IN PARTNERSHIP WITH:
CNRS

Université Pierre et Marie Curie (Paris 6)

Activity Report 2014

Project-Team POLSYS

Polynomial Systems

IN COLLABORATION WITH: Laboratoire d'informatique de Paris 6 (LIP6)

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team POLSYS

Keywords: Computer Algebra, Cryptography, Algorithmic Geometry, Algorithmic Number Theory, Complexity

Creation of the Team: 2012 January 01*, updated into Project-Team:* 2013 January 01.

1. Members

Research Scientists

Jean-Charles Faugère [Team leader, Inria, Senior Researcher, HdR]
Elias Tsigaridas [Inria, Researcher]
Dongming Wang [CNRS, Senior Researcher, HdR]

Faculty Members

Jérémy Berthomieu [UPMC (Univ. Paris 6), Associate Professor]
Alain Jacquemard [Univ. Bourgogne, Professor, delegation since Sep 2014, HdR]
Daniel Lazard [UPMC (Univ. Paris 6), Professor, Emeritat, HdR]
Ludovic Perret [UPMC (Univ. Paris 6), Associate Professor]
Guénaël Renault [UPMC (Univ. Paris 6), Associate Professor]
Mohab Safey El Din [UPMC (Univ. Paris 6), Professor, HdR]

PhD Students

Ivan Bannwarth [UPMC (Univ. Paris 6), since Sep 2014]
Simone Naldi [LAAS/CNRS, granted by ANR GEOLMI project]
Ulrick Severin [UPMC (Univ. Paris 6), Dassault Systèmes, from Apr 2014]
Jules Svartz [UPMC (Univ. Paris 6), until Aug 2014]
Frédéric Urvoy de Portzamparc [UPMC (Univ. Paris 6), GEMALTO]
Thibaut Verron [UPMC (Univ. Paris 6)]
Alexandre Wallet [Inria]
Rina Zeitoun [UPMC (Univ. Paris 6), Oberthur Technologies]

Post-Doctoral Fellows

Brice Boyer [UPMC (Univ. Paris 6), since Sep 2014]
Christian Eder [Inria, until Jan 2014]
Louise Huot [UPMC (Univ. Paris 6), ATER, until Aug 2014]

Visiting Scientists

Marta Conde Pena [Instituto de Tecnologías Físicas y de la Información, Spain, since Apr 2014 until Jul 2014]
Danilo Gligoroski [Norges Teknisk-Naturvitenskapelige Universitet, Norway, since Sep 2014 until Nov 2014]
Aaron Herman [North Carolina State University, U.S.A., since Sep 2014 until Nov 2014]
Nitin Saxena [Indian Institute of Technology Kanpur, India, Dec 2014]
Éric Schost [University of Western Ontario, Canada, Nov 2014]

Administrative Assistants

Laurence Bourcier [Inria]
Emmanuelle Grousset [AMUE, since Dec 2014]
Nelly Maloisel [Inria]

Others

Ivan Bannwarth [Univ. Versailles – St-Quentin-en-Yvelines, Internship, since Mar 2014 until Aug 2014]
Matías Bender [Inria, Internship, since Sep 2014]
Anca Nitulescu [Univ. Paris Diderot, Internship, since Mar 2014 until Aug 2014]
Ulrick Severin [Dassault Systèmes, Internship until Mar 2014]

2. Overall Objectives

2.1. Overall Objectives

The main focus of the POLSYS project is to solve systems of polynomial equations.

Our main objectives are:

- **Fundamental Algorithms and Structured Systems.** The objective is to propose fast exponential exact algorithms for solving polynomial equations and to identify large classes of structured polynomial systems which can be solved in polynomial time.
- **Solving Systems over the Reals and Applications.** For positive dimensional systems basic questions over the reals may be very difficult (for instance testing the existence of solutions) but also very useful in applications (e.g. global optimization problems). We plan to propose efficient algorithms and implementations to address the most important issues: computing sample points in the real solution sets, decide if two such sample points can be path-connected and, as a long term objective, perform quantifier elimination over the reals (computing a quantifier-free formula which is equivalent to a given quantified boolean formula of polynomial equations/inequalities).
- **Dedicated Algebraic Computation and Linear Algebra.** While linear algebra is a key step in the computation of Gröbner bases, the matrices generated by the algorithms F_4/F_5 have specific structures (quasi block triangular).The objective is to develop a dedicated efficient multi-core linear algebra package as the basis of a future open source library for computing Gröbner bases.
- **Solving Systems in Finite Fields, Applications in Cryptology and Algebraic Number Theory.** We propose to develop a systematic use of *structured systems* in Algebraic Cryptanalysis. We want to improve the efficiency and to predict the theoretical complexity of such attacks. We plan to demonstrate the power of algebraic techniques in new areas of cryptography such as Algebraic Number Theory (typically, in curve based cryptography).

3. Research Program

3.1. Introduction

Polynomial system solving is a fundamental problem in Computer Algebra with many applications in cryptography, robotics, biology, error correcting codes, signal theory, ... Among all available methods for solving polynomial systems, computation of Gröbner bases remains one of the most powerful and versatile method since it can be applied in the continuous case (rational coefficients) as well as in the discrete case (finite fields). Gröbner bases are also a building blocks for higher level algorithms who compute real sample points in the solution set of polynomial systems, decide connectivity queries and quantifier elimination over the reals. The major challenge facing the designer or the user of such algorithms is the intrinsic exponential behaviour of the complexity for computing Gröbner bases. The current proposal is an attempt to tackle these issues in a number of different ways: improve the efficiency of the fundamental algorithms (even when the complexity is exponential), develop high performance implementation exploiting parallel computers, and investigate new classes of structured algebraic problems where the complexity drops to polynomial time.

3.2. Fundamental Algorithms and Structured Systems

Participants: Jean-Charles Faugère, Mohab Safey El Din, Elias Tsigaridas, Guénaël Renault, Dongming Wang, Jérémy Berthomieu, Jules Svartz, Louise Huot, Thibaut Verron.

Efficient algorithms F_4/F_5 [1] for computing the Gröbner basis of a polynomial system rely heavily on a connection with linear algebra. Indeed, these algorithms reduce the Gröbner basis computation to a sequence of Gaussian eliminations on several submatrices of the so-called Macaulay matrix in some degree. Thus, we expect to improve the existing algorithms by
(i) developing dedicated linear algebra routines performing the Gaussian elimination steps: this is precisely the objective 2 described below;
(ii) generating smaller or simpler matrices to which we will apply Gaussian elimination.
We describe here our goals for the latter problem. First, we focus on algorithms for computing a Gröbner basis of *general polynomial systems*. Next, we present our goals on the development of dedicated algorithms for computing Gröbner bases of *structured polynomial systems* which arise in various applications.

Algorithms for general systems. Several degrees of freedom are available to the designer of a Gröbner basis algorithm to generate the matrices occurring during the computation. For instance, it would be desirable to obtain matrices which would be almost triangular or very sparse. Such a goal can be achieved by considering various interpretations of the F_5 algorithm with respect to different monomial orderings. To address this problem, the tight complexity results obtained for F_5 will be used to help in the design of such a general algorithm. To illustrate this point, consider the important problem of solving boolean polynomial systems; it might be interesting to preserve the sparsity of the original equations and, at the same time, using the fact that overdetermined systems are much easier to solve.

Algorithms dedicated to *structured* polynomial systems. A complementary approach is to exploit the structure of the input polynomials to design specific algorithms. Very often, problems coming from applications are not random but are highly structured. The specific nature of these systems may vary a lot: some polynomial systems can be sparse (when the number of terms in each equation is low), overdetermined (the number of the equations is larger than the number of variables), invariants by the action of some finite groups, multi-linear (each equation is linear w.r.t. to one block of variables) or more generally multihomogeneous. In each case, the ultimate goal is to identify large classes of problems whose theoretical/practical complexity drops and to propose in each case dedicated algorithms.

3.3. Solving Systems over the Reals and Applications.

Participants: Mohab Safey El Din, Daniel Lazard, Elias Tsigaridas, Simone Naldi, Ivan Bannwarth.

We will develop algorithms for solving polynomial systems over complex/real numbers. Again, the goal is to extend significantly the range of reachable applications using algebraic techniques based on Gröbner bases and dedicated linear algebra routines. Targeted application domains are global optimization problems, stability of dynamical systems (e.g. arising in biology or in control theory) and theorem proving in computational geometry.

The following functionalities shall be requested by the end-users:
(i) deciding the emptiness of the real solution set of systems of polynomial equations and inequalities,
(ii) quantifier elimination over the reals or complex numbers,
(iii) answering connectivity queries for such real solution sets.
We will focus on these functionalities.

[1] J.-C. Faugère. *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5).* In Proceedings of ISSAC '02, pages 75-83, New York, NY, USA, 2002. ACM.

