INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Team salsa

Solvers for ALgebraic Systems and Applications

Paris - Rocquencourt

THEME SYM

Table of contents

1. Team

Head of team
Fabrice Rouillier [DR,INRIA Paris-Rocquencourt, HdR]

Assistante de projet
Laurence Bourcier [Secretary (SAR) Inria]

Personnel Inria
Jean-Charles Faugère [DR,INRIA Paris-Rocquencourt, HdR]

Reserch scientists (external)
Amir Hashemi [ATER - Univ. Pierre et Marie Curie]
Daniel Lazard [Emeritus Professor]
Ludovic Perret [Assistant Professor - Univ. Pierre et Marie Curie]
Mohab Safey El Din [Assistant Professor - Univ. Pierre et Marie Curie]
Philippe Trébuchet [Assistant Professor - Univ. Pierre et Marie Curie]

Ph. D. student
Guillaume Moroz [AMN - defense planned in 2008 - F. Rouillier]
Sajjad Rahmany [SPHERE grant - defense planned in 2009 - J.C. - Faugère]
Rong Xiao [Ambassade de France en Chine - defense planned in 2010 - F. Rouillier/X. Bican]
Liang Ye [China Scholarship Council - defense planned in 2009 - J.-C. Faugère/D. Wang]
Ting ZHAO [Chinese Government - defense planned in 2010 - F. Rouillier/D. Wang]

2. Overall Objectives

2.1. Overall Objectives

The main objective of the SALSA project is to solve systems of polynomial equations and inequations. We emphasize on algebraic methods which are more robust and frequently more efficient than purely numerical tools.

Polynomial systems have many applications in various scientific - academic as well as industrial - domains. However much work is yet needed in order to define specifications for the output of the algorithms which are well adapted to the problems.

The variety of these applications implies that our software needs to be robust. In fact, almost all problems we are dealing with are highly numerically unstable, and therefore, the correctness of the result needs to be guaranteed.

Thus, a key target 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 sacrificing the efficiency. Theoretical complexity for our algorithms is only a preliminary step of our work which culminates with efficient implementations which are designed to solve significant applications.

A consequence of our way of working is that many of our contributions 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.

3. Scientific Foundations

3.1. Introduction

For polynomial system solving, the mathematical specification of the result of a computation, in particular when the number of solutions is infinite, is itself a difficult problem [49], [50], [76], [75]. 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 meaning 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 include 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 goal is to characterize 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 iniquity of the studied mathematical objects does not imply the uncut of the related algorithms.

The pressure of the concurrence 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, above items naturally structure the algorithmic part of our research topics 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 the 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 (the most known object used to represent an ideal without loss of information) and on 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 homogenization and comprehension of the triangular structures [50].

3.2. Gröbner basis and triangular sets

Participants: J.C. Faugère, F. Rouillier, M. Safey El Din, R. Xiao.

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

The ideal $\mathfrak{I}=\langle P_1,...,P_s\rangle$ generated by $P_1,...,P_s$ is the set of polynomials in $K[X_1,...,X_n]$ constituted by all the combinations $\sum_{k=1}^{R} P_k U_k$ with $U_k\in\mathbb{Q}[X_1,...,X_n]$. Since every element of $\mathfrak{I}$ vanishes at each zero of S, we denote by $V_C(S)=V_C(I)=\{x\in C^n \mid p(x)=0\ \forall p\in\mathfrak{I}\}$ (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 $\mathfrak{I}\subset\mathbb{Q}[X_1,...,X_n]$ for any monomial ordering $<$.

(i) a polynomial $p\in\mathbb{Q}[X_1,...,X_n]$ belongs to $\mathfrak{I}$ 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 $\mathfrak{I}$, 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 ([59], [58]). 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 ([63] - algorithm F_4) a new generation of powerful algorithms ([63]) 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 ([62]) 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 was 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 :

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

(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 :

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

(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 ([84]) 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 ([106], [107]). 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 [77] and Kalkbrener [74] presented triangular decomposition algorithms with nicer properties for their outputs, based on additional requirements for the triangular sets and a generalization of the gcd of univariate polynomials over a product of fields.

The concept of regular chain introduced in [74] and [108] 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 ([49]).

P. Aubry and D. Lazard contributed to the homogenization of the work completed in this field by proposing a series of specifications and definitions gathering the whole of former work [50]. 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 $p \in K[X_1, ..., X_n] \setminus \mathbb{Q}$, 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 $t_i \neq 0$) $s = \Pi_{i=1,t_i\neq 0}^{n} s_i$.
- $\mathrm{sat}(T) =< T >: h^\infty = \{p \in K[X_1, ..., X_n] \mid \exists m \in \mathbb{N},\ h^m p \in \langle T \rangle\}$; the variety of T is $\mathbf{V}(\mathrm{sat}(T))$ and we have $\overline{\mathbf{V}(T) \setminus \mathbf{V}(h)} = \mathbf{V}(sat(T))$ (elementary property of localization).

A triangular set $T = (t_1, ..., t_n) \subset K[X_1, ..., X_n]$ is said to be regular (resp. separable) if $\forall i \in \{1, ..., n\}$ 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 ([49], [50]) :

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

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 equidimensional. These properties are essential for some of our algorithms. For example, having radical and equidimensional 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 [51], [93], [94].

Triangular sets based technics are efficient for specific problems like computing Galois ideals [52], 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 $\mathrm{sat}(T_i)$).

3.3. Zero-dimensional systems

Participants: J.C. Faugère, A. Hashemi, D. Lazard, F. Rouillier, 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 bring them back to linear algebra problems. More precisely, the algebra $K[X_1, ..., X_n]/I$ is in fact a K-vector space of dimension equal to the number of complex roots of the system (counted with multiplicities). We chose to exploit this structure. Accordingly, computing a base of $K[X_1, ..., X_n]/I$ is essential. A Gröbner basis gives a canonical projection from $K[X_1, ..., X_n]$ to $K[X_1, ..., X_n]/I$, 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 ([64]) : 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 compute 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 favorable ordering and then to deduce, by linear algebra technics, a Gröbner base for a lexicographic ordering [64].

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 [78] 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 up 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 mainly 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 [89] : we shown that any zero-dimensional system, depending on variables $X_1, ...X_n$, can systematically be rewritten, without loss of information (multiplicities, real roots), in the form $f(T) = 0, X_i = g_i(T)/g(T), i = 1...n$ where the polynomials $f, g, g_1, ...g_n$ have coefficients in the same ground field as those of the system and where T is a new variable (independent from $X_1, ...X_n$).
- efficient algorithms for solving (real roots isolation and counting) univariate polynomials [92], [82].

Thus, the use of innovative algorithms for Gröbner bases computations [63], [62], Rational Univariate representations ([64] for the "shape position" case and [89] for the general case), allows to use zero-dimensional solving as sub-task in other algorithms.

3.4. Positive-dimensional and parametric systems

Participants: J.C. Faugère, A. Hashemi, D. Lazard, G. Moroz, F. Rouillier, M. Safey El Din, R. Xiao.

