RESEARCH CENTRE

**Inria Paris Centre at Sorbonne University**

**IN PARTNERSHIP WITH:**

**CNRS, Université Denis Diderot (Paris 7), Sorbonne Université**

2023
ACTIVITY REPORT

Project-Team

# OURAGAN

## Tools for resolutions in algebra, geometry and their applications

**IN COLLABORATION WITH: Institut de Mathématiques de Jussieu**

**DOMAIN**

**Algorithmics, Programming, Software and Architecture**

**THEME**

**Algorithmics, Computer Algebra and Cryptology**

# Contents

# Project-Team OURAGAN

*Creation of the Project-Team: 2019 May 01*

## Keywords

### Computer sciences and digital sciences

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 members, visitors, external collaborators

## Research Scientists

- Fabrice Rouillier [Team leader, INRIA, Senior Researcher, HDR]
- Yves Guiraud [INRIA, Researcher, HDR]
- Alban Quadrat [INRIA, Senior Researcher, HDR]
- Elias Tsigaridas [INRIA, Researcher]

## Faculty Members

- Jean Bajard [SORBONNE UNIVERSITE, Professor, HDR]
- Martin Deraux [UGA, Associate Professor Delegation, until Aug 2023]
- Elisha Falbel [SORBONNE UNIVERSITE, Professor, HDR]
- Antonin Guilloux [Sorbonne Université, Associate Professor, HDR]
- Antoine Joux [SORBONNE UNIVERSITE, Associate Professor, HDR]
- Pierre-Vincent Koseleff [SORBONNE UNIVERSITE, Associate Professor, HDR]
- Pascal Molin [UNIV PARIS - CITE, Associate Professor]
- Cathy Swaenepoel [UNIV PARIS - CITE, Associate Professor, from Nov 2023]

## Post-Doctoral Fellows

- Aurélien Gribinski [INRIA, Post-Doctoral Fellow]
- Manuel Radons [INRIA, Post-Doctoral Fellow, until Mar 2023]
- Owen Rouillé [Sorbonne Université, until Aug 2023]
- Grégoire Sergeant-Perthuis [INRIA, Post-Doctoral Fellow, until Aug 2023]

## PhD Students

- Thibauld Feneuil [CryptoExperts, until Sep 2023]
- Alexandre Lê [SAFRAN, CIFRE]
- Pierre Morain [SORBONNE UNIVERSITE, from Sep 2023]
- Camille Pinto [INRIA]
- Joao Ruiz [Sorbonne Université, from Aug 2023]
- Chaoping Zhu [Sorbonne Université]

## Technical Staff

- Christina Katsamaki [INRIA, Engineer, from Sep 2023]

### Interns and Apprentices

- Florian Chatel [INRIA, Intern, from Apr 2023 until Jul 2023]
- Nicolas Doineau [INRIA, Intern, from May 2023 until Jul 2023]
- Anwar El Rhirhayi [INRIA, Intern, from Mar 2023 until Jul 2023]
- Jules Tsukahara [INRIA, Intern, from May 2023 until Oct 2023]

### Administrative Assistants

- Laurence Bourcier [INRIA]
- Julien Guieu [INRIA]

## 2 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 functions 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.

## 2.1 Scientific ground

### 2.1.1 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 [69], subresultants [91], critical-point methods [46], 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 [110] [17], rational parameterizations of solutions of zero-dimensional systems with rational coefficients [55] [16] or discriminant varieties for solving systems depending on parameters [14], but we are also power users of existing software (mainly Sage [1], Maple [2], Pari-GP [3],Snappea [4]) and

[1] www.sagemath.org

[2] maplesoft.com

[3] pari.math.u-bordeaux.fr

[4] www.geometrygames.org/SnapPea

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 [105] (for example to make progress on the computation of class groups in number fields [92]), network reductions by means of LLL variants [80] and, obviously, various computations in linear algebra, for example dedicated to *almost sparse* matrices [106].

For the algorithmic approach to algebraic analysis of functional equations [50] [108] [109], we developed the effective study of both module theory and homological algebra [142] over certain non-commutative polynomial rings of functional operators [4], of Stafford's famous theorems on the Weyl algebras [133], of the equidimensional decomposition of functional systems [129], etc.

Finally, we study effective methods in algebraic topology, with a view towards the computation of normal forms or bases, and the construction of small resolutions of various algebraic structures: monoids and groups, algebras and operads, categories and higher structures, etc. The construction methods can come from combinatorial group theory (rewriting, Garside structures), combinatorial algebra (Gröbner bases), or homological algebra (Koszul duality, Morse theory). We explore potential deep foundational connexions between these different points of view, to unify, generalise and improve them.

### 2.1.2 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 [76], where they proposed a first instantiation of their paradigm based on the discrete logarithm problem in prime fields. The invention of RSA [140], based on the hardness of factoring came as a second example. The introduction of discrete logarithms on elliptic curves [111] [144] 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) [122],
- the quadratic field for factoring [126] and its variant for discrete log called the Gaussian integers method [119],
- the number field sieve (NFS) [121].

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

[5] gmplib.org
[6] www.mpfr.org
[7] flintlib.org
[8] arblib.org
[9] www.lmfdb.org

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[13]. 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 [104].

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 [105, 93].

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 [12].

The computations of *class groups in number fields* have 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 [92], 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 [49].

### 2.1.3 Topology in small dimension

**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 [146] 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.

[10] www.math.uic.edu/t3m/SnapPy

[11] regina-normal.github.io

[12] as part of the CURVE project

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 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 [48][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 [85] 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*.

**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[145].

A Chebyshev knot [113], 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 [114] 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 [116]. On the other hand, we propose the identification of Chebyshev knot diagrams [117] by developing new certified algorithms for computing trigonometric expressions [118]. These works share many tools with our action in visualization and computational geometry.

[13] www.math.uic.edu/t3m/SnapPy/ptolemy.html

[14] ANR project Structures Géométriques et Triangulations

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 ( [115]).

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 [62] [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 [61], the slide isotopies on trigonal diagrams, namely those that never increase the number of crossings [63].

**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: 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 [68], 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 [55, 110, 56, 57] which are basic engines for computing the topology [124, 75] and/or plotting.

### 2.1.4 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. [100] [108] [109] [112] [139] [127].

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* [108, 109, 50], a mathematical theory developed by the Japanese school of Sato, which studies linear differential

[15] Minimal degrees are listed in webusers.imj-prg.fr/ pierre-vincent.koseleff/knots/2bk-lexdeg.html

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 [100, 67, 141], differential algebra [52] [81], Spencer's theory [127], 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 [67]). Based on the effective aspects to algebraic analysis approach, the parametrizability problem [4], the reduction and (Serre) decomposition problems [5], the equidimensional decomposition [129], Stafford's famous theorems for the Weyl algebras [133], etc., have been studied and solutions have been implemented in `Maple`, `Mathematica`, and `GAP` [66][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 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.

Elimination theory is also deeply connected to Gröbner bases and rewriting, which are themselves linked to Garside theory and Koszul duality, establishing a continuum with the effective methods studied in algebraic topology.

**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 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 [75, 120, 56] 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 [79] have used them to provide some fast sophisticated factoring algorithms. As a consequence, it is natural to include these objects in our research directions.

**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

**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 [85, 97]; 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 [82]. 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 [86, 88]. 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 [95] and [97]). 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 [74, 87, 83].

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 [94]. Then, theoretical discussions around this conjecture led to a paper on a new approach to the Mahler measure of some 2-variables polynomials [96]. 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.

**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.

**Visualization 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

[16] for example the first rational knots are listed at team.Inria.fr/ouragan/knots

[17] isotop.gamble.loria.fr

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.

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 [142] which play important roles in algebraic analysis [50, 108, 109] 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 [128, 132] which play an important role in mathematical systems theory, control theory, and signal processing [128, 138, 131, 134].

The rings of integro-differential operators are highly more complicated than the purely differential case (i.e. Weyl algebras) [15], due to the existence of zero-divisors, or the fact of having a coherent ring instead of a noetherian ring [47]. Therefore, we want to develop an algorithmic study of these rings. Following the direction initiated in [132] 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 [143], algorithmically developed in [15] 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 [128, 131] 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) [45]. 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 [99]. For example, one can find algebraic proofs for the 40 possible solutions to the direct kinematics problem [123] for steward platforms and companion experiments based on Gröbner basis computations [89]. 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 [147]).

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 [65, 64, 101, 103, 102] 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 [51] on control theory of multidimensional systems. Moreover, the differential algebra approach to nonlinear control theory (see [78, 77] and the references therein) was a major motivation for the algorithmic study of differential algebra [52, 81]. Finally, the behaviour approach to linear systems theory [148, 125] advocates for an algorithmic study of algebraic analysis (see Section 2.1.4). 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 [51, 125] and infinite-dimensional systems [71] (such as 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 [107]. While extending those tests to multidimensional systems or differential time-delay systems, one had to tackle multivariate problems recursively with respect to the variables [51]. 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 [58, 59, 60]. 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, 59, 60] 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 [57, 56].

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 [54, 130, 136, 135, 137, 138].

## 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 [70] 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 [72] 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 [73]. 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* [98] 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 $\operatorname{argmin}_{u\in\mathbb{C}^n, v_1, v_2\in\mathbb{C}^m} \| M - u\, v_1^\star - D\, u\, v_2^\star \|_F$, 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 $v^\star$ is the Hermitian transpose of $v$. We have recently obtained closed-form solutions for the exact problem, i.e., $M = u\, v_1^\star + D\, u\, v_2^\star$, 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 [90], the problem consists in estimating a set $\theta$ 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 $\gamma$ denotes a structured perturbation and $\varpi$ a noise. It has been shown that $\theta$ can sometimes be explicitly determined by means of closed-form expressions using iterated integrals of $y$. These integrals are used to filter the noise $\varpi$. 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 [131] 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 Social and environmental responsibility

No particular action this year.

