RESEARCH CENTRE

Paris

IN PARTNERSHIP WITH:

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

2021
ACTIVITY REPORT

Project-Team
OURAGAN

Tools for resolutions in algebra, geometry and their applications

IN COLLABORATION WITH: Institut de Mathématiques de Jussieu

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team OURAGAN 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 Limit sets . . . 14
- 6.2 Hecke Grossencharacters . . . 15
- 6.3 Parallel mechanisms . . . 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

8 New results 16
- 8.1 Number Theory . . . 16
  - 8.1.1 A classification of ECM-friendly families using modular curves . . . 16
  - 8.1.2 Montgomery-friendly primes and applications to cryptography . . . 17
  - 8.1.3 Generating Residue Number System Bases . . . 17
- 8.2 Computer Algebra . . . 17
  - 8.2.1 Computation of the L-infinity norm of finite-dimensional linear systems . . . 17
  - 8.2.2 Computing the Homology of Semialgebraic Sets. II: General formulas . . . 17
  - 8.2.3 Koszul-type determinantal formulas for families of mixed multilinear systems . . . 17
  - 8.2.4 Multilinear Polynomial Systems: Root Isolation and Bit Complexity . . . 18
  - 8.2.5 Sampling the feasible sets of SDPs and volume approximation . . . 18
  - 8.2.6 Geometric algorithms for sampling the flux space of metabolic networks . . . 18
- 8.3 Algebraic Analysis . . . 19
  - 8.3.1 On the inverse Cauchy problem for linear ordinary differential equations . . . 19
- 8.4 Geometry . . . 19

8.4.1 Cartan connections and path structures with large automorphism groups 19
8.4.2 Geometric structures and configurations of flags in orbits of real forms 19
8.4.3 Volume function and Mahler measure of exact polynomials 19
8.5 Control Theory 19
8.5.1 Centrohermitian solutions of a factorization problem arising in vibration analysis. Part I: Lee's transformation 19
8.5.2 Centrohermitian Solutions of a Factorization Problem Arising in Vibration Analysis. Part II: A Coninvolutory Matrix Approach 20
8.6 Algebraic aspects of a rank factorization problem arising in vibration analysis 20

9 Bilateral contracts and grants with industry **20**
9.1 Bilateral contracts with industry 20

10 Partnerships and cooperations **20**
10.1 International initiatives 20
10.1.1 Inria associate team not involved in an IIL or an international program 20
10.1.2 Participation in other International Programs 21
10.2 National initiatives 21
10.2.1 ANR 21
10.2.2 Inria Exploratory actions 21

11 Dissemination **22**
11.1 Promoting scientific activities 22
11.1.1 Scientific events: selection 22
11.1.2 Journal 22
11.1.3 Invited talks 22
11.1.4 Leadership within the scientific community 23
11.1.5 Scientific expertise 23
11.1.6 Research administration 23
11.2 Teaching - Supervision - Juries 23
11.2.1 Teaching 23
11.2.2 Supervision 23
11.2.3 Juries 24
11.3 Popularization 24
11.3.1 Internal or external Inria responsibilities 24

12 Scientific production **24**
12.1 Major publications 24
12.2 Publications of the year 25
12.3 Other 27
12.4 Cited publications 27

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]
- Mahya Mehrabdollahei [Sorbonne Université, Researcher, from Sep 2021]
- Alban Quadrat [Inria, Senior Researcher, HDR]
- Elias Tsigaridas [Inria, Researcher]

Faculty Members

- Jean Bajard [Sorbonne Université, Professor, HDR]
- Martin Deraux [Université Grenoble Alpes, Associate Professor, from Sep 2021]
- Elisha Falbel [Sorbonne Université, Professor, HDR]
- Antonin Guilloux [Sorbonne Université, Associate Professor, HDR]
- Antoine Joux [Sorbonne Université, Associate Professor, Location : CISPA Helmholtz Center, HDR]
- Pierre-Vincent Koseleff [Sorbonne Université, Associate Professor, HDR]
- Pascal Molin [Université de Paris, Associate Professor]

Post-Doctoral Fellow

- Josue Tonelli Cueto [Inria]

PhD Students

- Raphael Alexandre [Sorbonne Université]
- Thibauld Feneuil [CryptoExperts, CIFRE]
- Christina Katsamaki [Inria]
- Mahya Mehrabdollahei [Inria, until Aug 2021]
- Grace Younes [Inria]

Interns and Apprentices

- Thi Thu Quyen Nguyen [Inria, from Apr 2021 until Jul 2021]
- Maya Saab Chartouni [Inria, from Apr 2021 until Jul 2021]

Administrative Assistant

- Laurence Bourcier [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 [70], subresultants [91], critical point methods [47], etc.) which are also deeply used in our developments. Second, for a selection of well-known problems, we propose different computational strategies (for example the use of approximate arithmetic to speed up LLL algorithm or root isolators, still certifying the final result). Last, we propose specialized variants of known algorithms optimized for a given problem (for example, dedicated solvers for degenerated bivariate polynomials to be used in the computation of the topology of plane curves).

In the activity of OURAGAN, many key objects or algorithms around the resolution of algebraic systems are developed or optimized within the team, such as the resolution of polynomials in one variable with real coefficients [110] [17], rational parameterizations of solutions of zero-dimensional systems with rational coefficients [56] [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 [105] (for example to make progress on the computation of class groups in number fields [92]), network reductions by means of LLL variants [81] and, obviously, various computations in linear algebra, for example dedicated to *almost sparse* matrices [106].

For the algorithmic approach to algebraic analysis of functional equations [51] [108] [109], we developed the effective study of both module theory and homological algebra [142] over certain non-commutative polynomial rings of functional operators [4], of Stafford's famous theorems on the Weyl algebras [133], of the equidimensional decomposition of functional systems [129], etc.

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

2.1.2 Computational Number Theory

Many frontiers between computable objects, algorithms (above section), computational number theory and applications, especially in cryptography are porous. However, one can classify our work in 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 [77], where they proposed a first instantiation of their paradigm based on the discrete logarithm problem in prime fields. The invention of RSA [140], based on the hardness of factoring came as a second example. The introduction of discrete logarithms on elliptic curves [111] [144] only confirmed this trend.

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

- the elliptic curve method (ECM) [122]
- the quadratic field for factoring [126] and its variant for discrete log called the Gaussian integers method [119]
- the number field sieve (NFS) [121]

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

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

Members of OURAGAN started working on the topic of discrete logarithms around 1998, with several computation records that were announced on the *NMBRTHRY* mailing list. In large characteristic, especially for the case of prime fields, the best current method is the number field sieve (NFS) algorithm. In particular, they published the first NFS based record computation[13]. Despite huge practical improvements, the prime field case algorithm hasn't really changed since that first record. Around the same time, we also presented small characteristic computation record based on simplifications of the Function Field Sieve (FFS) algorithm [104].

