SALSA

Solvers for ALgebraic Systems and Applications

Version 1.0.0

http://fgbrs.lip6.fr/salsa/

Research topics :	Solving polynomial systems of equalities and inequalities; Academic and industrial applications, software development.
Keywords :	computer algebra - polynomial systems - real roots - certified results - efficient software.

Contents

The SALSA project's speciality is the resolution of algebraic systems of equations and/or inequalities and the goal is to design and implement efficient algorithms with guaranteed results.
SALSA project's aim is to provide software which are competitive in terms of efficiency but preserve certified outputs. Therefore, we restrict ourselves to algorithms which verify the assumptions made on the input, check the correctness of possible random choices done during a computation without sacrifying the efficiency. Theoretical complexity for our algorithms is only a preliminary step of our work which culminates with efficient implementations which are faced to face with applications.
A consequence of our way of working is that our most well-known contributions (outside the Computer Algebra communauty) are related to applicative topics such as cryptography, error correcting codes, robotics and signal theory. We have to emphasize that these applied contributions rely on a long-term and global management of the project with clear and constant objectives leading to theoretical and deep advances.

1 The team

The project is located in Rocquencourt and in Paris at Pierre & Marie Curie University. All the members of the project are involved in the CALFOR team led by J.C. Faugère (vice-head of our project). This is mainly due to the participation of assistant professors teaching at Pierre & Marie Curie University. This administrative situation is favorable for two reasons :

- many projects members but also CALFOR participants are involved in teaching activities at several levels (organization, courses, etc). This situation supports a better dissemination of the results and know-how of the project for the training of students with a double competence (mathematics and computer science);
- several scientific topics (Galois Theory for example), developed in the CALFOR team, are strongly related to our base fields of research, so that further interactions can emerge from this scientific context.

1.1 Members

- **Head of project team** Fabrice Rouillier [research scientist INRIA]
- **Vice-head of project team** Jean-Charles Faugère [research scientist CNRS]
- **Administrative assistants**
  - Laurence Bourcier [INRIA, part time]
  - David Massot [UPMC, part time]
- **Staff member (University)**
  - Philippe Aubry [assistant professor, UPMC]
  - Daniel Lazard [professor, UPMC]
  - Mohab Safey El Din [assistant professor, UPMC]
  - Philippe Trébuchet [teaching assistant, UPMC]
- **Ph. D. Students**
  - Gwenolé Ars [DGA, defense planned in 2004] (J.C. Faugère)
  - Magali Bardet [teaching assistant, defense planned in 2004] (J.C. Faugère)
  - Solen Corvez [BDI CNRS, defense planned in 2005] (F. Rouillier)
  - Amir Hashemi [Sfere grant, defense planned in 2005] (D. Lazard)
  - Sylvain Lacharte [CIFRE grant with Thalès, defense planned in 2006] (J.C. Faugère)
  - Guillaume Moroz [AMN - defense planned in 2007] (F. Rouillier)

1.2 History

Solving polynomial systems of equations is a longstanding fundamental problem. Let us mention as witness the attempts to solve univariate equations by radicals until Abel and Galois proved (around 1830) that it is impossible, or the fact that the "fundamental theorem of algebra" deals with polynomial equations.

It is only at the end of the 19th century that the first general algorithms for polynomial systems appeared, with the works of Bézout, Sylvester, Kronecker, and Macaulay. However the computations were intractable, due to the complexity of the problem. Therefore the mathematicians gave up this effective approach to put the emphasis on qualitative theoretical results. With electronic computers and computer algebra systems, the problem of multivariate systems came back to the attention of the researchers around 1970, when polynomial gcd and factorization problems got a satisfactory answer. However, because of the difficulty of the problem, it is only in the second half of the 80's that computers began to solve problems which are really intractable by hand. At the beginning of the 90's, the only way to solve in practice multivariate polynomial systems, was the use of some implementations of the Cylindrical Algebraic Decomposition based on the elimination of variables one after the other and the underlying tools such as the computations of subresultants and Sturm sequences.

The history of our project goes back to the period where J.-C. Faugère and F. Rouillier were involved in the european project PoSSo during their PhD respectively supervised by D. Lazard and M.-F. Roy [27],[72]. One of the goals of this project was to encourage interactions between different teams to obtain significative advances on solving algebraic systems of equations. J.-C. Faugère was working on Gröbner bases and their implementation while F. Rouillier was working on algorithms for studying real roots of systems with a finite number of complex roots (number of roots, certified approximation, etc.), using Gröbner bases as input. The first implementations (GB for which J.-C. Faugère received the Seymour Cray award and REALSOLVING due to F. Rouillier) appear during the middle of the 90's (first official joint presentation at ICIAM' 95 [71]). The combination of these contributions applied to zero-dimensional systems (i.e. polynomial systems with a finite set of complex solutions) have made possible qualitative studies on parallel robots, which culminate at the end of the 90's by a contract for simulating the prototype of a machine tool [74]. In the same period, we obtained a patent for the design of filter banks for image compression [28]. Up to our knowledge, these results are the first examples of non-academic applications of using Computer Algebra methods in solving polynomial systems.

The latter application relied on the resolution of a positive dimensional system (i.e. the complex solution set is infinite). This led us to consider positive dimensional problems as a priority of our research program. The results obtained in P. Aubry's Phd thesis [1] (supervised by D. Lazard) and M. Safey El Din's Phd thesis [84] (supervised by F. Rouillier) have allowed to provide the first implemented alternative to the Cylindrical Algebraic Decomposition (CAD) to decide if a positive dimensional algebraic variety has real points and to provide at least one point in each connected component of its real counterpart. At the beginning of this decade, we have proposed to reinforce our activity by creating the LORIA/LIP6 SPACES project involving a part of Rouillier's former project (PolKA - LORIA) and a part of Faugère's team (CALFOR - University of Paris VI). Since the beginning of SPACES, our group has been reinforced by the recruitment of P. Aubry and M. Safey El Din as assistant professors at University of Paris VI.

The arithmetic part of the SPACES project, which is geographically located at the INRIA Lorraine research unit, has been reinforced by the recruitment of two junior researchers while as above mentioned, P. Aubry and M. Safey El Din joined the group working on polynomial systems, which is located in Paris. In addition, D. Lazard (actual head of the SPACES project) will retire at the end of the year, and F. Rouillier has been transfered to the INRIA Rocquencourt research unit. Thus, both parts of SPACES have now a size which is sufficient for an independent scientific action. This justifies to propose an autonomous project dedicated to polynomial systems solving in continuation of our previous activities.

These activities consist, on the one hand, in developing algorithms for algebraic elimination based on Gröbner bases and/or triangular sets, viewed as the computation of the complex solutions of algebraic systems. On the other hand, we tackle the problem of designing methods to study the real solutions of polynomial systems of equations and inequalities. Progress on this latter topic strongly needs progress on the former. Moreover, transversal actions coming from applications allow to fix our priorities in terms of scientific objectives and implementations. The relevance of the scientific foundations of our approach is confirmed by many reference books on the subject, which describe or cite our previous results [24], [11], [9], [40], [39], etc.

Our recent results correspond to the scientific objectives of the SPACES project. We proposed to develop the critical point methods in effective real algebraic geometry: as shown by the accumulation of results [82],[3],[87],[76],[88] in this field, this domain is now a stable axis of the project. We also proposed some developments improving Gröbner

bases computations, which were required by the applications in cryptography: numerous results have been obtained and are now the basis of further developments.

New thematics introduced in the present proposal have emerged under the impulse of the Ministry Grant (ACI "Jeunes", 2001) and some applications [56], [57], [20],[33], [58],[59]. Since parametric algebraic systems appear in many applications (celestial mechanics, cuspidal robots, design of filter banks, etc.) for which efficient algorithms have been designed, their resolution is now a major axis of research. Developing specific algorithms for algebraic optimization is also a priority since this topic has applications in effective real algebraic geometry via the critical point method. The study of real world applications remains a strong specificity of the project. Our activity in algebraic cryptanalysis is supported by several contracts with Thalès and CELAR (DGA). These studies have led to recent conspicuous advances on the computations and the complexity of Gröbner bases [7],[5]. Our longstanding collaborations with several industrials, COPRIN project and ENSAM (Metz) on path planning for parallel manipulator will probably be supported by the ANVAR and is the driving objective of our activity on zero-dimensional systems. Finally, our activity on parametric systems is led by our collaborations with IRCCyN, COPRIN and IRMAR (supported by a CNRS grant during the year 2002) which will keep on.

2 Scientific structure and Background

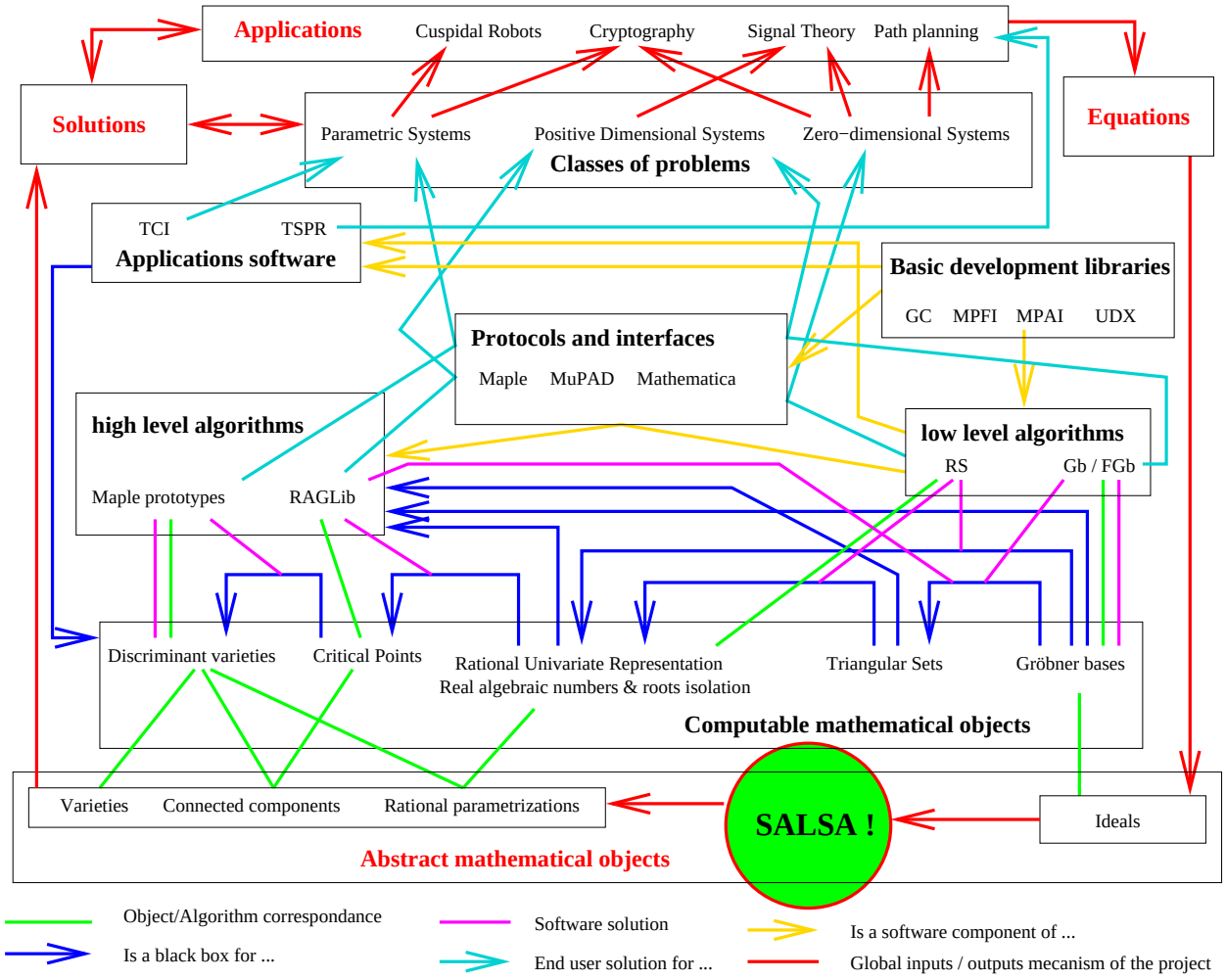

Figure 1: Activities of the project

2.1 Mathematical objects and Algorithms

The mathematical specification of the result of a computation, in particular when the number of solutions is infinite, is itself a difficult problem [1], [2], [53], [55]. Sorting the most frequently asked questions appearing in the applications, one distinguishes several classes of problems which are different either by their mathematical structure or by the significance that one can give to the word "solving".

Some of the following questions have a different meanings in the real case or in the complex case, others are posed only in the real case :

- zero-dimensional systems (with a finite number of complex solutions - which includes the particular case of univariate polynomials); The questions in general are well defined (numerical approximation, number of solutions, etc) and the handled mathematical objects are relatively simple and well-known;
- parametric systems; They are generally zero-dimensional for almost all the parameters' values. The objective consists in characterizing the solutions of the system (number of real solutions, existence of a parameterization, etc.) with respect to parameters' values.
- positive dimensional systems; For a direct application, the first question is the existence of zeros of a particular type (for example real, real positive, in a finite field). The resolution of such systems can be considered as a black box for the study of more general problems (semi-algebraic sets for example) and information to be extracted is generally the computation of a point per connected component in the real case.
- constructible and semi-algebraic sets; As opposed to what occurs numerically, the addition of constraints or inequalities complicates the problem. Even if semi-algebraic sets represent the basic object of the real geometry, their automatic "and effective study" remains a major challenge. To date, the state of the art is poor since only two classes of methods are existing :
  - the Cylindrical Algebraic Decomposition which basically computes a partition of the ambient space in cells where the signs of a given set of polynomials are constant;
  - deformations based methods that turn the problem into solving algebraic varieties.

  The first solution is limited in terms of performances (maximum 3 or 4 variables) because of a recursive treatment variable by variable, the second also because of the use of a sophisticated arithmetic (formal infinitesimals).
- quantified formulas; deciding efficiently if a first order formula is valid or not is certainly one of the greatest challenges in "effective" real algebraic geometry. However this problem is relatively well encircled since it can always be rewritten as the conjunction of (supposed to be) simpler problems like the computation of a point per connected component of a semi-algebraic set.

As explained in some parts of this document, the unicity of the studied mathematical objects does not imply the unicity of the related algorithms.

The pressure is relatively strong on zero-dimensional systems since we enter directly in competition with numerical methods (Newton, homotopy, etc), semi-numerical methods (interval analysis, eigenvalues computations, etc.) and formal methods (geometrical resolution, resultant based strategies, XL algorithm in cryptography, etc.). The pressure is much less on the other subjects: except the groups working on the Cylindrical Algebraic Decomposition, very few studies with practical vocation are to be counted and even less software achievements.

The priorities we put on our algorithmic work are generally dictated by the applications. Thus, one finds the cutting stated above in the identified research topics of our project for the algorithmic part. For each of these goals, our work is to design the most efficient possible algorithms: there is thus a strong correlation between implementations and applications, but a significant part of work is dedicated to the identification of black-box allowing a modular approach of the problems. For example, the resolution of the zero-dimensional systems is a prerequisite for the algorithms treating of parametric or positive dimensional systems.

An essential class of black-box developed in the project does not appear directly in the absolute objectives counted above : the "algebraic or complex" resolutions. They are mostly reformulations, more algorithmically usable, of the studied systems. One distinguishes two categories of complementary objects :

- ideals representations; From a computational point of view these are the structures which are used in the first steps;
- varieties representations; The algebraic variety, or more generally the constructible or semi-algebraic set is the studied object.

To give a simple example, in $\mathbb{C}^2$ the variety $\{(0,0)\}$ can be seen like the zeros set of more or less complicated ideals (for example, ideal(X, Y), ideal(X^2, Y), ideal(X^2, X, Y, Y^3), etc). The entry which is given to us is a system of equations, i.e. an ideal. It is essential, in many cases, to understand the structure of this object to be able to correctly treat the degenerated cases. A striking example is certainly the study of the singularities. To take again the preceding example, the variety is not singular, but this cannot be detected by the blind application of the Jacobian criterion (one could wrongfully think that all the points are singular, contradicting, for example, Sard's lemma).

The basic tools that we develop and use to understand in an automatic way the algebraic and geometrical structures are on the one hand Gröbner bases (most known object used to represent an ideal without loss of information) and in the other hand triangular sets (effective way to represent the varieties).

On these two points, the pressure is strong since many teams work on these two objects. To date, our project however has a consequent advance in the computation of Gröbner bases (algorithms F_5 and F_7 of Faugère for Gröbner bases) and is a main contributor in the homogeneisation and comprehension of the triangular structures [2].

