RESEARCH CENTRE

**Inria Paris Center**
**at Sorbonne University**

**IN PARTNERSHIP WITH:**

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

2022

# 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**

Inria

# Contents


**Project-Team OURAGAN** 1

**1 Team members, visitors, external collaborators** 2

**2 Overall objectives** 3
2.1 Scientific ground . . . 4
2.1.1 Basic computable objects and algorithms . . . 4
2.1.2 Computational Number Theory . . . 4
2.1.3 Topology in small dimension . . . 6
2.1.4 Algebraic analysis of functional systems . . . 8
2.2 Synergies . . . 8

**3 Research program** 9
3.1 Basic computable objects and algorithms . . . 9
3.2 Algorithmic Number Theory . . . 10
3.3 Topology in small dimension . . . 10
3.4 Algebraic analysis of functional systems . . . 11

**4 Application domains** 12
4.1 Security of cryptographic systems . . . 12
4.2 Robotics . . . 12
4.3 Control theory . . . 13
4.4 Signal processing . . . 13

**5 Social and environmental responsibility** 14

**6 Highlights of the year** 14
6.1 Science . . . 14
6.2 Partnerships . . . 15
6.3 Institutional life . . . 15

**7 New software and platforms** 15
7.1 New software . . . 15
7.1.1 ISOTOP . . . 15
7.1.2 RS . . . 15
7.1.3 A NewDsc . . . 16
7.1.4 SIROPA . . . 16
7.1.5 MPFI . . . 16
7.2 New platforms . . . 16
7.2.1 Visualisation of limit sets . . . 16

**8 New results** 17
8.1 Algebraic analysis of functional systems . . . 17
8.2 Computational Geometry . . . 18
8.3 Effective real algebraic geometry . . . 18
8.4 Number theory . . . 19
8.5 Numerical Algebraic Geometry . . . 21
8.6 Miscancellanous . . . 21
8.7 PhD thesis . . . 22

**9 Bilateral contracts and grants with industry** 23
9.1 Bilateral contracts with industry . . . 23

**10 Partnerships and cooperations** **23**
10.1 National initiatives . . . 23
10.1.1 ANR . . . 23
10.1.2 Inria Exploratory actions . . . 24

**11 Dissemination** **24**
11.1 Promoting scientific activities . . . 24
11.1.1 Scientific events: selection . . . 24
11.1.2 Journal . . . 25
11.1.3 Invited talks . . . 25
11.1.4 Scientific expertise . . . 25
11.1.5 Research administration . . . 26
11.2 Teaching - Supervision - Juries . . . 26
11.2.1 Teaching . . . 26
11.2.2 Supervision . . . 26
11.2.3 Juries . . . 27
11.3 Popularization . . . 27
11.3.1 Internal or external Inria responsibilities . . . 27

**12 Scientific production** **27**
12.1 Major publications . . . 27
12.2 Publications of the year . . . 28
12.3 Cited publications . . . 31

# 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]
- Elisha Falbel [SORBONNE UNIVERSITE, Professor, HDR]
- Antonin Guilloux [SORBONNE UNIVERSITE, Associate Professor, HDR]
- Antoine Joux [SORBONNE UNIVERSITE, Associate Professor, HDR]
- Pierre-Vincent Koseleff [SORBONNE UNIVERSITE, Associate Professor, HDR]
- Mahya Mehrabdollahei [Sorbonne Université, ATER]
- Pascal Molin [UNIVERSITE PARIS, Associate Professor]

## Post-Doctoral Fellows

- Aurelien Gribinski [INRIA, from Dec 2022]
- Manuel Radons [INRIA, from Oct 2022]
- Gregoire Sergeant-Perthuis [INRIA, from Oct 2022]

## PhD Students

- Raphael Alexandre [Sorbonne Université, until Aug 2022]
- Thibauld Feneuil [Crypto Experts, CIFRE]
- Christina Katsamaki [INRIA and FSMP]
- Alexandre Le [SAFRAN, CIFRE]
- Camille Pinto [INRIA (CORDI-S), from Oct 2022]
- Grace Younes [INRIA (CORDI-S), until Jan 2022]

## 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 function over an algebraic variety.

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

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

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

## 2.1 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 [74], subresultants [94], critical point methods [51], 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 [113] [17], rational parameterizations of solutions of zero-dimensional systems with rational coefficients [60] [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 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 [108] (for example to make progress on the computation of class groups in number fields [95]), network reductions by means of LLL variants [84] and, obviously, various computations in linear algebra, for example dedicated to *almost sparse* matrices [109].

For the algorithmic approach to algebraic analysis of functional equations [55] [111] [112], we developed the effective study of both module theory and homological algebra [145] over certain non-commutative polynomial rings of functional operators [4], of Stafford's famous theorems on the Weyl algebras [136], of the equidimensional decomposition of functional systems [132], 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 computa-

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

tional 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 [80], where they proposed a first instantiation of their paradigm based on the discrete logarithm problem in prime fields. The invention of RSA [143], based on the hardness of factoring came as a second example. The introduction of discrete logarithms on elliptic curves [114] [147] 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) [125]
- the quadratic field for factoring [129] and its variant for discrete log called the Gaussian integers method [122]
- the number field sieve (NFS) [124]

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

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

Members of OURAGAN started working on the topic of discrete logarithms around 1998, with several computation records that were announced on the *NMBRTHRY* mailing list. In large characteristic, especially for the case of prime fields, the best current method is the number field sieve (NFS) algorithm. In particular, they published the first NFS based record computation[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 [107].

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 [108, 96].

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* has strong links with the computations of discrete logarithms or factorizations using the NFS (number field sieve) strategy which as the name suggests is based on the use of number fields. Roughly speaking, the NFS algorithm uses two number fields and the strategy consists in choosing number fields with small sized coefficients in their definition polynomials. On the contrary, in class group computations, there is a single number field, which is clearly a simplification, but this field is given as input by some fixed definition polynomial. Obviously,

[9] www.lmfdb.org

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 [95], 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 [54].

### 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 [149] and is regularly used as a starting point in our work. Along the same philosophy of implementation, we can also cite Regina [11]. A specific trait of SnapPy is that it focuses on hyperbolic structures on the 3-dimensional manifolds. This setting is the object of a huge amount of theoretical work that were used to speed up computations. For example, some Newton methods were implemented without certification for solving a system of equations, but the theoretical knowledge of the uniqueness of the solution made this implementation efficient enough for the target applications. In recent years, in part under the influence of our team [12], more attention has been given to certified computations (at least with an error control) and now this is implemented in SnapPy.

