Symbolic-numeric methods for solving polynomial equations and applications

B. Mourrain,
INRIA, GALAAD, B.P. 93, Sophia-06902 Antipolis, France.
mourrain@sophia.inria.fr

Abstract

This tutorial gives an introductive presentation of algebraic and geometric methods for solving a polynomial system $f_1 = \cdots = f_m = 0$. The first class of methods is 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 the solutions, from the structure of $\mathcal{A}$ and in particular, how solving polynomial equations reduces to eigen computations of these multiplication operators. We mention briefly two general methods for computing the normal of elements in $\mathcal{A}$, used to obtain a representation of the multiplication operators. The geometric methods are based projection operations, which are closely related to the theory of resultants. We present different notions and 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 vision, robotics, computational biology and signal processing.

Contents

1 Introduction

Polynomial system solving is ubiquitous in many applications such as Robotics, Computer vision, Signal processing, ... Specific methods like minimization, Newton iterations, ... are often used, but not always with guarantees on the result. In this paper, we give an introductive 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 our computations. The tools that we introduce, are illustrated by explicit computations. A MAPLE package implements the algorithms described hereafter and is publicly available at `http://www.inria.fr/galaad/logiciels/multires.html`. We encourage the reader to do the experimentation by himself, with this package. For more advanced computations described in the last section, we use the C++ library SYNAPS available at `http://www.inria.fr/galaad/logiciels/synaps/index.html`.

The approach that we are going to follow is based on the study of the quotient algebra $\mathcal{A}$ of the polynomial ring by the ideal $I = (f_1, \ldots, f_m)$. We show in a first part how to deduce the geometry of the solutions, from the structure of $\mathcal{A}$. In particular, we recall how solving polynomial equations reduces to the computation of the eigenvalues or eigenvectors of the operators of multiplication in $\mathcal{A}$. In the case of real coefficients, we also recall how to recover information on the real roots, from this structure.

In the next part, we describe briefly a general method (known as Gröbner basis computation) for computing the normal 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.

Another major operation in effective algebraic geometry is the projection. It is related to the theory of resultants, that we briefly describe. We present different notions and constructions of resultants and different methods for solving a system of polynomial equations, based on these formulations. 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 applications in computer vision, robotics, computational biology and signal processing.

2 Solving polynomial equations

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

2.1 Analytic solvers

They exploit the value of the functional $\mathbf{f}$ and its derivatives, in order to converge to a solution of $f(\mathbf{x}) = 0$. Typical examples are Newton like methods, Minimization methods, Weierstrass method, [21], [70], [8], [56],

2.2 Homotopic solvers

The idea behind these methods is to deform a system with known roots into the system $f(\mathbf{x}) = 0$ that we want to solve. Examples of such continuation methods are based on projective [50], toric

[47, 76] or generally flat deformation of a polynomial system. See [2] for more details.

2.3 Subdivision solvers

They use an exclusion criterion to remove of a domain if it does not contain a root. These solvers are often use to isolate real roots. Exclusion criterion can be based on Taylor exclusion function [20], interval arithmetic [41], Turan test [60], Sturm method [6, 69], Descartes rule [74, 68, 59].

2.4 Algebraic solvers

They exploit the known relations between the unknowns. They are based on Gröbner basis [19] or normal form computations in a quotient algebra [57, 58] and reduces to a univariate or eigenvalue problem [53].

2.5 Geometric solvers

They project the problem onto a smaller subspace and exploit geometric properties of the solutions. Tools such as resultant constructions [34, 29, 12, 13, 11] are use to reduce the solution of the polynomial system to a univariate or eigenvalue problem.

3 Algebra and Geometry

3.1 The equations and solutions

Let $R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$ be the algebra of polynomials in the variables $\mathbf{x} = (x_1, \ldots, x_n)$ over the field $\mathbb{K}$. Let $f_1, \ldots, f_m \in R = \mathbb{K}[x_1, \ldots, x_n]$ be m polynomial. Our objective is to solve the system $f_1 = 0, \ldots, f_m = 0$. The algebraic closure of $\mathbb{K}$ will be denoted by $\overline{\mathbb{K}}$. The algebraic computation will give us informations on the roots on the algebraic closure. In order to have informations on the reals roots (when $\mathbb{K} = \mathbb{R}$), we will exploit additional sign informations.

3.2 Ideals and varieties

Let I be the ideal generated by these polynomials in the ring R. Let $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ be the set of solutions (with coordinates in $\overline{\mathbb{K}}$) of the system of polynomial equations $f_1 = 0, \ldots, f_m = 0$: $\mathcal{Z}_{\overline{\mathbb{K}}}(I) = \{\zeta \in \overline{\mathbb{K}}^n; f_1(\zeta) = \cdots = f_m(\zeta) = 0\}$. We will also denote this variety by $\mathcal{Z}(I)$. We will assume hereafter that $\mathcal{Z}(I)$ is finite (the system of equations $\mathbf{f} = 0$ has a finite number of solutions) or equivalently [19] that the variety $\mathcal{Z}(I)$ is of dimension 0. Our algebraic approach for solving the polynomial system $f_1 = \cdots = f_m = 0$ (also denoted $\mathbf{f} = 0$) is based on the study of the quotient ring $\mathcal{A}$ that we are going to define in section 4.1.

3.3 The dual

An important ingredient of our methods is the dual space $\widehat{R}$ that is, the space of linear forms $\Lambda : R \to \mathbb{K}$. The *evaluation at a fixed point* ζ is a well-known example of such linear forms: $\mathbf{1}_\zeta : R \to \mathbb{K}$ such that $\forall p \in R$, $\mathbf{1}_\zeta(p) = p(\zeta)$. Another class of linear forms is obtained by using

differential operators. Namely, for any $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, consider the map

$$\begin{array}{rcl} \mathbf{d}^\alpha : R & \to & \mathbb{K} \\ p & \mapsto & \dfrac{1}{\prod_{i=1}^n \alpha_i!} \, (d_{x_1})^{\alpha_1} \cdots (d_{x_n})^{\alpha_n} \, (p)(\mathbf{0}), \end{array} \tag{1}$$

where d_{x_i} is the derivative with respect to the variable x_i. For a moment, we assume that $\mathbb{K}$ is of characteristic 0. We denote this linear form $\mathbf{d}^\alpha = (\mathbf{d}_1)^{\alpha_1} \cdots (\mathbf{d}_n)^{\alpha_n}$ and for any $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n, (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ observe that

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

It immediately follows that $(\mathbf{d}^\alpha)_{\alpha \in \mathbb{N}^n}$ is the dual basis of the primal monomial basis $(\mathbf{x}^\alpha)_{\alpha \in \mathbb{N}^n}$. Notice that $(\mathbf{d}^\alpha)_{\alpha \in \mathbb{N}^n}$ can be defined even in characteristic $\neq 0$. Hereafter, we will assume again that $\mathbb{K}$ is a field of arbitrary characteristic. By applying Taylor's expansion formula at 0, we decompose any linear form $\Lambda \in \widehat{R}$ as $\Lambda = \sum_{\alpha \in \mathbb{N}^n} \Lambda(\mathbf{x}^\alpha) \, \mathbf{d}^\alpha$. The map $\Lambda \to \sum_{\alpha \in \mathbb{N}^n} \Lambda(\mathbf{x}^\alpha) \, \mathbf{d}^\alpha$ defines a one-to-one correspondence between the set of linear forms Λ and the set $\mathbb{K}[[\mathbf{d}_1, \ldots \mathbf{d}_n]] = \mathbb{K}[[\mathbf{d}]] = \{\sum_{\alpha \in \mathbb{N}^n} \Lambda_\alpha \, \mathbf{d}_1^{\alpha_1} \cdots \mathbf{d}_n^{\alpha_n}\}$ of formal power series (*f.p.s.*) in the variables $\mathbf{d}_1, \ldots, \mathbf{d}_n$.

Hereafter, **we will identify $\widehat{R}$ with $\mathbb{K}[[\mathbf{d}_1, \ldots, \mathbf{d}_n]]$**. The evaluation at 0 corresponds to the constant 1, under this definition. It will also be denoted $\mathbf{1_0} = \mathbf{d^0}$.

Example 3.1 The following computation gives the value of the linear form $1 + \mathbf{d}_1 + \mathbf{d}_1\mathbf{d}_2 + {\mathbf{d}_3}^2$ on the polynomial $1 + x_1 + x_1x_2$:

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

Let us next examine the structure of the dual space. We can multiply a linear form by a polynomial ($\widehat{R}$ is an R-module) as follows. For any $p \in R$ and $\Lambda \in \widehat{R}$, we define $p \cdot \Lambda$ as the map $p \cdot \Lambda : R \to \mathbb{K}$ such that $\forall q \in R, p \cdot \Lambda(q) = \Lambda(p\,q)$. For any pair of elements $p \in R$ and for $\alpha_i \in \mathbb{N}, \ \alpha_i \geq 1$, we check that we have $\mathbf{d}_i^{\alpha_i}(x_i\,p)(0) = d_i^{\alpha_i - 1}p(0)$. Consequently, for any pair of elements $p \in R, \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, where $\alpha_i \neq 0$ for a fixed i, we obtain that

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

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, [49]). If $\alpha_i = 0$, then $x_i \cdot \mathbf{d}^\alpha(p) = 0$, which allows us to redefine the product $p \cdot \Lambda$ as follows:

Proposition 3.2 *For any $p \in R$ and any $\Lambda(\mathbf{d}) \in \mathbb{K}[[\mathbf{d}]]$, we have*

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

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

See also [55], [33].

Example 3.1 continued.

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

We check that 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 $1 + x_1 + x_1x_2$.

4 Computing in the quotient algebra

4.1 The quotient algebra

We denote by $\mathcal{A} = R/I$ the quotient algebra of R by I, that is the set of classes of polynomials in R modulo the ideal I. The class of an element $p \in R$, is denoted by $\overline{p} \in \mathcal{A}$. Equality in $\mathcal{A}$ is denoted by $\equiv$ and we have $a \equiv a'$ iff $a - a' \in I$.

The hypothesis that $\mathcal{Z}(I)$ is finite implies that the $\mathbb{K}$-vector space $\mathcal{A}$ is of finite dimension (say D) over $\mathbb{K}$ [19, 27]. As we will see, we will transform the resolution of the non-linear system $\mathbf{f} = 0$, into linear algebra problems in the vector space $\mathcal{A}$, which exploits its algebraic structure. Let us start with an example of computation in the quotient ring $\mathcal{A}$.

Example 4.1 Let I be the ideal of $R = \mathbb{K}[x_1, x_2]$ generated by

$$\begin{aligned} f_1 &:= 13\,x_1^2 + 8\,x_1\,x_2 + 4\,x_2^2 - 8\,x_1 - 8\,x_2 + 2 \\ f_2 &:= x_1^2 + x_1\,x_2 - x_1 - \tfrac{1}{6}. \end{aligned}$$

The quotient ring $\mathcal{A} = \mathbb{K}[x_1, x_2]/I$ is a vector space of dimension 4. A basis of $\mathcal{A}$ is $1, x_1, x_2, x_1x_2$. We check that we have

$$x_1^2 \equiv x_1^2 - f_2 = -x_1x_2 + x_1 + \frac{1}{6}.$$

Similarly,

$$x_1^2x_2 \equiv x_1\,(x_1\,x_2) + \frac{1}{9}\,x_1\,f1 - (\frac{5}{9} + \frac{13}{9}\,x_1 + \frac{4}{9}\,x_2)\,f2) = -x_1x_2 + \frac{55}{54}\,x_1 + \frac{2}{27}\,x_2 + \frac{5}{54}.$$

More generally, any polynomial in $\mathbb{K}[x_1, x_2]$ can be reduced, modulo the polynomials f_1, f_2, to a linear combination of the monomials $1, x_1, x_2, x_1\,x_2$, which as we will see form a basis of $\mathcal{A}$.

