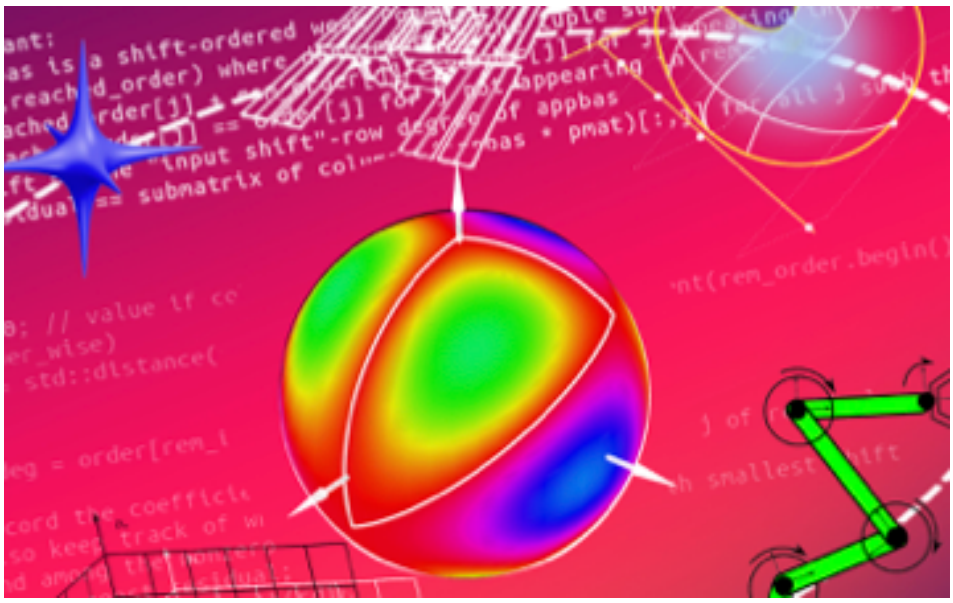
Fundamental Algorithms and Algorithmic Complexity



Rapport sur les contributions

https://indico.math.cnrs.fr/e/8113

ID de Contribution: **1** Type: **Non spécifié**

Efficient Algorithms for Integer and Polynomial Matrices by G. Labahn and A. Storjohann. University of Waterloo, Canada. 9:30-12:00. Amphitheater Darboux, IHP

lundi 18 septembre 2023 09:30 (2h 30m)

ID de Contribution: **2** Type: **Non spécifié**

Efficient Algorithms for Integer and Polynomial Matrices by G. Labahn and A. Storjohann. University of Waterloo, Canada. 9:30-12:00. Amphitheater Darboux, IHP

mardi 19 septembre 2023 09:30 (2h 30m)

ID de Contribution: **3** Type: **Non spécifié**

Efficient Algorithms for Integer and Polynomial Matrices by G. Labahn and A. Storjohann. University of Waterloo, Canada. 9:30-12:00. Amphitheater Darboux, IHP

jeudi 21 septembre 2023 09:30 (2h 30m)

ID de Contribution: **4** Type: **Non spécifié**

Efficient Algorithms for Integer and Polynomial Matrices by G. Labahn and A. Storjohann. University of Waterloo, Canada. 9:30-12:00. Amphitheater Darboux, IHP

vendredi 22 septembre 2023 09:30 (2h 30m)

ID de Contribution: **5** Type: **Non spécifié**

Euclidean Lattices by D. Stehlé. CryptoLab Inc., Lyon. 14:00-16:00. Amphitheater Darboux, IHP

mardi 19 septembre 2023 14:00 (2 heures)

ID de Contribution: **6** Type: **Non spécifié**

Euclidean Lattices by D. Stehlé. CryptoLab Inc., Lyon. 10:00-12:00. Amphitheater Hermite, IHP

mercredi 20 septembre 2023 10:00 (2 heures)

ID de Contribution: **7** Type: **Non spécifié**

General audience presentation by J. van der Hoeven, CNRS, LIX, Palaiseau. 16:00-17:00. Amphitheater Hermite, IHP

mercredi 20 septembre 2023 16:00 (1 heure)

ID de Contribution: **8** Type: **Non spécifié**

Welcome coffee

lundi 25 septembre 2023 08:45 (30 minutes)

ID de Contribution: **9** Type: **Non spécifié**

Opening by Dominique Mouhanna, IHP Deputy Director

lundi 25 septembre 2023 09:15 (15 minutes)

ID de Contribution: **10** Type: **Non spécifié**

A recent trend in Computer Algebra? Let's chat! by Joachim von zur Gathen

lundi 25 septembre 2023 09:30 (1 heure)

Abstract. Does the recent craze about chatbots affect Computer Algebra? If so, in which way? As a non-expert, I will share some observations.