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

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

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

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

[53][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 [88] 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[148].

A Chebyshev knot [116], 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 [117] 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 [119]. On the other hand, we propose the identification of Chebyshev knot diagrams [120] by developing new certified algorithms for computing trigonometric expressions [121]. These works share many tools with our action in visualization and computational geometry.

We made use of Chebyshev polynomials so as Fibonacci polynomials which are families of orthogonal polynomials. Considering the Alexander-Conway polynomials as continuant polynomials in the Fibonacci basis, we were able to give a partial answer to Hoste's conjecture on the roots of Alexander polynomials of alternating knots ( [118]).

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 [67] [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 [66], the slide isotopies on trigonal diagrams, namely those that never increase the number of crossings [68].

**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 [73], 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.

[14] ANR project Structures Géométriques et Triangulations

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

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 [60, 113, 61, 62] which are basic engines for computing the topology [127, 25] 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. [103] [111] [112] [115] [142] [130].

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* [111, 112, 55], a mathematical theory developed by the Japanese school of Sato, which studies linear differential systems by means of both algebraic and analytic methods. To develop an effective approach to algebraic analysis, we first have to make algorithmic standard results on rings of functional operators, module theory, homological algebra, algebraic geometry, sheaf theory, category theory, etc., and to implement them in computer algebra systems. Based on elimination theory (Gröbner or Janet bases [103, 72, 144], differential algebra [57] [85], Spencer's theory [130], 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 [72]). Based on the effective aspects to algebraic analysis approach, the parametrizability problem [4], the reduction and (Serre) decomposition problems [5], the equidimensional decomposition [132], Stafford's famous theorems for the Weyl algebras [136], etc., have been studied and solutions have been implemented in `Maple`, `Mathematica`, and `GAP` [71][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 [25, 123, 61] 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 [83] 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 [88, 100]; 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 [86]. 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 [89, 91]. 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 [98] and [100]). 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 [79, 90, 87].

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 [97]. Then, theoretical discussions around this conjecture led to a paper on a new approach to the Mahler measure of some 2-variables polynomials [99]. 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.

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

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

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 [145] which play important roles in algebraic analysis [55, 111, 112] 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 [131, 135] which play an important role in mathematical systems theory, control theory, and signal processing [131, 141, 134, 137].

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 [52]. Therefore, we want to develop an algorithmic study of these rings. Following the direction initiated in [135] 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

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

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 [146], 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 [131, 134] 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) [50]. 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 [102]. For example, one can find algebraic proofs for the 40 possible solutions to the direct kinematics problem [126] for steward platforms and companion experiments based on Gröbner basis computations [92]. 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 [150]).

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 [70, 69, 104, 106, 105] 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 [56] on control theory of multidimensional systems. Moreover, the differential algebra approach to nonlinear control theory (see [82, 81] and the references therein) was a major motivation for the algorithmic study of differential algebra [57, 85]. Finally, the behaviour approach to linear systems theory [151, 128] 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 [56, 128] and infinite-dimensional systems [76] (such as, e.g., differential time-delay systems).

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

In control theory, stability analysis of linear time-invariant control systems is based on the famous Routh-Hurwitz criterion (late 19th century) and its relation with Sturm sequences and Cauchy index. Thus, stability tests were only involving tools for univariate polynomials [110]. While extending those tests to multidimensional systems or differential time-delay systems, one had to tackle multivariate problems recursively with respect to the variables [56]. 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 [63, 64, 65]. 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 [58, 64, 65] 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 [62, 61].

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 [59, 133, 139, 138, 140, 141].

## 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 [75] 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 [77] 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 [78]. 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* [101] 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 [93], 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 [134] 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

## 6.1 Science

- One fascinating conjecture around Mahler measure is due to Lehmer: there exist a constant $c > 0$ such that if a univariate polynomial with integer coefficients has a non zero Mahler measure, then this Mahler measure is bigger than $c$. This conjecture attracts a lot of attention since its statement a century ago. One approach, following Boyd, is to understand the closedness of the set of all Mahler measures of all polynomials with integer coefficients.

  A celebrated theorem in this area was due to Boyd Lawton and stated that certain sequence of Mahler measures of univariate polynomials converge to the Mahler measure of a multivariate polynomial. The team took part in a breakthrough generalization of this theorem to sequences of multivariate polynomials as illustrated, for example, by [44].

- Pascal Molin, in a joint effort with Aurel Page from Inria Bordeaux, developped algorithms to compute with Hecke characters: these are ubiquitous object in modern number theory which were previously not fully handled by computer algebra systems. Their package is incorporated in Pari/GP 2.15, and the corresponding paper was presented at the ANTS XV conference ([35]).

- Josué Tonelli-Cueto wrote probably the shortest paper of the year (1 page) (see [29])

- Fabrice Rouillier did contribute to the first algorithm with a (supposed to be) optimal complexity for the computation of the topology of a real algebraic plane curve given in implicit form and without shearing the curve (see [25])

### 6.2 Partnerships

- our second important participation to an ANR funding fundamental mathematics starts with the project *SHoCoS*.

- a new contract has been signed with Safran defense and electronics about the conception of parallel robots for inertial stabilization.

### 6.3 Institutional life

The team wishes to thank the Commission d'Évaluation for its outstanding efforts, in 2022 and previous years, in defending the interests of the research community, keeping us thoroughly informed about topics relevant to the scientific life at Inria, and upholding the moral and intellectual values we are collectively proud of and which define our institute.

## 7 New software and platforms

### 7.1 New software

#### 7.1.1 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

#### 7.1.2 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

#### 7.1.3 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

#### 7.1.4 SIROPA

**Keywords:** Robotics, Kinematics

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

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

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

**Contact:** Guillaume Moroz

**Partner:** LS2N

#### 7.1.5 MPFI

**Keyword:** Arithmetic

**Functional Description:** MPFI is a C library based on MPFR and GMP for multi precision floating point arithmetic.

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

**Contact:** Fabrice Rouillier

### 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" ( http://limit-sets.imj-prg.fr). 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 [45].

# 8 New results

## 8.1 Algebraic analysis of functional systems

**On the Ore extension ring of differential time-varying delay operators** .

In [40], we propose an algebraic method to study linear differential time-varying delay (DTVD) systems. Our goal is to give an effective construction of the ring of DTVD operators as an Ore extension, thanks to the concept of skew polynomial rings developed by Ore in the 30s. Some algebraic properties of the DTVD operators ring are analyzed, such as its Noetherianity, its homological and Krull dimensions, and the existence of Gröbner bases, all given in terms of the time-varying delay function. The algebraic analysis framework for linear systems theory allows us to study linear DTVD systems and essential properties such as the existence of autonomous elements, controllability, parametrizability, flatness, etc., through methods coming from module theory, homological algebra, and constructive algebra.