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

Starting from 2012, new results appeared in small characteristic. Initially based on a simplification of the 2006 result, they quickly blossomed into the Frobenial representation methods, with quasi-polynomial time complexity [105, 93].

An interesting side-effect of this research was the need to revisit the key sizes of pairing-based cryptography. This type of cryptography is also a topic of interest for OURAGAN. In particular, it was introduced in 2000 [12].

The computations of *class groups in number fields* 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 [92], but many issues remain open.

Computing generators of principal ideals of cyclotomic fields is also strongly related to the computation of class groups in number fields. Ideals in cyclotomic fields are used in a number of recent public-key cryptosystems. Among the difficult problems that ensure the safety of these systems, there is one that consists in finding a small generator, if it exists, of an ideal. The case of cyclotomic fields is considered [50].

2.1.3 Topology in small dimension

Character varieties There is a tradition of using computations and software to study and understand the topology of small dimensional manifolds, going back at least to Thurston's works (and before him, Riley's pioneering work). The underlying philosophy of these tools is to build combinatorial models of manifolds (for example, the torus is often described as a square with an identification of the sides). For dimensions 2, 3 and 4, this approach is relevant and effective. In the team OURAGAN, we focus on the dimension 3, where the manifolds are modelized by a finite number of tetrahedra with identification of the faces. The software SnapPy [10] implements this strategy [146] and is regularly used as a starting point in our work. Along the same philosophy of implementation, we can also cite Regina [11]. A specific trait of SnapPy is that it focuses on hyperbolic structures on the 3-dimensional manifolds. This setting is the object of a huge amount of theoretical work that were used to speed up computations. For example, some Newton methods were implemented without certification for solving a system of equations, but the theoretical knowledge of the uniqueness of the solution made this implementation efficient enough for the target applications. In recent years, in part under the influence of our team [12], more attention has been given to certified computations (at least with an error control) and now this is implemented in SnapPy.

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

[49] [7] that have strictly no chance to be solved by blindly running the most powerful black boxes: we usually deal here with systems that have 24 to 64 variables, depend on 4 to 8 parameters and with degrees exceeding 10 in each variable. With an ANR [14] funding on the subject, the progress that we did [85] were (much) more significant than expected. In particular, we have introduced new computable objects with an immediate theoretical meaning (let us say rather with a theoretical link established with the usual objects of the domain), namely, the so-called *deformation variety*.

Knot theory Knot theory is a wide area of mathematics. We are interested in polynomial representations of long knots, that is to say polynomial embeddings $\mathbf{R} \to \mathbf{R}^3 \subset \mathbf{S}^3$. Every knot admits a polynomial representation and a natural question is to determine explicit parameterizations, minimal degree parameterizations. On the other hand we are interested to determine what is the knot of a given polynomial smooth embedding $\mathbf{R} \to \mathbf{R}^3$. These questions involve real algebraic curves. This subject was first considered by Vassiliev in the 90's[145].

A Chebyshev knot [113], is a polynomial knot parameterized by a Chebyshev curve $(T_a(t), T_b(t), T_c(t+\varphi))$ where $T_n(t) = \cos(n \arccos t)$ is the n-th Chebyshev polynomial of the first kind. Chebyshev knots are polynomial analogues of Lissajous knots that have been studied by Jones, Hoste, Lamm... It was first established that any knot can be parameterized by Chebyshev polynomials, then we have studied the properties of harmonic nodes [114] which then opened the way to effective computations.

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

Two-bridge knots (or rational knots) are particularly studied because they are much easier to study. The first 26 knots (except 8_5) are two-bridge knots. We were able to give an exhaustive, minimal and certified list of Chebyshev parameterizations of the first rational two-bridge knots, using blind computations [116]. On the other hand, we propose the identification of Chebyshev knot diagrams [117] by developing new certified algorithms for computing trigonometric expressions [118]. These works share many tools with our action in visualization and computational geometry.

We made use of Chebyshev polynomials so as Fibonacci polynomials which are families of orthogonal polynomials. Considering the Alexander-Conway polynomials as continuant polynomials in the Fibonacci basis, we were able to give a partial answer to Hoste's conjecture on the roots of Alexander polynomials of alternating knots ([115]).

We study the lexicographic degree of the two-bridge knots, that is to say the minimal (multi)degree of a polynomial representation of a N-crossing two-bridge knot. We show that this degree is $(3, b, c)$ with $b + c = 3N$. We have determined the lexicographic degree of the first 362 first two-bridge knots with 12 crossings or fewer [63] [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 [62], the slide isotopies on trigonal diagrams, namely those that never increase the number of crossings [64].

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 [69], 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 [56, 110, 57, 58] which are basic engines for computing the topology [124, 76] and / or plotting.

2.1.4 Algebraic analysis of functional systems

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

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

Complementary approaches, based on algebraic methods, are usually upstream or help the numerical simulation of systems of functional systems. These methods also tackle a different range of questions and problems such as algebraic preconditioning, elimination and simplification, completion to formal integrability or involution, computation of integrability conditions and compatibility conditions, index reduction, reduction of variables, choice of adapted coordinate systems based on symmetries, computation of first integrals of motion, conservation laws and Lax pairs, Liouville integrability, study of the (asymptotic) behavior of solutions at a singularity, etc. Although not yet very popular in applied mathematics, these theories have lengthy been studied in fundamental mathematics and were developed by Lie, Cartan, Janet, Ritt, Kolchin, Spencer, etc. [100] [108] [109] [112] [139] [127].

Over the past years, certain of these algebraic approaches to functional systems have been investigated within an algorithmic viewpoint, mostly driven by applications to engineering sciences such as mathematical systems theory and control theory. We have played a role towards these effective developments, especially in the direction of an algorithmic approach to the so-called *algebraic analysis* [108, 109, 51], 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 [100, 68, 141], differential algebra [53] [82], Spencer's theory [127], etc.), in [4, 5], we have initiated such a computational algebraic analysis approach for general classes of functional systems (and not only for holonomic systems as done in the literature of computer algebra [68]). Based on the effective aspects to algebraic analysis approach, the parametrizability problem [4], the reduction and (Serre) decomposition problems [5], the equidimensional decomposition [129], Stafford's famous theorems for the Weyl algebras [133], etc., have been studied and solutions have been implemented in `Maple`, `Mathematica`, and `GAP` [67][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 [76, 120, 57] 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 [80] have used them to provide some fast sophisticated factoring algorithms. As a consequence, it is natural to include these objects in our research directions.