# 6 Highlights of the year

- Christina Katsamaki ([41]) and Thibauld Feneuil ([40]) defended their PhD thesis.
- Antonin Guilloux is the PI of a new ANR pgoject named *HibertXField* around generalizations of Hilbert's geometry on convex real affine spaces.
- Yves Guiraud has participated to a collective book on the theoretical foundations of higher-dimensional rewriting and its applications in algebraic topology, group theory and higher algebra [38]. This 666-page monography is currently under press, to appear in the London Mathematical Society Lecture Note Series in 2024.

# 7 New software, platforms, open data

## 7.1 New software

### 7.1.1 A NewDsc

**Name:** A New Descartes

**Keyword:** Scientific computing

**Functional Description:** Computations of the real roots of univariate polynomials with rational coefficients.

**URL:** `https://anewdsc.mpi-inf.mpg.de`

**Authors:** Fabrice Rouillier, Alexander Kobel, Michael Sagraloff

**Contact:** Fabrice Rouillier

**Partner:** Max Planck Institute for Software Systems

### 7.1.2 Catex

**Keywords:** LaTeX, String diagram, Algebra

**Functional Description:** Catex is a Latex package and an external tool to typeset string diagrams easily from their algebraic expression. Catex works similarly to Bibtex.

**URL:** `https://plmlab.math.cnrs.fr/guiraud/catex`

**Contact:** Yves Guiraud

**Participant:** Yves Guiraud

### 7.1.3 Cox

**Keywords:** Computer algebra system (CAS), Rewriting systems, Algebra

**Functional Description:** Cox is a Python library for the computation of coherent presentations of Artin monoids, with experimental features to compute the lower dimensions of the Salvetti complex.

**URL:** `https://plmlab.math.cnrs.fr/guiraud/cox`

**Publications:** hal-00682233, hal-00818253

**Contact:** Yves Guiraud

**Participant:** Yves Guiraud

### 7.1.4 dCat

**Keywords:** Rewriting, Algebra, Termination, Complexity

**Functional Description:** dCat is a prototype for the automatic research of complexity bounds of polygraphic programs. It relies on the "termination by derivation" technique introduced in Termination orders for 3-dimensional rewriting and adapted to complexity analysis in Polygraphic programs and polynomial-time functions.

**URL:** https://plmlab.math.cnrs.fr/guiraud/dcat

**Publications:** tel-00006863, hal-00092196, hal-00092204, inria-00129391, inria-00122932

**Contact:** Yves Guiraud

**Participants:** Yves Guiraud, Frederic Blanqui

### 7.1.5 Garside.jl

**Keywords:** Algebra, Garside, Computer algebra

**Functional Description:** Garside.jl is a Julia library for the explicit computation of a minimal resolution (resolution by lcms) of Garside monoids, including the classical and dual braid monoids in spherical type, and dual monoids of some complex reflection groups.

**URL:** https://plmlab.math.cnrs.fr/guiraud/garside.jl

**Contact:** Yves Guiraud

**Participant:** Yves Guiraud

### 7.1.6 ISOTOP

**Name:** 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.

**URL:** https://isotop.gamble.loria.fr/

**Publications:** hal-00809430, hal-00809425, inria-00329754, inria-00580431, hal-00992634, hal-01342211, inria-00425383, inria-00517175, hal-01468796, hal-00977671

**Contact:** Marc Pouget

**Participants:** Luis Penaranda, Marc Pouget, Sylvain Lazard

### 7.1.7 MPFI

**Name:** Multiple Precision Floating-point Interval

**Keyword:** Arithmetic

**Functional Description:** MPFI is a C library based on MPFR and GMP for arbitrary precision interval arithmetic.

**Release Contributions:** Updated for the autoconf installation. New functions added: rev_sqrt, exp10, exp2m1, exp10m1, log2p1, log10p1.

**URL:** https://gitlab.inria.fr/mpfi/mpfi

**Contact:** Nathalie Revol

### 7.1.8 OreAlgebraicAnalysis

**Keywords:** Algebra, Computer algebra, Gröbner bases, Linear system, Ordinary differential equations, Differential algebraic equations, Partial differential equation, Equations algebraic partial derivatives, Polynomial equations, Automatic control

**Functional Description:** OreAlgebraicAnalysis is a Mathematica implementation of algorithms available in the OreModules and the OreMorphisms packages (developed in Maple). OreAlgebraicAnalysis is based on the implementation of Gröbner bases over Ore algebras available in the Mathematica HolonomicFunctions package developed by Christoph Koutschan (RICAM). OreAlgebraicAnalysis can handle larger classes of Ore algebras than the ones accessible in Maple, and thus we can study larger classes of linear functional systems. Finally, Mathematica internal design allows us to consider classes of systems which could not easily be considered in Maple such as generic linearizations of nonlinear functional systems defined by explicit nonlinear equations and systems containing transcendental functions (e.g., trigonometric functions, special functions). This package has been developed within the PHC Parrot project CASCAC.

**URL:** https://who.rocq.inria.fr/Alban.Quadrat/OreAlgebraicAnalysis/index.html

**Contact:** Alban Quadrat

**Participants:** Alban Quadrat, Thomas Cluzeau

### 7.1.9 OreMorphisms

**Keywords:** Algebra, Computer algebra, Gröbner bases, Linear system, Ordinary differential equations, Partial differential equation, Differential algebraic equations, Equations algebraic partial derivatives, Polynomial equations, Automatic control

**Functional Description:** The OreMorphisms package, based on OreModules, is dedicated to the implementation of homological algebra methods such as the computation of homomorphisms between two finitely presented modules over certain noncommutative polynomial algebras (Ore algebras), of kernel, coimage, image and cokernel of homomorphisms, Galois transformations of linear multidimensional systems and idempotents of the endomorphism ring. Using the packages Stafford and Quillen-Suslin, the factorization, reduction and decomposition problems can be effectively studied for different classes of linear multidimensional systems. Many linear functional systems studied in engineering sciences, mathematical physics and control theory have been factorized, reduced and decomposed thanks to the OreMorphisms package.

**URL:** https://who.rocq.inria.fr/Alban.Quadrat/OreMorphisms/index.html

**Contact:** Alban Quadrat

**Participants:** Alban Quadrat, Thomas Cluzeau

### 7.1.10 OreModules

**Keywords:** Algebra, Computer algebra, Gröbner bases, Linear system, Ordinary differential equations, Differential algebraic equations, Partial differential equation, Equations algebraic partial derivatives, Polynomial equations, Automatic control

**Functional Description:** OreModules is a Maple package dedicated to module theory and homological algebra for finitely presented modules defined over an Ore algebra of functional operators (e.g., ordinary or partial differential operators, shift operators, time-delay operators, difference operators) available in the Maple package Ore_algebra, and to their applications in mathematical systems theory and mathematical physics.

**URL:** https://who.rocq.inria.fr/Alban.Quadrat/OreModules/index.html

**Contact:** Alban Quadrat

#### 7.1.11 PTOPO

**Name:** Topology of Parametric Curves

**Keywords:** Parametric curve, 2D, 3D, Visualization, Computer algebra, Curve plotting, Topology

**Functional Description:** PTOPO computes (exactly) the topology and visualize parametric curves in 2D and in 3D.

**URL:** https://webusers.imj-prg.fr/~christina.katsamaki/ptopo/

**Contact:** Elias Tsigaridas

#### 7.1.12 PurityFiltration

**Keywords:** Symbolic computation, Partial differential equation

**Functional Description:** The PurityFiltration package, built upon the OreModules package, is an implementation of a new effective algorithm which computes the purity/grade filtration of linear functional systems (e.g., partial differential systems, differential time-delay systems, difference systems) and equivalent block-triangular matrices. This package is used to compute closed form solutions of over/underdetermined linear partial differential systems which cannot be integrated by the standard computer algebra systems such as Maple and Mathematica.

**URL:** https://who.rocq.inria.fr/Alban.Quadrat/PurityFiltration.html

**Contact:** Alban Quadrat

#### 7.1.13 Rewr

**Name:** Rewriting methods in algebra

**Keywords:** Computer algebra system (CAS), Rewriting systems, Algebra

**Functional Description:** Rewr is a prototype of computer algebra system, using rewriting methods to compute resolutions and homotopical invariants of monoids. The library implements various classical constructions of rewriting theory (such as completion), improved by experimental features coming from Garside theory, and allows homotopical algebra computations based on Squier theory. Specific functionalities have been developed for usual classes of monoids, such as Artin monoids and plactic monoids.

**URL:** https://plmlab.math.cnrs.fr/guiraud/rewr

**Publications:** hal-00326974, hal-00531242, hal-00682233, hal-00818253, hal-00932845, hal-01141226

**Contact:** Yves Guiraud

**Participants:** Yves Guiraud, Samuel Mimram

#### 7.1.14 RS

**Functional Description:** Real Roots isolation for algebraic systems with rational coefficients with a finite number of Complex Roots

**URL:** https://team.inria.fr/ouragan/software/

**Contact:** Fabrice Rouillier

**Participant:** Fabrice Rouillier

### 7.1.15 SIROPA

**Keywords:** Robotics, Kinematics

**Functional Description:** Library of functions for certified computations of the properties of articulated mechanisms, particularly the study of their singularities

**URL:** http://siropa.gforge.inria.fr/

**Authors:** Damien Chablat, Fabrice Rouillier, Guillaume Moroz, Philippe Wenger

**Contact:** Guillaume Moroz

**Partner:** LS2N

### 7.1.16 SLV

**Keywords:** Univariate polynomial, Real solving

**Functional Description:** SLV is a software package in C that provides routines for isolating (and subsequently refine) the real roots of univariate polynomials with integer or rational coefficients based on subdivision algorithms and on the continued fraction expansion of real numbers. Special attention is given so that the package can handle polynomials that have degree several thousands and size of coefficients hundrends of Megabytes. Currently the code consists of approx. 5000 lines.