**An integro-differential operator approach to linear differential systems** . In [36], we initiate a new algebraic analysis approach to linear differential systems based on rings of integro-differential operators. Within this algebraic analysis approach, we first interpret the method of variations of constants as an operator identity. Using this result, we show that the module associated with a state-space representation of a linear system is the same as the one associated with its standard convolution representation. This finitely presented module over the ring of integro-differential operators is proved to be stably free. Finally, we show how the reachability property can be expressed within this algebraic analysis approach.

**An Integro-differential-delay Operator Approach to Transformations of Linear Differential Time-delay Systems** . In [38], we further develop the study of rings of integro-differential-delay operators considered as noncommutative polynomial algebras satisfying standard calculus identities. Within the algebraic analysis approach, we show that transformations and reductions of linear differential time-delay systems can be interpreted as homomorphisms and isomorphisms of finitely presented left modules over an algebra of integro-differential-delay operators. In particular, we show how Fiagbedzi-Pearson's transformation can be found again and generalized. This transformation maps the solutions of a first-order differential linear system with state and input delays to the solutions of a purely state-space linear system. Fiagbedzi-Pearson's transformation reduces to the well-known Artstein's reduction when the system has no state delay and yields an isomorphism of the solution spaces.

**An Integro-differential Operator Approach to Linear State-space Systems** . In [37], the algebraic analysis approach to linear state-space systems is further developed using rings of integro-differential operators. The module structure of linear state-space systems is investigated over these rings. The module associated with a linear state-space system is shown to be the direct sum of the stably free module defined by the linear system without inputs and the free module defined by the inputs of the system.

**Computation of Koszul homology and application to involutivity of partial differential systems** . The formal integrability of systems of partial differential equations plays a fundamental role in different analysis and synthesis problems for both linear and nonlinear differential control systems. In [32], following Spencer's theory, to test the formal integrability of a system of partial differential equations, we must study when the symbol of the system, namely, the top-order part of the linearization of the system, is 2-acyclic or involutive, i.e., when certain Spencer cohomology groups vanish. Combining the fact that Spencer cohomology is dual to Koszul homology and symbolic computation methods, we show how to effectively compute the homology modules defined by the Koszul complex of a finitely presented module over a commutative polynomial ring. These results are implemented using the OreMorphisms package. We then use these results to effectively characterize 2-acyclicity and involutivity of the symbol of a linear system of partial differential equations. Finally, we show explicit computations on two standard examples.

## 8.2 Computational Geometry

**Efficient sampling in spectrahedra and volume approximation** . In [21], we present algorithmic, complexity, and implementation results on the problem of sampling points from a spectrahedron, that is, the feasible region of a semidefinite program. Our main tool is geometric random walks. We analyze the arithmetic and bit complexity of certain primitive geometric operations that are based on the algebraic properties of spectrahedra and the polynomial eigenvalue problem. This study leads to the implementation of a broad collection of random walks for sampling from spectrahedra that experimentally show faster mixing times than methods currently employed either in theoretical studies or in applications, including the popular family of Hit-and-Run walks. The different random walks offer a variety of advantages, thus allowing us to efficiently sample from general probability distributions, for example the family of log-concave distributions which arise in numerous applications. We focus on two major applications of independent interest: (i) approximate the volume of a spectrahedron, and (ii) compute the expectation of functions coming from robust optimal control. We exploit efficient linear algebra algorithms and implementations to address the aforementioned computations in very high dimension. In particular, we provide a C++ open source implementation of our methods that scales efficiently, for the first time, up to dimension 200. We illustrate its efficiency on various data sets.

**On the Complexity of the Plantinga-Vegter Algorithm** . In [23], we introduce a general toolbox for precision control and complexity analysis of subdivision based algorithms in computational geometry. We showcase the toolbox on a well known example from this family; the adaptive subdivision algorithm due to Plantinga and Vegter. The only existing complexity estimate on this rather fast algorithm was an exponential worst-case upper bound for its interval arithmetic version. We go beyond the worst-case by considering smoothed analysis, and prove polynomial time complexity estimates for both interval arithmetic and finite precision versions of the Plantinga-Vegter algorithm. The employed toolbox is a blend of robust probabilistic techniques coming from geometric functional analysis with condition numbers and the continuous amortization paradigm introduced by Burr, Krahmer and Yap. We hope this combination of tools from different disciplines would prove useful for understanding complexity aspects of the broad family of subdivision based algorithms in computational geometry.

**On the Error of Random Sampling: Uniformly Distributed Random Points on Parametric Curves** . Given a parametric polynomial curve $\gamma : [a,b] \to Rn$, how can we sample a random point $x \in im(\gamma)$ in such a way that it is distributed uniformly with respect to the arc-length? Unfortunately, we cannot sample exactly such a point—even assuming we can perform exact arithmetic operations. So we end up with the following question: how does the method we choose affect the quality of the approximate sample we obtain? In practice, there are many answers. However, in theory, there are still gaps in our understanding. In [31], we address this question from the point of view of complexity theory, providing bounds in terms of the size of the desired error.

## 8.3 Effective real algebraic geometry

**PTOPO: Computing the Geometry and the Topology of Parametric Curves** . In [27], we consider the problem of computing the topology and describing the geometry of a parametric curve in $R^n$. We present an algorithm, PTOPO, that constructs an abstract graph that is isotopic to the curve in the embedding space. Our method exploits the benefits of the parametric representation and does not resort to implicitization. Most importantly, we perform all computations in the parameter space and not in the implicit space. When the parametrization involves polynomials of degree at most $d$ and maximum bitsize of coefficients $\tau$, then the worst case bit complexity of PTOPO is $O_B(nd^6 + nd^5\tau + d^4(n^2 + n\tau) + d^3(n^2\tau + n^3) + n^3d^2\tau)$. This bound matches the current record bound $O_B(d^6 + d^5\tau)$ for the problem of computing the topology of a plane algebraic curve given in implicit form. For plane and space curves, if $N = max(d,\tau)$, the complexity of PTOPO becomes $O_B(N^6)$, which improves the stateof-the-art result,

due to Alcázar and Díaz-Toca [CAGD10], by a factor of $N^1 0$. In the same time complexity, we obtain a graph whose straight-line embedding is isotopic to the curve. However, visualizing the curve on top of the abstract graph construction, increases the bound to $OB(N^7)$. For curves of general dimension, we can also distinguish between ordinary and non-ordinary real singularities and determine their multiplicities in the same expected complexity of PTOPO by employing the algorithm of Blasco and Pérez-Díaz [CAGD'19]. We have implemented PTOPO in maple for the case of plane and space curves. Our experiments illustrate its practical nature.