ID de Contribution: **11** Type: **Non spécifié**

Coffee break

lundi 25 septembre 2023 10:30 (30 minutes)

ID de Contribution: **12** Type: **Non spécifié**

Recent progress on deterministic integer factorisation by David Harvey

lundi 25 septembre 2023 11:00 (1 heure)

Abstract. There are several deterministic factoring algorithms of complexity N1/4+o(1) going back to the 1970s. A few years ago Hittmeir lowered the exponent to 2/9, and I subsequently improved it further to 1/5. In this talk I will explain the key ideas behind these new algorithms.

ID de Contribution: **13** Type: **Non spécifié**

Lunch break

ID de Contribution: **14** Type: **Non spécifié**

Efficient approximation of polynomials by Guillaume Moroz

lundi 25 septembre 2023 14:00 (1 heure)

Abstract. In modern numerical computations, real numbers are approximated with floating-point numbers, of the form s2e, where s and e are integers with a fixed precision. This representation is compact and can represent numbers with small and large magnitudes. In this talk, we will generalize this idea to approximate univariate polynomial functions with piecewise polynomials of the form s(X)Xe where s is a polynomial of fixed degree and e is an integer. Using tools such as the Newton polygon, this representation can be computed efficiently both in theory and in practice. Moreover, it can be used to efficiently evaluate and find roots approximations of a high-degree polynomial.

ID de Contribution: **15** Type: **Non spécifié**

First-order factors of linear Mahler operators by Frédéric Chyzak

lundi 25 septembre 2023 15:00 (1 heure)

Abstract. We develop and compare two algorithms for computing first-order right-hand factors in the ring of linear Mahler operators $\ell_r M^r+\cdots+\ell_1 M+\ell_0$ where $\ell_0,\cdots,\ell_r$ are polynomials in x and $Mx=x^b M$ for some integer $b\geq 2$. In other words, we give algorithms for finding all formal infinite product solutions of linear functional equations $\ell_r(x)f(x^{b^r})+\cdots+\ell_1(x)f(x^b)+\ell_0(x)f(x)=0$.
The first of our algorithms is adapted from Petkovšek's classical algorithm for the analogous problem in the case of linear recurrences. The second one proceeds by computing a basis of generalized power series solutions of the functional equation and by using Hermite-Padé approximants to detect those linear combinations of the solutions that correspond to first-order factors.
We present implementations of both algorithms and discuss their use in combination with criteria from the literature to prove the differential transcendance of power series solutions of Mahler equations.

ID de Contribution: **16** Type: **Non spécifié**

Coffee break

lundi 25 septembre 2023 16:00 (30 minutes)

ID de Contribution: **17** Type: **Non spécifié**

The block Wiedemann algorithm and polynomial equations by Éric Schost

lundi 25 septembre 2023 16:30 (1 heure)

Abstract. Coppersmith's generalization of Wiedemann's algorithm is a key ingredient in algorithms for integer factorization or discrete logarithms. I will describe how, in recent years, it has also successfully been applied in contexts arising from algorithms for polynomial equations, such as sparse FGLM algorithms, or modular composition.

ID de Contribution: **18** Type: **Non spécifié**

Matrix multiplication via Lie groups by Chris Umans

mardi 26 septembre 2023 09:30 (1 heure)

Abstract. Cohn and Umans proposed a group-theoretic approach to bounding the exponent of matrix multiplication. Previous work within this approach ruled out certain families of groups as a route to obtaining ω=2, while other families of groups remain potentially viable. In this work we turn our attention to matrix groups, whose usefulness within this framework was relatively unexplored.

To study these groups, we propose working in the continuous setting of Lie groups, in which we develop an analogous theory. Obtaining the analogue of exponent 2 in this potentially easier setting is a key challenge that represents an intermediate goal short of actually proving ω=2. We give constructions in the continuous setting which are indeed best-possible in a precise sense.

We then describe a new ingredient – "separating polynomials" – which allow us to recover a full-fledged framework yielding actual (finite) algorithms in the Lie group setting, rather than constructions whose interest is only by analogy. This framework has some mathematically pleasing features: the notion of border rank arises naturally from the Lie algebra, and we have machinery that points to the main open question being that of finding a separating polynomial of appropriate degree in a certain ring of invariant polynomials.

This is based on joint work with Jonah Blasiak, Henry Cohn, Josh Grochow, and Kevin Pratt.