**URL:** https://who.paris.inria.fr/Elias.Tsigaridas/soft.html

**Contact:** Elias Tsigaridas

### 7.1.17 Stafford

**Keywords:** Symbolic computation, Partial differential equation

**Functional Description:** The Stafford package of OreModules contains an implementation of two constructive versions of Stafford's famous but difficult theorem [96] stating that every ideal over the Weyl algebra An(k) (resp., Bn(k)) of partial differential operators with polynomial (resp., rational) coefficients over a field k of characteristic 0 (e.g., k=Q,R) can be generated by two generators. Based on this implementation and algorithmic results developed by the authors of the package, two algorithms which compute bases of free modules over the Weyl algebras An(Q) and Bn(Q) have been implemented. The rest of Stafford's results developed in [96] have recently been made constructive (e.g., computation of unimodular elements, decomposition of modules, Serre's splitting-off theorem, Stafford's reduction, Bass' cancellation theorem, minimal number of generators) and implemented in the Stafford package. The development of the Stafford package was motivated by applications to linear systems of partial differential equations with polynomial or rational coefficients (e.g., computation of injective parametrization, Monge problem, differential flatness, the reduction and decomposition problems and Serre's reduction problem). To our knowledge, the Stafford package is the only implementation of Stafford's theorems nowadays available.

**URL:** https://who.rocq.inria.fr/Alban.Quadrat/OreModules/stafford.html

**Contact:** Alban Quadrat

**Participants:** Alban Quadrat, Daniel Robertz

## 7.2 New platforms

### 7.2.1 Visualisation of limit sets

Character varieties are studied in the team as an interesting algebraic object. This study is completed by an effort to understand the geometrical meaning of each points in some carefully chosen character varieties. One approach to this problem is the construction of geometric structures.

Another approach is the study of limit sets associated to such points and their deformations when moving in the character variety. Those are fractal objects in the 3-sphere $\mathbb{S}^3$, which shares numerous properties with the usual fractal from complex dynamics. In our work, we study this limit sets first and foremost in an experimental way, leading to a ( Landscape of limit sets). The computation of such visualisations leverages the theoretical properties of these limit sets, certified numerical approximations. An improved version of the visualisation is in progress, and will use the theory of automatic groups as well as new and more efficient parametrizations of the objects of study. The experimental approach in turns inform the theoretical one. One important new step, bridging the two approaches, is done in [84].

# 8 New results

## 8.1 Algorithmic number theory, rigorous numerical computations

**Fast verification and public key storage optimization for unstructured lattice-based signatures** A recent work of Sipasseuth, Plantard and Susilo proposed to accelerate lattice-based signature verifications and compress public key storage at the cost of a precomputation on a public key. This first approach, which focused on a restricted type of key, did not include most NIST candidates or most lattice representations in general. In [18], we first present a way to improve even further both their verification speed and their public key compression capability by using a generator of numbers that better suit the method needs. We then also generalize their framework to apply to q-ary lattice schemes as well as classical lattices using Hermite Normal Form, improving their security and applicable scope, thus exhibiting potential trade-offs to accelerate lattice-based signature verification in general and compression of the public key on the verifier side for unstructured lattices.

**Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature** Zero-knowledge proofs are an important tool for many cryptographic protocols and applications. The threat of a coming quantum computer motivates the research for new zero-knowledge proof techniques for (or based on) post-quantum cryptographic problems. One of the few directions is code-based cryptography for which the strongest problem is the syndrome decoding (SD) of random linear codes. This problem is known to be NP-hard and the cryptanalysis state of affairs has been stable for many years. A zero-knowledge protocol for this problem was pioneered by Stern in 1993. As a simple public-coin three-round protocol, it can be converted to a post-quantum signature scheme through the famous Fiat-Shamir transform. The main drawback of this protocol is its high soundness error of $2/3$, meaning that it should be repeated $1.7*\lambda$ times to reach a $\lambda$-bit security. In [28], we improve this three-decade-old state of affairs by introducing a new zero-knowledge proof for the syndrome decoding problem on random linear codes. Our protocol achieves a soundness error of $1/n$ for an arbitrary $n$ in complexity $O(n)$. Our construction requires the verifier to trust some of the variables sent by the prover which can be ensured through a cut-and-choose approach. We provide an optimized version of our zero-knowledge protocol which achieves arbitrary soundness through parallel repetitions and merged cut-and-choose phase. While turning this protocol into a signature scheme, we achieve a signature size of 17 KB for a 128-bit security. This represents a significant improvement over previous constructions based on the syndrome decoding problem for random linear codes.

**On the Hardness of the Finite Field Isomorphism Problem** The finite field isomorphism (FFI) problem was introduced in PKC'18, as an alternative to average-case lattice problems (like LWE, SIS, or NTRU).

As an application, the same paper used the FFI problem to construct a fully homomorphic encryption scheme. In [35], we prove that the decision variant of the FFI problem can be solved in polynomial time for any field characteristics $q = \Omega(\beta n^2)$, where $q, \beta, n$ parametrize the FFI problem. Then we use our result from the FFI distinguisher to propose polynomial-time attacks on the semantic security of the fully homomorphic encryption scheme. Furthermore, for completeness, we also study the search variant of the FFI problem and show how to state it as a q-ary lattice problem, which was previously unknown. As a result, we can solve the search problem for some previously intractable parameters using a simple lattice reduction approach.

## 8.2 Topology in small dimension (character varieties, knot theory, computational geometry)

**On subgroups of finite index in complex hyperbolic lattice triangle groups** In[24], we study several explicit finite index subgroups in the known complex hyperbolic lattice triangle groups, and show some of them are neat, some of them have positive first Betti number, some of them have a homomorphisms onto a non-Abelian free group. For some lattice triangle groups, we determine the minimal index of a neat subgroup. Finally, we answer a question raised by Stover and describe an infinite tower of neat ball quotients all with a single cusp.

**Torsion in 1-cusped Picard modular groups** In [25] present a systematic effective method to construct coarse fundamental domains for the action of the Picard modular groups $PU(2,1,\mathcal{O}_d)$ where $\mathcal{O}_d$ has class number one, i.e. $d = 1,2,3,7,11,19,43,67,163$. The computations can be performed quickly up to the value $d = 19$. As an application of this method, we classify conjugacy classes of torsion elements, deduce short presentations for the groups, and construct neat subgroups of small index.

**Computing the non-properness set of real polynomial maps in the plane** In [26], we introduce novel mathematical and computational tools to develop a complete algorithm for computing the set of non-properness of polynomials maps in the plane. In particular, this set, which we call *the Jelonek set*, is a subset of $\mathbb{K}^2$ where a dominant polynomial map $f : \mathbb{K}^2 \mapsto \mathbb{K}^2$ is not proper; $\mathbb{K}$ could be either $\mathbb{C}$ or $\mathbb{R}$. Unlike all the previously known approaches we make no assumptions on $f$ whenever $\mathbb{K} = \mathbb{R}$; this is the first algorithm with this property. The algorithm takes into account the Newton polytopes of the polynomials. As a byproduct we provide a finer representation of the set of non-properness as a union of semi-algebraic curves, that correspond to edges of the Newton polytopes, which is of independent interest. Finally, we present a precise Boolean complexity analysis of the algorithm and a prototype implementation in Maple.

**Trifocal Relative Pose From Lines at Points** In [27], we present a method for solving two minimal problems for relative camera pose estimation from three views, which are based on three view correspondences of ( i ) three points and one line and the novel case of ( ii ) three points and two lines through two of the points. These problems are too difficult to be efficiently solved by the state of the art Gröbner basis methods. Our method is based on a new efficient homotopy continuation (HC) solver framework MINUS, which dramatically speeds up previous HC solving by specializing hc methods to generic cases of our problems. We characterize their number of solutions and show with simulated experiments that our solvers are numerically robust and stable under image noise, a key contribution given the borderline intractable degree of nonlinearity of trinocular constraints. We show in real experiments that ( i ) sift feature location and orientation provide good enough point-and-line correspondences for three-view reconstruction and ( ii ) that we can solve difficult cases with too few or too noisy tentative matches, where the state of the art structure from motion initialization fails.

## 8.3 Algebraic analysis of functional systems, algebraic topology and group theory

**Algorithmic study of the algebraic parameter estimation problem for a class of perturbations** In [21], we consider the algebraic parameter estimation problem for a class of standard perturbations. We assume that the measurement $z(t)$ of a solution $x(t)$ of a linear ordinary differential equation, whose coefficients depend on a set $\theta = \{\theta_1, \ldots, \theta_r\}$ of unknown constant parameters,is affected by a perturbation $\gamma(t)$ whose structure is supposed to be known (e.g., an unknown bias, an unknown ramp), i.e., $z(t) = x(t,\theta) + \gamma(t)$. We investigate the problem of obtaining closed-form expressions for the parameters $\theta$ 's in terms of repeated $i$ indefinite integrals or convolutions of $z$. We illustrate the different results with explicit examples computed using the NonA package, developed in Maple, in which we have implemented our main contributions.

**Further results on the computation of the annihilators of integro-differential operators** In [34], we expose some effective aspects of the algebra of linear ordinary integro-differential operators with polynomial coefficients. More precisely, we prove that the annihilator of an evaluation operator is a finitely generated ideal which can be explicitly characterized and computed. This is an advance towards the development of an effective elimination theory for ordinary integro-differential operators and an effective study of linear systems of integro-differential equations with polynomial coefficients.

**Coherent presentations of monoids with a right-noetherian Garside family** In [22], the authors show how to construct coherent presentations (presentations by generators, relations and relations among relations) of monoids admitting a right-noetherian Garside family. Thereby, it resolves the question of finding a unifying generalisation of the following two distinct extensions of construction of coherent presentations for spherical Artin-Tits monoids: to general Artin-Tits monoids, and to Garside monoids. The result is applied to some monoids which are neither Artin-Tits nor Garside.

## 8.4 Basic theory and algorithms in algebra and geometry

**Geometric algorithms for sampling the flux space of metabolic networks** Metabolic networks and their reconstruction set a new era in the analysis of metabolic and growth functions in the various organisms. By modeling the reactions occurring inside an organism, metabolic networks provide the means to understand the underlying mechanisms that govern biological systems. Constraint-based approaches have been widely used for the analysis of such models and led to intriguing geometry-oriented challenges. In this setting, sampling uniformly points from polytopes derived from metabolic models (flux sampling) provides a representation of the solution space of the model under various conditions. However, the polytopes that result from such models are of high dimension (in the order of thousands) and usually considerably skinny. Therefore, to sample uniformly at random from such polytopes shouts for a novel algorithmic and computational framework specially tailored for the properties of metabolic models. In [19], we present a complete software framework to handle sampling in metabolic networks. Its backbone is a Multiphase Monte Carlo Sampling (MMCS) algorithm that unifies rounding and sampling in one pass, yielding both upon termination. It exploits an optimized variant of the Billiard Walk that enjoys faster arithmetic complexity per step than the original. We demonstrate the efficiency of our approach by performing extensive experiments on various metabolic networks. Notably, sampling on the most complicated human metabolic network accessible today, Recon3D, corresponding to a polytope of dimension 5335, took less than 30 hours. To the best of our knowledge, that is out of reach for existing software.