Hereafter, $(\mathbf{x}^\alpha)_{\alpha \in E} = \mathbf{x}^E$ will denote a monomial basis of $\mathcal{A}$. Any polynomial can be reduced modulo the polynomials $f_1, \ldots, f_m$, to a linear combination of the monomials of the basis $\mathbf{x}^E$ of $\mathcal{A}$.

Now, let denote by $\widehat{\mathcal{A}}$ the dual space of $\mathcal{A}$. A linear form on $\mathcal{A}$, can be identified with a linear form on R, which vanishes on I. Conversely, any linear form of $\widehat{R}$, which vanishes on I, defines an element of $\widehat{\mathcal{A}}$. Thus we will identify $\widehat{\mathcal{A}}$ and $I^\perp$, the set of elements of $\widehat{R}$ that vanish on I.

Notice for instance that the evaluation $\mathbf{1}_\zeta \in \widehat{\mathcal{A}}$ iff $\zeta \in \mathcal{Z}(I)$. Another interesting linear form $\in \widehat{\mathcal{A}}$ is the trace, denoted hereafter by Tr. We will see its definition in section 5.1 and its use in section 5.3.

Given such a linear form $\Lambda \in \widehat{\mathcal{A}}$, we associate to it, a quadratic linear form as follows:

Definition 4.2 *For any $\Lambda \in \widehat{\mathcal{A}}$, let*

$$\begin{array}{rcl} Q_\Lambda : \mathcal{A} \times \mathcal{A} & \to & \mathbb{K} \\ (a, b) & \mapsto & \Lambda(a\,b). \end{array}$$

Example 4.1 continued. Let Λ be the linear form

$$\Lambda = 2 \times \mathbf{1}_{(-1/3,5/6)} + 2 \times \mathbf{1}_{(1/3,7/6)}.$$

We check that $(-1/3, 5/6)$ and $(1/3, 7/6)$ are in $\mathcal{Z}(f_1, f_2)$. The matrix of Q_Λ in the basis $\{1, x_1, x_2, x_1\,x_2\}$ of $\mathcal{A}$ is

$$[Q_\Lambda] = \begin{bmatrix} \Lambda(1) & \Lambda(x_1) & \Lambda(x_2) & \Lambda(x_1\,x_2) \\ \Lambda(x_1) & \Lambda(x_1^2) & \Lambda(x_1x_2) & \Lambda(x_1^2\,x_2) \\ \Lambda(x_2) & \Lambda(x_1\,x_2) & \Lambda(x_2^2) & \Lambda(x_1\,x_2^2) \\ \Lambda(x_1\,x_2) & \Lambda(x_1^2\,x_2) & \Lambda(x_1x_2^2) & \Lambda(x_1^2x_2^2) \end{bmatrix} = \begin{bmatrix} 4 & 0 & 4 & \frac{2}{9} \\ 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ 4 & \frac{2}{9} & \frac{37}{9} & \frac{4}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \end{bmatrix}$$

Hereafter we will see how to use the signature of Q_{Tr} (and more generally of $Q_{h\cdot Tr}$ for any $h \in R$), in order to get information on the real roots in the case of the real field $\mathbb{K} = \mathbb{R}$.

Algebraic solvers exploit the properties of the quotient algebra $\mathcal{A}$, which means that they require to know how to compute effectively in this quotient. This is performed by a so-called *normal form* algorithm. We are going to describe two approaches to compute such a normal form.

4.2 Gröbner basis

Gröbner basis is a major tool in effective algebraic geometry, which yields algorithmic answers to many question of this domain [19, 5, 1, 25]. It is closely related to the use of a monomial ordering. Let us recall its definition.

Definition 4.3 *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) $\forall (\alpha, \beta, \gamma) \in (\mathbb{N}^n)^3,\ \mathbf{x}^\alpha < \mathbf{x}^\beta \Longrightarrow \mathbf{x}^{\alpha+\gamma} < \mathbf{x}^{\beta+\gamma}$.

Given such an ordering $>$, we define the leading term of a polynomial $p \in R$ as the term of p (the coefficient times its monomial) whose monomial is maximal for $>$. We denote it by $\mathcal{L}_>(p)$. Given an ideal I of $R = \mathbb{K}[\mathbf{x}]$, we also denote by $\mathcal{L}_>(I)$ the set of leading terms of the elements $p \in I$. Because of property (ii), $\mathcal{L}_>(I)$ is a monomial ideal.

By Dickson lemma [19] or by Noetherianity, the ideal $\mathcal{L}_>(I)$ is generated by a finite set of monomials. This naturally leads to the definition of Gröbner bases:

Definition 4.4 *A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subset \mathbb{K}[\mathbf{x}]$ is a Gröbner basis of I for the monomial order $>$, iff we have $\mathcal{L}_>(I) = \big(\mathcal{L}_>(g_1), \ldots, \mathcal{L}_>(g_t)\big)$.*

The interesting property which characterizes a Gröbner basis is the following. For any $p \in R$, let $N(p)$ be the remainder of p by division by G, according to the leading terms of G (see [19]). The polynomial $N(p)$ is such that any of its monomial is not divisible by the monomials $\mathcal{L}_>(g_i)$, $i = 1, \ldots, d$. Then, we have $N(p) = 0$ iff $p \in I$. In addition, the polynomial $N(p)$ is the normal form of p modulo the ideal I. It implies that a basis B of $\mathcal{A} = R/I$ is the set of monomials *which are not in* $\mathcal{L}_>(I)$. This allow us to define the multiplication table by an element $a \in \mathcal{A}$ as follows: we multiply first the elements as usual polynomials and then normalize by reduction by the Gröbner basis G.

Example 4.5 We compute the Gröbner basis of (f_1, f_2) for the degree ordering refined by the lexicographic ordering:

```
> 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 are $x_1\,x_2, x_1^2, x_2^3$. The set of monomials outside $\mathcal{L}_>(I)$ and which forms a basis of $\mathcal{A}$ is $\{1, x_1, x_2, x_2^2\}$. Let us compute the matrix of multiplication by x_1 in this basis, using our Gröbner basis `G`.

```
> 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]]);
```

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

Efficient algorithms have been developed over these decades to compute Gröbner bases. We mention in particular [32], [37], [39], [65].

4.3 General normal form

Unfortunately, the construction of Gröbner bases is not numerically stable as shown on the following example:

Example 4.6 Consider first the system:

```
> f1 := x[1]^2+x[2]^2 -x[1]+x[2]-2;
> f2 := x[1]^2-x[2]^2 + 2*x[2]-3;
> 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 are x_1^2, x_2^2 and the corresponding monomial basis of $\mathcal{A}$ is $\{1, x_1, x_2, x_1\,x_2\}$ Consider now a small perturbation:

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

$$\begin{aligned}[-2\,{x_2}^2+x_1+x_2-1+0.0000001\,x_1x_2,&\\ {x_1}^2+{x_2}^2-\,x_1+x_2-2,&\\ {x_2}^3-10000000.&99999999999995000000000000125\,{x_2}^2\\ +5000000.&25000001249999937499996875000156250000781250\,x_1\\ +5000000.&75000003749999312499990625001718750023437 50\,x_2\\ -5000000.&25000006249999937499984375000156250039062 50\end{aligned}$$

The leading monomials are now $x_1\,x_2, x_1^2, x_2^3$ and the corresponding basis of $\mathcal{A}$ is $\{1, x_1, x_2, x_2^2\}$. As we see on this simple example, in the result of a small perturbation, basis may "jump" from one set of monomials to another, though the two set of solutions are very closed to each other from a geometric point of view. Moreover, some of the polynomials of the Gröbner basis have large coefficients.

Thus, Gröbner basis computations may introduce artificial discontinuities, due to the choice of a monomial order. A recent generalization of these normal form computation has been proposed in [54, 57]. This construction is based on a new criterion, which gives a necessary and sufficient condition for a projection onto this set of polynomials, to be a normal form modulo the ideal I. It can be reformulated as follows:

Theorem 4.7 *Let B be a vector space of R connected to 1[1]. Let $B^+ = B \cup x_1 B \cup \cdots \cup x_n B$ $N : B^+ \to B$ be a $\mathbb{K}$-linear map such that $N_{|B} = \mathbb{I}_B$ is the identity on B. Let $I = (\ker(N))$ be the ideal generated by the kernel of N. We define*

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

The two properties are equivalent:

1. *For all $1 \leq i, j \leq n$, $M_i \circ M_j = M_j \circ M_i$.*
2. *$R = B \oplus I$.*

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

This leads to a completion-like algorithm which starts with the vector space $K_0 = \langle f_1, \ldots, f_m \rangle$ generated by the polynomials that we want 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 [54, 57] for more details. This approach allows us to fix first the set of monomials in which we want to do linear operations and thus allows us to treat more safely polynomials with approximate coefficients. It can be adapted very naturally to Laurent polynomials, which is not the case for Gröbner basis computation. 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 [57].

Example 4.8 For the perturbed polynomial of the previous example, we get the normal forms for the monomial on the border of B:

$$\begin{array}{l} x_1^2 = -0.00000005\, x_1 x_2 + 1/2\, x_1 - 3/2\, x_2 + 5/2 \\ x_2^2 = +0.00000005\, x_1 x_2 + 1/2\, x_1 + 1/2\, x_2 - 1/2 \\ {x_2 x_1}^2 = 0.49999999\, x_1 x_2 - 0.74999998\, x_1 + 1.75000003\, x_2 + 0.74999994, \\ {x_1 x_2}^2 = 0.49999999\, x_1 x_2 - 0.25000004\, x_1 - 0.74999991\, x_2 + 1.25000004] \end{array}$$

This set of relations yields directly the matrices of multiplication by the variables x_1, x_2 in $\mathcal{A}$.

5 Solving from the structure of $\mathcal{A}$

In this section, we see how to recover the solutions from the structure of $\mathcal{A}$.

5.1 The multiplication operators

The first operator that comes naturally in the study of $\mathcal{A}$ is the operator of multiplication by an element of $a \in \mathcal{A}$. For any element $a \in \mathcal{A}$, we define the map

$$\begin{array}{rcl} M_a : \mathcal{A} & \to & \mathcal{A} \\ b & \mapsto & a\, b. \end{array}$$

[1] Any monomial $m \in B$ is of the form $x_{i_1} m'$ with $m' \in B$.

We will also consider the transposed operator

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

The matrix associated to this operator in the dual basis of a basis of $\mathcal{A}$ is the transposed of the matrix of M_a in this basis.

Example 5.1 Let us compute the matrix of multiplication by x_1 in the basis $(1, x_1, x_2, x_1x_2)$ of $\mathcal{A} = \mathbb{K}[x_1, x_2]/(f_1, f_2)$, where f_1, f_2 are the polynomials of example 4.1. We multiply these monomials by x_1 and reduce them to a normal form. According to the computations of example 4.1, we have:

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

We deduce that

$$M_{x_1} = \begin{bmatrix} 0 & \frac{1}{6} & 0 & \frac{5}{54} \\ 1 & 1 & 0 & \frac{55}{54} \\ 0 & 0 & 0 & \frac{2}{27} \\ 0 & -1 & 1 & -1 \end{bmatrix}.$$

The multiplication map can be computed, when a normal form algorithm is available. This can be performed, for instance, by Gröbner basis computations (see section 4.2 and its generalization in section 4.3). In section 6, we will describe another way to compute implicitly the multiplication maps, based on resultant matrix computations.