**Bounds for polynomials on algebraic numbers and application to curve topology** .

Let $P \in Z[X,Y]$ be a given square-free polynomial of total degree d with integer coefficients of bitsize less than $\tau$, and let $VR(P) := (x,y) \in R^2, P(x,y) = 0$ be the real planar algebraic curve implicitly defined as the vanishing set of P. In [25], we give a deterministic algorithm to compute the topology of $VR(P)$ in terms of a simple straight-line planar graph G that is isotopic to $VR(P)$. The upper bound on the bit complexity of our algorithm is in $\tilde{O}(d^5\tau + d^6)$ which matches the current record bound for the problem of computing the topology of a planar algebraic curve. However, compared to existing algorithms with comparable complexity, our method does not consider any change of coordinates, and more importantly the returned simple planar graph $G$ yields the cylindrical algebraic decomposition information of the curve in the original coordinates. Our result is based on two main ingredients: First, we derive amortized quantitative bounds on the roots of polynomials with algebraic coefficients.

**Beyond Worst-Case Analysis for Root Isolation Algorithms** . Isolating the real roots of univariate polynomials is a fundamental problem in symbolic computation and it is arguably one of the most important problems in computational mathematics. The problem has a long history decorated with numerous ingenious algorithms and furnishes an active area of research. However, the worst-case analysis of root-finding algorithms does not correlate with their practical performance. In [33], we develop a smoothed analysis framework for polynomials with integer coefficients to bridge the gap between the complexity estimates and the practical performance. In this setting, we derive that the expected bit complexity of Descartes solver to isolate the real roots of a polynomial, with coefficients uniformly distributed, is $\tilde{O}B(d2 + d\tau)$, where d is the degree of the polynomial and $\tau$ the bitsize of the coefficients.

## 8.4 Number theory

**On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$** . Since their introduction in 2004,Polynomial Modular Number Systems (PMNS) have become a very interesting tool for implementing cryptosys- tems relying on modular arithmetic in a secure and efficient way. However, while their implementation is simple, their parameterization is not trivial and relies on a suitable choice of the polynomial on which the PMNS operates. The initial proposals were based on particular binomials and trinomials. But these polynomials do not always provide systems with interesting characteristics such as small digits, fast reduction, etc. In [19], we study a larger family of polynomials that can be exploited to design a safe and efficient PMNS. To do so, we first state a complete existence theorem for PMNS which provides bounds on the size of the digits for a generic polynomial, significantly improving previous bounds. Then, we present classes of suitable polynomials which provide numerous PMNS for safe and efficient arithmetic.

**Generating Very Large RNS Bases** .

Residue Number Systems (RNS) are proven to be effective in speeding up computations involving additions and products. For these representations, there exists efficient modular reduction algorithms that can be used in the context of arithmetic over finite fields or modulo large numbers, especially when used in the context of cryptographic engineering. Their independence allows random draws of bases, which also makes it possible to protect against side-channel attacks, or even to detect them using redundancy. These systems are easily scalable, however the existence of large bases for some specific uses remains a difficult question. In [18], we present four techniques to extract RNS bases from specific

sets of integers, giving better performance and flexibility to previous works in the litterature. While our techniques do not allow to solve efficiently every possible case, we provide techniques to provably and efficiently find the largest possible available RNS bases in several cases, improving the state-of-the-art on various works of the recent literature.

**A classification of ECM-friendly families using modular curves** . In [20], we establish a link between the classification of ECM-friendly curves and Mazur's program $B$, which consists in parameterizing all the families of elliptic curves with exceptional Galois image. Building upon two recent works which treated the case of congruence subgroups of prime-power level which occur for infinitely many $j$-invariants, we prove that there are exactly 1525 families of rational elliptic curves with distinct Galois images which are cartesian products of subgroups of prime-power level. This makes a complete list of rational families of ECM-friendly elliptic curves, out of which less than 25 were known in the literature. We furthermore refine a heuristic of Montgomery to compare these families and conclude that the best 4 families which can be put in $a = -1$ twisted Edwards' form are new.

**Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection** . In [34], we propose (honest verifier) zero-knowledge arguments for the modular subset sum problem. Previous combinatorial approaches, notably one due to Shamir, yield arguments with cubic communication complexity (in the security parameter). More recent methods, based on the MPC-in-the-head technique, also produce arguments with cubic communication complexity. We improve this approach by using a secret-sharing over small integers (rather than modulo q) to reduce the size of the arguments and remove the prime modulus restriction. Since this sharing may reveal information on the secret subset, we introduce the idea of rejection to the MPC-in-the- head paradigm. Special care has to be taken to balance completeness and soundness and preserve zero-knowledge of our arguments. We combine this idea with two techniques to prove that the secret vector (which selects the subset) is well made of binary coordinates. Our new protocols achieve an asymptotic improvement by producing arguments of quadratic size. This improvement is also practical: for a 256-bit modulus q, the best variant of our protocols yields 13 KB arguments while previous proposals gave 1180 KB arguments, for the best general protocol, and 122 KB, for the best protocol restricted to prime modulus. Our techniques can also be applied to vectorial variants of the subset sum problem and in particular the inhomogeneous short integer solution (ISIS) problem for which they provide an efficient alternative to state-of-the-art protocols when the underlying ring is not small and NTT-friendly. We also show the application of our protocol to build efficient zero-knowledge arguments of plaintext and/or key knowledge in the context of fully-homomorphic encryption. When applied to the TFHE scheme, the obtained arguments are more than 20 times smaller than those obtained with previous protocols. Eventually, we use our technique to construct an efficient digital signature scheme based on a pseudorandom function due to Boneh, Halevi, and Howgrave-Graham.

**Computing groups of Hecke characters** . In [35], we describe algorithms to represent and compute groups of Hecke characters. We make use of an idèlic point of view and obtain the whole family of such characters, including transcendental ones. We also show how to isolate the algebraic characters, which are of particular interest in number theory. This work has been implemented in Pari/GP, and we illustrate our work with a variety of explicit examples using our implementation.

**Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms** .

Elliptic bases, introduced by Couveignes and Lercier in 2009, give an elegant way of representing finite field extensions. A natural question which seems to have been considered independently by several groups is to use this representation as a starting point for small characteristic finite field discrete logarithm algorithms. This idea has been recently proposed by two groups working on it, in order to achieve provable quasi-polynomial time for discrete logarithms in small characteristic finite fields. In this paper, we don't try to achieve a provable algorithm but, instead, investigate the practicality of heuristic

algorithms based on elliptic bases. In [26], our key idea, is to use a different model of the elliptic curve used for the elliptic basis that allows for a relatively simple adaptation of the techniques used with former Frobenius representation algorithms. We haven't performed any record computation with this new method but our experiments with the field F 3 1345 indicate that switching to elliptic representations might be possible with performances comparable to the current best practical methods.

## 8.5 Numerical Algebraic Geometry

**Functional norms, condition numbers and numerical algorithms in algebraic geometry** . In numerical linear algebra, a well-established practice is to choose a norm that exploits the structure of the problem at hand in order to optimize accuracy or computational complexity. In numerical polynomial algebra, a single norm (attributed to Weyl) dominates the literature. In [22], we initiates the use of $L_p$ norms for numerical algebraic geometry, with an emphasis on $L_\infty$. This classical idea yields strong improvements in the analysis of the number of steps performed by numerous iterative algorithms. In particular, we exhibit three algorithms where, despite the complexity of computing $L_\infty$-norm, the use of $L_p$-norms substantially reduces computational complexity: a subdivision-based algorithm in real algebraic geometry for computing the homology of semialgebraic sets, a well-known meshing algorithm in computational geometry, and the computation of zeros of systems of complex quadratic polynomials (a particular case of Smale's 17th problem).

**Condition Numbers for the Cube. I: Univariate Polynomials and Hypersurfaces** .

The condition-based complexity analysis framework is one of the gems of modern numerical algebraic geometry and theoretical computer science. One of the challenges that it poses is to expand the currently limited range of random polynomials that we can handle. Despite important recent progress, the available tools cannot handle random sparse polynomials and Gaussian polynomials, that is polynomials whose coefficients are i.i.d. Gaussian random variables. In [30], we initiate a condition-based complexity framework based on the norm of the cube that is a step in this direction. We present this framework for real hypersurfaces and univariate polynomials. We demonstrate its capabilities in two problems, under very mild probabilistic assumptions. On the one hand, we show that the average run-time of the Plantinga-Vegter algorithm is polynomial in the degree for random sparse (alas a restricted sparseness structure) polynomials and random Gaussian polynomials. On the other hand, we study the size of the subdivision tree for Descartes' solver and run-time of the solver by Jindal and Sagraloff (2017). In both cases, we provide a bound that is polynomial in the size of the input (size of the support plus logarithm of the degree) for not only on the average, but all higher moments. [This is the journal version of the conference paper with the same title.]

## 8.6 Miscancellanous

**Generalized Perron roots and solvability of the absolute value equation** . Let A be a real $(n \times n)$-matrix.

The piecewise linear equation system $z - A|z| = b$ is called an absolute value equation (AVE). It is well-known to be equivalent to the linear complementarity problem (LCP). For AVE and LCP unique solvability is comprehensively characterized in terms of conditions on the spectrum (AVE), resp., the principal minors (LCP) of the coefficient matrix. For mere solvability no such characterization exists. In [39], we close this gap in the theory on the AVE-side. The aligning spectrum of A consists of real eigenvalues of the matrices SA, where $S \in diag(+/-n)$, which have a corresponding eigenvector in the positive orthant of Rn. For the mapping degree of the piecewise linear function $z \to z - A|z|$ we prove, under some mild genericity assumptions on A: The degree is 1 if all aligning values are smaller than 1, it is 0 if all aligning values are larger than 1, and in general it is congruent to (k + 1) mod 2 if k aligning values are larger than 1. The modulus cannot be omitted because the degree can both increase and decrease.

**The Multivariate Schwartz–Zippel Lemma** .

Motivated by applications in combinatorial geometry, we consider the following question: Let $\lambda = (\lambda 1, \lambda 2, ..., \lambda m)$ be an $m$-partition of a positive integer $n$, $Si \subseteq C\lambda i$ be finite sets, and let $S := S1 \times S2 \times ... \times Sm \subset Cn$ be the multi-grid defined by Si. Suppose p is an n-variate degree d polynomial. How many zeros does p have on S? In [28], we first develop a multivariate generalization of the Combinatorial Nullstellensatz that certifies the existence of a point $t \in S$ so that $p(t) \neq 0$. Then, we show that a natural multivariate generaliza- tion of the DeMillo-Lipton-Schwartz-Zippel lemma holds, except for a special family of polynomials that we call $\lambda$-reducible. This yields a simultaneous generalization of Szemer 'edi-Trotter theorem and Schwartz-Zippel lemma into higher dimensions, and has applications in incidence geometry. Finally, we develop a symbolic algorithm that identifies certain $\lambda$-reducible polynomials. More precisely, our symbolic algorithm detects polynomials that include a cartesian product of hypersurfaces in their zero set. It is likely that using Chow forms the algorithm can be generalized to handle arbitrary $\lambda$-reducible polynomials, which we leave as an open problem.

**A Geometric Summation of the Geometric Series** . (read the paper [29], this is a one page contribution).

**Coherent presentations of monoids with a right-noetherian Garside family** .

In [24], we 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.

## 8.7 PhD thesis

**Computation of the $L_\infty$-norm of finite-dimensional linear systems** . In the thesis [43], we study the computation of the $L_\infty$-norm of finite-dimensional linear time-invariant systems. This problem is first reduced to the computation of the maximal $y$-projection of the real solutions $(x, y)$ of a bivariate polynomial equations system $\Sigma : \{P = 0, \frac{\partial P}{\partial x} = 0\}$, where $P \in Z[x, y]$. Then, we use standard computer algebra methods to solve this problem. In particular, we alternatively study a method based on rational univariate representations, a method based on root separation, and finally a method first based on the sign variation of the leading coefficients of a signed subresultant sequence (Sturm-Habicht) and on the identification of an isolating interval for the maximal $y$-projection of the real solutions of $\Sigma$. We then compute the worst-case bit complexity of each method and compare their theoretical behavior. We also implement each method in Maple and compare their practical behavior (average complexity). A generalization of the above algorithms is finally proposed to the case where the polynomial P also depends on a set of parameters $\alpha = [\alpha_1, ..., \alpha_d] \in R^d$. To do that, we solve the problem using the notion of the Cylindrical Algebraic Decomposition, well-known in algebraic geometry.

