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

Research Scientist

Fabrice Rouillier [Team Leader, Research Director, INRIA, HdR]
Jean-Charles Faugère [Research Director, INRIA, HdR]
Dongming Wang [Research Director, CNRS, HdR]

Faculty Member

Daniel Lazard [Emeritus Professor, HdR]
Ludovic Perret [Assistant Professor - Univ. Pierre et Marie Curie]
Guénael Renault [Assistant Professor - Univ. Pierre et Marie Curie]
Mohab Safey El Din [Assistant Professor - Univ. Pierre et Marie Curie]

PhD Student

Guillaume Moroz [AMN - defense Dec. 9 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]
Ye Liang [China Scholarship Council - defense planned in 2009 - J.-C. Faugère/D. Wang]
Wei Niu [China Scholarship Council - defense planned in 2010 - D. Wang]
Ting Zhao [Chinese Scholarship Council - defense planned in 2010 - F. Rouillier/D. Wang]
Sylvain Lachartre [CIFRE - defense Dec 11 2008 - J.C. Faugèr]
Luk Bettale [DGA - defense planned in 2012 - J.-C. Faugère]

Administrative Assistant

Laurence Bourcier [Secretary (SAR) Inria]

2. Overall Objectives

2.1. Introduction

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.

2.2. Highlights of the year

- After FGb and RS in 2007, our library *DV* has been included in the official distribution of Maple (version 12) software;
- Pierre-Jean Spaenlehauer got the grand prix de stage de recherche de l'école Polytechnique.

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], [1], [71], [70]. 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 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).

3.2. Gröbner basis and triangular sets

Participants: J.C. Faugère, F. Rouillier, M. Safey El Din, D. Wang, 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 ([54], [53]). 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 ([4] - algorithm F_4) a new generation of powerful algorithms ([4]) 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 ([3]) 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 (equivalent system with a structured shape). 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.

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).

Triangular sets have a simplier structure, but, 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.

Lexicographic Gröbner bases	Triangular sets
$\begin{cases} f(X_1) = 0 \\ f_2(X_1, X_2) = 0 \\ \vdots \\ f_{k_2}(X_1, X_2) = 0 \\ f_{k_2+1}(X_1, X_2, X_3) = 0 \\ \vdots \\ f_{k_{n-1}+1}(X_1, ..., X_n) = 0 \\ \vdots \\ f_{k_n}(X_1, ..., X_n) = 0 \end{cases}$	$\begin{cases} t_1(X_1) = 0 \\ t_2(X_1, X_2) = 0 \\ \vdots \\ t_n(X_1, ..., X_n) = 0 \end{cases}$

Triangular sets appear under various names in the field of algebraic systems. In 1932 J.F. Ritt ([80]) 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.

The concept of regular chain introduced in [69] and [96] 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.

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 [1]. 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.

A remarkable and fundamental property in the use we have of the triangular sets is that the ideals induced by 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 [2], [9], [88].

In 1993, Wang [92] proposed a method for decomposing any polynomial system into *fine* triangular systems which have additional properties such as the projection property that may be used for solving parametric systems (see Section 3.4.2).

Triangular sets based techniques are efficient for specific problems like computing Galois ideals [50], 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.

3.3. Zero-dimensional systems

Participants: J.C. Faugère, D. Lazard, F. Rouillier.

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 ([58]) : 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 [58].

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 [72] 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 [7] : 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 [8], [77].

Thus, the use of innovative algorithms for Gröbner bases computations [4], [3], Rational Univariate representations ([58] for the "shape position" case and [7] 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, D. Lazard, G. Moroz, W. Niu, F. Rouillier, M. Safey El Din, D. Wang, R. Xiao, T. Zhao.

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 [56]. 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.

[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.

Since the end of the eighties, alternative strategies (see [66], [67], [68], [51], [52]) 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 [7]);

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

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

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

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

During the last years, we focused on providing efficient algorithms solving the problems (b) and (c). The used method rely on finding a polynomial mapping reaching its extrema on each connected component of the studied variety such that its critical locus is zero-dimensional. For example, in the case of a smooth hypersurface whose real counterpart is compact choosing a projection on a line is sufficient. This method is called in the sequel the critical point method. We started by studying problem (b) [84].

Even if we showed that our solution may solve new classes of problems ([85]), 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 ([86], [81]) and several strategies have been developed [2], [9], [88].

The properness assumption can be dropped by considering the square of a distance function to a generic point instead of a projection function: indeed each connected component contains at least a point minimizing locally this function. Performing a radical and 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 [2] 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 [9] consists in studying recursively the critical locus of projection functions on overlapped affine subspaces containing coordinate axes combined with the study of their set of non-properness. A more efficient one [88], avoiding the study of sets of non-properness is obtained by considering iteratively projections on *generic* affine subspaces restricted to the studied variety and fibers on arbitrary points of these subspaces intersected with the critical locus of the corresponding projection. The underlying algorithm is the most efficient we obtained.

In terms of complexity, we have proved in [89] 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 Bèzout 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.

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 [6] 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.

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). This is the case, for example of the Cylindrical Algebraic Decomposition adapted to $\mathcal{E} \bigcup \mathcal{F}$ [56], of algorithms based on "Comprehensive Gröbner bases" [94], [95], [93] or of methods that compute parameterizations of the solutions (see [90] for example). The consequence is that the output (case distinctions w.r.t. parameters' values) are huge compared with the results we can provide.

3.5. Cryptography

Participants: J.-C. Faugère, L. Perret, G. Renault, L. Bettale.