We will develop algorithms based on the so-called critical point method to tackle systems of equations and inequalities (problem *(i)*) . These techniques are based on solving 0-dimensional polynomial systems encoding "critical points" which are defined by the vanishing of minors of jacobian matrices (with polynomial entries). Since these systems are highly structured, the expected results of Objective 1 and 2 may allow us to obtain dramatic improvements in the computation of Gröbner bases of such polynomial systems. This will be the foundation of practically fast implementations (based on singly exponential algorithms) outperforming the current ones based on the historical Cylindrical Algebraic Decomposition (CAD) algorithm (whose complexity is doubly exponential in the number of variables). We will also develop algorithms and implementations that allow us to analyze, at least locally, the topology of solution sets in some specific situations. A long-term goal is obviously to obtain an analysis of the global topology.

3.4. Low level implementation and Dedicated Algebraic Computation and Linear Algebra.

Participants: Jean-Charles Faugère, Christian Eder, Elias Tsigaridas.

Here, the primary objective is to focus on *dedicated* algorithms and software for the linear algebra steps in Gröbner bases computations and for problems arising in Number Theory. As explained above, linear algebra is a key step in the process of computing efficiently Gröbner bases. It is then natural to develop specific linear algebra algorithms and implementations to further strengthen the existing software. Conversely, Gröbner bases computation is often a key ingredient in higher level algorithms from Algebraic Number Theory. In these cases, the algebraic problems are very particular and specific. Hence dedicated Gröbner bases algorithms and implementations would provide a better efficiency.

Dedicated linear algebra tools.FGB is an efficient library for Gröbner bases computations which can be used, for instance, via MAPLE. However, the library is sequential. A goal of the project is to extend its efficiency to new trend parallel architectures such as clusters of multi-processor systems in order to tackle a broader class of problems for several applications. Consequently, our first aim is to provide a durable, long term software solution, which will be the successor of the existing FGB library. To achieve this goal, we will first develop a high performance linear algebra package (under the LGPL license). This could be organized in the form of a collaborative project between the members of the team. The objective is not to develop a general library similar to the LINBOX project but to propose a dedicated linear algebra package taking into account the specific properties of the matrices generated by the Gröbner bases algorithms. Indeed these matrices are sparse (the actual sparsity depends strongly on the application), almost block triangular and not necessarily of full rank. Moreover, most of the pivots are known at the beginning of the computation. In practice, such matrices are huge (more than 10^6 columns) but taking into account their shape may allow us to speed up the computations by one or several orders of magnitude. A variant of a Gaussian elimination algorithm together with a corresponding C implementation has been presented. The main peculiarity is the order in which the operations are performed. This will be the kernel of the new linear algebra library that will be developed.

Fast linear algebra packages would also benefit to the transformation of a Gröbner basis of a zero–dimensional ideal with respect to a given monomial ordering into a Gröbner basis with respect to another ordering. In the generic case at least, the change of ordering is equivalent to the computation of the minimal polynomial of a so-called multiplication matrix. By taking into account the sparsity of this matrix, the computation of the Gröbner basis can be done more efficiently using variant of the Wiedemann algorithm. Hence, our goal is also to obtain a dedicated high performance library for transforming (i.e. change ordering) Gröbner bases.

Dedicated algebraic tools for Algebraic Number Theory. Recent results in Algebraic Number Theory tend to show that the computation of Gröbner basis is a key step toward the resolution of difficult problems in this domain [2]. Using existing resolution methods is simply not enough to solve relevant problems. The main algorithmic look to overcome is to adapt the Gröbner basis computation step to the specific problems. Typically, problems coming from Algebraic Number Theory usually have a lot of symmetries or the input

[2] P. Gaudry, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, Journal of Symbolic Computation 44,12 (2009) pp. 1690-1702

systems are very structured. This is the case in particular for problems coming from the algorithmic theory of Abelian varieties over finite fields [3] where the objects are represented by polynomial system and are endowed with intrinsic group actions. The main goal here is to provide dedicated algebraic resolution algorithms and implementations for solving such problems. We do not restrict our focus on problems in positive characteristic. For instance, tower of algebraic fields can be viewed as triangular sets; more generally, related problems (e.g. effective Galois theory) which can be represented by polynomial systems will receive our attention. This is motivated by the fact that, for example, computing small integer solutions of Diophantine polynomial systems in connection with Coppersmith's method would also gain in efficiency by using a dedicated Gröbner bases computations step.

3.5. Solving Systems in Finite Fields, Applications in Cryptology and Algebraic Number Theory.

Participants: Jean-Charles Faugère, Ludovic Perret, Guénaël Renault, Louise Huot, Frédéric Urvoy de Portzamparc, Rina Zeitoun, Jérémy Berthomieu.

Here, we focus on solving polynomial systems over finite fields (i.e. the discrete case) and the corresponding applications (Cryptology, Error Correcting Codes, ...). Obviously this objective can be seen as an application of the results of the two previous objectives. However, we would like to emphasize that it is also the source of new theoretical problems and practical challenges. We propose to develop a systematic use of *structured systems* in *algebraic cryptanalysis*.
(i) So far, breaking a cryptosystem using algebraic techniques could be summarized as modeling the problem by algebraic equations and then computing a, usually, time consuming Gröbner basis. A new trend in this field is to require a theoretical complexity analysis. This is needed to explain the behavior of the attack but also to help the designers of new cryptosystems to propose actual secure parameters.
(ii) To assess the security of several cryptosystems in symmetric cryptography (block ciphers, hash functions, ...), a major difficulty is the size of the systems involved for this type of attack. More specifically, the bottleneck is the size of the linear algebra problems generated during a Gröbner basis computation.

We propose to develop a systematic use of *structured systems* in *algebraic cryptanalysis*.

The first objective is to build on the recent breakthrough in attacking McEliece's cryptosystem: it is the first structural weakness observed on one of the oldest public key cryptosystem. We plan to develop a well founded framework for assessing the security of public key cryptosystems based on coding theory from the algebraic cryptanalysis point of view. The answer to this issue is strongly related to the complexity of solving bihomogeneous systems (of bidegree $(1, d)$). We also plan to use the recently gained understanding on the complexity of structured systems in other areas of cryptography. For instance, the MinRank problem – which can be modeled as an overdetermined system of bilinear equations – is at the heart of the structural attack proposed by Kipnis and Shamir against HFE (one of the most well known multivariate public cryptosystem). The same family of structured systems arises in the algebraic cryptanalysis of the Discrete Logarithmic Problem (DLP) over curves (defined over some finite fields). More precisely, some bilinear systems appear in the polynomial modeling the points decomposition problem. Moreover, in this context, a natural group action can also be used during the resolution of the considered polynomial system.

Dedicated tools for linear algebra problems generated during the Gröbner basis computation will be used in algebraic cryptanalysis. The promise of considerable algebraic computing power beyond the capability of any standard computer algebra system will enable us to attack various cryptosystems or at least to propose accurate secure parameters for several important cryptosystems. Dedicated linear tools are thus needed to tackle these problems. From a theoretical perspective, we plan to further improve the theoretical complexity of the hybrid method and to investigate the problem of solving polynomial systems with noise, i.e. some equations of the system are incorrect. The hybrid method is a specific method for solving polynomial systems over finite fields. The idea is to mix exhaustive search and Gröbner basis computation to take advantage of the over-determinacy of the resulting systems.

[3] e.g. point counting, discrete logarithm, isogeny.

Polynomial system with noise is currently emerging as a problem of major interest in cryptography. This problem is a key to further develop new applications of algebraic techniques; typically in side-channel and statistical attacks. We also emphasize that recently a connection has been established between several classical lattice problems (such as the Shortest Vector Problem), polynomial system solving and polynomial systems with noise. The main issue is that there is no sound algorithmic and theoretical framework for solving polynomial systems with noise. The development of such framework is a long-term objective.

4. Application Domains

4.1. Cryptology

We propose to develop a systematic use of structured systems in Algebraic Cryptanalysis. We want to improve the efficiency and to predict the theoretical complexity of such attacks. We plan to demonstrate the power of algebraic techniques in new areas of cryptography such as Algebraic Number Theory (typically, in curve based cryptography).

4.2. Engineering sciences

Solving polynomial systems over the reals arise as a critical issue in wide range of problems coming from engineering sciences (biology, physics, control theory, etc.). We will focus on developing general enough software that may impact on these domains with a particular focus on control theory

5. New Software and Platforms

5.1. FGb

Participant: Jean-Charles Faugère [contact].

FGb is a powerful software for computing Gröbner bases.It includes the new generation of algorihms for computing Gröbner bases polynomial systems (mainly the F4, F5 and FGLM algorithms). It is implemented in C/C++ (approximately 250000 lines), 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.
See also the web page http://www-polsys.lip6.fr/~jcf/Software/FGb/index.html.

5.2. GBLA

Participants: Jean-Charles Faugère [contact], Brice Boyer.

- ACM: I.1.2 Algebraic algorithms
- Programming language: C/C++

GBLA a new open source C library for linear algebra dedicated to Gröbner bases computations (see http://www-polsys.lip6.fr/~jcf/Software/index.html).

5.3. RAGlib

Participant: Mohab Safey El Din [contact].

RAGLib is a Maple library for solving over the reals polynomial systems and computing sample points in semi-algebraic sets.

5.4. Epsilon

Participant: Dongming Wang [contact].

Epsilon is a library of functions implemented in Maple and Java for polynomial elimination and decomposition with (geometric) applications.

5.5. SLV

Participant: Elias Tsigaridas [contact].