2.1.1 Gröbner basis and triangular sets

- **Contacts :** J.C. Faugère (Gröbner bases), P. Aubry (Triangular sets)
- **Other participants** G. Ars, M. Bardet, S. Lacharte, D. Lazard, M. Safey El Din.

Let us denote by $K[X_1, \ldots, X_n]$ the ring of polynomials with coefficients in a field K and indeterminates $X_1, \ldots, X_n$ and $S = \{P_1, \ldots, P_s\}$ any subset of $K[X_1, \ldots, X_n]$. A point $x \in \mathbb{C}^n$ is a zero of S if $P_i(x) = 0 \quad \forall i = 1 \ldots s$.

The ideal $\mathcal{I} = \langle P_1, \ldots, P_s \rangle$ generated by $P_1, \ldots, P_s$ is the set of polynomials in $K[X_1, \ldots, X_n]$ constituted by all the combinations $\sum_{k=1}^{R} P_k U_k$ with $U_k \in \mathbb{Q}[X_1, \ldots, X_n]$. Since every element of $\mathcal{I}$ vanishes at each zero of S, we denote by $V_C(S) = V_C(I) = \{x \in C^n \mid p(x) = 0 \; \forall p \in \mathcal{I}\}$ (resp. $V_R(S) = V_R(I) = V_{\mathbb{C}}(I) \bigcap \mathbb{R}^n$), the set of complex (resp. real) zeros of S, where R is a real closed field containing K and C its algebraic closure.

One Gröbner basis' main property is to provide an algorithmic method for deciding if a polynomial belongs or not to an ideal through a reduction function denoted "Reduce" from now.

If G is a Gröbner basis of an ideal $\mathcal{I} \subset \mathbb{Q}[X_1, \ldots, X_n]$ for any monomial ordering $<$.

(i) a polynomial $p \in \mathbb{Q}[X_1, \ldots, X_n]$ belongs to $\mathcal{I}$ if and only if Reduce$(p, G, <) = 0$,

(ii) Reduce(p,G,$<$) does not depend on the order of the polynomials in the list G, thus, this is a canonical reduced expression modulus $\mathcal{I}$, and the Reduce function can be used as a *simplification* function.

Gröbner bases are computable objects. The most popular method for computing them is Buchberger's algorithm ([15], [14]). It has several variants and it is implemented in most of general computer algebra systems like Maple or Mathematica. The computation of Gröbner bases using Buchberger's original strategies has to face to two kind of problems :

- (A) arbitrary choices : the order in which are done the computations has a dramatic influence on the computation time;
- (B) useless computations : the original algorithm spends most of its time in computing 0.

For problem (A), J.C. Faugère proposed ([26] - algorithm F_4) a new generation of powerful algorithms ([26]) based on the intensive use of linear algebra technics. In short, the arbitrary choices are left to computational strategies related to classical linear algebra problems (matrix inversions, linear systems, etc.).

For problem (B), J.C. Faugère proposed ([34]) a new criterion for detecting useless computations. Under some regularity conditions on the system, it is now proved that the algorithm do never perform useless computations.

A new algorithm named F_5 has been built using these two key results. Even if it still computes a Gröbner basis, the gap with existing other strategies is consequent. In particular, due to the range of examples that become computable, Gröbner basis can be considered as a reasonable computable object in large applications.

We pay a particular attention to Gröbner bases computed for elimination orderings since they provide a way of "simplifying" the system (a equivalent system with a structured shape). For example, a lexicographic Gröbner basis has always the following shape :

$$\begin{cases} f(X_1) = 0 \\ f_2(X_1, X_2) = 0 \\ \vdots \\ f_{k_2}(X_1, X_2) = 0 \\ f_{k_2+1}(X_1, X_2, X_3) = 0 \\ \vdots \\ f_{k_{n-1}+1}(X_1, \ldots, X_n) = 0 \\ \vdots \\ f_{k_n}(X_1, \ldots, X_n) = 0 \end{cases}.$$

(some of the polynomials may be identically null). A well known property is that the zeros of the first non null polynomial define the Zariski closure (classical closure in the case of complex coefficients) of the projection on the coordinate's space associated with the smallest variables.

A triangular set is a system with the following shape :

$$\begin{cases} t_1(X_1) = 0 \\ t_2(X_1, X_2) = 0 \\ \vdots \\ t_n(X_1, \ldots, X_n) = 0 \end{cases}$$

(some polynomials may be identically null).

Such kinds of systems are algorithmically easy to use, for computing numerical approximations of the solutions in the zero-dimensional case or for the study of the singularities of the associated variety (triangular minors in the Jacobian matrices). Except if they are linear, algebraic systems cannot, in general, be rewritten as a single triangular set, one speaks then of decomposition of the systems in several triangular sets.

Triangular sets appear under various names in the field of algebraic systems. In 1932 J.F. Ritt ([69]) introduced them as characteristic sets for prime ideals in the context of differential algebra. His constructive algebraic tools were adapted by W.T. Wu in the late seventies for geometric applications. Wu presented an algorithm for computing characteristic sets of finite polynomial sets which do not generate necessarily prime ideals ([103],[104]). With Wu, several authors such S.C. Chou, X.S. Gao, G. Gallo, B. Mishra, D. Wang then developed this approach to make it more efficient.

In 1991, Lazard [50] and Kalkbrener [47] presented triangular decomposition algorithms with nicer properties for their outputs, based on additional requirements for the triangular sets and a generalisation of the gcd of univariate polynomials over a product of fields.

The concept of regular chain introduced in [47] and [105] is adapted for recursive computations in a univariate way and provides a membership test and a zero-divisor test for the strongly unmixed dimensional ideal it defines. Kalkbrenner defined regular triangular sets and showed how to decompose algebraic varieties as a union of Zariski closures of zeros of regular triangular sets. Gallo showed that the principal component of a triangular decomposition can be computed in $O(d^{O(n^2)})$ (n= number of variables, d=degree in the variables). During the 90s, implementations of various strategies of decompositions multiply, but they drain relatively heterogeneous specifications.

Following Kalkbrener's work, Aubry presented an algorithm for decomposing the radical of an ideal into separable regular chains that define radical strongly unmixed dimensional ideals ([1]).

P. Aubry and D. Lazard contributed to the homogenisation of the work completed in this field by proposing a series of specifications and definitions gathering the whole of former work [2]. Two essential concepts for the use of these sets (regularity, separability) at the same time allow from now on to establish a simple link with the studied varieties and to specify the computed objects precisely.

For $p \in K[X_1, \ldots, X_n] \setminus \mathbb{Q}$, we denote by $\mathrm{mvar}(p)$ (and we call *main variable* of p) the greatest variable appearing in p w.r.t. a fixed lexicographic ordering.

- h_i the leading coefficient of t_i (when $t_i \neq 0$ it is seen as a univariate polynomial in its main variable), and $h = \Pi_{i=1,t_i\neq 0}^{n} h_i$.
- $s_i = \frac{\partial t_i}{\partial X_i}$ the separant of t_i (when $t_i \neq 0$) $s = \Pi_{i=1,t_i\neq 0}^{n} s_i$.
- $\mathrm{sat}(T) =< T >: h^\infty = \{p \in K[X_1, \ldots, X_n] \mid \exists m \in \mathbb{N},\ h^m p \in \langle T \rangle\}$; the variety of T is $\mathrm{V}(\mathrm{sat}(T))$ and we have $\overline{\mathrm{V}(T) \setminus \mathrm{V}(h)} = \mathrm{V}(sat(T))$ (elementary property of localization).

A triangular set $T = (t_1, \ldots, t_n) \subset K[X_1, \ldots, X_n]$ is said to be regular (resp. separable) if $\forall i \in \{1, \ldots, n\}$ such that $t_i \neq 0$, the normalization of its initial h_i (resp. of its separant s_i) is a non zero polynomial.

One can always decompose a variety as the union of the varieties of regular and separable triangular sets ([1],[2]) :

$$V_C = \bigcup_i \mathrm{V}(\mathrm{sat}(T_i)). \tag{1}$$

A remarkable and fundamental property in the use we have of the triangular sets is that the ideals $\mathrm{sat}(T_i)$, for regular and separable triangular sets, are radical and equi-dimensional. These properties are essential for some of our algorithms. For example, having radical and equi-dimensional ideals allows us to compute straightforwardly the singular locus of a variety by canceling minors of good dimension in the Jacobian matrix of the system. This is naturally a basic tool for some algorithms in real algebraic geometry [3], [87], [88].

Triangular sets based technics are efficient for specific problems like computing Galois ideals [4], but the implementations of direct decompositions into triangular sets do not currently reach the level of efficiency of Gröbner bases in terms of computable classes of examples. Anyway, our team benefits from the progress carried out in this last field since we currently perform decompositions into regular and separable triangular sets through lexicographical Gröbner bases computations (the process provides in the meantime Gröbner bases of the ideals $\mathrm{sat}(T_i)$).

2.1.2 Zero-dimensional systems

- **Contacts :** F. Rouillier (Real Roots) J.C. Faugère (Gröbner bases)
- **Other participants** P. Aubry, A. Hashemi, D. Lazard, P. Trébuchet.

A system is zero-dimensional if the set of the solutions in an algebraically closed field is finite. In this case, the set of solutions does not depend on the chosen algebraically closed field.

Such a situation can easily be detected on a Gröbner basis for any admissible monomial ordering.

These systems are mathematically particular since one can systematically bing back to solve linear algebra problems. More precisely, the algebra $K[X_1, \ldots, X_n]/I$ is in fact a K - vector space of dimension equal to the numer of complex roots of the system (counted with multiplicities). We chose to exploit this structure. Accordingly, computing a base of $K[X_1, \ldots, X_n]/I$ is essential. A Gröbner basis gives a canonical projection from $K[X_1, \ldots, X_n]$ to $K[X_1, \ldots, X_n]/I$, and thus provides a base of the quotient algebra and many other informations more or less straightforwardly (number of complex roots for example).

The use of this vector-space structure is well known and at the origin of the one of the most known algorithms of the field ([29]) : it allows to deduce, starting from a Gröbner basis for any ordering, a Gröbner base for any other ordering (in practice, a lexicographic basis, which are very difficult to calculate directly). It is also common to certain semi-numerical methods since it allows to obtain quite simply (by a computation of eigenvalues for example) the numerical approximation of the solutions (this type of algorithms is developed, for example, in the INRIA Galaad project).

Contrary to what is written in a certain literature, the computation of Gröbner bases is not "doubly exponential" for all the classes of problems. In the case of the zero-dimensional systems, it is even shown that it is simply exponential in the number of variables, for a degree ordering and for the systems without zeros at infinity. Thus, an effective strategy consists in computing a Gröbner basis for a favourable ordering and then to deduce, by linear algebra technics, a Gröbner base for a lexicographic ordering [29].

The case of the zero-dimensional systems is also specific for triangular sets. Indeed, in this particular case, we have designed algorithms that allow to compute them efficiently [51] starting from a lexicographic Gröbner basis. Note that, in the case of zero-dimensional systems, regular triangular sets are Gröbner bases for a lexicographical order.

Many teams work on Gröbner bases and some use triangular sets in the case of the zero-dimensional systems, but to our knowledge, very few continue the work until a numerical resolution and even less tackle the specific problem

of computing the real roots. It is illusory, in practice, to hope to obtain numerically and in a reliable way a numerical approximation of the solutions straightforwardly from a lexicographical basis and even from a triangular set. This is manily due to the size of the coefficients in the result (rational number).

Our specificity is to carry out the computations until their term thanks to two types of results :

- the computation of the Rational Univariate Representation [73] : we shown that any zero-dimensional system, depending on variables $X_1, \dots X_n$, can systematically be rewritten, without loss of information (multiplicities, real roots), in the form $f(T) = 0, X_i = g_i(T)/g(T), i = 1 \dots n$ where the polynomials $f, g, g_1, \dots g_n$ have coefficients in the same ground field as those of the system and where T is a new variable (independant from $X_1, \dots X_n$).
- efficient algorithms for solving (real roots isolation and counting) univariate polynomials [83],[62],[61].

Thus, the use of innovative algorithms for Gröbner bases computations [26], [34], Rational Univariate representations ([29] for the "shape position" case and [73] for the general case), allows to use zero-dimensional solving as sub-task in other algorithms.

2.1.3 Positive-dimensional and parametric systems

- **Contacts :** F. Rouillier (Parametric systems), M. Safey El Din (Critical points methods)
- **Other participants** P. Aubry, J.C. Faugère, A. Hashemi, D. Lazard, G. Moroz.

When a system is **positive dimensional** (with an infinite number of complex roots), it is no more possible to enumerate the solutions. Therefore, the solving process reduces to decomposing the set of the solutions into subsets which have a well-defined geometry. One may perform such a decomposition from an algebraic point of view or from a geometrical one, the latter meaning not taking the multiplicities into account (structure of primary components of the ideal is lost).

Although there exist algorithms for both approaches, the algebraic point of view is presently out of the possibilities of practical computations, and we restrict ourselves to geometrical decompositions.

When one studies the solutions in an algebraically closed field, the decompositions which are useful are the equi-dimensional decomposition (which consists in considering separately the isolated solutions, the curves, the surfaces, $\dots$) and the prime decomposition (decomposes the variety into irreducible components). In practice, our team works on algorithms for decomposing the system into *regular separable triangular sets*, which corresponds to a decomposition in equi-dimensional but not necessarily irreducible components. These irreducible components may be obtained at the end by using polynomial factorization.

However, in many situations one is looking only for real solutions satisfying some inequalities ($P_i > 0$ or $P_i \geq 0$)[1]. In this case, there are various kinds of decompositions besides the above ones: connected components, cellular or simplicial decompositions, $\dots$

There are general algorithms for such tasks, which rely on Tarski's quantifier elimination. Unfortunately, these problems have a very high complexity, usually doubly exponential in the number of variables or the number of blocks of quantifiers, and these general algorithms are intractable. It follows that the output of a solver should be restricted to a partial description of the topology or of the geometry of the set of solutions, and our research consists in looking for more specific problems, which are interesting for the applications, and which may be solved with a reasonable complexity.

We focus on 2 main problems :

- computing one point on each connected components of a semi-algebraic set;
- solving systems of equalities and inequalities depending on parameters.

[1] In the zero-dimensional case, inequations and inequalities are usually taken into account only at the end of the computation, to eliminate irrelevant solutions.

Critical point methods The most widespread algorithm computing sampling points in a semi-algebraic set is the Cylindrical Algebraic Decomposition Algorithm due to Collins [19]. With slight modifications, this algorithm also solves the problem of Quantifier Elimination. It is based on the recursive elimination of variables one after an other ensuring nice properties between the components of the studied semi-algebraic set and the components of semi-algebraic sets defined by polynomial families obtained by the elimination of variables. It is doubly exponential in the number of variables and its best implementations are limited to problems in 3 or 4 variables.

Since the end of the eighties, alternative strategies (see [41, 42, 43, 10, 8]) with a single exponential complexity in the number of variables have been developed. They are based on the progressive construction of the following subroutines:

(a) solving zero-dimensional systems: this can be performed by computing a Rational Univariate Representation (see [73]);

(b) computing sampling points in a real hypersurface: after some infinitesimal deformations, this is reduced to problem (a) by computing the critical locus of a polynomial mapping reaching its extrema on each connected component of the real hypersurface;

(c) computing sampling points in a real algebraic variety defined by a polynomial system: this is reduced to problem (b) by considering the sum of squares of the polynomials;

(d) computing sampling points in a semi-algebraic set: this is reduced to problem (c) by applying an infinitesimal deformation.

On the one hand, the relevance of this approach is based on the fact that its complexity is asymptotically optimal. On the other hand, some important algorithmic developments have been necessary to obtain efficient implementations of subroutines (b) and (c).

During the last years, we focused on providing efficient algorithms solving the problems (b) and (c). The used method rely on finding a polynomial mapping reaching its extrema on each connected component of the studied variety such that its critical locus is zero-dimensional. For example, in the case of a smooth hypersurface whose real counterpart is compact choosing a projection on a line is sufficient. This method is called in the sequel the critical point method. We started by studying problem (b) [81].

Even if we showed that our solution may solve new classes of problems ([82]), we have chosen to skip the reduction to problem (b), which is now considered as a particular case of problem (c), in order to avoid an artificial growth of degree and the introduction of singularities and infinitesimals.

Putting the critical point method into practice in the general case requires to drop some hypotheses. First, the compactness assumption, which is in fact intimately related to an implicit properness assumption, has to be dropped. Second, algebraic characterizations of critical loci are based on assumptions of non-degeneracy on the rank of the Jacobian matrix associated to the studied polynomial system. These hypotheses are not satisfied as soon as this system defines a non-radical ideal and/or a non equi-dimensional variety, and/or a non-smooth variety. Our contributions consist in overcoming efficiently these obstacles ([84],[76]) and several strategies have been developed [3], [87],[88].