**Truncated Log-concave Sampling for Convex Bodies with Reflective Hamiltonian Monte Carlo** In [20], we introduce Reflective Hamiltonian Monte Carlo (ReHMC), an HMC-based algorithm to sample from a log-concave distribution restricted to a convex body. The random walk is based on incorporating reflections to the Hamiltonian dynamics such that the support of the target density is the convex body. We develop an efficient open source implementation of ReHMC and perform an experimental study on various high-dimensional datasets. The experiments suggest that ReHMC outperforms Hit-and-Run and Coordinate-Hit-and-Run regarding the time it needs to produce an independent sample, introducing practical truncated sampling in thousands of dimensions.

**Segre-driven radicality testing** In [29], wee present a probabilistic algorithm to test if a homogeneous polynomial ideal $I$ defining a scheme $X$ in $\mathbb{P}^n$ is radical using Segre classes and other geometric notions from intersection theory. Its worst case complexity depends on the geometry of $X$. If the scheme $X$ has reduced isolated primary components and no embedded components supported the singular locus of $X_{red} = V(\sqrt{I})$, then the worst case complexity is doubly exponential in n; in all the other cases the complexity is singly exponential. The realm of the ideals for which our radical testing procedure requires only single exponential time includes examples which are often considered pathological, such as the ones drawn from the famous Mayr-Meyer set of ideals which exhibit doubly exponential complexity for the ideal membership problem.

**Randomized geometric tools for anomaly detection in stock markets** In [33], we propose novel randomized geometric tools to detect low-volatility anomalies in stock markets; a principal problem in financial economics. Our modeling of the (detection) problem results in sampling and estimating the (relative) volume of geodesically non-convex and non-connected spherical patches that arise by intersecting a non-standard simplex with a sphere. To sample, we introduce two novel Markov Chain Monte Carlo (MCMC) algorithms that exploit the geometry of the problem and employ state-of-the-art continuous geometric random walks (such as Billiard walk and Hit-and-Run) adapted on spherical patches. To our knowledge, this is the first geometric formulation and MCMC-based analysis of the volatility puzzle in stock markets. We have implemented our algorithms in C++ (along with an R interface) and we illustrate the power of our approach by performing extensive experiments on real data. Our analyses provide accurate detection and new insights into the distribution of portfolios' performance characteristics. Moreover, we use our tools to show that classical methods for low-volatility anomaly detection in finance form bad proxies that could lead to misleading or inaccurate results.

**On Isolating Roots in a Multiple Field Extension** In [36], we address univariate root isolation when the polynomial's coefficients are in a multiple field extension. We consider a polynomial $F \in L[Y]$, where $L$ is a multiple algebraic extension of $\mathbb{Q}$. We provide aggregate bounds for $F$ and algorithmic and bit-complexity results for the problem of isolating its roots. For the latter problem we follow a common approach based on univariate root isolation algorithms. For the particular case where $F$ does not have multiple roots, we achieve a bit-complexity in $\tilde{O}_B(nd^{2n+2}(d+n\tau))$, where $d$ is the total degree and $\tau$ is the bitsize of the involved polynomials. In the general case we need to enhance our algorithm with a preprocessing step that determines the number of distinct roots of $F$. We follow a numerical, yet certified, approach that has bit-complexity $\tilde{O}_B(n^2d^{3n+3}\tau + n^3d^{2n+4})$.

## 8.5 Applications

**On the Certification of the Kinematics of 3-DOF Spherical Parallel Manipulators** In [31] we aims to study a specific kind of parallel robot: Spherical Parallel Manipulators (SPM) that are capable of unlimited rolling. A focus is made on the kinematics of such mechanisms, especially taking into account uncertainties (e.g. on conception & fabrication parameters, measures) and their propagations. Such considerations are crucial if we want to control our robot correctly without any undesirable behavior in its workspace (e.g. effects of singularities). In this paper, we will consider two different approaches to study the kinematics and the singularities of the robot of interest: symbolic and semi-numerical. By doing so, we can compute a singularity-free zone in the work- and joint spaces, considering given uncertainties on the parameters. In this zone, we can use any control law to inertially stabilize the upper platform of the robot.

# 9 Bilateral contracts and grants with industry

## 9.1 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 manpower, 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.

- A research contract covering, in particular, a CIFRE grant for a PhD (Alexandre Lê) was signed with the company Safran Electronics & Defense for the conception of parallel robots for inertial stabilization.

- A research contract covering, in particular, a CIFRE grant for a PhD (Thibault Feneuil was signed with the company CryptoExperts.

# 10 Partnerships and cooperations

## 10.1 National initiatives

### 10.1.1 ANR

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

  Coordinator: Elias Tsigaridas

  Duration: 2018 – 2023

  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.

- ANR JCJC SHoCoS (Structure and Homotopy of Configuration Spaces)

  Coordinator: Najib Idrissi (Univ. Paris Cité, IMJ-PRG)

  Participant: Yves Guiraud

  Duration: 2022 – 2026

  This is a project of fundamental research in mathematics, specifically algebraic topology, homotopical algebra, and quantum algebra. It is concerned with configuration spaces, which consist in finite sequences of pairwise distinct points in a manifold. Over the past couple of decades, strides have been made in the study and computation of the homotopy types of configuration spaces, i.e., their shape up to continuous deformation. These advances were possible thanks to the rich structure of configuration spaces, which comes from the theory of operads. Moreover, a new theory, factorization homology, allowed the use of configuration spaces to compute topological field theories, topological invariants of manifolds inspired by physics. Our purpose is to exploit the full operadic structure of configuration spaces to obtain new kinds of stabilizations in the homotopy types of configuration spaces, and to use this stability to effectively compute topological field theories from deformation quantization.

#### 10.1.2 Inria Exploratory actions

- LOCUS (non-Linear geOmetriC compUting at Scale) Inria Exploratory Action

  Coordinator: Elias Tsigaridas

  Duration 2022 - 2025

  Summary : LOCUS shapes a novel theoretical, algorithmic, and computational framework at the intersection of computational algebra, high dimensional geometric and statistical computing, and optimization. It focuses on sampling and integrating in convex bodies, algorithms for convex optimization, and applications in structural biology. It aims to deliver effective theoretical algorithms and efficient open source software for the problems of interest.

- Réal (Réécriture algébrique) Inria Exploratory Action

  Coordinator : Yves Guiraud

  Duration : 2022-2025

  Summary : Rewriting is a branch of computer algebra consisting in transforming mathematical expressions according to admissible rules. Examples range from elementary situations, such as a remarkable identity $(a+b)^2 = a^2+2ab+b^2$ in a ring, to calculations in complex algebraic structures, such as the Jacobi relation [[x,y],z] = [x,[y,z]] - [[x,z],y] in a Lie algebra.

  The Réal project proposes to explore the connections between rewriting and algebra. The aim is to understand the algebraic foundations of rewriting, to integrate similar calculation mechanisms known in algebra, and to develop new calculation tools with a view to applications in three areas of mathematics: combinatorial and higher algebra, theory groups and representations, study of algebraic systems and varieties.

#### 10.1.3 Technological Development Actions

- ACE (2023 - ) Coordinated by F. Rouillier. With the help of a research engineer from Inria who is working full time for OURAGAN, pass from prototypes that did serve to validate some computational strategies related to our collaborations with Safran (Control Theory, Robotics, etc.) to full solutions with an interface directly usable by specialized Engineers.

# 11 Dissemination

## 11.1 Promoting scientific activities

### 11.1.1 Scientific events: organisation

**Member of the organizing committees**

- Yves Guiraud was an organiser of the *Workshop on Homology of Configuration Spaces and related topics*, Paris, May 2023.

- Alban Quadrat organized two mini-workshops on multidimensional systems (02-03/11, Sorbonne University) and on time-delay systems (15-16/11, Inria Paris).

### 11.1.2 Scientific events: selection

- Elias Tsigaridas co-supervised the edition of the Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation [39].

#### Chair of conference program committees

- Elias Tsigaridas was the program chair of International Symposium on Symbolic and Algebraic Computation (ISSAC), which was held at Tromso, Norway, July 2023.

#### Member of the conference program committees

- Alban Quadrat is member of the technical committee Linear Systems of the International Federation of Automatic Control (IFAC).
- Pierre-Vincent Koseleff is a member of the organizing committee of the conference *Fondation of Computational Mathematics* (FoCM 2023).
- Elias Tsigaridas co-organized (with Matías Bender) a session on *Nonlinear Algebra and its Application,s* during the PGMO days 2023, at the EDF'Lab Palaiseau, November 2023.
- Elias Tsigaridas co-organized (with Matías Bender) a minisymposium on *Efficient Symbolic and Numerical Algorithms for Polynomial Systems* at SIAM Conference on Applied Algebraic Geometry, Eindhoven, 2023.

### 11.1.3 Journal

#### Member of the editorial boards

- Elisha Falbel is a member of the editorial board of *São Paulo Journal of Mathematical Sciences - Springer*.
- Elisha Falbel is a member of the editorial board of *Moduli - Foundation Compositio Mathematica*.
- Alban Quadrat is associate editor of *Multidimensional Systems and Signal Processing*, Springer.
- Alban Quadrat is a member of the editorial board of *Maple Transactions*.
- Fabrice Rouillier is a member of the editorial board of *Journal of Symbolic Computation*.
- Fabrice Rouillier is a member of the editorial board of *Maple Transactions*.
- Elias Tsigaridas is a member of the editorial board of *Journal of Symbolic Computation*.