SLV is a software package in C that provides routines for isolating (and subsequently refine) the real roots of univariate polynomials with integer or rational coefficients based on subdivision algorithms and on the continued fraction expansion of real numbers. Special attention is given so that the package can handle polynomials that have degree several thousands and size of coefficients hundrends of Megabytes. Currently the code consists of $\sim 5\,000$ lines.

- ACM: I.1.2 Algebraic algorithms
- Programming language: C/C++

6. New Results

6.1. Highlights of the Year

Jointly with Univ. Of Kaiserslautern (C. Eder), we have released a new open source C library for linear algebra dedicated to Gröbner bases computations (see http://www-polsys.lip6.fr/~jcf/Software/index.html). This new library opens the door to high performance applications

- The library is specialized in reducing matrices generated during Gröbner bases computations. Optimizing this reduction step is crucial for the overall computation.
- Our approach takes even more advantage of the very special structure (quasi unit-triangular sparse matrices with patterns in the data)
- We also reduce the number of operations, in a parallel friendly fashion, by changing the order of the operations in the elimination.
- We present experimental results for sequential and parallel computations on NUMA architectures. We also get good scaling up until 32 (non hyper-threaded) cores: we have speed-ups around 14 or 16.

6.2. Fundamental algorithms and structured polynomial systems

6.2.1. Sparse Gröbner Bases

Sparse elimination theory is a framework developped during the last decades to exploit monomial structures in systems of Laurent polynomials. Roughly speaking, this amounts to computing in a *semigroup algebra*, *i.e.* an algebra generated by a subset of Laurent monomials. In order to solve symbolically sparse systems, we introduce *sparse Gröbner bases*, an analog of classical Gröbner bases for semigroup algebras, and we propose sparse variants of the F_5 and FGLM algorithms to compute them.

In the case where the generating subset of monomials corresponds to the points with integer coordinates in a normal lattice polytope $\mathcal{P} \subset \mathbb{R}^n$ and under regularity assumptions, we prove in [19] complexity bounds which depend on the combinatorial properties of $\mathcal{P}$. These bounds yield new estimates on the complexity of solving 0-dim systems where all polynomials share the same Newton polytope (*unmixed case*). For instance, we generalize the bound $\min(n_1, n_2) + 1$ on the maximal degree in a Gröbner basis of a 0-dim. Bilinear system with blocks of variables of sizes (n_1, n_2) to the multihomogeneous case: $n + 2 - \max_i (\lceil (n_i + 1)/d_i \rceil)$. We also propose a variant of Fröberg's conjecture which allows us to estimate the complexity of solving overdetermined sparse systems.

Moreover, our prototype "proof-of-concept" implementation shows large speed-ups (more than 100 for some examples) compared to optimized (classical) Gröbner bases software.

6.2.2. Gröbner bases for weighted homogeneous systems

Solving polynomial systems arising from applications is frequently made easier by the structure of the systems. Weighted homogeneity (or quasi-homogeneity) is one example of such a structure: given a system of weights $W = (w_1, \cdots, w_n)$, W-homogeneous polynomials are polynomials which are homogeneous w.r.t the weighted degree $\deg_W (X_1^{\alpha_1}, \cdots, X_n^{\alpha_n}) = \sum w_i \alpha_i$.

Gröbner bases for weighted homogeneous systems can be computed by adapting existing algorithms for homogeneous systems to the weighted homogeneous case. In [29], we show that in this case, the complexity estimate for Algorithm F5 $\left(\binom{n+d_{\max}-1}{d_{\max}}^{\omega}\right)$ can be divided by a factor $\left(\prod w_i\right)^{\omega}$. For zero-dimensional systems, the complexity of Algorithm FGLM nD^{ω} (where D is the number of solutions of the system) can be divided by the same factor $\left(\prod w_i\right)^{\omega}$. Under genericity assumptions, for zero-dimensional weighted homogeneous systems of W-degree $(d_1, \cdots, d_n)$, these complexity estimates are polynomial in the weighted Bézout bound $\prod_{i=1}^{n} d_i / \prod_{i=1}^{n} w_i$.

Furthermore, the maximum degree reached in a run of Algorithm F5 is bounded by the weighted Macaulay bound $\sum (d_i - w_i) + w_n$, and this bound is sharp if we can order the weights so that $w_n = 1$. For overdetermined semi-regular systems, estimates from the homogeneous case can be adapted to the weighted case.

We provide some experimental results based on systems arising from a cryptography problem and from polynomial inversion problems. They show that taking advantage of the weighted homogeneous structure yields substantial speed-ups, and allows us to solve systems which were otherwise out of reach.

6.2.3. Computing necessary integrability conditions for planar parametrized homogeneous potentials

Let $V \in \mathbb{Q}(i)(\mathbf{a}_1, \cdots, \mathbf{a}_n)(\mathbf{q}_1, \mathbf{q}_2)$ be a rationally parametrized planar homogeneous potential of homogeneity degree $k \neq -2, 0, 2$. In [12], we design an algorithm that computes polynomial *necessary* conditions on the parameters $(\mathbf{a}_1, \cdots, \mathbf{a}_n)$ such that the dynamical system associated to the potential V is integrable. These conditions originate from those of the Morales-Ramis-Simó integrability criterion near all Darboux points and make use of Gröbner bases algorithms. The implementation of the algorithm allows to treat applications that were out of reach before, for instance concerning the non-integrability of polynomial potentials up to degree 9. Another striking application is the first complete proof of the non-integrability of the *collinear three body problem*.

6.3. Solving Polynomial Systems over the Reals and Applications

6.3.1. Exact algorithms for polynomial optimization

Let $f, f_1, ..., f_s$ be n-variate polynomials with rational coefficients of maximum degree D and let V be the set of common complex solutions of $\mathbf{F} = (f_1, ..., f_s)$. In [7], we give an algorithm which, up to some regularity assumptions on $\mathbf{F}$, computes an *exact* representation of the global infimum $f^{\bigstar}$ of the restriction of the map $x \to f(x)$ to $V \cap \mathbb{R}^n$, i.e. a univariate polynomial vanishing at $f^{\bigstar}$ and an isolating interval for $f^{\bigstar}$. Furthermore, it decides whether $f^{\bigstar}$ is reached and if so, it returns $x^{\bigstar} \in V \cap \mathbb{R}^n$ such that $f(x^{\bigstar}) = f^{\bigstar}$.

This algorithm is *probabilistic*. It makes use of the notion of polar varieties. Its complexity is essentially *cubic* in $(sD)^n$ and linear in the complexity of evaluating the input. This fits within the best known *deterministic* complexity class $D^{O(n)}$.

We report on some practical experiments of a first implementation that is available as a MAPLE package. It appears that it can tackle global optimization problems that were unreachable by previous exact algorithms and can manage instances that are hard to solve with purely numeric techniques. As far as we know, even under the extra genericity assumptions on the input, it is the first probabilistic algorithm that combines practical efficiency with good control of complexity for this problem.

It is known that point searching in basic semialgebraic sets and the search for globally minimal points in polynomial optimization tasks can be carried out using $(s\,d)^{O(n)}$ arithmetic operations, where n and s are the numbers of variables and constraints and d is the maximal degree of the polynomials involved.
Subject to certain conditions, we associate in [2] to each of these problems an intrinsic system degree which becomes in worst case of order $(n\,d)^{O(n)}$ and which measures the intrinsic complexity of the task under consideration.
We design non-uniform deterministic or uniform probabilistic algorithms of intrinsic, quasi-polynomial complexity which solve these problems.

6.3.2. Algorithms for answering connectivity queries

Let $\mathbf{R}$ be a real closed field and $\mathbf{D} \subset \mathbf{R}$ an ordered domain. In [4], we give an algorithm that takes as input a polynomial $Q \in \mathbf{D}[X_1, ..., X_k]$, and computes a description of a roadmap of the set of zeros, $\mathrm{Zer}(Q, \mathbf{R}^k)$, of Q in $\mathbf{R}^k$. The complexity of the algorithm, measured by the number of arithmetic operations in the ordered domain $\mathbf{D}$, is bounded by $D^{O(k\sqrt{k})}$, where $D = \deg(Q) \geq 2$. As a consequence, there exist algorithms for computing the number of semi-algebraically connected components of a real algebraic set, $Z(Q, \mathbf{R}^n)$, whose complexity is also bounded by $D^{O(n\sqrt{n})}$, where $D = \deg(Q) \geq 2$. The best previously known algorithm for constructing a roadmap of a real algebraic subset of $\mathbf{R}^n$ defined by a polynomial of degree D has complexity $D^{O(n^2)}$.

In [36], we provide a probabilistic algorithm which computes roadmaps for smooth and bounded real algebraic sets such that the output size and the running time are polynomial in $(nD)^{n\log(n)}$. More precisely, the running time of the algorithm is essentially subquadratic in the output size. Even under these extra assumptions, it is the first roadmap algorithm with output size and running time polynomial in $(nD)^{n\log(n)}$.