The properness assumption can be dropped by considering the square of a distance function to a generic point instead of a projection function: indeed each connected component contains at least a point minimizing locally this function. Performing a radical and equi-dimensional decomposition of the ideal generated by the studied polynomial system allows to avoid some degeneracies of its associated Jacobian matrix. At last, the recursive study of overlapped singular loci allows to deal with the case of non-smooth varieties. These algorithmic issues allow to obtain a first algorithm [3] with reasonable practical performances.

Since projection functions are linear while the distance function is quadratic, computing their critical points is easier. Thus, we have also investigated their use. A first approach [87] consists in studying recursively the critical locus of projection functions on overlapped affine subspaces containing coordinate axes combined with the study of their set of non-properness. A more efficient one [88], avoiding the study of sets of non-properness is obtained by considering iteratively projections on *generic* affine subspaces restricted to the studied variety and fibers on arbitrary points of these subspaces intersected with the critical locus of the corresponding projection. The underlying algorithm is the most efficient we obtained.

The algorithms of [3],[87] are provided in the Maple Library RAGLib. It is built upon the softwares Gb and RS. It contains functionalities for computing sample points in real algebraic varieties, semi-algebraic sets defined by non-strict inequalities, and the radical and equi-dimensional decomposition of an ideal. The experimental version of the algorithm provided in [85] will be included in the next release which is in preparation.

In terms of complexity, we have proved in [86] that when the studied polynomial system generates a radical ideal and defines a smooth algebraic variety, the output of our algorithms is smaller than what could be expected by applying the classical Bézout bound and than the output of the previous algorithms. This has also given new upper bounds on the number of connected components of a smooth real algebraic variety which improve the classical Thom-Milnor bound. The technique we used, also allows to prove that the degree of the critical locus of a projection function is inferior or equal to the degree of the critical locus of a distance function. Finally, it shows how to drop the assumption of equidimensionality required in the aforementioned algorithms. This technique is based on the study of the Lagrange's system associated to a polynomial family, the study of its bi-homogeneous structure, and a strong bi-homogeneous Bézout theorem we proved which allows to bound the sum of the degrees of all the isolated primary components of an ideal generated by a bi-homogeneous system.

Parametric systems Most of the applications we recently solved (celestial mechanics, cuspidal robots, statistics, etc.) require the study of semi-algebraic systems depending on parameters. Although we covered these subjects in an independent way, some general algorithms for the resolution of this type of systems can be proposed from these experiments.

The general philosophy consists in studying the generic solutions independently from algebraic subvarieties (which we call from now on discriminant varieties) of dimension lower than the semi-algebraic set considered. The study of the varieties thus excluded can be done separately to obtain a complete answer to the problem, or is simply neglected if one is interested only in the generic solutions, which is the case in some applications.

We recently proposed a new framework for studying basic constructible (resp. semi-algebraic) sets defined as systems of equations and inequations (resp. inequalities) depending on parameters. Let's consider the basic semi-algebraic set

$$\mathcal{S} = \{x \in \mathbb{R}^n \ , \ p_1(x) = 0, \ldots, p_s(x) = 0, f_1(x) > 0, \ldots f_s(x) > 0\}$$

and the basic constructible set

$$\mathcal{C} = \{x \in \mathbb{C}^n \ , \ p_1(x) = 0, \ldots, p_s(x) = 0, f_1(x) \neq 0, \ldots f_s(x) \neq 0\}$$

where p_i, f_j are polynomials with rational coefficients.

- $[U, X] = [U_1, \ldots U_d, X_{d+1}, \ldots X_n]$ is the set of *indeterminates* or variables, while $U = [U_1, \ldots U_d]$ is the set of *parameters* and $X = [X_{d+1}, \ldots X_n]$ the set of *unknowns*;
- $\mathcal{E} = \{p_1, \ldots p_s\}$ is the set of polynomials defining the equations;
- $\mathcal{F} = \{f_1, \ldots f_l\}$ is the set of polynomials defining the inequations in the complex case (resp. the inequalities in the real case);
- For any $u \in C^d$ let ϕ_u be the specialization $U \longrightarrow u$;
- $\Pi_U : \mathbb{C}^n \longrightarrow \mathbb{C}^d$ denotes the canonical projection on the parameter's space $(u_1, \ldots, u_d, x_{d+1}, \ldots, x_n) \longrightarrow (u_1, \ldots, u_d)$;
- Given any ideal I we denote by $\mathrm{V}(I) \subset \mathbb{C}^n$ the associated (algebraic) variety. If a variety is defined as the zero set of polynomials with coefficients in $\mathbb{Q}$ we call it a $\mathbb{Q}$-algebraic variety; we extend naturally this notation in order to talk about $\mathbb{Q}$-irreducible components, $\mathbb{Q}$-Zariski closure, etc.
- for any set $\mathcal{V} \subset \mathbb{C}^n$, $\overline{\mathcal{V}}$ will denote its $\mathbb{C}$-Zariski closure in $\mathbb{C}^n$.

In most applications, $\mathrm{V}(< \phi_u(\mathcal{E}) >))$ as well as $\phi_u(\mathcal{C}) = \Pi_U^{-1}(u) \bigcap \mathcal{C}$ are finite and not empty for almost all parameter's u. Most algorithms that study $\mathcal{C}$ or $\mathcal{S}$ (number of real roots w.r.t. the parameters, parameterizations of the solutions, etc.) compute in any case a $\mathbb{Q}$-Zariski closed set $W \subset C^d$ such that for any $u \in \mathbb{C}^d \setminus W$, there exists a neighborhood $\mathcal{U}$ of u with the following properties :

- $(\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}$; this implies that the elements of $\mathcal{F}$ do not vanish (and so have constant sign in the real case) on the connected components of $\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}$;

We recently show that the parameters' set such that there doesn't exist any neighborhood $\mathcal{U}$ with the above analytic covering property is a $\mathbb{Q}$-Zariski closed set which can exactly be computed. We name it the *minimal discriminant variety of $\mathcal{C}$ with respect to* Π_U and propose also a definition in the case of non generically zero-dimensional systems [80], [79].

Being able to compute the minimal discriminant variety allows to simplify the problem depending on n variables to a similar problem depending on d variables (the parameters) : it is sufficient to describe its complementary in the parameters' space (or in the closure of the projection of the variety in the general case) to get the full information about the generic solutions (here generic means for parameters' values outside the discriminant variety).

Then being able to describe the connected components of the complementary of the discriminant variety in $\mathbb{R}^d$ becomes a main challenge which is strongly linked to the work done on positive dimensional systems. Moreover, rewriting the systems involved and solving zero-dimensional systems are major components of the algorithms we plan to build up.

We currently propose several computational strategies. An a priori decomposition into equidimensional components as zeros of radical ideals simplifies the computation and the use of the discriminant varieties. This preliminary computation is however sometimes expensive, so we are developing adaptive solutions where such decompositions are call by need. The main progress is that the resulting methods are fast on easy problems (generic) and slower on the problems with strong geometrical contents.

We also defined (large) *discriminant varieties of $\mathcal{C}$ with respect to* Π_U as being any $\mathbb{Q}$-Zariski closed set W containing the minimal discriminant variety of $\mathcal{C}$ with respect to Π_U (the minimal dicriminant variety is the smallest discriminant variety and it is uniquely defined).

The existing implementations of algorithms able to "solve" (to get some information about the roots) parametric systems do all compute (directly or indirectly) discriminant varieties but none computes optimal objects (strict discriminant variety). The consequence is that the output (case distinctions w.r.t. parameters' values) are huge compared with the results we can provide.

The Cylindrical Algebraic Decomposition adapted to $\mathcal{E} \bigcup \mathcal{F}$ [19] computes explicitly a discriminant variety of $\mathcal{C}$ as soon as the recursive projection steps w.r.t. $X_{d+1}, \ldots, X_n$ are done first. A discriminant variety will then be defined by the union of the varieties associated with the polynomials obtained after the $n-d$-th projection step. It is far from being optimal with respect to the number of elements in the induced partition; in fact it contains at least, a discriminant variety for any system of equalities and inequalities that can be constructed with the polynomials of $\mathcal{E} \bigcup \mathcal{F}$. The same remark applies for recursive methods based on univariate resultant.

Algorithms based on "Comprehensive Gröbner bases" [97], [98], [99], compute also (implicitly or explicitly) discriminant varieties. In the case of parametric systems, such a discriminant variety contains the parameters' values for which a Gröbner basis do not specialize properly. Again, it is far from being optimal since it contains the parameter's values where the staircase varies, which depend on the strategy used (for example the choice of a monomial ordering).

Methods that compute parameterizations of the solutions (see [89] for example) compute also discriminant varieties. Again, these are not optimal since they depend on the strategy used. Precisely, the result depends on an arbitrary chosen "separating element" $t \in \mathbb{Q}[X_{d+1}, \ldots, X_n]$ which is a polynomial (often a linear form) that induces, for almost all the parameters, an injective map from $\mathrm{V}(< \mathcal{E} >)$ to C^d. If p is the minimal polynomial of t viewed as an element of $\mathbb{Q}(U_1, \ldots, U_d)[X_{d+1}, \ldots, X_n]/\sqrt{< \mathcal{E} >}$, the induced discriminant variety contains all the parameters' values such that the leading coefficient of p or its discriminant vanishes; this includes, in particular, the parameter's values such that t does not separate the zeros of the corresponding specialization of $\sqrt{< \mathcal{E} >}$.

2.2 Applications

Applications are fundamental for our research for several reasons.

The first one is that they are the only source of fair tests for the algorithms. In fact, the complexity of the solving process depends very irregularly of the problem itself. Therefore, random tests do not give a right idea of the practical behavior of a program, and the complexity analysis, when possible, does not necessarily provide realistic information.

A second reason is that, as quoted above, we need real world problems to determine which specifications of algorithms are really useful. Conversely, it is frequently by solving specific problems through ad hoc methods that we found new algorithms with general impact.

Finally, obtaining successes with problems which are intractable by the other known approaches is the best proof for the quality of our work.

On the other hand, there is a specific difficulty. The problems which may be solved with our methods may be formulated in many different ways, and their usual formulation is rarely well suited for polynomial system solving or for exact computations. Frequently, it is not even clear that the problem is purely algebraic, because researchers and engineers are used to formulate them in a differential way or to linearize them.

Therefore, our software may not be used as black boxes, and we have to understand the origin of the problem in order to translate it in a form which is well suited for our solvers.

It follows that many of our results, published or in preparation, are classified in scientific domains which are different from ours, like cryptography, error correcting codes, robotics, signal processing, statistics or biophysics.

2.2.1 Cryptography

- **Contact :** J.C. Faugère
- **Other participants** G. Ars, M. Bardet, S. Lacharte

The idea of using multivariate (quadratic) equations as a basis for building public key cryptosystems appeared with the Matsumoto-Imai cryptosystem. This system was first broken by Patarin and, shortly after, Patarin proposed to repair it and thus devised the hidden field equation (HFE) cryptosystem.

The basic idea of HFE is simple: build the secret key as a univariate polynomial $S(x)$ over some (big) finite field (often GF(2^n)). Clearly, such a polynomial can be easily evaluated; moreover, under reasonable hypotheses, it can also be "inverted" quite efficiently. By inverting, we mean finding any solution to the equation $S(x) = y$, when such a solution exists. The secret transformations (decryption and/or signature) are based on this efficient inversion. Of course, in order to build a cryptosystem, the polynomial S must be presented as a public transformation which hides the original structure and prevents inversion. This is done by viewing the finite field GF(2^n) as a vector space over GF(2) and by choosing two linear transformations of this vector space L_1 and L_2. Then the public transformation is the composition of L_1, S and L_2. Moreover, if all the terms in the polynomial $S(x)$ have Hamming weight 2, then it is obvious that all the (multivariate) polynomials of the public key are of degree two.

By using fast algorithms for computing Gröbner bases, it was possible to break the first HFE challenge [44] (real cryptographic size 80 bits and a symbolic prize of 500 US$) in only two days of CPU time. More precisely we have used the $F_5/2$ version of the fast F_5 algorithm for computing Gröbner bases (implemented in C). The algorithms available up to now (Buchberger) were extremely slow and could not have been used to break the code (they should have needed at least a few centuries of computation). The new algorithm is thousands of times faster than previous algorithms. Several matrices have to be reduced (Echelon Form) during the computation: the biggest one has no less than 1.6 million columns, and requires 8 gigabytes of memory. Implementing the algorithm thus required significant programming work and especially efficient memory management.

A new result is that the weakness of the systems of equations coming from HFE instances can be *explained* by the algebraic properties of the secret key (work presented at Crypto 2003 in collaboration with A. Joux). From this study we are able to predict the maximal degree occurring in the Gröbner basis computation, so that we can establish precisely the complexity of the Gröbner attack and compare it with the theoretical bounds.

Since it is easy to transform many cryptographic problems into polynomial equations, our group is in a position to apply this general method to other cryptosystems. Thus we have a new general cryptanalysis approach, called algebraic cryptanalysis. The team is currently testing the robustness of cryptosystems based on nonlinear filter generators (with G. Ars, J.-C. Faugère) and in collaboration with the Codes team and DGA (Celar).

Another relevant tool in the study of cryptographic problems is the LLL algorithm which is able to compute in polynomial time a "good" approximation for the shortest vector problem. Since a Gröbner basis can be seen as the set of smallest polynomials in an ideal with respect to the divisibility of leading terms, it is natural to compare both algorithms: an interesting link between LLL (polynomial version) and Gröbner bases was suggested by a member of our group.

A standard algorithm for implementing the arithmetic of Jacobian groups of curves is LLL. By replacing LLL by the FGLM algorithm we establish a new structure theorem for Gröbner bases; consequently, on a generic input we were able to establish explicit and optimized formulas for basic arithmetic operations in the Jacobian groups of C_{34} curves [6].

As an application of the LLL algorithm we have presented [7], an algorithm for converting a Gröbner basis of an ideal with respect to any given ordering into a Gröbner basis with respect to any other ordering. This algorithm is based on a modified version of the LLL algorithm. The worst case, the theoretical complexity of this algorithm is not necessarily better than the complexity of the FGLM algorithm; but when the output (the final Gröbner basis) is small this algorithm is experimentally more efficient.

2.2.2 Parallel robots

- **Contact :** F. Rouillier
- **Other participants** J.C. Faugère

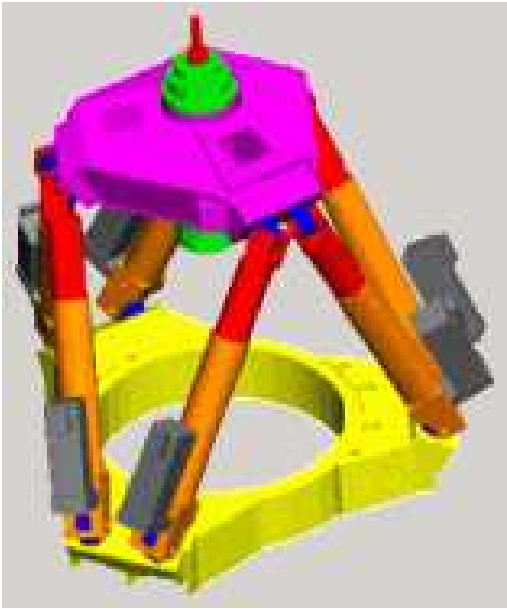

Figure 2: An Hexapod

The (parallel) manipulators we study are general parallel robots: the hexapods are complex mechanisms made up of six (often identical) kinematic chains, of a base (fixed rigid body including six joints or articulations) and of a platform (mobile rigid body containing six other joints).

The design and the study of parallel robots require the resolution of direct geometrical models (computation of the absolute coordinates of the joints of the platform knowing the position and the geometry of the base, the geometry of the platform as well as the distances between the joints of the kinematic chains at the base and the platform) and inverse geometrical models (distances between the joints of the kinematic chains at the base and the platform knowing the absolute positions of the base and the platform).

Since the inverse geometrical models can be easily solved, we focus on the resolution of the direct geometrical models.

The study of the direct geometrical model is a recurrent activity for several members of the project. One can say that the progress carried out in this field illustrates perfectly the evolution of the methods for the resolution of algebraic systems. The interest carried on this subject is old. The first work in which the members of the project took part in primarily concerned the study of the number of (complex) solutions of the problem [54],[52]. The results were often illustrated by Gröbner bases done with Gb software (see section 2.3). One of the remarkable points of this study is certainly the classification suggested in [30]. The next efforts were related to the real roots and the effective computation of the solutions [70]. The studies then continued following the various algorithmic progresses, until the developed tools made possible to solve non-academic problems. In 1999, the various efforts were concretized by an industrial contract with the SME CMW (*Constructions Mécaniques des Vosges-Marioni*) for studying a robot dedicated to machine tools.