Our matrix approach is based on the following fundamental theorem (see [4], [53], [71]):

Theorem 5.2 *Assume that* $\mathcal{Z}_{\overline{\mathbb{K}}^n}(I) = \{\zeta_1, \ldots, \zeta_d\}$.

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

Notice that if $(\mathbf{x}^\alpha)_{\alpha \in E}$ is a monomial basis of $\mathcal{A}$, then the coordinates of the evaluation $\mathbf{1}_{\zeta_i}$ in the dual basis of $(\mathbf{x}^\alpha)_{\alpha \in E}$ are $(\zeta_i^\alpha)_{\alpha \in E}$ where $\zeta^\alpha = \mathbf{1}_\zeta(\mathbf{x}^\alpha)$. Thus, if the basis $(\mathbf{x}^\alpha)_{\alpha \in E}$ contains $1, x_1, \ldots, x_n$ (which is often the case), the coordinates $[v_\alpha]_{\alpha \in E}$ (in the dual basis) of the eigenvectors of $M_a^{\mathbf{t}}$ yield all the coordinates of the root: $\zeta = [\frac{v_{x_1}}{v_1}, \ldots, \frac{v_{x_n}}{v_1}]$. It leads to the following algorithm:

Algorithm 5.3 Solving in the case of simple roots.

Let $a \in R$ *and* $\mathtt{M}_a$ *be the matrix of multiplication in a 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* $\mathtt{M}_a^{\mathbf{t}}$.
2. *For each eigenvector* Λ *with* $\Lambda_1 \neq 0$*, compute and output* $\zeta = \left(\frac{\Lambda_{x_1}}{\Lambda_1}, \ldots, \frac{\Lambda_{x_n}}{\Lambda_1}\right)$.

The set of output points ζ contains the set of simple roots of $\mathcal{Z}(I)$, since for such roots the eigenspace is one-dimensional. But as we will see on the next example, it can also yield in some cases[2] the multiple roots :

[2] depending on the type of multiplicity

Example 4.1 continued. We compute the eigenvalues, their multiplicity, and the corresponding normalized eigenvector of the transposed of the matrix of multiplication by x_1:

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

$$[-\frac{1}{3}, 2, \left\{[1, -\frac{1}{3}, \frac{5}{6}, -\frac{5}{18}]\right\}], [\frac{1}{3}, 2, \left\{[1, \frac{1}{3}, \frac{7}{6}, \frac{7}{18}]\right\}].$$

As the basis chosen for the computation is $(1, x_1, x_2, x_1x_2)$, the previous theorem tells us that the solutions of the system can be read off, from the 2^{nd} and the 3^{rd} coordinates of the normalized eigenvectors: $\zeta_1 = (-\frac{1}{3}, \frac{5}{6})$ and $\zeta_2 = (\frac{1}{3}, \frac{7}{6})$. Moreover, the 4^{th} coordinate of these vectors is the product of the 2^{nd} by the 3^{rd} coordinates.

In order to compute exactly the set of roots, counted with their multiplicity, we exploit the following theorem. It is based on the fact that commuting matrices share common eigenspaces.

Theorem 5.4 *[53, 55, 18] There exists a basis of $\mathcal{A}$ such that $\forall a \in R$, the matrix M_a is, in this basis, of the form*

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

Here again, it leads to an algorithm:

Algorithm 5.5 SOLVING BY SIMULTANEOUS TRIANGULATION.

Input: The matrices of multiplication $\mathtt{M}_{x_i}$ $(i = 1, \ldots, n)$ in a basis of $\mathcal{A}$.

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

The first step is performed by computing a ordered Schur decomposition of M_l (where l is a generic linear form) which yields a matrix P of change of basis. Next, we compute the matrices $\mathtt{T}_{x_i} = \mathtt{P}\mathtt{M}_{x_i}\mathtt{P}^{-1}$ $(i = 1, \ldots, n)$ which are triangular, since they commute with M_l. The decomposition of the multiplication operators in theorem 5.4 is in fact induced by a decomposition of the algebra

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

where $\mathcal{A}_i$ is the local algebra associated with the root ζ_i. More precisely, there exists elements $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathcal{A}$, such that $i, j = 1, \ldots, d$

$$\begin{cases} \mathbf{e}_i^2 \equiv \mathbf{e}_i, \\ \mathbf{e}_i\mathbf{e}_j \equiv 0, i \neq j \\ \mathbf{e}_1 + \cdots + e_d \equiv 1 \end{cases}$$

These polynomials, which generalist the univariate Lagrange polynomials, are called the fundamental idempotents of $\mathcal{A}$. They are such that $\mathcal{A}_i = \mathbf{e}_i\,\mathcal{A}$ 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 the *multiplicity* μ_{ζ_i} of ζ_i. See [75, 53, 27].

5.2 The Chow form and the rational representation of the roots

In some problems, it is important to have an exact representation of the roots. As the coordinates of these roots are algebraic numbers, we will represent them in terms of the roots of a univariate polynomial. More precisely, they will be the image of such roots by a rational map. It is the aim of the foregoing developments, to show how to construct explicitly such a representation.

Definition 5.6 *The Chow form of $\mathcal{A}$ is the homogeneous polynomial in $\mathbf{u} = (u_0, \ldots, u_n)$ of degree D, defined by:*

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

According to theorem 5.4, we have

Theorem 5.7 *The Chow form of $\mathcal{A}$ is*

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

Example 6.1 continued. We compute the Chow form of the variety $I = (f_1, f_2)$, using the matrices of multiplication by x_1 and x_2, computed previously.

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

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

We check that it is a product of linear forms, whose coefficients yield the roots $\zeta_1 = (-\frac{1}{3}, \frac{5}{6})$ and $\zeta_2 = (\frac{1}{3}, \frac{7}{6})$. The exponents yield the multiplicity of the roots (here 2). As here the roots are rational, we can easily factories this polynomial as a product of linear forms. But usually, this factorization is possible only on an algebraic extension of the coefficient field. From this Chow form, it is possible to deduce a rational representation of the points of $\mathcal{Z}(I)$:

Theorem 5.8 *Let $\Delta(\mathbf{u})$ be a multiple of the Chow form $\mathcal{C}(\mathbf{u})$. Then for a generic vector $\mathbf{t} \in \mathbb{K}^{n+1}$ we have*

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

where $d_i(u_0) \in \mathbb{K}[u_0], R(u) \in (u_1, \ldots, u_n)^2$, $\gcd\big(d_0(u_0), d_0'(u_0)\big) = 1$ and for all $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathcal{Z}_0$,

$$\zeta_i = \frac{d_i(\zeta_0)}{d_0'(\zeta_0)} \quad , \quad i = 1, \ldots, n\ ,$$

for some root ζ_0 of $d_0(u_0)$.

See also [64, 3, 67, 26, 46]. This result describes the coordinates of the points of $\mathcal{Z}_0$ 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 $\mathcal{Z}_0$, so that this representation may be redundant. However the redundant factors can be removed by substituting the rational representation back into the equations $f_1, \ldots, f_n$. It leads to the following algorithm :

Algorithm 5.9 UNIVARIATE RATIONAL REPRESENTATION

INPUT: *a* multiple $\Delta(\mathbf{u})$ *of the Chow form* $I \subset R$.

1. *Compute the square free part of* $\Delta(u)$.
2. *Choose a generic* $\mathbf{t} \in \mathbb{K}^{n+1}$ *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* $\zeta_1 = \frac{d_1(u_0)}{d_0'(u_0)}$, $\ldots$, $\zeta_n = \frac{d_n(u_0)}{d_0'(u_0)}$, $d_0(u_0) = 0$.
4. *Factories* $d_0(u_0)$, *keep the good prime factors and output the corresponding simplified rational univariate representations of the roots* $\mathcal{Z}(I)$.

In the last step, for each prime factors of $d_0(u_0)$, we compute the remainder r_i and r_0, respectively of degree d_i and d_0' and check if $f_i(\frac{r_1}{r_0}(u_0), \ldots, \frac{r_n}{r_0}(u_0))$ vanishes for $i = 1, \ldots, m$.

Example 5.10 From the Chow form of the last example, we deduce:

$$\xi_1 = -\frac{1}{6\,(1+u_0)},\ \xi_2 = \frac{11+12\,u_0}{12\,(1+u_0)},\ \left(u_0+\frac{3}{2}\right)\left(u_0+\frac{1}{2}\right) = 0.$$

which reduces to the constant representations

$$\begin{cases} u_0 = -3/2, x_1 = 1/3, x_2 = 5/6 \\ u_0 = -1/2, x_1 = -1/3, x_2 = 7/6 \end{cases}$$

5.3 Real roots and radical

Let suppose now that the input polynomials have real coefficients: $f_i \in \mathbb{R}[\mathbf{x}]$, $i = 1, \ldots, m$. A natural question, which may arise in many practical problems is *how many real solutions this polynomial system has ?* In order to answer it, we will use the properties of the following linear form:

Definition 5.11 *The linear form* Tr *is defined over* $\mathbb{K}$ *by*

$$\begin{array}{rcl} \mathrm{Tr} : R & \to & \mathbb{K} \\ a & \mapsto & trace(M_{\overline{a}}), \end{array}$$

where $trace(M_{\overline{a}})$ *is the usual trace of the linear operator* $M_{\overline{a}}$.

According to theorem 5.4, we also have

$$\forall a \in \mathcal{A},\ Tr(a) = \sum_{\zeta \in \mathcal{Z}(I)} \mu_\zeta\, a(\zeta)$$

where μ_ζ is the multiplicity of ζ.

Example 5.12

$$\mathrm{Tr}(x_1) = trace\left(\begin{bmatrix} 0 & \frac{1}{6} & 0 & \frac{5}{54} \\ 1 & 1 & 0 & \frac{55}{54} \\ 0 & 0 & 0 & \frac{2}{27} \\ 0 & -1 & 1 & -1 \end{bmatrix}\right) = 0$$

By theorem 5.4, this linear form can also be defined by $Tr = 2 \times \mathbf{1}_{(-1/3,5/6)} + 2 \times \mathbf{1}_{(1/3,7/6)}$.

To this *linear form* $\mathrm{Tr} \in \widehat{\mathcal{A}}$ and for any element h in $\mathcal{A}$, we associate the *quadratic form*:

$$Q_{h\cdot\mathrm{Tr}} : (a, b) \mapsto \mathrm{Tr}(hab)$$

with which we analyze the number of real roots.

Theorem 5.13 (Hermite) *Let $h \in \mathbb{R}[\mathbf{x}]$. Then we have*

1. *The rank of the quadratic form Q_h is the number of distinct (complex) roots ζ such that $h(\zeta) \neq 0$.*
2. *The signature of Q_h is $\#\{\ \zeta$ real with $h(\zeta) > 0\ \} - \#\{\ \zeta$ real with $h(\zeta) < 0\ \}$*

See [62, 36]. In particular, if $h = 1$, the rank of Q_1 is the number of distinct roots and its signature is the number of real roots. This allow us to analyze more closely the geometry of the real roots, as it is illustrated now.