6.3.3. Nearly Optimal Refinement of Real Roots of a Univariate Polynomial

In [33], we consider the following problem. We assume that a real square-free polynomial A has a degree d, a maximum coefficient bitsize τ and a real root lying in an isolating interval and having no nonreal roots nearby (we quantify this assumption). Then we combine the Double Exponential Sieve algorithm (also called the Bisection of the Exponents), the bisection, and Newton iteration to decrease the width of this inclusion interval by a factor of $t = 2^L$. The algorithm has Boolean complexity $O(d^2\tau + dL)$. This substantially decreases the known bound $O(d^3 + d^2L)$. Furthermore we readily extend our algorithm to support the same complexity bound for the refinement of r real roots, for any $r \leq d$, by incorporating the known efficient algorithms for multipoint polynomial evaluation. The main ingredient for the latter ones is an efficient algorithm for (approximate) polynomial division; we present a variation based on structured matrices computation with quasi-optimal Boolean complexity.

6.3.4. Accelerated Approximation of the Complex Roots of a Univariate Polynomial

Highly efficient and even nearly optimal algorithms have been developed for the classical problem of univariate polynomial root-finding, but this is still an area of active research. By combining some powerful techniques developed in this area we devise in [20] new nearly optimal algorithms, whose substantial merit is their simplicity, important for the implementation.

6.3.5. Nearly Optimal Computations with Structured Matrices

In [21], we estimate the Boolean complexity of multiplication of structured matrices by a vector and the solution of nonsingular linear systems of equations with these matrices. We study four basic most popular classes, that is, Toeplitz, Hankel, Cauchy and Vandermonde matrices, for which the cited computational problems are equivalent to the task of polynomial multiplication and division and polynomial and rational multipoint evaluation and interpolation. The Boolean cost estimates for the latter problems have been obtained by Kirrinnis, except for rational interpolation, which we provide now. All known Boolean cost estimates for these problems rely on using Kronecker product. This implies the d-fold precision increase for the d-th degree output, but we avoid such an increase by relying on distinct techniques based on employing FFT. Furthermore we simplify the analysis and make it more transparent by combining the representation of our tasks and

algorithms in terms of both structured matrices and polynomials and rational functions. This also enables further extensions of our estimates to cover Trummer's important problem and computations with the popular classes of structured matrices that generalize the four cited basic matrix classes.

6.3.6. Bounds for the Condition Number for Polynomials with Integer Coefficients

In [31], we consider the problem of bounding the condition number of the roots of univariate polynomials and polynomial systems, when the input polynomials have integer coefficients. We also introduce an aggregate version of the condition numbers and we prove bounds of the same order of magnitude as in the case of the condition number of a single root.

6.4. Solving Systems in Finite Fields, Applications in Cryptology and Algebraic Number Theory

6.4.1. Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case

Let $\mathbf{f} = (f_1, ..., f_m)$ and $\mathbf{g} = (g_1, ..., g_m)$ be two sets of $m \geq 1$ nonlinear polynomials in $\mathbb{K}[x_1, ..., x_n]$ ($\mathbb{K}$ being a field). In [25], we consider the computational problem of finding – if any – an invertible transformation on the variables mapping $\mathbf{f}$ to $\mathbf{g}$. The corresponding equivalence problem is known as *Isomorphism of Polynomials with one Secret* (IP1S) and is a fundamental problem in multivariate cryptography. Amongst its applications, we can cite Graph Isomorphism (GI) which reduces to equivalence of cubic polynomials with respect to an invertible linear change of variables, according to Agrawal and Saxena. The main result of our work is a randomized polynomial-time algorithm for solving IP1S for quadratic instances, a particular case of importance in cryptography.

To this end, we show that IP1S for quadratic polynomials can be reduced to a variant of the classical module isomorphism problem in representation theory. We show that we can essentially *linearize* the problem by reducing quadratic-IP1S to test the orthogonal simultaneous similarity of symmetric matrices; this latter problem was shown by Chistov, Ivanyos and Karpinski (ISSAC 1997) to be equivalent to finding an invertible matrix in the linear space $\mathbb{K}^{n\times n}$ of $n \times n$ matrices over $\mathbb{K}$ and to compute the square root in a certain representation in a matrix algebra. While computing square roots of matrices can be done efficiently using numerical methods, it seems difficult to control the bit complexity of such methods. However, we present exact and polynomial-time algorithms for computing a representation of the square root of a matrix in $\mathbb{K}^{n\times n}$, for various fields (including finite fields), as a product of two matrices. Each coefficient of these matrices lie in an extension field of $\mathbb{K}$ of polynomial degree. We then consider #IP1S, the counting version of IP1S for quadratic instances. In particular, we provide a (complete) characterization of the automorphism group of homogeneous quadratic polynomials. Finally, we also consider the more general *Isomorphism of Polynomials* (IP) problem where we allow an invertible linear transformation on the variables *and* on the set of polynomials. A randomized polynomial-time algorithm for solving IP when $\mathbf{f} = (x_1^d, ..., x_n^d)$ is presented. From an algorithmic point of view, the problem boils down to factoring the determinant of a linear matrix (*i.e.* a matrix whose components are linear polynomials). This extends to IP a result of Kayal obtained for PolyProj.

6.4.2. A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems

In [15], we investigate the security of the family of MQQ public key cryptosystems using multivariate quadratic quasigroups (MQQ). These cryptosystems show especially good performance properties. In particular, the MQQ-SIG signature scheme is the fastest scheme in the ECRYPT benchmarking of cryptographic systems (eBACS). We show that both the signature scheme MQQ-SIG and the encryption scheme MQQ-ENC, although using different types of MQQs, share a common algebraic structure that introduces a weakness in both schemes. We use this weakness to mount a successful polynomial time key-recovery attack. Our key-recovery attack finds an equivalent key using the idea of so-called good keys that reveals the structure gradually. In the process we need to solve a MinRank problem that, because of the structure, can be solved in polynomial-time assuming some mild algebraic assumptions. We highlight that our theoretical results work in characteristic 2

which is known to be the most difficult case to address in theory for MinRank attacks. Also, we emphasize that our attack works without any restriction on the number of polynomials removed from the public-key, that is, using the minus modifier. This was not the case for previous MinRank like-attacks against MQ schemes. From a practical point of view, we are able to break an MQQ-SIG instance of 80 bits security in less than 2 days, and one of the more conservative MQQ-ENC instances of 128 bits security in little bit over 9 days. Altogether, our attack shows that it is very hard to design a secure public key scheme based on an easily invertible MQQ structure.

6.4.3. Algebraic Cryptanalysis of a Quantum Money Scheme – The Noise-Free Case

In [13], we investigate the Hidden Subspace Problem (HSP_q) over $\mathbb{F}_q$:

Input : $p_1, ..., p_m, q_1, ..., q_m \in \mathbb{F}_q[x_1, ..., x_n]$ of degree $d \geq 3$ (and $n \leq m \leq 2n$).
Find : a subspace $A \subset \mathbb{F}_q^n$ of dimension $n/2$ (n is even) such that

$$p_i(A) = 0 \ \forall i \in \{1, ..., m\} \text{ and } q_j(A^\perp) = 0 \ \forall j \in \{1, ..., m\},$$

where $A^\perp$ denotes the orthogonal complement of A with respect to the usual scalar product in $\mathbb{F}_q$.

This problem underlies the security of the first public-key quantum money scheme that is proved to be cryptographically secure under a non quantum but classic hardness assumption. This scheme was proposed by S. Aaronson and P. Christiano at STOC'12. In particular, it depends upon the hardness of HSP_2. More generally, Aaronson and Christiano left as an open problem to study the security of the scheme for a general field $\mathbb{F}_q$. We present a randomized polynomial-time algorithm that solves the HSP_q for $q > 2$ with success probability $\approx 1 - 1/q$. So, the quantum money scheme extended to $\mathbb{F}_q$ is not secure. Finally, based on experimental results and a structural property of the polynomials that we prove, we conjecture that there is also a randomized polynomial-time algorithm solving the HSP_2 with high probability. To support our theoretical results, we also present several experimental results confirming that our algorithms are very efficient in practice. We emphasize that Aaronson and Christiano propose a non-noisy and a noisy version of the public-key quantum money scheme. The noisy version of the quantum money scheme remains secure.