A fundamental problem in cryptography is to evaluate the security of cryptosystems against the most powerful techniques. To this end, several *general* methods have been proposed: linear cryptanalysis, differential cryptanalysis, *etc ... Algebraic cryptanalysis* is another general method which permits to study the security of the main public-key and secret-key cryptosystems.

Algebraic cryptanalysis can be described as a general framework that permits to asses the security of a wide range of cryptographic schemes. In fact the recent proposal and development of algebraic cryptanalysis is now widely considered as an important breakthrough in the analysis of cryptographic primitives. It is a powerful technique that applies potentially to a large range of cryptosystems. The basic principle of such cryptanalysis is to model a cryptographic primitive by a set of algebraic equations. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the cryptographic primitive (for instance, the secret key of an encryption scheme).

Even if the principle of algebraic attacks can probably be traced back to the work of Shannon, algebraic cryptanalysis has only recently been investigated as a cryptanalytic tool. To summarize algebraic attack is divided into two steps :

1. Modeling, i.e. representing the cryptosystem as a polynomial system of equations
2. Solving, i.e. finding the solutions of the polynomial system constructed in Step 1.

Typically, the first step leads usually to rather "big" algebraic systems (at least several hundreds of variables for modern block ciphers). Thus, solving such systems is always a challenge. To make the computation efficient, we usually have to study the structural properties of the systems (using symmetries for instance). In addition, one also has to verify the consistency of the solutions of the algebraic system with respect to the desired solutions of the natural problem. Of course, all these steps must be constantly checked against the natural problem, which in many cases can guide the researcher to an efficient method for solving the algebraic system.

Multivariate cryptography comprises any cryptographic scheme that uses multivariate polynomial systems. The use of such polynomial systems in cryptography dates back to the mid eighties [78], and was motivated by the need for alternatives to number theoretic-based schemes. Indeed, multivariate systems enjoy low computational requirements and can yield short signatures; moreover, schemes based on the hard problem of solving multivariate equations over a finite field are not concerned with the quantum computer threat, whereas as it is well known that number theoretic-based schemes like RSA, DH, or ECDH are. Multivariate cryptosystems represent a target of choice for algebraic cryptanalysis due to their intrinsic multivariate repesentation.

The most famous multivariate public key scheme is probably the Hidden Field Equation (HFE) cryptosystem proposed by Patarin [79]. 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 [5] (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.

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, it is possible 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.

The same kind of technique has since been used for successfully attacking other types of multivariate cryptosystems : IP [59], 2R [64], ℓ-IC [65], and MinRank [29].

On the one hand algebraic techniques have been successfully applied against a number of multivariate schemes and in stream cipher cryptanalysis. On the other hand, the feasibility of algebraic cryptanalysis remains the source of speculation for block ciphers, and an almost unexplored approach for hash functions. The scientific lock is that the size of the corresponding algebraic systems are so huge (thousands of variables and equations) that nobody is able to predict correctly the complexity of solving such polynomial systems. Hence one goal of the team is ultimately to design and implement a new generation of efficient algebraic cryptanalysis toolkits to be used against block ciphers and hash functions. To achieve this goal, we will investigate *non-conventional* approaches for modeling these problems.

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. Robotic

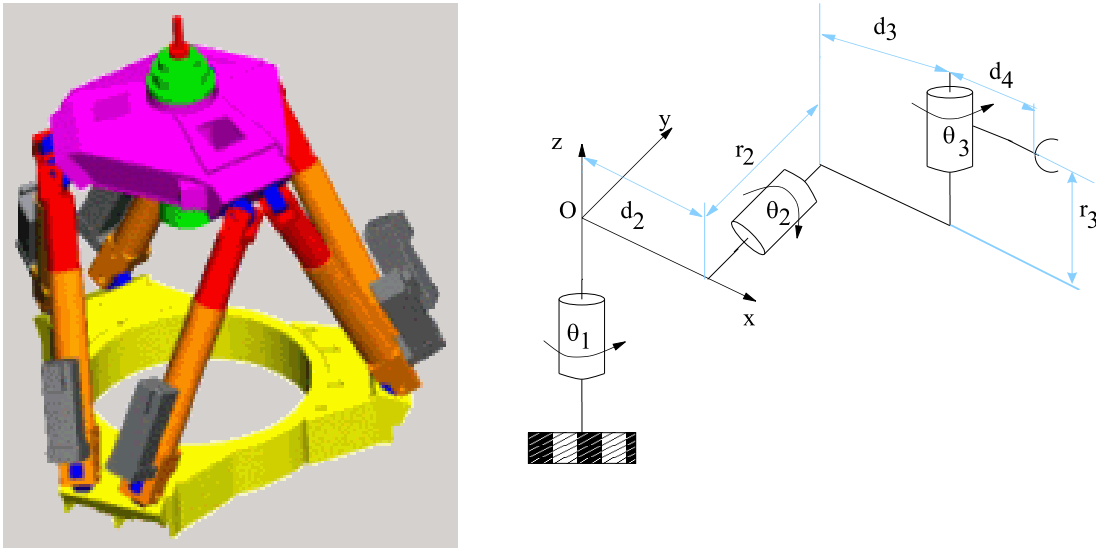

Figure 1. An Hexapod / A serial robot with 3 D.O.F.

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 [74], [73]. 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 [63]. The next efforts were related to the real roots and the effective computation of the solutions [82]. 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.