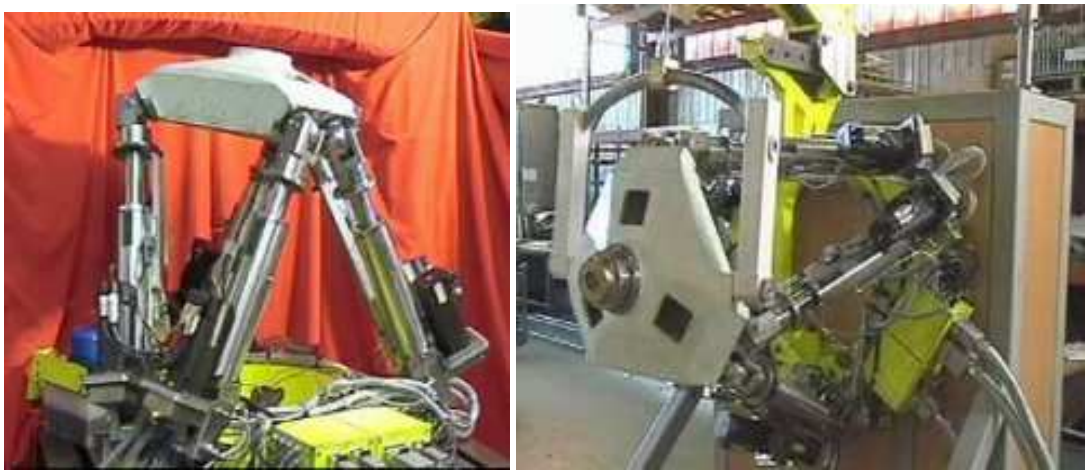

Figure 3: The CMW300

We conceived, in collaboration with the COPRIN project, a prototype of simulator for validating a fixed trajectory, i.e. :

- check that the trajectory is nonsingular for a series of functions modelizing the length of the legs : let us recall that for given values of the legs' length, there exists up to 40 possible positions. To check that the trajectory is nonsingular, one must ensure, for example, that 2 possible trajectories do not intersect (in which case the robot cannot be controlled);
- measure without ambiguity the difference between two trajectories corresponding to different legs' length functions (this is a tool for checking "numerical" singularities).

This tool is single in the world : concurrent solutions exist but can treat only particular robots (plan, symmetrical, less joints, etc). It is necessary to know to how to solve the general case because a small modification of the design parameters' (unavoidable in practice) has serious consequences on the behavior of the robot. For example, the theoretical robot we use (based on the left-hand parallel manipulator due to J.-P. Merlet) for our study admits at most 36 solutions for the direct geometrical model (either up to 36 possible trajectories for fixed length legs' functions), whereas the actually built robot (with small errors on the positions of the joints) has up to 40 possible positions.

The main algorithmic tool present in this simulator (partially presented in [77]) is a hybrid method (mixing computer algebra, numerical computation and interval analysis) for the resolution of the direct geometrical model.

A part of the work was to develop a semi-numerical method (based on Newton's method), powerful in terms of computation time (4000 computations per minute) and certified, i.e. always returning a correct result: the answer is either a set of numerical values with a certified precision or a failure message. The strategy used combines interval arithmetics and convergence results. The failure remains exceptional (less than 10 percent of the practical problems) and, when it occurs, the result is obtained using a special version of the F_4 algorithm for Gröbner bases computation and an optimized version (adapted to that particular case of systems) of the Rational Univariate Representation algorithm.

Our simulator has been used to diagnose the problems related to the solutions currently employed (CAD, look-ahead, algorithms for interpoling the trajectories, etc).

2.2.3 Serial Robots

- **Contact :** F. Rouillier
- **Other participants** P. Aubry, S. Corvez, J.C. Faugère, G. Moroz

Industrial robotic (serial) manipulators with 3 degrees of freedom are currently designed with very simple geometric rules on the designed parameters, the ratios between them are always of the same kind. In order to enlarge the possibilities of such manipulators, it may be interesting to relax some constraints on the parameters.

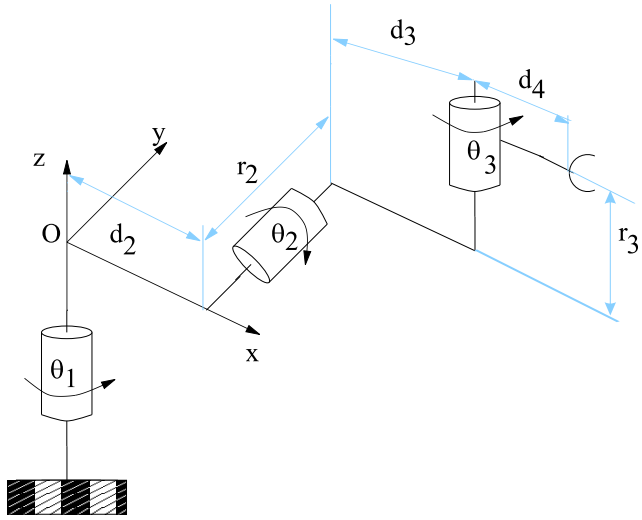

Figure 4: A serial robot with 3 D.O.F.

However, the diversity of the tasks to be done carries out to the study of other types of robots whose parameters of design differ from what is usual and which may have new properties, like stability or existence of new kinds of trajectories.

An important difficulty slows down the industrial use of such new robots : recent studies ([102],[100],[101] and [65]) showed that they may have a behavior which is qualitatively different from those of the robots currently used in industry and allows new changes of posture. These robots, called cuspidal, cannot be controlled like the others. The majority of the robots are in fact cuspidal: the industrial robots currently on the market form a very restricted subclass of all the possible robots.

A full characterization of all the cuspidal robots is of a great interest for the designer and the user. Such a project forms part of a current tendency in robotics which consists in designing a robot in order that its performances are optimal for a given application while preserving the possibility of using it for another task, that is to say to specialize it to the maximum for an application in order to reduce its cost and to increase its operational safety.

The study of the behavior at a change of posture is identical, from the computer algebra point of view, to solving a system of equalities and inequalities depending on three or four parameters which correspond to the design parameters of this kind of robots. The method we basically used was "ad hoc", and no known automatic computer algebra methods were able to solve completely the problem before the work done in collaboration with COPRIN (INRIA Sophia), IRMAR (University of Rennes I) and IRRCyN (CNRS - Nantes) teams.

From a robotic point of view, the result obtained is a full classification of a class of serial robots with three degrees of freedom according to their cuspidal character. Since then, toward the end of the Maths-Stic project "Robots Cuspidaux", these results were simplified and analyzed to allow a better description of the workspace of such mechanisms.

The computations done for this application were critical also for the development of the general and systematic methods for solving parametric systems. We have shown that these general methods can now be used in place of ad hoc computations to calculate the same classification and a recent experiment even shows that they allow to relax one more parameter and thus to solve a more general problem.

2.2.4 Signal Processing

- **Contact :** J.C. Faugère
- **Other participant** F. Rouillier

Some problems in signal theory are naturally formulated in terms of algebraic systems. In [35], we had studied the Kovacevic-Vetterli 's family of filters banks. To be used for image compression, a wavelet transformation must be

defined by a function having a maximum of partial derivative that vanishes at the corners of the image. These conditions can be translated to polynomial systems that can be solved with our methods. We showed that to get physically acceptable solutions, it was necessary to choose the number of conditions so that the solutions' space is of dimension 0, 2 or 4 (according to the size of the filter). This result (parametric family of filters) is subject to a patent [28]. To exploit these filters in practice, it remains to choose the best transformation, according to non-algebraic criteria, which is easily done with traditional tools for optimization (with a reduced number of variables).

As for most of applications on which we work, it took more than three years to obtain concrete results bringing real practical progress (the results mentioned in [72] are partial), and still a few years more to be able to disseminate information towards our community [36]. Our software tools are now used to solve nearby problems [60].

Our activity in signal processing started again a few months ago through a collaboration with the APICS project (collabooration with F. Seyfert) on the synthesis and identification of hyperfrequency filters made of coupled resonant cavities. It is now part of our research objectives (see section 3.3.3).

2.3 Software

Implementation of algorithms is a paramount task to which the members of the project take an active part: indeed a bad implementation can make completely ineffective a potentially good algorithm. An objective of the project is to implement in low-level languages (C/C++) all the critical parts of new algorithms, the remainder of the implementations being more often carried out in high level computer algebra languages such as Maple or MuPAD.

The principal objective of our software activity is the design and the implementation of new algorithms improving the computations' efficiency or their applicability.

A natural classification of our software lies in their bond with our algorithmic research. Indeed, beside software that directly depend on our research activity, the team is brought to develop other software having their own interest, but classified as basic development tools (memory manager, communications protocol) or of software designed to apply our algorithms to specific problems.

Available software can be donwload from `http://fgbrs.lip6.fr/salsa/`.

2.3.1 Basic development packages

GC

- **Contact :** J.C. Faugère
- **Other participant :** F. Rouillier

One specificity in computer algebra is to manipulate huge objects with a size that varies along the algorithm. Having a specific memory manager, adapted to the objects handled in the various implementations is thus essential. Based on one concept suggested by J-C. Faugère in his PhD thesis, several versions implemented in C are used in different software packages of the project (GB, FGB, RS) as well as in implementations due to collaborators (F. Boulier - LIFL). The various suggested implementations are very simple and it seems preferable to precisely describe the process and its use in some key situations than to propose a standardized implementation as a library.

UDX

- **Contact :** F. Rouillier
- **Other participant :** J.C. Faugère

The result of a Gröbner basis computation may be huge and is the main input of our high-level algorithms. The time needed for transfering such an object using ascii files or pipes may be greater than the computation time.

UDX is a software for binary data exchange. It was initially developed to show the power of a new protocol, object of a patent by INRIA and UPMC [31]. The resulting code, written in ANSI C (9500 lines), is very portable and very efficient, even when the patented protocol is not used. UDX is composed of five independent modules:

- base: optimized system of buffers and synchronization of the input and output channels;
- supports: read/write operations on various supports (sockets, files, shared memory, etc.);

- protocols: various exchange protocols (patented protocol, XDR, etc.);
- exchange of composite types: floating-point numbers (simple and double precision), multiprecision integers, rational numbers;
- interfaces: user interfaces implementing high level callings to the four other modules.

UDX is used in some interfaces developed in the project (GB, RS, MuPAD) but also in software from other projects (SYNAPS and ROXANE, in collaboration with the INRIA project GALAAD [66], MuPAD/Scilab interface distributed with MuPAD 2.5.1).

MPFI

- **Contact :** F. Rouillier

MPFI is a library for multiprecision interval arithmetic, written in C (approximately 1000 lines), based on MPFR. It is developped in collaboration with N. Revol (ARENAIRE project). Initially, MPFI was developed for the needs of a new hybrid algorithm for the isolation of real roots of polynomials with rational coefficients. MPFI contains the same number of operations and functions as MPFR, the code is available and documented.

MPAI

- **Contact :** P. Trébuchet
- **Other participant :** F. Rouillier

MPAI is a library for computing with algebraic infinitesimals. The infinitesimals are represented as truncated series. The library provides all the arithmetic functions needed to perform computations with infinitesimals. The interface is both GMP and RS compliant. It is implemented in the C language and represents approximatively 1000 lines of code. The algorithms proposed in MPAI include Karatsuba's product and the short product, ... The code is available.

INTERFACES

- **Contacts :** J.C. Faugère (Maple, Mathematica), F. Rouillier (UDX, MuPAD)

In order to ease the use of the various software developed in the project, some conventions for the exchange of ASCII and binary files were developed and allow a flexible use of the servers GB , FGB or RS .

To make transparent the use of our servers from general computer algebra systems such as Maple or MuPAD we currently propose a common distribution for GB , FGB and RS including the servers as well as the interfaces for Maple and MuPAD. The instructions are illustrated by concrete examples and a simple installation process.

2.3.2 Low level Algorithms

GB

- **Contact :** J.C. Faugère.

Gb is one of the most powerful software for computing Gröbner bases currently diffused. Implemented in C/C++ (approximately 100000 lines), it is distributed since 1994 in the form of specific servers (direct computations, changes of orders, Hilbert's function, etc.). The initial interface (interactive system of commands) was abandoned for lighter solutions (ASCII interface, UDX protocol) which are more powerful but for the moment more rudimentary. With the new algorithms proposed by J-C. Faugère ($F_n, n > 1$), GB is always maintained but is not developed any more. Indeed, data structures as well as basic algorithms necessary to implementations of these new methods being radically different from precedents, the GB servers will be gradually replaced by FGB servers. The existing prototypes of interfaces (ASCII, Maple, MuPAD, RS) were homogenized in order to provide a framework, initially based on GB, but evolutionary (towards FGB) in a transparent way. They will be kept. The future evolutions will follow then algorithmic progress.

RS

- **Contact :** F. Rouillier.

RS is a software dedicated to the study of real roots of algebraic systems. It is entirely developed in C (100000 lines approximately) and succeeds to REALSOLVING developed during the European projects PoSSo and FRISCO. RS mainly contains functions for counting and isolating of real zeros of zero-dimensional systems. The user interfaces of RS are entirely compatible with those of GB/FGB (ASCII, MuPAD, Maple). RS is used in the project since several years and several development versions have been installed by numerous other teams. The following evolutions will depend on algorithmic progress and the users' needs (many internal functions are exported on demand).

TRIANGULAR DECOMPOSITIONS

- **Contact :** P. Aubry

Triangular Decomposition is a library devoted to the decomposition of systems of polynomial equations and inequations and provides some tools for working with triangular sets. It decomposes the radical of the ideal generated by a family of polynomials into regular triangular sets that represents radical equidimensional ideals. It also performs the computation of polynomial gcd over an extension field or a product of such fields given by a triangular set.

A first version of this library is implemented in the Axiom computer algebra system. It is now developed in Magma.

2.3.3 High level algorithms

RAGLIB

- **Contact :** M. Safey El Din

The **RAGLib** (**R**eal **A**lgebraic **G**eometry **Lib**rary) is a Maple library of symbolic algorithms devoted to some problems of Effective Real Algebraic Geometry, and more particularly, to the study of real solutions of polynomial systems of equations and inequalities. It contains algorithms performing:

- the *equi-dimensional decomposition* of an ideal generated by a polynomial family.
- the *emptiness test* of a real algebraic variety defined by a polynomial system of equations.
- the *computation of at least one point in each connected component* of a real algebraic variety defined by a polynomial system of equations.
- the *emptiness test* of a semi-algebraic set defined by a polynomial system of equations and non strict inequalities.
- the *computation of at least one point in each connected component* of a semi-algebraic set defined by a polynomial system of equations and non strict inequalities.

2.3.4 Applicative software

Specific FGB **servers**

- **Contact :** J.C. Faugère

As mentionned above, current implementations of the F_5 algorithm depend on many options. For efficiency reasons, it is currently preferable to compile specific servers, setting algorithms parameters like matrices sizes, linear algebra strategies for sparse matrices by hand. This has already successfully been done for path planning problems (parallel robots), and however helps to understand the main constraints in order to provide, in the future, software solutions that are independent from the type of system to be solved.

Implicit curves drawing (TCI)

- **Contact :** F. Rouillier
- **Other participant :** J.C. Faugère

As soon as they come from real applications, the polynomials resulting from processes of elimination (Gröbner bases, triangular sets) are very often too large to be studied by general computer algebra systems.

In the case of polynomials in two variables, a certified layout is enough in much cases to solve the studied problem (it was the case in particular for some applications in celestial mechanics). This type of layout is now possible thanks to the various tools developed in the project.

Two components are currently under development: the routine of computation (taking as input the polynomial function and returning a set of points) is stable (about 2000 lines in the C language, using the internal libraries of RS) and can be used as a black box in stand-alone mode or through Maple; the routine of layout is under study.

Trajectory Simulator for Parallel Robots (TSPR)

- **Contact :** F. Rouillier
- **Other participant :** J.C. Faugère

The purpose of project TSPR (Trajectory Simulator for Parallel Robots) is to homogenize and export the tools developed within the framework of our applications in parallel robotics. The software components of TSPR (about 1500 lines) are primarily written in C following the standards of RS and FGB and algorithms implemented in Maple using the prototypes of interfaces for FGB and RS . The encapsulation of all these components in a single distribution is available but not downloadable.

Prototypes of components for real-time resolution of certain types of systems now use also the ALIAS library developed in the INRIA project COPRIN.

