IN PARTNERSHIP WITH:
CNRS

Sorbonne Université (UPMC)

Université Denis Diderot (Paris 7)

Activity Report 2019

Project-Team OURAGAN

Tools for resolutions in algebra, geometry and their applications

IN COLLABORATION WITH: Institut de Mathématiques de Jussieu

RESEARCH CENTER
Paris

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team OURAGAN

Creation of the Team: 2012 January 01, updated into Project-Team: 2019 May 01

Keywords:

Computer Science and Digital Science:

A4.3. - Cryptography
A4.3.1. - Public key cryptography
A4.3.2. - Secret key cryptography
A4.3.3. - Cryptographic protocols
A4.3.4. - Quantum Cryptography
A7.1. - Algorithms
A7.1.4. - Quantum algorithms
A8.1. - Discrete mathematics, combinatorics
A8.3. - Geometry, Topology
A8.4. - Computer Algebra
A8.5. - Number theory
A8.10. - Computer arithmetic

Other Research Topics and Application Domains:

B5.6. - Robotic systems
B9.5.1. - Computer science
B9.5.2. - Mathematics

1. Team, Visitors, External Collaborators

Research Scientists

Fabrice Rouillier [Team leader, Inria, Senior Researcher, HDR]
Mohamed Yacine Bouzidi [Inria, Starting Research Position]
Alban Quadrat [Inria, Senior Researcher, HDR]
Robin Timsit [Univ Pierre et Marie Curie, Researcher, until Sep 2019]
Elias Tsigaridas [Inria, Researcher, from Sep 2019]

Faculty Members

Jean Bajard [Univ Pierre et Marie Curie, Professor, from Sep 2019]
Elisha Falbel [Univ Pierre et Marie Curie, Professor]
Antonin Guilloux [Univ Pierre et Marie Curie, Associate Professor, HDR]
Antoine Joux [Univ Pierre et Marie Curie, Associate Professor, HDR]
Pierre-Vincent Koseleff [Univ Pierre et Marie Curie, Associate Professor, HDR]
Pascal Molin [Univ Denis Diderot, Associate Professor]

PhD Students

Christina Katsamaki [Inria, PhD Student, from Oct 2019]
Mahya Mehrabdollahei [Inria, PhD Student]
Sudarshan Shinde [Univ Pierre et Marie Curie, PhD Student, until Sep 2019]
Grace Younes [Inria, PhD Student]

Administrative Assistants

Laurence Bourcier [Inria, Administrative Assistant]

Maryse Desnous [Inria, Administrative Assistant, until Apr 2019]
Julien Guieu [Inria, Administrative Assistant, from Apr 2019]

Visiting Scientist
Thomas Espitau [Univ de Nanterre, Sep 2019]

External Collaborator
Razvan Barbulescu [CNRS, until Aug 2019]

2. Overall Objectives

2.1. Overall Objectives

OURAGAN proposes to focus on the transfer of computational algebraic methods to some related fields (computational geometry, topology, number theory, etc.) and some carefully chosen application domains (robotics, control theory, evaluation of the security of cryptographic systems, etc.), which implies working equally on the use (modeling, know - how) and on the development of new algorithms. The latest breakthrough developments and applications where algebraic methods are currently decisive remain few and very targeted. We wish to contribute to increase the impact of these methods but also the number of domains where the use of computational algebraic methods represent a significant added value. This transfer-oriented positioning does not imply to stop working on the algorithms, it simply sets the priorities.

An original aspect of the OURAGAN proposal is to blend into an environment of fundamental mathematics, at the Institut de Mathématiques de Jussieu – Paris Rive Gauche (IMJ-PRG CNRS 7586), and to be cross-functional to several teams (Algebraic Analysis, Complex Analysis and Geometry, Number Theory to name only the main ones), which will be our first source of transfer of computational know-how. The success of this coupling allows to maintain a strong theoretical basis and to measure objectively our transfer activity in the direction of mathematicians (in geometry, topology, number theory, algebraic analysis, etc.) and to consolidate the presence of Inria in scientific areas among the most theoretical.

We propose three general directions with five particular targets:

- Number Theory
  - Algorithmic Number Theory
  - Rigorous Numerical Computations
- Topology in small dimension
  - Character varieties
  - Knot theory
  - Computational geometry
- Algebraic analysis of functional systems

These actions come, of course, in addition to the study and development of a common set of core elements of

- Basic theory and algorithms in algebra and geometry [Transverse activity].

This core activity is the invention and study of fundamental algebraic algorithms and objects that can be grouped into 2 categories: algorithms designed to operate on finite fields and algorithms running on fields of characteristic 0; with 2 types of computational strategies: the exactness and the use of approximate arithmetic (but with exact results). This mix also installs joint studies between the various axes and is an originality of the project-team. For example many kinds of arithmetic tools around algebraic numbers have to face to similar theoretical problems such as finding a good representation for a number field; almost all problems related to the resolution of algebraic systems will reduce to the study of varieties in small dimension and in particular, most of the time, to the effective computation of the topology of curves and surfaces, or the certified drawing of non algebraic function over an algebraic variety.

The tools and objects developed for research on algorithmic number theory as well as in computational geometry apply quite directly on some selected connected challenging subjects:

- Security of cryptographic systems
- Control theory
- Robotics
- Signal processing

These applications will serve for the evaluation of the general tools we develop when used in a different context, in particular their capability to tackle state of the art problems.

2.2. Scientific ground

2.2.1. Basic computable objects and algorithms

The basic computable objects and algorithms we study, use, optimize or develop are among the most classical ones in computer algebra and are studied by many people around the world: they mainly focus on basic computer arithmetic, linear algebra, lattices, and both polynomial system and differential system solving.

In the context of OURAGAN, it is important to avoid reinventing the wheel and to re-use wherever possible existing objects and algorithms, not necessarily developed in our team so that the main effort is focused on finding good formulations/modelisations for an efficient use. Also, our approach for the development of basic computable objects and algorithms is *application driven* and follows a simple strategy : use the existing tools in priority, develop missing tools when required and then optimize the critical operations. First, for some selected problems, we do propose and develop general key algorithms (isolation of real roots of univariate polynomials, parametrisations of solutions of zero-dimensional polynomial systems, solutions of parametric equations, equidimensional decompositions, etc.) in order to complement the existing set computable objects developed and studied around the world (Gröbner bases, resultants [64], subresultants [85], critical point methods [41], etc.) which are also deeply used in our developments. Second, for a selection of well-known problems, we propose different computational strategies (for example the use of approximate arithmetic to speed up LLL algorithm or root isolators, still certifying the final result). Last, we propose specialized variants of known algorithms optimized for a given problem (for example, dedicated solvers for degenerated bivariate polynomials to be used in the computation of the topology of plane curves).

In the activity of OURAGAN, many key objects or algorithms around the resolution of algebraic systems are developed or optimized within the team, such as the resolution of polynomials in one variable with real coefficients [105] [14], rational parameterizations of solutions of zero-dimensional systems with rational coefficients [49] [13] or discriminant varieties for solving systems depending on parameters [11], but we are also power users of existing software (mainly Sage [1], Maple [2], Pari-GP [3],Snappea [4]) and libraries (mainly gmp [5], mpfr [6], flint [7], arb [8], etc.) to which we contribute when it makes sense.

For our studies in number theory and applications to the security of cryptographic systems, our team works on three categories of basic algorithms: discrete logarithm computations [99] (for example to make progress on the computation of class groups in number fields [90]), network reductions by means of LLL variants [75] and, obviously, various computations in linear algebra, for example dedicated to *almost sparse* matrices [100].

Finally, for the algorithmic approach to algebraic analysis of functional equations [45] [103] [104], we developed the effective study of both module theory and homological algebra [136] over certain noncommutative polynomial rings of functional operators [4], of Stafford's famous theorems on the Weyl algebras [127], of the equidimensional decomposition of functional systems [122], etc.

[1] http://www.sagemath.org/
[2] https://maplesoft.com
[3] https://pari.math.u-bordeaux.fr
[4] http://www.geometrygames.org/SnapPea/
[5] https://gmplib.org/
[6] https://www.mpfr.org/
[7] http://www.flintlib.org/
[8] http://arblib.org/

2.2.2. Computational Number Theory

Many frontiers between computable objects, algorithms (above section), computational number theory and applications, especially in cryptography are porous. However, one can classify our work in computational number theory into two classes of studies : computational algebraic number theory and (rigorous) numerical computations in number theory.

Our work on rigorous numerical computations is somehow a transverse activity in Ouragan : floating point arithmetic is used in many basic algorithms we develop (root isolation, LLL) and is thus present in almost all our research directions. However there are specific developments that could be labelized *Number Theory*, in particular contributions to numerical evaluations of L-functions which are deeply used in many problems in number theory (for example the Riemann Zeta function). We participate, for example to the *L-functions and Modular Forms Database* [9] a world wide collaborative project.

Our work in computational algebraic number theory is driven by the algorithmic improvement to solve presumably hard problems relevant to cryptography. The use of number-theoretic hard problems in cryptography dates back to the invention of public-key cryptography by Diffie and Hellman [71], where they proposed a first instantiation of their paradigm based on the discrete logarithm problem in prime fields. The invention of RSA [134], based on the hardness of factoring came as a second example. The introduction of discrete logarithms on elliptic curves [106] [116] only confirmed this trend.

These crypto-systems attracted a lot of interest on the problems of factoring and discrete log. Their study led to the invention of fascinating new algorithms that can solve the problems much faster than initially expected :

- the elliptic curve method (ECM) [101]
- the quadratic field for factoring [120] and its variant for discrete log called the Gaussian integers method [114]
- the number field sieve (NFS) [39]

Since the invention of NFS in the 90's, many optimizations of this algorithm have been performed. However, an algorithm with better complexity hasn't been found for factoring and discrete logarithms in large characteristic.

While factorization and discrete logarithm problems have a long history in cryptography, the recent post-quantum cryptosystems introduce a new variety of presumably hard problems/objects/algorithms with cryptographic relevance: the shortest vector problem (SVP), the closest vector problem (CVP) or the computation of isogenies between elliptic curves, especially in the supersingular case.

Members of OURAGAN started working on the topic of discrete logarithms around 1998, with several computation records that were announced on the *NMBRTHRY* mailing list. In large characteristic, especially for the case of prime fields, the best current method is the number field sieve (NFS) algorithm. In particular, they published the first NFS based record computation[10]. Despite huge practical improvements, the prime field case algorithm hasn't really changed since that first record. Around the same time, we also presented small characteristic computation record based on simplifications of the Function Field Sieve (FFS) algorithm [98].

In 2006, important changes occurred concerning the FFS and NFS algorithms, indeed, while the algorithms only covered the extreme case of constant characteristic and constant extension degree, two papers extended their ranges of applicability to all finite fields. At the same time, this permitted a big simplification of the FFS, removing the need for function fields.

Starting from 2012, new results appeared in small characteristic. Initially based on a simplification of the 2006 result, they quickly blossomed into the Frobenial representation methods, with quasi-polynomial time complexity [99], [91].

An interesting side-effect of this research was the need to revisit the key sizes of pairing-based cryptography. This type of cryptography is also a topic of interest for OURAGAN. In particular, it was introduced in 2000 [9].

[9] http://www.lmfdb.org

The computations of *class groups in number fields* has strong links with the computations of discrete logarithms or factorizations using the NFS (number field sieve) strategy which as the name suggests is based on the use of number fields. Roughly speaking, the NFS algorithm uses two number fields and the strategy consists in choosing number fields with small sized coefficients in their definition polynomials. On the contrary, in class group computations, there is a single number field, which is clearly a simplification, but this field is given as input by some fixed definition polynomial. Obviously, the degree of this polynomial as well as the size of its coefficients are both influencing the complexity of the computations so that finding other polynomials representing the same class group but with a better characterization (degree or coefficient's sizes) is a mathematical problem with direct practical consequences. We proposed a method to address the problem [90], but many issues remain open.

Computing generators of principal ideals of cyclotomic fields is also strongly related to the computation of class groups in number fields. Ideals in cyclotomic fields are used in a number of recent public-key cryptosystems. Among the difficult problems that ensure the safety of these systems, there is one that consists in finding a small generator, if it exists, of an ideal. The case of cyclotomic fields is considered [44].

2.2.3. Topology in small dimension

2.2.3.1. Character varieties

There is a tradition of using computations and software to study and understand the topology of small dimensional manifolds, going back at least to Thurston's works (and before him, Riley's pioneering work). The underlying philosophy of these tools is to build combinatorial models of manifolds (for example, the torus is often described as a square with an identification of the sides). For dimensions 2, 3 and 4, this approach is relevant and effective. In the team OURAGAN, we focus on the dimension 3, where the manifolds are modelized by a finite number of tetrahedra with identification of the faces. The software SnapPy [10] implements this strategy [139] and is regularly used as a starting point in our work. Along the same philosophy of implementation, we can also cite Regina [11]. A specific trait of SnapPy is that it focuses on hyperbolic structures on the 3-dimensional manifolds. This setting is the object of a huge amount of theoretical work that were used to speed up computations. For example, some Newton methods were implemented without certification for solving a system of equations, but the theoretical knowledge of the uniqueness of the solution made this implementation efficient enough for the target applications. In recent years, in part under the influence of our team [12], more attention has been given to certified computations (at least with an error control) and now this is implemented in SnapPy.