Since 2002, we are interested in the study of singularities of manipulators (serial or parallel). The first results we obtained (characterization of all the cuspidal serial robots with 3 D.O.F.) have been computed using a very primary variant of the Discriminant Variety [57]. Since 2007, we are working on the singularities of parallel planar robots (ANR grand "SIROPA").

4.3. Signal Processing

Some problems in signal theory are naturally formulated in terms of algebraic systems. In [62], 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 [61]. 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 [83] are partial), and still a few years more to be able to disseminate information towards our community [60]. Our software tools are now used to solve nearby problems [76].

Our activity in signal processing started again through a collaboration with the APICS project-team (collaboration with F. Seyfert) on the synthesis and identification of hyperfrequency filters made of coupled resonant cavities [55].

5. Software

5.1. 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.

5.2. FGb

Participant: J.C. Faugère [contact].

FGb is the most powerful software for computing Gröbner bases currently diffused. Implemented in C/C++ (approximately 250000 lines counting the old *Gb* software), standalone servers are available on demand. Since 2006, FGb is dynamically linked with *Maple* software (version 11 and higher) and is part of the official distribution of this software.

5.3. 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 (150000 lines approximately). RS mainly contains functions for counting and isolating of real zeros of zero-dimensional systems. Since 2006, RS is dynamically linked with *Maple* software (version 11 and higher) and is part of the official distribution of this software.

5.4. 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. More precisely, it computes sampling points of some semi-algebraic systems (including algebraic systems).

5.5. DV

Participants: G. Moroz [contact], F. Rouillier [contact].

DV stands for *Discriminant Varieties* and is a software developped in Maple language, using FGB/RS and RAG as black boxes. It basically contains algorithms for computing Discriminant varieties, but also some variants of cylindrical algebraic decompositions (CAD). Since 2008 it is part of the official Maple distribution (version 12 and higher).

5.6. Epsilon

Participant: D. Wang [contact].

Epsilon is a library of functions implemented in Maple and Java for polynomial elimination and decomposition with (geometric) applications. It has 8 modules and contains more than 70 functions, which allow one to

- triangularize systems of multivariate (differential) polynomials,
- decompose polynomial systems into triangular systems of various kinds (regular, normal, simple, irreducible, or with projection property),
- decompose algebraic varieties into irreducible or unmixed subvarieties,
- decompose polynomial ideals into primary components,
- factorize polynomials over algebraic extension fields,
- solve systems of polynomial equations and inequations, and
- handle and prove geometric theorems automatically.

The entire library with documentation, examples, and Maple worksheets has been distributed by Imperial College Press with a book [91] and its current version is available for download.

6. New Results

6.1. General Solving

In the invited paper [18], a brief and subjective history of *polynomial system solving* is used to define the main challenging problems in the domain. This defines a framework for the future research to which belong most results of the team.

The invited contribution [24] was presented in a special session on optimization in a conference of numerical analysis (NOLTA 08). It describes four applied problems of optimization which were solved earlier by members of SALSA. All together these examples show that the exact methods of solving developed in SALSA may help to solve various optimization problems, and that in some cases they are the only available solution.

Among the general methods for solving, the *Cylindrical Algebraic Decomposition* (CAD) [56] is one on which the team has few publications. Usully these publications consist in proposing alternative methods to solve more efficiently specific problems. This is especially the case of [75]. In [19], we describe a factorization of the iterated discriminant which allow us to optimize, in some cases, the CAD itself.

In [42], 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. Be- side, 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 preliminary implementation shows promising results.

6.2. Parametric Polynomial and Positive Dimensional Systems

Classifying the Perspective-Three-Point problem (abbreviated by P3P in the sequel) consists in determining the number of possible positions of a camera with respect to the apparent position of three points. In the case where the three points form an isosceles triangle, we give a full classification of the P3P. This leads to consider a polynomial system of polynomial equations and inequalities with 4 parameters which is generically zero-dimensional. In the present situation, the parameters represent the apparent position of the three points so that solving the problem means determining all the possible numbers of real solutions with respect to the parameters' values and give a sample point for each of these possible numbers. One way for solving such systems consists first in computing a *discriminant variety*. Then, one has to compute at least one point in each connected component of its real complementary in the parameter's space. The last step consists in specializing the parameters appearing in the initial system by these sample points. Many computational tools may be used for implementing such a general method, starting with the well known Cylindrical Algebraic Decomposition (CAD in short), which provides more information than required. In a first stage, we propose in [30] a full algorithm based on the straightforward use of some sophisticated software such as FGb (Gröbner bases computations) RS (real roots of zero-dimensional systems), DV (Discriminant varieties) and RAGlib (Critical point methods for semi-algebraic systems). We then improve the global algorithm by refining the required computable mathematical objects and related algorithms and finally provide the classification. In particular, we use a new efficient algorithm computing sampling points in a semi-algebraic set defined by inequations and inequalities which is implemented in RAGlib. Three full days of computation were necessary to get this classification which is obtained from more than 40000 points in the parameter's space.

The study of Hass systems ([33]) can be veiwed as another application validating in practice our strategy for solving parametric systems. The Haas family is a set of parametric polynomial equations of degree $2k$. The description of the open cells of the parameters' space where the number of real solutions is constant has only been done up to $k = 3$ until now. We show how to automatically recover such a clas- sification up to $k = 4$ using discriminant varieties. Then, adapting our computations to the special structure of the Haas equations, we classify the real roots of these systems up to $k = 9$.