Example 5.14 By a direct computation, we get $Tr(1) = 4,\ Tr(x_1) = 0,\ Tr(x_2) = 4, Tr(x_1x_2) = \frac{2}{9}$ and we deduce the value of the linear form Tr on the other interesting monomials by using the transposed operators $\mathtt{M}_{x_i}^{\mathtt{t}}$ 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]);
```

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

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

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

$$2, \quad [2, 0], \quad 2, \quad [1, 1],$$

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

6 Resultant constructions

Projection is one of the more used operation in Effective Algebraic Geometry [25, 19]. It allows to reduce the dimension of the problem that we have to solve and often to simplify it. The resultant is a tool to perform it and has many applications in this domain. It leads in particular to efficient methods for solving polynomial equations, based on matrix formulations [29]. We are going to present here several notions and constructions of these resultants.

Before considering the multivariate case, let us first recall the construction of the well-known Sylvester matrix in the univariate case. Given two univariate polynomials, $f_0 = f_{0,0} + \cdots + f_{0,d_0}\, x^{d_0}$ of degree d_0 and $f_1 = f_{1,0} + \ldots + f_{1,d_1}\, x^{d_1}$ of degree d_1, let $\mathtt{S}$ be the matrix of

$$f_0, x\, f_0, \ldots, x^{d_1-1}\, f_0, f_1, x\, f_1, \ldots, x^{d_0-1}\, f_1$$

in the monomial basis $\{1, \ldots, x^{d_0+d_1-1}\}$. This matrix is called the Sylvester matrix of f_0 and f_1. Let $\mathcal{V}_0, \mathcal{V}_1$, and $\mathcal{V}$ denote the vector spaces generated by the monomials $\{1, \ldots, x^{d_1-1}\}$, $\{1, \ldots, x^{d_0-1}\}$, and $\{1, \ldots, x^{d_0+d_1-1}\}$, respectively. Then, the Sylvester matrix is the matrix of the map $\mathcal{S} : \mathcal{V}_0 \times \mathcal{V}_1 \to \mathcal{V}$ such that $\forall (q_0, q_1) \in \mathcal{V}_0 \times \mathcal{V}_1,\ \mathcal{S}(q_0, q_1) = f_0\, q_0 + f_1\, q_1$, in the corresponding monomial bases. The determinant of this $(d_0+d_1) \times (d_0+d_1)$ matrix is the *resultant* $\mathrm{Res}(f_0, f_1)$ of f_0 and f_1. It vanishes iff f_0 and f_1 have a common root (in $\overline{\mathbb{K}}$), assuming that $f_{0,d_0} \neq 0, f_{1,d_1} \neq 0$. Thus, we have projected the problem of a common root of the two polynomials onto a problem in the space of coefficients $\mathrm{Res}(f_0, f_1) = 0$.

We can generalize this approach to the multivariate case as follows: let $f_0, f_1, \ldots, f_n \in R$ be $n+1$ polynomials in n variables, of degree $d_0, \ldots, d_n$. The matrices used to construct resultants, as in the work of F.S. Macaulay [48] for instance, are matrices associated to maps of the form:

$$\begin{array}{rcl} \mathcal{S} : \mathcal{V}_0 \times \cdots \times \mathcal{V}_n & \to & \mathcal{V} \\ (q_0, \ldots, q_n) & \mapsto & \displaystyle\sum_{i=0}^{n} f_i\, q_i. \end{array} \tag{2}$$

where $\mathcal{V}_i = \langle \mathbf{x}^{E_i} \rangle$ is a vector space generated by a finite number of monomials. We denote by E_i the set of exponents of these monomials: $E_i = \{\beta_{i,1}, \beta_{i,2}, \ldots\}$. The vector space $\mathcal{V} = \langle \mathbf{x}^{F} \rangle$ is also a vector space generated by monomials, whose exponents are in the set F. The matrix of this map, in the canonical monomial bases, is obtained as follows. The image of an element $(0, \ldots, 0, \mathbf{x}^{\beta_{i,j}}, 0, \ldots, 0)$ is the polynomial $\mathbf{x}^{\beta_{i,j}}\, f_i$. Its expansion in the monomial basis of $\mathcal{V}$ gives the corresponding column of the matrix of $\mathcal{S}$. The matrix of $\mathtt{S}$ can be divided into blocks $[\mathtt{S}_0, \mathtt{S}_1, \ldots, \mathtt{S}_n]$:

$$\begin{array}{c} \\ \mathcal{V} \left\{ \begin{array}{l} \mathbf{x}^{\alpha_1} \\ \cdot \\ \cdot \\ \cdot \\ \mathbf{x}^{\alpha_N} \end{array} \right. \end{array} \begin{array}{c} \overbrace{\phantom{\mathbf{x}^{\beta_{0,1}} f_0 \quad \cdots}}^{\mathcal{V}_0} \quad \overbrace{\phantom{\mathbf{x}^{\beta_{1,1}} f_1 \quad \cdots}}^{\mathcal{V}_1} \qquad\qquad \overbrace{\phantom{\mathbf{x}^{\beta_{n,1}} f_n \quad \cdots}}^{\mathcal{V}_n} \\ \left[\begin{array}{c|c|c|c} \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \mathbf{x}^{\beta_{0,1}} f_0 \quad \cdots & \mathbf{x}^{\beta_{1,1}} f_1 \quad \cdots & \cdots\cdots\cdots & \mathbf{x}^{\beta_{n,1}} f_n \quad \cdots \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \end{array} \right]. \end{array} \tag{3}$$

The columns of the block $\mathtt{S}_i$ correspond to the multiples of f_i expressed in the monomial basis $\mathbf{x}^F$.

6.1 Projective resultant

Let $\nu_0 = \sum_{i=0}^{n} d_i - n$ and let R_k be the set of polynomials in R, of degree $\leq k$. In order to construct the resultant of these polynomials (in fact the homogenization f_i^h of these polynomials), F.S Macaulay [48] took for $\mathcal{V}_i$ a vector space $\mathcal{V}_i = \langle \mathbf{x}^{E_i} \rangle \subset R_{\nu - d_i}$ generated by some of the monomials of degree $\leq \nu - d_i$, and for $\mathcal{V}$ the vector space $\mathcal{V} = \langle \mathbf{x}^F \rangle = R_\nu$ of polynomials of degree $\leq \nu$. The construction is such that when $f_0 = 1$ and $f_i = x_i^{d_i}$ we get the identity matrix. We illustrate this construction for 3 polynomials in 2 variables.

Example 6.1 Let us compute the Macaulay matrix associated to the polynomials f_1, f_2 of example 4.1, and a generic linear form $f_0 = u_0 + u_1 x_1 + u_2 x_2$:

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

$$\left[\begin{array}{cccc|ccc|ccc} u_0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & -\frac{1}{6} \\ u_2 & u_0 & 0 & 0 & 2 & 0 & -8 & 0 & -\frac{1}{6} & 0 \\ u_1 & 0 & u_0 & 0 & 0 & 2 & -8 & -\frac{1}{6} & 0 & -1 \\ 0 & u_1 & u_2 & u_0 & -8 & -8 & 8 & 0 & -1 & 1 \\ \hline 0 & 0 & u_1 & 0 & 0 & -8 & 13 & -1 & 0 & 1 \\ 0 & u_2 & 0 & 0 & -8 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 13 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u_1 & 13 & 8 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & u_2 & 8 & 4 & 0 & 0 & 1 & 0 \end{array}\right].$$

We have

$$\begin{array}{rcl} E_2 & = & \{1, x_1, x_2\}, \\ E_1 & = & \{1, x_1, x_2\}, \\ E_0 & = & \{1, x_1, x_2, x_1 x_2\}, \\ F & = & \{1, x_1, x_2, x_1\,x_2, x_1^2, x_1^3, x_1^2 x_2, x_2^2, x_1 x_2^2, x_2^3\}. \end{array}$$

When $n = 1$, this construction yields the Sylvester matrix of the two polynomials f_0, f_1. F.S. Macaulay has shown [48] that the resultant of the homogenized polynomials $f_0^h, \ldots, f_n^h$ is the ratio of the determinant of `S` by another subminor of `S`. The matrix `S` may be degenerate, independently of f_0. This is the case, for instance, when the number of isolated roots of $\mathcal{Z}(f_1, \ldots, f_n)$, counted with multiplicities, is not the bound $\prod_{i=1}^{n} d_i$, given by Bezout's theorem. If we are not in this degenerate situation, we will say that $f_1, \ldots, f_n$ is a *generic* system for Macaulay's construction. A fundamental property of this construction is that for generic systems $f_1, \ldots, f_n$, the set of monomials $\mathbf{x}^{E_0}$ is a basis of $\mathcal{A} = R/(f_1, \ldots, f_n)$ [48].

6.2 Toric resultant

A refined notion of resultants (on toric varieties) has been studied recently, which takes into account the actual monomials appearing in the polynomials f_i. Its construction follows the same process as in the previous section, except that the notion of degree is changed. We consider $n+1$ Laurent polynomials $f_0, \ldots, f_n \in L = \mathbb{K}[t_1^{\pm 1}, \ldots, t_n^{\pm 1}]$, and we replace the constrains on the degree by constrains on the support[3] of the polynomials [34, 72, 28]: Let fix a polytope $A_i \subset \mathbb{Z}^n$ and assume that the support of f_i is in A_i:

$$f_i = \sum_{\alpha \in A_i} c_{i,\alpha}\, \mathbf{t}^\alpha.$$

[3]The support of $p = \sum_\alpha c_\alpha \mathbf{x}^\alpha$ is the set of $\alpha \in \mathbb{Z}^n$ such that $c_\alpha \neq 0$

We denote by A the Minkowski sum of these polytopes ($A = A_0 \oplus \cdots \oplus A_n$), to which we associate the toric variety $\mathcal{T}_A$ as follows. We consider the map

$$\begin{array}{rcl} \sigma : (\mathbb{K}^*)^n & \to & \mathbb{P}^N \\ \mathbf{t} & \mapsto & \left(\mathbf{t}^{\alpha_0} : \cdots : \mathbf{t}^{\alpha_N}\right) \end{array}$$

where $A = \{\alpha_0, \ldots, \alpha_N\} \subset \mathbb{Z}^n$. The closure of its image is the Toric variety $\mathcal{T}_A$. The toric resultant is the necessary and sufficient condition on the coefficients of the polynomials $f_i, i = 0, \ldots, n$, such that they have a common root in $\mathcal{T}_A$.

Let us fix a vector $\delta \in \mathbb{Q}^n$. For any polytope C, we denote by C^δ, the set of points in $C \cap \mathbb{Z}^n$, when we remove all the facets, for which the inner-product of the normal with δ is negative. Let $\mathcal{V}_i$ be the vector space generated by a certain subset of the monomials $\mathbf{x}^\beta$ with $\beta \in (\oplus_{j \neq i} A_j)^\delta$ and $\mathcal{V}$ is the vector space generated by $\mathbf{x}^\alpha$, with $\alpha \in F = (\oplus_{i=0}^n A_i)^\delta$. This define a map $\tilde{\mathcal{S}}$ and matrix $\tilde{\mathrm{S}}$, from which a square matrix is deduced [15]. Its determinant is a non-zero multiple of the toric resultant over $\mathcal{T}_A$.

Example 6.2 We consider the system

$$\left\{ \begin{array}{l} f_0 = c_{0,0} t_1 t_2 + c_{0,1} t_1 + c_{0,2} t_2 + c_{0,3}, \\ f_1 = c_{1,0} t_1 t_2 + c_{1,1} t_1 + c_{1,2} t_2 + c_{1,3}, \\ f_2 = c_{2,0}, {t_1}^2 + c_{2,1} {t_2}^2 + c_{2,1} t_1 + c_{2,2} t_2 + c_{2,3}. \end{array} \right.$$

A resultant matrix, which yields a multiple of the toric resultants and computed by the algorithm described in [15] is