This philosophy (modelization of manifolds by quite simple combinatoric models to compute such complicated objects as representations of the fundamental group) was applied in a pioneering work of Falbel [8] when he begins to look for another type of geometry on 3-dimensional manifolds (called CR-spherical geometry). From a computational point of view, this change of objectives was a jump in the unknown: the theoretical justification for the computations were missing, and the number of variables of the systems were multiplied by four. So instead of a relatively small system that could be tackled by Newton methods and numerical approximations, we had to deal with/study (were in front of) relatively big systems (the smallest example being 8 variables of degree 6) with no a priori description of the solutions.

Still, the computable objects that appear from the theoretical study are very often outside the reach of automated computations and are to be handled case by case. A few experts around the world have been tackling this kind of computations (Dunfield, Goerner, Heusener, Porti, Tillman, Zickert) and the main current achievement is the *Ptolemy module* [13] for SnapPy.

From these early computational needs, topology in small dimension has historically been the source of collaboration with the IMJ-PRG laboratory. At the beginning, the goal was essentially to provide computational tools for finding geometric structures in triangulated 3-dimensional varieties. Triangulated varieties can be

[10] https://www.math.uic.edu/t3m/SnapPy/
[11] https://regina-normal.github.io
[12] as part of the CURVE project
[13] https://www.math.uic.edu/t3m/SnapPy/ptolemy.html

topologically encoded by a collection of tetrahedra with gluing constraints (this can be called a triangulation or mesh, but it is not an approximation of the variety by simple structures, rather a combinatorial model). Imposing a geometric structure on this combinatorial object defines a number of constraints that we can translate into an algebraic system that we then have to solve to study geometric structures of the initial variety, for example in relying on solutions to study representations of the fundamental group of the variety. For these studies, a large part of the computable objects or algorithms we develop are required, from the algorithms for univariate polynomials to systems depending on parameters. It should be noted that most of the computational work lies in the modeling of problems [43][7] that have strictly no chance to be solved by blindly running the most powerful black boxes: we usually deal here with systems that have 24 to 64 variables, depend on 4 to 8 parameters and with degrees exceeding 10 in each variable. With an ANR [14] funding on the subject, the progress that we did [79] were (much) more significant than expected. In particular, we have introduced new computable objects with an immediate theoretical meaning (let us say rather with a theoretical link established with the usual objects of the domain), namely, the so-called *deformation variety*.

2.2.3.2. Knot theory

Knot theory is a wide area of mathematics. We are interested in polynomial representations of long knots, that is to say polynomial embeddings $\mathbf{R} \to \mathbf{R}^3 \subset \mathbf{S}^3$. Every knot admits a polynomial representation and a natural question is to determine explicit parameterizations, minimal degree parameterizations. On the other hand we are interested to determine what is the knot of a given polynomial smooth embedding $\mathbf{R} \to \mathbf{R}^3$. These questions involve real algebraic curves. This subject was first considered by Vassiliev in the 90's [138].

A Chebyshev knot [108], is a polynomial knot parameterized by a Chebyshev curve $(T_a(t), T_b(t), T_c(t+\varphi))$ where $T_n(t) = \cos(n \arccos t)$ is the n-th Chebyshev polynomial of the first kind. Chebyshev knots are polynomial analogues of Lissajous knots that have been studied by Jones, Hoste, Lamm... It was first established that any knot can be parameterized by Chebyshev polynomials, then we have studied the properties of harmonic nodes [110] which then opened the way to effective computations.

Our activity in Knot theory is a bridge between our work in computational geometry (topology and drawing of real space curves) and our work on topology in small dimensions (varieties defined as a knot complement).

Two-bridge knots (or rational knots) are particularly studied because they are much easier to study. The first 26 knots (except 8_5) are two-bridge knots. We were able to give an exhaustive, minimal and certified list of Chebyshev parameterizations of the first rational two-bridge knots, using blind computations [111]. On the other hand, we propose the identification of Chebyshev knot diagrams [112] by developing new certified algorithms for computing trigonometric expressions [113]. These works share many tools with our action in visualization and computational geometry.

We made use of Chebyshev polynomials so as Fibonacci polynomials which are families of orthogonal polynomials. Considering the Alexander-Conway polynomials as continuant polynomials in the Fibonacci basis, we were able to give a partial answer to Hoste's conjecture on the roots of Alexander polynomials of alternating knots ([109]).

We study the lexicographic degree of the two-bridge knots, that is to say the minimal (multi)degree of a polynomial representation of a N-crossing two-bridge knot. We show that this degree is $(3, b, c)$ with $b + c = 3N$. We have determined the lexicographic degree of the first 362 first two-bridge knots with 12 crossings or fewer [58] [15]. These results make use of the braid theoretical approach developped by Y. Orevkov to study real plane curves and the use of real pseudoholomorphic curves [56], the slide isotopies on trigonal diagrams, namely those that never increase the number of crossings [57].

2.2.3.3. Visualization and Computational Geometry

The drawing of algebraic curves and surfaces is a critical action in OURAGAN since it is a key ingredient in numerous developments. For example, a certified plot of a discriminant variety could be the only admissible answer that can be proposed for engineering problems that need the resolution of parametric algebraic systems:

[14] ANR project Structures Géométriques et Triangulations
[15] Minimal degrees are listed in https://webusers.imj-prg.fr/~pierre-vincent.koseleff/knots/2bk-lexdeg.html

this variety (and the connected components of its counter part) defines a partition of the parameter's space in regions above which the solutions are numerically stable and topologically simple. Several directions have been explored since the last century, ranging from pure numerical computations to infallible exact ones, depending on the needs (global topology, local topology, simple drawing, etc.). For plane real algebraic curves, one can mention the cylindrical algebraic decomposition [63], grids methods (for ex. the marching square algorithm), subdivision methods, etc.

As mentioned above, we focus on curves and surfaces coming from the study of parametric systems. They mostly come from some elimination process, they highly (numerically) unstable (a small deformation of the coefficients might change a lot the topology of the curve) and we are mostly interested in getting qualitative information about their counter part in the parameter's space.

For this work, we are associated with the GAMBLE EPI (Inria Nancy Grand Est) with the aim of developing computational techniques for the study, plotting and topology. In this collaboration, Ouragan focuses on CAD-Like methods while Gamble develops numerical strategies (that could also apply on non algebraic curves). Ouragan's work involves the development of effective methods for the resolution of algebraic systems with 2 or 3 variables [49], [105], [50], [51] which are basic engines for computing the topology [118], [70] and / or plotting.

2.2.4. Algebraic analysis of functional systems

Systems of functional equations or simply functional systems are systems whose unknowns are functions, such as systems of ordinary or partial differential equations, of differential time-delay equations, of difference equations, of integro-differential equations, etc.

Numerical aspects of functional systems, especially differential systems, have been widely studied in applied mathematics due to the importance of numerical simulation issues.

Complementary approaches, based on algebraic methods, are usually upstream or help the numerical simulation of systems of functional systems. These methods also tackle a different range of questions and problems such as algebraic preconditioning, elimination and simplification, completion to formal integrability or involution, computation of integrability conditions and compatibility conditions, index reduction, reduction of variables, choice of adapted coordinate systems based on symmetries, computation of first integrals of motion, conservation laws and Lax pairs, Liouville integrability, study of the (asymptotic) behavior of solutions at a singularity, etc. Although not yet very popular in applied mathematics, these theories have lengthy been studied in fundamental mathematics and were developed by Lie, Cartan, Janet, Ritt, Kolchin, Spencer, etc. [94] [103] [104] [107] [133] [121].

Over the past years, certain of these algebraic approaches to functional systems have been investigated within an algorithmic viewpoint, mostly driven by applications to engineering sciences such as mathematical systems theory and control theory. We have played a role towards these effective developments, especially in the direction of an algorithmic approach to the so-called *algebraic analysis* [103], [104], [45], a mathematical theory developed by the Japanese school of Sato, which studies linear differential systems by means of both algebraic and analytic methods. To develop an effective approach to algebraic analysis, we first have to make algorithmic standard results on rings of functional operators, module theory, homological algebra, algebraic geometry, sheaf theory, category theory, etc., and to implement them in computer algebra systems. Based on elimination theory (Gröbner or Janet bases [94], [62], [135], differential algebra [47] [76], Spencer's theory [121], etc.), in [4], [5], we have initiated such a computational algebraic analysis approach for general classes of functional systems (and not only for holonomic systems as done in the literature of computer algebra [62]). Based on the effective aspects to algebraic analysis approach, the parametrizability problem [4], the reduction and (Serre) decomposition problems [5], the equidimensional decomposition [122], Stafford's famous theorems for the Weyl algebras [127], etc., have been studied and solutions have been implemented in `Maple`, `Mathematica`, and `GAP` [61][5]. But these results are only the first steps towards computational algebraic analysis, its implementation in computer algebra systems, and its applications to mathematical systems, control theory, signal processing, mathematical physics, etc.

2.2.5. Synergies

Outside applications which can clearly be seen as transversal acitivies, our development directions are linked at several levels : shared computable objects, computational strategies and transversal research directions.
Sharing basic algebraic objects As seen above, is the well-known fact that the elimination theory for functional systems is deeply intertwined with the one for polynomial systems so that, topology in small dimension, applications in control theory, signal theory and robotics share naturally a large set of computable objects developped in our project team.

Performing efficient basic arithmetic operations in number fields is also a key ingredient to most of our algorithms, in Number theory as well as in topology in small dimension or , more generally in the use of roots of polynomials systems. In particular, finding good representations of number fields, lead to the same computational problems as working with roots of polynomial systems by means of triangular systems (towers of number fields) or rational parameterizations (unique number field). Making any progress in one direction will probably have direct consequences for almost all the problems we want to tackle.
Symbolic-numeric strategies. Several general low-level tools are also shared such as the use of approximate arithmetic to speed up certified computations. Sometimes these can also lead to improvement for a different purpose (for example computations over the rationals, deeply used in geometry can often be performed in parallel combining computations in finite fields together with fast Chinese remaindering and modular evaluations).

As simple example of this sharing of tools and strategies, the use of approximate arithmetic is common to the work on LLL (used in the evaluation of the security of cryptographic systems), resolutions of real-world algebraic systems (used in our applications in robotics, control theory, and signal theory), computations of signs of trigonometric expressions used in knot theory or to certified evaluations of dilogarithm functions on an algebraic variety for the computation of volumes of representations in our work in topology, numerical integration and computations of L-functions.
Transversal research directions. The study of the topology of complex algebraic curves is central in the computation of periods of algebraic curves (number theory) but also in the study of character varieties (topology in small dimension) as well as in control theory (stability criteria). Very few computational tools exists for that purpose and they mostly convert the problem to the one of variety over the reals (we can then recycle our work in computational geometry).

As for real algebraic curves, finding a way to describe the topology (an equivalent to the graph obtained in the real case) or computing certified drawings (in the case of a complex plane curve, a useful drawing is the so called associated amoeba) are central subjects for Ouragan.

As mentioned in the section 3.3.1 the computation of the Mahler measure of an algebraic implicit curve is either a challenging problem in number theory and a new direction in topology. The basic formula requires the study of points of moduli 1 , as for stability problems in Control Theory (stability problems), and certified numerical evaluations of non algebraic functions at algebraic points as for many computations for L-Functions.

3. Research Program

3.1. Basic computable objects and algorithms

The development of basic computable objects is somehow *on demand* and depends on all the other directions. However, some critical computations are already known to be bottlenecks and are sources of constant efforts.

Computations with algebraic numbers appear in almost all our activities: when working with number fields in our work in algorithmic number theory as well as in all the computations that involve the use of solutions of zero-dimensional systems of polynomial equations. Among the identified problems: finding good representations for single number fields (optimizing the size and degree of the defining polynomials), finding good representations for towers or products of number fields (typically working with a tower or finding a unique good extension), efficiently computing in practice with number fields (using certified approximation vs working with the formal description based on polynomial arithmetics). Strong efforts are currently done in the understanding of the various strategies by means of tight theoretical complexity studies [70], [115], [50] and many other efforts will be required to find the right representation for the right problem in practice. For example, for isolating critical points of plane algebraic curves, it is still unclear (at least the theoretical complexity cannot help) that an intermediate formal parameterization is more efficient than a triangular decomposition of the system and it is still unclear that these intermediate computations could be dominated in time by the certified final approximation of the roots.

3.2. Algorithmic Number Theory

Concerning algorithmic number theory, the main problems we will be considering in the coming years are the following:

- *Number fields.* We will continue working on the problems of class groups and generators. In particular, the existence and accessibility of *good* defining polynomials for a fixed number field remain very largely open. The impact of better polynomials on the algorithmic performance is a very important parameter, which makes this problem essential.
- *Lattice reduction.* Despite a great amount of work in the past 35 years on the LLL algorithm and its successors, many open problems remain. We will continue the study of the use of interval arithmetic in this field and the analysis of variants of LLL along the lines of the *Potential*-LLL which provides improved reduction comparable to BKZ with a small block size but has better performance.
- *Elliptic curves and Drinfeld modules.* The study of elliptic curves is a very fruitful area of number theory with many applications in crypto and algorithms. Drinfeld modules are "cousins" of elliptic curves which have been less explored in the algorithm context. However, some recent advances [74] have used them to provide some fast sophisticated factoring algorithms. As a consequence, it is natural to include these objects in our research directions.

