INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Team salsa

Solvers for ALgebraic Systems and Applications

Paris - Rocquencourt

Theme : Algorithms, Certification, and Cryptography

Activity Report

2009

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

Pierre-Vincent Koseleff [On leave from Univ. Pierre et Marie Curie]
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 [On leave from Univ. Pierre et Marie Curie]

PhD Student

Guillaume Moroz [AMN - defense Dec. 9 2008 - F. Rouillier]
Sajjad Rahmany [SPHERE grant - defense Jul. 2009 - J.C. - Faugère]
Rong Xiao [Ambassade de France en Chine - defense in 2010 - F. Rouillier/X. Bican]
Ye Liang [China Scholarship Council - defense in 2010 - J.-C. Faugère/D. Wang]
Wei Niu [China Scholarship Council - defense in 2010 - D. Wang]
Ting Zhao [Chinese Scholarship Council - defense in 2010 - F. Rouillier/D. Wang]
Chenqi Mou [China Scholarship Council - defense in 2012 - J.-C. Faugère/D. Wang]
Sylvain Lachartre [CIFRE - defense Dec 11 2008 - J.C. Faugère]
Luk Bettale [DGA - defense in 2012 - J.-C. Faugère/L. Perret]
Pierre-Jean Spaenlehauer [AMX - defense in 2013 - J.-C. Faugère/M. Safey El Din]
Christopher Goyet [CIFRE - defense in 2013 - J.-C. Faugère/G. Renault]

Post-Doctoral Fellow

Matte Soos [INRIA Rhone Alpes]

Visiting Scientist

Rune Ødegård [visiting PhD student]

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

- **Cryptography**. *ECRYPT II* : European Network of Excellence for Cryptology II. (SALSA joint the network in 2009); ANR Grant *CAC* : Computer Algebra and Cryptography. (started in october 2009 for 4 years).
- **Computational Geometry**: SALSA software as the first algebraic kernel of *CGAL* (version 3.6 - June 2010)
- **Chinese-SALSA** : *Chinese-SALSA* became a em *LIAMA* team in 2009. ANR Grant *EXACTA* : the project will start in January 2010.
- **Maple**. Maple 13 release : inclusion of the DV package (parametric systems) from SALSA Software.

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 [1], [76], [75]. Sorting the most frequently asked questions appearing in the applications, one distinguishes several classes of problems which are different either by their mathematical structure or by the significance that one can give to the word "solving".

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

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

The first solution is limited in terms of performances (maximum 3 or 4 variables) because of a recursive treatment variable by variable, the second also because of the use of a sophisticated arithmetic (formal infinitesimals).

- quantified formulas; deciding efficiently if a first order formula is valid or not is certainly one of the greatest challenges in "effective" real algebraic geometry. However this problem is relatively well encircled since it can always be rewritten as the conjunction of (supposed to be) simpler problems like the computation of a point per connected component of a semi-algebraic set.

As explained in some parts of this document, the iniquity of the studied mathematical objects does not imply the uncut of the related algorithms. The 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, G. Renault, F. Rouillier, M. Safey El Din, P.J. Spaenlehauer, 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 $\mathcal{I}=\langle P_1,...,P_s\rangle$ generated by $P_1,...,P_s$ is the set of polynomials in $K[X_1,...,X_n]$ constituted by all the combinations $\sum_{k=1}^{R} P_kU_k$ with $U_k\in\mathbb{Q}[X_1,...,X_n]$. Since every element of $\mathcal{I}$ vanishes at each zero of S, we denote by $V_C(S)=V_C(I)=\{x\in C^n \mid p(x)=0\ \forall p\in\mathcal{I}\}$ (resp. $V_R(S)=V_R(I)=V_{\mathbb{C}}(I)\bigcap\mathbb{R}^n$), the set of complex (resp. real) zeros of S, where R is a real closed field containing K and C its algebraic closure.

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

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

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

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

Gröbner bases are computable objects. The most popular method for computing them is Buchberger's algorithm ([60], [59]). 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.

Triangular sets appear under various names in the field of algebraic systems. J.F. Ritt ([83]) introduced them as characteristic sets for prime ideals in differential algebra. His constructive algebraic tools were adapted by W.T. Wu in the late seventies for geometric applications. The concept of regular chain (see [74] and [96]) is adapted for recursive computations in a univariate way.

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

It 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, 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: L. Bettale, J.C. Faugère, D. Lazard, F. Rouillier, P.J. Spaenlehauer.

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

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

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

The use of this vector-space structure is well known and at the origin of the one of the most known algorithms of the field ([64]) : it allows to deduce, starting from a Gröbner basis for any ordering, a Gröbner base for any other ordering (in practice, a lexicographic basis, which are very difficult to compute directly). It is also common to certain semi-numerical methods since it allows to obtain quite simply (by a computation of eigenvalues for example) the numerical approximation of the solutions (this type of algorithms is developed, for example, in the INRIA Galaad project).

Contrary to what is written in a certain literature, the computation of Gröbner bases is not "doubly exponential" for all the classes of problems. In the case of the zero-dimensional systems, it is even shown that it is simply exponential in the number of variables, for a degree ordering and for the systems without zeros at infinity. Thus, an effective strategy consists in computing a Gröbner basis for a favorable ordering and then to deduce, by linear algebra technics, a Gröbner base for a lexicographic ordering [64].

The case of the zero-dimensional systems is also specific for triangular sets. Indeed, in this particular case, we have designed algorithms that allow to compute them efficiently [77] 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 proved 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 isolating and counting the real roots of univariate polynomials [8].

Thus, the use of innovative algorithms for Gröbner bases computations [4], [3], Rational Univariate representations ([64] 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.

[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.

We focus on 2 main problems:
1. computing one point on each connected components of a semi-algebraic set;
2. 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 [62]. With slight modifications, this algorithm also solves the problem of Quantifier Elimination. It is based on the recursive elimination of variables one after an other ensuring nice properties between the components of the studied semi-algebraic set and the components of semi-algebraic sets defined by polynomial families obtained by the elimination of variables. It is doubly exponential in the number of variables and its best implementations are limited to problems in 3 or 4 variables. Since the end of the eighties, alternative strategies (see [73], [58] and references therein) 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) [86]. Even if we showed that our solution may solve new classes of problems ([87]), 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 and several strategies have been developed [2], [9].
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, $U = [U_1, ...U_d]$ 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 $\mathcal{E} \bigcup \mathcal{F}$ [62], 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).

Although 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 [81], 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 [82]. 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. This permits to 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 [66], 2R [71], ℓ-IC [72], and MinRank [65].

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

h

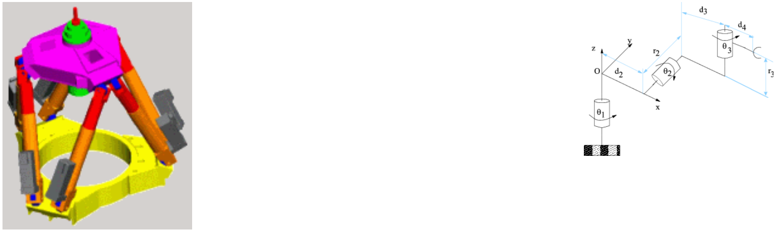

Figure 1.