```
> S:= spresultant([f0,f1,f2],[t[1],t[2]]);
```

$$\left[\begin{array}{cccc|cccccc|ccc} c_{0,3} & 0 & 0 & 0 & c_{1,3} & 0 & 0 & 0 & 0 & c_{2,3} & 0 & 0 \\ c_{0,2} & c_{0,3} & 0 & 0 & c_{1,2} & c_{1,3} & 0 & 0 & 0 & c_{2,2} & 0 & 0 \\ 0 & 0 & c_{0,3} & 0 & 0 & 0 & c_{1,3} & 0 & 0 & 0 & c_{2,3} & 0 \\ c_{0,1} & 0 & c_{0,2} & c_{0,3} & c_{1,1} & 0 & c_{1,2} & c_{1,3} & 0 & c_{2,1} & c_{2,2} & c_{2,3} \\ 0 & 0 & c_{0,1} & 0 & 0 & 0 & c_{1,1} & 0 & c_{1,3} & 0 & c_{2,1} & 0 \\ c_{0,0} & c_{0,1} & 0 & c_{0,2} & c_{1,0} & c_{1,1} & 0 & c_{1,2} & 0 & 0 & c_{2,1} & c_{2,2} \\ 0 & c_{0,0} & 0 & 0 & 0 & c_{1,0} & 0 & 0 & 0 & 0 & 0 & c_{2,1} \\ 0 & c_{0,2} & 0 & 0 & 0 & c_{1,2} & 0 & 0 & 0 & c_{2,1} & 0 & 0 \\ 0 & 0 & c_{0,0} & c_{0,1} & 0 & 0 & c_{1,0} & c_{1,1} & c_{1,2} & c_{2,0} & 0 & c_{2,1} \\ 0 & 0 & 0 & c_{0,0} & 0 & 0 & 0 & c_{1,0} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{1,1} & 0 & c_{2,0} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{1,0} & 0 & 0 & c_{2,0} \end{array}\right]$$

We observe that there are 4 columns in f_0, which is also the generic number of roots of $f_1 = 0, f_2 = 0$.

The construction will not be degenerate, when *the polynomials $f_1, \ldots, f_n$ intersect properly, in the underlying projective toric variety.* In this case, we will say that the system $f_1, \ldots, f_n$ is *generic* for this construction. In this case, the dimension of $\mathcal{A}$ is the mixed-volume of the polytopes of $f_1, \ldots, f_n$ [34]. Here, again we have the property that for generic systems $f_1, \ldots, f_n$ with support respectively in $A_1, \ldots, A_n$, the set of monomials $\mathbf{x}^{E_0}$ is a basis of $\mathcal{A} = R/(f_1, \ldots, f_n)$ [61, 30].

6.3 Resultant over a unirational variety

A natural extension of the toric case consists in replacing the monomial parameterization by "any" rational one. The input system, also defined on an open subset of $\mathbb{K}^n$ is of the form

$$\mathbf{f_c} := \left\{ \begin{array}{rcl} f_0(\mathbf{t}) & = & \sum_{j=0}^{k_0} c_{0,j}\, \kappa_{0,j}(\mathbf{t}) \\ \vdots & & \\ f_n(\mathbf{t}) & = & \sum_{j=0}^{k_n} c_{n,j}\, \kappa_{n,j}(\mathbf{t}) \end{array} \right. \tag{4}$$

where $\mathbf{t} = (t_1, \ldots, t_n)$ and the $\kappa_{i,j}$ are non-zero rational functions, which we can assume to be polynomials by reduction to the same denominator.

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

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

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

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

Let X^o be the image of σ and X its closure in $\mathbb{P}^N$. We are looking for conditions on the coefficients $\mathbf{c} = (c_{i,j})$ such that the "homogenized" system has a root in X. Under the following hypotheses:

$$(\mathbf{D}) \left\{ \begin{array}{l} \text{the Jacobian matrix of } \sigma = (\sigma_i)_{i=0,\ldots,N} \text{ is of rank } n \text{ at one point of } U, \\ \text{for generic } \mathbf{c},\ f_1 = \cdots = f_n = 0 \text{ has a finite number of solutions in } U, \end{array} \right.$$

it is proved in [12], that the resultant $\mathrm{Res}_X(\mathbf{f_c})$ can be defined. In order to compute a non-trivial multiple of this resultant, we use the Bezoutian matrix defined as follows.

Definition 6.3 *The Bezoutian $\Theta_{f_0,\ldots,f_n}$ of $f_0, \ldots, f_n \in R$ is the element of $R \otimes_{\mathbb{K}} R$ defined by*

$$\Theta_{f_0,\ldots,f_n}(\mathbf{x},\mathbf{z}) := \begin{vmatrix} f_0(\mathbf{x}) & \theta_1(f_0)(\mathbf{x},\mathbf{z}) & \cdots & \theta_n(f_0)(\mathbf{x},\mathbf{z}) \\ \vdots & \vdots & \vdots & \vdots \\ f_n(\mathbf{x}) & \theta_1(f_n)(\mathbf{x},\mathbf{z}) & \cdots & \theta_n(f_n)(\mathbf{x},\mathbf{z}) \end{vmatrix},$$

where $\mathbf{z} = (z_1, \ldots, z_n)$ and

$$\theta_i(f_j)(\mathbf{x},\mathbf{z}) := \frac{f_j(z_1, \ldots, z_{i-1}, x_i, \ldots, x_n) - f_j(z_1, \ldots, z_i, x_{i+1}, \ldots, x_n)}{x_i - z_i}.$$

Let $\Theta_{f_0,\ldots,f_n}(\mathbf{x},\mathbf{z}) = \sum \theta_{\alpha\beta}\, \mathbf{x}^\alpha \mathbf{z}^\beta, \theta_{\alpha,\beta} \in \mathbb{K}$. The Bezoutian matrix of $f_0, \ldots, f_n$ is the matrix $B_{f_0,\ldots,f_n} = (\theta_{\alpha\beta})_{\alpha,\beta}$.

The Bezoutian was initially used by E. Bézout to construct the resultant of two polynomials in one variable [7].

In the multivariate case, we have the following property.

Theorem 6.4 *[12] Assume that the conditions* **(D)** *are satisfied. Then any maximal minor of the Bezoutian matrix $B_{f_0,\ldots,f_n}$ is divisible by the resultant* $\mathrm{Res}_X(\mathbf{f_c})$.

This leads us to an algorithm for computing a non-trivial multiple of generalized resultant, that we illustrate below:

Example 6.5 Here is an example where the classical and toric resultants are degenerate. Consider the three following polynomials:

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

We are looking for conditions on the coefficients $c_{i,j}$ such that these three polynomials have a common "root". The resultant of these polynomials over $\mathbb{P}^2$ is zero (whatever the values of $(c_{i,j})$ are), for the homogenized polynomials f_0^h, f_1^h, f_2^h vanish at the points $(0:1:\mathbf{i})$ and $(0:1:-\mathbf{i})\big)$. For the same reason, the toric resultant also vanishes (these polynomials have common roots in the associated toric variety). Now applying the previous results, we consider the map

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

whose Jacobian is of rank 2. Let

$$\begin{array}{rcl} \psi_0 & = & (x_0, x_1, x_2, x_3) \\ \psi_1 & = & (x_0^2, x_0x_1, x_0x_2, x_0x_3, x_3^2) \\ \psi_2 & = & (x_0^2, x_0x_1, x_0x_2, x_0x_3, x_3^2) \end{array}$$

where $(x_0 : x_1 : x_2 : x_3)$ are the homogeneous coordinates of $\mathbb{P}^3$. 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 $\mathbb{K}^2$, and so that by theorem 6.4, 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]);
```

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

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

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 [52]), $\mathrm{Res}_X(f_0, f_1, f_2)$ is homogeneous of degree 4 in the coefficients of each f_i. Thus, $\mathrm{Res}_X(f_0, f_1, f_2)$ corresponds to the last factor ρ.

6.4 Residual resultant

In many situations coming from practical problems, the equations have commons zeroes which are independent of the parameters of the problems, and which are not interesting. We are going to

present here a resultant construction, which allows us to remove these degenerated solutions, when they form a complete intersection [13] (see also [10, 16]).

Let $g_1, \ldots, g_r$ be r homogeneous polynomials of degree $k_1 \geq \ldots \geq k_r$ in $R = \mathbb{K}[x_0, \ldots, x_n]$ and $d_0 \geq \ldots \geq d_n$ be $n+1$ integers such that $d_n \geq k_1$ and $r \leq n+1$. We suppose that $(g_1, \ldots, g_r)$ is a complete intersection and that $d_n \geq k_r + 1$. We consider the following system:

$$\mathbf{f_c} := \left\{ \begin{array}{rcl} f_0(\mathbf{x}) & = & \sum_{i=1}^{r} h_{i,0}(\mathbf{x})\, g_i(\mathbf{x}) \\ \vdots & & \\ f_n(\mathbf{x}) & = & \sum_{i=1}^{r} h_{i,n}(\mathbf{x})\, g_i(\mathbf{x}) \end{array} \right. \tag{5}$$

where $h_{i,j}(\mathbf{x}) = \sum_{|\alpha|=d_j-k_i} c_\alpha^{i,j}\, \mathbf{x}^\alpha$ is generic homogeneous polynomial of degree $d_j - k_i$. The polynomial f_i is generic of degree d_i in the ideal $G = (g_1, \ldots, g_r)$.
We are looking for a condition on the coefficients $\mathbf{c} = (c_\alpha^{i,j})$ such that $\mathbf{f_c}$ has a solution "outside" the variety $\mathcal{Z}(G)$ defined by G. Such a condition is given by the residual resultant defined in [13]. This resultant is constructed as a general resultant over the blow-up of $\mathbb{P}^n$ along the ideal G.

Theorem 6.6 *[13] There exists an irreducible and homogeneous polynomial of $\mathbb{K}[\mathbf{c}]$, denoted $\mathrm{Res}_{G,d_0,\ldots,d_n}$, which satisfies*

$$\begin{array}{rcl} \mathrm{Res}_{G,d_0,\ldots,d_n}(f_0, \ldots, f_n) = 0 & \Leftrightarrow & F^{sat} \neq G^{sat} \\ & \Leftrightarrow & (F^{sat} : G^{sat}) \neq R \\ & \Leftrightarrow & \mathcal{Z}(F : G) \neq \emptyset \end{array}$$

where F^{sat} and G^{sat} are respectively the saturations of the ideals $F = (f_0, \ldots, f_n)$ and G.

The degree of $\mathrm{Res}_{G,d_0,\ldots,d_n}$ in the coefficients $(c_\alpha^{i,j})$ of each f_j is

$$N_j = \frac{P_{r_j}}{P_1}(k_1, \ldots, k_r) \tag{6}$$

where, $r_j(T) = \sigma_n(\mathbf{d}) + \sum_{l=r}^{n} \sigma_{n-l}(\mathbf{d})\, T^l$, with the notations $\mathbf{d} = (d_0, \ldots, d_{j-1}, d_{j+1}, \ldots, d_n)$, $\sigma_0(\mathbf{d}) = (-1)^n$, $\sigma_1(\mathbf{d}) = (-1)^{n-1} \sum_{l \neq j} d_l$, $\sigma_2(\mathbf{d}) = (-1)^{n-2} \sum_{j_1 \neq j, j_2 \neq j, j_1 < j_2} d_{j_1} d_{j_2}$, $\ldots$, $\sigma_n(\mathbf{d}) = \prod_{l \neq j} d_l$, and

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

We denote by H the matrix $(h_{i,j})_{1 \leq i \leq r, 0 \leq j \leq n}$ and by $\Delta_{i_1 \ldots i_r}$ the $r \times r$ minor of H corresponding to the columns $i_1, \ldots, i_r$. A matrix whose determinant is a non-trivial multiple of the residual resultant can be constructed based on the following result:

Theorem 6.7 *[13] The following map, for $\nu \geq \sum_{i=0}^{n} d_i - n - (n-r+2)k_r$,*

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

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

$$e_i^{'} \longrightarrow f_i$$

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

Example 6.8 We consider the following system of cubics of $\mathbb{P}^3$ containing the umbilic:

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

We set $G=(x_3,x_0^2+x_1^2+x_2^2)$. 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 non-zero determinant. It yields a non-zero-multiple of the residual resultant. Notice that the projective and toric resultants are identically 0 in this case.