6.4.4. Algebraic Algorithms for LWE Problems

In [23], we analyse the complexity of algebraic algorithms for solving systems of linear equations with *noise*. Such systems arise naturally in the theory of error-correcting codes as well as in computational learning theory. More recently, linear systems with noise have found application in cryptography. The *Learning with Errors* (LWE) problem has proven to be a rich and versatile source of innovative cryptosystems, such as fully homomorphic encryption schemes. Despite the popularity of the LWE problem, the complexity of algorithms for solving it is not very well understood, particularly when variants of the original problem are considered. Here, we focus on and generalise a particular method for solving these systems, due to Arora & Ge, which reduces the problem to non-linear but noise-free system solving. Firstly, we provide a refined complexity analysis for the original Arora-Ge algorithm for LWE. Secondly, we study the complexity of applying algorithms for computing Gröbner basis, a fundamental tool in computational commutative algebra, to solving Arora-Ge-style systems of non-linear equations. We show positive and negative results. On the one hand, we show that the use of Gröbner bases yields an exponential speed-up over the basic Arora-Ge approach. On the other hand, we give a negative answer to the natural question whether the use of such techniques can yield a subexponential algorithm for the LWE problem. Under a mild algebraic assumption, we show that it is highly unlikely that such an improvement exists. We also consider a variant of LWE known as BinaryError-LWE introduced by Micciancio and Peikert recently. By combining Gröbner basis algorithms with the Arora-Ge modelling, we show under a natural algebraic assumption that BinaryError-LWE can be solved in subexponential time as soon as the number of samples is quasi-linear. We also derive precise complexity bounds for BinaryError-LWE with $m = O(n)$, showing that this new approach yields better results than best currently-known generic (exact) CVP solver as soon as $m/n \geq 6.6$. More generally, our results provide a good picture of the hardness degradation of BinaryError-LWE for various number of samples.. This addresses an open question from Micciancio and Peikert. Whilst our results do not contradict

the hardness results obtained by Micciancio and Peikert, they should rule out BinaryError-LWE for many cryptographic applications. The results in this work depend crucially on the assumption the algebraic systems considered systems are not easier and not harder to solve than a random system of equations. We have verified experimentally such hypothesis. We also have been able to prove formally the assumptions is several restricted situations. We emphasize that these issues are highly non-trivial since proving our assumptions in full generality would allow to prove a famous conjecture in commutative algebra known as Fröberg's Conjecture.

6.4.5. Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions

In [10], we investigate the security of a public-key encryption scheme introduced by Huang, Liu and Yang (HLY) at PKC'12. This new scheme can be provably reduced to the hardness of solving a set of quadratic equations whose coefficients of highest degree are chosen according to a discrete Gaussian distributions. The other terms being chosen uniformly at random. Such a problem is a variant of the classical problem of solving a system of non-linear equations (PoSSo), which is known to be hard for random systems. The main hypothesis of Huang, Liu and Yang is that their variant is not easier than solving PoSSo for random instances. In this paper, we disprove this hypothesis. To this end, we exploit the fact that the new problem proposed by Huang, Liu and Yang reduces to an easy instance of the Learning With Errors (LWE) problem. The main contribution of this paper is to show that security and efficiency are essentially incompatible for the HLY proposal. That is, one cannot find parameters which yield a secure and a practical scheme. For instance, we estimate that a public-key of at least 1.03 GB is required to achieve 80-bit security against the simplest of our attacks. As a proof of concept, we present 3 practical attacks against all the parameters proposed by Huang, Liu and Yang. With the most efficient attack, we have been able to recover the private-key in roughly 5 minutes for the first challenge (i.e. Case 1) proposed by HLY and less than 30 minutes for the second challenge (i.e. Case 2).

6.4.6. Lazy Modulus Switching for the BKW Algorithm on LWE

Some recent constructions based on LWE do not sample the secret uniformly at random but rather from some distribution which produces small entries. The most prominent of these is the binary-LWE problem where the secret vector is sampled from $\{0,1\}^*$ or $\{-1,0,1\}^*$. In [9], we present a variant of the BKW algorithm for binary-LWE and other small secret variants and show that this variant reduces the complexity for solving binary-LWE. We also give estimates for the cost of solving binary-LWE instances in this setting and demonstrate the advantage of this BKW variant over standard BKW and lattice reduction techniques applied to the SIS problem. Our variant can be seen as a combination of the BKW algorithm with a lazy variant of modulus switching which might be of independent interest.

In [1], we present a study of the complexity of the Blum-Kalai-Wasserman (BKW) algorithm when applied to the Learning with Errors (LWE) problem, by providing refined estimates for the data and computational effort requirements for solving concrete instances of the LWE problem. We apply this refined analysis to suggested parameters for various LWE-based cryptographic schemes from the literature and compare with alternative approaches based on lattice reduction. As a result, we provide new upper bounds for the concrete hardness of these LWE-based schemes. Rather surprisingly, it appears that BKW algorithm outperforms known estimates for lattice reduction algorithms starting in dimension $n \approx 250$ when LWE is reduced to SIS. However, this assumes access to an unbounded number of LWE samples.

6.4.7. Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form

In [17], we present a new algebraic attack against some special cases of Wild McEliece Incognito, a generalization of the original McEliece cryptosystem. This attack does not threaten the original McEliece cryptosystem. We prove that recovering the secret key for such schemes is equivalent to solving a system of polynomial equations whose solutions have the structure of a usual vector space. Consequently, to recover a basis of this vector space, we can greatly reduce the number of variables in the corresponding algebraic system. From these solutions, we can then deduce the basis of a GRS code. Finally, the last step of the cryptanalysis of those schemes corresponds to attacking a McEliece scheme instantiated with particular GRS codes (with a polynomial relation between the support and the multipliers) which can be done in polynomial-time thanks

to a variant of the Sidelnikov-Shestakov attack. For Wild McEliece & Incognito, we also show that solving the corresponding algebraic system is notably easier in the case of a non-prime base field $\mathbb{F}_q$. To support our theoretical results, we have been able to practically break several parameters defined over a non-prime base field $q \in \{9, 16, 25, 27, 32\}, t < 7$, extension degrees $m \in \{2, 3\}$, security level up to 2^{129} against information set decoding in few minutes or hours.

6.4.8. Folding Alternant and Goppa Codes with Non-Trivial Automorphism Groups

The main practical limitation of the McEliece public-key encryption scheme is probably the size of its key. A famous trend to overcome this issue is to focus on subclasses of alternant/Goppa codes with a non trivial automorphism group. Such codes display then *symmetries* allowing compact parity-check or generator matrices. For instance, a key-reduction is obtained by taking *quasi-cyclic* (QC) or *quasi-dyadic* (QD) alternant/Goppa codes. We show in [6], [18], [28] that the use of such *symmetric* alternant/Goppa codes in cryptography introduces a fundamental weakness. It is indeed possible to reduce the key-recovery on the original symmetric public-code to the key-recovery on a (much) smaller code that has not anymore symmetries. This result is obtained thanks to a new operation on codes called *folding* that exploits the knowledge of the automorphism group. This operation consists in adding the coordinates of codewords which belong to the same orbit under the action of the automorphism group. The advantage is twofold: the reduction factor can be as large as the size of the orbits, and it preserves a fundamental property: folding the dual of an alternant (*resp*. Goppa) code provides the dual of an alternant (*resp*. Goppa) code. A key point is to show that all the existing constructions of alternant/Goppa codes with symmetries follow a common principal of taking codes whose support is globally invariant under the action of affine transformations (by building upon prior works of T. Berger and A. Dür). This enables not only to present a unified view but also to generalize the construction of QC, QD and even *quasi-monoidic* (QM) Goppa codes. All in all, our results can be harnessed to boost up any key-recovery attack on McEliece systems based on symmetric alternant or Goppa codes, and in particular algebraic attacks.

6.4.9. Rounding and Chaining LLL: Finding Faster Small Roots of Univariate Polynomial Congruences

In a seminal work at EUROCRYPT '96, Coppersmith showed how to find all small roots of a univariate polynomial congruence in polynomial time: this has found many applications in public-key cryptanalysis and in a few security proofs. However, the running time of the algorithm is a high-degree polynomial, which limits experiments: the bottleneck is an LLL reduction of a high-dimensional matrix with extra-large coefficients. We present in [11] the first significant speedups over Coppersmith's algorithm. The first speedup is based on a special property of the matrices used by Coppersmith's algorithm, which allows us to provably speed up the LLL reduction by rounding, and which can also be used to improve the complexity analysis of Coppersmith's original algorithm. The exact speedup depends on the LLL algorithm used: for instance, the speedup is asymptotically quadratic in the bit-size of the small-root bound if one uses the Nguyen-Stehlé L2 algorithm. The second speedup is heuristic and applies whenever one wants to enlarge the root size of Coppersmith's algorithm by exhaustive search. Instead of performing several LLL reductions independently, we exploit hidden relationships between these matrices so that the LLL reductions can be somewhat chained to decrease the global running time. When both speedups are combined, the new algorithm is in practice hundreds of times faster for typical parameters.

6.4.10. Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus

Decomposition-based index calculus methods are currently efficient only for elliptic curves E defined over non-prime finite fields of very small extension degree n. This corresponds to the fact that the Semaev summation polynomials, which encode the relation search (or "sieving"), grows over-exponentially with n. Actually, even their computation is a first stumbling block and the largest Semaev polynomial ever computed is the 6-th. Following ideas from Faugère, Gaudry, Huot and Renault, our goal is to use the existence of small order torsion points on E to define new summation polynomials whose symmetrized expressions are much

more compact and easier to compute. This setting allows to consider smaller factor bases, and the high sparsity of the new summation polynomials provides a very efficient decomposition step. In [16], the focus is on 2-torsion points, as it is the most important case in practice. We obtain records of two kinds: we successfully compute up to the 8-th symmetrized summation polynomial and give new timings for the computation of relations with degree 5 extension fields.