6.3. Positive Dimensional Systems: Testing sign conditions on a multivariate polynomial

Let $f \in \mathbb{Q}[X_1, ..., X_n]$ be a polynomial of degree D. Computing the set of *generalized critical values* of the mapping $\widetilde{f} : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$ (i.e. $\{c \in \mathbb{C} \mid \exists (x_k)_{k\in\mathbb{N}} \ f(x_k) \to c$ and $||x_k||.||d_{x_k} f|| \to 0$ when $k \to \infty\}$) is an important step in algorithms computing sampling points in semi-algebraic sets defined by a single inequality.

A previous algorithm [87] allows 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. These properties, which are generically satisfied, are difficult to check in practice. Moreover, choosing randomly the plane P induces a growth of the coefficients appearing in the computations.

We provide in [43] 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 $\langle \frac{\partial f}{\partial X_1}, ..., \frac{\partial f}{\partial X_n} \rangle$.

We also provide complexity estimates on the number of arithmetic operations performed by a probabilistic version of our algorithm.

Practical experiments at the end of the paper show the relevance and the importance of these results which improve significantly in practice previous contributions.

6.4. Positive Dimensional Systems: Global algebraic optimization

Let f be a polynomial in $\mathbb{Q}[X_1, ..., X_n]$ of degree D. In [37], we provide an efficient algorithm in practice to compute the global supremum $\sup_{x\in\mathbb{R}^n} f(x)$ of f (or its infimum $\inf_{x\in\mathbb{R}^n} f(x)$). The complexity of our method is bounded by $D^{\mathcal{O}(n)}$. In a probabilistic model, a more precise result yields a complexity bounded by $\mathcal{O}(n^7 D^{4n})$ arithmetic operations in $\mathbb{Q}$. Our implementation is more efficient by several orders of magnitude than previous ones based on quantifier elimination. Sometimes, it can tackle problems that numerical techniques do not reach. Our algorithm is based on the computation of generalized critical values of the mapping $x \to f(x)$, i.e. the set of points $\{c \in \mathbb{C} \mid \exists (x_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^n \ f(x_\ell) \to c, \ \ ||x_\ell||||d_{x_\ell} f|| \to 0$ when $\ell \to \infty\}$. We prove that the global optimum of f lies in its set of generalized critical values and provide an efficient way of deciding which value is the global optimum.

6.5. Splitting Field Computation

Let f be a univariate monic integral polynomial of degree n and let $(\alpha_1, ..., \alpha_n)$ be an n-tuple of its roots in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Obtaining an algebraic representation of the splitting field $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ of f is a question of first importance in effective Galois theory. For instance, it allows us to manipulate symbolically the roots of f. In [36], we propose a new method based on multi-modular strategy. Actually, we provide algorithms for this task which return a triangular set encoding the *splitting ideal* of f. We examine the ability/practicality of the method by experiments on a real computer and study its complexity.

6.6. Computational Geometry

Our collaboration on computational geometry with the VEGAS project (INRIA Nancy) is continuing.

For this year, it has been concretized by the final publication of a series of papers [14], [15], [16] in which is given the first complete classification of the intersections of quadic surfaces together with an algorithm wich decide to which class belongs a given intersection and outputs a quasi-optimal parameterization of the components of this intersection.

In [39] and [35], we revisit the problem of computing the topology and geometry of a real algebraic plane curve. The topology is of prime interest but geometric information, such as the position of singular and critical points, is also relevant. A challenge is to compute efficiently this information for the given coordinate system even if the curve is not in generic position.

Previous methods based on the cylindrical algebraic decomposition (CAD) use subresultant sequences and computations with polynomials with algebraic coefficients.

A novelty of our approach is to replace these tools by Gröbner basis computations and isolation with rational univariate representations. This has the advantage of avoiding computations with polynomials with algebraic coefficients, even in non-generic positions. These choices induce different methods for computing multiplicities in systems and in fibers.

Our algorithms isolate critical points in boxes and computes a decomposition of the plane (which is not a CAD) by rectangular boxes. Such a decomposition also induces a new approach for computing an arrangement of polylines isotopic to the input curve. In [39], the strategy was applied to *ridges* using a known classification of the singularities of such curves, while the general algorithm proposed in [35] is general.

An implementation of our algorithm demonstrates its efficiency, in particular on high-degree non-generic curves.

6.7. Cryptography

In [26], we have investigated the security of the Tractable Rationale Maps Signature (TRMS) signature scheme proposed at PKC'05. To do so, we have presented a hybrid approach for solving the algebraic systems naturally arising when mounting a signature-forgery attack. The basic idea is to compute Gröbner bases of several modified systems rather than a Gröbner basis of the initial system. We have been able to provide a precise bound on the (worst-case) complexity of this approach. For that, we have however assumed a technical condition on the systems arising in our attack; namely the systems are *semi-regular*. This claim is supported by experimental evidences. Finally, it turns out that our approach is efficient. We have obtained a complexity bounded from above by 2^{57} to forge a signature on the parameters proposed by the designers of TRMS . This bound can be improved; assuming an access to 2^{16} processors (which is very reasonable), one can actually forge a signature in approximately 51 hours.

In [31], we have investigated the security of the Unbalanced Oil and Vinegar Scheme. To do so, we have used the hybrid approach described previously for solving the algebraic systems naturally arising when mounting a signature-forgery attack. We have obtained a complexity bounded from above by $2^{40.3}$ (or 9 hours of computation) to forge a signature on a set of parameters proposed by the designers of UOV.