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 [79], [78]. 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 [70]. The next efforts were related to the real roots and the effective computation of the solutions [84]. 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 [63]. 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 [69], we had studied the Kovacevic-Vetterli 's family of filters banks. To be used for image compression, a wavelet transformation must be defined by a function having a maximum of partial derivative that vanishes at the corners of the image. These conditions can be translated to polynomial systems that can be solved with our methods. We showed that to get physically acceptable solutions, it was necessary to choose the number of conditions so that the solutions' space is of dimension 0, 2 or 4 (according to the size of the filter). This result (parametric family of filters) is subject to a patent [68]. To exploit these filters in practice, it remains to choose the best transformation, according to non-algebraic criteria, which is easily done with traditional tools for optimization (with a reduced number of variables).

As for most of applications on which we work, it took more than three years to obtain concrete results bringing real practical progress (the results mentioned in [85] are partial), and still a few years more to be able to disseminate information towards our community [67]. Our software tools are now used to solve nearby problems [80]. 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 [61].

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].

RAGLib is a Maple library for computing sampling points in semi-algebraic sets.

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. Solving systems with symmetries

In [11], [34], we propose an efficient method to solve polynomial systems whose equations are invariant by the action of a finite group G. The idea is to simultaneously compute a truncated SAGBI-Gröbner bases (a generalisation of Gröbner bases to ideals of subalgebras of polynomial ring) and a Gröbner basis in the invariant ring $\mathbb{K}[\sigma_1, ..., \sigma_n]$ where σ_i is the i-th elementary symmetric polynomial. To this end we provide two algorithms: first, from the F_5 algorithm we can derive an efficient and easy to implement algorithm for computing truncated SAGBI–Gröbner bases of the ideals in invariant rings. A first implementation in C has been to estimate the practical efficiency: for instance it takes 1m30 to compute a SAGBI basis of Cyclic 9 modulo p. The second algorithm is inspired by the FGLM algorithm: from a truncated SAGBI–Gröbner basis of a zero-dimensional ideal we can compute efficiently a Gröbner basis in some invariant rings $\mathbb{K}[h_1, ..., h_n]$. Finally, we show how this algorithms can be used for solving algebraic systems which are invariant by the action of some finite groups.

6.2. Parametric Polynomial Systems

In [43], we study some tools to decompose polynomial systems depending on parameters in order to optimize the computation of so called discriminant varieties. We focus on the use of triangular representations of systems which theoretically make possible to split the systems into subsystems with good properties (radical, equidimensional, as many equations as unknowns, etc.) with the drawback of representing constructible sets instead of algebraic varieties. Our study is driven by two main objectives:

- to measure the difference between the remarkable objects induced by triangular structures such as initials and separants (defining straightforwardly a large discriminant variety) with the mathematical intrinsic object (the minimal discriminant variety) related to the problem. In other words, measure the difference between what is computed and what is theoretically required.
- to propose optimizations to speed up the resolution of such systems by means of discriminant varieties, using triangular decompositions.

6.3. Positive dimensional polynomial systems solving

We have developed in the past several algorithms with intrinsic complexity bounds for the problem of point finding in real algebraic varieties. In [13], we give a comprehensive presentation of the geometrical tools which are necessary to prove the correctness and complexity estimates of these algorithms. Our results form also the geometrical main ingredients for the computational treatment of singular hypersurfaces. In particular, we show the non–emptiness of suitable generic dual polar varieties of (possibly singular) real varieties, show that generic polar varieties may become singular at smooth points of the original variety and exhibit a sufficient criterion when this is not the case. Further, we introduce the new concept of meagerly generic polar varieties and give a degree estimate for them in terms of the degrees of generic polar varieties. The statements are illustrated by examples and a computer experiment.

Let $(f_1, ..., f_s) \subset \mathbb{Q}[X_1, ..., X_n]$ and $D \geq \deg(f_i)$. In [30], we consider the problem of deciding the emptiness of the semi-algebraic set defined by $f_i \, \sigma_i \, 0 \;, 1 \leq i \leq s$ with $\sigma_i \in \{>, <, \neq\}$ and/or computing sampling points in the semi-algebraic set under consideration. We present an algorithm solving these problems. It uses algebraic computations of critical points and *asymptotic* critical values. We first show that its complexity is in the state of the art (i.e. $s^{n+1}D^{O(n)}$). We find that its implementation can tackle important and challenging problems arising in different areas (biology, robotics, theorem proving) which are out of reach of previous algorithms/implementations.

In [51], we consider the problem of constructing roadmaps of real algebraic sets. This problem was introduced by Canny to answer connectivity questions and solve motion planning problems. Given s polynomial equations with rational coefficients, of degree D in n variables, Canny's algorithm has a Monte Carlo cost of $s^n \log(s) D^{O(n^2)}$ operations in $\mathbb{Q}$; a deterministic version runs in time $s^n \log(s) D^{O(n^4)}$. A subsequent improvement was due to Basu, Pollack and Roy, with an algorithm of deterministic cost $s^{d+1}D^{O(n^2)}$ for the more general problem of computing roadmaps of a semi-algebraic set ($d \leq n$ is the dimension of an associated object). We first prove a new connectivity result in compact real algebraic sets with a finite number of singular points. We give a probabilistic algorithm of complexity $(nD)^{O(n^{1.5})}$ for the problem of computing a roadmap of a closed and bounded hypersurface V of degree D in n variables, with a finite number of singular points. The computed roadmap has degree $(nD)^{O(n^{1.5})}$. Even under these extra assumptions, no previous algorithm featured a cost better than $D^{O(n^2)}$. A deterministic algorithm outputting a roadmap of degree bounded by $(nD)^{O(n^{1.5})}$ can be derived from this work.

In [52], we provide an algorithm deciding if a convex semi-algebraic set contains points with rational coordinates and and give complexity estimates on his running time and the height of the outputted point in case of non-emptiness. We use these results to give some bounds on the height of the rationals in a sums-of-squares decomposition of a multivariate polynomial. More precisely, let $\mathcal{P} = \{h_1, ..., h_s\} \subset \mathbb{Z}[Y_1, ..., Y_k]$, $D \geq \deg(h_i)$ for $1 \leq i \leq s$, σ bounding the bit length of the coefficients of the h_i's, and Φ be a quantifier-free $\mathcal{P}$-formula defining a convex semi-algebraic set. We design an algorithm returning a rational point in

$\mathcal{S}$ if and only if $\mathcal{S} \cap \mathbb{Q} \neq \varnothing$. It requires $\sigma^{O(1)}D^{O(k^3)}$ bit operations. If a rational point is outputted its coordinates have bit length dominated by $\sigma D^{O(k^3)}$. Using this result, we obtain a procedure deciding if a polynomial $f \in \mathbb{Z}[X_1, ..., X_n]$ is a sum of squares of polynomials in $\mathbb{Q}[X_1, ..., X_n]$. Denote by d the degree of f, τ the maximum bit length of the coefficients in f, $D = \binom{n+d}{n}$ and $k \leq D(D+1) - \binom{n+2d}{n}$. This procedure requires $\tau^{O(1)}D^{O(k^3)}$ bit operations and the coefficients of the outputted polynomials have bit length dominated by $\tau D^{O(k^3)}$.