6.4.11. Sub-cubic Change of Ordering for Gröner Basis: A Probabilistic Approach

The usual algorithm to solve polynomial systems using Gröbner bases consists of two steps: first computing the DRL Gröbner basis using the F5 algorithm then computing the LEX Gröbner basis using a change of ordering algorithm. When the Bézout bound is reached, the bottleneck of the total solving process is the change of ordering step. For 20 years, thanks to the FGLM algorithm the complexity of change of ordering is known to be cubic in the number of solutions of the system to solve. We show in [14] that, in the generic case or up to a generic linear change of variables, the multiplicative structure of the quotient ring can be computed with no arithmetic operation. Moreover, given this multiplicative structure we propose a change of ordering algorithm for Shape Position ideals whose complexity is polynomial in the number of solutions with exponent ω where $2 \leq \omega < 2.3727$ is the exponent in the complexity of multiplying two dense matrices. As a consequence, we propose a new Las Vegas algorithm for solving polynomial systems with a finite number of solutions by using Gröbner basis for which the change of ordering step has a sub-cubic (i.e. with exponent ω) complexity and whose total complexity is dominated by the complexity of the F5 algorithm. In practice we obtain significant speedups for various polynomial systems by a factor up to 1500 for specific cases and we are now able to tackle some instances that were intractable.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- **ANR Grant (international program) EXACTA (2010-2013): Exact/Certified Algorithms with Algebraic Systems.**
  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 (2010-2013) 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.
- **ANR Grant HPAC: High Performance Algebraic Computing (2012-2016).** The pervasive ubiquity of parallel architectures and memory hierarchy has led to a new quest for parallel mathematical algorithms and software capable of exploiting the various levels of parallelism: from hardware acceleration technologies (multi-core and multi-processor system on chip, GPGPU, FPGA) to cluster and global computing platforms. For giving a greater scope to symbolic and algebraic computing, beyond the optimization of the application itself, the effective use of a large number of resources (memory and specialized computing units) is expected to enhance the performance multi-criteria objectives: time, resource usage, reliability, even energy consumption. The design and the implementation of mathematical algorithms with provable, adaptive and sustainable performance is a major challenge. In this context, this project is devoted to fundamental and practical research specifically in exact linear algebra and system solving that are two essential "dwarfs" (or "killer kernels") in scientific and algebraic computing. The project should lead to progress in matrix algorithms and challenge solving in cryptology, and should provide new insights into high performance programming and library design problems (J.-C. Faugère [contact], L. Perret, G. Renault, M. Safey El Din).

- **ANR Grant GeoLMI: Geometry of Linear Matrix Inequalities (2011-2015).** GeoLMI project aims at developing an algebraic and geometric study of linear matrix inequalities (LMI) for systems control theory. It is an interdisciplinary project at the border between information sciences (systems control), pure mathematics (algebraic geometry) and applied mathematics (optimisation). The project focuses on the geometry of determinantal varieties, on decision problems involving positive polynomials, on computational algorithms for algebraic geometry, on computational algorithms for semi-definite programming, and on applications of algebraic geometry techniques in systems control theory, namely for robust control of linear systems and polynomial optimal control (Participants: J.-C. Faugère, M. Safey El Din [contact], E. Tsigaridas).

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. A3

Type: PEOPLE

Defi:

Instrument: Career Integration Grant

Objectif: NC

Duration: May 2013 - April 2017

Coordinator: Jean-Charles Faugère

Partner: Institut National de Recherche en Informatique et en Automatique (Inria), France

Inria contact: Elias Tsigaridas

Abstract: The project Algebraic Algorithms and Applications (A3) is an interdisciplinary and multidisciplinary project, with strong international synergy. It consists of four work packages The first (Algebraic Algorithms) focuses on fundamental problems of computational (real) algebraic geometry: effective zero bounds, that is estimations for the minimum distance of the roots of a polynomial system from zero, algorithms for solving polynomials and polynomial systems, derivation of non-asymptotic bounds for basic algorithms of real algebraic geometry and application of polynomial system solving techniques in optimization. We propose a novel approach that exploits structure and symmetry, combinatorial properties of high dimensional polytopes and tools from mathematical physics. Despite the great potential of the modern tools from algebraic algorithms, their use requires a combined effort to transfer this technology to specific problems. In the second package (Stochastic Games) we aim to derive optimal algorithms for computing the values of stochastic games, using techniques from real algebraic geometry, and to introduce a whole new arsenal of algebraic tools to computational game theory. The third work package (Non-linear Computational Geometry), we focus on exact computations with implicitly defined plane and space curves. These are challenging problems that commonly arise in geometric modeling and computer aided design, but they also have applications in polynomial optimization. The final work package (Efficient Implementations) describes our plans for complete, robust and efficient implementations of algebraic algorithms.

7.3. International Initiatives

7.3.1. Inria International Labs

We are involved in the ECCA (Exact/Certifed Computation with Algebraic Systems) Team of LIAMA. Our partners are mainly from the Chinese Academy of Sciences and Beihang Univ. Our research focuses mainly on polynomial system solving and its applications.

7.3.2. Inria Associate Teams

7.3.2.1. QOLAPS

Title: Hybrid Methodologies for Quantifier Elimination, Global Optimization, Linear Algebra and Polynomial System Solving

International Partner (Institution - Laboratory - Researcher):

North Carolina State University (ÉTATS-UNIS)

Duration: 2012 - 2014

See also: http://www-polsys.lip6.fr/QOLAPS/index.html

Reliable and certified computing is a major issue in computer science motivated by huge needs in engineering sciences and in the industry (aeronautics, railway transports, etc.). At the same time, the need for high-performance computational routines is constantly increasing. It is tackled on the one hand by designing asymptotically fast algorithms which often have the feature to be randomized and/or approximate and/or probabilistic and on the other hand by developing high performance implementations. Our goal is to conciliate high-performance computing with certification and/or validation issues. We will mainly focus on algebraic problems, and precisely on linear and non-linear systems of equations and/or inequalities. In this context, hybrid methodologies combining exact and numeric computation are traditionally used in two separate ways: either exact computation is used to analyze the robustness of numerical schemes or numerical computation is used to speed up computations. Our viewpoint is to mix these trends in hybrid methodologies by exploiting the scientific continuum from linear algebra to quantifier elimination and global optimization through Grobner bases computations for polynomial system solving.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Éric Schost, Univ. Western Ontario, Canada.

Nitin Saxena, IIT Kanpur, India.

Danilo Gligoroski, NTNU, Norway.

7.4.1.1. Internships

Ivan Bannwarth

Date: Mar 2014 – Aug 2014

Institution: Université de Versailles – Saint-Quentin-en-Yvelines (France)

Matías Bender

Date: Sep 2014 – Feb 2015

Institution: Universidad de Buenos Aires (Argentine)

Anca Nitulescu

Date: Mar 2014 – Aug 2014

Institution: Université Paris Diderot (France)

Ulrick Severin

Date: Sep 2013 – Mar 2014

Institution: Dassault Systèmes (France)

8. Dissemination

8.1. POLSYS seminar

Our seminar hosted over twenty invited speakers in 2014.

http://www-polsys.lip6.fr/Seminar/index.html

8.2. Promoting Scientific Activities

8.2.1. Scientific events organisation

8.2.1.1. member of the organizing committee

Dongming Wang was involved in the organization of the following conferences

- Third International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2014) (Vienna, Austria, July 17-18, 2014).
- Software for Geometry at the 4th International Congress on Mathematical Software (ICMS 2014) (Seoul, Korea, August 5-9, 2014).

8.2.2. Scientific events selection

8.2.2.1. member of the conference program committee

Ludovic Perret was member of the program committee of the following conference:

- Eurocrypt 2014 is the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (11 ? 15 May 2014 Copenhagen, Denmark)

Mohab Safey El Din was member of the program committee of the following conferences:

- 39-th Symposium on Symbolic and Algebraic Computation (ISSAC 2014) (Kobe, Japan, July 23-25, 2014)
- ACM Symbolic-Numeric Computation Conference (SNC 2014) (Shangai, China, July 28-31, 2014)

Jean-Charles Faugère and Ludovic Perret were involved in a special Issue of the Journal Of Symbolic Compuation (JSC) devoted to Mathematical and Computer Algebra Techniques in Cryptology.

Jean-Charles Faugère was member of the program committee of the following conferences:

- 39-th Symposium on Symbolic and Algebraic Computation (ISSAC 2014) (Kobe, Japan, July 23-25, 2014)
- The IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'2015)
- The thirteenth conference MEGA (University of Trento, Italy)

Elias Tsigaridas was member of the program committee of the following conferences:

- ACM Symbolic-Numeric Computation Conference (SNC 2014) (Shangai, China, July 28-31, 2014)

Dongming Wang was member of the program committes of the following conferences

- 6th International Symposium on Symbolic Computation in Software Science (SCSS 2014) (Gammarth, Tunisia, December 7-11, 2014),
- 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2014) (Timisoara, Romania, September 22-25, 2014),
- 12th International Conference on Artificial Intelligence and Symbolic Computation (AISC 2014) (Sevilla, Spain, December 11-13, 2014),
- 10th International Workshop on Automated Deduction in Geometry (ADG 2014) (Coimbra, Portugal, July 9-11, 2014).

8.2.3. Journal

8.2.3.1. member of the editorial board

Ludovic Perret is member of the editorial board of Designs, Codes and Cryptography published by Springer.

Mohab Safey El Din is member of the editorial board of Journal of Symbolic Computation (published by Academic Press/Elsevier, London).