3.2.1. Rigorous numerical computations

Some studies in this area will be driven by some other directions, for example, the rigorous evaluation of non algebraic functions on algebraic varieties might become central for some of our work on topology in small dimension (volumes of varieties, drawing of amoeba) or control theory (approximations of discriminant varieties) are our two main current sources of interesting problems. In the same spirit, the work on L-functions computations (extending the computation range, algorithmic tools for computing algebraic data from the L function) will naturally follow.

On the other hand, another objective is to extend existing results on periods of algebraic curves to general curves and higher dimensional varieties is a general promising direction. This project aims at providing tools for integration on higher homology groups of algebraic curves, ie computing Gauss-Manin connections. It requires good understanding of their topology, and more algorithmic tools on differential equations.

3.3. Topology in small dimension

3.3.1. Character varieties

The brute force approach to computable objects from topology of small dimension will not allow any significant progress. As explained above, the systems that arise from these problems are simply outside the range of doable computations. We still continue the work in this direction by a four-fold approach, with all three directions deeply inter-related. First, we focus on a couple of especially meaningful (for the applications)

cases, in particular the 3-dimensional manifold called Whitehead link complement. At this point, we are able to make steps in the computation and describe part of the solutions [79], [89]; we hope to be able to complete the computation using every piece of information to simplify the system. Second, we continue the theoretical work to understand more properties of these systems [77]. These properties may prove how useful for the mathematical understanding is the resolution of such systems - or at least the extraction of meaningful information. This approach is for example carried on by Falbel and his work on configuration of flags [80], [82]. Third, we position ourselves as experts in the know-how of this kind of computations and natural interlocutors for colleagues coming up with a question on such a computable object (see [87] and [89]). This also allows us to push forward the kind of computation we actually do and make progress in the direction of the second point. We are credible interlocutors because our team has the blend of theoretical knowledge and computational capabilities that grants effective resolutions of the problems we are presented. And last, we use the knowledge already acquired to pursue our theoretical study of the CR-spherical geometry [69], [81], [78].

Another direction of work is the help to the community in experimental mathematics on new objects. It involves downsizing the system we are looking at (for example by going back to systems coming from hyperbolic geometry and not CR-spherical geometry) and get the most out of what we can compute, by studying new objects. An example of this research direction is the work of Guilloux around the volume function on deformation varieties. This is a real-analytic function defined on the varieties we specialized in computing. Being able to do effective computations with this function led first to a conjecture [86]. Then, theoretical discussions around this conjecture led to a paper on a new approach to the Mahler measure of some 2-variables polynomials [88]. In turn, this last paper gave a formula for the Mahler measure in terms of a function akin to the volume function applied at points in an algebraic variety whose moduli of coordinates are 1. The OURAGAN team has the expertise to compute all the objects appearing in this formula, opening the way to another area of application. This area is deeply linked with number theory as well as topology of small dimension. It requires all the tools at disposition within OURAGAN.

3.3.2. Knot theory

We will carry on the exhaustive search for the lexicographic degrees for the rational knots. They correspond to trigonal space curves: computations in the braid group B_3, explicit parametrization of trigonal curves corresponding to "dessins d'enfants", etc. The problem seems much more harder when looking for more general knots.

On the other hand, a natural direction would be: given an explicit polynomial space curve, determine the under/over nature of the crossings when projecting, draw it and determine the known knot [16] it is isotopic to.

3.3.3. Vizualisation and Computational Geometry

As mentioned above, the drawing of algebraic curves and surfaces is a critical action in OURAGAN since it is a key ingredient in numerous developments. In some cases, one will need a fully certified study of the variety for deciding existence of solutions (for example a region in a robot's parameter's space with solutions to the DKP above or deciding if some variety crosses the unit polydisk for some stability problems in control-theory), in some other cases just a partial but certified approximation of a surface (path planning in robotics, evaluation of non algebraic functions over an algebraic variety for volumes of knot complements in the study of character varieties).

On the one hand, we will contribute to general tools like ISOTOP [17] under the supervision of the GAMBLE project-team and, on the other hand, we will propose ad-hoc solutions by gluing some of our basic tools (problems of high degrees in robust control theory). The priority is to provide a first software that implements methods that fit as most as possible the very last complexity results we got on several (theoretical) algorithms for the computation of the topology of plane curves.

[16] for example the first rational knots are listed at https://team.Inria.fr/ouragan/knots
[17] https://isotop.gamble.loria.fr

A particular effort will be devoted to the resolution of overconstraint bivariate systems which are useful for the studies of singular points and to polynomials systems in 3 variables in the same spirit : avoid the use of Gröbner basis and propose a new algorithm with a state-of-the-art complexity and with a good practical behavior.

In parallel, one will have to carefully study the drawing of graphs of non algebraic functions over algebraic complex surfaces for providing several tools which are useful for mathematicians working on topology in small dimension (a well known example is the drawing of amoebia, a way of representing a complex curve on a sheet of paper).

3.4. Algebraic analysis of functional systems

We want to further develop our expertise in the computational aspects of algebraic analysis by continuing to develop effective versions of results of module theory, homological algebra, category theory and sheaf theory [136] which play important roles in algebraic analysis [45], [103], [104] and in the algorithmic study of linear functional systems. In particular, we shall focus on linear systems of integro-differential-constant/varying/distributed delay equations [124], [126] which play an important role in mathematical systems theory, control theory, and signal processing [124], [131], [125], [128].

The rings of integro-differential operators are highly more complicated than the purely differential case (i.e. Weyl algebras) [12], due to the existence of zero-divisors, or the fact of having a coherent ring instead of a noetherian ring [42]. Therefore, we want to develop an algorithmic study of these rings. Following the direction initiated in [126] for the computation of zero divisors (based on the polynomial null spaces of certain operators), we first want to develop algorithms for the computation of left/right kernels and left/right/generalized inverses of matrices with entries in such rings, and to use these results in module theory (e.g. computation of syzygy modules, (shorter/shortest) free resolutions, split short/long exact sequences). Moreover, Stafford's results [137], algorithmically developed in [12] for rings of partial differential operators (i.e. the Weyl algebras), are known to still hold for rings of integro-differential operators. We shall study their algorithmic extensions. Our corresponding implementation will be extended accordingly.

Finally, within a computer algebra viewpoint, we shall continue to algorithmically study issues on rings of integro-differential-delay operators [124], [125] and their applications to the study of equivalences of differential constant/varying/distributed delay systems (e.g. Artstein's reduction, Fiagbedzi-Pearson's transformation) which play an important role in control theory.

4. Application Domains

4.1. Security of cryptographic systems

The study of the security of asymmetric cryptographic systems comes as an application of the work carried out in algorithmic number theory and revolves around the development and the use of a small number of general purpose algorithms (lattice reduction, class groups in number fields, discrete logarithms in finite fields, ...). For example, the computation of generators of principal ideals of cyclotomic fields can be seen as one of these applications since these are used in a number of recent public key cryptosystems.

The cryptographic community is currently very actively assessing the threat coming for the development of quantum computers. Indeed, such computers would permit tremendous progress on many number theoretic problems such as factoring or discrete logarithm computations and would put the security of current cryptosystem under a major risk. For this reason, there is a large global research effort dedicated to finding alternative methods of securing data. For example, the US standardization agency called NIST has recently launched a standardization process around this issue. In this context, OURAGAN is part of the competition and has submitted a candidate (which has not been selected) [40]. This method is based on number-theoretic ideas involving a new presumably difficult problem concerning the Hamming distance of integers modulo large numbers of Mersenne.

4.2. Robotics

Algebraic computations have tremendously been used in Robotics, especially in kinematics, since the last quarter of the 20th century [93]. For example, one can find algebraic proofs for the 40 possible solutions to the direct kinematics problem [117] for steward platforms and companion experiments based on Gröbner basis computations [83]. On the one hand, hard general kinematics problems involve too many variables for pure algebraic methods to be used in place of existing numerical or semi-numerical methods everywhere and everytime, and on the other hand, global algebraic studies allow to propose exhaustive classifications that cannot be reached by other methods,for some quite large classes.

Robotics is a long-standing collaborative work with LS2N (Laboratory of Numerical Sciences of Nantes). Work has recently focused on the offline study of mechanisms, mostly parallel, their singularities or at least some types of singularities (cuspidals robots [140]).

For most parallel or serial manipulators, pose variables and joints variables are linked by algebraic equations and thus lie an algebraic variety. The two-kinematics problems (the direct kinematics problem - DKP- and the inverse kinematics problem - IKP) consist in studying the preimage of the projection of this algebraic variety onto a subset of unknowns. Solving the DKP remains to computing the possible positions for a given set of joint variables values while solving the IKP remains to computing the possible joints variables values for a given position. Algebraic methods have been deeply used in several situations for studying parallel and serial mechanisms, but finally their use stays quite confidential in the design process. Cylindrical Algebraic Decomposition coupled with variable's eliminations by means of Gröbner based computations can be used to model the workspace, the joint space and the computation of singularities. On the one hand, such methods suffer immediately when increasing the number of parameters or when working with imprecise data. On the other hand, when the problem can be handled, they might provide full and exhaustive classifications. The tools we use in that context [60], [59], [95], [97], [96] depend mainly on the resolution of parameter-based systems and therefore of study-dependent curves or flat algebraic surfaces (2 or 3 parameters), thus joining our thematic *Computational Geometry*.

4.3. Control theory

Certain problems studied in mathematical systems theory and control theory can be better understood and finely studied by means of algebraic structures and methods. Hence, the rich interplay between algebra, computer algebra, and control theory has a long history. For instance, the first main paper on Gröbner bases written by their creators, Buchberger, was published in Bose's book [46] on control theory of multidimensional systems. Moreover, the differential algebra approach to nonlinear control theory (see [72], [73] and the references therein) was a major motivation for the algorithmic study of differential algebra [47], [76]. Finally, the behaviour approach to linear systems theory [141], [119] advocates for an algorithmic study of algebraic analysis (see Section 2.2.4). More generally, control theory is porous to computer algebra since one finds algebraic criteria of all kinds in the literature even if the control theory community has a very few knowledge in computer algebra.

OURAGAN has a strong interest in the computer algebra aspects of mathematical systems theory and control theory related to both functional and polynomial systems, particularly in the direction of robust stability analysis and robust stabilization problems for multidimensional systems [46], [119] and infinite-dimensional systems [66] (such as, e.g., differential time-delay systems).

Let us shortly state a few points of our recent interests in this direction.

In control theory, stability analysis of linear time-invariant control systems is based on the famous Routh-Hurwitz criterion (late 19th century) and its relation with Sturm sequences and Cauchy index. Thus, stability tests were only involving tools for univariate polynomials [102]. While extending those tests to multidimensional systems or differential time-delay systems, one had to tackle multivariate problems recursively with respect to the variables [46]. Recent works use a mix of symbolic/numeric strategies, Linear Matrix Inequalities (LMI), sums of squares, etc. But still very few practical experiments are currently involving certified algebraic computations based on general solvers for polynomial equations. We have recently started to study

certified stability tests for multidimensional systems or differential time-delay systems with an important observation: with a correct modelization, some recent algebraic methods – derived from our work in algorithmic geometry and shared with applications in robotics – can now handle previously impossible computations and lead to a better understanding of the problems to be solved [52], [54], [55]. The previous approaches seem to be blocked on a recursive use of one-variable methods, whereas our approach involves the direct processing of the problem for a larger number of variables.

The structural stability of n-D discrete linear systems (with $n \geq 2$) is a good source of problems of several kinds ranging from solving univariate polynomials to studying algebraic systems depending on parameters. For instance, we show [53], [54], [55] that the standard characterization of the structural stability of a multivariate rational transfer function (namely, the denominator of the transfer function does not have solutions in the unit polydisc of $\mathbb{C}^n$) is equivalent to deciding whether or not a certain system of polynomial equations has real solutions. The use state-of-the-art computer algebra algorithms to check this last condition, and thus the structural stability of multidimensional systems has been validated in several situations from toy examples with parameters to state-of-the-art examples involving, e.g., the resolution of bivariate systems [51], [50].

The rich interplay between control theory, algebra, and computer algebra is also well illustrated with our recent work on robust stabilization problems for multidimensional and finite/infinite-dimensional systems [48], [123], [129], [132], [130], [131].

4.4. Signal processing

Due to numerous applications (e.g. sensor network, mobile robots), sources and sensors localization has intensively been studied in the literature of signal processing. The *anchor position self calibration problem* is a well-known problem which consists in estimating the positions of both the moving sources and a set of fixed sensors (anchors) when only the distance information between the points from the different sets is available. The position self-calibration problem is a particular case of the *Multidimensional Unfolding* (MDU) problem for the Euclidean space of dimension 3. In the signal processing literature, this problem is attacked by means of optimization problems (see [65] and the references therein). Based on computer algebra methods for polynomial systems, we have recently developed a new approach for the MDU problem which yields closed-form solutions and a very efficient algorithm for the estimation of the positions [68] based only on linear algebra techniques. This first result, done in collaboration with Dagher (Inria Chile) and Zheng (DEFROST, Inria Lille), yielded a recent patent [67]. This result advocates for the study of other localization problems based on the computational polynomial techniques developed in OURAGAN.