**The Mahler measure of a family of exact polynomials** . In the thesis [42], we investigate the sequence of Mahler measures of a family of bivariate regular exact polynomials, called $Pd := P0 \leq i + j \leq d x i y j$ , unbounded in both degree and the genus of the algebraic curve. We obtain a closed formula for the Mahler measure of Pd in termsof special values of the Bloch–Wigner dilogarithm. We approximate $m(Pd)$, for $1 \leq d \leq 1000$, with arbitrary precision using SageMath. Using 3 different methods we prove that the limitof the sequence of the Mahler measure of this family converges to $9/(2\pi^2)\zeta(3)$. Moreover, we compute the asymptotic expansion of the Mahler measure of Pd which implies that the rate of the convergence is $O(log(d)/d^2)$. We also prove a generalization of the theorem of the Boyd-Lawton which asserts that the multivariate Mahler measures can be approximated using the lower dimensional Mahler measures. Finally, we prove that the Mahler measure of Pd, for arbitrary d can be written as a linear combination of

L-functions associated with an odd primitive Dirichlet character. In addition, we compute explicitly the representation of the Mahler measure of Pd in terms of $L$-functions, for $1 \leq d \leq 6$.

**Structures géométriques et bords des espaces symétriques** . Dans [41], nous montrons des résultats de complétude et d'incomplétude de certaines variétés fermées portant une structure nil-affine plate, dite à rayons. Ces géométries à rayons apparaissent aux bords des espaces symétriques et dans des contextes variés comme la géométrie affine ou de contact. Nous montrons que les variétés incomplètes ont une développante qui revêt son image. Cela permet de montrer de nouveaux cas de la conjecture de Markus sur les variétés affines fermées à volume parallèle. Nous étudions ensuite les représentations du census de Falbel-Koseleff-Rouillier de groupes fondamentaux de 3-variétés dans le groupe des isométries du plan hyperbolique complexe. Nous proposons le calcul numérique de leurs ensembles limites et désignons ceux qui sont fractals et présentent donc expérimentalement la qualité d'être discret. Nous montrons que les représentations qui semble discrètes grâce à leur ensemble limite se factorisent la plupart du temps par un groupe d'un triangle hyperbolique complexe. Cela généralise un phénomène constaté par Deraux dans un cadre plus large et systématique.

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

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

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

  In particular, it covers our collaborative work with some of our partners, especially the Gamble Project-Team - Inria Nancy Grand Est.

- 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.

# 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 – 2022

  GALOP is a Young Researchers (JCJC) project with the purpose of extending the limits of the state-of-the-art algebraic tools in computer science, especially in stochastic games. It brings original and innovative algebraic tools, based on symbolic-numeric computing, that exploit the geometry and the structure and complement the state-of-the-art. We support our theoretical tools with a

highly efficient open-source software for solving polynomials. Using our algebraic tools we study the geometry of the central curve of (semi-definite) optimization problems. The algebraic tools and our results from the geometry of optimization pave the way to introduce algorithms and precise bounds for stochastic games.

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

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

  Participant: Yves Guiraud

  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.

# 11 Dissemination

## 11.1 Promoting scientific activities

### 11.1.1 Scientific events: selection

**Member of the conference program committees**

- Alban Quadrat co-organized with Eva Zerz the invited session *Algebraic and Geometric Approaches to Systems Structure and Control* at the 5th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2022), 12-16 September 2022, Bayreuth, Germany, and the invited session *Algebraic and symbolic methods for mathematical system theory* at the 8th IFAC Symposium on System Structure and Control (SSSC), September 27-30, Montreal, Canada, with Thomas Cluzeau.

- Pierre-Vincent Koseleff co-organized the *Journées Nationales de Calcul Formel*, Luminy, mars 2022 (JNCF2022).

- Pierre-Vincent Koseleff is a member of the Scientific Committee of the Journées Nationales de Calcul Formel (JNCF).

- Pierre-Vincent Koseleff is a Member of the organizing committee of the conference *Fondation of Computational Mathematics* (FoCM 2023).

- Martin Deraux and Fabrice Rouillier co-organized the meeting *Complex Hyperbolic Geometry and Related Topics / Autour de la géométrie hyperbolique complexe* at Centre International de Rencontres Mathématiques (CIRM), 4-8 July 2022, Luminy, France.

#### 11.1.2 Journal

**Member of the editorial boards**

- Elisha Falbel is a member of the editorial board of São Paulo Journal of Mathematical Sciences - Springer

- Antoine Joux is a member of the editorial board of Designs, Codes and Cryptography

- Alban Quadrat is an associate editor of *Multidimensional Systems; and Signal Processing*, Springer,

- Alban Quadrat is is an associate editor of *Maple Transactions*.

- Fabrice Rouillier is an associate editor of *Journal of Symbolic Computation*, Elsevier,

- Fabrice Rouillier is an associate editor of *Maple Transactions*.

#### 11.1.3 Invited talks

- Yves Guiraud gave a talk on *Collapsing schemes for differential graded algebras* at the Séminaire d'algèbre de l'Institut Camille Jordan, Saint-Étienne, November 2022.

- Antonin Guilloux gave an invited talk on *Slimness in the 3-sphere* at the conference *Complex Hyperbolic Geometry and Related Topics / Autour de la géométrie hyperbolique complexe* at Centre International de Rencontres Mathématiques (CIRM).

#### 11.1.4 Scientific expertise

- Yves Guiraud is an elected member of the Comité National de la Recherche Scientifique, section 41 (mathematics), 2021-2026. He is an appointed member of the section bureau.

- Yves Guiraud was an elected member of the Conseil scientifique of the department of mathematics of Univ. Paris Cité, 2019-2022.

- Alban Quadrat was a member of the Scientific Committee of the *Journées Nationales de Calcul Formel* (JNCF). He is also a member of the technical committee *Linear Systems* of the *International Federation of Automatic Control* (IFAC).

#### 11.1.5 Research administration

- Alban Quadrat was a member of the Conseil d'Administration of the *Société Mathématique de France* (SMF).
- Yves Guiraud is an elected member of the Conseil de laboratoire of IMJ-PRG, since 2021.