6.4. Quantifier Elimination/Cylindrical Algebraic Decomposition

Cylindrical Algebraic Decomposition (CAD) is is a well known tool for quantifier elimination. It is also an important tool for computing the topology of a semi-algebraic set. In [23] we have shown that the discriminant of a discriminant has a natural factorization which allows to improve the projection step of this algorithm. In [55] we show that the output of CAD algorithm may may be not sufficient to compute the topology of a surface, and we describe a simple modification of this algorithm which is topologically convenient.

In [36], we study a variant of the real quantifier elimination problem (QE):

$$\exists \mathbf{Y} \in \mathbb{R}^n \; f_1(\mathbf{Y}) = \cdots = f_k(\mathbf{Y}) = 0, g(\mathbf{X}, \mathbf{Y}) > 0.$$

The variant problem requires the input to satisfy certain extra conditions ($\langle f_1, ..., f_k \rangle$ is radical and defines a smooth equidimensional variety of co-dimension k whose set of real points is compact in the $\mathbf{Y}$-space), and allows the ouput to be almost equivalent to the input. In a sense, we are strengthening the pre-condition and weakening the post-condition of the standard QE problem.

The motivation/rationale for studying such a variant QE problem is that many quantified formulas arising in applications do satisfy the extra conditions. We focus in particular on quantified formulas arising from the stability analysis of numerical schemes for PDE's or initial-boundary value problems. Furthermore, in most of these applications, it is sufficient that the ouput formula is almost equivalent to the input formula. Thus, we propose to solve a variant of the initial quantifier elimination problem.

We present an algorithm (VQE) , that exploits the strengthened pre-condition and the weakened post-condition. The main idea underlying the algorithm is to substitute the repeated projection step of CAD by a single projection without carrying out a parametric existential decision over the reals.

We find that the algorithm VQE can tackle important and challenging problems, such as numerical stability analysis of the widely-used MacCormack's scheme. The problem has been practically out of reach for standard QE algorithms in spite of many attempts to tackle it. However the current implementation of VQE can solve it in about 1 day.

In [35], this algorithm is generalized to input formulas

$$\exists \mathbf{Y} \in \mathbb{R}^n \; f_1(\mathbf{X}, \mathbf{Y}) = \cdots = f_k(\mathbf{X}, \mathbf{Y}) = 0, g_1(\mathbf{X}, \mathbf{Y}) > 0, ..., g_s(\mathbf{X}, \mathbf{Y}) > 0$$

such that the projection $(\mathbf{x}, \mathbf{y}) \rightarrow \mathbf{x}$ restricted to the real variety defined by $f_1, ..., f_k$ is proper and $\langle f_1, ..., f_k \rangle$ is radical and defines a smooth equidimensional algebraic variety of co-dimension $p \leq k$.

6.5. Computational Geometry

In [17], we give a complete description of the Voronoi diagram, in $\mathbb{R}^3$, of three lines in general position, that is, that are pairwise skew and not all parallel to a common plane. In particular, we show that the topology of the Voronoi diagram is invariant for three such lines. The description is complete as it contains algorithms for answering the usual queries on the output, like deciding to which cell belong a given point of sorting points on a curve.

The proof technique is of interest in its own right not only because it requires state of the art tools of computer algebra, but also because it has led to improve three such tools (finding a point on every connected component of a semi-algebraic set (RAGLIB), decomposing a polynomial into a sum of squares and primary decomposition of the radical of an ideal).

This proof has been presented in [29], [56] as a rare example of a proof of a new theorem in geometry which requires machine computation.

In [32] the results of [17] have been extended to the case of three arbitrary lines.

In [39], we show that the usal representation of a point as a vector of coordinates does not works easily for algebraic point which are obtained as intersection of curves and surfaces. On the other hand, the representation of a point as the unique solution of a system of algebraic equations and inequalities allows to implement robustly and efficiently all the basic operations on points. The efficiency of this approach is shown on a classical challenge of quantifier elimination (see also [55]).

In [42], 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 use sub-resultant 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. Our algorithm isolates critical points in boxes and computes a decomposition of the plane by rectangular boxes. This decomposition also induces a new approach for computing an arrangement of polylines isotopic to the input curve. We also present an analysis of the complexity of our algorithm. An implementation of our algorithm demonstrates its efficiency, in particular on high-degree non-generic curves.

6.6. Functional Decomposition Problem

In [18], we present an improved method for decomposing multivariate polynomials. This problem, also known as the *Functional Decomposition Problem* (FDP), is classical in computer algebra.

Functional Decomposition Problem (FDP):. Given a set of u polynomials $h = (h_1, \cdots, h_u)$ over a polynomial ring $\mathbb{K}[x_1, \cdots, x_n]$ ($\mathbb{K}$ denoting an arbitrary field) our algorithm permits to recover – if any – $f = (f_1, \cdots, f_u) \in \mathbb{K}[x_1, \cdots, x_n]^u$ and $g = (g_1, \cdots, g_n) \in \mathbb{K}[x_1, \cdots, x_n]^n$ whose composition equals to h, i.e. $h = (h_1, \cdots, h_u) = (f_1(g_1, \cdots, g_n), \cdots, f_u(g_1, \cdots, g_n))$. This 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 method relies on the computation of the column ideal of the ideal generated by the partial derivatives of the polynomials obtained from the composition. This computation can be done efficiently using Gröbner bases. The complexity of the algorithm depends on the ratio between the number of variables and the number of polynomials; for example, polynomials of degree four can be decomposed in $\mathcal{O}(n^{12})$ when this ratio is less that $\frac{1}{2}$.

More recently in [33], we propose to use high order partial derivatives to improve the previous algorithm. Our new approach is more simple, and in some sense more natural. From a practical point of view, this new approach will lead to more efficient algorithms. The complexity of our algorithms will depend of the degree of the input polynomials, and the ratio n/u between the number of variables/polynomials.

6.7. Algebraic Cryptanalysis

In [14], [31], we present an improved approach to solve multivariate systems over finite fields. Our approach is a tradeoff between exhaustive search and Gröbner bases techniques. We give theoretical evidences that our method brings a significant improvement in a very large context and we clearly define its limitations. The efficiency depends on the choice of the tradeoff. Our analysis gives an explicit way to choose the best tradeoff as well as an approximation. From our analysis, we present a new general algorithm to solve multivariate polynomial systems. Our theoretical results are experimentally supported by successful cryptanalysis of several multivariate schemes (TRMS, UOV, MPH ...). As a proof of concept, we were able to break the proposed parameters assumed to be secure until now. Parameters that resists to our method are also explicitly given. Our work permits to refine the parameters to be chosen for multivariate schemes.