In [27], we have studied the security of a hash function based on the evaluation of multivariate polynomials. The security of such hash function is related to the difficulty of solving (under-defined) systems of algebraic equations. To solve these systems, we have used the hybrid approach mixing exhaustive search and Gröbner bases solving. For the sparse construction, we have refined this strategy. From a practical point of view, we have been able to break several challenges proposed by Ding and Yang in real time.

Trivium is a synchronous stream cipher designed to provide a flexible trade-off between speed and gate count in hardware, and reasonably efficient software implementation. It was designed in 2005 by C. De Cannière and B. Preneel for the European project eSTREAM. It has successfully moved into phase two of the selection process and is currently in the focus group under the hardware category. As of yet there has been no attack on Trivium faster than exhaustive search. Bivium-A and Bivium-B are truncated versions of Trivium that are built on the same design principles. These simplified versions are used for investigating Trivium-like ciphers with a reduced complexity. There have been successful attempts in the cryptanalysis of Bivium ciphers. In [38], we have compared a basic Gröbner basis attack against these ciphers with other known methods. We have presented some experimental results.

In [29], we have investigated the difficulty of one of the most relevant problems in multivariate cryptography – namely MinRank – about which no real progress has been reported since. Our starting point is the Kipnis-Shamir attack. We first show new properties of the ideal generated by Kipnis-Shamir's equations. We then propose a new modeling of the problem. Concerning the practical resolution, we adopt a Gröbner basis approach that permitted us to actually solve challenges A and B proposed by Courtois. Using the multi-homogeneous structure of the algebraic system, we have been able to provide a theoretical complexity bound reflecting the practical behavior of our approach. Namely, when r' the dimension of the matrices minus the rank of the target matrix in the MinRank problem is constant, then we have a polynomial time attack $\mathcal{O}\left(\ln(q)\ n^{3\,r'^2}\right)$. For the challenge C, we obtain a theoretical bound of $2^{66.3}$ operations.

In [17], we present an efficient and general algorithm for decomposing multivariate polynomials of the same arbitrary degree. This problem, also known as the *Functional Decomposition Problem* (FDP), is classical in computer algebra. It is the first general method addressing the decomposition of multivariate polynomials (any degree, any number of polynomials). As a byproduct, our approach can be also used to recover an ideal $\mathcal{I}$ from its k-th power $\mathcal{I}^k$. The complexity of the algorithm depends on the ratio between the number of variables (n) and the number of polynomials (u). For example, polynomials of degree four can be decomposed in $\mathcal{O}(n^{12})$, when this ratio is smaller than $\frac{1}{2}$. This works was initially motivated by a cryptographic application, namely the cryptanalysis of $2R^-$ schemes. From a cryptographic point of view, the new algorithm is so efficient that the principle of two-round schemes, including $2R^-$ schemes, becomes useless. Besides, we believe that our algorithm is of independent interest.

In [23], we present an improved method for decomposing multivariate polynomials. We propose to use high order partial derivatives to improve the algorithm described in [17].

6.8. Error Correcting Codes

In [13], we revisit the concept of decoding binary cyclic codes with Gröbner bases. These ideas were first introduced by Cooper, then Chen, Reed, Helleseth and Truong, and eventually by Orsini and Sala. We discuss here another way of putting the decoding problem into equations: the Newton's identities. Although these identities have been extensively used for decoding, the work was done manually, to provide formulas for the coefficients of the locator polynomial. This was achieved by Reed, Chen, Truong and others in a long series of papers, for decoding quadratic residue codes, on a case-by-case basis. It is tempting to automate these computations, using elimination theory and Gröbner bases.

Thus, we study the properties of the system defined by the Newton's identities, for decoding binary cyclic codes. This is done in two steps, first we prove some facts about the variety associated to this system, then we prove that the ideal itself contains relevant equations for decoding, which lead to formulas.

Then, we consider the so-called online Gröbner bases decoding, where the work of computing a Gröbner basis is done for each received word. It is much more efficient for practical purposes than preprocessing and substituting into the formulas. Finally, we conclude with some computational results, for codes of interesting length (about one hundred).

6.9. Algebraic Biology

In [21], [34], we have shown how to analyze stability, bifurcation, and limit cycles for biological systems by using an algebraic approach based on triangular decomposition, Gröbner bases, discriminant varieties, real solution classification, and quantifier elimination by partial CAD. The analysis of stability, bifurcation, and limit cycles for a concrete two-dimensional system, the self-assembling micelle system with chemical sinks, is presented in detail. It is proved that this system may have a focus of order 3, from which three limit cycles can be constructed by small perturbation. The applicability of our approach is further illustrated by the construction of limit cycles for a two-dimensional Kolmogorov prey-predator system and a three-dimensional Lotka–Volterra system. We have also provided experimental results with comparisons for the stability analysis of 15 biological models taken from the literature.

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.

7.2.2. ANR Grant "SIROPA"

Participants: F. Rouillier [contact], J.-C. Faugère, M. Safey El Din, G. Moroz.

In collaboration with COPRIN project-team (Sophia - Antipolis), IRCcYN and LINA (University / CNRS - Nantes), IRMAR (CNRS/University of Rennes I)

The goal of this projects is to study the singularities of parallel robots from the theoretical aspects (classifications) to the most practical ones (behavior).