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 equidimensional decomposition (which consists in considering separately the isolated solutions, the curves, the surfaces, ...) 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 into equidimensional but not necessarily irreducible components. These irreducible components may be obtained eventually 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, ...

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.

3.4.1. Critical point methods

The most widespread algorithm computing sampling points in a semi-algebraic set is the Cylindrical Algebraic Decomposition Algorithm due to Collins [60]. 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 [71], [72], [73], [56], [57]) 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 [89]);

(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.

[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.

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) [90].

Even if we showed that our solution may solve new classes of problems ([91]), 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 equidimensional variety, and/or a non-smooth variety. Our contributions consist in overcoming efficiently these obstacles ([95], [85]) and several strategies have been developed [51], [93], [94].

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 equidimensional 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 [51] 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 [93] 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 [94], 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 [51], [93] 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 equidimensional decomposition of an ideal. The experimental version of the algorithm provided in [96] will be included in the next release which is in preparation.

In terms of complexity, we have proved in [97] 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.

3.4.2. 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

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

and the basic constructible set

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

where p_i, f_j are polynomials with rational coefficients.

- $[U, X] = [U_1, ...U_d, X_{d+1}, ...X_n]$ is the set of *indeterminates* or variables, while $U = [U_1, ...U_d]$ is the set of *parameters* and $X = [X_{d+1}, ...X_n]$ the set of *unknowns*;
- $\mathcal{E} = \{p_1, ...p_s\}$ is the set of polynomials defining the equations;
- $\mathcal{F} = \{f_1, ...f_l\}$ 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 $(u_1, \cdots, u_d, x_{d+1}, ..., x_n) \longrightarrow (u_1, \cdots, u_d)$;
- Given any ideal I we denote by $\mathbf{V}(I) \subset \mathbb{C}^n$ 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, $\mathbf{V}(< \phi_u(\mathcal{E}) >))$ 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.

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 called 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 discriminant 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 $\mathcal{E} \bigcup \mathcal{F}$ [60] computes explicitly a discriminant variety of $\mathcal{C}$ as soon as the recursive projection steps w.r.t. $X_{d+1}, ..., X_n$ 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" [101], [102], [100], 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 [99] 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" $t \in \mathbb{Q}[X_{d+1}, ..., X_n]$ which is a polynomial (often a linear form) that induces, for almost all the parameters, an injective map from $\mathbf{V}(< \mathcal{E} >)$ to C^d. If p is the minimal polynomial of t viewed as an element of $\mathbb{Q}(U_1, ..., U_d)[X_{d+1}, ..., X_n]/\sqrt{< \mathcal{E} >}$, 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 $\sqrt{< \mathcal{E} >}$.

4. Application Domains

4.1. Panorama

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.

4.2. Cryptography

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 [65] (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 various cryptographic primitives using such approach [28], [27], [29]. For instance, we are investigating the security of a nonlinear filter generators (with J.-C. Faugère and L. Perret) in collaboration with the 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 [53].

As an application of the LLL algorithm we have presented [54], 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. In 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.

4.3. Parallel robots

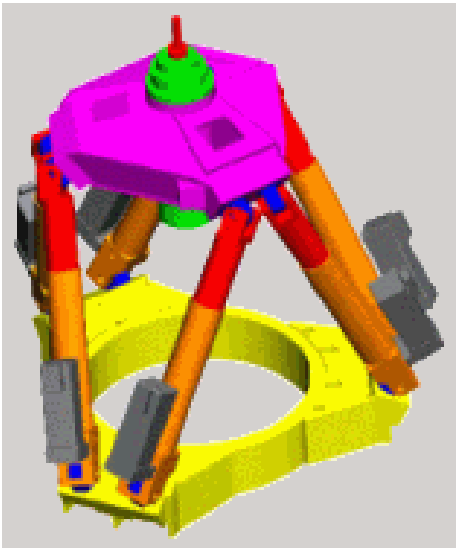

Figure 1. An Hexapod

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 [80], [79]. The results were often illustrated by Gröbner bases done with Gb software. One of the remarkable points of this study is certainly the classification suggested in [69]. The next efforts were related to the real roots and the effective computation of the solutions [87]. 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 2. 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 presently 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 [86]) 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 interpolating the trajectories, etc).

4.4. Serial robots

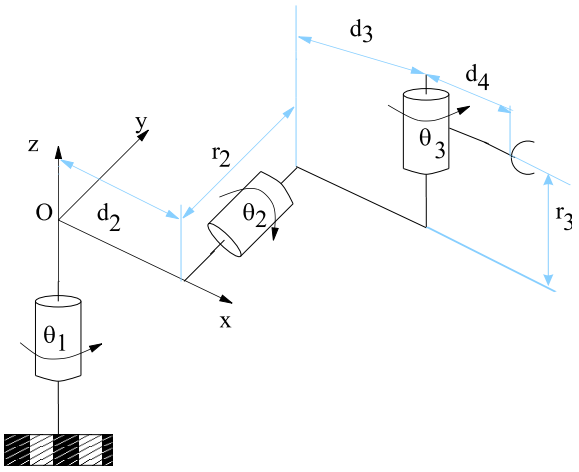

Figure 3. A serial robot with 3 D.O.F.

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.

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 ([103], [105], [104] and [83]) 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 compute 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.

4.5. Signal Processing

Some problems in signal theory are naturally formulated in terms of algebraic systems. In [70], 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 [68]. 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 [88] are partial), and still a few years more to be able to disseminate information towards our community [67]. Our software tools are now used to solve nearby problems [81].

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

5. Software

5.1. GC

Participants: J.C. Faugère [contact], 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.

5.2. UDX

Participants: F. Rouillier [contact], J.C. Faugère.

See http://fgbrs.lip6.fr/salsa/. The result of a Gröbner basis computation may be huge and is the main input of our high-level algorithms. The time needed for transferring 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 [66]. 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.

5.3. MPFI

Participants: F. Rouillier [contact], N. Revol [ARENAIRE Project].

MPFI is a library for multiprecision interval arithmetic, written in C (approximately 1000 lines), based on MPFR. It is developed 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.

5.4. MPAI

Participants: P. Trébuchet [contact], 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.

5.5. Interfaces

Participants: J.C. Faugère [contact], F. Rouillier.

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.

5.6. Gb

Participant: J.C. Faugère [contact].

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.

5.7. FGb Servers

Participant: J.C. Faugère [contact].

As mentioned 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.

5.8. RS

Participant: F. Rouillier [contact].

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).

5.9. RAGlib

Participant: M. Safey El Din [contact].

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 *equidimensional 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.

5.10. TCI

Participants: F. Rouillier [contact], 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.

5.11. TSPR

Participants: F. Rouillier [contact], 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.

5.12. NetTask

Participants: F. Rouillier [contact], J.C. Faugère.

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.

6. New Results

6.1. Univariate polynomials

In [36], we describe the design of a `C` library which is named `PTPol` implementing arithmetic operations for univariate polynomials. We report on practical experiments showing the relevance of using threads on recent multi-core computers.