### 11.2 Teaching - Supervision - Juries

#### 11.2.1 Teaching

- Antonin Guilloux, 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 supervises the PhD of Thibauld Feneuil since 10/2020,
- Elias Tsigaridas supervises the PhD of Carles Checa, since 10/2020 (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 supervise the PhD of Christina Katsamaki, defense planned in early 2023.
- Yves Guiraud supervises, with Pierre-Louis Curien (CNRS, Univ. Paris Cité, IRIF) the PhD thesis of Alen Đurić. Defence is planned in March 2023
- 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)

- Yves Guiraud supervised, with Muriel Livernet (Univ. Paris Cité, IMJ-PRG) the research internship of Filipp Buryak (Ukrainian master student, hosted by Univ. Paris Cité), *On the classifying space of Artin monoids (after G. Paolini)*.
- Yves Guiraud supervised, with Emmanuel Wagner (Univ. Paris Cité, IMJ-PRG) the research internship of Antoine Bussy (M2 mathématiques fondamentales, Sorbonne Université), *Diagrammatics for Coxeter groups and their braid groups (after B. Elias and G. Williamson)*.
- Alban Quadrat supervised the Master thesis of Camille Pinto, *Towards an effective integro-differential elimination theory*, M2 Algèbre Appliquée, University of Paris Saclay.
- Pierre-Vincent Koseleff supervised Théophile Cartraud with J. -P. Marco, *Propriétés et relations entre signaux périodiques et attracteurs nodaux pour la reconstruction de dynamiques complexes*, M2 Mathematiques fondamentales, Sorbonne Université.
- Pierre Vicent Koseledd supervised Thibaut Misme *Générateurs de l'anneau des entiers d'extensions cyclotomiques réelles*, M2 Algèbre Appliquée, University of Paris Saclay.

#### 11.2.3 Juries

- Alban Quadrat was a referee of the PhD thesis of Alexandre Rigaud *Analyse des notions de stabilité pour les modèles 2D de Roesser et Fornasini-Marchesini*, University of Poitiers, December, 2022.
- Fabrice Rouillier was a referee of the PhD thesis of Owen Rouillé []
- Antonin Guilloux and Fabrice Rouillier where in the Jury of the PhD of Mahya Mehrabdollahei [42]
- Alban Quadrat en Fabrice Rouillier were in the jury of the PhD of Grace Younes (January 2022)
- Elisah Falbel, Antonin Guilloux and Fabrice Rouillier where in the Jury of the PhD of Raphaël Alexandre, June 2022 [41]

### 11.3 Popularization

- 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 est membre du Jury des Olympiades Nationales de Mathématiques

#### 11.3.1 Internal or external Inria responsibilities

- Yves Guiraud is an elected member of the Comité de centre of the INRIA Research Center of Paris, since 2019 (the committee is inactive since the COVID).

## 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. 'Generating Very Large RNS Bases'. In: *IEEE Transactions on Emerging Topics in Computing* (2022), pp. 1–12. DOI: 10.1109/TETC.2022.3187072. URL: https://hal.sorbonne-universite.fr/hal-03719386.

[19] J.-C. Bajard, J. Marrez, T. Plantard and P. Véron. 'On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$'. In: *Advances in Mathematics of Communications* (2022). DOI: 10.3934/amc.2022018. URL: https://hal.archives-ouvertes.fr/hal-03611829.

[20] R. Barbulescu and S. Shinde. 'A classification of ECM-friendly families using modular curves'. In: *Mathematics of Computation* 91 (2022), pp. 1405–1436. DOI: 10.1090/mcom/3697. URL: https://hal.science/hal-01822144.

[21] A. Chalkis, I. Z. Emiris, V. Fisikopoulos, P. Repouskos and E. Tsigaridas. 'Efficient sampling in spectrahedra and volume approximation'. In: *Linear Algebra and its Applications* 648 (1st Sept. 2022), pp. 205–232. DOI: 10.1016/j.laa.2022.04.002. URL: https://hal.inria.fr/hal-03659476.

[22] F. Cucker, A. A. Ergür and J. Tonelli-Cueto. 'Functional norms, condition numbers and numerical algorithms in algebraic geometry'. In: *Forum of Mathematics, Sigma* 10 (22nd Nov. 2022), e103. DOI: 10.1017/fms.2022.89. URL: https://hal.inria.fr/hal-03151436.

[23] F. Cucker, A. A. Ergür and J. Tonelli-Cueto. 'On the Complexity of the Plantinga-Vegter Algorithm'. In: *Discrete and Computational Geometry* (29th Aug. 2022). DOI: 10.1007/s00454-022-00403-x. URL: https://hal.inria.fr/hal-02552018.

[24] 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* (2022). URL: https://hal.archives-ouvertes.fr/hal-03276119.

[25] 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 (15th Feb. 2022), pp. 631–697. DOI: 10.1007/s00454-021-00353-w. URL: https://hal.inria.fr/hal-01891417.

[26] A. Joux and C. Pierrot. 'Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms'. In: *Advances in Mathematics of Communications* (2022). URL: https://hal.sorbonne-universite.fr/hal-02173688.

[27] C. Katsamaki, F. Rouillier, E. Tsigaridas and Z. Zafeirakopoulos. 'PTOPO: Computing the Geometry and the Topology of Parametric Curves'. In: *Journal of Symbolic Computation* (5th Aug. 2022). DOI: 10.1016/j.jsc.2022.08.012. URL: https://hal.archives-ouvertes.fr/hal-03090184.

[28] M. Levent Doğan, A. Ergür, J. Mundo and E. Tsigaridas. 'The Multivariate Schwartz–Zippel Lemma'. In: *SIAM Journal on Discrete Mathematics* 36.2 (June 2022), pp. 888–910. DOI: 10.1137/20M1333869. URL: https://hal.inria.fr/hal-03637826.

[29] J. Tonelli-Cueto. 'A Geometric Summation of the Geometric Series'. In: *The American Mathematical Monthly* (16th Sept. 2022), pp. 1–1. DOI: 10.1080/00029890.2022.2115825. URL: https://hal.inria.fr/hal-03779492.

[30] J. Tonelli-Cueto and E. Tsigaridas. 'Condition Numbers for the Cube. I: Univariate Polynomials and Hypersurfaces'. In: *Journal of Symbolic Computation* 115 (2022), pp. 142–173. DOI: 10.1016/j.jsc.2022.08.013. URL: https://hal.inria.fr/hal-03086875.

**International peer-reviewed conferences**

[31] A. Chalkis, C. Katsamaki and J. Tonelli-Cueto. 'On the Error of Random Sampling: Uniformly Distributed Random Points on Parametric Curves'. In: ISSAC '22 - International Symposium on Symbolic and Algebraic Computation. Villeneuve-d'Ascq, France, 5th July 2022. DOI: 10.1145/3476446.3536190. URL: https://hal.inria.fr/hal-03601563.

[32] C. Chenavier, T. Cluzeau and A. Quadrat. 'Computation of Koszul homology and application to involutivity of partial differential systems'. In: SSSC 2022 - 8th IFAC Symposium on System Structure and Control. Montréal, Canada, 30th Sept. 2022. URL: https://hal.inria.fr/hal-03908688.