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

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

3.3 Topology in small dimension

Character varieties The brute force approach to computable objects from topology of small dimension will not allow any significant progress. As explained above, the systems that arise from these problems are simply outside the range of doable computations. We still continue the work in this direction by a four-fold approach, with all three directions deeply inter-related. First, we focus on a couple of especially meaningful (for the applications) cases, in particular the 3-dimensional manifold called Whitehead link complement. At this point, we are able to make steps in the computation and describe part of the solutions [85, 97]; we hope to be able to complete the computation using every piece of information to simplify the system. Second, we continue the theoretical work to understand more properties of these systems [83]. These properties may prove how useful for the mathematical understanding is the resolution of such systems - or at least the extraction of meaningful information. This approach is for example carried on by Falbel and his work on configuration of flags [86, 88]. Third, we position ourselves as experts in the know-how of this kind of computations and natural interlocutors for colleagues coming up with a question on such a computable object (see [95] and [97]). This also allows us to push forward the kind of computation we actually do and make progress in the direction of the second point. We are credible interlocutors because our team has the blend of theoretical knowledge and computational capabilities that grants effective resolutions of the problems we are presented. And last, we use the knowledge already acquired to pursue our theoretical study of the CR-spherical geometry [75, 87, 84].

Another direction of work is the help to the community in experimental mathematics on new objects. It involves downsizing the system we are looking at (for example by going back to systems coming from hyperbolic geometry and not CR-spherical geometry) and get the most out of what we can compute, by studying new objects. An example of this research direction is the work of Guilloux around the volume function on deformation varieties. This is a real-analytic function defined on the varieties we specialized in computing. Being able to do effective computations with this function led first to a conjecture [94]. Then, theoretical discussions around this conjecture led to a paper on a new approach to the Mahler measure of some 2-variables polynomials [96]. In turn, this last paper gave a formula for the Mahler measure in terms of a function akin to the volume function applied at points in an algebraic variety whose moduli of coordinates are 1. The OURAGAN team has the expertise to compute all the objects appearing in this formula, opening the way to another area of application. This area is deeply linked with number theory as well as topology of small dimension. It requires all the tools at disposition within OURAGAN.

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

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

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 [142] which play important roles in algebraic analysis [51, 108, 109] and in the algorithmic study of linear functional systems. In particular, we shall focus on linear systems of integro-differential-constant/varying/distributed delay equations [128, 132] which play an important role in mathematical systems theory, control theory, and signal processing [128, 138, 131, 134].

The rings of integro-differential operators are highly more complicated than the purely differential case (i.e. Weyl algebras) [15], due to the existence of zero-divisors, or the fact of having a coherent ring instead of a noetherian ring [48]. Therefore, we want to develop an algorithmic study of these rings. Following the direction initiated in [132] for the computation of zero divisors (based on the polynomial null spaces of certain operators), we first want to develop algorithms for the computation of left/right

[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 [143], algorithmically developed in [15] for rings of partial differential operators (i.e. the Weyl algebras), are known to still hold for rings of integro-differential operators. We shall study their algorithmic extensions. Our corresponding implementation will be extended accordingly.

Finally, within a computer algebra viewpoint, we shall continue to algorithmically study issues on rings of integro-differential-delay operators [128, 131] and their applications to the study of equivalences of differential constant/varying/distributed delay systems (e.g. Artstein's reduction, Fiagbedzi-Pearson's transformation) which play an important role in control theory.

4 Application domains

4.1 Security of cryptographic systems

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

The cryptographic community is currently very actively assessing the threat coming for the development of quantum computers. Indeed, such computers would permit tremendous progress on many number theoretic problems such as factoring or discrete logarithm computations and would put the security of current cryptosystem under a major risk. For this reason, there is a large global research effort dedicated to finding alternative methods of securing data. For example, the US standardization agency called NIST has recently launched a standardization process around this issue. In this context, OURAGAN is part of the competition and has submitted a candidate (which has not been selected) [46]. This method is based on number-theoretic ideas involving a new presumably difficult problem concerning the Hamming distance of integers modulo large numbers of Mersenne.

4.2 Robotics

Algebraic computations have tremendously been used in Robotics, especially in kinematics, since the last quarter of the 20th century [99]. For example, one can find algebraic proofs for the 40 possible solutions to the direct kinematics problem [123] for steward platforms and companion experiments based on Gröbner basis computations [89]. On the one hand, hard general kinematics problems involve too many variables for pure algebraic methods to be used in place of existing numerical or semi-numerical methods everywhere and everytime, and on the other hand, global algebraic studies allow to propose exhaustive classifications that cannot be reached by other methods,for some quite large classes.

Robotics is a long-standing collaborative work with LS2N (Laboratory of Numerical Sciences of Nantes). Work has recently focused on the offline study of mechanisms, mostly parallel, their singularities or at least some types of singularities (cuspidals robots [147]).

For most parallel or serial manipulators, pose variables and joints variables are linked by algebraic equations and thus lie an algebraic variety. The two-kinematics problems (the direct kinematics problem - DKP- and the inverse kinematics problem - IKP) consist in studying the preimage of the projection of this algebraic variety onto a subset of unknowns. Solving the DKP remains to computing the possible positions for a given set of joint variables values while solving the IKP remains to computing the possible joints variables values for a given position. Algebraic methods have been deeply used in several situations for studying parallel and serial mechanisms, but finally their use stays quite confidential in the design process. Cylindrical Algebraic Decomposition coupled with variable's eliminations by means of Gröbner based computations can be used to model the workspace, the joint space and the computation of singularities. On the one hand, such methods suffer immediately when increasing the number of parameters or when working with imprecise data. On the other hand, when the problem can be handled, they might provide full and exhaustive classifications. The tools we use in that context [66, 65, 101, 103, 102] depend mainly on the resolution of parameter-based systems and therefore of study-dependent curves or flat algebraic surfaces (2 or 3 parameters), thus joining our thematic *Computational Geometry*.

4.3 Control theory

Certain problems studied in mathematical systems theory and control theory can be better understood and finely studied by means of algebraic structures and methods. Hence, the rich interplay between algebra, computer algebra, and control theory has a long history.

For instance, the first main paper on Gröbner bases written by their creators, Buchberger, was published in Bose's book [52] on control theory of multidimensional systems. Moreover, the differential algebra approach to nonlinear control theory (see [79, 78] and the references therein) was a major motivation for the algorithmic study of differential algebra [53, 82]. Finally, the behaviour approach to linear systems theory [148, 125] advocates for an algorithmic study of algebraic analysis (see Section 2.1.4). More generally, control theory is porous to computer algebra since one finds algebraic criteria of all kinds in the literature even if the control theory community has a very few knowledge in computer algebra.