We show how to use efficiently an API named `OpenMP` and POSIX Threads to achieve scalability. On multi-core architectures, we obtain a speed-up equivalent to the number of cores on addition and multiplication on univariate polynomials even for moderate degrees.

6.2. Algebraic processings

In [33], we introduce the notion of *regular decomposition* of an ideal and present a first algorithm to compute it. Designed to avoid generic perturbations and eliminations of variables, our algorithm seems to have a good behaviour with respect to the sparsity of the input system. Beside, the properties of the regular decompositions allow us to deduce new algorithms for the computation of the radical and the weak equidimensional decomposition of an ideal. A first implementation shows promising results.

6.3. Zero dimensional systems

Variants of our general framework for solving zero-dimensional systems have been designed for specific uses in challenging applications such as the study of ridges in computational geometry, the resolution of the direct kinematics problem for parallel robots or the synthesis of hyperfrequencies filters [12].

6.4. Parametric Polynomial Systems

In [21], we present a new algorithm for solving basic parametric constructible or semi-algebraic systems like $\mathcal{C} = \{x \in \mathbb{C}^n, p_1(x) = 0, ..., p_s(x) = 0, f_1(x) \neq 0, ..., f_l(x) \neq 0\}$ or $\mathcal{S} = \{x \in \mathbb{R}^n, p_1(x) = 0, ..., p_s(x) = 0, f_1(x) > 0, ..., f_l(x) > 0\}$, where $p_i, f_i \in \mathbb{Q}[U, X]$, $U = [U_1, ..., U_d]$ is the set of parameters and $X = [X_{d+1}, ..., X_n]$ the set of unknowns.

If Π_U denotes the canonical projection on the parameter's space, solving $\mathcal{C}$ leads to compute sub-manifolds $\mathcal{U} \subset \overline{\Pi_U(\mathcal{C})}$ such that $(\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}$ (we say that $\mathcal{U}$ has the $(\Pi_U, \mathcal{C})$-*covering property*). This guarantees that the cardinal of $\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}$ is locally constant on $\mathcal{U}$ and that $\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}$ is a finite collection of sheets which are all locally homeomorphic to $\mathcal{U}$. In the case where $\Pi_U(\mathcal{C})$ is dense in $\mathbb{C}^d$, known algorithms for solving $\mathcal{C}$ or $\mathcal{S}$ ([61], [98], [102]) compute implicitly or explicitly a Zariski closed subset W such that any sub-manifold of $\overline{\Pi_U(\mathcal{C})} \setminus W$ has the $(\Pi_U, \mathcal{C})$-covering property.

We introduce the *discriminant varieties of* $\mathcal{C}$ *with respect to* Π_U which are algebraic sets with the above property. We then show that the set of points of $\overline{\Pi_U(\mathcal{C})}$ which do not have any neighborhood with the $(\Pi_U, \mathcal{C})$-covering property is a Zariski closed set and thus define the *minimal discriminant variety of* $\mathcal{C}$ *with respect to* Π_U, and we propose an algorithm to compute it efficiently. Thus, solving $\mathcal{C}$ (resp. $\mathcal{S}$) is reduced to describing $\overline{\Pi_U(\mathcal{C})} \setminus W_D$ (resp.) which can be done using critical point methods such as in [55] or partial CAD based strategies [61].

Discriminant varieties have been successfully used for certifying a numerical global optimization process [18] and [17].

6.5. Critical point methods

Let f be a polynomial in $\mathbb{Q}[X_1, ..., X_n]$ of degree D. We focus on testing the emptiness and computing at least one point in each connected component of the semi-algebraic set defined by $f > 0$ (or $f < 0$ or $f \neq 0$). To this end, the problem is reduced to computing at least one point in each connected component of a hypersurface defined by $f - e = 0$ for $e \in \mathbb{Q}$ *positive and small enough*. We provide an algorithm allowing us to determine a positive rational number e which is small enough in this sense. This is based on the efficient computation of the set of *generalized critical values* of the mapping $f : y \in \mathbb{C}^n \to f(y) \in \mathbb{C}$ which is the union of the classical set of critical values of the mapping f and the set of *asymptotic critical values* of the mapping f. In [22], we provide a first algorithm allowing us to compute the set of generalized critical values of $\widetilde{f}$. This one is based on the computation of the critical locus of a projection on a plane P. This plane P must be chosen such that some global properness properties of some projections are satisfied. First practical experiments have shown the relevance of this approach.

Nevertheless, these properties of global properness, which are generically satisfied, can be difficult to check in practice. Moreover, choosing randomly the plane P induces a growth of the coefficients appearing in the computations.

In [34], we provide a new certified algorithm computing the set of generalized critical values of $\widetilde{f}$. This one is still based on the computation of the critical locus on a plane P. The certification process consists here in checking that this critical locus has dimension 1 (which is easy to check in practice), without any assumption of global properness. Moreover, this allows us to limit the growth of coefficients appearing in the computations by choosing a plane P defined by sparse equations. Additionally, we prove that the degree of this critical curve is bounded by $(D-1)^{n-1} - \mathfrak{d}$ where $\mathfrak{d}$ is the sum of the degrees of the positive dimensional components of the ideal $\langle \frac{\partial f}{\partial X_1}, ..., \frac{\partial f}{\partial X_n} \rangle$.

This latter algorithm is the most efficient in practice to compute generalized critical values. We also give complexity estimates for the algorithms designed in [22] and [34].

Additionnally, we show in [22] how to use the computation of generalized critical values in order to obtain an efficient algorithm deciding the emptiness of a semi-algebraic set defined by a single inequality or a single inequation. At last, we show how to apply our contribution to determining if a hypersurface contains real regular points.

The implementations obtained from this work are integrated in the RAGlib Maple package. Their efficiency have allowed us to solve real-life applications. In particular, they have been used for the problem of determining topology changes of the Voronoi diagram of three lines in the space [25], [39] (see below). This illustrates that an important general application of the critical point method is the proof that a multivariate polynomial is always positive or never negative.

In [35], we consider the case of polynomial systems of inequalities

$$f_1 > 0, ..., f_s > 0, \qquad \text{with } f_i \in \mathbb{Q}[X_1, ..., X_n]$$

defining *bounded* semi-algebraic sets. The case of bounded semi-algebraic sets appears frequently in applications. We provide an algorithm computing at least one point in each connected component of $\mathcal{S}$. This algorithm follows the spirit of the ones given in [22], [34]: infinitesimal deformations occuring in previous works are substituted by computations of critical values of some polynomial mappings. Finally, the initial problem is reduced to computing sampling points in several real algebraic sets defined by polynomial systems with coefficients in $\mathbb{Q}$. The subsequent implementation is integrated in the RAGlib Maple package and allows us to deal with problems coming from computational geometry, robotics and artifical vision which are not tractable by the best implementations of the Cylindrical Algebraic Decomposition algorithm.