3 Objectives

3.1 Mathematical objects and algorithms

3.1.1 Gröbner bases and triangular sets

With the development of algorithms using the F_5 technology (criterion and algorithms), one never reaches such a level of performance for the computation of Gröbner bases. This is clearly validated by our work in cryptology.

Complexity Gröbner bases are "doubly exponential" only in pathological cases (never arrive in practice, only one family of examples known). Complexities spread out more subtly depending on the systems' properties. For example, it is well known, that their computation is simply exponential for zero-dimensional systems not admitting zeros at infinity, but on the other hand there are classes of examples for which the final object (output of the algorithm) has a double exponential size. In the case of the applications with coefficients in a finite field (cryptology, error correcting codes) one can easily show that its computation is in the worst case simply exponential (in the number of variables). On the other hand it is necessary to insist on the a priori (simply) exponential character which induces anyway difficult computations in practice.

As the algorithm F_5 avoids the reductions to zero, one can follow it step by step and derive complexity results (as one can easily do it for the Gaussian elimination algorithm). One can thus obtain new complexity formulas (generalizing the results of Macaulay) for the case of over-determined systems. Another drawback of such complexity studies is to guess with precision the cost of the computation of a Gröbner base by way of F_5 algorithm and thus to measure future theoretical improvements of the algorithms. As a first result linked to such studies, we propose a definition of weak regular sequences and their associated notion of regularity. The motivation for studying such regular sequences is that "random" sequences are weak regular, and the degree of regularity is closely related to the global cost of the Gröbner basis computation for a graded admissible monomial order. Following the F_5 algorithm, we show that for (weak) regular sequences, one can precisely control the size of all matrices and deduce the regularity of the sequences.

Using asymptotic analysis methods we can then compute the asymptotic expansion of the maximal degree D_{max} of the polynomials that appear in the algorithm. We show for instance that for n *quadratic equations over GF*(2), we have

$$D_{max} \simeq 0.0900\, n + 1.00\, n^{1/3} - 1.58 + O(n^{-1/3}).$$

The global cost of the Gröbner basis computation is then

$$1.35^{\omega(n+0.77n^{\frac{1}{3}}+O(\log(n)))}$$

with ω the exponent of matrix multiplication complexity.

Systems with coefficients in a field of characteristic zero These last years, we gave the priority to the resolution of systems with coefficients in finite fields, the applications in cryptology having drained a lot of specific developments. This has permitted to grind the computational strategies for algorithms F_4 and F_5. It should be noted, however, that the current implementations of F_5 are limited to particular cases: limited degrees or nature of the coefficients (modulo 2) or homogeneous polynomials. One objective is thus to obtain an efficient general and reliable implementation of this algorithm.

Now that the basic strategies are well understood, one can estimate, at first approximation, that what differentiates the case of systems with coefficients in a field of characteristic 0 from the case of the systems with coefficients in a finite field, lies in the management of linear algebra strategies. Let us recall that the algorithms F_4 and F_5 have as basic sub-routine the resolution of sparse linear systems. If one takes the case of systems with rational coefficients, it will be necessary, for example, to manage problems of growths of coefficients in intermediate computations, which influence dramatically the computing times.

For some coefficients fields (rational or rational fractions for example), one can, via the Chinese theorem or a p-adic method, recover strategies and algorithms developed in the case of finite fields : a first solution will then remain to precisely study the management of the number of specializations to carry out (bounds or strategies for a posteriori checking the result). This type of strategy is already well known by some members of the project, progress and implementations are thus awaited in a near future.

Decompositions of ideals and varieties It appears clearly that the tools for decomposing ideals or varieties in the cases of positive dimensional systems are central in our activity, in particular for the real part.

The needs can be classified into three categories :

(Rad) the computation of a system of generators of the radical of an ideal ; one loses information on the multiplicities but one sticks then to the Nullstellentsatz, which cancels, in some sense, the distinction between ideal and variety representations;

(Dec) equidimensional decomposition of an ideal (i.e. for example to separate the isolated points from the curves and surfaces in the solutions set) ; It is a significant point, in particular in the study of the singular locus of a variety.

(Prim) decomposition of an ideal into prime components;

Note that Gröbner bases, which is the base tool for many algorithms for solving systems without parameters, is not adapted any more, in the state, to answer to questions (Rad), (DEC) or (Prim) since it preserves all the information (multiplicities for example).

In existing strategies, these three simplified forms of systems are generally calculated starting from a Gröbner basis for a lexicographical order. One falls then into a class of complexity doubly exponential in the number of variables as regards intermediate objects sizes, whereas the final objects seem, according to experiment, of moderate size.

It should be noted that (Rad) (respectively (DEC)) results easily from (DEC) (resp. (Prim)). One could thus expect (Rad) to be less expensive than (Prim), however the experiment shows that one of the strategies we intend to develop ([32]) carries out all these tasks in an efficient way and with quite the same computation times. Moreover, even if the time needed to calculate (Prim) is slightly higher than for (Rad) or for (DEC), as the result of (Prim) is to break the initial problem into independent subproblems of smaller sizes, the algorithms for the study of the zeros can then continue on each component (possibly in parallel).

Several members of the project proposed algorithms to calculate (DEC): these algorithms are based on triangular sets. That kind of methods is potentially better than those purely based on Gröbner basis since one considers the radical

of the ideal (ensemblist method) from the beginning and because they induce splits in the algorithm. Another advantage of triangular sets is that the number of generators is bounded by the number of variables. Spectacular progress have already been achieved in terms of efficiency. However there still remains an important work of optimization and fine implementations of these methods to solve large problems.

J.-C. Faugère proposes a new algorithm (F_7 - [32]) which calculates (Prim), the algorithm F_7 itself being based on the algorithm F_5. This algorithm tries to calculate a traditional Gröbner basis but manages to detect the singular matrices which appear in F_5; when it is the case, a split is carried out allowing to break the problem prematurely. The algorithm F_7 also uses in its final phase recent work on fast factorization of polynomials. A first prototype of this algorithm has been implemented showing that, very often, the computation is faster than a basic Gröbner basis computation and, moreover, the quality of the result is strongly improved: the result is unique and mathematically well specified; it has a smaller size (sometimes of a factor 1000 compared with a Gröbner basis) and the structure of each obtained component is more simple.

However the best way of representing mathematically and by means of computable objects a prime component is still an open problem.

Coupling the algorithms described in this paragraph and those from the real part will constitute the core of a complete solver for parameteric and positive dimensional systems.

3.1.2 Zero-dimensional systems

On zero-dimensional systems with coefficients in a field of characteristic 0 (the treatment in the case of finite fields is specific), the possible progress on the algorithms and strategies that we usually use are weak since with our current implementations, the computing times depends mostly on the size of the result, due to massive use of multi-modular computations.

One of our objectives is to increase the classes of examples we can solve: our methods is proved to be reliable on large systems and they are currently conceived to carry out large and long computations. In fact, one realizes that many applications requires the resolution of large numbers of systems which we consider now to be "easy". Without speaking about real time, effectiveness on these examples has to be considered. We should concentrate more on the implementation strategies than on algorithms themselves. The example of the path planning for parallel robots illustrates this problem perfectly (recall it took near from two days of computation a few years ago while approximately a second is now necessary for solving a direct geometrical model).

A part of our work will be turned towards the use of approximate arithmetics and towards the generation of programs without however deviating of our absolute objectives (exact results without nonverifiable assumption on the systems). In many applications, one is brought to solve systems with identical mathematical properties (structure of the algebra quotient, number and multiplicity of the roots). In other words, computations that we carry out generally only differ by the value of the scalars (in opposition to monomials) appearing in handled objects. The idea is to perform a first "normal" computation while keeping some trace, i.e. by locating the operations whose result is necessary for the final expression we want to obtain. This trace will then be used to generate a program, whose parameters will be the scalars appearing in the data, which will calculate the result in a minimal number of operations.

With the first tests on the basic tools for critical points methods in the case of systems of equalities and large inequalities, the resolution of difficult zero-dimensional systems (containing inequalities) becomes one of the blocking step in practice.

Suppose that $\mathcal{S} = \{p_1 = 0, \dots p_r = 0\}$, $p_i \in \mathbb{Q}[X_1, \dots X_n]$ is a zero-dimensional system with D complex roots counted with multiplicities, and let $f_1, \dots f_s$, $f_i \in \mathbb{Q}[X_1, \dots X_n]$ be polynomials with coefficients in $\mathbb{Q}$. One would like to compute the signs of the f_i at the real roots of $\mathcal{S}$. A direct method consists in computing a Rational Univariate Representation [73] of the roots of $\mathcal{S}$ and then to plug it in the expressions of the f_i to reduce the problem to computing the sign of univariate polynomials at the real roots of another univariate polynomial. Suppose that $\{f(T), g_1(T)/g(T), \dots, g_n(T)/g(T)\}$ is a RUR of $\mathcal{S}$. For computing such a substitution, one may homogeneize the f_i and then apply the substitution $h \longrightarrow g$, $X_i \longrightarrow g_i$, $i = 1 \dots n$, where h is the homogeneization variable. Such a computation would cost at least $O(D^3)$ arithmetic operations in $\mathbb{Q}$ and the induced growth of coefficients makes it unfeasible for large problems. We can show that a RUR of $\mathcal{S}'$ can be deduced from a RUR of $\mathcal{S}$ using $O(sD^2)$ arithmetic operations, if algorithm [73] or [13] is used. Note that our strategy gives also better complexity upper bounds for computing simultaneous inequalities than those proposed in [9] in the case of zero-dimensional systems (the problem is fully reduced to compute simultaneous inequalities with univariate polynomials of degree at most D).

The problem is thus currently deferred to the determination of signs of polynomials in one variable at the zeros of another. One can then fully recover our optimizations of algorithms based on Descartes' rule of signs [83] and their generalization for using multiprecision interval arithmetic (see MPFI library in the software section) to carry out this type of treatment. The main difficulty is then to manage carefully the precision used to guarantee at least the sign of the expressions.

This type of strategy is a modest step towards the implementation of an arithmetic on real algebraic numbers. Before attacking this type of ambitious objectives, an intermediate stage and of importance is certainly the resolution of triangular systems without passing by the computation of a RUR. Indeed, this type of systems appears naturally in many problems from algorithmic geometry, mainly in the study of curves and surfaces for Computer Aided Design, as well as in the computation of sample points in the algorithm of Cylindrical Algebraic Decomposition. Let us recall that it is also one of the outputs which we can efficiently provide in the case of the zero-dimensional systems. The existing libraries handling real algebraic numbers are supposed to allow the resolution of polynomials whose coefficients are real algebraic algebraic (one can for example quote the LEDA library), but they, in general do it very ineffectively in the degenerated cases (for example if a polynomial is not squarefree). Indeed, most strategies use bounds to certify the signs of expressions: those being in general catastrophic.

One can easily show that if a triangular set is regular and separable, the computation of its real roots is technically not so much more complicated than the evaluation of a RUR. A first stage, which in addition joined our effective ambitions about the implementation of algorithms for computing triangular sets, will be thus to succeed in calculating in decent times these regular and separable triangular sets. It will primarily be a question of developing methods breaking up an already triangular sytem and of optimizing the strategies on small examples such as those related to the problems of Computer Aided Design. One will slip then gradually to more general systems.

3.1.3 Critical points methods and optimization

The use of the critical point method to compute sampling points in an algebraic variety is now well understood, at least in the cases where the studied variety is smooth and defined by a set of polynomials generating a radical ideal. Even if we will keep on developping strategies to improve our algorithms in these degenerate situations, the core of our project is now oriented according to two axes we describe in detail below:

- the first one focuses on the exploitation of the bi-homogeneous structure of polynomial systems defining critical points of a polynomial mapping in the algorithms of algebraic elimination; it will lead to specific algorithms solving this problem of algebraic optimization;
- the second one focuses on solving polynomial systems of equations and inequalities (by computing sampling points in the semi-algebraic sets they define); by investigating at the same time the use of an infinitesimal arithmetic and the use, in this context, of a notion of generalized critical values.

Algebraic Optimization. As mentioned above, we plan to develop sharper interactions between real solving and algebraic elimination by taking advantage of the bi-homogeneous structure of the Lagrange's system associated to a polynomial family defining the critical locus of a polynomial mapping.

In the context of Gröbner bases, the degree of polynomials appearing during the computations is an important parameter to estimate the complexity of the computation, at least in the case of regular sequences. In the homogeneous case, some results have been obtained by the SPACES project (see [5]) by analyzing the behaviour of the algorithm F_5 (see [34]). A first work consists in estimating this degree in the bi-homogeneous case, and study if some improvements can be brought to the algorithm F_5 in this case.

The structure of bi-homogeneous systems is already exploited in the theory of sparse resultants (see [25]). It allows to predict in the *generic* cases a basis of the ring of polynomials quotiented by the studied ideal. Following [63, 92, 64] linking the work of Macaulay, the methods based on resultant computations and the point of view of Gröbner bases in the homogeneous case, one can hope to use the theory of sparse resultants to compute adapted bases. A first step consists in dealing with *generic* cases which are zero-dimensional regular sequences and then extending the results first to zero-dimensional non-regular sequences and second to positive dimensional cases.

We also plan to develop interactions with triangular sets. Computations of triangular sets are based on gcd computations on algebraic towers of extensions and deal with some splits when a division modulo the considered tower is not possible.

In generic cases, one can prove nice properties on polynomials of the Lagrange's system where Lagrange multipliers are involved. These properties allow to avoid some unnecessary steps testing the invertibility of polynomials modulo a tower of extensions.

Finally, from a more theoretical point of view, we will keep on the quantitative study initiated in [86]. Our aim is to sharpen the given bounds on the degree of critical loci and to generalize the results to non-smooth varieties.

Systems of equations and inequalities. In [10, 8], the authors reduce the problem of computing sampling points in a semi-algebraic set defined by a polynomial system of rational coefficients to the problem of computing sampling points in a real algebraic set defined by polynomial systems with coefficients in a Puiseux series field. This can be done using a single infinitesimal deformation, but then in terms of complexity, a large combinatorial factor is introduced. This combinatorial factor can be decreased by introducing a second infinitesimal: this allows to put the studied polynomial family in general position, so that the co-dimension of the algebraic variety it defines is its cardinality.

A first step of our project consists in isolating the computational problems related to the introduction of the first infinitesimal. To this end, we will keep on the development of the library MPAI [91] which encodes infinitesimals by truncated series with fixed precision. A mechanism, allowing to increase the precision if necessary, has to be incorporated. Then, this arithmetic has to be interfaced with elimination tools used in [85]. To avoid the introduction of a second infinitesimal, some ideal membership tests can be used.
Developping such a strategy requires also strong theoretical developments: knowing in advance the required precision is an information of first importance. There already exist results on the height of coefficients appearing in a Rational Univariate Representation (see [49]), but these results are general while the performed infinitesimal deformation is particular. Thus, one can try to give more accurate bounds on our specific problems, at least in the worst case.

An alternative point of view comes from the fact that an infinitesimal can always be replaced by a *small enough* positive rational number. Consider the introduced infinitesimal as a variable, and the projection on this variable. The bifurcation set B of this projection restricted to the studied variety lies in $\mathbb{C}$ and is defined in the seventies by Wallace [95], Varchenko [93] and Verdier [94] as a set such that the projection restricted to the variety minus the pre-image of B realizes a locally trivial fibration on the complementary of B. Thus, one can choose a rational number which is inferior to the smallest positive bifurcation point.
Obviously, B contains the critical points of the considered projections, but, in non-proper situations, it contains also bifurcation points at infinity. In [45, 46], Kurdyka and Jelonek define a notion of generalized critical values (which is the union of the traditional critical values and *asymptotic* critical values) containing the bifurcation set. They prove that the latter is a proper algebraic subset, giving thus a quantitative generalized Bertini-Sard theorem. Moreover, they prove that the degree of generalized critical values is bounded by a Bézout bound, showing that their mathematical object is optimal. Nevertheless, the algorithm they provide to compute them is far from being tractable.
We will investigate how to compute these generalized critical values, with an acceptable complexity (in theory and in practice). To this end, we will use classical ideas coming from algebraic geometry: when a phenomenon occurs at infinity a linear change of variables brings back this phenomenon at finite distance. Combining this principle to our results in [87] which ensure properness properties of critical loci after a generic linear change of variables, we aim to reduce the problem of computing the asymptotic critical values to the computation of the set of non-properness of a projection restricted to a curve. This part of the project is naturally strongly related to the part dealing with algebraic optimization.

3.1.4 Parametric Systems

We showed that our definition of the discriminant varieties is optimal for the various concepts of "generic solutions" used in practice (compact fibers, continuity of the complex solutions, applicability of the implicit function theorem, etc.). We also showed that we know how to calculate them exactly (and not only to calculate any sub-variety with the same dimension containing it).