OURAGAN has a strong interest in the computer algebra aspects of mathematical systems theory and control theory related to both functional and polynomial systems, particularly in the direction of robust stability analysis and robust stabilization problems for multidimensional systems [52, 125] and infinite-dimensional systems [72] (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 [107]. While extending those tests to multidimensional systems or differential time-delay systems, one had to tackle multivariate problems recursively with respect to the variables [52]. 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 [59, 60, 61]. 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 [54, 60, 61] 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 [58, 57].

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 [55, 130, 136, 135, 137, 138].

4.4 Signal processing

Due to numerous applications (e.g. sensor network, mobile robots), sources and sensors localization has intensively been studied in the literature of signal processing. The *anchor position self calibration problem* is a well-known problem which consists in estimating the positions of both the moving sources and a set of fixed sensors (anchors) when only the distance information between the points from the different sets is available. The position self-calibration problem is a particular case of the *Multidimensional Unfolding* (MDU) problem for the Euclidean space of dimension 3. In the signal processing literature, this problem is attacked by means of optimization problems (see [71] 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 [73] 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 [74]. This result advocates for the study of other localization problems based on the computational polynomial techniques developed in OURAGAN.

In collaboration with *Safran Tech* (Barau, Hubert) and Dagher (Inria Chile), a symbolic-numeric study of the new *multi-carrier demodulation method* [98] has recently been initiated. *Gear fault diagnosis* is an important issue in aeronautics industry since a damage in a gearbox, which is not detected in time, can have dramatic effects on the safety of a plane. Since the vibrations of a spur gear can be modeled as a product of two periodic functions related to the gearbox kinematic, it is proposed to recover each function from the global signal by means of an optimal reconstruction problem which, based on Fourier analysis, can be rewritten as $\mathrm{argmin}_{u\in\mathbb{C}^n, v_1, v_2\in\mathbb{C}^m} \parallel M - u\, v_1^\star - D\, u\, v_2^\star \parallel_F$, 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), $\parallel \cdot \parallel_F$ is the Frobenius norm, and $v^\star$ is the Hermitian transpose of v. We have recently obtained closed-form solutions for the exact problem, i.e., $M = u\, v_1^\star + D\, u\, v_2^\star$, which is a polynomial system with parameters. This first result gives interesting new insides for the study of the non-exact case, i.e. for the above optimization problem.

Our expertise on *algebraic parameter estimation problem*, developed in the former NON-A project-team (Inria Lille), will be further developed. Following this work [90], the problem consists in estimating a set θ of parameters of a signal $x(\theta, t)$ – which satisfies a certain dynamics – when the signal $y(t) = x(\theta, t) + \gamma(t) + \varpi(t)$ is observed, where γ denotes a structured perturbation and ϖ a noise. It has been shown that θ can sometimes be explicitly determined by means of closed-form expressions using iterated integrals of y. These integrals are used to filter the noise ϖ. Based on a combination of algebraic analysis techniques (rings of differential operators), differential elimination theory (Gröbner basis techniques for Weyl algebras), and operational calculus (Laplace transform, convolution), an algorithmic approach to algebraic parameter estimation problem has been initiated in [131] for a particular type of structured perturbations (i.e. bias) and was implemented in the `Maple` prototype `NonA`. The case of a general structured perturbation is still lacking.

5 Social and environmental responsibility

We have set a machine for a collective use and implementing as virtual machines a server for computations, another for visio-conferencing and a last one for website.

The advantages of such a strategy is to avoid to buy costly laptops for difficult computations but also to dynamically set the power of each virtual machine depending on the use. For example, we give more power to the virtual machine for visio-conferences when needed and give back this power to the server for computations the rest of the time.

6 Highlights of the year

6.1 Limit sets

Limit sets in the 3-dimensional sphere are a general generalization of the well-known fractal sets in the plane given by the complex dynamic, a.k.a Julia and Mandelbrot sets. The efficient computation and rendering of the latter has been a powerful drive for their theoretical and algorithmic study and can now be considered as achieved (real time rendering, arbitrary precision...). However, passing to dimension 3 is a challenge and is yet at its first steps. The website limit-sets.imj-prg.fr presents the first result of an effort leaded by R. Alexandre and A. Guilloux to compute and render such limit sets. Though still experimental, they are already used for improving the theoretical understanding of these limit sets. Moreover, one can hope that their visual attractiveness helps attract interest for this fields of research.

6.2 Hecke Grossencharacters

A collaboration between Pascal Molin and Aurel Page (Inria Bordeaux, Lfant team) recently added to the Pari/GP number theory software the support of Hecke Grossencharacters. These objects have been mathematically understood from the 1950s and establish explicit links between remote parts of number theory (algebraic curves, galois representations, L functions). Despite their immense computational interest, there has been no computer implementation until a partial Magma package in 2015. This is due to the fact that these characters are defined on infinite spaces which cannot be represented on a computer. The algorithm introduced by Molin and Page is the first to give access to the full family of Hecke characters, with routine interfaces to Pari/GP.

6.3 Parallel mechanisms

In 2021, we did sign a contract with Safran Technologies and Defense and the CNRS Laboratory LS2B (Nantes) for working on the design of parallel manipulators. After few months it has been decided that this contrat will be extended 3 years more at least and a co-dupervised PhD will start on the subject in January 2022.

7 New software and platforms

A new developement in 2021 : PTOPO - a Maple package for the study of the Topology of Parametric Algebraic Curves.

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

No new platforms.

8 New results

8.1 Number Theory

8.1.1 A classification of ECM-friendly families using modular curves

In [19], 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.

8.1.2 Montgomery-friendly primes and applications to cryptography

The paper [18] deals with Montgomery-friendly primes designed for the modular reduction algorithm of Montgomery. These numbers are scattered in the literature and their properties are partially exploited. We exhibit a large family of Montgomery-friendly primes which give rise to efficient modular reduction algorithms. We develop two main uses. The first one is dedicated directly to cryptography, in particular for isogeny based approaches and more generally to Elliptic Curves Cryptography. We suggest more appropriate finite fields and curves in terms of complexity for the recommended security levels, for both isogeny-based cryptography and ECC. The second use is purely arithmetic, and we propose families of alternative RNS bases. We show that, for dedicated architectures with word operators, we can reach, for a same or better complexity, larger RNS bases with Montgomery-friendly pair-wise co-primes than the RNS bases generally used in the literature with Pseudo-Mersenne numbers. This is particularly interesting for modular arithmetic used in cryptography.