6.6. General solving

Many algorithms for solving polynomial systems involve the computation of the discriminant of a polynomial with respect to some variable. Especially Collins CAD has to compute and factor discriminants of discriminants. In [32], we show that the discriminant of a discriminant factors naturally in seven factors such that four of them are generically equal to one. The three others are have respectively a multiplicity of at least 1, 2, 3 in the iterated discriminant. As these factor may be computed directly, this provides a dramatic improvement in the computation of the irreducible factors of the discriminant of a discriminant.

6.7. Computing Gröbner bases numerically

It is well known that in the computation of Gröbner bases an arbitrarily small perturbation in the coefficients of polynomials may lead to a completely different staircase even if the roots of the polynomials change continuously. In [26], this phenomenon is called pseudo singularity. We show how such phenomenon may be detected and even "repaired" by adding a new variable and a binomial relation each time. To investigate how often likely pseudo singularities may happen in numerical computation of Gröbner bases, two algorithms e-Buchberger and e-MatrixF5 are provided. The two algorithms are the modified versions of the Buchberger's algorithm and matrix F_5 algorithm. Using these methods, we can compute "more stable" Gr¨obner bases of equivalent ideals (with the same set of zeros) and thus they are suitable for the computation of Gröbner

bases for ideals generated by polynomials with floating-point coefficients. The main theorem of [26] is that any monomial basis (containing 1) of the quotient ring can be found out using VSGB strategy; this theorem provides us a great freedom to repair pseudo singularities. Experiments show that the algorithms can be used to solve some non-trivial problems.

6.8. Computational geometry

Ridges are curves of extremal curvature and therefore encode important informations used in segmentation, registration, matching and surface analysis. our first result was to show that ridges on parametric polynomial surfaces can be viewed as the zero set of an implicit plane curve whose singular points are well identified by specialists (so called ombilics or purple points). A consequence was that we were able to provide a certified drawing of such curves using the univariate capabilities of RS. A second result was to exploit the particular structure of the singular locus of this plane curve in order to propose a new algorithm for computing its topology (and thus the topology of the ridges)[13].

We have a long term collaboration with project VEGAS which began with the complete classification and the parameterization of real quadric intersections [14], [15], [16].

This collaboration is now pursued by the study of the Voronoi of linear structures in $\mathbb{R}^d$. This is a continuation of the preceding work, as the bisector of two linear objects is a quadric and the trisectors are thus intersections of quadrics.

We have given a complete description of the Voronoi diagram, in $\mathbb{R}^3$, of three lines in general position, that is, that are pairwise skew and not all parallel to a common plane [25], [39]. In particular, we show that the topology of the Voronoi diagram is invariant for three such lines. For the proof, we needed to use heavily the software of the team, especially the Gröbner basis engine FGB and the work on the critical point method (see above).

This opens the possibility to design an efficiently implementable algorithm to compute the Voronoi diagram of a finite set of linear structures (points, segments, lines, polygons, polyhedrons, polytopes, etc.). This has been sketchly described by D. Lazard at the workshop without proceedings *WRSO (Workshop on Robust Shape Operations), Sophia-Antipolis, September 2007*. This algorithm will involve, as basic operations, the zero-dimensional solving and the computation of the Voronoi diagram of three basic objects, the case of three lines, just solved, being the most difficult.

6.9. Cryptography

In *"Block Ciphers Sensitive to Gröbner Basis Attacks"* (CT RSA 2006), Buchmann, Pyshkin and Weinmann have described two families of Feistel and SPN block-ciphers called Flurry and Curry respectively. These two families of ciphers are fully parametrizable and have a sound design strategy against classical statistical attacks (i.e. linear and differential attacks). In addition, the encryption process can be easily described by a set of algebraic equations. These ciphers are then targets of choices for algebraic attacks. In particular, the authors have reduced the key-recovery problem to the problem of changing the order of a Gröbner basis. This attack – although being more efficient that linear and differential attacks – remains quite limited. By using more efficient algorithms, we first propose a practical improvement of this attack[42], [43]. However, this will not permit to change the theoretical complexity of the attack. We have then investigate the possibility of using a small number of suitably chosen pairs of message/ciphertext for improving algebraic attacks. It turns out that this approach permits to go one step further in the (algebraic) cryptanalysis of Flurry and Curry. From our experiments, we estimate that this last approach is of polynomial-time complexity when the S-box is a power function. For instance, we have been able to break a 128-bit Flurry – with 7 rounds – in less that one hour. Note that this work has been initiated by a previous study which was partially financed by a contract with DGA.

In 2004, a new attack against SHA-1 has been proposed by a team leaded by Wang. The aim of [37] is to sophisticate and improve Wang's attack by using algebraic techniques. To do so, we introduce new notions (semi-neutral bit, adjuster) and propose then an improved message modification technique based on algebraic techniques. In the case of the 58-round SHA-1, the experimental complexity of our improved attack is 2^{31} SHA-1 computations, whereas Wang's method needs 2^{34} SHA-1 computations. We have found many new collisions for the 58-round SHA-1. We also study the complexity of our attack for the full SHA-1.

We have described [29] an efficient forgery and full-key recovery attacks on the ℓ-IC$^-$ signature scheme recently proposed at PKC 2007. This cryptosystem is a multivariate scheme based on a new internal quadratic primitive which avoids some drawbacks of multivariate schemes. The public and secret key are shorter than in many multivariate signature schemes. Our attacks rely on the recent cryptanalytic tool developed by Dubois *et al.* against the SFLASH signature scheme. However, the final stage of the attacks require the use of Gröbner basis techniques to actually forge a signature (resp. to recover the secret key).

6.10. Error Correcting Codes

In [24] we address the problem of the algebraic decoding of any cyclic code up to the true minimum distance. For this, we use the classical formulation of the problem, which is to find the error locator polynomial in terms of the syndroms of the received word. This is usually done with the Berlekamp-Massey algorithm in the case of BCH codes and related codes, but for the general case, there is no generic algorithm to decode cyclic codes. Even in the case of the quadratic residue codes, which are good codes with a very strong algebraic structure, there is no available general decoding algorithm. For this particular case of quadratic residue codes, several authors have worked out, by hand, formulas for the coefficients of the locator polynomial in terms of the syndroms, using the Newton identities. This work has to be done for each particular quadratic residue code, and is more and more difficult as the length is growing. Furthermore, it is error-prone. We propose to automate these computations, using elimination theory and Gröbner bases. We prove that, by computing appropriate Gröbner bases, one automatically recovers formulas for the coefficients of the locator polynomial, in terms of the syndroms.

6.11. Signal processing

Synthesis and identification of hyperfrequency filters made of coupled resonant cavities. Our contribution to the ARC SILA is summarized in [12] : we propose a new approach to the synthesis of coupling matrices for microwave filters is presented. This new approach represents an advance on existing direct and optimization methods for coupling matrix synthesis in that it will exhaustively discover all possible coupling matrix solutions for a network if more than one exists. We illustrate this by carrying out the synthesis process of two asymmetric filters of 8th and 10th degree.