Once discriminant varieties are computed, several possibilities are offered to us. In the case of low-dimension problems, one can continue rather easily without the study of the discriminant varieties by deducing their topology from the study of the generic solutions of the system. In the case of problems of greater dimension (for example the application to cuspidal robots [21]), one can calculate a partial cellular decomposition of the parameter's space according to a fixed property (for example a constant number of real solutions).

We will first focus on problems that require a decomposition of the system: this is the hard step in many non generic situations. For inductively decomposing the radical of an ideal given by a lexicographical Gröbner basis into equidimensional components (that may be represented by a triangular set), we showed that some computations can be avoided by some filters. We are now studying the choices offered among the possible strategies for obtaining the better behavior in practice. Moreover, a triangular decomposition of the radical of an ideal is generally redundant in the sense that the ideal represented by a component may be included in another one. A solution to avoid such redundancies is to compute a Gröbner basis of each component. Since it may be costly, we developed some techniques that avoid this computation as much as possible.

In a second stage, we will concentrate on describing the cells of the complementary of the discriminant variety in the parameter's space. This part is strongly linked to the part on critical points methods for two reasons :

- computing a point in each connected component of a semi-algebraic set remains a difficult problem in practice, and for the moment remains to be one of our objective. Combining such information for the complementary of a discriminant variety gives immediatly a qualitative description of the generic solutions of a parametric system (existence and number of real roots w.r.t parameters' values).
- these two domains share a lot of commun objects. For example, properness defects properties for some projections functions (critical points methods) and mathematically well identified parts of the discriminant varieties may be described in a similar manner.

With critical points methods, we will a priori be able to answer several important questions: deciding if semi-algebraic set is empty or not, calculating a point in each connected component of it.

Potentially, techniques developed for the resolution of parametric systems can easily be used for general positive dimensional systems: it is enough to calculate a subset of transcendental variables which will play the role of parameters. This does not describe however all the semi-algebraic set since basically only the zeros which do not project on the discriminant variety are considered. However, the application of our computational strategies gives us the equations of this particular variety. One can then think that it is thus enough to add them to the initial system and to start again the process to obtain a complete description of its solutions. Coupled with our versions of critical points methods, such a process will give certainly a certain volume of qualitative information (emptiness test, computation of a point per connected component), but several points remain to be studied :

- efficiency and complexity of such an algorithm; this is a shared subject with critical points methods since the basic tools used (decompositions for example) as well as the intrinsic objects (cascades of singular loci and properness defects of certain projections) are common;
- final form of the result; several change of transcendent variables may be necessary if one considers the strategy described above. It is thus false to think that we are exactly in the situation of the parametric systems, or at least that the output will be also as simple (global properties of a semi-algebraic from a strict subspace of the parameter' space);
- exploitation within the framework of quantifier elimination problems; The use of our ideas on this subject is still fuzzy, but solving a system dependending on parameters is equivalent to eliminating a block of quantifier. It remains to know if the expression of the simplified formula we obtain could be easily injected into a more general formula.

3.2 Software

The development of software listed in section 2.3 will follow, some other will increase the list, accoarding to our research program.

Development of existing software New developments on MPFR are currently done inside the SPACES project. They mainly concern the efficiency aspects when using a low precision (less than 256 bits). The development of the MPAI library is subject to the future position of P. Trébuchet and the development of TSPR depends on the applications in robotics and related contracts.

As recalled in section 2.3, GB is not developed anymore (but still maintained). GB servers will be gradually replaced by FGB servers. In a first stage we plan to build specific servers for specific applications, for technical and efficiency reasons. Our objective is to propose general implementations of the algorithms F_5 and F_7.

For the RS software, a short term objective is to consolidate the implementations for computing the sign of polynomials at the real roots of a zero-dimensional system (black boxes for some critical points methods and general systems with inequalities).

The RAGLIB Maple package is recent (first distribution in november 2003). So, the short term objective is to intensively test the implementations (the RAGLIB package inherits from all problems related to the basic libraries and low-level software). Many improvements are currently under study such as filters for equi-dimensional and radical decomposition of ideal (to avoid useless computations), upgrade of existing algorithms on critical points methods using new results such as [87] or extensions of these methods for systems with inequalities.

For triangular sets, we have to face difficult choices for data-structures. The original implementation (in Axiom) used a recursive data structures for polynomials : it is mathematically well suited (triangular sets computations lead naturally to recursive algorithms) but slow in practice. The current implementation (in MAGMA) uses distributed polynomials and is at least as efficient as in Axiom. So a first stage will be to specify all the sub-algorithms involved w.r.t. both data structures. We then would like to test other languages like OCaml and make some tests also in C. Among the critical operation, we will pay a particular attention to the gcd computations over a tower of extensions (adaptation of modular computations, computation of the resultant of a set of polynomials).

New software : NetTask

- **Contacts :** F. Rouillier, J.C. Faugère

We benefited during nearly one year of the assistance of Étienne Petitjean (SEDRE-LORIA) for this development.

The developed tool (about 11,000 lines in C++) makes possible the use of software installed on a network which then becomes usable even if it is not ready to be distributed and thus allows the experimental validation of algorithms proposed in articles or allows an external user to have a more precise idea of the possibilities offered by recent algorithmic progress. It will be useful in our project to export some of our prototypes.

NetTask is very flexible since it doesn't need any change in the software to be demonstrated. It is compatible with the current safety requirements and contains some powerful tools:

- allocation of the tasks launched by the users according to the availability of the software but also the load of the nodes on a given network of machines;
- system of queue for the tasks;
- complete control of the launched tasks by the user himself;
- many options of configuration such as for example the declaration of the machines and tasks available on a given network, the maximum number of tasks per user.

3.3 Applications

Applications are fundamental for our project and are often long-term activities. One of the principal reasons is that problems are often posed to stick to known numerical and ad hoc methods and underwent a series of transformations such that they are not directly accessible for us (abusive linearization or use of inequalities, etc).

3.3.1 Cryptography

The first results obtained in cryptology (mainly breaking the HFE challenge) have catched the curiosity of several industrials. Several research and prospective contracts rose from this experience and lay down our main short and medium term objectives:

Contract with Celar (DGA) The objective is to evaluate, on examples of realistic size, attacks of algebraic type (and in particular Gröbner bases) on filtered registers (stream ciphers). This kind of crypto-systems is, in particular, used in mobile communications (mobile phones, decoders...) because the needed resources are easy to implement in hardware and allows extremely fast encoding/decoding. The workplan proposed by this contract is original since Celar emits "challenges" of realistic size (that means registers of size from 60 to 128 bits); the attack step induces a specific modelization of the problem (which represents a significant part of the computation time) then a resolution step which

uses our most efficient algorithms (F5 modulo 2). It should be pointed out that all the results of this study are publishable and that this contract is in fact a true scientific partnership.

Contract and PhD grant "CIFRE" with Thales The objective of this research is to find solutions to speed-up the core of Gröbner bases computation (algorithm F_5 and F_4) which is the linear algebra part. The main research subjects will be on the one hand the use of the sparse linear algebra techniques and the development of dedicated algorithms taking into acount the particular structure of the involved linear systems (mainly matrices that are triangular per blocks); a second objective is to be able to carry out these algorithms on massively parallel machines and thus to distribute and parallelize the current algorithms and software.

A last long term objective (independent from our above contracts) and for which the scientific risk is high is to attack crypto-systems like AES (a standard coding). It is known that these systems admit an algebraic formulation. However the size of the systems thus generated seem, at present, unreachable for the existing algorithms (see invited conference AES IV by J.C. Faugère).

3.3.2 Robotics

Our activity in robotics was separate up to now into two fields:

- the study of path planning for parallel robots;
- the study of the cuspidal character of some families of serial robots.

This cutting appears in the methods or algorithms studied and used (zero-dimensional systems for the parallel robots and systems depending on parameters for the serial robots).

The work carried out with the COPRIN project, the IRMAR and IRRCyN teams during the Maths-Stic project (Ministry grant) "robots cuspidaux" was a good framework for exporting our tools, explaining their constraints and advantages for the study of some serial robots with 3 degrees of freedom. By multiplying collaborations with some members of these teams, we discover more and more open problems (even if they were already studied) but accessible by our algorithms.

Cuspidal Robots Up to now, we have studied a set of serial robots with 3 degrees of freedom whose general outline is given by figure 2.2.3.

The parameters of the problem are the design parameters (d_4, d_3, r_2, r_3). Until now, we have considered the case $r_3 = 0$ and provided a full classification of the robots according to their cuspidal character. In practice, we provided a partition of the parameter's space defined as being the complementary of the strict discriminant variety of the algebraic system modelling the problem (see section 2.1.3), which defines areas where the system admits a finite number of real solutions (if the robot is not cuspidal for a given set of parameters, the system has no real solutions). Additional work made possible to connect this classification to a finer one depending on the number of cusps points (0, 2 or 4).

We will tackle the general case $r_3 \neq 0$. The same computational process currently makes possible (calculation done recently) to provide a partition having the same properties as for the case $r_3 = 0$, but this direct computation provides a too fine partition, made up of several thousands of cells. One can thus say that we know how to solve the problem, but that the output is not exploitable for a quantitative study by roboticians. The simplification of this output requires to amalgamate cells. Mathematically, the most direct way to do this is to conceive a method to decide if 2 points are in the same (semi-algebraically) connected component. This problem (roadmaps computations) is known to be very delicate in practice and being able to perform such a computation would be a significant progress; For example our critical point methods calculate at least one point in each connected component of a semi-algebraic set : having a roadmap function would refine the output to exactly one point on each connected component. However, we do not need, for the cuspidal robot application, such a level of precision. A second way, a priori easier, is to study what occurs over the discriminant variety, i.e. to deal with the problem recursively as recommended in section 3.1.4, in order to eliminate the borders between cells not inducing a change in the number of real roots of the system modelling the problem.

A long-term objective is the study of cuspidal parallel robots. It is, in the current state of our knowledge and of the performances of existing algorithms, illusory to tackle such a characterization for general parallel robots according to their design parameters (too many variables). We however carried out tests on particular robots (plane base and platform) having many symmetries but however intensively studied by the engineers, and we hope to obtain significant progress in the medium and long term.

Path planning Parallel robots are, in practice, excessively delicate to control for geometrical reasons (up to 40 solutions to the direct kinematics problem) but also because there is no specific control charts (the originators use similar charts than those used for the serial robots). A major difference is that the legs of a robot parallels cannot be controlled independently, which poses serious problems of synchronization, interpolation, etc.

Our simulator has been used to diagnose the problems related to the solutions currently employed (Computer Aided Design, look-ahead, algorithms for interpoling the trajectories, etc). It will enable us to validate and simulate new adapted approaches for controlling such mechanisms (for example speed control recommended by Jean-Pierre Merlet).

One of the principal concern in the whole of the components constituting the command is certainly the discretization of the trajectories at the Computer Aided Design step. The behavior of this kind of mechanisms being nonlinear, such discretizations generates, in some cases, an important source of errors. An ambitious objective is to change the output of the Computer Aided Design step by replacing the discretization points currently provided by equation of algebraic curves. There are two interests with that :

- at the command level, having equations for the trajectory would allow to avoid of many strange interpolations source of 90 per cent of the current errors;
- for simulation tools, that would enable us to obtain formal expressions instead of bounds and would facilitate consequently the analysis of the problems.

In terms of methods for polynomials solvers, this results by a parametric model of the direct geometrical problem (one parameter) and would give a good objective for our research on the subject.

3.3.3 Signal Processing

The synthesis and identification of hyperfrequency filters made of coupled resonant cavities is the subject of a recent collaboration with the APICS INRIA project (Sophia-Antipolis Unit).

For the synthesis or identification of linear systems (modelized by linear differential equations), one key question is to characterize and compute the parameters' values of an original physical model, given the transfer function.

More precisely, if $(A(p), B(p), C(p), D(p))$ is an instance depending on parameters' vector p and H is a given tranfer function, we are interested in the set

$$E_H = \{p, C(p)(sId - A(p))^{-1}B(p) + D(p) = H(s)\}.$$

For frequential devices synthesis, determining E_H remains to describing the equivalent devices from the point of view of their frequency response. In the low-pass model used for hyperfrequency filtering, the entries of the parameters' vector p are the electro-magnetical coupling values of the resonators used in the filter.

$(A(p), B(p), C(p), D(p))$ are polynomials in these coupling values so that the main problems concerning the values and the computation of E_H can naturally be expressed in terms of polynomial equations. For example, it remains to study the rank of a jacobian matrix to know if E_H is generically discrete or not. In this case, the points of E_H are the real roots of a zero-dimensional system. When $E(H)$ is a positive dimensional variety, one goal would be to find the critical values/points of a given criteria, but the subject has not been explored yet (related to our work on parametric or positive dimensional systems).

As for many applications to be solved using computer algebra systems, a part of the work is dedicated to finding a good modelisation. For this problem, one can, for example, take into account the symetry group acting on the solution set.

Software solutions developped in our project allowed to find exhaustive answers for some filters for which classical numerical method [16] [18] (based on optimisation technics) gave only partial and sometimes wrong informations (no solutions found whereas several exists).

The various elements of $E(H)$ are analyzed by the originator, and the best configuration of the couplings is then retained, according to technological criteria (for example the size of the coupling screws), to produce the filter.

The methodology developed for the computation of $E(H)$ is effective for most usual filters but the asymmetrical filters recently introduced [17] still resist and become a relevant and motivating challenge. One goal in our collaboration with APICS project is to propose software solutions for solving industrial problems by way of writing a software dedicated to filters' synthesis.

For our project, this applications sets new objectives for zero-dimensional systems solving. When the coefficients of the systems to be solved are supposed exactly known (rational numbers), we are currently in the extreme case of what our software can compute (size of the coefficients during the computations and in the result).

In practice, most systems are over-determined and have approximate coefficients, which places them far from the mathematical generic cases (complete intersection). A naive modeling (direct conversion of the coefficients to rational numbers) will then give systems with theoretically (and consequently in practice for our software) no solution.

4 Project positionning

4.1 Scientifi c positionning

Our team is one of the rare world teams to pay attention to all the aspects of polynomial system solving, without limiting itself to a particular technique or to a particular class of problems.

Another originality that our team shares with a small number of world teams, is to privilege in the algorithmic developments, the practical efficiency as much as theoretical complexity ; indeed, as in other fields, there is not necessarily a link between good theoretical complexity and acceptable practical efficiency.

Lastly, we privilege the "certified" approach for numerical computations (error bounds, uniqueness of the result, etc.) as well as for exact computations (no algorithms such that the validity of the result is not guaranteed to 100 %).

4.1.1 Gröbner bases and triangular sets

Competition on Gröbner bases computations is very strong since this object is the only known way to represent ideals. Our advance, thanks to the algorithms F_4 and F_5, is comfortable in terms of performances.

During the last years, the main algorithmic progress come from our team [26],[32],[34]. However, several teams currently work on implmentations for a large diffusion. Mainly, Macaulay (D. Grayson, Urbana et M. Stillman, Cornell), Magma (J. Cannon, Sidney), Singular (G.-M. Greuel, G. Pfister and H. Schönemann, Kaiserlautern) Risa/Asir and Cocoa (L. Robbiano et al., Gènes).

One may point out that Magma, Macaulay and Risa/Asir currently work on implementations of F_4 algorithm [26] and most of general purpose computer algebra software (Maple, Mathematica, $\ldots$) contain a version of the FGLM algorithm [29].

The use of triangular sets is now confirmed for differential systems (work done by the CAFE project and the CALFOR team), for some problems in elementary geometry or for implicitization of curves [96]. For general algebraic systems, the existing implementations do not validate this approach yet in practice although one progressed in the comprehension of such objects ([90]).

Rare concurrent approaches exist to represent algebraic varieties by other means. One can quote work of Jan Vershelde on homotopy methods, which make possible, in some sense, to represent the irreducible components of algebraic varieties: it is a semi-numerical and probabilistic representation and its use remains restricted. One can also quote work of STIX's team on rational parameterizations but this strategy is closer to our studies on parametric systems.

Excepted M. Kalkbrenner (Zürich) — but which recently gave up research — and our team, research concerning triangular sets are mainly resulting from Wu Wentsün (Beijing) and his/her collaborators : Cabbage (Wichita State University), Gao (Beijing), Dongming Wang (CALFOR - LIP6). For a long time, this technique was handicapped by the fact that, for lack of sufficient theoretical bases, there were many different specifications for the input/output of the algorithms. Now that the situation is clarified [2], efficient implementations should appear, beyond those carried out in our team and collaborators (mainly M. Moreno-Maza and F. Boulier at LIFL).

4.1.2 Zero-dimensional systems

In the field of solving zero-dimensional systems, the most serious competitor or complementary results are those GALAAD and COPRIN projects as regards the INRIA, homotopy methods and work of the TERA group.