7 Geometric solvers

Let us described now how to exploit these resultant constructions to solve a (square or overdetermined) polynomial system.

7.1 The multiplicative structure from resultant matrices

Assume here that E_0 is a subset of F (this is immediate if f_0 contains a constant term) so that the matrix $\mathtt{S}$ can be divided into 4 blocks:

$$\mathtt{S}=\left[\begin{array}{c|c} \mathtt{A} & \mathtt{B} \\ \hline \mathtt{C} & \mathtt{D} \end{array}\right]$$

where the rows and columns of $\mathtt{A}$ are indexed by the monomials $\mathbf{x}^{E_0}$, and the columns of $\mathtt{B}$ and $\mathtt{D}$ are indexed by the monomials $\cup_{i=1,\ldots,n}\mathbf{x}^{E_i}$.

Theorem 7.1 *[61, 30, 55] For generic systems $f_1,\ldots,f_n$, the matrix of multiplication by f_0 in the basis $\mathbf{x}^{E_0}$ of $\mathcal{A}=R/(f_1,\ldots,f_n)$ is the Schur complement of $\mathtt{D}$ in $\mathtt{S}$: $M_{f_0}=\mathtt{A}-\mathtt{B}\,\mathtt{D}^{-1}\,\mathtt{C}$.*

Example 6.1 continued. Let us compute the Schur complement $\mathtt{A}-\mathtt{B}\mathtt{D}^{-1}\mathtt{C}$ of size 4, of the Macaulay matrix S:

```
> Mu := uschur(S,4);
```

$$\left[\begin{array}{cccc} u_0 & -\frac{25}{24}\,u_2 & \frac{1}{6}\,u_1 & \frac{5}{54}\,u_1-\frac{5}{54}\,u_2 \\ u_2 & u_0+2\,u_2 & 0 & \frac{2}{27}\,u_1+\frac{5}{54}\,u_2 \\ u_1 & -\frac{5}{4}\,u_2 & u_0+u_1 & \frac{55}{54}\,u_1-\frac{55}{54}\,u_2 \\ 0 & u_1+\frac{5}{4}\,u_2 & u_2-u_1 & u_0-u_1+2\,u_2 \end{array}\right]$$

By theorem 7.1, the coefficient of u_i in this matrix 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. This

formula is a continuous function of the coefficients of the input polynomials in the open set of systems such that $\mathtt{D}$ is invertible. Thus it can be used with approximated coefficients, which is of importance in many practical applications. The main drawback is however that the size of the matrix $\mathtt{S}$ 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 [55, 9]. Another way to handle it and to keep a continuous representation of the matrix of multiplication, has been proposed in [57]. In some sense, it combines the previous resultant approach with the normal form method of section 4.3, replacing the computation of a big Schur complement $\mathtt{A} - \mathtt{B}\,\mathtt{D}^{-1}\mathtt{C}$ by the inversion of much smaller systems. In the next table, we compare the size of the system to invert with the size of $\mathtt{D}$, in the case of the projective resultants of quadrics ($d_i = 2$) in $\mathbb{P}^n$: Σ is the sum of the system to invert, M is the size of the matrix $\mathtt{D}$ in the Macaulay's formulation and D is the dimension of the linear 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**	**1 652**	**6 307**	**24 054**	**91 866**	**351 692**	**1 350 030**
D	32	64	128	256	512	1024	2048

7.2 Solving by hiding a variable

Another approach for solving 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 value of this hidden variable (or parameter) for which the system has a solution. Typically, when 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 the 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 will lead us to a resultant matrix $\mathtt{S}(x_n)$, which entries are polynomial 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 are looking 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

$$\mathbf{v}(\zeta')^t\, \mathtt{S}(\zeta_n) = \mathbf{0} \tag{7}$$

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 $\mathtt{S}(\zeta')^t\, \mathbf{v} = \mathbf{0}$ are scalar multiples of $\mathtt{v}(\zeta')$. From the entries

of this vector we can usually deduce the other coordinates of the point ζ'. This will be assumed hereafter[4].

The relation (7) 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

$$\left(\begin{bmatrix} \mathbf{0} & \mathbb{I} & \cdots & \mathbf{0} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbb{I} \\ \mathtt{S}_0^t & \mathtt{S}_1^t & \cdots & \mathtt{S}_{d-1}^t \end{bmatrix} - \zeta_n \begin{bmatrix} \mathbb{I} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \mathbb{I} & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & -\mathtt{S}_d^t \end{bmatrix} \right) \mathbf{w} = 0. \tag{8}$$

The set of eigenvalues of (8) contains the values of ζ_n for which (7) has a solution. The corresponding eigenvectors $\mathbf{w}$ are decomposed as $\mathbf{w} = (\mathbf{w}_0, \ldots, \mathbf{w}_{d-1})$ so that the corresponding solution vector $\mathbf{v}(\zeta')$ of (7) 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:

Algorithm 7.2 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* $\mathtt{S}(x_n)^{\mathbf{t}}\, \mathtt{v} = \mathbf{0}$.
3. *Deduce the coordinates of the 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 7.3 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 of section 6.1. We obtain a 15×15 matrix $\mathtt{S}(x_3)$, and compute its determinant:

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

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

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 $\mathtt{S}(1)^t$ is generated by

$$[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]$$

which implies that the corresponding root is $(1, 1, 1)$. For the other eigenvalues (which are the roots of the last factor), we proceed similarly in order to obtain the 5 other (simple) roots of $f_1 = f_2 = f_3 = 0$.

[4]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 $\mathtt{S}(\zeta_n)$.

7.3 The isolated points from resultant matrices

In this section, we consider n equations in n unknowns, but we do not assume necessarily that the variety $\mathcal{Z}(f_1, \ldots, f_n)$ is zero-dimensional. We are interested in computing a rational representation of the isolated points. We denote by I_0 the intersection of the primary components of I corresponding to isolated points of $\mathcal{Z} = \mathcal{Z}(I)$ and $\mathcal{Z}_0 = \mathcal{Z}(I_0)$. The variety $\mathcal{Z}$ is zero-dimensional iff $\mathcal{Z} = \mathcal{Z}_0$. We denote by $\mathcal{C}_0(\mathbf{u})$ the Chow form associated with the ideal I_0 (see section 5.2).

Let us however consider first the case where $I = I_0$ define a 0-dimensional variety. Let $f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n$ be a generic affine form (the u_i are considered as variables). Let us choose one of the previous resultant construction for $f_0, \ldots, f_n$, which yields a matrix

$$\mathtt{S} = \begin{bmatrix} \mathtt{A} & \mathtt{B} \\ \mathtt{C} & \mathtt{D} \end{bmatrix}$$

such that $\mathtt{D}$ is invertible (if it exists). The blocks $\mathtt{A}$, $\mathtt{C}$ are depending only on the coefficients of f_0. From section 7.1 and according to the relation

$$\begin{bmatrix} \mathtt{A} & \mathtt{B} \\ \mathtt{C} & \mathtt{D} \end{bmatrix} \begin{bmatrix} \mathbb{I} & \mathbf{0} \\ -\mathtt{D}^{-1}\mathtt{C} & \mathbb{I} \end{bmatrix} = \begin{bmatrix} \mathtt{A} - \mathtt{B}\mathtt{D}^{-1}\mathtt{C} & \mathtt{B} \\ \mathbf{0} & \mathtt{D} \end{bmatrix}$$

we deduce that

$$\det(\mathtt{S}) = \det(M_{f_0}) \det(\mathtt{D}).$$

In other words $\det(\mathtt{S})$ is scalar multiple of the Chow form $\det(\mathtt{M}_{f_0}) = \mathcal{C}(\mathbf{u})$. Such a construction applies for a system which is generic for any of resultant formulation that we have presented. Applying algorithm 5.9, we obtain a rational representation of the roots.

In the case where our variety $\mathcal{Z}(f_1, \ldots, f_n)$ is not zero-dimensional, we can still deduce a rational representation of the isolated points of the variety, 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 regular system $\mathbf{f}_\epsilon$ (for instance $\mathbf{f}_\epsilon = \mathbf{f} + \epsilon\,\mathbf{f}_0$), we obtain a resultant matrix $\mathtt{S}_\epsilon(\mathbf{u})$, which determinant is of the form

$$\Delta(\mathbf{u}, \epsilon) = \epsilon^k \Delta_k(\mathbf{u}) + \epsilon^{k+1} \Delta_{k+1}(\mathbf{u}) + \cdots$$

It can be shown that the trailing coefficient (in ϵ) $\Delta_k(\mathbf{u}) \neq 0$ of the determinant of the resultant matrix is a multiple of the Chow form of the isolated points $\mathcal{Z}(I_0)$. Applying algorithm 5.9 to this multiple of the Chow form yields a rational representation of the isolated points. See [40, 17, 14, 35, 43] for more information and examples.

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 defined in 6.3 :

Proposition 7.4 *[26, 12] Any nonzero maximal minor $\Delta(\mathbf{u})$ of the Bezoutian matrix of the polynomials $f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n, f_1, \ldots, f_n$ is divisible by the Chow form $\mathcal{C}_0(\mathbf{u})$ of the isolated points.*

The interesting point here is that we get directly the Chow form of the isolated points of $\mathcal{Z}$ even if this variety is not zero-dimensional. In other words, we do not need to consider perturbed systems, to compute 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 the minors). It leads to the following algorithm:

Algorithm 7.5 Univariate rational 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. *Apply algorithm 5.9, in order to get a rational representation of the isolated (and maybe some embedded) roots.*

In practice, instead of expanding completely the polynomial $d(\mathbf{t} + \mathbf{u})$ in algorithm 5.9, 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. Moreover, we can describe these terms as sums of determinants of matrices deduced from the resultant matrices. This allows us to use fast interpolation methods to compute efficiently the polynomials $d_i(u_0)$.

7.4 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 error for instance).

Here again we are interested by matrix methods, which allow to handle such systems with approximate coefficients. The method of the previous sections, for the construction of resultant matrices $\mathtt{S}$ admit natural generalizations [44] to overconstrained systems, that is, to systems of equations $f_1 = 0, \ldots, f_m = 0$, with $m > n$, defining a finite number of roots. We still consider a map of the form

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

which yields a rectangular matrix $\tilde{\mathtt{S}}$.

A case of special interest is the case where this matrix is of rank $N - 1$, where N is the number of row of $\tilde{\mathtt{S}}$. In this case, it can be proved [27] that $\mathcal{Z}(f_1, \ldots, f_m)$ is reduced to one point $\zeta \in \mathbb{K}^n$ and if $(\mathbf{x}^\alpha)_{\alpha \in F}$ is the set of monomials indexing the rows of $\tilde{\mathtt{S}}$, that

$$[\zeta^\alpha]_{\alpha \in F}^{\mathbf{t}} \, \tilde{\mathtt{S}} = \mathbf{0}.$$

Using Cramer's rule, we see that $\zeta^\alpha / \zeta^\beta$ ($\alpha, \beta \in F$, $\zeta^\beta \neq 0$) can be expressed as the ratio of two maximal minors of $\tilde{\mathtt{S}}$. 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 $\tilde{\mathtt{S}}$, and thus of the input coefficients of polynomials f_i.