Global convergence of a numerical optimization process. The global convergence of a recently proposed constant modulus (CM) and cross-correlation (CC)-based algorithm (CC-CMA) is studied in [18] and [17]. The convergence of this process, and more generally global convergent analysis of gradient stochastic algorithms including is strongly related to the study of some parametric semi-algebraic sets. In [17], we show that CC-CMA can converge globally if the parameter which mix the CM and CC terms is properly selected.

6.12. Robotics

We work for a long time on the direct kinematics problem for parallel robots. Our last results consists in exploiting some linear relations very early in the computations so that the difficult part is now reduced to the resolution of a non linear system of equations depending on 3 variables (instead of 7 in the best known alternatives). A direct consequence is that its resolution using pure algebraic methods decreases to less than 1 sec for any kind of robot to get all the possible solutions in a certified way [38].

7. Contracts and Grants with Industry

7.1. WMI (Maple)

Participants: F. Rouillier [contact], J.-C. Faugère [contact].

A contract as been signed with the Canadian company *Waterloo Maple Inc* in 2005. The objective is to integrate *SALSA* software into one of the most well known general computer algebra system (*Maple*).

The basic term of the contract is of four years (renewable).

7.2. CELAR (DGA)

Participants: J.C. Faugère [contact], L. Perret.

The new contract begin in september 2007 and the objective is to evaluate, on examples of realistic size, how to apply multivariate decomposition technique to recover the secret key on some symmetric cryptosystems like Trivium or Bivium. New algorithms for solving efficiently the problem of recovering a decomposition in the case of multivariate systems in 2006 and 2007 by Faugère and Perret.

7.2.1. ANR Grant "MAC"

Participants: J.C. Faugère [contact], L. Perret.

In collaboration with France Telecom and ENSTA.

This project is to be replaced in the more general context of information protection. Its research areas are cryptography and symbolic computation. We are here essentially – but not exclusively – concerned with public key cryptography. One of the main issues in public key cryptography is to identify hard problems, and propose new schemes that are not based on number theory. Following this line of research, *multivariate schemes* have been introduced in the mid eighties [Diffie and Fell 85, Matsumoto and Imai 85].

In order to evaluate the security of new proposed schemes, strong and efficient cryptanalytic methods have to be developped. The main theme we shall address in this project is the evaluation of the security of cryptographic primitives by means of algebraic methods. The idea is to model a cryptographic primitive as a system of algebraic equations. The system is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the considered primitive. Once this modeling is done, the problem is then to solve an algebraic system. Up to now, Gröbner bases appear to yield the best algorithms to do so.

7.3. International Actions

7.3.1. INRIA Associate Team "Chinese SALSA"

Chineese Salsa is an associate team created in January 2006. It brings together most of the members of SALSA and researchers from Beihang university, Beijing (university and academy of science). The general objectives of *Chinese-Salsa* are mainly the same as those of *SALSA*.

8. Dissemination

8.1. Scientific Animation

8.1.1. Journals - Associate Editor

- journal “Mathematics in Computer Science” (Birkhauser). J.C. Faugère
- journal “Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences” Springer J.C. Faugère

- Special issue of the Journal of Symbolic Computation on Gröbner Bases and Applications in Cryptology and Error Correcting Codes. Editors J.C. Faugère, L. Perret.
- RISC book series (Springer, Heidelberg), “Gröbner Bases, Coding, and Cryptography”. Editors: L. Perret (with T. Mora, S. Sakata, M. Sala, C. Traverso).
- Special issue of the Journal of Symbolic Computation on Efficient Computation of Gröbner Bases. Editors J.C. Faugère.
- Special issue of the Journal of Symbolic Computation on Polynomial System Solving. Editors J.C. Faugère, F. Rouillier.
- Special issue of the Journal “Mathematical Aspects in Computer Science”. Editor F. Rouillier.

8.1.2. Programm Committees

- International Conference on Mathematical Aspects of Computer and Information Sciences MACIS : J.C. Faugère and F. Rouillier
- Parallel Symbolic Computation, PASCO 2007 : J.C. Faugère
- Advisory Board MEGA Conference: J.C. Faugère

8.1.3. Conferences (organization)

- MACIS 2007 : F. Rouillier (general chair) - M. Safey El Din (local chair)
- MACIS 2008 : F. Rouillier (chair of the Steering commitee)
- ECRYPT PhD SUMMER SCHOOL on “Emerging Topics in Cryptographic Design and Cryptanalysis" (2007) : L. Perret (with C. Cid)
- SCC 2008: J.C. Faugère and L. Perret.

8.1.4. Invited lectures

- F. Rouillier : Workshop on Robust Shape Operations [47]
- M. Safey El Din : Journées Nationales du Calcul Formel, 2007 [48]
- J.C. Faugère: [42], [40], [41], [43], invited by CNR (Roma, Italy).
- L. Perret : Sage Days 6 [46]
- L. Perret : ECRYPT PhD SUMMER SCHOOL : An Overview [45]

9. Bibliography

Major publications by the team in recent years

[1] P. AUBRY, D. LAZARD, M. MORENO MAZA. *On the theories of triangular sets*, in "Journal of Symbilic Computation", vol. 28, 1999, p. 105-124.

[2] P. AUBRY, F. ROUILLIER, M. SAFEY EL DIN. *Real Solving for Positive Dimensional Systems*, in "Journal of Symbolic Computation", vol. 34, n^{o} 6, 2002, p. 543–560.

[3] J.-C. 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.

[4] J.-C. FAUGÈRE. *A New Efficient Algorithm for Computing Gröbner bases (F_4)*, in "Journal of Pure and Applied Algebra", vol. 139, n^o 1-3, June 1999, p. 61-88.

[5] J.-C. FAUGÈRE, A. JOUX. *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases*, in "CRYPTO 2003", 2003, p. 44-60.

[6] J.-C. FAUGÈRE, F. MOREAU DE SAINT MARTIN, F. ROUILLIER. *Design of regular nonseparable bidimensional wavelets using Groebner basis techniques*, in "IEEE SP Transactions Special Issue on Theory and Applications of Filter Banks and Wavelets", vol. 46, n^o 4, apr 1998, p. 845-856.

[7] F. ROUILLIER. *Solving zero-dimensional systems through the rational univariate representation*, in "Journal of Applicable Algebra in Engineering, Communication and Computing", vol. 9, n^o 5, 1999, p. 433–461.

[8] F. ROUILLIER, P. ZIMMERMANN. *Efficient Isolation of Polynomial Real Roots*, in "Journal of Computational and Applied Mathematics", vol. 162, n^o 1, 2003, p. 33-50.

[9] M. SAFEY EL DIN, E. SCHOST. *Polar varieties and computation of one point in each connected component of a smooth real algebraic set*, in "International Symposium on Symbolic and Algebraic Computation 2003 - ISSAC'2003, Philadelphie, USA", J. SENDRA (editor), ACM Press, aug 2003, p. 224-231.