7.3. International Actions

7.3.1. INRIA Associate Team "Chinese SALSA"

Chinese 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 of Symbolic Computation: F. Rouillier, J.-C. Faugère (guest editor [45], [44]) and L. Perret (guest editor [44])
- Mathematics in Computer Science: D. Wang, J.C. Faugère and L. Perret (guest editor)
- Editorial board "Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences" Springer : J.-C. Faugère
- Journal of Symbolic Computation (Elsevier): F. Rouillier and D. Wang, Editorial Board Members
- Journal "Mathematics in Computer Science" (Birkhäuser): J.-C. Faugère, Editorial Board Member; D. Wang, Editor-in-Chief and Managing Editor
- Journal "Science in China Series F: Information Sciences" (Science in China Press and Springer): D. Wang, Executive Associate Editor-in-Chief
- Journal "Frontiers of Computer Science in China" (Higher Education Press and Springer): D. Wang, Editorial Board Member
- Book series "Texts and Monographs in Symbolic Computation" (Springer): D. Wang, Editorial Board Member
- Book "Gröbner, Coding, and Cryptography" (RISC Book Series, Springer): L. Perret, Editorial Board Member [48]

8.1.2. Programm Committees

- Inscrypt 2008: J.-C. Faugère, L. Perret
- SCC 2008: D. Wang (PC co-chair) and J.-C. Faugère(PC co-chair) [46], L. Perret
- 6th Asian Workshop on Foundations of Software (Tokyo, Japan, April 6–8, 2009): D. Wang
- 3rd International Workshop on Symbolic-Numeric Computation (Kyoto, Japan, August 3–5, 2009): D. Wang
- 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (Phuket, Thailand, August 6–8, 2008): D. Wang
- 4th International Conference on Algebraic Biology (Research Triangle Park, North Carolina, USA, June 21–23, 2009): D. Wang
- 3rd International Conference on Algebraic Biology (Hagenberg, Austria, July 31 – August 2, 2008): D. Wang
- 9th International Conference on Artificial Intelligence and Symbolic Computation (Birmingham, UK, July 31 – August 2, 2008): D. Wang
- 7th International Workshop on Automated Deduction in Geometry (Shanghai, China, September 22–24, 2008): D. Wang

- Computer Algebra in Scientific Computing 2009: M. Safey El Din

8.1.3. Conferences (organization)

- SCC First International Conference on Symbolic and Cryptography, Beijing: D. Wang, J.-C. Faugère, L .Perret
- Inscrypt 2008: Special track on symbolic computation: J.-C. Faugère, L. Perret

- 1st International Conference on Symbolic Computation and Cryptography (Beijing, China, April 28–30, 2008): J.-C. Faugère and D. Wang, Program Committee Co-chairs
- Second Chinese-SALSA Workshop (Beijing, China, April 25–27, 2008): F. Rouillier, Organization Committee Co-chair; D. Wang, Organization Committee Member
- International Seminar on Symbolic Real Algebra and Trustworthy Computing (Shanghai, China, April 3–5, 2008): D. Wang, Program Co-chair
- MACIS Steering Committee: F. Rouillier, Chair; D. Wang, Member
- Sage Days 10 (Nancy, France, October 2008): L. Perret, Program Co-chair

8.1.4. Invited lectures

- G. Renault gave invited lecture during the *Journées Nationales du Calcul Formel* 2008. Lecture notes are electronically published in [25].
- J.-C. Faugèregave invited lecture [22] during the *Second Workshop on Mathematical Cryptology* in Santander (Spain).
- D. Wang gave invited talk at the *10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing* (Timisoara, Romania, September 26–29, 2008).
- L. Perret gave an invited talk at the *Journées du GDR Informatique Mathématique 2008* (Paris, 24-25 January 2008)
- L. Perret gave an invited talk at the *Rencontres Arithmétique de l'Informatique Mathématique* (Lille, 3–5 June 2008)
- L. Perret gave an invited talk at the *workshop on Cryptography and Computer Algebra* (Pisa, 7-8 November 2008)
- J.-C. Faugère, and L. Perret will give tutorial talks at the *Inscrypt 2008 : Special track on symbolic computation* (Beijing, 14 December 2008)
- G. Renault gave invited talk during the *SAGE Days 10* (Nancy, October 10–15, 2008).
- D. Lazard gave an invited contribution [24] at the 2008 International Symposium on Nonlinear Theory and its Applications (NOLTA 08).
- D. Lazard wrote an invited introductory paper [18] to the special issue of *Journal of Symbolic Computation* devoted to the *International Conference on Polynomial System Solving (ICPSS)*.
- F. Rouillier gave invited lecture at *EuroCG'08* (Nancy March 18Â§20)

8.1.5. Scientific visits and international seminar

- M. Safey El Din was invited 2 weeks by L. Zhi at the KLMM (Key Laboratory of Mechanization and Mathematics) of the Chinese Academy of Sciences in the frame of the Chinese-SALSA project team. He gave a talk about *Real Solving Polynomial Systems of Inequalities and Inequations*.
- M. Safey El Din was invited 1 week by H. Hong (Editor-in-Chief of Journal of Symbolic Computation) at the KIAS (Korean Institute for Advanced Study), South Korea. He gave a talk about *Critical points methods: from Theory to Practice*.
- M. Safey El Din was invited 10 days by E. Schost at the University of Western Ontario, Canada (ORCCA Lab).
- J.C. Faugère gave invited lecture at the State Key Laboratory Of Information Security (SKLOIS), Chinese Academy of Sciences.
- J.C. Faugère and L. Perret gave invited lectures Institute of Software, Chinese Academy of Sciences
- Prof. Dr. Alexander May (Horst Görtz Institute, Ruhr-University Bochum) was invited by the SALSA project team during one week (September).