### 11.1.4 Research administration

- Elisha Falbel is director of the "École Doctorale Sciences Mathématiques de Paris Centre - ED 386".
- Yves Guiraud is an elected member of the Comité National de la Recherche Scientifique (the evaluation body of the CNRS), Section 41 (Mathematics), and an appointed member of the section board (2021-2025).
- Yves Guiraud was an elected member of the scientific council of the department of mathematics of Université Paris 7 / Université de Paris / Université Paris Cité (2019-2022).
- Yves Guiraud is an elected member of the laboratory council of IMJ-PRG (since 2021).
- Fabrice Rouillier is a member of the scientific commitee of the Indo French Centre for Applied Mathematics.
- Elias Tsigaridas is an elected member of the Commission d'évaluation d'Inria (CE) since 2019.

## 11.2 Teaching - Supervision - Juries

### 11.2.1 Teaching

- Antonin Guilloux, Alban Quadrat, Elias Tsigaridas, Master 1, Effective Linear Algebra and Polynomials. (24h course + 36h exercises) .
- Antonin Guilloux, Fabrice Rouillier, Master 1, Introduction to Algebraic geometry (24h course + 36h exercises).
- Jean-Claude Bajard, Antonin Guilloux, Pierre-Vincent Koseleff and Fabrice Rouillier take part to the "agrégation de mathématiques - option C" at Sorbonne Université.
- Pierre-Vincent Koseleff : Master 1 Maths - Sorbonne Université : Algebraic Cryptography (36H) at Sorbonne Université.
- Pierre-Vincent Koseleff : Master 2 EducFellow in Maths - Computer Algebra (120H) at Sorbonne Université.
- Pierre-Vincent Koseleff : Master 1 Maths - Sorbonne Université : Algebraic Algorithmic (36H) at Sorbonne Université.
- Pascal Molin manages the Master *math-info spécialités crypto et big-data* at Paris Université.
- Pascal Molin : teaches *codes et crypto* and *théorie de l'information* in Master 1 at Paris Université.
- Elias Tsigaridas, 24h "Algebraic techniques in optimation", Master 2 Mathématiques fondamentales, Sorbonne Université.
- Elias Tsigaridas : Algorithms and Competitive Programming, Ingénieur 2A, modal. 20h lectures and 25h TD. Department of Informatics (LIX), École Polytechnique, France.
- Elias Tsigaridas : Algorithms for data analysis in C++, Ingénieur 2A. 40h TD. Department of Informatics (LIX), École Polytechnique, France.

### 11.2.2 Supervision

- Jean-Claude Bajard supervised the PhD of Thibauld Feneuil until 09/2023 (defense date).
- Elias Tsigaridas supervised the PhD of Carles Checa, since (co-supervision with Ioannis Emiris).
- Pierre-Vincent Koseleff supervises the PhD of Andrea Negro , since 10/2021, (co-supervision with Julien Marché IMJ-PRG).
- Elias Tsigaridas and Fabrice Rouillier supervised the PhD of Christina Katsamaki until 07/2023 (defense date).
- Yves Guiraud supervised, with Pierre-Louis Curien (CNRS, Univ. Paris Cité, IRIF) the PhD thesis of Alen Đurić until 04/2023 (Defense).
- Alban Quadrat supervises the PhD of Camille Pinto since 10/2022.
- Fabrice Rouillier supervises the PhD of Alexandre Lê (Safran CIFRE Grant) (co-dupervision with Damien Chablat - LS2N Nantes) since 01/2021.
- Fabrice Rouillier supervises the PhD of Joao Ruiz since 09/2023.
- Elias Tsigaridas, Alban Quadrat and Fabrice Rouillier supervised the PhD of Chaoping Zhu since 09/2023.

### 11.2.3 Juries

- Yves Guiraud was a referee for the PhD thesis of Sophie d'Espalungue, *Operads in categories and models of structure interchange*, Univ. Lille, December 2023.
- Alban Quadrat was a referee for the Habilitation thesis of Michaël Di Loreto *Propriétés structurelles des systèmes dynamiques pour le contrôle*, Institut National des Sciences Appliquées de Lyon, October, 2023.

## 11.3 Popularization

- Antonin Guilloux is involved in the action Maths C pour L at Sorbonne Université.
- Pascal Molin teaches DAEU at the detention center of Fresnes', enabling prisoners access scientific university studies.
- Owen Rouillé did animate several sessions for the association Les Maths en Scène.
- Fabrice Rouillier is the chair of the association Animath.
- Fabrice Rouillier is Chargé de mission médiation for the Inria Paris research center.
- Fabrice Rouiller is a member of the "Conseil d'administration" of the association Math.En.Jeans.
- Fabrice Rouillier is a member of the comité de pilotage de la semaine des mathématiques.
- Fabrice Rouillier is a member of the Jury des Olympiades Nationales de Mathématiques.

# 12 Scientific production

## 12.1 Major publications

[1] Y. Bouzidi, S. Lazard, G. Moroz, M. Pouget, F. Rouillier and M. Sagraloff. 'Solving bivariate systems using Rational Univariate Representations'. In: *Journal of Complexity* 37 (2016), pp. 34–75. DOI: 10.1016/j.jco.2016.07.002. URL: https://hal.inria.fr/hal-01342211.

[2] E. Brugallé, P.-V. Koseleff and D. Pecker. 'On the lexicographic degree of two-bridge knots'. In: *Journal Of Knot Theory And Its Ramifications (JKTR)* 25.7 (June 2016). 14p., 21 figs. DOI: 10.1142/S0218216516500449. URL: https://hal.archives-ouvertes.fr/hal-01084472.

[3] E. Brugallé, P.-V. Koseleff and D. Pecker. 'Untangling trigonal diagrams'. In: *Journal Of Knot Theory And Its Ramifications (JKTR)* 25.7 (June 2016). 10p., 24 figs. DOI: 10.1142/S0218216516500437. URL: https://hal.archives-ouvertes.fr/hal-01084463.

[4] F. Chyzak, A. Quadrat and D. Robertz. 'Effective algorithms for parametrizing linear control systems over Ore algebras'. In: *Applicable Algebra in Engineering, Communications and Computing* 16 (2005), pp. 319–376.

[5] T. Cluzeau and A. Quadrat. 'Factoring and decomposing a class of linear functional systems'. In: *Linear Algebra and Its Applications* 428 (2008), pp. 324–381.

[6] E. Falbel and A. Guilloux. 'Dimension of character varieties for 3-manifolds'. In: *Proceedings of the American Mathematical Society* (2016). DOI: 10.1090/proc/13394. URL: https://hal.archives-ouvertes.fr/hal-01370284.

[7] E. Falbel, A. Guilloux, P.-V. Koseleff, F. Rouillier and M. Thistlethwaite. 'Character Varieties For SL(3,C): The Figure Eight Knot'. In: *Experimental Mathematics* 25.2 (2016), p. 17. DOI: 10.1080/10586458.2015.1068249. URL: https://hal.inria.fr/hal-01362208.

[8] E. Falbel and J. Wang. 'Branched spherical CR structures on the complement of the figure-eight knot'. In: *Michigan Mathematical Journal* 63 (2014), pp. 635–667. URL: https://hal.archives-ouvertes.fr/hal-01374789.

[9] S. Gaussent, Y. Guiraud and P. Malbos. ‘Coherent presentations of Artin monoids’. In: *Compositio Mathematica* 151.5 (2015), pp. 957–998. DOI: 10.1112/S0010437X14007842. URL: https://hal.archives-ouvertes.fr/hal-00682233.

[10] Y. Guiraud, E. Hoffbeck and P. Malbos. ‘Convergent presentations and polygraphic resolutions of associative algebras’. In: *Mathematische Zeitschrift* 293.1-2 (2019), pp. 113–179. DOI: 10.1007/s00209-018-2185-z. URL: https://hal.archives-ouvertes.fr/hal-01006220.

[11] Y. Guiraud and P. Malbos. ‘Higher-dimensional normalisation strategies for acyclicity’. In: *Advances in Mathematics* 231.3-4 (2012), pp. 2294–2351. DOI: 10.1016/j.aim.2012.05.010. URL: https://hal.archives-ouvertes.fr/hal-00531242.

[12] A. Joux. ‘A one round protocol for tripartite Diffie-Hellman’. In: *J. Cryptology* 17.4 (2004), pp. 263–276.

[13] A. Joux and 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.* 72.242 (2003), pp. 953–967.

[14] D. Lazard and F. Rouillier. ‘Solving Parametric Polynomial Systems’. In: *Journal of Symbolic Computation* 42 (June 2007), pp. 636–667.

[15] A. Quadrat and D. Robertz. ‘Computation of bases of free modules over the Weyl algebras’. In: *Journal of Symbolic Computation* 42 (2007), pp. 1113–1141.

[16] F. Rouillier. ‘Solving zero-dimensional systems through the rational univariate representation’. In: *Journal of Applicable Algebra in Engineering, Communication and Computing* 9.5 (1999), pp. 433–461.

[17] F. Rouillier and P. Zimmermann. ‘Efficient Isolation of Polynomial Real Roots’. In: *Journal of Computational and Applied Mathematics* 162.1 (2003), pp. 33–50.

## 12.2 Publications of the year

### International journals

[18] J.-C. Bajard, K. Fukushima, T. Plantard and A. Sipasseuth. ‘Fast verification and public key storage optimization for unstructured lattice-based signatures’. In: *Journal of Cryptographic Engineering*. Journal of Cryptographic Engineering (2023) (19th Jan. 2023). DOI: 10.1007/s13389-023-00309-1. URL: https://hal.sorbonne-universite.fr/hal-03959746.

[19] A. Chalkis, I. Z. Emiris, V. Fisikopoulos, E. Tsigaridas and H. Zafeiropoulos. ‘Geometric algorithms for sampling the flux space of metabolic networks’. In: *Journal of Computational Geometry* 14.1 (2023). DOI: 10.20382/jocg.v14i1a8. URL: https://inria.hal.science/hal-04310109.