8.1.3 Generating Residue Number System Bases

Residue number systems provide efficient techniques for speeding up calculations and/or protecting against side channel attacks when used in the context of cryptographic engineering. One of the interests of such systems is their scalability, as the existence of large bases for some specialized systems is often an open question. In [29], we present highly optimized methods for generating large bases for residue number systems and, in some cases, the largest possible bases. We show their efficiency by demonstrating their improvement over the state-of-the-art bases reported in the literature. This work make it possible to address the problem of the scalability issue of finding new bases for a specific system that arises whenever a parameter changes, and possibly open new application avenues.

8.2 Computer Algebra

8.2.1 Computation of the L-infinity norm of finite-dimensional linear systems

In [22], we study the problem of computing the $\mathscr{L}_\infty$ norm of finite-dimensional linear time-invariant systems. This problem is first reduced to the computation of the maximal x-projection of the real solutions (x, y) of a bivariate polynomial system $\Sigma = \{P, \frac{\partial P}{\partial y}\}$, with $P \in \mathbb{Q}[x, y]$. Then, we use standard computer algebra methods to solve the problem. In this paper, 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 the signed subresultant sequence and then based on the identification of an isolating interval for the maximal x-projection of the real solutions of Σ.

8.2.2 Computing the Homology of Semialgebraic Sets. II: General formulas

In [23], we describe and analyze a numerical algorithm for computing the homology (Betti numbers and torsion coefficients) of semialgebraic sets given by Boolean formulas. The algorithm works in weak exponential time. This means that outside a subset of data having exponentially small measure, the cost of the algorithm is single exponential in the size of the data. This extends the work in Part I to arbitrary semialgebraic sets. All previous algorithms proposed for this problem have doubly exponential complexity.

8.2.3 Koszul-type determinantal formulas for families of mixed multilinear systems

Effective computation of resultants is a central problem in elimination theory and polynomial system solving. Commonly, we compute the resultant as a quotient of determinants of matrices and we say that there exists a determinantal formula when we can express it as a determinant of a matrix whose elements are the coefficients of the input polynomials. In [20], we study the resultant in the context of mixed multilinear polynomial systems, that is multilinear systems with polynomials having different supports, on which determinantal formulas were not known. We construct determinantal formulas for two kind of multilinear systems related to the Multiparameter Eigenvalue Problem (MEP): first, when the polynomials agree in all but one block of variables; second, when the polynomials are bilinear with different supports, related to a bipartite graph. We use the Weyman complex to construct Koszul-type determinantal formulas that generalize Sylvester-type formulas. We can use the matrices associated to these formulas to solve square systems without computing the resultant. The combination of the resultant matrices with the eigenvalue and eigenvector criterion for polynomial systems leads to a new approach for solving MEP.

8.2.4 Multilinear Polynomial Systems: Root Isolation and Bit Complexity

In [25], we exploit structure in polynomial system solving by considering polyno-mials that are linear in subsets of the variables. We focus on algorithms and their Boolean complexity for computing isolating hyperboxes for all the isolated complex roots of well-constrained, unmixed systems of multilinear polynomials based on resultant methods. We enumerate all expressions of the multihomogeneous (or multigraded) resultant of such systems as a determinant of Sylvester-like matrices, aka generalized Sylvester matrices. We construct these matrices by means of Weyman homological complexes, which generalize the Cayley-Koszul complex. The computation of the determinant of the resultant matrix is the bottleneck for the overall complexity. We exploit the quasi-Toeplitz structure to reduce the problem to efficient matrix-vector multiplication, which corresponds to multivariate polynomial multiplication, by extending the seminal work on Macaulay matrices of Canny, Kaltofen, and Yagati [9] to the multihomogeneous case. We compute a rational univariate representation of the roots, based on the primitive element method. In the case of 0-dimensional systems we present a Monte Carlo algorithm with probability of success $1-1/2^r$, for a given $r \geq 1$, and bit complexity $O_B(n^2D^(4+e)(n^(N+1)+\tau)+nD^(2+e)r(D+r))$ for any $e>0$, where n is the number of variables, D equals the multilinear Bézout bound, N is the number of variable subsets, and τ is the maximum coefficient bitsize. We present an algorithmic variant to compute the isolated roots of overdetermined and positive-dimensional systems. Thus our algorithms and complexity analysis apply in general with no assumptions on the input.

8.2.5 Sampling the feasible sets of SDPs and volume approximation

In [24], we present algorithmic, complexity, and implementation results on the problem of sampling points in the interior and the boundary of a spectrahedron, that is the feasible region of a semidefinite program. Our main tool is random walks. We define and analyze a set of primitive geometric operations that exploits the algebraic properties of spectrahedra and the polynomial eigenvalue problem, and leads to the realization of a broad collection of efficient random walks. We demonstrate random walks that experimentally show faster mixing time than the ones used previously for sampling from spectrahedra in theory or applications, for example Hit and Run. Consecutively, the variety of random walks allows us to sample from general probability distributions, for example the family of log-concave distributions which arise frequently in numerous applications. We apply our tools to compute (i) the volume of a spectrahedron and (ii) the expectation of functions coming from robust optimal control. We provide a C++ open source implementation of our methods that scales efficiently up to to dimension 200. We illustrate its efficiency on various data sets.

8.2.6 Geometric algorithms for sampling the flux space of metabolic networks

Systems Biology is a fundamental field and paradigm that introduces a new era in Biology. The crux of its functionality and usefulness relies on metabolic networks that model the reactions occurring inside an organism and provide the means to understand the underlying mechanisms that govern biological systems. Even more, metabolic networks have a broader impact that ranges from resolution of ecosystems to personalized medicine. The analysis of metabolic networks is a computational geometry oriented field as one of the main operations they depend on is sampling uniformly points from polytopes; the latter provides a representation of the steady states of the metabolic networks. However, the polytopes that result from biological data are of very high dimen- sion (to the order of thousands) and in most, if not all, the cases are considerably skinny. Therefore, to perform uniform random sampling efficiently in this setting, we need a novel algorithmic and computational framework specially tailored for the properties of metabolic networks. In [30], we present a complete software framework to handle sampling in metabolic networks. Its backbone is a Multiphase Monte Carlo Sampling (MMCS) algorithm that unifies rounding and sampling in one pass, obtaining both upon termination. It exploits an improved variant of the

Billiard Walk that enjoys faster arithmetic complexity per step. We demonstrate the efficiency of our approach by performing extensive experiments on various metabolic networks. Notably, sampling on the most complicated human metabolic network accessible today, Recon3D, corresponding to a polytope of dimension 5 335 took less than 30 hours. To our knowledge, that is out of reach for existing software.