Year Publications

Doctoral dissertations and Habilitation theses

[10] J.-C. FAUGÈRE. *Calcul efficace des bases de Gröbner et Applications.*, Habilitation à Diriger des Recherches, Université Pierre et Marie Curie - Paris VI, 2007.

[11] F. ROUILLIER. *Algorithmes pour l'étude des solutions réelles des systèmes polynomiaux*, Habilitation à Diriger des Recherches, Université Pierre et Marie Curie - Paris VI, 2007.

Articles in refereed journals and book chapters

[12] R. CAMERON, J.-C. FAUGÈRE, F. ROUILLIER, F. SEYFERT. *An Exhaustive Approach to the Coupling Matrix Synthesis Problem Application to the Design of High Degree Asymmetric Filters*, in "International Journal of RF and Microwave Computer-Aided Engineering", vol. 17, n^o 1, 2007, p. 4–12.

[13] F. CAZALS, J.-C. FAUGÈRE, M. POUGET, F. ROUILLIER. *8*, in "Ridges and Umbilics of Polynomial Parametric Surfaces", Geometric Modeling and Algebraic Geometry, vol. 8, n^o 232, Springer, 2007, p. 141–160.

[14] L. DUPONT, D. LAZARD, S. LAZARD, S. PETITJEAN. *Near-Optimal Parameterization of the Intersection of Quadrics : I. The Generic Algorithm*, in "Journal of Symbolic Computation", to appear, 2007.

[15] L. DUPONT, D. LAZARD, S. LAZARD, S. PETITJEAN. *Near-Optimal Parameterization of the Intersection of Quadrics : II. A classification of pencils*, in "Journal of Symbolic Computation", to appear, 2007.

[16] L. DUPONT, D. LAZARD, S. LAZARD, S. PETITJEAN. *Near-Optimal Parameterization of the Intersection of Quadrics : III. Parameterizing Singular Intersections.*, in "Journal of Symbolic Computation", to appear, 2007.

[17] N. GU, D. LAZARD, F. ROUILLIER, Y. XIANG. *Using computer algebra to certify the global convergence of a numerical optimization process*, in "Mathematics in Computer Science", to appear, online version available, 2007.

[18] N. GU, Y. XIANG, F. ROUILLIER. *Comments on A blind Signal Separation Method for Multiuser Communications*, in "IEEE Transactions on Signal Processing", vol. 55, n^{o} 5, 2007, p. 2355–2356.

[19] A. HASHEMI. *Polynomial Complexity for Hilbert Series of Borel Type Ideals*, in "Albanian Journal of Mathematics", vol. 1, 2007, p. 145-155.

[20] A. HASHEMI. *Sharper Degree Bound for Polynomial Representation and Complexity of Gröbner Bases*, in "Journal of Computational Complexity", to appear, 2007.

[21] D. LAZARD, F. ROUILLIER. *Solving parametric polynomial systems*, in "Journal of Symbolic Computation", vol. 42, 2007, p. 636-667.

[22] M. SAFEY EL DIN. *Testing Sign Conditions on a Multivariate Polynomial and Applications*, in "Mathematics in Computer Science", to appear,online version available, 2007.

Publications in Conferences and Workshops

[23] G. ARS, A. HASHEMI. *Efficient Computation of Syzygies by Faugere's F5 algorithm*, in "MACIS 2007: Mathematical Aspects of Computer and Information Sciences", 12 2007.

[24] D. AUGOT, M. BARDET, J.-C. FAUGÈRE. *On formulas for decoding binary cyclic codes.*, in "IEEE International Symposium on Information Theory 2007", GOLDSMITH, MEDARD, SHOKROLLAHI, ZAMIR (editors), June 2007, http://www.isit2007.org/.

[25] H. EVERETT, D. LAZARD, S. LAZARD, M. SAFEY EL DIN. *The Voronoi diagram of three lines in R^3*, in "SoCG '07: Proceedings of the twenty-third annual symposium on Computational geometry", 6 2007, p. 255–264.

[26] J.-C. FAUGÈRE, L. YE. *Numerical Computation of Grobner Bases for Zero-dimensional Polynomial Ideals*, in "Mathematical Aspects of Computer and Information Sciences 2007, Paris, France", December 2007, http://www-spiral.lip6.fr/MACIS2007/schedule.html.

[27] J.-C. FAUGÈRE, L. PERRET. *Cryptanalysis of $2R^-$ Schemes*, in "Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference", Lecture Notes in Computer Science, vol. 4117, Springer, 2007, p. 357-372.

[28] J.-C. FAUGÈRE, L. PERRET. *Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects*, in "Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Lecture Notes in Computer Science, vol. 4004, Springer, 2007, p. 30-47.

[29] P.-A. FOUQUE, G. MACARIORAT, L. PERRET, J. STERN. *On the Security of the ℓ-IC Signature Scheme*, in "Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2008", Lecture Notes in Computer Science, to appear, Springer, 2007.

[30] A. HASHEMI. *Efficient Algorithms for Computing Noether Normalization*, in "ASCM 2007: The 8th ASian Symposium on Computer Mathematics", 12 2007.

[31] A. HASHEMI. *Polynomial-Time Algorithm for Hilbert Series of Borel Type Ideals*, in "SNC'07: Symbolic-Numeric Computation'07", 7 2007.

[32] D. LAZARD, S. MCCALLUM. *Iterated Discriminants*, in "MEGA 2007: Effective Methods in Algebraic Geometry", 6 2007.

[33] G. MOROZ. *Regular Decompositions*, in "Proceedings of the Asian Symposia on Computer Mathematics", to appear, 2007.

[34] M. SAFEY EL DIN. *Practical and theoretical issues for the computation of generalized critical values of a polynomial mapping and its applications*, in "Proceedings of Asian Symposium on Computer Mathematics 2007", Lecture Notes in Computer Science, to appear, 2007.

[35] M. SAFEY EL DIN. *Real solving polynomial systems of inequalities: the case of bounded sets of solutions (extended abstract)*, in "Mathematical Aspects of Computer and Information Sciences 2007", 2007.

[36] M. SAFEY EL DIN, P. TRÉBUCHET. *POSIX threads polynomials(PTPol): a scalable implementation of univariate arithmetic operations*, in "PASCO '07: Proceedings of the 2007 international workshop on Parallel symbolic computation, New York, NY, USA", ACM, 2007, p. 104–106, http://doi.acm.org/10.1145/1278177.1278198.

[37] M. SUGITA, M. KAWAZOE, L. PERRET, H. IMAI. *Algebraic Cryptanalysis of 58-Round SHA-1*, in "Fast Software Encryption, 14th International Workshop, FSE", Lecture Notes in Computer Science, vol. 4593, Springer, 2007, p. 349-365.

Internal Reports

[38] J.-C. FAUGÈRE, J.-P. MERLET, F. ROUILLIER. *On solving the direct kinematics problem for parallel robots*, Submitted to J. of Robotics Research - Under revision, Technical report, n^{o} RR-5923, INRIA, 2007, http://hal.inria.fr/inria-00072366/fr/.