- Prof. Dongdai Lin (Institute of Software,Chines Academy of Science, China) was invited by the SALSA project team during one month (mid October – mid November).
- Dr. Frederik Armknecht (Horst Görtz Institute, Ruhr-University Bochum) was invited by the SALSA project team during one week (December).

8.2. Teaching

- Cours 2-13 du MPRI, “Codes correcteurs d’erreurs, calcul formel: applications à la cryptologie” J.C. Faugère, L. Perret
- Cours M2 UPMC spécialité STL “Solutions réelles des systèmes polynomiaux” F. Rouillier, M. Safey El Din

Moreover, J.-C. Faugère and M. Safey El Din wrote a course [40] which is an introduction to polynomial system solving.

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

[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.

[10] D. WANG. *Elimination Methods*, Springer-Verlag, Wien New York, 2001.

Year Publications

Doctoral Dissertations and Habilitation Theses

[11] S. LACHARTRE. *Algèbre linéaire dans la résolution de systèmes polynomiaux Applications en cryptologie*, Ph. D. Thesis, Université Paris 6, 2008.

[12] G. MOROZ. *Sur la décomposition réelle et algébrique des systèmes dépendant de paramètres*, Ph. D. Thesis, Université Paris 6, 2008.

Articles in International Peer-Reviewed Journal

[13] D. AUGOT, M. BARDET, J.-C. FAUGÈRE. *On the decoding of cyclic codes with the Newton's identities*, in "Journal of Symbolic Computation", to appear.

[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", vol. 43, n^{o} 3, 2008.

[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", vol. 43, n^{o} 3, 2008.

[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", vol. 43, n^{o} 3, 2008.

[17] J.-C. FAUGÈRE, L. PERRET. *An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography*, in "Journal of Symbolic Computation", to appear.

[18] D. LAZARD. *Thirty years of Polynomial System Solving, and now ?*, in "Journal of Symbolic Computation", to appear, In Press, corrected proof, available online 25 September 2008.

[19] D. LAZARD, S. MCCALLUM. *Iterated Discriminants*, in "Journal of Symbolic Computation", to appear, (Accepted on Feb. 22, 2008).

[20] K. M., R. G., Y. K.. *Quintic polynomials of Hashimoto-Tsunogai, Brumer, and Kummer*, in "International Journal of Number Theory", to appear, (Accepted Dec 18 2007).

[21] W. NIU, D. WANG. *Algebraic Approaches to Stability Analysis of Biological Systems*, in "Mathematics in Computer Science", vol. 1, n^{o} 3, 2008, p. 507–539.

Invited Conferences

[22] J.-C. FAUGÈRE. *On the complexity of the Minrank problem*, in "Second Workshop on Mathematical Cryptology, Santander, Spain", October 2008, p. 15–19.

[23] J.-C. FAUGÈRE, L. PERRET. *High order derivatives and decomposition of multivariate polynomials*, in "Second Workshop on Mathematical Cryptology, Santander (Spain)", October 2008, p. 15–19.

[24] D. LAZARD. *Can Exact Computation Help Optimization ?*, in "Proceedings of the 2008 International Symposium on Nonlinear Theory and its Applications (NOLTA 08)", T. UETA (editor), IEICE Japan, September 2008, p. 672-675.

[25] G. RENAULT. *Introduction à la Théorie de Galois Effective*, in "JNCF'08: Journées Nationales du Calcul Formel (online)", oct 2008, p. 141 – 197.

International Peer-Reviewed Conference/Proceedings

[26] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Cryptanalysis of the TRMS Cryptosystem of PKC'05*, in "AfricaCrypt 2008, Casablanca, Morocco", S. VAUDENAY (editor), Lecture Notes in Computer Science, to appear, vol. 5023, Springer, p. 143–155.

[27] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Security Analysis of Multivariate Polynomials for Hashing*, in "Information Security and Cryptology - Inscrypt 2008, Beijing, China", M. YUNG, D. LIN, P. LIU (editors), Lecture Notes in Computer Science, to appear, Springer.

[28] X. CHEN, Y. HUANG, D. WANG. *On the Design and Implementation of a Geometric Knowledge Base*, in "Proceedings of ADG 2008 - Seventh International Workshop on Automated Deduction in Geometry, Shanghai, China, September 22-24, 2008", M. KAUERS, M. WU, Z. ZENG (editors), Chinese version in Journal of Computer Applications, East China Normal University, China, 2008, p. 62–78.

[29] J.-C. FAUGÈRE, F. LEVY-DIT-VEHEL, L. PERRET. *Cryptanalysis of Minrank*, in "Advances in Cryptology CRYPTO 2008, Santa-Barbara, USA", D. WAGNER (editor), Lecture Notes in Computer Science, vol. 5157, Springer-Verlag, 2008, p. 280–296.

[30] J.-C. FAUGÈRE, G. MOROZ, F. ROUILLIER, M. SAFEY EL DIN. *Classification of the Perspective-Three-Point problem, discriminant variety and real solving polynomial systems of inequalities*, in "ISSAC '08: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation, New York, NY, USA", D. JEFFREY (editor), ACM, 2008, p. 79–86.

[31] J.-C. FAUGÈRE, L. PERRET. *On the Security of UOV*, in "First International Conference on Symbolic Computation and Cryptography, SCC 08, Beijing, China", LMIB, April 2008, p. 103–109.

[32] 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, vol. 4939, Springer, 2008, p. 1–17.