8.3 Algebraic Analysis

8.3.1 On the inverse Cauchy problem for linear ordinary differential equations

The Cauchy problem characterizes the solutions of a linear ordinary differential equation that satisfies initial conditions. In [31], we investigate the converse problem, namely, given a function that is known to satisfy a linear ordinary differential equation of a fixed order, determine the coefficients of the ordinary differential equation and the initial conditions. The techniques used to investigate the inverse Cauchy problem come from the algebraic estimation problem introduced by Fliess and Sira-Ramírez. From the perfect observation of the solution, i.e., without external perturbation and noise corrupting it, the initial value problem can be explicitly reconstructed using only iterative indefinite integrals of the solution.

8.4 Geometry

8.4.1 Cartan connections and path structures with large automorphism groups

In [27], we classify compact manifolds of dimension three equipped with a path structure and a fixed contact form (which we refer to as a strict path structure) under the hypothesis that their automorphism group is non-compact. We use a Cartan connection associated to the structure and show that its curvature is constant.

8.4.2 Geometric structures and configurations of flags in orbits of real forms

[26] is an introduction and a survey on geometric structures modelled on closed orbits of real forms acting on spaces of flags. We focus on 3-manifolds and the flag space of all pairs of a point and a line containing it in $\mathbb{P}(\mathbb{C}^3)$. It includes a description of general flag structures which are not necessarily flat and a combinatorial description of flat structures through con- figurations of flags in closed orbits of real forms. We also review volume and Chern-Simons invariants for those structures.

8.4.3 Volume function and Mahler measure of exact polynomials

In [28], we study a class of two-variable polynomials called exact polynomials which contains A-polynomials of knot complements. The Mahler measure of these polynomials can be computed in terms of a volume function defined on the vanishing set of the polynomial. We prove that the local extrema of the volume function are on the two-dimensional torus and give a closed formula for the Mahler measure in terms of these extremal values. This formula shows that the Mahler measure of an irreducible and exact polynomial divided by π is greater than the amplitude of the volume function. We also prove a K-theoretic criterion for a polynomial to be a factor of an A-polynomial and give a topological interpretation of its Mahler measure.

8.5 Control Theory

8.5.1 Centrohermitian solutions of a factorization problem arising in vibration analysis. Part I: Lee's transformation

Motivated by an application of vibration analysis to gearbox fault surveillance, a new demodulation approach for gearbox vibration signals has recently been developed. Within this approach, the demodulation problem yields the study of a rank factorization problem for centrohermitian matrices. In [32], using the properties of centrohermitian matrices, we first show that the rank factorization problem for centrohermitian matrices can be transformed into a rank factorization problem for real matrices. Based on previous works, we then show how to parametrize a class of centrohermitian solutions of the rank factorization problem that is important in practice.

8.5.2 Centrohermitian Solutions of a Factorization Problem Arising in Vibration Analysis. Part II: A Coninvolutory Matrix Approach

In "Centrohermitian solutions of a factorization problem arising in vibration analysis. Part I: Lee's Transformation", we showed that the structure of centrohermitian matrices and Lee's transformation can be used to transform the search for centrohermitian solutions of a rank factorization problem – at the core of a new demodulation approach arising in gearbox vibration analysis – into the search for real solutions of a polynomial system. Hence, in "Centrohermitian solutions of a factorization problem arising in vibration analysis. Part I: Lee's Transformation", we parametrized a class of centrohermitian solutions of the rank factorization problem that is interesting in practice. Despite its effectiveness, Lee's transformation can be seen as a black box hiding information on the resolution of the rank factorization problem for centrohermitian solutions. To get more insight, in [33], we develop an alternative approach to the centrohermitian rank factorization problem.

8.6 Algebraic aspects of a rank factorization problem arising in vibration analysis

The article [21] continues the study of a rank factorization problem arising in gear fault surveillance. The structure of a class of solutions – important in practice – of the rank factorization problem is studied. We show that these solutions can be parametrized. Using module theory and computer algebra methods, the parameter space P is explicitly characterized and is shown to be the complementary of an algebraic set. Finally, a finite open cover of P is obtained and for each basic open subset of the cover of P, a closed-form solution is characterized.

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 was signed with the company Safran Electronics & Defense on the study of parallel mecanisms.

10 Partnerships and cooperations

10.1 International initiatives

10.1.1 Inria associate team not involved in an IIL or an international program

MACAO

Title: Mathematics and Algorithms for Cryptographic Advanced Objects

Duration: 2019 ->2021

Coordinator: Thomas Plantard (thomaspl@uow.edu.au)

Partners:

- University of Wollongong

Inria contact: Antoine Joux

10.1.2 Participation in other International Programs

AFRIMath

Title: Afrique France Réseau International de Mathématiques

Date/Duration : 2021 - 2026

Additionnal info/keywords : International Research Network (IRN)

10.2 National initiatives

10.2.1 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.

10.2.2 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

- Elias Tsigaridas : Minisymposium Algebraic and Geometric Tools for High Dimensional Computing SIAM Conference on Applied Algebraic Geometry, Texas (virtual)

Member of the conference program committees

- Fabrice Rouillier is member of the scientific committee of the conference for the 150 years of the SMF (Société Mathématique de France)
- Elisa Tsigaridas was member of the conference program committees 2021 22th International Workshop on Computer Algebra in Scientific Computing (CASC)

Reviewer

- Pascal Molin reviewed a book proposed to Springer.
- Alban Quadrat reviewed a book proposed to Springer and articles submitted to Internal Journal of Robust and Nonlinear Control, Mathematics in Computer Science, European Control Conference, Maple Conference, etc.

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 associate editor of Multidimensional Systems and Signal Processing, Springer
- Alban Quadrat is associate editor of Maple Transactions
- Fabrice Rouillier is associate editor of Journal of Symbolic Computation, Elsevier
- Fabrice Rouillier is associate editor of Maple Transactions

11.1.3 Invited talks

- Alban Quadrat gave the talk *On the general solutions of a rank factorization problem arising in vibration analysis* at the Aromath seminar, Inria Sophia Antipolis - Méditerranée, France, 10/02/2021, and at the Séminaire de Calcul Formel de Limoges, France, 18/03/2021
- Alban Quadrat gave the talk *Algorithmic aspects of the algebraic parameter estimation problem* at the 91st Annual Meeting of the International Association of Applied Mathematics and Mechanics (GAMM 2020), Kassel, Germany, 15-19/03/2021
- Alban Quadrat gave the talk *An introduction to the Quillen-Suslin theorem: algorithms and applications* at the Symbolic Computation Seminar at North Carolina State University, USA, 03/05/2021
- Alban Quadrat gave the talks *Centrohermitian solutions of a factorization problem arising in vibration analysis, Part I: Lee's transformation, Part II: A coninvolutory matrix approach*, at European Control Conference 2021, Netherlands, 03/06/2021

11.1.4 Leadership within the scientific community

- Alban Quadrat is member of the technical committee Linear Systems of the International Federation of Automatic Control (IFAC)

11.1.5 Scientific expertise

- Alban Quadrat reviewed a project submitted to the LabEx CIMI "Centre International de Mathématiques et d'Informatique" (Institut de Mathématiques de Toulouse et Institut de Recherche en Informatique de Toulouse).