Algorithm 7.6 Solving an overconstrained system defining a single root

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

- *Compute the resultant matrix* $\tilde{\mathtt{S}}$ *for one the proposed resultant formulation.*
- *Compute the kernel of* $\tilde{\mathtt{S}}^{\mathbf{t}}$ *and check that it is generate 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 algorithms, with a projective resultant construction.

Example 7.7 We consider the case of 3 quadrics:

```
> 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]);
```

$$\begin{bmatrix}
-3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -9 & 0 & 0 & 0 \\
0 & -3 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -9 & 2 & 0 & 0 & 0 \\
0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -9 \\
-1 & 0 & 0 & -3 & 0 & -1 & -2 & 0 & 1 & 0 & -1 & 1 & -9 & 0 & 2 \\
0 & 1 & -1 & 0 & -1 & -2 & 0 & 1 & 1 & 0 & 0 & 0 & -1 & 2 & 1 \\
0 & -1 & 1 & 0 & 0 & 1 & 0 & -1 & -2 & -1 & 1 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 1 & -2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1 & 1 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -9 & -1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & -9 & 2 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

The rows of 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 the transposed matrix, 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 $\zeta = (1, 2)$.

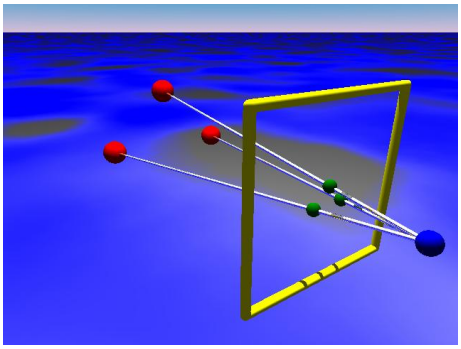
In the case where the overdetermined system has more than one root, we can follow the same approach. We chose a subset E of F (if possible containing the monomials $1, x_1, \ldots, x_n$) such that the matrix indexed the monomials $\mathbf{x}^{F-E}$ is of rank, the rank $r = N - D$ of $\tilde{\mathtt{S}}$. 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 $\tilde{\mathtt{S}}$ with the block of the coefficients $f_0\,\mathbf{x}^{E_0}$, 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 5.1, we deduce the roots of the overdetermined system $f_1, \ldots, f_m$. See eg. [29] for more details on this approach.

8 Applications

8.1 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:

$$\begin{cases} x_1^2 + x_2^2 - 2\cos(\gamma) x_1 x_2 - c^2 = 0 \\ x_1^2 + x_3^2 - 2\cos(\beta) x_1 x_3 - b^2 = 0 \\ x_2^2 + x_3^2 - 2\cos(\alpha) x_2 x_3 - a^2 = 0, \end{cases} \tag{9}$$

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 (9) 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 equation. 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). We obtain

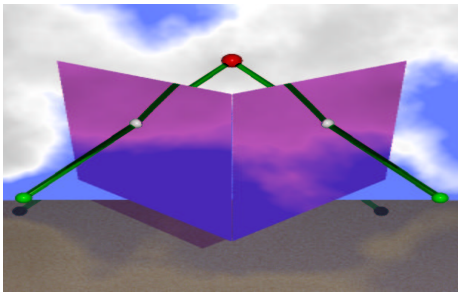
```
> melim([f1,f2,f3],[x2,x3]);
```

$$2\,\cos(\alpha)\left(64\cos(\beta)^2\cos(\alpha)^2\cos(\gamma)^2 - 64\cos(\beta)^3\cos(\alpha)\cos(\gamma) - 64\cos(\beta)\cos(\alpha)^3\cos(\gamma) - 64\cos(\beta)\cos(\alpha)\cos(\gamma)^3 + 16\cos(\beta)^4 + 32\cos(\beta)^2\cos(\alpha)^2 + 32\cos(\beta)^2\cos(\gamma)^2 + 16\cos(\alpha)^4 + 32\cos(\alpha)^2\cos(\gamma)^2 + 16\cos(\gamma)^4 + 64\cos(\beta)\cos(\alpha)\cos(\gamma) - 32\cos(\beta)^2 - 32\cos(\alpha)^2 - 32\cos(\gamma)^2 + 16\right) x_1^8 + \cdots$$

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

8.2 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 a same scene. Following the approach described in [31], 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 **m** F**m'**=0, where F is the fundamental matrix.



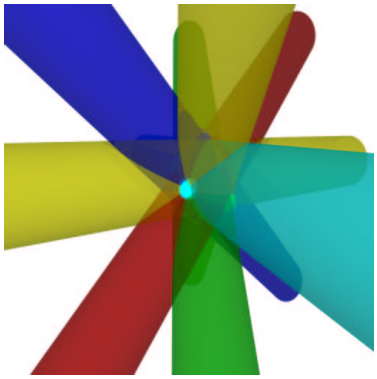
From 3 images and the 3 corresponding fundamental matrices, we deduce the so-called Kruppa equations on the 6 intrinsic parameters of the camera. See [42], [31] for more details. This is a system of 6 quadratic homogeneous equations in 6 variables. We solve this overdetermined system, by choosing 5 equations among the six, solving the corresponding affine system and choosing the best solution 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 [73] and is available in the library SYNAPS [24].

8.3 Cylinders through 4 and 5 points

We consider the problem of finding cylinders through 4 or 5 points. The modelisation that we use is described in [22].



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.
- Line 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:

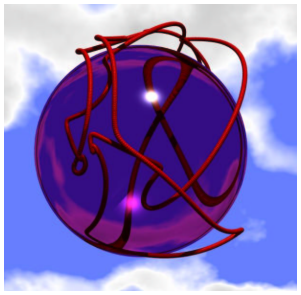
Problem	*time*	$max(\|f_i\|)$
Cylinders through 5 points	$0.03s$	$5 \cdot 10^{-9}$
Parallel cylinders through 2×4 points	$0.03s$	$5 \cdot 10^{-9}$
Cylinders through 4 points, extremal radius	$2.9s$	10^{-6}

The computation was performed on an Intel PII 400 128 Mo of Ram. The relatively huge time spent in the last problem, is due to the treatment of multiple roots.

8.4 The position of a parallel robot

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

From the measurements of the 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 [66], [45], [51], that this problem has at most 40 solutions and that this bound is reached [23]. 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:

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

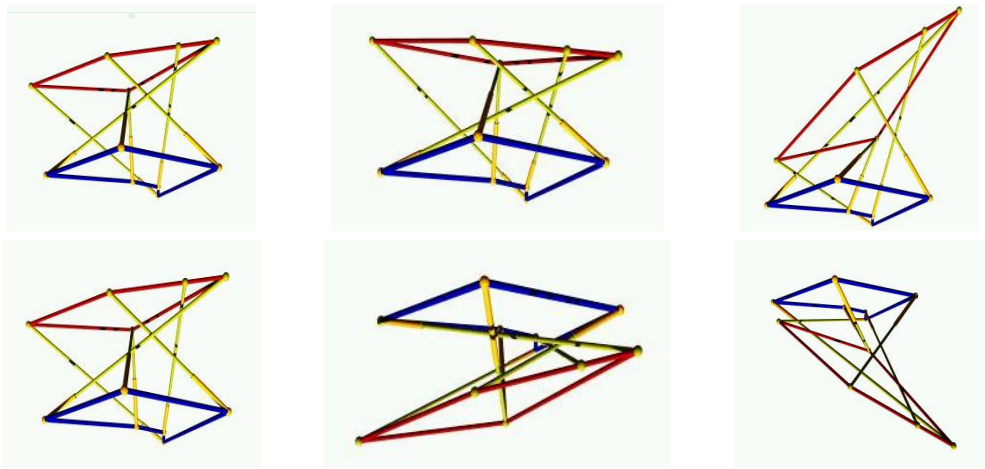
where $R = \frac{1}{a^2+b^2+c^2+d^2} \begin{bmatrix} a^2 - b^2 - c^2 + d^2 & 2\,ab - 2\,cd & 2\,ac + 2\,bd \\ 2\,ab + 2\,cd & -a^2 + b^2 - c^2 + d^2 & 2\,bc - 2\,ad \\ 2\,ac - 2\,bd & 2\,ad + 2\,bc & -a^2 - b^2 + c^2 + d^2 \end{bmatrix}$ is the rotation of the platform with respect to a referential and $T = [u, v, w,]$ its translation. Using again the solver by Ph. Trébuchet and different modelisation, one deduced from residual resultant construction as described in [11] 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 $nb.$ means n bits used in the computation.

8.5 Direct kinematic problem of a parallel robot

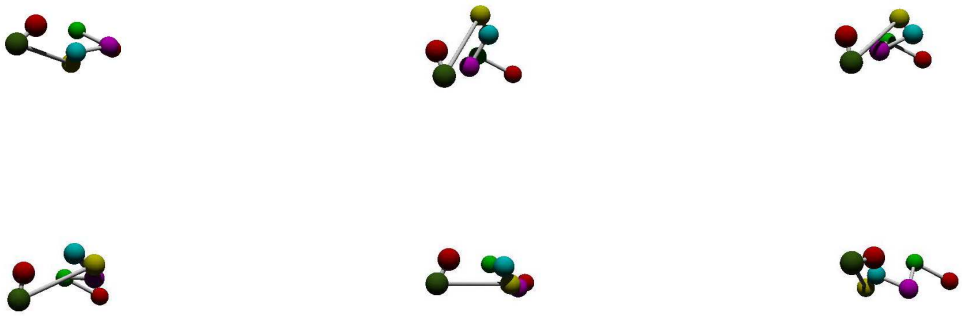
Resultant constructions can also be used for some special geometry of the platform. Here is an example where two attached points of the arms on the platform are identical. We solve this problem by using the Bezoutian formulation, which yields a 20×20 matrix of polynomials in one variable. The number 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, 1 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 a Intel PII 400, 128 Mo of Ram.

8.6 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 [63]. 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 work station.

8.7 Blind identification in signal processing

Finally, we consider a problem from signal processing, described in detail in [38]. It is related to the transmition 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:

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

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

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

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 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 $= 0.76s$	

References

[1] W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, AMS, Providence RI, 1994.

[2] E. L. Allgower and K. Georg, *Numerical Path Following*, Springer, 1990.

[3] M. Alonso, E. Becker, M. Roy, and T. Wörmann, *Zeros, multiplicities and idempotents for zero dimensional systems*, in Algorithms in Algebraic Geometry and Applications, L. González-Vega and T. Recio, eds., vol. 143 of Prog. in Math., Birkhäuser, Basel, 1996, pp. 1–15.

[4] W. Auzinger and H. J. Stetter, *An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations*, in Proc. Intern. Conf. on Numerical Math., vol. 86 of Int. Series of Numerical Math, Birkhäuser Verlag, 1988, pp. 12–30.

[5] T. Becker, V. Weispfenning, and H. Kredel, *Gröbner Bases. A Computational Approach to Commutative Algebra*, vol. 141 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1993.

[6] R. Benedetti and J. Risler, *Real algebraic and semi-algebraic sets*, Hermann, 1990.

[7] E. Bézout, *Recherches sur les degrés des équations résultantes de l'évanouissement des inconnues et sur les moyens qu'il convient d'employer pour trouver ces équations*, Hist de l'Aca. Roy. des Sciences, (1764), pp. 288–338.

[8] D. Bini, *Numerical computation of polynomial zeros by means of aberth's method*, Numerical Algorithms, 13 (1996).

[9] D. Bondyfalat, B. Mourrain, and V. Y. Pan, *Computation of a specified root of a polynomials system of equations using eigenvector*, Lin. Alg. and its Appl., 319 (2000), pp. 193–209.

[10] W. Bruns, A. R. Kustin, and M. Miller, *The resolution of the generic residual intersection of a complete intersection*, Journal of Algebra, 128 (1990), pp. 214–239.