In collaboration with *Safran Tech* (Barau, Hubert) and Dagher (Inria Chile), a symbolic-numeric study of the new *multi-carrier demodulation method* [92] has recently been initiated. *Gear fault diagnosis* is an important issue in aeronautics industry since a damage in a gearbox, which is not detected in time, can have dramatic effects on the safety of a plane. Since the vibrations of a spur gear can be modeled as a product of two periodic functions related to the gearbox kinematic, it is proposed to recover each function from the global signal by means of an optimal reconstruction problem which, based on Fourier analysis, can be rewritten as $\text{argmin}_{u \in \mathbb{C}^n, v_1, v_2 \in \mathbb{C}^m} \| M - u\, v_1^{\bigstar} - D\, u\, v_2^{\bigstar} \|_F$, where $M \in \mathbb{C}^{n \times m}$ (resp. $D \in \mathbb{C}^{n \times n}$) is a given matrix with a special shape (resp. diagonal matrix), $\| \cdot \|_F$ is the Frobenius norm, and $v^{\bigstar}$ is the Hermitian transpose of v. We have recently obtained closed-form solutions for the exact problem, i.e., $M = u\, v_1^{\bigstar} + D\, u\, v_2^{\bigstar}$, which is a polynomial system with parameters. This first result gives interesting new insides for the study of the non-exact case, i.e. for the above optimization problem.

Our expertise on *algebraic parameter estimation problem*, developed in the former NON-A project-team (Inria Lille), will be further developed. Following this work [84], the problem consists in estimating a set θ of parameters of a signal $x(\theta, t)$ – which satisfies a certain dynamics – when the signal $y(t) = x(\theta, t) + \gamma(t) + \varpi(t)$ is observed, where γ denotes a structured perturbation and ϖ a noise. It has been shown that θ can sometimes be explicitly determined by means of closed-form expressions using iterated integrals of y. These integrals are used to filter the noise ϖ. Based on a combination of algebraic analysis techniques (rings of differential

operators), differential elimination theory (Gröbner basis techniques for Weyl algebras), and operational calculus (Laplace transform, convolution), an algorithmic approach to algebraic parameter estimation problem has been initiated in [125] for a particular type of structured perturbations (i.e. bias) and was implemented in the `Maple` prototype `NonA`. The case of a general structured perturbation is still lacking.

5. Highlights of the Year

5.1. Highlights of the Year

Two new projects have started this year

- the MACAO associated team in collaboration with the University of Wollongong (Australia) - see 9.3.1
- a collaboration with Safran Tech - see 8.1

6. New Software and Platforms

6.1. ISOTOP

Topology and geometry of planar algebraic curves

KEYWORDS: Topology - Curve plotting - Geometric computing

FUNCTIONAL DESCRIPTION: Isotop is a Maple software for computing the topology of an algebraic plane curve, that is, for computing an arrangement of polylines isotopic to the input curve. This problem is a necessary key step for computing arrangements of algebraic curves and has also applications for curve plotting. This software has been developed since 2007 in collaboration with F. Rouillier from Inria Paris - Rocquencourt.

- Participants: Luis Penaranda, Marc Pouget and Sylvain Lazard
- Contact: Marc Pouget
- Publications: Rational Univariate Representations of Bivariate Systems and Applications - Separating Linear Forms for Bivariate Systems - On The Topology of Planar Algebraic Curves - New bivariate system solver and topology of algebraic curves - Improved algorithm for computing separating linear forms for bivariate systems - Solving bivariate systems using Rational Univariate Representations - On the topology of planar algebraic curves - On the topology of real algebraic plane curves - Bivariate triangular decompositions in the presence of asymptotes - Separating linear forms and Rational Univariate Representations of bivariate systems
- URL: https://isotop.gamble.loria.fr/

6.2. RS

FUNCTIONAL DESCRIPTION: Real Roots isolation for algebraic systems with rational coefficients with a finite number of Complex Roots

- Participant: Fabrice Rouillier
- Contact: Fabrice Rouillier
- URL: https://team.inria.fr/ouragan/software/

6.3. A NewDsc

A New Descartes

KEYWORD: Scientific computing

FUNCTIONAL DESCRIPTION: Computations of the real roots of univariate polynomials with rational coefficients.

- Authors: Fabrice Rouillier, Alexander Kobel and Michael Sagraloff
- Partner: Max Planck Institute for Software Systems
- Contact: Fabrice Rouillier
- URL: https://anewdsc.mpi-inf.mpg.de

6.4. SIROPA

KEYWORDS: Robotics - Kinematics

FUNCTIONAL DESCRIPTION: Library of functions for certified computations of the properties of articulated mechanisms, particularly the study of their singularities

- Authors: Damien Chablat, Fabrice Rouillier, Guillaume Moroz and Philippe Wenger
- Partner: LS2N
- Contact: Guillaume Moroz
- URL: http://siropa.gforge.inria.fr/

6.5. MPFI

KEYWORD: Arithmetic

FUNCTIONAL DESCRIPTION: MPFI is a C library based on MPFR and GMP for multi precision floating point arithmetic.

- Contact: Fabrice Rouillier
- URL: http://mpfi.gforge.inria.fr

7. New Results

7.1. Certified non-conservative tests for the structural stability of discrete multidimensional systems

In [18], we present new computer algebra based methods for testing the structural stability of n-D discrete linear systems (with n at least 2). More precisely, we show that the standard characterization of the structural stability of a multivariate rational transfer function (namely, the denominator of the transfer function does not have solutions in the unit polydisc of $\mathbb{C}^n$) is equivalent to the fact that a certain system of polynomials does not have real solutions. We then use state-of-the-art computer algebra algorithms to check this last condition, and thus the structural stability of multidimensional systems.

7.2. Computing period matrices and the Abel-Jacobi map of superelliptic curves

In [24], we present an algorithm for the computation of period matrices and the Abel-Jacobi map of complex superelliptic curves given by an equation y m = f (x). It relies on rigorous numerical integration of differentials between Weierstrass points, which is done using Gauss method if the curve is hyperelliptic (m = 2) or the Double-Exponential method. The algorithm is implemented and makes it possible to reach thousands of digits accuracy even on large genus curves.

7.3. Voronoi diagram of orthogonal polyhedra in two and three dimensions

Voronoi diagrams are a fundamental geometric data structure for obtaining proximity relations. In [28], we consider collections of axis-aligned orthogonal polyhedra in two and three-dimensional space under the max-norm, which is a particularly useful scenario in certain application domains. We construct the exact Voronoi diagram inside an orthogonal polyhedron with holes defined by such polyhedra. Our approach avoids creating full-dimensional elements on the Voronoi diagram and yields a skeletal representation of the input object. We introduce a complete algorithm in 2D and 3D that follows the subdivision paradigm relying on a bounding-volume hierarchy; this is an original approach to the problem. The complexity is adaptive and comparable to that of previous methods. Under a mild assumption it is $O(n/\Delta)$ in 2D or $O(n.\alpha^2/\Delta^2)$ in 3D, where n is the number of sites, namely edges or facets resp., Δ is the maximum cell size for the subdivision to stop, and α bounds vertex cardinality per facet. We also provide a numerically stable, open-source implementation in Julia, illustrating the practical nature of our algorithm.

7.4. A symbolic computation approach towards the asymptotic stability analysis of differential systems with commensurate delays

In [30], the work aims at studying the asymptotic stability of retarded type linear differential systems with commensurate delays. Within the frequency-domain approach, it is well-known that the asymptotic stability of such a system is ensured by the condition that all the roots of the corresponding quasipolynomial have negative real parts. A classical approach for checking this condition consists in computing the set of critical zeros of the quasipolynomial, i.e., the roots (and the corresponding delays) of the quasipolynomial that lie on the imaginary axis, and then analyzing the variation of these roots with respect to the variation of the delay. Following this approach, based on solving algebraic systems techniques, we propose a certified and efficient symbolic-numeric algorithm for computing the set of critical roots of a quasipolynomial. Moreover, using recent algorithmic results developed by the computer algebra community, we present an efficient algorithm for the computation of Puiseux series at a critical zero which allows us to finely analyze the stability of the system with respect to the variation of the delay. Explicit examples are given to illustrate our algorithms.

7.5. On the computation of stabilizing controllers of multidimensional systems

In [25], we consider the open problem consisting in the computation of stabilizing controllers of an internally stabilizable MIMO multidimensional system. Based on homological algebra and the so-called *Polydisk Nullstellensatz*, we propose a general method towards the explicit computation of stabilizing controllers. We show how the homological algebra methods over the ring of structurally stable SISO multidimensional transfer functions can be made algorithmic based on standard Gröbner basis techniques over polynomial rings. The problem of computing stabilizing controllers is then reduced to the problem of obtaining an effective version of the Polydisk Nullstellensatz which, apart from a few cases, stays open and will be studied in forthcoming publications.

7.6. Algebraic aspects of the exact signal demodulation problem

In [29], we introduce a general class of problems originating from gearbox vibration analysis. Based on a previous work where demodulation was formulated as a matrix approximation problem, we study the specific case applicable to amplitude and phase demodulation. This problem can be rewritten as a polynomial system. Based on algebraic methods such as linear algebra and homological algebra, we focus on the characterization of the problem and solve it in the noise-free case.

7.7. General closed-form solutions of the position self-calibration problem

The work in [36] investigates the anchors and sources position self-calibration problem in the 3D space based on range measurements and without any prior restriction on the network configuration. Using a well known low-rank property of Euclidean distance matrices, we first reduce the problem to finding 12 unknowns ascribed

in a 3×3 transformation matrix and a 3×1 translation vector. In order to estimate them, we then introduce a polynomial parametrization with 9 unknowns that are estimated by solving a linear system. Afterwards, we identify an intrinsic matrix polynomial system that encodes the solution set of the problem and provide a direct method for solving it. The resulting procedure is simple and straightforward to implement using standard numerical tools. We also show that closed-form solutions can always be obtained when the reference frame is fixed. This is illustrated by adopting reference frames from the literature and by introducing a triangular reference frame whose constraints are imposed only on one position set (anchor or source). Experimental results on synthetic and real sound data show that the proposed closed-form solutions efficiently solve the position self-calibration problem.

7.8. Certified lattice reduction

Quadratic form reduction and lattice reduction are fundamental tools in computational number theory and in computer science, especially in cryptography. The celebrated Lenstra–Lenstra–Lovász reduction algorithm (so-called LLL) has been improved in many ways through the past decades and remains one of the central methods used for reducing integral lattice basis. In particular, its floating-point variants—where the rational arithmetic required by Gram–Schmidt orthogonalization is replaced by floating-point arithmetic—are now the fastest known. However, the systematic study of the reduction theory of real quadratic forms or, more generally, of real lattices is not widely represented in the literature. When the problem arises, the lattice is usually replaced by an integral approximation of (a multiple of) the original lattice, which is then reduced. While practically useful and proven in some special cases, this method doesn't offer any guarantee of success in general. In [22], we present an adaptive-precision version of a generalized LLL algorithm that covers this case in all generality. In particular, we replace floating-point arithmetic by Interval Arithmetic to certify the behavior of the algorithm. We conclude by giving a typical application of the result in algebraic number theory for the reduction of ideal lattices in number fields.

7.9. Using Maple to analyse parallel robots

In [27], we present the SIROPA Maple Library which has been designed to study serial and parallel manipulators at the conception level. We show how modern algorithms in Computer Algebra can be used to study the workspace, the joint space but also the existence of some physical capabilities w.r.t. to some design parameters left as degree of freedom for the designer of the robot.

7.10. On the effective computation of stabilizing controllers of 2D systems

In [26], we show how stabilizing controllers for 2D systems can effectively be computed based on computer algebra methods dedicated to polynomial systems, module theory and homological algebra. The complete chain of algorithms for the computation of stabilizing controllers, implemented in Maple, is illustrated with an explicit example.

7.11. Updating key size estimations for pairings

Recent progress on NFS imposed a new estimation of the security of pairings. In [15], we study the best attacks against some of the most popular pairings. It allows us to propose new pairing-friendly curves of 128 bits and 192 bits of security.

7.12. Matrix formulae for Resultants and Discriminants of Bivariate Tensor-product Polynomials

The construction of optimal resultant formulae for polynomial systems is one of the main areas of research in computational algebraic geometry. However, most of the constructions are restricted to formulae for unmixed polynomial systems, that is, systems of polynomials which all have the same support. Such a condition is restrictive, since mixed systems of equations arise frequently in many problems. Nevertheless,

resultant formulae for mixed polynomial systems is a very challenging problem. In [19], we present a square, Koszul-type, matrix, the determinant of which is the resultant of an arbitrary (mixed) bivariate tensor-product polynomial system. The formula generalizes the classical Sylvester matrix of two univariate polynomials, since it expresses a map of degree one, that is, the elements of the corresponding matrix are up to sign the coefficients of the input polynomials. Interestingly, the matrix expresses a primal-dual multiplication map, that is, the tensor product of a univariate multiplication map with a map expressing derivation in a dual space. In addition we prove an impossibility result which states that for tensor-product systems with more than two (affine) variables there are no universal degree-one formulae, unless the system is unmixed. Last but not least, we present applications of the new construction in the efficient computation of discriminants and mixed discriminants.