Algebraic cryptanalysis is as a general framework that permits to assess the security of a wide range of cryptographic schemes. However, the feasibility of algebraic cryptanalysis against block ciphers remains the source of speculation and especially in targeting modern block ciphers. The main problem is that the size of the corresponding algebraic system is so huge (thousand of variables and equations) that nobody is able to predict correctly the complexity of solving such polynomial systems. To make algebraic attacks efficient it seems clear that new ideas are required. One possible room for improvement is related to the modeling. A new trend in this area is to combine statistical and algebraic attacks. In [28], we present an attack against round-reduced version on DES mixing algebraic and differential techniques. The use of differential permits to ease the solving step; whilst algebraic techniques allows to decrease the numbers of pairs required for a classical differential cryptanalysis. In particular, we have reduced the minimum numbers of pairs required for 6, 7 and 8 rounds of DES. On the other hand, the cost of the attack is higher than a standard usual differential cryptanalysis (but remaining at a reasonable level). For instance, for 6 rounds of DES we have reduced the number of pairs to 32 and the cost is 3000 seconds (to be compared with 240 pairs for the original attack of Biham and Shamir).

In [16], we present an algebraic attack on NTRU (restricted to case where the parameter q is a power of two) using the method of the Witt vectors proposed by Silverman, Smart and Vercauteren the latter considered only the first two bits of a Witt vector attached to the recovering of the secret key in order to reduce the problem to the resolution of an algebraic system over $\mathbb{F}_2$. The theoretical complexity of this resolution was not studied by the authors. In this paper, we use the first three bits of the Witt vectors to obtain supplementary equations which allow us to reduce the complexity of the attack. Using Gröbner basis complexity results of overdetermined systems, we have been able to provide a theoretical complexity analysis. Additionally we provide experimental results illustrating the efficiency of this approach. Moreover, we prove that the use of the fourth bit does not improve the complexity, what is surprising. Unfortunately, for standard values of the NTRU parameters, the proven complexity is around 2^{246} and this attack does not make it possible to find the private key.

6.8. Number Theory

In [41], we present new results about the computation of a general shape of a triangular basis generating the splitting ideal of an irreducible polynomial given with the permutation representation of its Galois group G. We provide some theoretical results and a new general algorithm based on the study of the non redundant bases of permutation groups. These new results deeply increase the efficiency of the computation of the splitting field of a polynomial. More precisely, during the conference ANTS'7 in 2006 new algorithms were proposed by Renault and Yokoyama for computing the splitting field of a monic irreducible polynomial f with coefficient in $\mathbb{Q}$ (more generally, these methods can be applied in any global fields). These new algorithms are based on the relationship between the representation of the splitting field by a Gröbner basis and the action of the corresponding Galois group on this basis. The core of this new approach, called *computation scheme*, uses the internal symmetries of the problem in order to speed up the Gröbner basis computation. This scheme is computed from the knowledge of a permutation representation of the Galois group G of f and provides a shape of the Gröbner basis of the splitting ideal of f. From this shape, these algorithms effectively compute the basis by interpolating its coefficients. The efficiency of these algorithms heavily depends on this computation scheme which is dependent on the choice of the representative of the conjugacy class of G in S_n. Thus, we are interested in finding the representative of G in its conjugacy class which gives the best computation scheme, i.e. the one given the best efficiency. This is exactly what the results of [41] provide.

In [19], by computing splitting fields of parametric polynomials, we establish an isomorphism between the quintic cyclic polynomials discovered by Hashimoto-Tsunogai and those arising from Kummer theory for certain algebraic tori. The Hashimoto-Tsunogai polynomial $\mathrm{HT}(A, B; X)$ is a generic polynomial for the cyclic group C_5 of order 5, that is, all cyclic quintic extensions over any fields K containing $\mathbb{Q}$ can be obtained from $\mathrm{HT}(A, B; X)$ by choosing appropriate parameters A and $B \in K$. The Kummer polynomial $\mathrm{Kum}(t_1, t_2, t_3, t_4; X)$ is also a generic polynomial for C_5 but with 4 parameters. In contrary to the Hashimoto-Tsunogai polynomial, one can deduce arithmetical properties (prime decompositions) of the field defined by instantiation of the Kummer polynomial and two such fields can be proved to be isomorphic from the corresponding instantiations, one says that the ismorphism problem is solved for the Kummer's polynomial. Since Hashimoto-Tsunogai polynomial is a better generic polynomial in the sense of the number of parameters (the minimal one for C_5), the main aim of this article was to solve the isomorphism problem in this case by giving a correspondance between $\mathrm{Kum}(t_1, t_2, t_3, t_4; X)$ and $\mathrm{HT}(A, B; X)$. This was done by the following theorem: *The polynomial* $\mathrm{Kum}(-A-5B, -5B-1, A-5B, 1-5B; X)$ *defines the same cyclic quintic field as* $\mathrm{HT}(A, B; X)$ *over* $\mathbb{Q}(A, B)$. This enables us to solve the isomorphism problem for the more famous Brumer's quintic polynomial which can be deduced from the polynomial of Hashimoto-Tsunogai.

In [57], we study the problem of integer factoring given *implicit* information of a special kind. The problem is as follows: let $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$ be two RSA moduli of same bit-size, where q_1, q_2 are α-bit primes. We are given the *implicit* information that p_1 and p_2 share t most significant bits. We present a novel and rigorous lattice-based method that leads to the factorization of N_1 and N_2 in polynomial time as soon as $t \geq 2\alpha + 3$. Subsequently, we heuristically generalize the method to k RSA moduli $N_i = p_i q_i$ where the p_i's all share t most significant bits (MSBs) and obtain an improved bound on t that converges to $t \geq \alpha + 3.55...$ as k tends to infinity. We study also the case where the k factors p_i's share t contiguous bits in the middle and find a bound that converges to $2\alpha + 3$ when k tends to infinity. This paper extends the work of May and Ritzenhofen , where similar results were obtained when the p_i's share least significant bits (LSBs). Sarkar and Maitra describe an alternative but heuristic method for only two RSA moduli, when the p_i's share LSBs and/or MSBs, or bits in the middle. In the case of shared MSBs or bits in the middle and two RSA moduli, they get better experimental results in some cases, but we use much lower (at least 23 times lower) lattice dimensions and so we obtain a great speedup (at least 10^3 faster). Our results rely on the following surprisingly simple algebraic relation in which the shared MSBs of p_1 and p_2 cancel out: $q_1 N_2 - q_2 N_1 = q_1 q_2 (p_2 - p_1)$. This relation allows us to build a lattice whose shortest vector yields the factorization of the N_i's.

6.9. Error Correcting Codes

In [12], we revisit in this paper 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).