Miscellaneous

[39] H. EVERETT, D. LAZARD, S. LAZARD, M. SAFEY EL DIN. *The Voronoi diagram of three lines in R^3*, Submitted on September 5, 2007, 2007.

[40] J.-C. FAUGÈRE. *Efficient algorithms for computing Gröbner bases*, 2007, http://ecrypt-ss07.rhul.ac.uk/, Emerging Topics in Cryptographic Design. and Cryptanalysis Samos Greece.

[41] J.-C. FAUGÈRE. *Efficient Gröbner bases computations and application in industry*, 2007, http://www.ciem.unican.es/encuentros/wcagmi/, Computer Algebra in Geometric Modeling and Industry, Castro Urdiales , Spain.

[42] J.-C. FAUGÈRE. *Groebner bases and cryptography.*, Lectures Notes in Computer Science, Springer Verlag, March 2007, http://fse2007.uni.lu/, Lectures Notes in Computer Science, Alex Biryukov, editor.

[43] J.-C. FAUGÈRE. , Z. LIU (editor)*The F5 algorithm and applications in Cryptology*, 2007, http://www.mmrc.iss.ac.cn/, Key Laboratory of Mathematics-Mechanization in the Chinese Academy of Sciences, Beijing, China.

[44] D. LAZARD, S. MCCALLUM. *Iterated Discriminants*, Submitted on November 13, 2007, 2007.

[45] L. PERRET. *Gröbner Bases in Cryptography : An Overview*, 2007, http://wiki.sagemath.org/days6, Invited lecture at SAGE Days 6.

[46] L. PERRET. *Gröbner Bases in Public Key Cryptography*, 2007, http://ecrypt-ss07.rhul.ac.uk/, lecture course at ECRYPT PhD SUMMER SCHOOL on “Emerging Topics in Cryptographic Design and Cryptanalysis".

[47] F. ROUILLIER. *Polynomial system solving and computational geometry*, 2007, http://www-sop.inria.fr/geometrica/events/WRSO/, Invited lecture at WRSO’07.

[48] M. SAFEY EL DIN. *Algorithmes efficaces en géométrie algébrique réelle*, 2007, http://jncf2007.loria.fr/, Invited course at JNCF’07.

References in notes

[49] P. AUBRY. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques*, Ph. D. Thesis, Université Paris 6, France, 1999.

[50] P. AUBRY, D. LAZARD, M. MORENO MAZA. *On the theories of triangular sets*, in "Journal of Symbilic Computation", vol. 28, 1999, p. 105-124.

[51] P. AUBRY, F. ROUILLIER, M. SAFEY EL DIN. *Real Solving for Positive Dimensional Systems*, in "Journal of Symbolic Computation", vol. 34, n^{o} 6, 2002, p. 543–560.

[52] P. AUBRY, A. VALIBOUZE. *Using Galois ideals for computing relative resolvents*, in "J. of Symbolic Computation", Special Issue on Algorithmic Galois Theory, vol. 30, n^{o} 6, 2000, p. 635-651.

[53] A. BASIRI, A. ENGE, J. FAUGÈRE, N. GÜREL. *Implementing the arithmetic of c34 curves.*, in "Sixth Algorithmic Number Theory Symposium, ANTS VI proceedings (Vermont, USA, June 13–18, 2004)", D. BUELL (editor), LNCS, vol. 3076, Springer-Verlag, 2004, p. 57–71.

[54] A. BASIRI, J.-C. FAUGÈRE. *Changing the ordering of Gröbner bases with LLL: case of two variables*, in "ISSAC 2003", 2003, p. 23-29.

[55] S. BASU, R. POLLACK, M.-F. ROY. *Algorithms in real algebraic geometry*, Algorithms and Computations in Mathematics, vol. 10, Springer-Verlag, 2003.

[56] S. BASU, R. POLLACK, M. ROY. *On the combinatorial and algebraic complexity of quantifier elimination*, in "Journal of Assoc. Comput. Machin.", 1996, p. 1002–1045.

[57] S. BASU, R. POLLACK, 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.

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

[59] B. BUCHBERGER, G.-E. COLLINS, R. LOOS. *Computer Algebra Symbolic and Algebraic Computation*, second edition, Springer-Verlag, 1982.

[60] G. COLLINS. *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, in "Springer Lecture Notes in Computer Science 33", vol. 33, 1975, p. 515-532.

[61] G. E. COLLINS, H. HONG. *Partial Cylindrical Algebraic Decomposition*, in "Journal of Symbolic Computation", vol. 12, n^{o} 3, 1991, p. 299–328.

[62] J.-C. 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.

[63] J.-C. FAUGÈRE. *A New Efficient Algorithm for Computing Gröbner bases (F_4)*, in "Journal of Pure and Applied Algebra", vol. 139, n^{o} 1-3, June 1999, p. 61-88.

[64] J. FAUGÈRE, P. GIANNI, D. LAZARD, T. MORA. *Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering*, in "Journal of Symbolic Computation", vol. 16, n^{o} 4, Oct. 1993, p. 329–344.

[65] J.-C. FAUGÈRE, A. JOUX. *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases*, in "CRYPTO 2003", 2003, p. 44-60.

[66] J. FAUGÈRE, F. ROUILLIER. *Dispositif d'échanges de données entre matériels informatiques*, 1999, Patent proposal number 99 08172.

[67] J.-C. FAUGÈRE, F. ROUILLIER. *Design of filter and filter banks using dedicated Computer Algebra Tools*, in "International Conference on Applications of Computer Algebra (ACA'99)", Applications of Computer Algebra to Signal Processing, Jeremy Johnson and Markus Pueschel, 1999.

[68] J. FAUGÈRE, F. MOREAU DE SAINT MARTIN, F. ROUILLIER. *Une famille de bancs de filtres 2D non séparables*, 1997, Patent.

[69] J. FAUGÈRE, D. LAZARD. *The Combinatorial Classes of Parallel Manipulators*, in "Mechanism and Machine Theory", vol. 30, 1995, p. 765–776.

[70] J.-C. FAUGÈRE, F. MOREAU DE SAINT MARTIN, F. ROUILLIER. *Design of regular nonseparable bidimensional wavelets using Groebner basis techniques*, in "IEEE SP Transactions Special Issue on Theory and Applications of Filter Banks and Wavelets", vol. 46, n^{o} 4, Apr 1998, p. 845-856.

[71] D. GRIGOR'EV, N. VOROBJOV. *Solving Systems of Polynomial Inequalities in Subexponential Time*, in "J. Symbolic Comput.", vol. 5, 1988, p. 37–64.

[72] J. HEINTZ, M.-F. ROY, P. SOLERNÓ. *On the Complexity of Semi-Algebraic Sets*, in "Proc. IFIP 89, San Francisco", 1989, p. 293-298.

[73] J. HEINTZ, M.-F. ROY, P. SOLERNÓ. *On the Theoritical an Practical Complexity of the Existential Theory of Reals*, in "The Computer Journal", vol. 36, n^{o} 5, 1993, p. 427-431.