11.1.6 Research administration

- Yves Guiraud is elected member of the *bureau du Comité National de la Recherche Scientifique, section 41 (mathématiques)*

- Yves Guiraud is elected member of the *Conseil scientifique de l'UFR de mathématiques de l'Université de Paris*

- Yves Guiraud is elected member of the *Conseil de laboratoire de l'IMJ-PRG*

- Alban Quadrat is member of the *Conseil d'Administration of the Société Mathématique de France (SMF)*

- Elisa Tsigaridas is elected member of the CE

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- 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 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 : Algorithms and CompetitiveProgramming, 2021 Ingénieur 2A, modal. 20h lectures and 25h TD. Department of Informatics (LIX), École Polytechnique, France

- Elias Tsigaridas : Algorithms for data analysis in C++, 2021 Ingénieur 2A. 40h TD. Department of Informatics (LIX), École Polytechnique, France

11.2.2 Supervision

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

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

- PhD in progress: Alen Ðurić, 10/2019, directed by Yves Guiraud (co-supervision with Pierre-Louis Curien, IRIF)

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

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

- PhD in progress : Thibauld Feneuil, 10/2020, directed by Jean-Claude Bajard
- PhD in progress : Carles Checa, 10/2020, directed by Elias Tsigaridas (co-supervision with Ioannis Emiris)
- PhD in Progress : Andrea Negro , 10/2021, directed by Pierre-Vincent Koseleff (co-supervision with Julien Marché IMJ-PRG)
- Antonin Guilloux co-supervised with Julien Tierny (LIP6) the Master thesis of Quyen Nguyen, M2 Algèbre appliquée, Université Paris Saclay
- Yves Guiraud co-supervised with Emmanuel Wagner (IMJ-PRG) the Master thesis of Octave Mestoudjian, M2 Mathématiques Fondamentales, Sorbonne Université
- Alban Quadrat supervised the Master thesis of Maya Chartouny, *Étude algorithmique du problème d'estimation de paramètres*, M2 Algèbre Appliquée, University of Paris Saclay

11.2.3 Juries

- Alban Quadrat was president of the jury of the PhD defense of P.-C. Aubin-Frankowski, *Estimation and Control under Constraints through Kernel Methods*, MINES ParisTech, 05/07/2021

11.3 Popularization

11.3.1 Internal or external Inria responsibilities

- Fabrice Rouillier is the chair of the association *Animath*
- Fabrice Rouillier is *Chargé de mission médiation* for the Inria Paris research center
- 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

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 and S. Duquesne. 'Montgomery-friendly primes and applications to cryptography'. In: *Journal of Cryptographic Engineering* 11.4 (2021), pages 399–415. DOI: 10.1007/s13389-021-00260-z. URL: https://hal.sorbonne-universite.fr/hal-02883333.

[19] R. Barbulescu and S. Shinde. 'A classification of ECM-friendly families using modular curves'. In: *Mathematics of Computation* (1st Sept. 2021). URL: https://hal.archives-ouvertes.fr/hal-01822144.

[20] M. R. Bender, J.-C. Faugère, A. Mantzaflaris and E. Tsigaridas. 'Koszul-type determinantal formulas for families of mixed multilinear systems'. In: *SIAM Journal on Applied Algebra and Geometry* (2021). DOI: 10.1137/20M1332190. URL: https://hal.inria.fr/hal-03236344.

[21] Y. Bouzidi, R. Dagher, E. Hubert and A. Quadrat. 'Algebraic aspects of a rank factorization problem arising in vibration analysis'. In: *Communications in Computer and Information Science*. Maple in Mathematics Education and Research 1414 (4th Jan. 2021). DOI: 10.1007/978-3-030-81698-8_8. URL: https://hal.inria.fr/hal-03529914.

[22] Y. Bouzidi, A. Quadrat, F. Rouillier and G. Younes. 'Computation of the $\mathscr{L}\infty$ -norm of finite-dimensional linear systems'. In: *Communications in Computer and Information Science* (Aug. 2021). URL: https://hal.inria.fr/hal-03328685.

[23] P. Bürgisser, F. Cucker and J. Tonelli-Cueto. 'Computing the Homology of Semialgebraic Sets. II: General formulas'. In: *Foundations of Computational Mathematics* (4th Jan. 2021). DOI: 10.1007/s10208-020-09483-8. URL: https://hal.inria.fr/hal-02878370.

[24] T. Chalkis, V. Fisikopoulos, P. Repouskos and E. Tsigaridas. 'Sampling the feasible sets of SDPs and volume approximation'. In: *ACM Communications in Computer Algebra* (2021). DOI: 10.1145/3457341.3457349. URL: https://hal.inria.fr/hal-02572792.

[25] I. Z. Emiris, A. Mantzaflaris and E. Tsigaridas. 'Multilinear Polynomial Systems: Root Isolation and Bit Complexity'. In: *Journal of Symbolic Computation*. Special Issue on Milestones in Computer Algebra (MICA 2016) 105 (2021), pp. 145–164. DOI: 10.1016/j.jsc.2020.06.005. URL: https://hal.inria.fr/hal-02099556.

[26] E. Falbel, A. Guilloux and Q. Wang. 'Geometric structures and configurations of flags in orbits of real forms'. In: *São Paulo Journal of Mathematical Sciences* 15.1 (June 2021), pp. 175–213. DOI: 10.1007/s40863-020-00175-3. URL: https://hal.sorbonne-universite.fr/hal-03377097.

[27] E. Falbel, M. Mion-Mouton and J. M. Veloso. 'Cartan connections and path structures with large automorphism groups'. In: *International Journal of Mathematics* (27th Oct. 2021). DOI: 10.1142/S0129167X21400164. URL: https://hal.archives-ouvertes.fr/hal-03214060.

[28] A. Guilloux and J. Marché. 'Volume function and Mahler measure of exact polynomials'. In: *Compositio Mathematica* 157.4 (Apr. 2021), pp. 809–834. DOI: 10.1112/S0010437X21007016. URL: https://hal.sorbonne-universite.fr/hal-03377099.