[11] L. Busé, *Étude du résultant sur une variété algébrique*, PhD thesis, Université de Nice Sophia-Antipolis, 2001.

[12] L. Busé, M. Elkadi, and B. Mourrain, *Generalized resultant over unirational algebraic varieties*, J. of Symbolic Computation, 29 (2000), pp. 515–526.

[13] ———, *Resultant over the residual of a complete intersection*, J. of Pure and Applied Algebra, 164 (2001), pp. 35–57.

[14] J. Canny, *Generalised Characteristic Polynomials*, J. of Symbolic Computation, 9 (1990), pp. 241–250.

[15] J. Canny and I. Emiris, *A subdivision-based algorithm for the sparse resultant*, J. ACM, 47 (2000), pp. 417–451.

[16] M. Chardin and B. Ulrich, *Liaison and Castelnuovo-Mumford regularity.* Preprint, 2000.

[17] A. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time*, J. Sov. Math, 34 (1986), pp. 1838–1882.

[18] R. Corless, P. Gianni, and B. Trager, *A reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots*, in Porc. ISSAC, W. Küchlin, ed., 1997, pp. 133–140.

[19] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer Verlag, New York, 1992.

[20] J.-P. Dedieu and J.-C. Yakoubsohn, *Computing the real roots of a polynomial by the exclusion algorithm*, Numerical Algorithms, 4 (1993), pp. 1–24.

[21] J. W. Demmel, *On condition numbers and the distance to the nearest ill-posed problem*, Numer. Math., 51 (1987), pp. 251–289.

[22] O. Devillers, B. Mourrain, F. P. Preparata, and P. Trebuchet, *Circular cylinders by four or five points in space*, Discrete and Computational Geometry, 29 (2003), pp. 83–104.

[23] P. Dietmaier, *The Stewart-Gough platform of general geometry can have 40 real postures*, in Advances in robot kinematics: analysis and control (Salzburg, 1998), Kluwer Acad. Publ., Dordrecht, 1998, pp. 7–16.

[24] G. Dos Reis, B. Mourrain, R. Rouillier, and P. Trébuchet, *An environment for symbolic and numeric computation*, in Proc. of the International Conference on Mathematical Software, World Scientific, 2002, pp. 239–249.

[25] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, vol. 150 of Graduate Texts in Math., Berlin, Springer-Verlag, 1994.

[26] M. Elkadi and B. Mourrain, *Algorithms for residues and Lojasiewicz exponents*, J. of Pure and Applied Algebra, 153 (2000), pp. 27–44.

[27] ———, *Introduction à la résolution des systèmes d'équations algébriques*, 2003. Notes de cours, Univ. de Nice (310 p.). Soumis pour publication dans la srie mathmatiques appliques (SMAI).

[28] I. Emiris and J. Canny, *Efficient incremental algorithms for the sparse resultant and the mixed volume*, J. Symbolic Computation, 20 (1995), pp. 117–149.

[29] I. Emiris and B. Mourrain, *Matrices in Elimination Theory*, J. of Symbolic Computation, 28 (1999), pp. 3–44.

[30] I. Emiris and A. Rege, *Monomial bases and polynomial system solving*, in Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation, Oxford, July 1994, pp. 114–122.

[31] O. Faugeras, *Three-Dimensional Computer Vision: a Geometric Viewpoint*, MIT press, 1993.

[32] J. Faugère, *A new efficient algorithm for computing Gröbner Basis (F4)*, J. of Pure and Applied Algebra, 139 (1999), pp. 61–88.

[33] P. Fuhrmann, *A polynomial approach to linear algebra*, Springer-Verlag, 1996.

[34] I. Gelfand, M. Kapranov, and A. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*, Boston, Birkhäuser, 1994.

[35] M. Giusti and J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, in Proc Int. Meeting on Commutative Algebra, vol. XXXIV of Symp. Mathematica, Cortona,1991, pp. 216–255.

[36] L. Gonzalez-Vega, F. Rouillier, and M. Roy, *Symbolic Recipes for Polynomial System Solving*, Some Tapas of Computer Algebra, Springer, 1997.

[37] D. R. Grayson and M. E. Stillman, *Macaulay 2, a software system for research in algebraic geometry*. Available at `http://www.math.uiuc.edu/Macaulay2`.

[38] O. Grellier, P. Comon, B. Mourrain, and P. Trébuchet, *Analytical blind channel identification*, IEEE Trans. on Signal Processing, 50 (2002), pp. 2196–2207.

[39] G.-M. Greuel, G. Pfister, and H. Schoenemann, *Singular, a computer algebra system for polynomial computations*. Available at `http://www.singular.uni-kl.de/team.html`.

[40] D. Grigoryev, *Factorization of polynomials over finite field and the solution of systems of algebraic equations*, J. Sov. Math, 34 (1986), pp. 1762–1803.

[41] R. B. Kearfott, *Interval arithmetic techniques in the computational solution of nonlinear systesm of equations: Introduction, examples and comparisons*, Lectures in Applied Mathemetics, AMS Press, 1990, pp. 337–357.

[42] E. Kruppa, *Zur Ermittlung eines Objektes aus zwei Perspektiven mit innere Orientierung*, Sitz.-Ber. Akad. Wiss., Wien, Math.-Naturw. Kl., Abt. IIa (1913), pp. 1939–1948.

[43] Y. N. Lakshman and D. Lazard, *On the complexity of zero-dimensional algebraic systems*, in Effective Methods in Algebraic Geometry (MEGA'90), vol. 94 of Progress in Math., Castiglioncello (Italy), 1991, Birkhäuser, pp. 217–225.

[44] D. Lazard, *Algèbre linéaire sur* $k[x_1, \ldots, x_n]$ *et élimination*, Bull. Soc math. France, 105 (1977), pp. 165–190.

[45] ———, *Generalized Stewart platform: How to compute with rigid motions?*, in IMACS -SC'93, 1993.

[46] G. Lecerf, *Computing an equidimensional decomposition of an algebraic varety bymeans of geometric resolutions*, Proc. ISSAC, (2000), pp. 209–216.

[47] T. Li, *Numerical solution of multivariate polynomial systems by homotopy continuation methods*, Acta Numerica, 6 (1997), pp. 399–436.

[48] F. Macaulay, *Some formulae in elimination*, Proc. London Math. Soc., 1 (1902), pp. 3–27.

[49] F. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press, 1916.

[50] A. Morgan and A. Sommese, *A homotopy for solving general polynomial systems that respects m-homogeneous structures*, Appl. Math. Comput., 24 (1987), pp. 101–113.

[51] B. Mourrain, *The 40 generic positions of a parallel robot*, in Proc. Intern. Symp. on Symbolic and Algebraic Computation, M. Bronstein, ed., ACM press, Kiev (Ukraine), July 1993, pp. 173–182.

[52] ———, *Enumeration problems in Geometry, Robotics and Vision*, in Algorithms in Algebraic Geometry and Applications, L. González and T. Recio, eds., vol. 143 of Prog. in Math., Birkhäuser, Basel, 1996, pp. 285–306.

[53] ———, *Computing isolated polynomial roots by matrix methods*, J. of Symbolic Computation, Special Issue on Symbolic-Numeric Algebra for Polynomials, 26 (1998), pp. 715–738.

[54] ———, *A new criterion for normal form algorithms*, in Proc. AAECC, M. Fossorier, H. Imai, S. Lin, and A. Poli, eds., vol. 1719 of LNCS, Springer, Berlin, 1999, pp. 430–443.

[55] B. Mourrain and V. Y. Pan, *Multivariate polynomials, duality and structured matrices*, J. of Complexity, 16 (2000), pp. 110–180.

[56] B. Mourrain and O. Ruatta, *Relation between roots and coefficients, interpolation and application to system solving*, JSC, 33 (2002), pp. 679–699.

[57] B. Mourrain and P. Trébuchet, *Solving projective complete intersection faster*, in Proc. Intern. Symp. on Symbolic and Algebraic Computation, C. Traverso, ed., New-York, ACM Press., 2000, pp. 231–238.

[58] ———, *Algebraic methods for numerical solving*, in Proc. of the 3rd International Workshop on Symbolic and Numeric Algorithms for Scientific Computing'01 (Timisoara, Romania), 2002, pp. 42–57.

[59] B. Mourrain, M. Vrahatis, and J. Yakoubsohn, *On the complexity of isolating real roots and computing with certainty the topological degree*, J. of Complexity, 18 (2002), pp. 612–640.

[60] V. Pan, *Optimal and nearly optimal algorithms for approximating polynomial zeros*, Comp. and Math. (with Appl.), 31 (1996), pp. 97–138.

[61] P. Pedersen and B. Sturmfels, *Mixed monomial bases*, in Effective Methods in Algebraic Geometry, L. González-Vega and T. Recio, eds., vol. 143 of Progress in Mathematics, Boston, 1996, Birkhäuser, pp. 307–316. (Proc. MEGA '94, Santander, Spain).

[62] P. S. Pedersen, M.-F. Roy, and A. Szpirglas, *Counting Real Zeros in the multivariate Case*, in Effective Methods in Algebraic Geometry (MEGA'92), A. Galligo and F. Eyssette, eds., Progress in Math., Nice (France), 1993, Birkhuser, pp. 203–223.

[63] M. Raghavan and B. Roth, *Solving polynomial systems for the the kinematic analysis of mechanisms and robot manipulators*, ASME J. of Mechanical Design, 117 (1995), pp. 71–79.

[64] J. Renegar, *On the computational complexity and geometry of the first order theory of reals (I, II, III)*, J. Symbolic Computation, 13 (1992), pp. 255–352.

[65] L. Robbianno, *Cocoa, computational commutative algebra.* Available at `http://www.singular.uni-kl.de/team.html`.

[66] F. Ronga and T. Vust, *Stewart platforms without computer?*, in International Conference on Real Analytic and Algebraic Geometry, Berlin, 1995, W. de Gruyter. Prsent lors de la confrence en 1992, Trento, Italie.

[67] F. Rouillier, *Solving zero-dimensional polynomial systems throuhg Rational Univariate Representation*, App. Alg. in Eng. Com. Comp., 9 (1999), pp. 433–461.

[68] F. Rouillier and P. Zimmermann, *Efficient isolation of a polynomial real roots.* Preprint.

[69] M. Roy, *Basic algorithms in real algebraic geometry: from Sturm theorem to the existential theory of reals*, in Lectures on Real Geometry in memorianm of Mario Raimondo, vol. 23 of Exposition in Mathematics, 1996, pp. 1–67.

[70] M. Shub and S. Smale, *On the complexity of Bezout's theorem I – geometric aspects*, J. AMS, 6 (1993), pp. 459–501.

[71] H. J. Stetter, *Eigenproblems are at the heart of polynomial system solving*, SIGSAM Bulletin, 30 (1996), pp. 22–25.

[72] B. Sturmfels, *Sparse elimination theory*, in Computational Algebraic Geometry and Commutative Algebra, D. Eisenbud and L. Robianno, eds., Cambridge, Cambridge Univ. Press, 1993, pp. 264–298.

[73] P. Trébuchet, *Vers une résolution stable et rapide des équations algébriques*, PhD thesis, Université Pierre et Marie Curie, 2002.

[74] J. Uspensky, *Theory of equations*, Mac Graw Hill, 1948.

[75] W. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*, vol. 2 of Algorithms and Computation in Mathematics, Springer-Verlag, 1998.

[76] J. Verschelde, P. Verlinden, and R. Cools, *Homotopies exploiting Newton polytopes for solving sparse polynomial systems*, SIAM J. Numerical Analysis, 31 (1994), pp. 915–930.