7.13. Separation bounds for polynomial systems

In [21], we rely on aggregate separation bounds for univariate polynomials to introduce novel worst-case separation bounds for the isolated roots of zero-dimensional, positive-dimensional, and overde- termined polynomial systems. We exploit the structure of the given system, as well as bounds on the height of the sparse (or toric) resultant, by means of mixed volume, thus establishing adaptive bounds. Our bounds improve upon Canny's Gap theorem [9]. Moreover, they exploit sparseness and they apply without any assumptions on the input polynomial system. To evaluate the quality of the bounds, we present polynomial systems whose root separation is asymptotically not far from our bounds. We apply our bounds to three problems. First, we use them to estimate the bitsize of the eigenvalues and eigenvectors of an integer matrix; thus we provide a new proof that the problem has polynomial bit complexity. Second, we bound the value of a positive polynomial over the simplex: we improve by at least one order of magnitude upon all existing bounds. Finally, we asymptotically bound the number of steps of any purely subdivision-based algorithm that isolates all real roots of a polynomial system.

7.14. On the maximal number of real embeddings of minimally rigid graphs in $\mathbb{R}^2$, $\mathbb{R}^3$ and S^2

Rigidity theory studies the properties of graphs that can have rigid embeddings in a euclidean space $\mathbb{R}^d$ or on a sphere and other manifolds which in addition satisfy certain edge length constraints. One of the major open problems in this field is to determine lower and upper bounds on the number of realizations with respect to a given number of vertices. This problem is closely related to the classification of rigid graphs according to their maximal number of real embeddings. In [17], we are interested in finding edge lengths that can maximize the number of real embeddings of minimally rigid graphs in the plane, space, and on the sphere. We use algebraic formulations to provide upper bounds. To find values of the parameters that lead to graphs with a large number of real realizations, possibly attaining the (algebraic) upper bounds, we use some standard heuristics and we also develop a new method inspired by coupler curves. We apply this new method to obtain embeddings in $\mathbb{R}^3$. One of its main novelties is that it allows us to sample efficiently from a larger number of parameters by selecting only a subset of them at each iteration. Our results include a full classification of the 7-vertex graphs according to their maximal numbers of real embeddings in the cases of the embeddings in $\mathbb{R}^2$ and $\mathbb{R}^3$, while in the case of S^2 we achieve this classification for all 6-vertex graphs. Additionally, by increasing the number of embeddings of selected graphs, we improve the previously known asymptotic lower bound on the maximum number of realizations.

7.15. Multilinear Polynomial Systems: Root Isolation and Bit Complexity

In [20], we exploit structure in polynomial system solving by considering polyno-mials that are linear in subsets of the variables. We focus on algorithms and their Boolean complexity for computing isolating hyperboxes for all the isolated complex roots of well-constrained, unmixed systems of multilinear polynomials based on resultant methods. We enumerate all expressions of the multihomogeneous (or multigraded) resultant of such systems as a determinant of Sylvester-like matrices, aka generalized Sylvester matrices. We construct

these matrices by means of Weyman homological complexes, which generalize the Cayley-Koszul complex. The computation of the determinant of the resultant matrix is the bottleneck for the overall complexity. We exploit the quasi-Toeplitz structure to reduce the problem to efficient matrix-vector multiplication, which corresponds to multivariate polynomial multiplication, by extending the seminal work on Macaulay matrices of Canny, Kaltofen, and Yagati [9] to the multi-homogeneous case. We compute a rational univariate representation of the roots, based on the primitive element method. In the case of 0-dimensional systems we present a Monte Carlo algorithm with probability of success $1 - 1/2^{\eta}$, for a given $\eta \geq 1$, and bit complexity $O_B(n^2 D^{4+\epsilon}(n^{N+1} + \tau) + nD^{2+\epsilon}\eta(D + \eta))$ for any $\epsilon > 0$, where n is the number of variables, D equals the multilinear Bézout bound, N is the number of variable subsets, and τ is the maximum coefficient bitsize. We present an algorithmic variant to compute the isolated roots of overdetermined and positive-dimensional systems. Thus our algorithms and complexity analysis apply in general with no assumptions on the input.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- The objective of our Agrement with WATERLOO MAPLE INC. is to promote software developments to which we actively contribute.

  On the one hand, WMI provides man power, software licenses, technical support (development, documentation and testing) for an inclusion of our developments in their commercial products. On the other hand, OURAGAN offers perpetual licenses for the use of the concerned source code.

  As past results of this agreement one can cite our C-Library *RS* for the computations of the real solutions zero-dimensional systems or also our collaborative development around the Maple package *DV* for solving parametric systems of equations.

  For this term, the agreement covers algorithms developed in areas including but not limited to: 1) solving of systems of polynomial equations, 2) validated numerical polynomial root finding, 3) computational geometry, 4) curves and surfaces topology, 5) parametric algebraic systems, 6) cylindrical algebraic decompositions, 7) robotics applications.

  In particular, it covers our collaborative work with some of our partners, especially the Gamble Project-Team - Inria Nancy Grand Est.
- In 2019, a contract was signed with the company *Safran Tech*. Its goal is to bring our scientific expertise on mathematical and algorithmic aspects on certain problems studied in gearbox vibration analysis. Gear fault diagnosis is an important issue in aeronautics industry since a damage in a gearbox, which is not detected in time, can have dramatic effects on the safety of a plane. Since the vibrations of a spur gear can be modeled as a product of two periodic functions related to the gearbox kinematic, [92] has proposed to recover each function from the global signal by means of an optimal reconstruction problem which, by means of Fourier analysis, yields a Frobenius norm minimization problem for structured matrices. The goal of the collaboration is to use symbolic-numeric to study this problem.

9. Partnerships and Cooperations

9.1. National Initiatives

- FMJH Program, PGMO grant

  ALMA (Algebraic methods in games and optimization).

  Duration: 2018 – 2020. (2 years project)

  Coordinator: Elias Tsigaridas, with Stéphane Gaubert and Xavier Allamigeon (CMAP, École Polytechnique)

9.1.1. ANR

- ANR JCJC GALOP (Games through the lens of ALgebra and OPptimization)

  Coordinator: Elias Tsigaridas

  Duration: 2018 – 2022

  GALOP is a Young Researchers (JCJC) project with the purpose of extending the limits of the state-of-the-art algebraic tools in computer science, especially in stochastic games. It brings original and innovative algebraic tools, based on symbolic-numeric computing, that exploit the geometry and the structure and complement the state-of-the-art. We support our theoretical tools with a highly efficient open-source software for solving polynomials. Using our algebraic tools we study the geometry of the central curve of (semi-definite) optimization problems. The algebraic tools and our results from the geometry of optimization pave the way to introduce algorithms and precise bounds for stochastic games.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

Program: H2020-EU.1.1. - EXCELLENT SCIENCE - European Research Council (ERC)

Project acronym: Almacrypt

Project title: Algorithmic and Mathematical Cryptology

Duration: 01/2016 - 12/2010

Coordinator: Antoine Joux

Abstract: Cryptology is a foundation of information security in the digital world. Today's internet is protected by a form of cryptography based on complexity theoretic hardness assumptions. Ideally, they should be strong to ensure security and versatile to offer a wide range of functionalities and allow efficient implementations. However, these assumptions are largely untested and internet security could be built on sand. The main ambition of Almacrypt is to remedy this issue by challenging the assumptions through an advanced algorithmic analysis. In particular, this proposal questions the two pillars of public-key encryption: factoring and discrete logarithms. Recently, the PI contributed to show that in some cases, the discrete logarithm problem is considerably weaker than previously assumed. A main objective is to ponder the security of other cases of the discrete logarithm problem, including elliptic curves, and of factoring. We will study the generalization of the recent techniques and search for new algorithmic options with comparable or better efficiency. We will also study hardness assumptions based on codes and subset-sum, two candidates for post-quantum cryptography. We will consider the applicability of recent algorithmic and mathematical techniques to the resolution of the corresponding putative hard problems, refine the analysis of the algorithms and design new algorithm tools. Cryptology is not limited to the above assumptions: other hard problems have been proposed to aim at post-quantum security and/or to offer extra functionalities. Should the security of these other assumptions become critical, they would be added to Almacrypt's scope. They could also serve to demonstrate other applications of our algorithmic progress. In addition to its scientific goal, Almacrypt also aims at seeding a strengthened research community dedicated to algorithmic and mathematical cryptology.

9.3. International Initiatives

- Partenariat Hubert Curien franco-turc (PHC Bosphore) with Gebze Technical University, Turkey.

  Title: "Gröbner bases, ResultAnts and Polyhedral gEometry" (GRAPE)

  Duration: 2019 – 2020 (2 years project)

  Coordinator: Elias Tsigaridas

9.3.1. Inria Associate Teams Not Involved in an Inria International Labs

9.3.1.1. MACAO

Title: Mathematics and Algorithms for Cryptographic Advanced Objects

International Partner (Institution - Laboratory - Researcher):

University of Wollongong (Australia) - Thomas Plantard

Start year: 2019

See also: https://ssl.informatics.uow.edu.au/MACAO/

Since quantum computers have the ability to break the two main problems on which current public cryptography relies, i.e., the factoring and discrete logarithm problem, every step towards the practical realization of these computers raises fears about potential attacks on cryptographic systems. By scrutinizing the techniques proposed to build post-quantum cryptography, we can identify a few candidate hard problems which underly the proposals. One objective of this international project is to precisely assess the security of these cryptographic algorithms. First, by analyzing in a systematic manner the existing resolution algorithms and by assessing their complexity as a function of security parameters. Then, we will consider new algorithmic techniques to solve these candidate hard Post-Quantum problems, both on classical computers and quantum machines aiming at the discovery of new and better algorithms to solve them.

9.3.2. Inria International Partners

9.3.2.1. Declared Inria International Partners

- University of Wollongong (Australia)

9.3.2.2. Informal International Partners

- CQT Singapour (UMI CNRS Majulab)
- UFPA - Para -Brésil (José Miguel Veloso)
- Institut Joseph Fourier - Université Grenoble Alpes (Martin Deraux, V. Vitse et Pierre Will)
- Max-Planck-Institut für Informatik - Saarbrücken - Germany (Alex. Kobel)
- Holon Institute of Technology, Israel (Jeremy Kaminsky)
- Department of Informatics, National Kapodistrian University of Athens, Greece (Ioannis Emiris)

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events: Organisation

10.1.1.1. General Chair, Scientific Chair

- Elias Tsigaridas was the program chair of Mathematical Aspects of Computer and Information Sciences (MACIS 2019), which was held at Istanbul, 13-15 November 2019.

10.1.1.2. Member of the Organizing Committees

A. Quadrat was a member of the organization committee of the *Journées Nationales de Calcul Formel* (JNCF), Luminy, France, 04-08/02/2019. He is now a member of the scientific committee of JNCF.

10.1.2. Scientific Events: Selection

10.1.2.1. Member of the Conference Program Committees

Elias Tsigaridas was a program committee member of Computer Algebra in Scientific Computing (CASC 2019).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Elisha Falbel is a member of the editorial board of *São Paulo Journal of Mathematical Sciences - Springer*
- Antoine Joux is a member of the editorial board of *Designs, Codes and Cryptography*
- Alban Quadrat is associate editor of *Multidimensional Systems and Signal Processing*, Springer
- Fabrice Rouillier is a member of the editorial board of *Journal of Symbolic Computation*

10.1.4. Leadership within the Scientific Community

Alban Quadrat co-organized the invited sessions *Algebraic and symbolic methods for mathematical systems theory* and *New trends in computational methods for time-delay systems* at the Join *Joint IFAC Conference 7th Symposium on Systems Structure and Control and 15th Workshop on Time Delay Systems*, 9–11 September 2019, Sinaia, Romania

Elias Tsigaridas organized a session on *Algebraic and geometric tools for optimisation and statistics* during the PGMO days 2019, at the EDF'Lab Palaiseau, December 2019.

10.1.5. Research Administration

- Alban Quadrat is a member of the Conseil d'Administration of the Société Mathématique de France (SMF).
- Fabrice Rouillier is a member of the scientific commitee of the Indo French Centre for Applied Mathematics.
- Elisha Falbel is director of the "École Doctorale Sciences Mathématiques de Paris Centre - ED 386".

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Fabrice Rouillier: Course in Algebraic Computations, M1, 24h, Sorbonne Université
- Fabrice Rouillier: Course in "Agrégation Option - C", M2, 31 heures, Sorbonne Université
- Antonin Guilloux: Courses and administration of the general math courses in L1 at Sorbonne Université
- Elisha Falbel: First year 'mathématiques approfondie' and master class on Riemann surfaces.
- Pierre-Vincent Koseleff : head of the Master 2 "pr éparation à l'agrégation de mathématiques" at Sorbonne Université.
- Pierre-Vincent Koseleff : Course in M2 "Agrégation de Mathématiques", Computer Algebra, Option C, 100h. Sorbonne Université.
- Pierre-Vincent Koseleff : Course in L3, "algèbre appliquée".