[33] A. A. Ergür, J. Tonelli-Cueto and E. Tsigaridas. 'Beyond Worst-Case Analysis for Root Isolation Algorithms'. In: ISSAC '22 - International Symposium on Symbolic and Algebraic Computation. Villeneuve-d'Ascq, France, 5th July 2022. URL: https://hal.inria.fr/hal-03575449.

[34] T. Feneuil, J. Maire, M. Rivain and D. Vergnaud. 'Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection'. In: *Advances in Cryptology - Asiacrypt 2022*. ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13792. Lecture Notes in Computer Science. Taipei, Taiwan: Springer, 2022, pp. 1–32. DOI: 10.1007/978-3-031-22966-4_13. URL: https://hal.inria.fr/hal-03941457.

[35] P. Molin and A. Page. 'Computing groups of Hecke characters'. In: ANTS-XV 2022 - Fifteenth Algorithmic Number Theory Symposium. Bristol, United Kingdom, 13th Oct. 2022. URL: https://hal.inria.fr/hal-03795267.

[36] A. Quadrat. 'An integro-differential operator approach to linear differential systems'. In: MTNS 2022 - 25th International Symposium on Mathematical Theory of Networks and Systems. Bayreuth, Germany, 16th Sept. 2022. DOI: 10.1016/j.ifacol.2022.11.054. URL: https://hal.inria.fr/hal-03908541.

[37] A. Quadrat. 'An Integro-differential Operator Approach to Linear State-space Systems'. In: SSSC 2022 - 8th IFAC Symposium on System Structure and Control. Montreal, Canada, 30th Sept. 2022. DOI: 10.1016/j.ifacol.2022.11.299. URL: https://hal.inria.fr/hal-03908550.

[38] A. Quadrat. 'An Integro-differential-delay Operator Approach to Transformations of Linear Differential Time-delay Systems'. In: SSSC 2022 - 8th IFAC Symposium on System Structure and Control. Montréal, Canada, 30th Sept. 2022. DOI: 10.1016/j.ifacol.2022.11.301. URL: https://hal.inria.fr/hal-03908561.

[39] M. Radons and J. Tonelli-Cueto. 'Generalized Perron roots and solvability of the absolute value equation'. In: Discrete Mathematics Days 2022. Santander, Spain: Editorial Universidad de Cantabria, 4th July 2022, pp. 237–242. DOI: 10.22429/Euc2022.016. URL: https://hal.inria.fr/hal-03739462.

### Scientific book chapters

[40] A. Quadrat and R. Ushirobira. 'On the Ore extension ring of differential time-varying delay operators'. In: *Accounting for Constraints in Delay Systems, Advances in Delays and Dynamics (ADD), volume 12, Springer, pp. 87-107*. Vol. ADD-2. Advances in Delays and Dynamics. Springer, 3rd Apr. 2022, pp. 87–107. DOI: 10.1007/978-3-030-89014-8_5. URL: https://hal.inria.fr/hal-03908643.

### Doctoral dissertations and habilitation theses

[41] R. V. Alexandre. 'Geometric structures and boundaries of symmetric spaces'. Sorbonne Université, 20th June 2022. URL: https://theses.hal.science/tel-03779876.

[42] M. Mehrabdollahei. 'The Mahler measure of a family of exact polynomials'. Sorbonne Université, 6th July 2022. URL: https://theses.hal.science/tel-03928278.

[43] G. Younes. 'Computation of the L∞-norm of finite-dimensional linear systems'. Sorbonne Université, 20th Jan. 2022. URL: https://theses.hal.science/tel-03863650.

### Reports & preprints

[44] F. Brunault, A. Guilloux, M. Mehrabdollahei and R. Pengo. *Limits of Mahler measures in multiple variables*. 22nd Mar. 2022. URL: https://hal.sorbonne-universite.fr/hal-03615999.

[45] E. Falbel, A. Guilloux and P. Will. *Slim curves, limit sets and spherical CR uniformisations*. 19th May 2022. URL: https://hal.science/hal-03673101.

[46] K. Kozhasov and J. Tonelli-Cueto. *Probabilistic bounds on best rank-one approximation ratio*. 7th Jan. 2022. URL: https://hal.inria.fr/hal-03517267.

[47] M. Radons and J. Tonelli-Cueto. *Generalized Perron Roots and Solvability of the Absolute Value Equation*. 20th June 2022. URL: https://hal.inria.fr/hal-03738197.

[48] J. Tonelli-Cueto. *A p-adic Descartes solver: the Strassman solver*. 15th Mar. 2022. URL: https://hal.inria.fr/hal-03609363.

**Other scientific publications**

[49] J. G. Suchen and J. Tonelli-Cueto. 'Ultrametric Smale's $\alpha$-theory'. In: International Symposium on Symbolic and Algebraic Computation. Vol. 56. 2. Lille, France, June 2022, pp. 56–59. DOI: 10.1145/3572867.3572875. URL: https://hal.inria.fr/hal-03738191.

## 12.3 Cited publications

[50] 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.

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

[52] 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.

[53] 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.

[54] 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.

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

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

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

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

[77] 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).

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

[79] 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.

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

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

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

[83] 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.

[84] 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.

[85] 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.

[86] 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.

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

[88] 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.

[89] 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.

[90] 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.

[91] 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.

[92] 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.

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

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

[95] 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.

[96] 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.

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

[98] 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.

[99] 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.

[100] 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.

[101] 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.

[102] 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.

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

[104] 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.

[105] 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.

[106] 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.

[107] 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.

[108] 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.

[109] 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.

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

[111] 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.

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

[113] 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.

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

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

[116] 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.

[117] 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.

[118] 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.

[119] 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.

[120] 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.

[121] 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.

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

[123] 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.

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

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

[126] 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.

[127] 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.

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

[129] 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.

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

[131] 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.

[132] 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.

[133] 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.

[134] 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.

[135] 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.

[136] 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.

[137] 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.

[138] 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.

[139] 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.

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

[141] G. Rance, Y. Bouzidi, A. Quadrat, A. Quadrat and F. Rouillier. 'Explicit H∞ controllers for 4th order single-input single-output systems with parameters and their applications to the two mass-spring system with damping'. In: *IFAC 2017 Workshop Congress*. Toulouse, France, July 2017. URL: https://hal.inria.fr/hal-01667368.

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

[143] 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.

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

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

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

[147] 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.

[148] 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.

[149] 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.

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

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