[20] A. Chalkis, V. Fisikopoulos, M. Papachristou and E. Tsigaridas. ‘Truncated Log-concave Sampling for Convex Bodies with Reflective Hamiltonian Monte Carlo’. In: *ACM Transactions on Mathematical Software* 49.2 (30th June 2023), pp. 1–25. DOI: 10.1145/3589505. URL: https://inria.hal.science/hal-04222039.

[21] M. Chartouny, T. Cluzeau and A. Quadrat. ‘Algorithmic study of the algebraic parameter estimation problem for a class of perturbations’. In: *Maple Transactions* 3 (1st Feb. 2023). DOI: 10.5206/mt.v2i2.14467. URL: https://inria.hal.science/hal-04203089.

[22] P.-L. Curien, A. Đurić and Y. Guiraud. ‘Coherent presentations of monoids with a right-noetherian Garside family’. In: *Journal of Homotopy and Related Structures* 18 (2023), pp. 115–152. DOI: 10.1007/s40062-023-00323-4. URL: https://hal.science/hal-03276119.

[23] C. Dartyge, B. Martin, J. Rivat, I. E. Shparlinski and C. Swaenepoel. ‘Reversible primes’. In: *Journal of the London Mathematical Society* (2024). URL: https://hal.science/hal-04430339.

[24] M. Deraux. ‘On Subgroups Finite Index in Complex Hyperbolic Lattice Triangle Groups’. In: *Experimental Mathematics* (2023), pp. 1–26. DOI: 10.1080/10586458.2022.2158969. URL: https://hal.science/hal-04000578.

[25] M. Deraux and M. Xu. ‘Torsion in 1-Cusped Picard Modular Groups’. In: *Transformation Groups* (9th Jan. 2023). DOI: 10.1007/s00031-022-09783-z. URL: https://hal.science/hal-03981593.

[26] B. El Hilany and E. Tsigaridas. ‘Computing the non-properness set of real polynomial maps in the plane’. In: *Vietnam Journal of Mathematics* (26th June 2023). DOI: 10.1007/s10013-023-00652-0. URL: https://hal.science/hal-04223513.

[27] R. Fabbri, T. Duff, H. Fan, M. Regan, D. da Costa de Pinho, E. Tsigaridas, C. Wampler, J. Hauenstein, P. Giblin, B. Kimia, A. Leykin and T. Pajdla. ‘Trifocal Relative Pose From Lines at Points’. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 45.6 (1st June 2023), pp. 7870–7884. DOI: 10.1109/TPAMI.2022.3226165. URL: https://inria.hal.science/hal-04226115.

[28] T. Feneuil, A. Joux and M. Rivain. ‘Shared permutation for syndrome decoding: new zero-knowledge protocol and code-based signature’. In: *Designs, Codes and Cryptography* 91.2 (Feb. 2023), pp. 563–608. DOI: 10.1007/s10623-022-01116-1. URL: https://hal.science/hal-04218321.

[29] M. Helmer and E. Tsigaridas. ‘Segre-driven radicality testing’. In: *Journal of Symbolic Computation* 122 (May 2024), p. 102262. DOI: 10.1016/j.jsc.2023.102262. URL: https://inria.hal.science/hal-04222033.

[30] K. Kozhasov and J. Tonelli-Cueto. ‘Probabilistic bounds on best rank-one approximation ratio’. In: *Linear and Multilinear Algebra* (3rd Mar. 2024), pp. 1–29. DOI: 10.1080/03081087.2024.2304146. URL: https://inria.hal.science/hal-03517267.

[31] A. Lê, D. Chablat, G. Rance and F. Rouillier. ‘On the Certification of the Kinematics of 3-DOF Spherical Parallel Manipulators’. In: *Maple Transactions* 3.2 (28th Aug. 2023). DOI: 10.5206/mt.v3i2.15660. URL: https://hal.science/hal-04189637.

[32] M. Radons and J. Tonelli-Cueto. ‘Generalized Perron Roots and Solvability of the Absolute Value Equation’. In: *SIAM Journal on Matrix Analysis and Applications* 44.4 (30th Oct. 2023), pp. 1645–1666. DOI: 10.1137/22M1517184. URL: https://inria.hal.science/hal-03738197.

### International peer-reviewed conferences

[33] C. Bachelard, A. Chalkis, V. Fisikopoulos and E. Tsigaridas. ‘Randomized geometric tools for anomaly detection in stock markets’. In: *Proceedings of Machine Learning Research*. 26th International Conference on Artificial Intelligence and Statistics (AISTATS). Valencia, Spain, 25th Apr. 2023. URL: https://hal.science/hal-04223511.

[34] T. Cluzeau, C. Pinto and A. Quadrat. ‘Further results on the computation of the annihilators of integro-differential operators’. In: 2023 International Symposium on Symbolic and Algebraic Computation. Tromso, Norway, 24th July 2023, p. 9. DOI: 10.1145/3597066.3597083. URL: https://inria.hal.science/hal-04203853.

[35] D. Das and A. Joux. ‘On the Hardness of the Finite Field Isomorphism Problem’. In: *LNCS - Lecture Notes in Computer Science*. Eurocrypt 2023 - Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland, 16th Apr. 2023, pp. 343–359. DOI: 10.1007/978-3-031-30589-4_12. URL: https://hal.science/hal-04294817.

[36] C. Katsamaki and F. Rouillier. ‘On Isolating Roots in a Multiple Field Extension’. In: ISSAC ’23: 2023 International Symposium on Symbolic and Algebraic Computation. Tromso, Norway: ACM; ACM, 24th Aug. 2023, pp. 363–371. DOI: 10.1145/3597066.3597107. URL: https://hal.science/hal-04116621.

[37] A. Lê, G. Rance, F. Rouillier and D. Chablat. ‘Inertial line-of-sight stabilization using a 3-dof spherical parallel manipulator with coaxial input shafts’. In: *11th International Symposium on Optronics in Defense and Security*. OPTRO2024 - 11th International Symposium on Optronics in defence & security. Bordeaux, France, 23rd Jan. 2024. URL: https://inria.hal.science/hal-04483255.

### Scientific books

[38] D. Ara, A. Burroni, Y. Guiraud, P. Malbos, F. Métayer and S. Mimram. *Polygraphs: From Rewriting to Higher Categories*. London Mathematical Society Lecture Note Series. 2023. URL: https://hal.science/hal-04322821.

### Edition (books, proceedings, special issue of a journal)

[39] A. Dickenstein, G. Jeronimo and E. Tsigaridas, eds. *ISSAC '23: Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*. ACM; ACM, 24th July 2023. DOI: 10.1145/3597066. URL: https://hal.science/hal-04223439.

### Doctoral dissertations and habilitation theses

[40] T. Feneuil. 'Post-Quantum Signatures from Secure Multiparty Computation'. Sorbonne Université, 23rd Oct. 2023. URL: https://hal.science/tel-04316885.

[41] C. Katsamaki. 'Exact Algebraic and Geometric Computations for Parametric Curves'. Sorbonne Université, 21st June 2023. URL: https://theses.hal.science/tel-04167904.

### Reports & preprints

[42] E. Falbel and J. M. Veloso. *A global invariant for path structures and second order differential equations*. 12th June 2023. URL: https://hal.science/hal-04121036.

[43] C. Katsamaki, F. Rouillier and E. Tsigaridas. *Exact Convex Hull Computation for Plane and Space Parametric Curves*. 14th Dec. 2023. URL: https://inria.hal.science/hal-04345541.

[44] G. Sergeant-Perthuis, N. Ruet, D. Rudrauf, D. Ognibene and Y. Tisserand. *Influence of the Geometry of the world model on Curiosity Based Exploration*. 13th Feb. 2024. URL: https://hal.science/hal-04054736.

## 12.3 Cited publications

[45] D. Aggarwal, A. Joux, A. Prakash and 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. DOI: 10.1007/978-3-319-96878-0_16. URL: https://doi.org/10.1007/978-3-319-96878-0%5C_16.

[46] S. Basu, R. Pollack and M.-F. Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Berlin, Heidelberg: Springer-Verlag, 2006.

[47] V. Bavula. 'The algebra of integro-differential operators on an affine line and its modules'. In: *J. Pure Appl. Algebra* 217 (2013), pp. 495–529.

[48] N. Bergeron, E. Falbel and A. Guilloux. 'Tetrahedra of flags, volume and homology of SL(3)'. In: *Geometry & Topology Monographs* 18 (2014). DOI: 10.2140/gt.2014.18.1911. URL: https://hal.archives-ouvertes.fr/hal-01370258.

[49] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin and P. Kirchner. 'Computing generator in cyclotomic integer rings'. In: *36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2017)*. Vol. 10210. Lecture Notes in Computer Science. Paris, France, Apr. 2017, pp. 60–88. DOI: 10.1007/978-3-319-56620-7_3. URL: https://hal.archives-ouvertes.fr/hal-01518438.

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

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

[52] F. Boulier, D. Lazard, F. Ollivier and M. Petitot. 'Computing representations for radicals of finitely generated differential ideals'. In: *Applicable Algebra in Engineering, Communication and Computing* 20 (2009), pp. 73–121.

[53] Y. Bouzidi, A. Quadrat and 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)*. Proceedings of the IEEE 9th International Workshop on Multidimensional (nD) Systems (IEEE nDS 2015). Vila Real, Portugal, Sept. 2015. URL: https://hal-centralesupelec.archives-ouvertes.fr/hal-01259968.

[54] Y. Bouzidi, T. Cluzeau, G. Moroz and A. Quadrat. 'Computing effectively stabilizing controllers for a class of *n*D systems'. In: *The 20th World Congress of the International Federation of Automatic Control*. Vol. 50. 1. Toulouse, France, July 2017, pp. 1847–1852. DOI: 10.1016/j.ifacol.2017.08.200. URL: https://hal.archives-ouvertes.fr/hal-01667161.

[55] Y. Bouzidi, S. Lazard, G. Moroz, M. Pouget and 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. URL: https://hal.inria.fr/hal-00992634.

[56] Y. Bouzidi, S. Lazard, G. Moroz, M. Pouget, F. Rouillier and M. Sagraloff. 'Solving bivariate systems using Rational Univariate Representations'. In: *Journal of Complexity* 37 (2016), pp. 34–75. DOI: 10.1016/j.jco.2016.07.002. URL: https://hal.inria.fr/hal-01342211.