Dongming Wang has the following editorial activities:

- Editor-in-Chief and Managing Editor for the journal
  Mathematics in Computer Science (published by Birkhäuser/Springer, Basel).
- Executive Associate Editor-in-Chief for the journal
  SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).
- Member of the Editorial Boards for the
  - Journal of Symbolic Computation (published by Academic Press/Elsevier, London),
  - Frontiers of Computer Science (published by Higher Education Press, Beijing and Springer, Berlin),
  - Texts and Monographs in Symbolic Computation (published by Springer, Wien New York),
  - Book Series on Mathematics Mechanization (published by Science Press, Beijing),
  - Book Series on Fundamentals of Information Science and Technology (published by Science Press, Beijing).
- Member of the International Advisory Board for the Communications of JSSAC (Japan Society for Symbolic and Algebraic Computation) (published by JSSAC).
- Editor for the Book Series in Computational Science (published by Tsinghua University Press, Beijing).

8.2.4. Invited Talks

Jean-Charles Faugère was invited talk at:

- Workshop on Polynomials over Finite Fields - Barcelona - Centre de Recerca Matemàtica (CRM) - Spain
- Computational Nonlinear Algebra - Computational Nonlinear Algebra (ICERM) - Providence - USA
- Main lecture - Journées Nationales de Calcul Formel

Guénaël Renault was invited speaker for the following international conferences:

- Espaces de modules effectifs et application à la cryptographie (June 10-13, 2014, Rennes, France)
- 18th Workshop On Elliptic Curve Cryptography (October 8-10, 2014, Chennai, India)

Mohab Safey El Din was invited talk at:

- Workshop *Solving Polynomial Equations* as part of the *Algorithms and Complexity in Algebraic Geometry* program, Simons Institute, Berkeley, Oct. 2014.
- Special track on *Algebraic techniques in polynomial optimization*, IFORS, Barcelona, Spain, July, 2014.
- *Real Algebraic Geometry With A View Toward Systems Control and Free Positivity*, Oberwolfach, Germany, April, 2014.

8.3. Teaching - Supervision - Juries

8.3.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 54 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : Algèbre linéaire et applications, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : Introduction à la Sécurité, 32 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction au Calcul Scientifique, 40 heures équivalent TD, niveau L2, Université Pierre-et-Marie-Curie, France

Jean-Charles Faugère had the following teaching activities:

Master : Résolution de systèmes polynomiaux, 12 heures équivalent TD, niveau M2, MPRI

Ludovic Perret had the following teaching activities:

Master : Résolution de systèmes polynomiaux, 12 heures équivalent TD, niveau M2, MPRI

Master : Responsable Introduction à la sécurité, 96 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : Responsable Complexité, 48 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction à l'Algorithmique, niveau L2, Université Pierre-et-Marie-Curie, France

Licence : Responsable en L2 du parcours informatique-mathématiques appliquées (PIMA), niveau L2, Université Pierre-et-Marie-Curie, France

Guénaël Renault had the following teaching activities:

Master : Co-responsable de la spécialité SFPN du master d'informatique, Université Pierre-et-Marie-Curie, France

Master : Responsable Cryptologie Avancée et Appliquée, 50 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : Responsable Sécurité et Canaux Auxiliaires, 12 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : Responsable Modélisation des attaques et des menaces, 25 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : Responsable Algèbre linéaire et applications, 25 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Responsable Introduction à la cryptologie, 40 heures équivalent TD, niveau L3, Université Pierre-et-Marie-Curie, France

Mohab Safey El Din had the following teaching activities:

Master : Résolution de systèmes polynomiaux, 30 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 21 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction à la Cryptologie, 20 heures équivalent TD, niveau L3, Université Pierre-et-Marie-Curie, France

8.3.2. Supervision

PhD : Jules Svartz, Résolution de Systèmes polynomiaux structurés de Dimension zéro, Université Pierre-et-Marie-Curie (Univ. Paris 6), 30 Oct. 2014, Jean-Charles Faugère

PhD in progress : Ivan Bannwarth, Fast algorithms for studying real algebraic sets, Sept. 2014, Mohab Safey El Din

PhD in progress : Simone Naldi, Exact algorithms for rank defects in linear matrices, Sept. 2012, Didier Henrion and Mohab Safey El Din

PhD in progress : Fréderic Urvoy de Portzamparc, Algebraic Cryptanalysis and Physical Attacks in Code-Based Cryptography, Fev. 2012, Jean-Charles Faugère and Ludovic Perret

PhD in progress : Thibaut Verron, Gröbner bases and structured polynomial systems, Sept. 2012, Jean-Charles Faugère and Mohab Safey El Din

PhD in progress : Rina Zeitoun, Coppersmith's Algorithm and Applications in Cryptology, Jan. 2011, Jean-Charles Faugère and Guénaël Renault

8.3.3. Juries

Jen-Charles Faugère

member of the HDR committee of Guillaume Chèze

member of the HDR committee of Frederic Chyzac

member of the HDR committee of Clement Pernet

member of the PhD committee of Ruixian Renaud as the president of the committee.

member of the PhD committee of Jules Svartz as a an examiner.

Mohab Safey El Din was:

member of the PhD committee of Marta Abril Buccerro as a reviewer;

member of the PhD committee of Pierre Lairez as a reviewer;

member of the PhD committee of Jules Svartz as a an examiner.

member of the PhD committee of Sébastien Tavenas as a reviewer;

8.4. Popularization

Guénaël Renault was invited speaker for the workshop *Fabriquer le Hazard du forum Science, Recherche et Société* (May 22, 2014) organized by the newspapers Le Monde et La Recherche.

9. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] M. ALBRECHT, C. CID, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *On the complexity of the BKW algorithm on LWE*, in "Designs, Codes and Cryptography", February 2015, vol. 74, n° 2, 26 p. [*DOI :* 10.1007/s10623-013-9864-x], https://hal.inria.fr/hal-00921517

[2] B. BANK, M. GIUSTI, J. HEINTZ, M. SAFEY EL DIN. *Intrinsic complexity estimates in polynomial optimization*, in "Journal of Complexity", February 2014, vol. 30, n° 4, pp. 430-443 [*DOI :* 10.1016/j.jco.2014.02.005], https://hal.inria.fr/hal-00815123

[3] M. BARDET, J.-C. FAUGÈRE, B. SALVY. *On the complexity of the F5 Gröbner basis algorithm*, in "Journal of Symbolic Computation", September 2014, pp. 1-24 [*DOI :* 10.1016/J.JSC.2014.09.025], https://hal.inria.fr/hal-01064519

[4] S. BASU, M.-F. ROY, M. SAFEY EL DIN, E. SCHOST. *A Baby Step–Giant Step Roadmap Algorithm for General Algebraic Sets*, in "Foundations of Computational Mathematics", 2014, vol. 14, n° 6, pp. 1117 - 1172 [*DOI :* 10.1007/S10208-014-9212-1], https://hal.inria.fr/hal-01096209

[5] J. C. COSTELLO, L. M. HEISER, E. GEORGII, M. GÖNEN, M. P. MENDEN, N. J. WANG, M. BANSAL, M. AMMAD-UD-DIN, P. HINTSANEN, S. A. KHAN, J.-P. MPINDI, O. KALLIONIEMI, A. HONKELA, T. AITTOKALLIO, K. WENNERBERG, J.-P. ABBUEHL, J. ALLEN, R. B. ALTMAN, S. BALCOME, A. BATTLE, A. BENDER, B. BERGER, J. BERNARD, M. BHATTACHARJEE, K. BHUVANESHWAR, A. A. BIEBERICH, F. BOEHM, A. CALIFANO, C. CHAN, B. CHEN, T.-H. CHEN, J. CHOI, L. P. COELHO, T. COKELAER, J. C. COLLINS, C. J. CREIGHTON, J. CUI, W. DAMPIER, V. J. DAVISSON, B. D. BAETS, R. DESHPANDE, B. DICAMILLO, M. DUNDAR, Z. DUREN, A. ERTEL, H. FAN, H. FANG, D. GALLAHAN, R. GAUBA, A. GOTTLIEB, M. GRAU, J. W. GRAY, Y. GUSEV, M. J. HA, L. HAN, M. HARRIS, N. HENDERSON, H. A. HEJASE, K. HOMICSKO, J. P. HOU, W. HWANG, A. P. IJZERMAN, B. KARACALI, S. KASKI, S. KELES, C. KENDZIORSKI, J. KIM, M. KIM, Y. KIM, D. A. KNOWLES, D. KOLLER, J. LEE, J. K. LEE, E. B. LENSELINK, B. LI, B. LI, J. LI, H. LIANG, J. MA, S. MADHAVAN, S. MOONEY, C. L. MYERS, M. A. NEWTON, J. P. OVERINGTON, R. PAL, J. PENG, R. PESTELL, R. J. PRILL, P. QIU, B. RAJWA, A. SADANANDAM, J. SAEZ-RODRIGUEZ, F. SAMBO, H. SHIN, D. SINGER, J. SONG, L. SONG, A. SRIDHAR, M. STOCK, G. STOLOVITZKY, W. SUN, T. TA, M. TADESSE, M. TAN, H. TANG, D. THEODORESCU, G. M. TOFFOLO, A. TOZEREN, W. TREPICCHIO, N. VAROQUAUX, J.-P. VERT, W. WAEGEMAN, T. WALTER, Q. WAN, D. WANG, W. WANG, Y. WANG, Z. WANG, J. K. WEGNER, T. WU, T. XIA, G. XIAO, Y. XIE, Y. XU, J. YANG, Y. YUAN, S. ZHANG, X.-S. ZHANG, J. ZHAO, C. ZUO, H. W. T. V. VLIJMEN, G. J. P. V. WESTEN, J. J. COLLINS. *A community effort to assess and improve drug sensitivity prediction algorithms*, in "Nature Biotechnology", 2014, vol. 32, pp. 1202-1212 [*DOI :* 10.1038/NBT.2877], https://hal-mines-paristech.archives-ouvertes.fr/hal-01101874