6.10. Geometric Knowledge Management

In [24], [45], [53], we have proposed methodologies and strategies for the modeling, encapsulation, formalization, specification, representation, organization, and processing of geometric knowledge and knowledge objects for the purpose of electronic storage and management. We classify geometric knowledge into knowledge objects according to how knowledge has been accumulated and represented in the geometric literature, formalize geometric knowledge objects using the language of predicate logic with embedded knowledge, and organize them by modeling the hierarchic structure of relations among them. The proposed methodologies and strategies allow one to design and create formalized geometric knowledge bases, to construct electronic geometry textbooks from knowledge data stored in the bases, and to manage the knowledge contained in the textbooks. Using plane Euclidean geometry, we have demonstrated the validity of our design methodologies and ideas by the implementation of a knowledge management system. This prototyping system has interface with our geometric knowledge base and provides a platform and a number of basic functionalities for constructing electronic geometry textbooks and managing the knowledge in the textbooks interactively. Preliminary experiments have shown the advantages of our system. Moreover, in [44] we have identified some basic elements that are required and should be studied for the development of computer geometry software. Such elements include geometric primitives, concepts, configurations, and constraints, algebraic representations, dynamic diagrams, and knowledge objects. On the basis of these elements, the main content of Euclidean geometry can be formalized and digitalized and geometric computation, reasoning, diagram generation, and knowledge management can be mechanized and automated.

6.11. Knot theory

For every odd integer N we give in [20] an explicit construction of a polynomial curve $\mathcal{C}(t) = (x(t), y(t))$, where $\deg x = 3$, $\deg y = N + 1 + 2\lfloor \frac{N}{4} \rfloor$ that has exactly N crossing points $\mathcal{C}(t_i) = \mathcal{C}(s_i)$ whose parameters satisfy $s_1 < ... < s_N < t_1 < ... < t_N$. Our proof makes use of the theory of Stieltjes series and Padé approximants. This allows us an explicit polynomial parametrization of the torus knot $K_{2,2n+1}$ with polynomials of degrees $(3, 3n + 1, 3n + 2)$. Furthermore the diagram we obtain is alternating.

In [21] we determine the Conway and Alexander polynomials modulo 2 of Fibonacci knots. We show that the Conway polynomial of a generalized Fibonacci knot is a Fibonacci polynomial modulo 2. As an application, we show that if $(n, j) \neq (3, 3)$ and $n\neg \equiv 0(\mathrm{mod}\, 4)$ the Fibonacci knot $\mathcal{F}_j^{(n)}$ is not a Lissajous knot. Our results are obtained by continued fraction expansions.

In [38], [54], we show that any two-bridge knot is a Chebyshev knot with $a = 3$ and also with $a = 4$. For every a, b, c integers ($a = 3, 4$ and a, b coprime), we describe an algorithm that gives all Chebyshev knots $\mathcal{C}(a, b, c, \varphi)$. We deduce a list of minimal Chebyshev representations of two-bridge knots with small crossing number. We describe 3 algorithms.
1. For $a = 3$ and $a = 4$ we determine the minimal integer b such that the Chebyshev curve $\mathcal{C}(a, b) : x = T_a(t),\ y = T_b(t)$ is a plane projection of K. This algorithm is based on continued fraction expansions.
2. Let $\mathcal{Z}_{a,b,c}$ be the set of φ such that $\mathcal{C}(a, b, c, \varphi)$ is singular. $\mathcal{Z}_{a,b,c}$ is finite. The knot type of $K(\varphi) = \mathcal{C}(a, b, c, \varphi)$ is constant over any interval of $\mathbf{R} - \mathcal{Z}_{a,b,c}$. Then we determine a rational number in each component of $\mathbf{R} - \mathcal{Z}_{a,b,c}$.
3. We determine the Schubert fraction of the knot $\mathcal{C}(a, b, c, r)$ by evaluating the (under/over) nature of the crossings.We make use of an algorithm based on a combination of floating point and multi precision arithmetic for real root isolations (see [8]). This amounts to evaluating the signs of polynomials at the real solutions of a zero-dimensional system.

7. Contracts and Grants with Industry

7.1. WMI (Maple)

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

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. Contract with Thalès

Participants: J.-C. Faugère [contact], G. Renault, C. Goyet.

The goal of this contract (including a CIFRE PhD grant) is to mix side chanel attacks (DPA) and algebraic cryptanalysis.

8. Other Grants and Activities

8.1. National Initiatives

8.1.1. 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 project is to study the singularities of parallel robots from theoretical aspects (classifications) to the practical ones (behavior).

8.1.2. ANR Grant "MAC"

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

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.

8.1.3. ANR Jeunes Chercheurs "CAC"

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

The new contract CAC " Computer Algebra and Cryptography" begins in October 2009 for a period of 4 years. This project will investigate the areas of cryptography and computer algebra, and their influence on the security and integrity of digital data. This proposal is a follow-up of the ANR MAC described below. In CAC, we plan to follow the methodology proposed in MAC, namely using basic tools of computer algebra to evaluate the security of cryptographic schemes. However, whilst ANR MAC was mainly interested develop new algebraic tools for studying the security of multivariate public key cryptosystems, CAC will focus on three new challenging applications of algebraic techniques in cryptography; namely block ciphers, hash functions, and factorization with known bits. To this hand, we will use Gröbner bases techniques but also lattice tools. In this proposal, we will explore non-conventional approaches in the algebraic cryptanalysis of these problems.

8.2. European Initiatives

8.2.1. ECRYPT II - European Network of Excellence for Cryptology

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

ECRYPT II - European Network of Excellence for Cryptology II is a 4-year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7) under contract number ICT-2007-216676. It falls under the action line Secure, dependable and trusted infrastructures. ECRYPT II started on 1 August 2008. Its objective is to continue intensifying the collaboration of European researchers in information security. The ECRYPT II research roadmap is motivated by the changing environment and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, and by the requirements of new applications and cryptographic implementations. Its main objective is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, 11 leading players have integrated their research capabilities within three virtual labs focusing on symmetric key algorithms (SymLab), public key algorithms and protocols (MAYA), and hardware and software implementations associate (VAMPIRE). They are joined by more than 20 adjoint members to the network who will closely collaborate with the core partners. The team joins the European Network of Excellence for Cryptology ECRYPT II this academic year as associate member.

8.3. International Initiatives

8.3.1. 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*.

8.3.2. ANR International Grant "EXACTA"

Participants: D. Wang [contact], J.-C. Faugère, D. Lazard, L. Perret, G. Renault, F. Rouillier, M. Safey El Din.

The main objective of this project is to study and compute the solutions of nonlinear algebraic systems and their structures and properties with selected target applications using exact or certified computation. The project consists of one main task of basic research on the design and implementation of fundamental algorithms and four tasks of applied research on computational geometry, algebraic cryptanalysis, global optimization, and algebraic biology. It will last for three years (2010–2012) with 300 person-months of workforce. Its consortium is composed of strong research teams from France and China (KLMM, SKLOIS, and LMIB) in the area of solving algebraic systems with applications.

8.4. Invitations

Ioannis Emiris (National Kapodistrian University of Athens) has been invited, on an INRIA grant, to spend two months in Lyon. The work focused on computational geometry problems.