The GALAAD project is currently turned toward symbolic-numeric strategies and concentrates mainly on structured systems or with a low number of variables for an intensive use for the geometrical study of curves and surfaces. This subject as well as the applications in Computer Aided Design are complementary to ours. A strong intersection exists since the GALAAD project proposes an alternative to Gröbner bases for the computation and the representation of the quotient algebra $K[X_1, \ldots, X_n]/I$ (see section 2.1.2). This alternative could become a subject of co-operation since

most of the methods using the quotient algebra structure we propose could easily come to supplement this work. One of the basic tools studied in the GALAAD project is related to the use of (sparse) resultant for solving algebraic systems, this subject is also developped by I. Emiris (Univ. of Athens).

The COPRIN project works on methods based on interval analysis. These methods generally require the knowledge of an approximation of the solutions (bounds for example) and proved to be powerful for a local resolution. In our joint work on parallel robots, we showed that the conjunction of the two approaches made possible to obtain excellent practical results (speed of the methods from interval analysis in the generic cases, treatment of the degenerate cases by algebraic methods).

Homotopy methods are most known by numericians for solving zero-dimensional systems. The algorithms and implementations of Jan Vershelde or T Lee for example, illustrate all the power of these methods. They enter directly in competition with ours except for the quality of the output: we are able to undoubtedly distinguish real zeros from the complex zeros, to distinguish multiple points from simple points and to calculate their multiplicities. To date, the tests carried out show our advance in terms of efficiency in most cases, on a panel of several hundreds of examples coming from varied applications.

The Singular team (Kaiserslautern University) develops computer algebra solutions. For zero-dimensional systems, they implements mainly classical algorithms (Buchberger algorithm for Gröbner bases computations for example), and some strategies proposed by our team (for example the FGLM + triangular sets decompositions). As already mentionned, the last step for real roots computations is done through numerical strategies (for example Newton) on triangular sets. This do not offer the garantee of the result, and moreover, up to our experiments, is limited to quite small systems (numerical instability).

The TERA group (un-formal group made up teams French, Spanish, Argentina, German, etc). As regards zero-dimensional systems, the contributions closest to ours are due to STIX team. The geometrical resolution suggested in [37] reiterates a part of the specifications of the rational univariate representation [73], with two details near: the computation of the multiplicities and the probabilistic character of the algorithms (choice of an injective linear form on the whole of the solutions). In spite of these notable differences, the implementation of this method (called Kronecker) remains slower in practice, parhaps due to the language currently used (general computer algebra software MAGMA). A recent contribution from STIX is the extension of the formulas of the RUR: in [73], the coefficients of the polynomials are defined according to traces of endomorphisms, whereas [13] leaves the possibility of using other linear forms. In this last article an algorithm taking up the ideas of Shoup (baby step Giant step) is proposed and has a theoretical complexity presumed better than that of [73]. In fact, the algorithm is a probabilistic, evacuating by an arbitrary choice the problem of finding the injective linear form. F. Rouillier showed very recently that this algorithm should become deterministic without losing in theoretical complexity. Currently, its implementation requires the complete computation and storage of the multiplication table in $K[X_1, \ldots, X_n]/I$, which is the blocking point to solve consequent problems. It may be interesting to cooperate on this subject.

For systems with coefficients in a finite field, the main concurrent, at least for problems coming from cryptography, is the XL algorithm [23]. From a mathematical point of view, it is a naive solver (inverting a generalized Sylvester/Macaulay matrix) with many variants. According to numerous article on the subject it is to be easy to implement but no precise information is available on its practical efficiency.

4.1.3 Critical points methods

Several groups work on the critical point method and solving optimization problems with a view toward effective real algebraic geometry. Major contributions come from the team “Real algebraic geometry, Computer algebra and Complexity” team of the IRMAR (Rennes I University), the “Algorithmic” team of the STIX Lab (École polytechnique) and the works of P. Parillo (Swiss Federal Institute of technology, Zurich) and his collaborators.

The team of Rennes I university has produced several algorithms based on the critical point method in collaboration with S. Basu (Georgia Tech. institute, Atlanta) and R. Pollack (Courant institute, New-York). These are the starting point of our studies. Their contributions are essentially complexity results showing the class of complexity required to solve some questions arising in effective real algebraic geometry. This leads to algorithms which are not tractable in practice: the problem of providing efficient implementations is not tackled.

The approach of the team of STIX Lab is a priori similar to ours since it consists in trying to improve the complexity results of the aforementioned team to obtain significative practical results. Nevertheless, they restrict themselves to smooth cases, without dealing with polynomial systems generating non-radical ideals and to the use of Lecerf’s algorithm (see [37]) which is probabilistic.

Finally, P. Parillo's approach is based on applying techniques coming from convex optimization to algebraic optimization and provides implementations. This leads to several improvements but is valid only on some kinds of problems (optimization of sums of squares). As shown in [12], the volume of polynomials which are sums of squares tends to zero in the family of positive polynomials when the number of variables grows. Thus, this approach is only relevant on very specific problems.

4.1.4 Parametric systems

Some groups around the world are working on the resolution of parametric systems. Again, few efficient implementations exists. It seems that we are the first ones who define an intrinsic object (minimal discriminant variety) that specifies the notion of resolution in the case of parametric systems while being able to compute it efficiently.

Of course, the Cylindrical Algebraic Decomposition (CAD) is a concurrent solution. The most diffused implementation (QEPCAD) is due to collaborators of Collins and Hoon-hong. A version "B" is currently developed by C. Brown (United States Naval Academy - Annapolis). Weispfenning's (University of Passau) group also develops a collection of tools related to the CAD which are implemented in the general computer algebra software Reduce. The CAD is doubly exponential in the number of variables, as well for calculation as for the size of the output, whereas our discriminant variety for example is of simply exponential size (and optimal). This theoretical complexity gap is also observed in practice. However, there exists, no other practical tools for solving quantified formulas or even simply solving systems without equalities.

The members of Weispfenning's team (University of Passau) develop solutions based on "comprehensive Gröbner bases" and derived (for example adaptation of the algorithm of Hermite to the systems depending on parameters). As described in section 2.1.3, this kind of techniques induced the computation of large discriminat variety. In the case of parametric systems, such large discriminant variety contains the parameters' values for which any Gröbner basis do not specialize properly. Again, it is far from being optimal since it contains the parameter's values where the staircase vary, which depend one the strategy used (for example the choice of a monomial ordering).

TERA group, and mainly our colleagues of STIX team, also work on parametric systems. They, for example, extended the computation of their "geometrical resolution" (valid in the zero-dimensional case) by way of straight-line programs to the case of generically zero-dimensional parametric systems. The developed methods are probabilistic and calculate also implicitely a large discriminant variety as recalled in section 2.1.3. We do not have much information on their real efficiency, but the related complexity studies could however help for better understanding our concept of strict discriminant variety.

4.2 Relationships

4.2.1 INRIA projects

We maintain relationships with the majority of INRIA projects of program 3B (Symbolic Systems - Algebra, Geometry and Algorithms), but also to other projects via transverse actions or through specific applications.

Algo. Our links with ALGO are mostly indirect (via our respective collaborations with STIX team), or take the form of specific common contributions such as for example [5]. It is true that the links and objectives (put aside subjects common with STIX team) are relatively distant.

APICS. Our collaboration with APICS is recent (around 2003, January) and already detailed in this document in the sections about signal processing. We plan having long term research with this project on synthesis and identification of hyperfrequency filters.

Arénaire. With the reorganization of SPACES, our links with Arenaire reduce from now on developments related to multiprecision interval arithmetic (articles [68], [67] or development of the MPFI library).

Codes. Solving polynomial systems with coefficients in a field with two elements has many potential applications in coding and cryptology (in particular as a tool to break the codes).

A few years ago, this led J.-C. Faugère to develop a specific version of GB which was used in D. Augot PhD's thesis. Different research objectives made distent these relations, which actively began again since the starting of SPACES. This resumption of collaboration is at the origin of the one of our principal application field (cryptology).

ISA. The ISA project is an important user of our software, in particular for the use of surface and surfacic models in Computer Aided Design. ISA already uses "beta" versions of our most recent software. These applications are particularly interesting for us by the unusual problems of efficiency they pose : it is a question of carrying out a great number of easy or fairly difficult computations, whereas the majority of our other applications correspond to a small number of very difficult ones. This collaboration, developed since the creation of SPACES, leads in particular to a common article on the robust parameterization of quadric surfaces and their intersections as well as the implementation of robust methods for solving univariate polynomials with algebraic real coefficients, especially optimized for the problems in Computer Aided Design treated by project ISA.

Scilab. This very specific collaboration is related only to the development of an interface between the computer algebra system MuPAD and the numerical software Scilab, based on the communication protocol udx. This interface is the origin a contract for the period 1998-2006 between the INRIA and the company SciFace Software which distributes MuPAD.

Coprin. J.-P. Merlet being the principal specialist in parallel robots, it is quite naturally that we collaborate with him since many years on these questions (cf [54], CMW contract, Maths-stic grant with IRRCyN and advising, with F. Rouillier, Luc Rolland's thesis).

Several common projects and work are already planned in the short and medium term (articles, projects of development around the studies done for CMW).

Galaad. It is the INRIA project having the objectives closest to ours. Its approach is complementary : it uses mainly numerical or semi-numerical methods resulting from geometry, whereas our approach is mainly algebraic and based on exact arithmetic. In addition to thesis advising (P. Trébuchet), we collaborate in the development of a software environment containing various developments carried out by two projects (alp, GB, mpfr, rs, udx, etc).

Moreover, we also have joint teaching activities (common courses for undergraduate students, organization of summer schools, etc.).

SPACES - Lorraine Our collaboration with the other part of the actual SPACES project will obviously follow on many items (arithmetics, linear algebra, cryptography, etc.)

4.2.2 Outside INRIA

Rennes 1 University The collaboration with the real geometry team of the University of Rennes I is old, constant and profitable. In addition to shared Phd students, the participation to three European projects (PoSSo-FRISCO-RAAG), many progresses on effective algorithms in real geometry result from a common work. New common actions are in hand via European network RAAG or a project of interactive book.

LIFL. For several years, François Boulier has had a great expertise in the implementation of triangular sets for the differential algebra. It was joined by Marc Moreno-Maza, who prepared his thesis on triangular sets with D. Lazard. Collaboration with the LIFL is thus natural. Currently it concerns mainly teaching since several members of our project are associated to the teaching staff for the development of modules of computer algebra and F. Rouillier gives regularly courses in this module.

STIX. As seen several times in this text, the STIX team works on a complementary approach of ours for algebraic resolution. This complementarity was concretized by several collaborations with STIX members, which in particular gave place to several articles [82], [88],[88].

Paderborn University. The collaboration with the university of Paderborn is old. For example, software GB and RS were interfaced with MuPAD. We also took part in the development of the MuPAD/Scilab interface. The collaboration will continue since the protocol of communication udx, developed in the project, was chosen by MuPAD for various developments (for example the MuPAD/Scilab interface).

Beijing Academy of Science. MMRC team (Academy of Science of Beijing) works on the resolution of the polynomial systems and their applications. D. Wang, former member of SPACES, maintains a close cooperation with the MMRC (a cooperation agreement was signed between SPACES and the MMRC). We intend to preserve this collaboration in the SALSA project (F. Rouillier and P. Aubry are invited in Beijing in July 2003).

4.3 Scientifi c animation

National. Fabrice Rouillier is currently vice head of the SPACES project while J.C. Faugère is the head of the CALFOR team.

F. Rouillier is elected member of the INRIA evaluation commission since 2002 and took part in the CR2 admissibility commission of Rocquencourt INRIA Research Unit in 2003. He organized a general assembly of French Computer Algebra in September 2001 and was member of the scientific committee of "Action Specific Math-Stic Calcul Formel". He was in the organizing commitee of the workshop on "free software and computer algebra" in Lyon (2002) and was one of the organizers of the "National days of computer algebra" in Lumini (January 2003). Finally J.C. Faugère and F Rouillier, in collaboration with B. Mourrain, have organized a summer school on "free computer algebra tools" in Giens (September 2002).

J.C. Faugère is member of the scholarship committee at INRIA Rocquencourt research unit.

International. The SALSA's members are regularly invited in international conferences and workshops. In the first half of 2004 for example, J.C. Faugère is invited to AES IV conference, D. Lazard is invited to ECCAD, F. Rouillier to Dagstuhl [80], Berkeley (MSRI) [79] and P. Aubry and F. Rouillier to Beijing (Seventh International Workshop on Mathematical Mechanization).

We also take part in the organization of international workshops or summer schools [38],[22],[78].

4.4 National or European projects

Most of the project's members were actors of the two European projects PoSSo and Frisco on Solving polynomial systems.

J.C. Faugère and F Rouillier obtained a ministry grant "ACI Jeunes" (2000-2003) to develop algorithms for the resolution of parametric systems.

J.C. Faugère takes part to the project (minitry grant) "ACI cryptology" (2001-2004) managed per G Hanrot (project SPACES).

F. Rouillier and Mohab Safey El Din take part in European network RAAG (2002-2006), F. Rouillier being (with L. Gonzalez-Vega) in charge for the part "Applications and links with industry".

J.C. Faugère, F Rouillier and M. Safey El Din took part in the action "Maths-stic" (ministry grant 2002-2003) on "cuspidal Robots" managed by our colleagues of IRRCyN.

5 Contracts

RAAG European Network

- **Contact :** F. Rouillier

This project started in 2002 and will end in 2006.

The SPACES project takes part in the European project RAAG (Real Algebraic and Analytic Geometry), F. Rouillier being involved in the applications and connection with industry item.

RAAG is a Research Training Network of the "Human Potential" program of the European Commission, sponsored for 48 months starting from March 2002. The network is managed by the University of Passau (Germany), the coordination of the French team being ensured by the team of real geometry and computer algebra of the University of Rennes I.

The main goal of this project is to increase the links between the various fields of research listed in the topics of the project (real algebraic geometry, analytical geometry, complexity, formal calculation, applications, etc.) by means of conferences, schools and exchanges of young researchers. It brings together a great number of European teams and in particular the majority of the French teams working in the scientific fields falling under the topics of the project.

Ministry Grant (ACI) "Cryptologie"

- **Contact :** J.C. Faugère

This project started in 2002 and will end in 2004.

The main goal of this project is to study the interactions between cryptography and Computer Algebra and more specifically the impact of fast polynomial system algorithms on public key cryptosystems based on multivariate (quadratic) equations (such as HFE). For instance a member of this project was able to “break” the first HFE challenge by computing a huge Gröbner basis.

Sciface Software

- **Contact :** F. Rouillier

In November 2001, a cooperation agreement around the UDXF program for binary data exchange was signed between the SciFace company (which distributes the computer algebra system MuPAD) and INRIA Lorraine (representing the University Pierre and Marie Curie). UDXF takes as parameter a communication protocol, for example that of patent UDX, but it can also be another protocol. Within the framework of this agreement, SciFace has the right to use UDXF for the MuPAD-Scilab interface. In exchange, SciFace takes part in the development and the improvement of UDX. Version 2.5.x of MuPAD, distributed since September 2002, integrates this interface.

Constructions Mécaniques des Vosges - Marioni

- **Contact :** F. Rouillier

Since 1997, we work with the SME CMW on the design of a parallel robot for high speed machining. A first agreement was signed in 1999 and CMW partially sponsored the PhD of Luc Rolland (defense in december 2003).

The year 2002 was devoted to the search of partners to constitute a complete chain (software and electronic components) for proposing a new control device for this type of manipulators (work done in cooperation with the INRIA project COPRIN). Since all the partners agreed, the year 2003 was devoted to raise funds. We are currently waiting for an answer from ANVAR and "région Lorraine".

CELAR (DGA)

- **Contact :** J.C. Faugère

The objective is to evaluate, on examples of realistic size, attacks of algebric kind (and in particular Gröbner bases) on filtered registers (stream ciphers).

THALES

- **Contact :** J.C. Faugère

The objective of this research is to find solutions to speed-up the core of Gröbner bases computation (algorithm F_5 and F_4) which is the linear algebra part. A CIFRE grant (S. Lacharte) is related to the contract.

References

[1] P. Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques*. PhD thesis, Université Paris 6, France, 1999.

[2] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbilic Computation*, 28:105–124, 1999.

[3] P. Aubry, F. Rouillier, and M. Safey. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[4] P. Aubry and A. Valibouze. Using galois ideals for computing relative resolvents. *J. of Symbolic Computation*, 30(6):635–651, 2000. Special Issue on Algorithmic Galois Theory.