[57] Y. Bouzidi, S. Lazard, M. Pouget and F. Rouillier. 'Separating linear forms and Rational Univariate Representations of bivariate systems'. In: *Journal of Symbolic Computation* 68.0 (May 2015), pp. 84–119. DOI: 10.1016/j.jsc.2014.08.009. URL: https://hal.inria.fr/hal-00977671.

[58] Y. Bouzidi, A. Poteaux and 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, Mar. 2017. URL: https://hal.inria.fr/hal-01485536.

[59] Y. Bouzidi, A. Quadrat and F. Rouillier. 'Certified Non-conservative Tests for the Structural Stability of Multidimensional Systems'. Research Report. To appear in Multidimensional Systems and Signal Processing, https://link.springer.com/article/10.1007/s11045-018-0596-y. Aug. 2017. URL: https://hal.inria.fr/hal-01571230.

[60] Y. Bouzidi and 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*. Proceedings of the 22nd International Symposium on Mathematical Theory of Networks and Systems. Minneapolis, United States, July 2016. URL: https://hal.inria.fr/hal-01366202.

[61] E. Brugallé, P.-V. Koseleff and D. Pecker. 'On the lexicographic degree of two-bridge knots'. In: *Journal Of Knot Theory And Its Ramifications (JKTR)* 25.7 (June 2016). 14p., 21 figs. DOI: 10.1142/S0218216516500449. URL: https://hal.archives-ouvertes.fr/hal-01084472.

[62] E. Brugallé, P.-V. Koseleff and D. Pecker. 'The lexicographic degree of the first two-bridge knots'. In: *Annales de la Faculté des Sciences de Toulouse. Mathématiques*. 29.4 (Dec. 2020), pp. 761–793. DOI: 10.5802/afst.1645. URL: https://hal.archives-ouvertes.fr/hal-01108678.

[63] E. Brugallé, P.-V. Koseleff and D. Pecker. 'Untangling trigonal diagrams'. In: *Journal Of Knot Theory And Its Ramifications (JKTR)* 25.7 (June 2016). 10p., 24 figs. DOI: 10.1142/S0218216516500437. URL: https://hal.archives-ouvertes.fr/hal-01084463.

[64] D. Chablat, R. Jha, F. Rouillier and 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. URL: https://hal.archives-ouvertes.fr/hal-00956325.

[65] D. Chablat, R. Jha, F. Rouillier and 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*. Vol. Volume 5A. Buffalo, United States, Aug. 2014, pp. 1–10. URL: https://hal.archives-ouvertes.fr/hal-01006614.

[66] F. Chyzak, A. Quadrat and D. Robertz. 'Effective algorithms for parametrizing linear control systems over Ore algebras'. In: *Applicable Algebra in Engineering, Communications and Computing* 16 (2005), pp. 319–376.

[67] F. Chyzak and B. Salvy. 'Non-commutative elimination in Ore algebras proves multivariate identities'. In: *Journal of Symbolic Computation* 26.2 (1998), pp. 187–227.

[68] 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*. Ed. by H. Brakhage. Berlin, Heidelberg: Springer Berlin Heidelberg, 1975, pp. 134–183.

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

[70] M. Crocco, A. Del Bue and V. Murino. 'A bilinear approach to the position self-calibration of multiple sensors'. In: *IEEE Transactions on Signal Processing* 60.2 (2012), pp. 660–673.

[71] R. Curtain and H. Zwart. *An Introduction to Infinite-Dimensional Linear Systems Theory*. Texts in Applied Mathematics. Springer New York, 2012.

[72] R. Dagher, A. Quadrat and G. Zheng. 'Algebraic solutions to the metric multidimensional unfolding. Application to the position self-calibration problem'. In: *in preparation* (2019).

[73] R. Dagher, A. Quadrat and G. Zheng. 'Auto-localisation par mesure de distances'. In: *Pattern n. FR1853553* (2018).

[74] M. Deraux and E. Falbel. 'Complex hyperbolic geometry of the figure eight knot'. In: *Geometry and Topology* 19 (Feb. 2015), pp. 237–293. DOI: 10.2140/gt.2015.19.237. URL: https://hal.archives-ouvertes.fr/hal-00805427.

[75] D. N. Diatta, S. Diatta, F. Rouillier, M.-F. Roy and M. Sagraloff. 'Bounds for polynomials on algebraic numbers and application to curve topology'. In: *Discrete and Computational Geometry* 67 (Feb. 2022), pp. 631–697. DOI: 10.1007/s00454-021-00353-w. URL: https://inria.hal.science/hal-01891417.

[76] W. Diffie and M. E. Hellman. 'New directions in cryptography'. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[77] S. Diop. 'Differential-algebraic decision methods and some applications to system theory'. In: *Theoret. Comput. Sci.* 98 (1992), pp. 137–161.

[78] S. Diop. 'Elimination in control theory'. In: *Math. Control Signals Systems* 4 (1991), pp. 17–32.

[79] J. Doliskani, A. K. Narayanan and É. Schost. 'Drinfeld Modules with Complex Multiplication, Hasse Invariants and Factoring Polynomials over Finite Fields'. In: *CoRR* abs/1712.00669 (2017). arXiv: 1712.00669. URL: http://arxiv.org/abs/1712.00669.

[80] T. Espitau and A. Joux. 'Adaptive precision LLL and Potential-LLL reductions with Interval arithmetic'. In: *IACR Cryptology ePrint Archive* 2016 (2016), p. 528. URL: http://eprint.iacr.org/2016/528.

[81] H. Evelyne. 'Notes on Triangular Sets and Triangulation-Decomposition Algorithms II: Differential Systems'. In: *Symbolic and Numerical Scientific Computation*. Ed. by F. Winkler and U. Langer. Lecture Notes in Computer Science 2630. Springer, 2003, pp. 40–87.

[82] E. Falbel and A. Guilloux. 'Dimension of character varieties for 3-manifolds'. In: *Proceedings of the American Mathematical Society* (2016). DOI: 10.1090/proc/13394. URL: https://hal.archives-ouvertes.fr/hal-01370284.

[83] E. Falbel, A. Guilloux and P. Will. 'Hilbert metric, beyond convexity'. working paper or preprint. 2018. URL: https://hal.archives-ouvertes.fr/hal-01768400.

[84] E. Falbel, A. Guilloux and P. Will. 'Slim curves, limit sets and spherical CR uniformisations'. working paper or preprint. May 2022. URL: https://hal.science/hal-03673101.

[85] E. Falbel, P.-V. Koseleff and F. Rouillier. 'Representations of fundamental groups of 3-manifolds into PGL(3,C): Exact computations in low complexity'. In: *Geometriae Dedicata* 177.1 (Aug. 2015), p. 52. DOI: 10.1007/s10711-014-9987-x. URL: https://hal.inria.fr/hal-00908843.

[86] E. Falbel, M. Maculan and G. Sarfatti. 'Configurations of flags in orbits of real forms'. working paper or preprint. Apr. 2018. URL: https://hal.archives-ouvertes.fr/hal-01779459.

[87] E. Falbel and R. Santos Thebaldi. 'A Flag structure on a cusped hyperbolic 3-manifold with unipotent holonomy'. In: *Pacific Journal of Mathematics* 278.1 (2015), pp. 51–78. URL: https://hal.archives-ouvertes.fr/hal-00958255.

[88] E. Falbel and J. Veloso. 'Flag structures on real 3-manifolds'. working paper or preprint. Apr. 2018. URL: https://hal.archives-ouvertes.fr/hal-01778582.

[89] J. Faugère and D. Lazard. 'Combinatorial classes of parallel manipulators'. In: *Mechanism and Machine Theory* 30.6 (1995), pp. 765–776. DOI: https://doi.org/10.1016/0094-114X(94)00069-W. URL: http://www.sciencedirect.com/science/article/pii/0094114X9400069W.

[90] M. Fliess and H. Sira-Ramırez. 'An algebraic framework for linear identification'. In: *ESAIM Control Optim. Calc. Variat.* 9 (2003), pp. 151–168.

[91] J. v. z. Gathen and J. Gerhard. *Modern Computer Algebra*. 3rd. New York, NY, USA: Cambridge University Press, 2013.

[92] A. Gélin and A. Joux. 'Reducing number field defining polynomials: an application to class group computations'. In: *Algorithmic Number Theory Symposium XII*. Vol. 19. LMS Journal of Computation and Mathematics A. Kaiserslautern, Germany, Aug. 2016, pp. 315–331. DOI: 10.1112/S1461157016000255. URL: https://hal.archives-ouvertes.fr/hal-01362144.

[93] F. Göloğlu and A. Joux. 'A Simplified Approach to Rigorous Degree 2 Elimination in Discrete Logarithm Algorithms'. In: *IACR Cryptology ePrint Archive* 2018 (2018), p. 430. URL: https://eprint.iacr.org/2018/430.

[94] A. Guilloux. 'Volume of representations and birationality of peripheral holonomy'. In: *Experimental Mathematics* (May 2017). URL: https://hal.archives-ouvertes.fr/hal-01370287.

[95] A. Guilloux and I. Kim. 'Deformation space of discrete groups of SU(2,1) in quaternionic hyperbolic plane'. working paper or preprint. Mar. 2018. URL: https://hal.archives-ouvertes.fr/hal-01736953.

[96] A. Guilloux and J. Marché. 'Volume function and Mahler measure of exact polynomials'. working paper or preprint. Apr. 2018. URL: https://hal.archives-ouvertes.fr/hal-01758986.

[97] A. Guilloux and P. Will. 'On SL(3,C)-representations of the Whitehead link group'. To appear in Geom. Ded. 2018. URL: https://hal.archives-ouvertes.fr/hal-01370289.

[98] E. Hubert, A. Barrau and M. El Badaoui. 'New Multi-Carrier Demodulation Method Applied to Gearbox Vibration Analysis'. In: Apr. 2018, pp. 2141–2145. DOI: 10.1109/ICASSP.2018.8461924.