9. Dissemination

9.1. Scientific Animation

9.1.1. Journals – Associate Editors and Program Committees

J.-C. Faugère is member of the editorial board of Journal "Mathematics in Computer Science" (Birkhäuser) and Journal "Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences" (Springer); guest editor for special issues in Journal of Symbolic Computation (Elsevier) and Journal "Mathematics in Computer Science" (Birkhäuser).

F. Rouillier is member of the editorial board of Journal of Symbolic Computation (Elsevier) and was guest editor for special issues in Journal "Mathematics in Computer Science" (Birkhäuser).

L. Perret edited the Book “Gröbner Bases, Coding, and Cryptography” (RISC Book Series, Springer) [50], [47].

J.-C. Faugère and F. Rouillier were guest editors for special issues in Journal of Symbolic Computation (Elsevier) [49].

J.-C. Faugère and L. Perret were guest editors for special issues in Journal of Symbolic Computation (Elsevier) [48] and Journal “Mathematics in Computer Science” (Birkhäuser).

D. Wang is member of the editorial board of Journal of Symbolic Computation (Elsevier), Journal “Frontiers of Computer Science in China” (Higher Education Press and Springer), Book series “Texts and Monographs in Symbolic Computation” (RISC Book Series, Springer); editor-in-chief and managing editor for Journal “Mathematics in Computer Science” (Birkhäuser); and Executive Associate Editor-in-Chief for Journal “Science in China Series F: Information Sciences” (Science in China Press and Springer).

J.-C. Faugère is member of the program committee for the 35th International Symposium on Symbolic and Algebraic Computation Issac’09 (Munich, Germany, July 25–28 2010), program committee of 5th China International Conference on Information Security and Cryptology (Beijing, China, December 12–15 th, 2009) program co-chair of the 2nd International Conference on Symbolic Computation and Cryptography (Royal Holloway, University of London, June 23-25 2010), scientific and program committee of Yet Another Conference on Cryptography (October 4 – October 8, 2010, Porquerolles Island, France).

L. Perret is member of the program committee of the 2nd International Conference on Symbolic Computation and Cryptography (Royal Holloway, University of London, June 23-25 2010), program committee of Yet Another Conference on Cryptography (October 4 – October 8, 2010, Porquerolles Island, France).

G. Renault was member of the program committee of the Joint Conference of ASCM 2009 and MACIS 2009 (Fukuoka, Japan, December 14–17, 2009).

F. Rouillier was member of the program committees of the Joint Conference of ASCM 2009 and MACIS 2009 (Fukuoka, Japan, December 14–17, 2009).

M. Safey El Din was member of the program committees of the 11th International Workshop on Computer Algebra in Scientific Computing (Kobe, Japan, September 13–17, 2009) and the Joint Conference of ASCM 2009 and MACIS 2009 (Fukuoka, Japan, December 14–17, 2009).

D. Wang was member of the program committees of the 6th Asian Workshop on Foundations of Software (Tokyo, Japan, April 6–8, 2009), the 3rd International Workshop on Symbolic-Numeric Computation (Kyoto, Japan, August 3–5, 2009), International Conference on Knowledge Engineering and Ontology Development (Madeira, Portugal, October 6–8, 2009), the 10th International Conference on Artificial Intelligence and Symbolic Computation (Paris, France, July 5–10, 2010), the 8th International Workshop on Automated Deduction in Geometry (Munich, Germany, July 22–24, 2010); Scientific Committee member for the 3rd Summer School in Symbolic Computation (Chengdu, China, August 10–16, 2009) and Advisory Program Committee member for the 3rd International Congress of Mathematical Software (Kobe, Japan, September 13–17, 2010).

9.1.2. Conferences (organization)

J.-C. Faugère, L. Perret, G. Renault organized Les Journées "Codage et Cryptographie" (GDR-IM CNRS) (Fréjus, France, October 4–9, 2009).

J.-C. Faugère, L. Perret, organized a special Track on Post-quantum Cryptology (December 14th, 2009, Beijing, China).

J.-C. Faugère, is member of the MEGA Advisory Board.

G. Renault organized a special track on Computational Algebraic Number Theory during ASCM 2009 (December 16th, 2009, Fukuoka, Japan)

F. Rouillier is member of the MACIS Steering Committee.

M. Safey El Din organized a special track on Real Solving Polynomial Systems during MACIS 2009 (December 16th, 2009, Fukuoka, Japan)

D. Wang is member of the MACIS Steering Committee; Co-chair for the International Symposium on Revision Calculus and Applications (Nanjing, China, October 12–14, 2009) and Track co-chair for the 11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (Timisoara, Romania, September 26–29, 2009).

9.1.3. Invited lectures

J.-C. Faugère [26] was invited speaker (tutorial) at International Symposium on Symbolic and Algebraic Computation (ISSAC) (Seoul Korea July 28–31, 2009). J.-C. Faugère [25] was invited speaker at the 11th International Workshop on Computer Algebra in Scientific Computing CASC, (Kobe Japan Sept 13–17, 2009). J.-C. Faugère was invited speaker at the Internation Conference "Polynomial Computer Algebra" (St Petersburg, Russia 2009).

D. Lazard was invited speaker at International Conference on Mathematics Mechanization (Beijing, China, May 11–13, 2009).

D. Wang was invited speakers at International Conference on Mathematics Mechanization (Beijing, China, May 11–13, 2009), Third Summer School in Symbolic Computation (Chengdu, China, August 10–16, 2009), Summer Symposium on Mathematical Problems in Complex Systems (Beijing, China, August 24–26, 2009) and Tunisia-Japan Workshop on Symbolic Computation in Software Science (Gammarth, Tunisia, September 22–24, 2009).

9.1.4. Scientific visits and international seminar

J.-C Faugère, and L. Perret were invited 1 week by J. von zur Gathen at Bit Institute (Bonn, Germany) and give one lecture.

J.-C Faugère, and L. Perret were invited 1 week by S.-J. Knapskog and D. Gligoroski at Norwegian University of Science and Technology and gave 4 lectures.

L. Perret was invited 1 week by Frederik Armknecht HGI, Ruhr-University Bochum (Germany)

G. Renault was invited 3 weeks in January 2009 by K. Yokoyama at Rikkyo University (Tokyo, Japan) and gave a lecture on Efficient Computation of Splitting Fields at the seminar of The University of Tokyo.

M. Safey El Din was invited 1 week by H. Hong at KIAS (South-Korea), 1 week by S. Basu at Purdue University (USA), and 25 days by E. Schost at the University of Western Ontario (Canada). He visited also the Symbolic Computation Group at North Carolina State University (Raleigh, USA) from October 1-st to October 31-st thanks to a grant obtained from the INRIA Program <<Explorateurs>>. During this latter visit, he gave a lecture on quantifier elimination over the reals and a lecture on the computation of roadmaps in real algebraic sets.

D. Wang was invited 1 week by A. M. Cohen at Eindhoven University of Technology (The Netherlands), 1 week by V. Gerdt and W. Plesken at RWTH Aachen University (Germany), and 1 week by T. Ida at University of Tsukuba (Japan).