International peer-reviewed conferences

[29] J.-C. Bajard, K. Fukushima, S. Kiyomoto, T. Plantard, A. Sipasseuth and W. Susilo. 'Generating Residue Number System Bases'. In: ARITH 2021- IEEE 28th Symposium on Computer Arithmetic. Virtual, France: IEEE, 14th June 2021, pp. 86–93. DOI: 10.1109/ARITH51176.2021.00027. URL: https://hal.sorbonne-universite.fr/hal-03457951.

[30] A. Chalkis, V. Fisikopoulos, E. Tsigaridas and H. Zafeiropoulos. 'Geometric algorithms for sampling the flux space of metabolic networks'. In: The 37th International Symposium on Computational Geometry (SoCG). Buffalo, United States, 2021. URL: https://hal.inria.fr/hal-03047049.

[31] M. Chartouny, T. Cluzeau and A. Quadrat. 'On the inverse Cauchy problem for linear ordinary differential equations'. In: GAMM 2021 - 92nd Annual Meeting of the International Association of Applied Mathematics and Mechanics. Vol. 21. Applied Mathematics and Mechanics PAMM 2021 1. Kassel, Germany, 14th Dec. 2021. DOI: 10.1002/pamm.202100214. URL: https://hal.inria.fr/hal-03530281.

[32] E. Hubert, Y. Bouzidi, R. Dagher and A. Quadrat. 'Centrohermitian solutions of a factorization problem arising in vibration analysis. Part I: Lee's transformation'. In: ECC 2021 - European Control Conference. Delft (Virtual), Netherlands, 29th June 2021. DOI: 10.23919/ECC54610.2021.9655069. URL: https://hal.inria.fr/hal-03530244.

[33] E. Hubert, Y. Bouzidi, R. Dagher and A. Quadrat. 'Centrohermitian Solutions of a Factorization Problem Arising in Vibration Analysis. Part II: A Coninvolutory Matrix Approach'. In: ECC 2021 - European Control Conference. Delft (Virtual), Netherlands, 29th June 2021. DOI: 10.23919/ECC54610.2021.9655115. URL: https://hal.inria.fr/hal-03530258.

Reports & preprints

[34] R. V. Alexandre. *Closed ray affine manifolds*. 26th Nov. 2021. URL: https://hal.archives-ouvertes.fr/hal-03358563.

[35] R. V. Alexandre. *Closed ray nil-affine manifolds and parabolic geometries*. 17th Nov. 2021. URL: https://hal.archives-ouvertes.fr/hal-03433549.

[36] R. V. Alexandre. *Redundancy of triangle groups in spherical CR representations.* 28th Oct. 2021. DOI: 10.1080/10586458.2021.1985655. URL: https://hal.archives-ouvertes.fr/hal-02867990.

[37] M. Chartouny, T. Cluzeau and A. Quadrat. *Algorithmic study of the algebraic parameter estimation problem for a class of perturbations.* RR-9441. Inria Paris, Sobonne Université; XLIM, 15th Dec. 2021, p. 26. URL: https://hal.inria.fr/hal-03502443.

[38] F. Cucker, A. A. Ergür and J. Tonelli-Cueto. *Functional norms, condition numbers and numerical algorithms in algebraic geometry.* 24th Feb. 2021. URL: https://hal.inria.fr/hal-03151436.

[39] P.-L. Curien, A. Ðurić and Y. Guiraud. *Coherent presentations of a class of monoids admitting a Garside family.* 1st July 2021. URL: https://hal.archives-ouvertes.fr/hal-03276119.

[40] R. Dagher, E. Hubert and A. Quadrat. *On the general solutions of a rank factorization problem.* RR-9438. Inria Paris, Sobonne Université; Inria Lille - Nord Europe; Laboratoire d'Analyse des Signaux et Processus Industriels, 14th Dec. 2021, p. 57. URL: https://hal.inria.fr/hal-03479643.

[41] E. Falbel, I. Pasquinelli and A. Ucan-Puc. *Reachability results for perturbed heat equations.* 7th Dec. 2021. URL: https://hal.archives-ouvertes.fr/hal-03468849.

[42] E. Falbel, I. Pasquinelli and A. Ucan-Puc. *Representations of Deligne-Mostow lattices into PGL(3, C).* 3rd Aug. 2021. URL: https://hal.archives-ouvertes.fr/hal-03313111.

[43] A. Guilloux and T. Horesh. *p-adic Directions of Primitive Vectors.* 14th Oct. 2021. URL: https://hal.sorbonne-universite.fr/hal-03377102.

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

12.3 Other

Scientific popularization

[45] J. Tonelli-Cueto. *Semi... ¿qué? Las múltiples formas de lo semialgebraico y cómo determinarlas.* Virtual, Spain, 26th May 2021. DOI: 10.5281/zenodo.4718329. URL: https://hal.inria.fr/hal-03236067.

12.4 Cited publications

[46] 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.

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

[48] 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.

[49] 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.

[50] 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.

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

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

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

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

[73] 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).

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

[75] 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.

[76] D. N. Diatta, S. Diatta, F. Rouillier, M.-F. Roy and M. Sagraloff. 'Bounds for polynomials on algebraic numbers and application to curve topology'. working paper or preprint. Oct. 2018. URL: https://hal.inria.fr/hal-01891417.

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

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

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

[80] 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.

[81] 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.

[82] 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.

[83] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[102] R. Jha, D. Chablat, F. Rouillier and G. Moroz. 'An algebraic method to check the singularity-free paths for parallel robots'. In: *International Design Engineering Technical Conferences & Computers and Information in Engineering Conference*. ASME. Boston, United States, Aug. 2015. URL: https://hal.archives-ouvertes.fr/hal-01142989.

[103] R. Jha, D. Chablat, F. Rouillier and G. Moroz. 'Workspace and Singularity analysis of a Delta like family robot'. In: *4th IFTOMM International Symposium on Robotics and Mechatronics*. Poitiers, France, June 2015. URL: https://hal.archives-ouvertes.fr/hal-01142465.

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

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

[106] A. Joux and C. Pierrot. 'Nearly Sparse Linear Algebra and application to Discrete Logarithms Computations'. In: *Contemporary Developments in Finite Fields and Applications*. WorldScientific, 2016. DOI: 10.1142/9789814719261_0008. URL: https://hal.inria.fr/hal-01154879.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[136] G. Rance, Y. Bouzidi, A. Quadrat and A. Quadrat. 'A symbolic-numeric method for the parametric H∞ loop-shaping design problem'. In: *22nd International Symposium on Mathematical Theory of Networks and Systems (MTNS)*. Minneapolis, United States, July 2016, p. 8. URL: https://hal.inria.fr/hal-01415294.

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

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

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

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

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

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

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

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

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

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

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

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