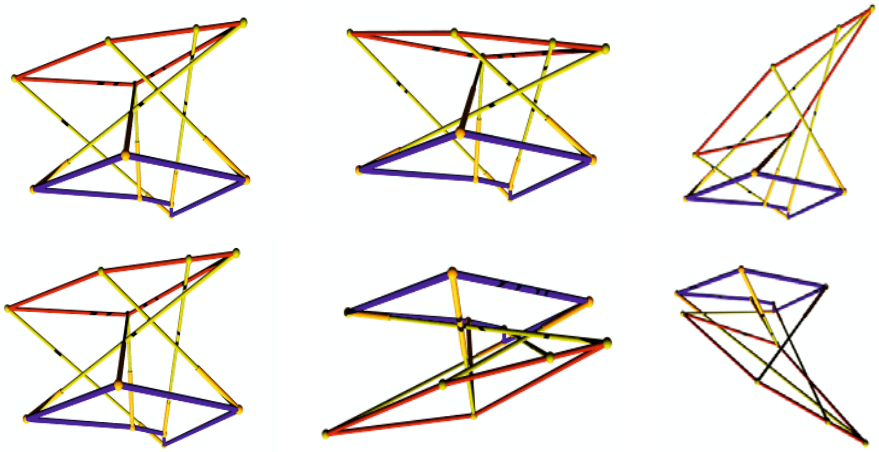
i.e. the rotation of the platform with respect to a reference frame, and $T = (u, v, w)$ is its translation. Using again the solver by Ph. Trébuchet and a different modelisation (with point coordinates in the first column, and quaternions in the second column), and one deduced from the residual resultant construction (in the column "redundant") as described in [Bus01a], and different numerical precision, we obtain the following results:

Direct modelisation		Quaternions		Redundant	
250 b. $3.21s$	128 b. -	250 b. $8.46s$	128 b. $6.25s$	250 b. $1.5s$	128 b. $1.2s$

Here n b. denotes the number n of bits used in the computation.

3.6.6 Direct kinematic problem of a special parallel robot

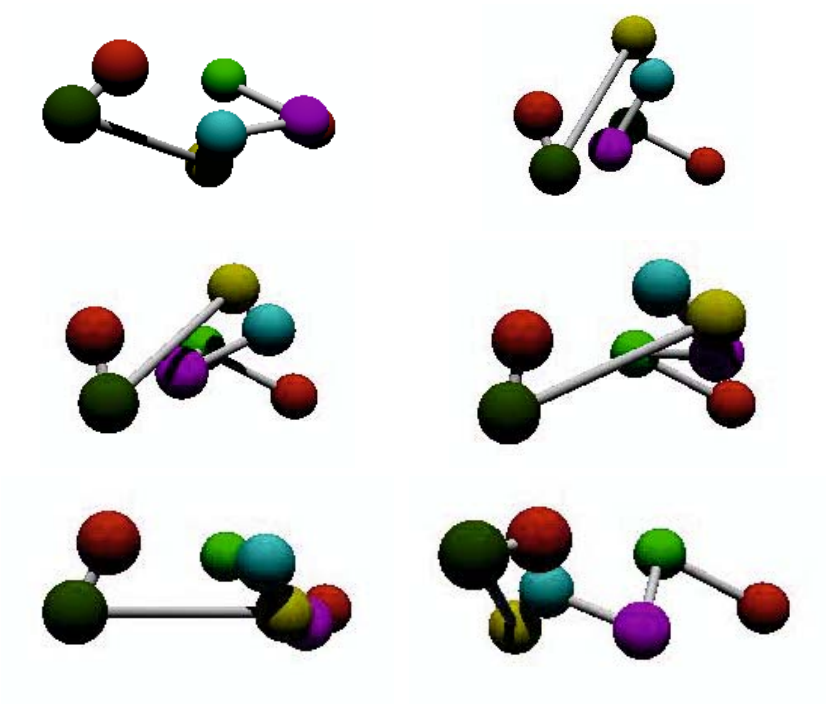
Resultant constructions can also be used for some special geometry of the platform. Here is an example where two attached points of the arms on the platform are identical. We solve this problem by using the Bezoutian formulation, which yields a 20×20 matrix of polynomials in one variable. The number of complex solutions is also 40. The code for the construction of the matrix is generated in a pre-processing step and the parameters defining the geometry of the platform are instantiated at run time. This yields the following results. There are 6 real solutions, one being of multiplicity 2:



We obtain the following error $|\|RY_i + T - X_i\|^2 - d_i^2| < 10^{-6}$ and the time for solving is $0.5s$ on an Intel PII 400, 128 MB of RAM.

3.6.7 Molecular conformation

Similar resultant constructions can also be used, in order to compute the possible conformations of a molecule when the position and orientation of the links at the extremity are known. The approach is similar to the one described in [RR95]. It was developed by O. Ruatta, based on the SYNAPS library. Here also, the resultant matrix is constructed in a preprocessing step and we instantiate the parameters describing the geometry of the molecule at run-time. In this example, we obtain 6 real solutions among the 16 complex possible roots:



The numeric error on the solutions is bounded by 10^{-6} and the time for solving is $0.090s$, on a standard workstation.

3.6.8 Blind identification in signal processing

Finally, we consider a problem from signal processing described in detail in [GCMT02]. It is related to the transmission of an input signal $\mathbf{x}(n)$ of size p depending on the discrete time n into a convolution channel of length L. The output is $\mathbf{y}(n)$ and we want to compute the impulse response matrix $H(n)$ satisfying:

$$\mathbf{y}(n) = \sum_{m=0}^{L-1} H(m)\mathbf{x}(n-m) + \mathbf{b}(\mathbf{n}),$$

where $\mathbf{b}(n)$ is the noise. If $\mathbf{b}(n)$ is Gaussian centered, a statistic analysis of the output signal yields the equations:

$$\sum_{m=0}^{L-1} \sum_{i=1}^{p} h_{\alpha,i}(m)h_{\beta,i}(m)(-1)^{n-m} = E(y_\alpha(n)y_\beta(n-l)) \ ,$$

where $h_{\alpha,i}(m)$ are the unknowns and the $E(y_\alpha(n)y_\beta(n-l))$ are known from the output signal measurements. We solve this system of polynomial equations of degree 2 in 6 variables, which has 64 solutions for $p = 1$, with the algebraic solver of Ph. Trébuchet and we obtain the following results:

	A real root
x0	-1.803468527372455
x1	-5.162835380624794
x2	-7.568759900599482
x3	-6.893354578266418
x4	-3.998807562745594
x5	-1.164422870375179
Error $= 10^{-8}$, Time $= 0.76s$	