Rune Ødegård is a novergian PhD student invited by his University (Univ of Trondheim) to visit the SALSA team for one year.

The following researchers also visited the team: Alexander May, HGI, Ruhr-University Bochum, Germany (1 week, September 2008), Frederik Armknecht HGI, Ruhr-University Bochum, Germany (December, 2008), Dongdai Lin, Institute of Software Chinese Academy of Sciences, China (2 months, October–November invited by CNRS), Martin Albrecht, RHUL, UK (1 week, September 2009), François-Xavier Standaert, UCL, Belgium (1 week, October 2009), Joachim von zur Gathen (December 2009).

9.2. Committees

F. Rouillier and J.-C. Faugère are member of the hiring committee in computer science at the <<Université Pierre et Marie Curie>>.

J.-C. Faugère is a member of the evaluation committee (AERES) of the Jean Kuntzmann lab (Grenoble).

M. Safey El Din is a member of the board of examiners for the PhD defense of A. Urguplu (expected in December 2009 or January 2010). M. Safey El Din was an external member of the hiring committee in computer science at the <<Université des Sciences et Technologies de Lille>>.

L. Perret is examiner for the PhD defense of Anna Rimold (defense on December 4 th, 2009). and was examiner for the PhD defense of Ilaria Simonetti (defended on March, 30 th, 2009).

9.2.1. Teaching

J.C. Faugère, L. Perret, F. Rouillier and M. Safey El Din give a course on Polynomial System Solving, Computer Algebra and Applications at the <<Master Parisien de Recherche en Informatique>> (MPRI).

F. Rouillier gives a course on real root finding for polynomial systems at the <<Master d'Informatique de l'Université Paris 6>>.

G. Renault gives a course on Computational Number Theory and Cryptology at the <<Master d'Informatique de l'Université Paris 6>>.

Moreover, J.-C. Faugère and M. Safey El Din wrote a chapter book [46] which is an introduction to polynomial system solving.

10. 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. RAHMANY. *Utilisation des bases de Gröbner SAGBI pour la résolution des systèmes polynômiaux invariants par symétries*, Université Paris 6, 2009, Ph. D. Thesis.

Articles in International Peer-Reviewed Journal

[12] D. AUGOT, M. BARDET, J.-C. FAUGÈRE. *On the decoding of binary cyclic codes with the Newton identities*, in "J. Symb. Comput.", vol. 44, n° 12, 2009, p. 1608–1625, http://dx.doi.org/10.1016/j.jsc.2008.02.006.

[13] B. BANK, M. GIUSTI, J. HEINTZ, M. SAFEY EL DIN, E. SCHOST. *On the geometry of polar varieties*, in "Applicable Algebra in Engineering, Communication and Computing", 2010, to appear DE AR CA .

[14] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Hybrid approach for solving multivariate systems over finite fields*, in "Journal of Mathematical Cryptology", 2009, p. 1-21, to appear.

[15] F. BOULIER, D. LAZARD, F. OLLIVIER, M. PETITOT. *Computing representations for radicals of finitely generated differential ideals*, in "Appl. Algebra Engrg. Comm. Comput.", vol. 20, n° 1, 2009, p. 5–6 and 73–121.

[16] G. BOURGEOIS, J.-C. FAUGÈRE. *Algebraic Attack on NTRU using Witt Vectors and Gröbner bases*, in "Journal of Mathematical Cryptology", 2009, p. 205-214, to appear.

[17] H. EVERETT, D. LAZARD, S. LAZARD, M. SAFEY EL DIN. *The Voronoi diagram of three lines in $\mathbb{R}^3$*, in "Discrete and Computational Geometry", vol. 42, n° 1, 2009, p. 94-130.

[18] J.-C. FAUGÈRE, L. PERRET. *An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography*, in "J. Symb. Comput.", vol. 44, n° 12, 2009, p. 1676–1689, http://dx.doi.org/10.1016/j.jsc.2008.02.005.

[19] M. KIDA, G. RENAULT, K. YOKOYAMA. *Quintic Polynomials of Hashimoto-Tsunogai, Brumer, and Kummer*, in "International Journal of Number Theory", vol. 5, n° 4, 2009, p. 555–571, http://dx.doi.org/10.1142/S1793042109002250JP.

[20] P.-V. KOSELEFF, D. PECKER. *A construction of polynomial torus knots*, in "Journal of Applicable Algebra in Engineering, Communication and Computing", vol. 20, n° 5-6, 2009, p. 361-377.

[21] P.-V. KOSELEFF, D. PECKER. *On Fibonacci knots*, in "Fibonacci Quarterly", 2010, 7p., to appear.

[22] D. LAZARD. *Thirty years of Polynomial System Solving, and now?*, in "Journal of Symbolic Computation", vol. 44, n° 3, 2009, p. 222–231.

[23] D. LAZARD, S. MCCALLUM. *Iterated Discriminants*, in "Journal of Symbolic Computation", vol. 44, n^{O} 9, 2009, p. 1176–1193 AU .

Articles in National Peer-Reviewed Journal

[24] D. WANG, Y. HUANG, X. CHEN. *Design and Implementation of Geometric Knowledge Base*, in "Journal of Computer Applications", vol. 29, n^{O} 2, 2009, p. 398–402, in Chinese (revised English version submitted for publication) CN .

Invited Conferences

[25] J.-C. FAUGÈRE. *Efficient algorithms to compute Groebner Bases and applications in Cryptology*, in "Polynomial Computer Algebra'09", April 2009.

[26] J.-C. FAUGÈRE. *Interactions between computer algebra (Gröbner bases) and cryptology*, in "ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation, New York, NY, USA", ACM, 2009, p. 383–384, http://doi.acm.org/10.1145/1576702.1576755.

[27] J.-C. FAUGÈRE. *Solving Structured Polynomial Systems and Applications to Cryptology*, in "Computer Algebra in Scientific Computing - CASC'09", V. GERDT, E. MAYR, E. VOROZHTSOV (editors), 2009, p. 79-80, http://dx.doi.org/10.1007/978-3-642-04103-7_7, DBLP:conf/casc/2009.

[28] J.-C. FAUGÈRE, L. PERRET, P.-J. SPAENLEHAUER. *Algebraic-Differential Cryptanalysis of DES*, in "Western European Workshop on Research in Cryptology - WEWoRC 2009", 2009, p. 79-80, http://dx.doi.org/10.1007/978-3-642-04103-7_7.

[29] D. LAZARD. *Theorem Proving in Geometry and Tools for Polynomial System Solving*, in "International Conference on Mathematics Mechanization (ICMM) in honor of professor Wen-Tsun Wu's nineties birthday", 11-13 May 2009.

[30] M. SAFEY EL DIN. *Fast Algorithms for Real Solving Polynomial Systems of Inequalities/inequations*, in "SIAM Conference on Parallel Processing and Scientific Computing – High Performance Symbolic Computing", SIAM, 2010, to appear.