10.2.2. Supervision

PhD in progress: Thomas Espitau, 09/2016, directed by Antoine Joux

PhD in progress: Natalia Kharchenko, 09/2016, directed by Antoine Joux

PhD in progress: Mahya Mehrabdollahei, 09/2018, directed by Antonin Guilloux and Fabrice Rouillier

PhD in progress: Grace Younes, 09/2018, directed by Alban Quadrat and Fabrice Rouillier

PhD in progress: Christina Katsamaki, 09/2019, directed by Elias Tsigaridas and Fabrice Rouillier

PhD in progress: Sudarshan Shinde, 09/2016, directed by Razvan Barbulescu and Pierre-Vincent Koseleff

PhD in progress: Raphael Alexandre, 09/2019, directed by Elisha Falbel.

10.2.3. Juries

Alban Quadrat was a member of the PhD defense committee of Elisa Hubert, *Surveillance vibratoire d'une transmission de puissance aéronautique*, University of Lyon & Safran Tech, 28/06/2019.

Elisha Falbel was a member of the Habilitation defense committee of Junyan Cao, *Positivité des images directees, extension d'Ohsawa-Takegoshi et applications*, Sorbonne Université , 25/10/2019.

10.3. Popularization

- Alban Quadrat co-edited the book *Le Jeu de rôle sur table : un laboratoire de l'imaginaire*, Carrefour des lettres modernes, n. 7, Classiques Garnier, 2019.
- Fabrice Rouillier is a member of the editorial board of *Interstices*
- Fabrice Rouillier is *chargé de mission médiation* at Inria Paris
- Fabrice Rouillier is a member of the *comité de pilotage de l'année des mathématiques*
- Fabrice Rouillier is a member of the *comité de pilotage de la semaine des mathématiques*
- Fabrice Rouillier is the president of the association *Animath* [18]
- Fabrice Rouillier is member of the scientific board of the SMF [19]conference *Mathématiques étonnantes* [20]

10.3.1. Internal or external Inria responsibilities

- Alban Quadrat is a member of the technical committee *Linear Systems* of the *International Federation of Automatic Control* (IFAC)
- Elias Tsigaridas is a member of the Evaluation committee (Commission d'Évaluation) of Inria.

10.3.2. Interventions

- Fabrice Rouillier participated to the *semaine des mathématiques* for the Paris Inria Paris research center
- Fabrice Rouillier participated to the welcoming of schoolchildren for their *semaine d'observation* at Inria Paris research center.

11. Bibliography

Major publications by the team in recent years

[1] Y. BOUZIDI, S. LAZARD, G. MOROZ, M. POUGET, F. ROUILLIER, M. SAGRALOFF. *Solving bivariate systems using Rational Univariate Representations*, in "Journal of Complexity", 2016, vol. 37, pp. 34–75 [*DOI :* 10.1016/J.JCO.2016.07.002], https://hal.inria.fr/hal-01342211

[2] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *On the lexicographic degree of two-bridge knots*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", June 2016, vol. 25, n° 7, 14p., 21 figs [*DOI :* 10.1142/S0218216516500449], https://hal.archives-ouvertes.fr/hal-01084472

[3] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *Untangling trigonal diagrams*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", June 2016, vol. 25, n° 7, 10p., 24 figs [*DOI :* 10.1142/S0218216516500437], https://hal.archives-ouvertes.fr/hal-01084463

[4] F. CHYZAK, A. QUADRAT, D. ROBERTZ. *Effective algorithms for parametrizing linear control systems over Ore algebras*, in "Applicable Algebra in Engineering, Communications and Computing", 2005, vol. 16, pp. 319–376

[18] http://www.animath.fr
[19] Société Mathématique de France
[20] https://smf.emath.fr/actualites-smf/mathematiques-etonnantes-programme

[5] T. CLUZEAU, A. QUADRAT. *Factoring and decomposing a class of linear functional systems*, in "Linear Algebra and Its Applications", 2008, vol. 428, pp. 324–381

[6] E. FALBEL, A. GUILLOUX. *Dimension of character varieties for 3-manifolds*, in "Proceedings of the American Mathematical Society", 2016 [*DOI :* 10.1090/PROC/13394], https://hal.archives-ouvertes.fr/hal-01370284

[7] E. FALBEL, A. GUILLOUX, P.-V. KOSELEFF, F. ROUILLIER, M. THISTLETHWAITE. *Character Varieties For SL(3,C): The Figure Eight Knot*, in "Experimental Mathematics", 2016, vol. 25, n° 2, 17 p. [*DOI :* 10.1080/10586458.2015.1068249], https://hal.inria.fr/hal-01362208

[8] E. FALBEL, J. WANG. *Branched spherical CR structures on the complement of the figure-eight knot*, in "Michigan Mathematical Journal", 2014, vol. 63, pp. 635-667, https://hal.archives-ouvertes.fr/hal-01374789

[9] A. JOUX. *A one round protocol for tripartite Diffie-Hellman*, in "J. Cryptology", 2004, vol. 17, n° 4, pp. 263–276

[10] A. JOUX, R. LERCIER. *Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the gaussian integer method*, in "Math. Comput.", 2003, vol. 72, n° 242, pp. 953-967

[11] D. LAZARD, F. ROUILLIER. *Solving Parametric Polynomial Systems*, in "Journal of Symbolic Computation", June 2007, vol. 42, pp. 636-667

[12] A. QUADRAT, D. ROBERTZ. *Computation of bases of free modules over the Weyl algebras*, in "Journal of Symbolic Computation", 2007, vol. 42, pp. 1113–1141

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

[14] F. ROUILLIER, P. ZIMMERMANN. *Efficient Isolation of Polynomial Real Roots*, in "Journal of Computational and Applied Mathematics", 2003, vol. 162, n° 1, pp. 33–50

Publications of the year

Articles in International Peer-Reviewed Journals

[15] R. BARBULESCU, S. DUQUESNE. *Updating key size estimations for pairings*, in "Journal of Cryptology", 2019, vol. 32, n° 4, pp. 1298–1336 [*DOI :* 10.1007/s00145-018-9280-5], https://hal.archives-ouvertes.fr/hal-01534101

[16] R. BARBULESCU, J. RAY. *Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture*, in "Journal de Théorie des Nombres de Bordeaux", 2019, forthcoming, https://hal.archives-ouvertes.fr/hal-01534050

[17] E. BARTZOS, I. Z. EMIRIS, J. LEGERSKÝ, E. TSIGARIDAS. *On the maximal number of real embeddings of minimally rigid graphs in* $\mathbb{R}^2$, $\mathbb{R}^3$ *and* S^2, in "Journal of Symbolic Computation", 2019, https://arxiv.org/abs/1811.12800 , forthcoming [*DOI :* 10.1016/J.JSC.2019.10.015], https://hal.archives-ouvertes.fr/hal-02271782

[18] Y. M. BOUZIDI, A. QUADRAT, F. ROUILLIER. *Certified Non-conservative Tests for the Structural Stability of Discrete Multidimensional Systems*, in "Multidimensional Systems and Signal Processing", July 2019, vol. 30, n° 3, 31 p. [*DOI :* 10.1007/S11045-018-0596-Y], https://hal.inria.fr/hal-01951765

[19] L. BUSÉ, A. MANTZAFLARIS, E. TSIGARIDAS. *Matrix formulae for Resultants and Discriminants of Bivariate Tensor-product Polynomials*, in "Journal of Symbolic Computation", June 2020, vol. 98, pp. 65-83 [*DOI :* 10.1016/J.JSC.2019.07.007], https://hal.inria.fr/hal-01654263

[20] I. Z. EMIRIS, A. MANTZAFLARIS, E. TSIGARIDAS. *Multilinear Polynomial Systems: Root Isolation and Bit Complexity*, in "Journal of Symbolic Computation", 2019, Special Issue of the Journal of Symbolic Computation on Milestones in Computer Algebra (MICA 2016), forthcoming, https://hal.inria.fr/hal-02099556

[21] I. Z. EMIRIS, B. MOURRAIN, E. TSIGARIDAS. *Separation bounds for polynomial systems*, in "Journal of Symbolic Computation", 2019 [*DOI :* 10.1016/J.JSC.2019.07.001], https://hal.inria.fr/hal-01105276

[22] T. ESPITAU, A. JOUX. *Certified lattice reduction*, in "Advances in Mathematics of Communications", February 2020, vol. 14, n° 1, pp. 137-159 [*DOI :* 10.3934/AMC.2020011], https://hal.archives-ouvertes.fr/hal-02383752

[23] F. GÖLOĞLU, A. JOUX. *A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms*, in "Mathematics of Computation", 2019, 1 p. , https://hal.archives-ouvertes.fr/hal-01960765

[24] P. MOLIN, C. NEUROHR. *Computing period matrices and the Abel-Jacobi map of superelliptic curves*, in "Mathematics of Computation", 2019, https://hal.inria.fr/hal-02416012

International Conferences with Proceedings

[25] Y. BOUZIDI, T. CLUZEAU, A. QUADRAT. *On the computation of stabilizing controllers of multidimensional systems*, in "SSSC 2019 - 7th IFAC Symposium on Systems Structure and Control", Sinai, Romania, September 2019 [*DOI :* 10.1016/J.IFACOL.2019.11.032], https://hal.inria.fr/hal-02419696

[26] Y. BOUZIDI, T. CLUZEAU, A. QUADRAT, F. ROUILLIER. *On the effective computation of stabilizing controllers of 2D systems*, in "Maple Conference", Waterloo, Canada, October 2019, https://hal.inria.fr/hal-02419719

[27] D. CHABLAT, G. MOROZ, F. ROUILLIER, P. WENGER. *Using Maple to analyse parallel robots*, in "Maple Conference 2019", Waterloo, Canada, October 2019, https://hal.inria.fr/hal-02406703

[28] I. Z. EMIRIS, C. KATSAMAKI. *Voronoi diagram of orthogonal polyhedra in two and three dimensions*, in "SEA 2019 - Symposium on Experimental Algorithms", Kalamata, Greece, I. KOTSIREAS, P. PARDALOS, K. E. PARSOPOULOS, D. SOURAVLIAS, A. TSOKAS (editors), LNCS - Lecture Notes in Computer Science, Springer, June 2019, vol. 11544 [*DOI :* 10.1007/978-3-030-34029-2_1], https://hal.inria.fr/hal-02398736

[29] E. HUBERT, Y. BOUZIDI, R. DAGHER, A. BARRAU, A. QUADRAT. *Algebraic aspects of the exact signal demodulation problem*, in "SSSC 2019 - 7th IFAC Symposium on Systems Structure and Control", Sinaia, Romania, September 2019 [*DOI :* 10.1016/J.IFACOL.2019.11.031], https://hal.inria.fr/hal-02419824

Scientific Books (or Scientific Book chapters)

[30] Y. BOUZIDI, A. POTEAUX, A. QUADRAT. *A symbolic computation approach to the asymptotic stability analysis of differential systems with commensurate delays*, in "Delays and Interconnections: Methodology, Algorithms and Applications, Advances in Delays and Dynamics", G. VALMORBIDA, A. SEURET, I. BOUSSAADA, R. SIPAHI (editors), Springer, October 2019, vol. 10, 16 p. [*DOI :* 10.1007/978-3-030-11554-8_11], https://hal.inria.fr/hal-01485536

[31] T. CLUZEAU, C. KOUTSCHAN, A. QUADRAT, M. TÕNSO. *Effective algebraic analysis approach to linear systems over Ore algebras*, in "Algebraic and Symbolic Computation Methods in Dynamical Systems", Advances in Delays and Dynamics, Springer, 2020, https://hal.archives-ouvertes.fr/hal-02436985

[32] T. CLUZEAU, A. QUADRAT. *Equivalence of Linear Functional Systems*, in "Algebraic and Symbolic Computation Methods in Dynamical Systems", Advances in Delays and Dynamics, Springer, 2020, https://hal.archives-ouvertes.fr/hal-02436978

Other Publications

[33] J. G. ALCÁZAR, J. CARAVANTES, G. M. DIAZ-TOCA, E. TSIGARIDAS. *Computing the topology of a planar or space hyperelliptic curve*, January 2019, working paper or preprint, https://hal.inria.fr/hal-01968776

[34] R. BARBULESCU, N. EL MRABET, L. GHAMMAM. *A taxonomy of pairings, their security, their complexity*, May 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-02129868

[35] R. BARBULESCU, S. SHINDE. *A classification of ECM-friendly families using modular curves*, February 2019, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01822144

[36] R. DAGHER, G. ZHENG, A. QUADRAT. *General closed-form solutions of the position self-calibration problem*, October 2019, Paper under submission, https://hal.inria.fr/hal-02419854

[37] G. IVANYOS, A. JOUX, M. SANTHA. *Discrete logarithm and Diffie-Hellman problems in identity black-box groups*, November 2019, https://arxiv.org/abs/1911.01662 - working paper or preprint, https://hal.sorbonne-universite.fr/hal-02350271