[33] G. MOROZ, F. ROUILLIER. *Explicit classification of the 9 first Haas parametric systems*, in "ADG'08: Proceedings of the 2008 conference on Automated Deduction in Geometry", T. STURM (editor), 2008.

[34] W. NIU, D. WANG. *Algebraic Analysis of Bifurcation and Limit Cycles for Biological Systems*, in "Proceedings of the Third International Conference on Algebraic Biology (AB 2008), Hagenberg, Austria, July 31 - August 2, 2008", Lecture Notes in Computer Science, vol. 5147, Springer-Verlag, Berlin Heidelberg, July/August 2008, p. 156–171.

[35] M. POUGET, S. LAZARD, F. ROUILLIER, E. TSIGARIDAS, L. PENARANDAS. *On the Topology of Planar Algebraic Curves*, in "European Workshop on Computational Geometry", 2008.

[36] G. RENAULT, K. YOKOYAMA. *Multi-modular Algorithm for Computing the Splitting Field of a Polynomial*, in "ISSAC'08: Proceedings of the 2008 international symposium on Symbolic and algebraic computation", D. JEFFREY (editor), ACM, 2008.

[37] M. SAFEY EL DIN. *Computing the global optimum of a multivariate polynomial over the reals*, in "ISSAC '08: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation, New York, NY, USA", D. JEFFREY (editor), ACM, 2008, p. 71–78.

[38] I. SIMONETTI, J.-C. FAUGÈRE, L. PERRET. *Algebraic Attack Against Trivium*, in "First International Conference on Symbolic Computation and Cryptography, SCC 08, Beijing, China", LMIB, April 2008, p. 95–102.

Scientific Books (or Scientific Book chapters)

[39] F. CAZALS, J.-C. FAUGÈRE, M. POUGET, F. ROUILLIER. *8*, in "Ridges and Umbilics of Polynomial Parametric Surfaces", isbn: 978-3-540-72184-0, vol. 8, n^{o} 232, Springer, 2008, p. 141–160.

[40] J.-C. FAUGÈRE, M. SAFEY EL DIN. *De l'algèbre linéaire à la résolution des systèmes polynomiaux*, in "Mathématiques Appliquées (L3)", to appear, Pearson.

[41] F. LEVY-DIT-VEHEL, M. G. MARINARI, L. PERRET, C. TRAVERSO. *A Survey on Polly Cracker Systems*, in "Bases, Coding, and Cryptography", to appear, Springer.

[42] G. MOROZ. *Regular Decompositions*, Springer-Verlag, Berlin, Heidelberg, 2008, p. 263–277.

[43] M. SAFEY EL DIN. *Practical and Theoretical Issues for the Computation of Generalized Critical Values of a Polynomial Mapping*, Springer-Verlag, Berlin, Heidelberg, 2008, p. 42–56.

Books or Proceedings Editing

[44] D. AUGOT, J.-C. FAUGÈRE, L. PERRET (editors). *Gröbner Bases Techniques in Coding Theory and Cryptography*, to appear, 160 pages, in press, Elsevier.

[45] J.-C. FAUGÈRE, F. R. (editors). *Polynomial system solving*, to appear, 140 pages, in press, Elsevier.

[46] J.-C. FAUGÈRE, D. WANG (editors). *Proceedings of the First International Conference on Symbolic Computation and Cryptography (SCC 2008), Beijing, China, April 28–30, 2008*, 240 pages, Beihang University, China, 2008.

[47] T. IDA, Q. JIANG, D. WANG (editors). *Foundations of Software - Special focus of Frontiers of Computer Science in China*, Higher Education Press, Beijing and Springer, Berlin, 2008.

[48] M. SALA, T. MORA, L. PERRET, S. SAKATA, C. TRAVERSO (editors). *Bases, Coding, and Cryptography*, to appear, Springer.

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, 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.

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

[52] 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.

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

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

[55] 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.

[56] G.-E. 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.

[57] S. CORVEZ, F. ROUILLIER. *Using computer algebra tools to classify serial manipulators*, in "Automated Deduction in Geometry", Lecture Notes in Artificial Intelligence, vol. 2930, Springer, 2003, p. 31–43.

[58] J.-C. 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.

[59] 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.

[60] 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.

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

[62] 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.

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

[64] 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.

[65] 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, vol. 4939, Springer, 2008, p. 1–17.

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

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

[68] 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° 5, 1993, p. 427-431.

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

[70] 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.

[71] 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.

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

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

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

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

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

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

[78] T. MATSUMOTO, H. H. IMAI. *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption*, in "Advances in Cryptology: EUROCRYPT 1988", Lecture Notes in Computer Science, vol. 330, Springer-Verlag, 1988, p. 497–506.

[79] J. PATARIN. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms*, in "Advances in Cryptology: EUROCRYPT 1996", Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, p. 33-48.

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

[81] 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.

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

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

[84] F. ROUILLIER, M.-F. 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.

[85] F. ROUILLIER, M. SAFEY EL DIN, E. 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.

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

[87] M. SAFEY EL DIN. *Testing Sign Conditions on a Multivariate Polynomial and Applications*, in "Mathematics in Computer Science", vol. 1, n^{o} 1, December 2007, p. 177-207.

[88] 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.

[89] 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.

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

[91] D. WANG. *Elimination Practice: Software Tools and Applications*, Imperial College Press, London, 2004.

[92] D. WANG. *An Elimination Method for Polynomial Systems*, in "Journal of Symbolic Computation", vol. 16, 1993, p. 83–114.

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

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

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

[96] 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.