[74] M. KALKBRENNER. *Three contributions to elimination theory*, Ph. D. Thesis, Johannes Kepler University, Linz, 1991.

[75] D. LAZARD. *Resolution of polynomial systems*, in "4th Asian Symposium on Computer Mathematics - ASCM 2000, Chiang Mai, Thailand", Lecture Notes Series on Computing, vol. 8, World Scientific, Dec 2000, p. 1 - 8.

[76] D. LAZARD. *On the specification for solvers of polynomial systems*, in "5th Asian Symposium on Computers Mathematics -ASCM 2001", Lecture Notes Series in Computing, vol. 9, World Scientific, 2001, p. 66-75.

[77] D. LAZARD. *A new method for solving algebraic systems of positiove dimension*, in "Discrete Applied Mathematics", 1991.

[78] D. LAZARD. *Solving Zero - dimensional algebraic systems*, in "Journal of Symbolic Computation", vol. 13, 1992, p. 117-132.

[79] D. LAZARD. *Stewart platforms and Gröbner basis*, in "Proceedings of Advances in Robotics Kinematics", Sep 1992, p. 136-142.

[80] D. LAZARD, J.-P. MERLET. *The (true) Stewart platform has 12 configurations*, in "Proc. of IEEE Conference on Robotics and Vision, San Diego", 1994.

[81] J. LEBRUN, I.-W. . SELESNICK. *Gröbner bases and wavelet design*, in "Journal of Symbolic Computtation", vol. 37, n^{o} 2, 2004, p. 227-259.

[82] H. LOMBARDI, M.-F. ROY, M. SAFEY EL DIN. *New Structure Theorems for subresultants*, in "Journal of Symbolic Computations", May, 2000.

[83] J. E. OMRI. *Analyse géomtrique et cinématique des mécanismes de type manipulateur*, Ph. D. Thesis, Université de Nantes, Feb. 1996.

[84] J. RITT. *Differential equations from an algebraic standpoint*, in "American Mathematical Society Colloquium Publications", vol. 14, 1932.

[85] F. ROUILLIER. *Efficient algorithms based on critical points method*, in "Algorithmic and Quantitative Real Algebraic Geometry", S. BASU, L. GONZALEZ-VEGA (editors), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 60, American Mathematical Society, 2003, p. 123–138.

[86] F. ROUILLIER. *Efficient real solutions and robotics*, in "First EMS -SMAI -SMF Joint Conference Applied Mathematics and Applications of Mathematics", 2003.

[87] F. ROUILLIER. *Real Root Counting For some Robotics problems*, in "Solid Mechanics and its Applications, Kluwer Academic Publishers", vol. 40, 1995, p. 73-82.

[88] F. ROUILLIER. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*, Ph. D. Thesis, Université de Rennes I, may 1996.

[89] F. ROUILLIER. *Solving zero-dimensional systems through the rational univariate representation*, in "Journal of Applicable Algebra in Engineering, Communication and Computing", vol. 9, n^{o} 5, 1999, p. 433–461.

[90] F. ROUILLIER, M. ROY, M. SAFEY EL DIN. *Finding at least one point in each connected component of a real algebraic set defined by a single equation*, in "Journal of Complexity", vol. 16, 2000, p. 716–750.

[91] F. ROUILLIER, M. SAFEY EL DIN, É. SCHOST. *Solving the Birkhoff Interpolation Problem via the Critical Point Method: An Experimental Study*, in "Automated Deduction in Geometry - Third International Workshop ADG 2000, Zurich Switzerland, September 2000, Revised Papers", J. RICHTER-GEBERT, D. WANG (editors), Lecture Notes in Artificial Intelligence, n^{o} 2061, Springer, 2001, p. 26–40.

[92] F. ROUILLIER, P. ZIMMERMANN. *Efficient Isolation of Polynomial Real Roots*, in "Journal of Computational and Applied Mathematics", vol. 162, n^{o} 1, 2003, p. 33-50.

[93] M. SAFEY EL DIN, E. SCHOST. *Polar varieties and computation of one point in each connected component of a smooth real algebraic set*, in "International Symposium on Symbolic and Algebraic Computation 2003 - ISSAC'2003, Philadelphie, USA", J. SENDRA (editor), ACM Press, aug 2003, p. 224-231.

[94] M. SAFEY EL DIN, E. SCHOST. *Properness defects of projection functions and computation of at least one point in each connected component of a real algebraic set*, in "Journal of Discrete and Computational Geometry", sep 2004.

[95] M. SAFEY EL DIN. *Résolution Réelle des Systèmes Polynomiaux en Dimension Positive*, Ph. D. Thesis, Université de Paris VI, 2001.

[96] M. SAFEY EL DIN. *RAGLib (Real Algebraic Library Maple package)*, 2003, http://www-calfor.lip6.fr/~safey/RAGLib.

[97] M. SAFEY EL DIN, P. TRÉBUCHET. *Strong bihomogeneous Bézout theorem and degree bounds for algebraic optimization*, submitted to Journal of Pure and Applied Algebra, Technical report, n^{o} 5071, INRIA, 2004, http://hal.inria.fr/inria-00071512.

[98] É. SCHOST. *Sur la résolution des systèmes polynomiaux à paramètres*, Ph. D. Thesis, École polytechnique, 2000.

[99] É. SCHOST. *Computing Parametric Geometric Resolutions*, in "Applicable Algebra in Engineering, Communication and Computing", vol. 13, n^{o} 5, 2003, p. 349 - 393.

[100] V. WEISPFENNING. *Canonical comprehensive Gröbner bases*, in "Proceedings of the 2002 international symposium on Symbolic and algebraic computation", ACM Press, 2002, p. 270–276.

[101] V. WEISPFENNING. *Comprehensive Gröbner bases*, in "Journal of Symbolic Computation", vol. 14, 1992, p. 1–29.

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

[103] P. WENGER, J. E. OMRI. *Changing Posture for cuspidal Robot Manipulators*, in "Proceeding of the 1996 IEEE Int. Conf on Robotics and Automation", 1996, p. 3173-3178.

[104] P. WENGER. *Some guidelines for the kinematic design of new manipulators*, in "Mechanism and Machine Theory", vol. 35, 2000, p. 437-449.

[105] P. WENGER. *Classification of 3R Positioning Manipulators*, in "Journal of Mechanical Design", vol. 120, June 1998, p. 327-332.

[106] W. T. WU. *Basic principles of mechanical theorem proving in elementary geometries*, in "J. Sys. Sci. Math. Sci.", vol. 4, 1984, p. 207–235.

[107] W. T. WU. *A Zero Structure Theorem for polynomial equations solving*, in "MM Research Preprints", vol. 1, 1987, p. 2-12.

[108] L. YANG, J. ZHANG. *Searching dependency between algebraic equations: an algorithm applied to automated reasoning*, in "Artificial intelligence in mathematics", JOHNSON, MCKEE, VELLA (editors), Oxford University Press, 1994, p. 147–156.