[99] M. L. Husty and H.-P. Schröcker. 'Algebraic Geometry and Kinematics'. In: *Nonlinear Computational Geometry*. Ed. by I. Z. Emiris, F. Sottile and T. Theobald. New York, NY: Springer New York, 2010, pp. 85–107.

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

[101] R. Jha, D. Chablat, L. Baron, F. Rouillier and G. Moroz. 'Workspace, Joint space and Singularities of a family of Delta-Like Robot'. In: *Mechanism and Machine Theory* 127 (Sept. 2018), pp. 73–95. DOI: 10.1016/j.mechmachtheory.2018.05.004. URL: https://hal.archives-ouvertes.fr/hal-01796066.

[102] R. Jha, D. Chablat, F. Rouillier and 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*. ASME. Boston, United States, Aug. 2015. URL: https://hal.archives-ouvertes.fr/hal-01142989.

[103] R. Jha, D. Chablat, F. Rouillier and 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. URL: https://hal.archives-ouvertes.fr/hal-01142465.

[104] A. Joux and R. Lercier. 'The function field sieve is quite special'. In: *Algorithmic Number Theory-ANTS V*. Vol. 2369. Lecture Notes in Computer Science. Springer, 2002, pp. 431–445.

[105] A. Joux and 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*. Vol. 8873. Lecture Notes in Computer Science. Kaoshiung, Taiwan: Springer Berlin Heidelberg, Dec. 2014, pp. 378–397. DOI: 10.1007/978-3-662-45611-8_20. URL: https://hal.archives-ouvertes.fr/hal-01213649.

[106] A. Joux and 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. URL: https://hal.inria.fr/hal-01154879.

[107] T. Kailath. *Linear Systems*. Prentice-Hall, 1980.

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

[109] M. Kashiwara, T. Kawai and T. Kimura. *Foundations of Algebraic Analysis*. Vol. 37. Princeton University Press, 1986.

[110] A. Kobel, F. Rouillier and 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*. ISSAC '16 Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation. Waterloo, Canada, July 2016, p. 7. DOI: 10.1145/2930889.2930937. URL: https://hal.inria.fr/hal-01363955.

[111] N. Koblitz. 'Elliptic curve cryptosystems'. In: *Mathematics of Computation* 48.177 (Jan. 1987), pp. 203–209.

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

[113] P.-V. Koseleff and D. Pecker. 'Chebyshev Knots'. In: *Journal of Knot Theory and Its Ramifications* 20.4 (Apr. 2011), pp. 575–593. DOI: 10.1142/S0218216511009364. URL: https://hal.archives-ouvertes.fr/hal-00344501.

[114] P.-V. Koseleff and D. Pecker. 'Harmonic Knots'. In: *Journal Of Knot Theory And Its Ramifications (JKTR)* 25.13 (2016). 18 p., 30 fig., p. 18. DOI: 10.1142/S0218216516500747. URL: https://hal.archives-ouvertes.fr/hal-00680746.

[115] P.-V. Koseleff and D. Pecker. 'On Alexander–Conway polynomials of two-bridge links'. In: *Journal of Symbolic Computation*. Effective Methods in Algebraic Geometry Volume 68.2 (May 2015). 15p, pp. 215–229. DOI: 10.1016/j.jsc.2014.09.011. URL: https://hal.archives-ouvertes.fr/hal-00538729.

[116] P.-V. Koseleff, D. Pecker and F. Rouillier. 'The first rational Chebyshev knots'. In: *Journal of Symbolic Computation* 45.12 (Dec. 2010), pp. 1341–1358. DOI: 10.1016/j.jsc.2010.06.014. URL: https://hal.archives-ouvertes.fr/hal-00429510.

[117] P.-V. Koseleff, D. Pecker, F. Rouillier and C. Tran. 'Computing Chebyshev knot diagrams'. In: *Journal of Symbolic Computation* 86 (2018), p. 21. DOI: 10.1016/j.jsc.2017.04.001. URL: https://hal.inria.fr/hal-01232181.

[118] P.-V. Koseleff, F. Rouillier and C. Tran. 'On the sign of a trigonometric expression'. In: *ISSAC ' 15*. Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation. Bath, United Kingdom, July 2015. DOI: 10.1145/2755996.2756664. URL: https://hal.inria.fr/hal-01200820.

[119] B. A. LaMacchia and A. M. Odlyzko. 'Computation of discrete logarithms in prime fields'. In: *Designs, Codes and Cryptography* 1 (1991), pp. 47–62.

[120] S. Lazard, M. Pouget and F. Rouillier. ‘Bivariate triangular decompositions in the presence of asymptotes’. In: *Journal of Symbolic Computation* 82 (2017), pp. 123–133. DOI: 10.1016/j.jsc.2017.01.004. URL: https://hal.inria.fr/hal-01468796.

[121] A. K. Lenstra and H. W. Lenstra, eds. *The development of the number field sieve.* Vol. 1554. Lecture Notes in Mathematics. Springer-Verlag, 1993.

[122] H. Lenstra Jr. ‘Factoring integers with elliptic curves’. In: *Annals of Mathematics* 126.2 (1987), pp. 649–673.

[123] B. Mourrain. ‘The 40 Generic Positions of a Parallel Robot’. In: *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation.* ISSAC ’93. Kiev, Ukraine: ACM, 1993, pp. 173–182. DOI: 10.1145/164081.164120. URL: http://doi.acm.org/10.1145/164081.164120.

[124] D. Niang Diatta, F. Rouillier and M.-F. Roy. ‘On the computation of the topology of plane curves’. In: *International Symposium on Symbolic and Algebraic Computation.* Ed. by K. Nabeshima. Kobe University. Kobe, Japan: ACM Press, July 2014, pp. 130–137. DOI: 10.1145/2608628.2608670. URL: https://hal.archives-ouvertes.fr/hal-00935728.

[125] U. Oberst. ‘Multidimensional constant linear systems’. In: *Acta Appl. Math.* 20 (1990), pp. 1–175.

[126] C. Pomerance. ‘Analysis and comparison of some integer factoring methods’. In: *Computational methods in number theory – Part I.* Ed. by J. Hendrik W. Lenstra and R. Tijdeman. Vol. 154. Mathematical centre tracts. Amsterdam: Mathematisch Centrum, 1982, pp. 8–139.

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

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

[129] A. Quadrat. ‘Grade filtration of linear functional systems’. In: *Acta Applicandæ Mathematicæ* 127.1 (Oct. 2013), pp. 27–86. DOI: 10.1007/s10440-012-9791-2. URL: https://hal-supelec.archives-ouvertes.fr/hal-00925510.

[130] 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. URL: https://hal-supelec.archives-ouvertes.fr/hal-01108019.

[131] A. Quadrat. ‘Towards an effective study of the algebraic parameter estimation problem’. In: *IFAC 2017 Workshop Congress.* Toulouse, France, July 2017. URL: https://hal.inria.fr/hal-01415300.

[132] A. Quadrat and G. Regensburger. *Computing Polynomial Solutions and Annihilators of Integro-Differential Operators with Polynomial Coefficients.* Research Report RR-9002. Inria Lille - Nord Europe ; Institute for Algebra, Johannes Kepler University Linz, Dec. 2016, p. 24. URL: https://hal.inria.fr/hal-01413907.

[133] A. Quadrat and D. Robertz. ‘A constructive study of the module structure of rings of partial differential operators’. In: *Acta Applicandæ Mathematicæ* 133 (2014), pp. 187–243. DOI: 10.1007/s10440-013-9864-x. URL: https://hal-supelec.archives-ouvertes.fr/hal-00925533.

[134] A. Quadrat and 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, p. 8. URL: https://hal.inria.fr/hal-01415256.

[135] G. Rance. ‘Parametric $H_\infty$ control and its application to gyrostabilized sights’. Theses. Université Paris-Saclay, July 2018. URL: https://tel.archives-ouvertes.fr/tel-01904086.

[136] G. Rance, Y. Bouzidi, A. Quadrat and 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, p. 8. URL: https://hal.inria.fr/hal-01415294.

[137] G. Rance, Y. Bouzidi, A. Quadrat and A. Quadrat. 'Explicit H$\infty$ controllers for 1st to 3rd order single-input single-output systems with parameters'. In: *IFAC 2017 Workshop Congress*. Toulouse, France, July 2017. URL: https://hal.inria.fr/hal-01667410.

[138] G. Rance, Y. Bouzidi, A. Quadrat, A. Quadrat and F. Rouillier. 'Explicit H$\infty$ 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. URL: https://hal.inria.fr/hal-01667368.

[139] J. Ritt. *Differential Algebra*. Colloquium publications. American Mathematical Society, 1950.

[140] R. Rivest, A. Shamir and L. Adleman. 'A method for obtaining digital signatures and public-key cryptosystems'. In: *Commun. ACM* 21.2 (1978), pp. 120–126.

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

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

[143] J. T. Stafford. 'Module structure of Weyl algebras'. In: *J. London Math. Soc.* 18 (1978), pp. 429–442.

[144] V. Miller. 'Use of elliptic curves in cryptography'. In: *Advances in Cryptology — CRYPTO'85*. Ed. by H. Williams. Vol. 218. LNCS. Springer, 1986, pp. 417–428.

[145] V. A. Vassiliev. 'Cohomology of knot spaces'. In: *Theory of singularities and its applications*. Vol. 1. Adv. Soviet Math. Amer. Math. Soc., Providence, RI, 1990, pp. 23–69.

[146] J. Weeks. 'Chapter 10 - Computation of Hyperbolic Structures in Knot Theory'. In: *Handbook of Knot Theory*. Ed. by W. Menasco and M. Thistlethwaite. Amsterdam: Elsevier Science, 2005, pp. 461–480. DOI: https://doi.org/10.1016/B978-044451452-3/50011-3. URL: http://www.sciencedirect.com/science/article/pii/B9780444514523500113.

[147] P. Wenger. 'A new general formalism for the kinematic analysis of all nonredundant manipulators'. In: *ICRA*. 1992.

[148] J. Willems and J. Polderman. *Introduction to Mathematical Systems Theory: A Behavioral Approach*. Texts in Applied Mathematics. Springer New York, 2013.