[38] A. JOUX, C. PIERROT. *Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms*, July 2019, https://arxiv.org/abs/1907.02689 - working paper or preprint, https://hal.sorbonne-universite.fr/hal-02173688

References in notes

[39] A. K. LENSTRA, H. W. LENSTRA (editors). *The development of the number field sieve*, Lecture Notes in Mathematics, Springer-Verlag, 1993, vol. 1554

[40] D. AGGARWAL, A. JOUX, A. PRAKASH, M. SANTHA. *A New Public-Key Cryptosystem via Mersenne Numbers*, in "Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III", 2018, pp. 459–482, https://doi.org/10.1007/978-3-319-96878-0_16

[41] S. BASU, R. POLLACK, M.-F. ROY. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*, Springer-Verlag, Berlin, Heidelberg, 2006

[42] V. BAVULA. *The algebra of integro-differential operators on an affine line and its modules*, in "J. Pure Appl. Algebra", 2013, vol. 217, pp. 495–529

[43] N. BERGERON, E. FALBEL, A. GUILLOUX. *Tetrahedra of flags, volume and homology of SL(3)*, in "Geometry & Topology Monographs", 2014, vol. 18 [*DOI :* 10.2140/GT.2014.18.1911], https://hal.archives-ouvertes.fr/hal-01370258

[44] J.-F. BIASSE, T. ESPITAU, P.-A. FOUQUE, A. GÉLIN, P. KIRCHNER. *Computing generator in cyclotomic integer rings*, in "36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2017)", Paris, France, Lecture Notes in Computer Science, April 2017, vol. 10210, pp. 60-88 [*DOI :* 10.1007/978-3-319-56620-7_3], https://hal.archives-ouvertes.fr/hal-01518438

[45] A. BOREL. *Algebraic D-modules*, Perspectives in mathematics, Academic Press, 1987

[46] N. BOSE. *Multidimensional Systems Theory: Progress, Directions and Open Problems in Multidimensional Systems*, Mathematics and Its Applications, Springer Netherlands, 2001

[47] F. BOULIER, D. LAZARD, F. OLLIVIER, M. PETITOT. *Computing representations for radicals of finitely generated differential ideals*, in "Applicable Algebra in Engineering, Communication and Computing", 2009, vol. 20, pp. 73–121

[48] Y. BOUZIDI, T. CLUZEAU, G. MOROZ, A. QUADRAT. *Computing effectively stabilizing controllers for a class of nD systems*, in "The 20th World Congress of the International Federation of Automatic Control", Toulouse, France, July 2017, vol. 50, n° 1, pp. 1847 – 1852 [*DOI :* 10.1016/J.IFACOL.2017.08.200], https://hal.archives-ouvertes.fr/hal-01667161

[49] Y. BOUZIDI, S. LAZARD, G. MOROZ, M. POUGET, F. ROUILLIER. *Improved algorithm for computing separating linear forms for bivariate systems*, in "ISSAC - 39th International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, July 2014, https://hal.inria.fr/hal-00992634

[50] Y. BOUZIDI, S. LAZARD, G. MOROZ, M. POUGET, F. ROUILLIER, M. SAGRALOFF. *Solving bivariate systems using Rational Univariate Representations*, in "Journal of Complexity", 2016, vol. 37, pp. 34–75 [*DOI :* 10.1016/J.JCO.2016.07.002], https://hal.inria.fr/hal-01342211

[51] Y. BOUZIDI, S. LAZARD, M. POUGET, F. ROUILLIER. *Separating linear forms and Rational Univariate Representations of bivariate systems*, in "Journal of Symbolic Computation", May 2015, vol. 68, n° 0, pp. 84-119 [*DOI :* 10.1016/J.JSC.2014.08.009], https://hal.inria.fr/hal-00977671

[52] Y. BOUZIDI, A. POTEAUX, A. QUADRAT. *A symbolic computation approach to the asymptotic stability analysis of differential systems with commensurate delays*, in "Delays and Interconnections: Methodology, Algorithms and Applications", Advances on Delays and Dynamics at Springer, Springer Verlag, March 2017, https://hal.inria.fr/hal-01485536

[53] Y. BOUZIDI, A. QUADRAT, F. ROUILLIER. *Computer algebra methods for testing the structural stability of multidimensional systems*, in " IEEE 9th International Workshop on Multidimensional (nD) Systems (IEEE nDS 2015)", Vila Real, Portugal, Proceedings of the IEEE 9th International Workshop on Multidimensional (nD) Systems (IEEE nDS 2015), September 2015, https://hal-centralesupelec.archives-ouvertes.fr/hal-01259968

[54] Y. BOUZIDI, A. QUADRAT, F. ROUILLIER. *Certified Non-conservative Tests for the Structural Stability of Multidimensional Systems*, August 2017, 31 p. , To appear in Multidimensional Systems and Signal Processing, https://link.springer.com/article/10.1007/s11045-018-0596-y, https://hal.inria.fr/hal-01571230

[55] Y. BOUZIDI, F. ROUILLIER. *Certified Algorithms for proving the structural stability of two dimensional systems possibly with parameters*, in "MNTS 2016 - 22nd International Symposium on Mathematical Theory of Networks and Systems", Minneapolis, United States, Proceedings of the 22nd International Symposium on Mathematical Theory of Networks and Systems, July 2016, https://hal.inria.fr/hal-01366202

[56] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *On the lexicographic degree of two-bridge knots*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", June 2016, vol. 25, n^{o} 7, 14p., 21 figs [*DOI :* 10.1142/S0218216516500449], https://hal.archives-ouvertes.fr/hal-01084472

[57] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *Untangling trigonal diagrams*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", June 2016, vol. 25, n^{o} 7, 10p., 24 figs [*DOI :* 10.1142/S0218216516500437], https://hal.archives-ouvertes.fr/hal-01084463

[58] E. BRUGALLÉ, P.-V. KOSELEFF, D. PECKER. *The lexicographic degree of the first two-bridge knots*, September 2018, 30 p., 58 fig., 6 tables, submitted, https://hal.archives-ouvertes.fr/hal-01108678

[59] D. CHABLAT, R. JHA, F. ROUILLIER, G. MOROZ. *Non-singular assembly mode changing trajectories in the workspace for the 3-RPS parallel robot*, in "14th International Symposium on Advances in Robot Kinematics", Ljubljana, Slovenia, June 2014, pp. 149 – 159, https://hal.archives-ouvertes.fr/hal-00956325

[60] D. CHABLAT, R. JHA, F. ROUILLIER, G. MOROZ. *Workspace and joint space analysis of the 3-RPS parallel robot*, in "ASME 2013 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference", Buffalo, United States, August 2014, vol. Volume 5A, pp. 1-10, https://hal.archives-ouvertes.fr/hal-01006614

[61] F. CHYZAK, A. QUADRAT, D. ROBERTZ. *Effective algorithms for parametrizing linear control systems over Ore algebras*, in "Applicable Algebra in Engineering, Communications and Computing", 2005, vol. 16, pp. 319–376

[62] F. CHYZAK, B. SALVY. *Non-commutative elimination in Ore algebras proves multivariate identities*, in "Journal of Symbolic Computation", 1998, vol. 26, n^{o} 2, pp. 187–227

[63] G. E. COLLINS. *Quantifier elimination for real closed fields by cylindrical algebraic decompostion*, in "Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20–23, 1975", Berlin, Heidelberg, H. BRAKHAGE (editor), Springer Berlin Heidelberg, 1975, pp. 134–183

[64] D. A. COX, J. LITTLE, D. O'SHEA. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*, Springer-Verlag, Berlin, Heidelberg, 2007

[65] M. CROCCO, A. DEL BUE, V. MURINO. *A bilinear approach to the position self-calibration of multiple sensors*, in "IEEE Transactions on Signal Processing", 2012, vol. 60, n^{o} 2, pp. 660–673

[66] R. CURTAIN, H. ZWART. *An Introduction to Infinite-Dimensional Linear Systems Theory*, Texts in Applied Mathematics, Springer New York, 2012

[67] R. DAGHER, A. QUADRAT, G. ZHENG. *Auto-localisation par mesure de distances*, in "Pattern n. FR1853553", 2018

[68] R. DAGHER, A. QUADRAT, G. ZHENG. *Algebraic solutions to the metric multidimensional unfolding. Application to the position self-calibration problem*, in "in preparation", 2019

[69] M. DERAUX, E. FALBEL. *Complex hyperbolic geometry of the figure eight knot*, in "Geometry and Topology", February 2015, vol. 19, pp. 237–293 [*DOI :* 10.2140/GT.2015.19.237], https://hal.archives-ouvertes.fr/hal-00805427

[70] D. N. DIATTA, S. DIATTA, F. ROUILLIER, M.-F. ROY, M. SAGRALOFF. *Bounds for polynomials on algebraic numbers and application to curve topology*, October 2018, working paper or preprint, https://hal.inria.fr/hal-01891417

[71] W. DIFFIE, M. E. HELLMAN. *New directions in cryptography*, in "IEEE Transactions on Information Theory", 1976, vol. 22, n^{o} 6, pp. 644-654

[72] S. DIOP. *Elimination in control theory*, in "Math. Control Signals Systems", 1991, vol. 4, pp. 17–32

[73] S. DIOP. *Differential-algebraic decision methods and some applications to system theory*, in "Theoret. Comput. Sci.", 1992, vol. 98, pp. 137–161

[74] J. DOLISKANI, A. K. NARAYANAN, É. SCHOST. *Drinfeld Modules with Complex Multiplication, Hasse Invariants and Factoring Polynomials over Finite Fields*, in "CoRR", 2017, vol. abs/1712.00669, http://arxiv.org/abs/1712.00669

[75] T. ESPITAU, A. JOUX. *Adaptive precision LLL and Potential-LLL reductions with Interval arithmetic*, in "IACR Cryptology ePrint Archive", 2016, vol. 2016, 528 p. , http://eprint.iacr.org/2016/528

[76] H. EVELYNE. *Notes on Triangular Sets and Triangulation-Decomposition Algorithms II: Differential Systems*, in "Symbolic and Numerical Scientific Computation", F. WINKLER, U. LANGER (editors), Lecture Notes in Computer Science 2630, Springer, 2003, pp. 40-87

[77] E. FALBEL, A. GUILLOUX. *Dimension of character varieties for 3-manifolds*, in "Proceedings of the American Mathematical Society", 2016 [*DOI :* 10.1090/PROC/13394], https://hal.archives-ouvertes.fr/hal-01370284

[78] E. FALBEL, A. GUILLOUX, P. WILL. *Hilbert metric, beyond convexity*, 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01768400

[79] E. FALBEL, P.-V. KOSELEFF, F. ROUILLIER. *Representations of fundamental groups of 3-manifolds into PGL(3,C): Exact computations in low complexity*, in "Geometriae Dedicata", August 2015, vol. 177, n^{o} 1, 52 p. [*DOI :* 10.1007/s10711-014-9987-x], https://hal.inria.fr/hal-00908843

[80] E. FALBEL, M. MACULAN, G. SARFATTI. *Configurations of flags in orbits of real forms*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01779459

[81] E. FALBEL, R. SANTOS THEBALDI. *A Flag structure on a cusped hyperbolic 3-manifold with unipotent holonomy*, in "Pacific Journal of Mathematics", 2015, vol. 278, n^{o} 1, pp. 51-78, https://hal.archives-ouvertes.fr/hal-00958255

[82] E. FALBEL, J. VELOSO. *Flag structures on real 3-manifolds*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01778582

[83] J. FAUGÈRE, D. LAZARD. *Combinatorial classes of parallel manipulators*, in "Mechanism and Machine Theory", 1995, vol. 30, n^{o} 6, pp. 765 – 776 [*DOI :* 10.1016/0094-114X(94)00069-W], http://www.sciencedirect.com/science/article/pii/0094114X9400069W

[84] M. FLIESS, H. SIRA-RAMIREZ. *An algebraic framework for linear identification*, in "ESAIM Control Optim. Calc. Variat.", 2003, vol. 9, pp. 151—168

[85] J. V. Z. GATHEN, J. GERHARD. *Modern Computer Algebra*, 3rd, Cambridge University Press, New York, NY, USA, 2013

[86] A. GUILLOUX. *Volume of representations and birationality of peripheral holonomy*, in "Experimental Mathematics", May 2017, https://hal.archives-ouvertes.fr/hal-01370287

[87] A. GUILLOUX, I. KIM. *Deformation space of discrete groups of SU(2,1) in quaternionic hyperbolic plane*, March 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01736953

[88] A. GUILLOUX, J. MARCHÉ. *Volume function and Mahler measure of exact polynomials*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01758986

[89] A. GUILLOUX, P. WILL. *On SL(3,C)-representations of the Whitehead link group*, 2018, To appear in Geom. Ded, https://hal.archives-ouvertes.fr/hal-01370289

[90] A. GÉLIN, A. JOUX. *Reducing number field defining polynomials: an application to class group computations*, in "Algorithmic Number Theory Symposium XII", Kaiserslautern, Germany, LMS Journal of Computation and Mathematics, August 2016, vol. 19, n^{o} A, pp. 315–331 [*DOI :* 10.1112/S1461157016000255], https://hal.archives-ouvertes.fr/hal-01362144