[6] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, F. DE PORTZAMPARC, J.-P. TILLICH. *Structural Cryptanalysis of McEliece Schemes with Compact Keys*, in "Designs, Codes and Cryptography", January 2015, 26 p. , https://hal.inria.fr/hal-00964265

[7] A. GREUET, M. SAFEY EL DIN. *Probabilistic Algorithm for Polynomial Optimization over a Real Algebraic Set*, in "SIAM Journal on Optimization", August 2014, vol. 24, n° 3, pp. 1313-1343 [*DOI :* 10.1137/130931308], https://hal.archives-ouvertes.fr/hal-00849523

[8] X. LI, D. WANG. *Computing equilibria of semi-algebraic economies using triangular decomposition and real solution classification*, in "Journal of Mathematical Economics", 2014, vol. 54, pp. 48-58 [*DOI :* 10.1016/J.JMATECO.2014.08.007], https://hal.inria.fr/hal-01092169

International Conferences with Proceedings

[9] M. ALBRECHT, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *Lazy Modulus Switching for the BKW Algorithm on LWE*, in "Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography", Buenos Aires, Argentina, Springer, March 2014, https://hal.inria.fr/hal-00925187

[10] M. ALBRECHT, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET, Y. TODO, K. XAGAWA. *Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions*, in "PKC

2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography", Buenos Aires, Argentina, Springer, March 2014, https://hal.inria.fr/hal-00932382

[11] J. BI, J.-S. CORON, J.-C. FAUGÈRE, P. Q. NGUYEN, G. RENAULT, R. ZEITOUN. *Rounding and Chaining LLL: Finding Faster Small Roots of Univariate Polynomial Congruences*, in "PKC 2014 - 17th IACR International Conference on Practice and Theory of Public-Key Cryptography", Buenos Aires, Argentina, H. KRAWCZYK (editor), Springer, March 2014, vol. 8383, pp. 185-202 [*DOI :* 10.1007/978-3-642-54631-0_11], https://hal.inria.fr/hal-00926902

[12] A. BOSTAN, T. COMBOT, M. SAFEY EL DIN. *Computing necessary integrability conditions for planar parametrized homogeneous potentials*, in "ISSAC'14 - International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, ACM Press, July 2014 [*DOI :* 10.1145/2608628.2608662], https://hal.inria.fr/hal-00994116

[13] M. CONDE PENA, J.-C. FAUGÈRE, L. PERRET. *Algebraic Cryptanalysis of a Quantum Money Scheme The Noise-Free Case*, in "IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15)", Maryland, United States, March 2015, https://hal.inria.fr/hal-01098223

[14] J.-C. FAUGÈRE, P. GAUDRY, L. HUOT, G. RENAULT. *Sub-cubic Change of Ordering for Gröner Basis: A Probabilistic Approach*, in "ISSAC '14 - Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, ISSAC '14, ACM, July 2014, pp. 170–177 [*DOI :* 10.1145/2608628.2608669], https://hal.inria.fr/hal-01064551

[15] J.-C. FAUGÈRE, D. GLIGOROSKI, L. PERRET, S. SIMONA, E. THOMAE. *A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems*, in "IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15)", Maryland, United States, March 2015, https://hal.inria.fr/hal-01074194

[16] J.-C. FAUGÈRE, L. HUOT, A. JOUX, G. RENAULT, V. VITSE. *Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus*, in "EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques", Copenhagen, Denmark, May 2014 [*DOI :* 10.1007/978-3-642-55220-5_3], https://hal.inria.fr/hal-00935050

[17] J.-C. FAUGÈRE, L. PERRET, F. DE PORTZAMPARC. *Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form*, in "Advances in Cryptology Asiacrypt 2014", Kaohsiung, Taiwan, December 2014 [*DOI :* 10.1007/978-3-662-45611-8_2], https://hal.inria.fr/hal-01064687

[18] J.-C. FAUGÈRE, L. PERRET, F. DE PORTZAMPARC, A. OTMANI, J.-P. TILLICH. *Structural weakness of compact variants of the McEliece cryptosystem*, in "IEEE International Symposium on Information Theory - ISIT 2014", Honolulu, United States, June 2014, pp. 1717-1721, https://hal.archives-ouvertes.fr/hal-01096180

[19] J.-C. FAUGÈRE, P.-J. SPAENLEHAUER, J. SVARTZ. *Sparse Gröbner Bases: the Unmixed Case*, in "ISSAC 2014", Kobe, Japan, July 2014, 20 pages, Corollary 6.1 has been corrected [*DOI :* 10.1145/2608628.2608663], https://hal.archives-ouvertes.fr/hal-00953501

[20] V. Y. PAN, E. TSIGARIDAS. *Accelerated Approximation of the Complex Roots of a Univariate Polynomial (Extended Abstract)*, in "Proceedings of the 2014 Symposium on Symbolic-Numeric Computation", Shanghai, China, ACM, July 2014, pp. 132-134 [*DOI :* 10.1145/2631948.2631973], https://hal.inria.fr/hal-00980584

[21] V. Y. PAN, E. TSIGARIDAS. *Nearly Optimal Computations with Structured Matrices*, in "Proceedings of the 2014 Symposium on Symbolic-Numeric Computation", Shanghai, China, July 2014, pp. 21-30 [*DOI :* 10.1145/2631948.2631954], https://hal.inria.fr/hal-00980591

[22] J. YANG, D. WANG, H. HONG. *ImUp: A Maple Package for Uniformity-Improved Reparameterization of Plane Curves*, in "10th Asian Symposium on Computer Mathematics", Beijing, China, Computer Mathematics, Springer, October 2014, pp. 437-451 [*DOI :* 10.1007/978-3-662-43799-5_29], https://hal.inria.fr/hal-01092141

Other Publications

[23] M. ALBRECHT, C. CID, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *Algebraic Algorithms for LWE Problems*, October 2014, https://hal.inria.fr/hal-01072721

[24] M. ALBRECHT, J.-C. FAUGÈRE, R. FITZPATRICK, L. PERRET. *Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions*, January 2014, https://hal.inria.fr/hal-00918314

[25] J. BERTHOMIEU, J.-C. FAUGÈRE, L. PERRET. *Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case*, April 2014, https://hal.inria.fr/hal-00846041

[26] C. EDER, J.-C. FAUGÈRE. *A survey on signature-based Gröbner basis computations*, April 2014, https://hal.inria.fr/hal-00974810

[27] I. EMIRIS, B. MOURRAIN, E. TSIGARIDAS. *Separation bounds for polynomial systems*, January 2015, https://hal.inria.fr/hal-01105276

[28] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, F. DE PORTZAMPARC, J.-P. TILLICH. *Folding Alternant and Goppa Codes with Non-Trivial Automorphism Groups*, May 2014, forthcoming, https://hal.inria.fr/hal-00992389

[29] J.-C. FAUGÈRE, M. SAFEY EL DIN, T. VERRON. *On the complexity of computing Gröbner bases for weighted homogeneous systems*, December 2014, https://hal.inria.fr/hal-01097316

[30] D. HENRION, S. NALDI, M. SAFEY EL DIN. *Real root finding for determinants of linear matrices*, October 2014, Typos corrected, section 4 rewritten, https://hal.archives-ouvertes.fr/hal-01077888

[31] A. HERMAN, E. TSIGARIDAS. *Bounds for the Condition Number for Polynomials with Integer Coefficients*, December 2014, https://hal.inria.fr/hal-01098981

[32] V. Y. PAN, E. TSIGARIDAS, Z. LIANG. *Simple and Efficient Real Root-finding for a Univariate Polynomial*, January 2015, https://hal.inria.fr/hal-01105309

[33] V. Y. PAN, E. TSIGARIDAS. *Nearly Optimal Refinement of Real Roots of a Univariate Polynomial*, 2014, https://hal.inria.fr/hal-00960896

[34] V. Y. PAN, E. TSIGARIDAS. *Accelerated approximation of the complex roots of a univariate polynomial*, January 2015 [*DOI :* 10.1145/2631948.2631973], https://hal.inria.fr/hal-01105267

[35] V. Y. PAN, E. TSIGARIDAS. *Nearly optimal computations with structured matrices*, January 2015 [*DOI :* 10.1145/2631948.2631954], https://hal.inria.fr/hal-01105263

[36] M. SAFEY EL DIN, E. SCHOST. *A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets*, December 2014, https://hal.inria.fr/hal-00849057