International Peer-Reviewed Conference/Proceedings

[31] L. BETTALE, J.-C. FAUGÈRE, L. PERRET. *Security Analysis of Multivariate Polynomials for Hashing*, in "Information Security and Cryptology: 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, Berlin, Heidelberg", Springer-Verlag, 2009, p. 115–124, http://dx.doi.org/10.1007/978-3-642-01440-6_11.

[32] H. EVERETT, C. GILLOT, D. LAZARD, S. LAZARD, M. POUGET. *The Voronoi diagram of three arbitrary lines in* $\mathbb{R}^3$, in "25th Annual Symposium on Computational Geometry (SoCG09)", 16–18 March 2009.

[33] J.-C. FAUGÈRE, L. PERRET. *High order derivatives and decomposition of multivariate polynomials*, in "ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation, New York, NY, USA", ACM, 2009, p. 207–214, http://doi.acm.org/10.1145/1576702.1576732.

[34] J.-C. FAUGÈRE, S. RAHMANY. *Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases*, in "ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and alge-

braic computation, New York, NY, USA", ACM, 2009, p. 151–158, http://doi.acm.org/10.1145/1576702.1576725IR.

[35] H. HONG, M. SAFEY EL DIN. *Variant quantifier elimination: algorithm and applications to stability analysis*, in "Computer-assisted proofs - tools, methods and applications", Dagstuhl Seminar Proceedings 09471, 2009 US .

[36] H. HONG, M. SAFEY EL DIN. *Variant real quantifier elimination: algorithm and application*, in "ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation, New York, NY, USA", ACM, 2009, p. 183–190, http://doi.acm.org/10.1145/1576702.1576729US.

[37] Y. HUANG, D. WANG. *Computing Self-intersection Loci of Parametrized Surfaces Using Regular Systems and Gröbner Bases*, in "SYNASC 2009: Proceedings of the 11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Los Alamitos, CA", IEEE Computer Society, September 2009, to appear CN .

[38] P.-V. KOSELEFF, D. PECKER, F. ROUILLIER. *The first rational Chebyshev knots*, in "MEGA'09", 2009.

[39] D. LAZARD. *Algebraic points in geometry and application to CAD*, in "International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS)", 14–17 Dec. 2009.

[40] X. LI, C. MOU, W. NIU, D. WANG. *Stability Analysis for Discrete Biological Models Using Algebraic Methods*, in "MACIS 2009: Proceedings of the Third International Conference on Mathematical Aspects of Computer and Information Sciences", December 2009, to appear CN .

[41] S. ORANGE, G. RENAULT, K. YOKOYAMA. *Computation Schemes for Splitting Fields of Polynomials*, in "ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation, New York, NY, USA", ACM, 2009, p. 279–286, http://doi.acm.org/10.1145/1576702.1576741JP.

[42] M. POUGET, S. LAZARD, E. TSIGARIDAS, F. ROUILLIER, L. PEÑARANDA, J. CHENG. *On the topology of planar algebraic curves*, in "SOCG'09", 2009.

[43] F. ROUILLIER, R. XIAO. *On Using Triangular Decomposition for Solving Parametric Polynomial Systems*, in "MACIS'09", 2009.

[44] D. WANG. *Basic Elements of Computer Geometry*, in "SCSS 2009: Proceedings of the Tunisia-Japan Workshop on Symbolic Computation in Software Science", EasyChair, September 2009, p. 2–12.

[45] D. WANG. *Formalization and Specification of Geometric Knowledge Objects*, in "AWFS 2009: Proceedings of the Sixth Asian Workshop on Foundations of Software, Tokyo, Japan", National Institute of Informatics, April 2009, p. 86–98.

Scientific Books (or Scientific Book chapters)

[46] J.-C. FAUGÈRE, M. SAFEY EL DIN. *De l'algèbre linéaire à la résolution des systèmes polynomiaux*, in "Mathématiques Appliquées (L3)", Pearson, 2009.

[47] F. LEVY-DIT-VEHEL, M. G. MARINARI, L. PERRET, C. TRAVERSO. *A Survey on Polly Cracker Systems*, in "Gröbner Bases, Coding, and Cryptography", Springer, 2009, p. 143-155.

Books or Proceedings Editing

[48] D. Augot, J.-C. Faugère, L. Perret (editors). *Gröbner Bases Techniques in Coding Theory and Cryptography*, vol. 44, n^{o} 12, Academic Press, Inc., Journal of Symbolic Computation, 2009, http://dx.doi.org/10.1016/j.jsc.2008.11.004.

[49] J.-C. Faugère, F. Rouillier (editors). *Polynomial system solving*, vol. 44, n^{o} 3, Academic Press, Inc., Journal of Symbolic Computation, 2009, http://dx.doi.org/10.1016/j.jsc.2008.08.004.

[50] M. Sala, T. Mora, L. Perret, S. Sakata, C. Traverso (editors). *Gröbner Bases, Coding, and Cryptography*, Springer, 2009.

Research Reports

[51] M. Safey El Din, E. Schost. *A baby steps/giant steps Monte Carlo algorithm for computing roadmaps in smooth compact real hypersurfaces*, INRIA, 2009, submitted to Discrete and Computational Geometry, Technical report CA .

[52] M. Safey El Din, L. Zhi. *Computing rational points in convex semi-algebraic sets and SOS decompositions*, INRIA, 2009, submitted to SIAM Journal on Optimization, Technical report CN .

Other Publications

[53] X. Chen, D. Wang. *Management of Geometric Knowledge in Textbooks*, November 2009, submitted for publication CN .

[54] P.-V. Koseleff, D. Pecker, F. Rouillier. *The first rational Chebyshev knots*, 2009, submitted to Journal of Symbolic Computation, 22p. 27 fig., 3 tables CN .

[55] D. Lazard. *CAD and topology of semi-algebraic sets*, 2009, Submitted for the special issue Computational Geometry and Computer-aided Geometric Design of Mathematics in Computer Science.

[56] D. Lazard. *Theorem proving in geometry and tools for polynomial system solving*, 2009, Submitted for the special issue Mathematics Mechanization of Journal of Symbolic Computation.

[57] R. Marinier, J.-C. Faugère, G. Renault. *Implicit Factoring with Shared Most Significant and Middle Bits*, 2009, submitted.

References in notes

[58] 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.

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

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

[61] 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$^{\text{o}}$ 1, 2007, p. 4–12.

[62] 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.

[63] 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.

[64] 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$^{\text{o}}$ 4, Oct. 1993, p. 329–344.

[65] 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.

[66] 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.

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

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

[69] 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$^{\text{o}}$ 4, Apr 1998, p. 845-856.

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

[71] 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.

[72] 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.

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

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

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

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

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

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

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

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

[81] T. MATSUMOTO, 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.

[82] 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.

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

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

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

[86] 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.

[87] 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.

[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*, n^{o} 5071, INRIA, 2004, http://hal.inria.fr/inria-00071512, submitted to Journal of Pure and Applied Algebra, Technical report.

[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, http://doi.acm.org/10.1145/780506.780541.

[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", J. JOHNSON, S. MCKEE, A. VELLA (editors), Oxford University Press, 1994, p. 147–156.