[91] F. GÖLOĞLU, A. JOUX. *A Simplified Approach to Rigorous Degree 2 Elimination in Discrete Logarithm Algorithms*, in "IACR Cryptology ePrint Archive", 2018, vol. 2018, 430 p. , https://eprint.iacr.org/2018/430

[92] E. HUBERT, A. BARRAU, M. EL BADAOUI. *New Multi-Carrier Demodulation Method Applied to Gearbox Vibration Analysis*, 04 2018, pp. 2141-2145 [*DOI :* 10.1109/ICASSP.2018.8461924]

[93] M. L. HUSTY, H.-P. SCHRÖCKER. *Algebraic Geometry and Kinematics*, in "Nonlinear Computational Geometry", New York, NY, I. Z. EMIRIS, F. SOTTILE, T. THEOBALD (editors), Springer New York, 2010, pp. 85–107

[94] M. JANET. *Leçons sur les systèmes d'équations aux dérivées partielles*, Gauthier-Villars, 1929

[95] R. JHA, D. CHABLAT, L. BARON, F. ROUILLIER, G. MOROZ. *Workspace, Joint space and Singularities of a family of Delta-Like Robot*, in "Mechanism and Machine Theory", September 2018, vol. 127, pp. 73-95 [*DOI :* 10.1016/J.MECHMACHTHEORY.2018.05.004], https://hal.archives-ouvertes.fr/hal-01796066

[96] R. JHA, D. CHABLAT, F. ROUILLIER, G. MOROZ. *An algebraic method to check the singularity-free paths for parallel robots*, in "International Design Engineering Technical Conferences & Computers and Information in Engineering Conference", Boston, United States, ASME, August 2015, https://hal.archives-ouvertes.fr/hal-01142989

[97] R. JHA, D. CHABLAT, F. ROUILLIER, G. MOROZ. *Workspace and Singularity analysis of a Delta like family robot*, in "4th IFTOMM International Symposium on Robotics and Mechatronics", Poitiers, France, June 2015, https://hal.archives-ouvertes.fr/hal-01142465

[98] A. JOUX, R. LERCIER. *The function field sieve is quite special*, in "Algorithmic Number Theory-ANTS V", Lecture Notes in Computer Science, Springer, 2002, vol. 2369, pp. 431-445

[99] A. JOUX, C. PIERROT. *Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms - Simplified Setting for Small Characteristic Finite Fields*, in "20th International Conference on the Theory and Application of Cryptology and Information Security", Kaoshiung, Taiwan, Lecture Notes in Computer Science, Springer Berlin Heidelberg, December 2014, vol. 8873, pp. 378-397 [*DOI :* 10.1007/978-3-662-45611-8_20], https://hal.archives-ouvertes.fr/hal-01213649

[100] A. JOUX, C. PIERROT. *Nearly Sparse Linear Algebra and application to Discrete Logarithms Computations*, in "Contemporary Developments in Finite Fields and Applications ", WorldScientific, 2016 [*DOI :* 10.1142/9789814719261_0008], https://hal.inria.fr/hal-01154879

[101] H. L. JR.. *Factoring integers with elliptic curves*, in "Annals of Mathematics", 1987, vol. 126, n^{o} 2, pp. 649–673

[102] T. KAILATH. *Linear Systems*, Prentice-Hall, 1980

[103] M. KASHIWARA. *Algebraic study of systems of partial differential equations*, Mémoires de la S. M. F., 1995, vol. 63, Master's thesis 1970 (English translation)

[104] M. KASHIWARA, T. KAWAI, T. KIMURA. *Foundations of Algebraic Analysis*, Princeton University Press, 1986, vol. 37

[105] A. KOBEL, F. ROUILLIER, M. SAGRALOFF. *Computing Real Roots of Real Polynomials ... and now For Real!*, in " ISSAC '16 Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation", Waterloo, Canada, ISSAC '16 Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, July 2016, 7 p. [*DOI :* 10.1145/2930889.2930937], https://hal.inria.fr/hal-01363955

[106] N. KOBLITZ. *Elliptic curve cryptosystems*, in "Mathematics of Computation", January 1987, vol. 48, n^{o} 177, pp. 203–209

[107] E. KOLCHIN. *Differential Algebra & Algebraic Groups*, Pure and Applied Mathematics, Elsevier Science, 1973

[108] P.-V. KOSELEFF, D. PECKER. *Chebyshev Knots*, in "Journal of Knot Theory and Its Ramifications", April 2011, vol. 20, n^{o} 4, pp. 575-593 [*DOI :* 10.1142/S0218216511009364], https://hal.archives-ouvertes.fr/hal-00344501

[109] P.-V. KOSELEFF, D. PECKER. *On Alexander–Conway polynomials of two-bridge links*, in "Journal of Symbolic Computation", May 2015, vol. Volume 68, n^{o} 2, pp. 215-229, 15p [*DOI :* 10.1016/J.JSC.2014.09.011], https://hal.archives-ouvertes.fr/hal-00538729

[110] P.-V. KOSELEFF, D. PECKER. *Harmonic Knots*, in "Journal Of Knot Theory And Its Ramifications (JKTR)", 2016, vol. 25, n^{o} 13, 18 p. , 18 p., 30 fig. [*DOI :* 10.1142/S0218216516500747], https://hal.archives-ouvertes.fr/hal-00680746

[111] P.-V. KOSELEFF, D. PECKER, F. ROUILLIER. *The first rational Chebyshev knots*, in "Journal of Symbolic Computation", December 2010, vol. 45, n^{o} 12, pp. 1341-1358 [*DOI :* 10.1016/J.JSC.2010.06.014], https://hal.archives-ouvertes.fr/hal-00429510

[112] P.-V. KOSELEFF, D. PECKER, F. ROUILLIER, C. TRAN. *Computing Chebyshev knot diagrams*, in "Journal of Symbolic Computation", 2018, vol. 86, 21 p. [*DOI :* 10.1016/J.JSC.2017.04.001], https://hal.inria.fr/hal-01232181

[113] P.-V. KOSELEFF, F. ROUILLIER, C. TRAN. *On the sign of a trigonometric expression*, in "ISSAC ' 15", Bath, United Kingdom, Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, July 2015 [*DOI :* 10.1145/2755996.2756664], https://hal.inria.fr/hal-01200820

[114] B. A. LAMACCHIA, A. M. ODLYZKO. *Computation of discrete logarithms in prime fields*, in "Designs, Codes and Cryptography", 1991, vol. 1, pp. 47–62

[115] S. LAZARD, M. POUGET, F. ROUILLIER. *Bivariate triangular decompositions in the presence of asymptotes*, in "Journal of Symbolic Computation", 2017, vol. 82, pp. 123 – 133 [*DOI :* 10.1016/J.JSC.2017.01.004], https://hal.inria.fr/hal-01468796

[116] V. MILLER. *Use of elliptic curves in cryptography*, in "Advances in Cryptology — CRYPTO'85", H. WILLIAMS (editor), LNCS, Springer, 1986, vol. 218, pp. 417–428

[117] B. MOURRAIN. *The 40 Generic Positions of a Parallel Robot*, in "Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation", New York, NY, USA, ISSAC '93, ACM, 1993, pp. 173–182, http://doi.acm.org/10.1145/164081.164120

[118] D. NIANG DIATTA, F. ROUILLIER, M.-F. ROY. *On the computation of the topology of plane curves*, in "International Symposium on Symbolic and Algebraic Computation", Kobe, Japan, K. NABESHIMA (editor), ACM Press, July 2014, pp. 130-137 [*DOI :* 10.1145/2608628.2608670], https://hal.archives-ouvertes.fr/hal-00935728

[119] U. OBERST. *Multidimensional constant linear systems*, in "Acta Appl. Math.", 1990, vol. 20, pp. 1–175

[120] C. POMERANCE. *Analysis and comparison of some integer factoring methods*, in "Computational methods in number theory – Part I", Amsterdam, J. HENDRIK W. LENSTRA, R. TIJDEMAN (editors), Mathematical centre tracts, Mathematisch Centrum, 1982, vol. 154, pp. 8–139

[121] POMMARET. *Systems of Partial Differential Equations and Lie Pseudogroups*, Ellis Horwood Series in Mathematics and its Applications, Gordon and Breach Science Publishers, 1978

[122] A. QUADRAT. *Grade filtration of linear functional systems*, in "Acta Applicandæ Mathematicæ", October 2013, vol. 127, n^{o} 1, pp. 27–86 [*DOI :* 10.1007/s10440-012-9791-2], https://hal-supelec.archives-ouvertes.fr/hal-00925510

[123] A. QUADRAT. *Noncommutative geometric structures on stabilizable infinite-dimensional linear systems*, in "ECC 2014", Strasbourg, France, June 2014, pp. 2460 – 2465 [*DOI :* 10.1109/ECC.2014.6862563], https://hal-supelec.archives-ouvertes.fr/hal-01108019

[124] A. QUADRAT. *A constructive algebraic analysis approach to Artstein's reduction of linear time-delay systems*, in "12th IFAC Workshop on Time Delay Systems", Ann Arbor, United States, Proceedings of 12th IFAC Workshop on Time Delay Systems, University of Michigan, May 2016, https://hal-centralesupelec.archives-ouvertes.fr/hal-01259862

[125] A. QUADRAT. *Towards an effective study of the algebraic parameter estimation problem*, in " IFAC 2017 Workshop Congress", Toulouse, France, July 2017, https://hal.inria.fr/hal-01415300

[126] A. QUADRAT, G. REGENSBURGER. *Computing Polynomial Solutions and Annihilators of Integro-Differential Operators with Polynomial Coefficients*, Inria Lille - Nord Europe ; Institute for Algebra, Johannes Kepler University Linz, December 2016, n^{o} RR-9002, 24 p. , https://hal.inria.fr/hal-01413907

[127] A. QUADRAT, D. ROBERTZ. *A constructive study of the module structure of rings of partial differential operators*, in "Acta Applicandæ Mathematicæ", 2014, vol. 133, pp. 187–243 [*DOI :* 10.1007/s10440-013-9864-x], https://hal-supelec.archives-ouvertes.fr/hal-00925533

[128] A. QUADRAT, R. USHIROBIRA. *Algebraic analysis for the Ore extension ring of differential time-varying delay operators*, in " 22nd International Symposium on Mathematical Theory of Networks and Systems (MTNS)", Minneapolis, United States, July 2016, 8 p. , https://hal.inria.fr/hal-01415256

[129] G. RANCE, Y. BOUZIDI, A. QUADRAT, A. QUADRAT. *A symbolic-numeric method for the parametric H∞ loop-shaping design problem*, in "22nd International Symposium on Mathematical Theory of Networks and Systems (MTNS) ", Minneapolis, United States, July 2016, 8 p. , https://hal.inria.fr/hal-01415294

[130] G. RANCE, Y. BOUZIDI, A. QUADRAT, A. QUADRAT. *Explicit H∞ controllers for 1st to 3rd order single-input single-output systems with parameters*, in " IFAC 2017 Workshop Congress ", Toulouse, France, July 2017, https://hal.inria.fr/hal-01667410

[131] G. RANCE, Y. BOUZIDI, A. QUADRAT, A. QUADRAT, F. ROUILLIER. *Explicit H∞ controllers for 4th order single-input single-output systems with parameters and their applications to the two mass-spring system with damping*, in " IFAC 2017 Workshop Congress ", Toulouse, France, July 2017, https://hal.inria.fr/hal-01667368

[132] G. RANCE. *Parametric H_∞ control and its application to gyrostabilized sights*, Université Paris-Saclay, July 2018, https://tel.archives-ouvertes.fr/tel-01904086

[133] J. RITT. *Differential Algebra*, Colloquium publications, American Mathematical Society, 1950

[134] R. RIVEST, A. SHAMIR, L. ADLEMAN. *A method for obtaining digital signatures and public-key cryptosystems*, in "Commun. ACM", 1978, vol. 21, n^{o} 2, pp. 120–126

[135] D. ROBERTZ. *Formal Algorithmic Elimination for PDEs*, Lecture Notes in Mathematics 2121, Springer, 2014

[136] J. ROTMAN. *An Introduction to Homological Algebra*, Universitext, Springer New York, 2008

[137] J. T. STAFFORD. *Module structure of Weyl algebras*, in "J. London Math. Soc.", 1978, vol. 18, pp. 429–442

[138] V. A. VASSILIEV. *Cohomology of knot spaces*, in "Theory of singularities and its applications", Adv. Soviet Math., Amer. Math. Soc., Providence, RI, 1990, vol. 1, pp. 23–69

[139] J. WEEKS. *Chapter 10 - Computation of Hyperbolic Structures in Knot Theory*, in "Handbook of Knot Theory", Amsterdam, W. MENASCO, M. THISTLETHWAITE (editors), Elsevier Science, 2005, pp. 461 – 480 [*DOI :* 10.1016/B978-044451452-3/50011-3], http://www.sciencedirect.com/science/article/pii/B9780444514523500113

[140] P. WENGER. *A new general formalism for the kinematic analysis of all nonredundant manipulators*, in "ICRA", 1992

[141] J. WILLEMS, J. POLDERMAN. *Introduction to Mathematical Systems Theory: A Behavioral Approach*, Texts in Applied Mathematics, Springer New York, 2013