[5] M. Bardet, J.-C. Faugère, and B. Salvy. Complexity of gröbner basis computation for semi-regular overdetermined sequences over f_2 with solutions in f_2. Technical report, INRIA Research Report, 2003.

[6] A. Basiri, A. Enge, J.-C. Faugère, and N. Gürel. Implementing the arithmetic of $c_{3,4}$ curves. In *ANTS 2004*, pages 87–101, 2004.

[7] A. Basiri and J.-C. Faugère. Changing the ordering of gröbner bases with lll: case of two variables. In *ISSAC 2003*, pages 23–29, 2003.

[8] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier elimination and cylindrical algebraic decomposition*. Springer-Verlag, 1998.

[9] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computations in Mathematics*. Springer-Verlag, 2003.

[10] S. Basu, R. Pollack, and M.F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of Assoc. Comput. Machin.*, pages 1002–1045, 1996.

[11] T. Becker and V. Weispfenning. *Groebner bases: a computational approach to commutative algebra*. Graduate Texts in Mathematics: readings in mathematics. Springer, 1993.

[12] G. Blekherman. There are significantly more nonnegative polynomials than sums of squares. math ArXiv, num. 0309130, september 2003.

[13] A. Bostan, B. Salvy, and É. Schost. Fast algorithms for zero-dimensional polynomial systems using duality. *Applicable Algebra in Engineering, Communication and Computing*, 14(4):239 – 272, 2003.

[14] B. Buchberger. *"Groebner bases : an algorithmic method in polynomial ideal theory"*. Recent trends in multidimensional systems theory. Reider ed. Bose, 1985.

[15] B. Buchberger, G.-E. Collins, and R. Loos. *Computer Algebra Symbolic and Algebraic Computation*. Springer-Verlag, second edition edition, 1982.

[16] R. J. Cameron. General coupling matrix synthesis methods for chebyshev filtering functions. *IEEE Transaction on Microwave Theory and Techniques*, 47(4):433–442, 1999.

[17] R.J. Cameron, A.R. Harish, and C.J. Radcliffe. Synthesis of advanced microwave filters without diagonal cross-couplings. *Proceedings of the IMS 2002*, pages 1437–1440, 2002.

[18] D. Chambers and J.D Rhodes. A low pass prototype network allowing the placing of integrated poles at real frequencies. *IEEE Transaction on Microwave Theory and Techniques*, 31:40–45, 1983.

[19] G.E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Springer Lecture Notes in Computer Science 33*, 33:515–532, 1975.

[20] S. Corvez and F. Rouillier. Using computer algebra tools to classify serial manipulators. In *Fourth International Workshop on Automated Deduction in Geometry, ADG 2002, Linz*, 2002.

[21] S. Corvez and F. Rouillier. Using computer algebra tools to classify serial manipulators. In F. Winkler, editor, *Automated Deduction in Geometry*, volume 2930 of *Lecture Notes in Artificial Intelligence*, pages 31–43. Springer, 2003.

[22] Michel Coste, Laureano Gonzalez Vega, Fabrice Rouillier, Marie-Francoise Roy, and Markus Schweighofer. Summer school on computer tools for real algebraic geometry, 2003. Rennes - June 2003.

[23] Nicolas Courtois, Adi Shamir, Jacques Patarin, and A. Klimov. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Eurocrypt'2000*, volume 1807, pages 392–407. Springer Verlag, 2000.

[24] 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-Berlin-Paris, 1992.

[25] A. Dickenstein and I.Z. Emiris. Multihomogeneous resultant matrices. In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 46–54. ACM Press, 2002.

[26] J.-C. Faugère. A new efficient algorithm for computing gröbner bases (f_4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, June 1999.

[27] J.C. Faugère. *Résolution des systèmes d'équations polynômiales*. PhD thesis, Université de Paris VI, 1994.

[28] J.C. Faugère, F. Moreau de Saint-Martin, and F. Rouillier. Une famille de bancs de filtres 2d non séparables. Patent, 1997.

[29] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner basis by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, October 1993.

[30] J.C. Faugère and D. Lazard. The combinatorial classes of parallel manipulators. *Mechanism and Machine Theory*, 30:765–776, 1995.

[31] J.C. Faugère and F. Rouillier. Dispositif d'échanges de données entre matériels informatiques. Patent proposal number 99 08172, 1999.

[32] Jean-Charles Faugère. Finding all the solutions of cyclic 9 using gröbner basis techniques. In K. Shirayanagi and K. Yokoyama, editors, *Computer Mathematics - Proceedings of the 5th Asian Symposium (ASCM 2000)*, pages 1–12. World Scientific, Singapore, 2001.

[33] Jean-Charles Faugère. Classification of all planar central configurations of n bodies with equal masses in the case of the logarithmic potential and n<8. In *8th International Conference on Applications of Computer Algebra - ACA 2002 , Volos, Grèce*, Jun 2002.

[34] Jean-Charles Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero f_5. In *International Symposium on Symbolic and Algebraic Computation Symposium - ISSAC 2002, Villeneuve d'Ascq, France*, Jul 2002.

[35] Jean-Charles Faugère, François Moreau de Saint Martin, and Fabrice Rouillier. Design of regular nonseparable bidimensional wavelets using Groebner basis techniques. *IEEE SP Transactions Special Issue on Theory and Applications of Filter Banks and Wavelets*, 46(4):845–856, apr 1998.

[36] Jean-Charles Faugère and Fabrice Rouillier. Design of filter and filter banks using dedicated computer algebra tools. In *International Conference on Applications of Computer Algebra (ACA'99)*, 1999. Applications of Computer Algebra to Signal Processing, Jeremy Johnson and Markus Pueschel.

[37] M. Giusti, G. Lecerf, and B. Salvy. A gröbner free alternative for solving polynomial systems. *Journal of Complexity*, 17(1):154–211, 2001.

[38] L. Gonzalez-Vega, F. Rouillier, and M.-F. Roy. Workshop computations and applications in raag, 2002. Santander, Spain - June 2002.

[39] L. Gonzalez-Vega, Fabrice Rouillier, and M.F. Roy. *Symbolic Recipes for Polynomial System Solving*. Algorithms and Computation in Mathematics. Cohen, A.M. and Cuypers, H. and Sterk, H.,Springer, 1998.

[40] L. Gonzalez-Vega, Fabrice Rouillier, M.F. Roy, and G. Trujillo. *Symbolic Recipes for Real Solutions*. Algorithms and Computation in Mathematics. Cohen, A.M. and Cuypers, H. and Sterk, H.,Springer, 1998.

[41] D. Grigor'ev and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Comput.*, 5:37–64, 1988.

[42] J. Heintz, M.-F. Roy, and P. Solernó. On the complexity of semi-algebraic sets. In *Proc. IFIP 89, San Francisco*, pages 293–298, 1989.

[43] J. Heintz, M.-F. Roy, and P. Solerno. On the theoritical an practical complexity of the existential theory of reals. *The Computer Journal*, 36(5):427–431, 1993.

[44] A. Joux J.-C. Faugère. Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases. In *CRYPTO 2003*, pages 44–60, 2003.

[45] Z. Jelonek and K. Kurdyka. On asymptotic critical values of a complex polynomial. *J. Reine Angew. Math*, 565:1–11, 2001.

[46] Z. Jelonek and K. Kurdyka. Quantitative generalized bertini-sard theorem for smooth affine varieties. pre-print, 2002.

[47] M. Kalkbrenner. *Three contributions to elimination theory*. PhD thesis, Johannes Kepler University, Linz, 1991.

[48] M. Kern, J.-C. Faugère, and F. Rouillier. Using gröbner bases to compute higher order finite elements for maßlumping. In *ICIAM'99, Edimburgh*, 1999. Numerical Methods in Differential Equations,Contributed Lectures C-31.

[49] T. Krick, L.M. Pardo, and M. Sombra. Sharp estimates for the arithmetic nullstellensatz. *Duke Mathematical Journal Journal*, (109):521–598, 2001.

[50] D. Lazard. A new method for solving algebraic systems of positiove dimension. *Discrete Applied Mathematics*, 1991.

[51] D. Lazard. Solving zero - dimensional algebraic systems. *Journal of Symbolic Computation*, 13:117–132, 1992.

[52] D. Lazard. Stewart platforms and gröbner basis. In *Proceedings of Advances in Robotics Kinematics*, pages 136–142, Septembre 1992.

[53] D. Lazard. On the specification for solvers of polynomial systems. In *5th Asian Symposium on Computers Mathematics -ASCM 2001*, volume 9 of *Lecture Notes Series in Computing*, pages 66–75. World Scientific, 2001.

[54] D. Lazard and J.-P. Merlet. The (true) Stewart platform has 12 configurations. In *Proc. of IEEE Conference on Robotics and Vision, San Diego*, 1994.

[55] Daniel Lazard. Resolution of polynomial systems. In *4th Asian Symposium on Computer Mathematics - ASCM 2000, Chiang Mai, Thailand*, volume 8 of *Lecture Notes Series on Computing*, pages 1 – 8. World Scientific, Dec 2000.

[56] Daniel Lazard. Résolution numérique des systèmes algébriques par des techniques exactes : application à la mécanique céleste. In SMAI, editor, *Congrès national de mathématiques appliquées et industrielles, SMAI 2001, Pompadour, France*, pages 159–160. SMAI, May 2001.

[57] Daniel Lazard. Solving systems of algebraic equations. *ACM SIGSAM Bulletin*, 35(3):11–37, Sep 2001.

[58] Daniel Lazard. Central configurations of four gravitational masses with an axys of symmetry. In *Workshop on Applications of Commutative Algebra - Catania 2002, Catania, Italie*, Apr 2002.

[59] Daniel Lazard. Mélange de deux lois gaussiennes; systèmes sur-déterminés dépendant de paramètres approchés. In *Journees LNF, Liens Calcul Numerique-Calcul Formel, Toulouse, France*, Dec 2002.

[60] J. Lebrun and I.-W. . Selesnick. Gröbner bases and wavelet design. *Journal of Symbolic Computtation*, 37(2):227–259, 2004.

[61] H. Lombardi, M.-F. Roy, and M. Safey El Din. New structure theorems for subresultants. *Journal of Symbolic Computations*, 2000. May.

[62] B. Mourrain, F. Rouillier, and M.-F. Roy. Bernstein's basis and real root isolation. Technical Report RR-5149, INRIA, 2004.

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

[64] B. Mourrain and P. Trébuchet. Generalized normal forms for polynomial system solving. Technical report, INRIA Research report, 2004.

[65] J. El Omri. *Analyse géomtrique et cinématique des mécanismes de type manipulateur*. PhD thesis, Université de Nantes, Feb. 1996.

[66] G. Dos Reis, B. Mourrain, F. Rouillier, and P. Trébuchet. An environment for symbolic and numeric computation. In World Scientific Pub, editor, *International Congress of Mathematical Software*, pages 239–249, 2002.

[67] N. Revol and F. Rouillier. A library for arbitrary precision interval arithmetic. In *10th GAMM - IMACS International Symposium on Scientific Computing, Computer Arithmetic, and Validated Numerics (scan2002)*, 2002.

[68] N. Revol and F. Rouillier. Motivations for an arbitrary precision interval arithmetic and the mpfi library. Technical Report 4498, INRIA, 2002.

[69] J.F. Ritt. *Differential equations from an algebraic standpoint*, volume 14. New York, 1932.

[70] F. Rouillier. Real root counting for some robotics problems. *Solid Mechanics and its Applications, Kluwer Academic Publishers*, 40:73–82, 1995.

[71] F. Rouillier. Software for symbolic polynomial system solving: the posso solver. In *ICIAM'95 - Hambourg*, 1995. Polynomial System Solving: New Research Directions.

[72] F. Rouillier. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*. PhD thesis, Université de Rennes I, may 1996.

[73] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Journal of Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[74] F. Rouillier. Les robots parallèles adoptent le calcul exact. INédit numéro 23, 2000. `http://www.inria.fr/actualites/inedit/inedit23_parta.fr.html`.

[75] F. Rouillier. Calcul formel et calcul scientifique. In *Congrès National de Mathématiques Appliquées et Industrielles*, pages 151–164. SMAI, Mai 2001.

[76] F. Rouillier. Efficient algorithms based on critical points method. In Saugata Basu and Laureano Gonzalez-Vega, editors, *Algorithmic and Quantitative Real Algebraic Geometry*, volume 60 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 123–138. American Mathematical Society, 2003.

[77] F. Rouillier. Efficient real solutions and robotics. In *First EMS -SMAI -SMF Joint Conference Applied Mathematics and Applications of Mathematics*, 2003.

[78] F. Rouillier. Polynomial system solving in the real case, 2003. Summer School and Conference on Real Algebraic Geometry and its Applications,Trieste , 2003.

[79] F. Rouillier. Exact computations and real roots of polynomial systems. Workshop on Algorithmic, Combinatorial and Applicable Real Algebraic Geometry, 2004. MSRI - Berkeley.

[80] F. Rouillier. Real roots of parametice systems of polynomial equalities and inequalities. Workshop on Real Computation and Complexity, 2004. Dagstuhl.

[81] F. Rouillier, M.F. Roy, and M. Safey. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *Journal of Complexity*, 16:716–750, 2000.

[82] F. Rouillier, M. Safey, and É. Schost. Solving the birkhoff interpolation problem via the critical point method: An experimental study. In J. Richter-Gebert and D. Wang, editors, *Automated Deduction in Geometry - Third International Workshop ADG 2000, Zurich Switzerland, September 2000, Revised Papers*, number 2061 in Lecture Notes in Artificial Intelligence, pages 26–40. Springer, 2001.

[83] F. Rouillier and P. Zimmermann. Efficient isolation of polynomial real roots. *Journal of Computational and Applied Mathematics*, 162(1):33–50, 2003.

[84] M. Safey El Din. *Résolution Réelle des Systèmes Polynomiaux en Dimension Positive*. PhD thesis, Université de Paris VI, 2001.

[85] M. Safey El Din. RAGLib (real algebraic library maple package). available at `http://www-calfor.lip6.fr/~safey/RAGLib`, 2003.

[86] M. Safey El Din and P. Trébuchet. Strong bihomogeneous bézout theorem and degree bounds for algebraic optimization. *submitted to Journal of Pure and Applied Algebra*, 2004.

[87] Mohab Safey El Din and Eric Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In J.R. Sendra, editor, *International Symposium on Symbolic and Algebraic Computation 2003 - ISSAC'2003, Philadelphie, USA*, pages 224–231. ACM Press, aug 2003.

[88] Mohab Safey El Din and Eric Schost. Properness defects of projection functions and computation of at least one point in each connected component of a real algebraic set. *Journal of Discrete and Computational Geometry*, sep 2004.

[89] É. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):349 – 393, 2003.

[90] É. Schost. Degree bounds and lifting techniques for triangular sets. In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 238–245. ACM Press, 2002.

[91] P. Trébuchet. Mpai (multi-precision arithmetic of infinitesimals). available at `http://www-calfor.lip6.fr/~trebuche/`, 2004.

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

[93] A.N. Varshenko. Theorems on the topological equisingularity of families of algebraic varieties and families of polynomial mapping. *Math. USSR Izv.*, 6:949–1008, 1972.

[94] J.-L. Verdier. Stratifications de whitney et théorème de bertini-sard. *Invent. Math.*, 35:295–312, 1976.

[95] A.H. Wallace. Linear sections of algebraic varieties. *Indiana Univ. Math. Journal*, pages 1153–1162, 1971.

[96] D. Wang. *Elimination Methods*. Springer-Verlag,Wien New York, 2001.

[97] V. Weispfenning. Comprehensive gröbner bases. *Journal of Symbolic Computation*, 14:1–29, 1992.

[98] V. Weispfenning. *Solving parametric polynomial equations and inequalities by symbolic algorithms*. World Scientific, 1995.

[99] Volker Weispfenning. Canonical comprehensive gröbner bases. In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 270–276. ACM Press, 2002.

[100] P. Wenger. Classification of 3r positioning manipulators. *Journal of Mechanical Design*, 120:327–332, June 1998.

[101] P. Wenger. Some guidelines for the kinematic design of new manipulators. *Mechanism and Machine Theory*, 35:437–449, 2000.

[102] Ph. Wenger and J. El Omri. Changing posture for cuspidal robot manipulators. In *Proceeding of the 1996 IEEE Int. Conf on Robotics and Automation*, pages 3173–3178, 1996.

[103] W. T. Wu. Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. Math. Sci.*, 4:207–235, 1984.

[104] W. T. Wu. A zero structure theorem for polynomial equations solving. *MM Research Preprints*, 1:2–12, 1987.

[105] L. Yang and J. Zhang. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. In Johnson/McKee/Vella, editor, *Artificial intelligence in mathematics*, pages 147–156. Oxford University Press, 1994.