ID de Contribution: **19** Type: **Non spécifié**

Coffee break

mardi 26 septembre 2023 10:30 (30 minutes)

ID de Contribution: **20** Type: **Non spécifié**

Superpolynomial lower bounds against low-depth algebraic circuits by Sébastien Tavenas

mardi 26 septembre 2023 11:00 (1 heure)

Abstract. An algebraic circuit computes a polynomial using addition and multiplication operators. Understanding the power of algebraic circuits has close connections to understanding general computation. Despite this, not many lower bounds are known for even simple Sigma Pi Sigma (product-depth 1) circuits. Before our work, the best known lower bound for product-depth 1 circuit was (slightly less than) cubic. No lower bounds were known for general product-depth 2 circuits.
In this work, we show the first superpolynomial lower bound for low-product-depth algebraic circuits. In the talk, we discuss the main results and present the proof ideas used in the proof of the superpolynomial lower bound for product-depth 1 circuits.
This talk is based on joint work with Nutan Limaye and Srikanth Srinivasan.

ID de Contribution: **21** Type: **Non spécifié**

Free afternoon

ID de Contribution: **22** Type: **Non spécifié**

Reception

ID de Contribution: **23** Type: **Non spécifié**

Computing the non-commutative rank of linear matrices by Gábor Ivanyos

mercredi 27 septembre 2023 09:30 (1 heure)

Abstract. The topic of the talk connects skew-fields, polynomial identity testing, invariant theory and optimization. By a linear matrix we mean a matrix having homogeneous linear entries and the non-commutative rank is the rank when we consider the variables as elements of the appropriate free skew-field. Computing it is a relaxation of determining the maximal rank of a matrix in a given linear space of matrices. A remarkable characterization can be given in terms of a large common zero block of the coefficient matrices after a change of basis. We will present the main ideas of a deterministic polynomial time algorithm that computes the noncom-mutative rank. Note that existence of an efficient deterministic method computing the ordinary rank is a famous open problem in polynomial identity testing. The algorithm gives lower and upper witnesses for the rank. The lower witness is a polynomial invariant of a sub-matrix while the upper witness is given by a common zero block. We will also discuss some applications of the algorithm.
The talk is based on joint works with Youming Qiao and K. V. Subrahmanyam.

ID de Contribution: **24** Type: **Non spécifié**

Coffee break

mercredi 27 septembre 2023 10:30 (30 minutes)

ID de Contribution: **25** Type: **Non spécifié**

Closure of algebraic complexity classes under factoring by Nitin Saxena

mercredi 27 septembre 2023 11:00 (1 heure)

Abstract. Polynomial factoring is one of the most fundamental problems in the area of computational algebra. Its variants have attracted a huge amount of attention in the last half-a-century. On the other hand, algebraic complexity theory classifies polynomials, into complexity classes, according to computational resources. Could we show that these classes afford polynomial factoring algorithms?
In this talk we will focus on four algebraic complexity classes— size-s circuits VPnb, size-s degree-s circuits VP, size-s degree-s verifier circuits VNP, and size-s algebraic branching programs VBP. We will discuss the algebraic methods, inspired from analysis, that have been developed to do factoring in these complexity classes. We will list the open questions and make some related conjectures. [This is based on the joint work with Pranjal Dutta, Amit Sinhababu (J. ACM'22, STOC'18), and the follow-up papers by others.] [https://www.cse.iitk.ac.in/users/nitin/research.html]

ID de Contribution: **26** Type: **Non spécifié**

Clément Pernet

ID de Contribution: **27** Type: **Non spécifié**

Border rank, homogeneity and de-bordering paradigms in GCT by Pranjal Dutta

mardi 26 septembre 2023 14:00 (1 heure)

Abstract. Border (or approximative) complexity of polynomials plays an integral role in GCT (Geometric Complexity Theory) approach to P!=NP. This raises an important basic question: can arbitrary approximations of simple polynomials involve exponential-precision which may not be efficiently simulable? Circuits of depth 3 or 4, are a good testing ground for this question. Recently, Kumar proved that *any* polynomial f can be approximated arbitrarily well by restrictions of the polynomial x1 … xn - 1 for n large enough. In this talk, we will see a stronger connection (& reverse) of this result with the border rank of f, and how homogeneity can play an important role in border complexity.
Furthermore, we will see the border of constant top-fanin depth-3 circuits (which is far more general than x1…xn -1) is relatively easy & hierarchical - it can be computed by a polynomial-size algebraic branching program (ABP).
This is based on the joint works with – 1) Prateek Dwivedi & Nitin Saxena (FOCS'21) 2) Nitin Saxena (FOCS'22) 3) Fulvio Gesmundo, Christian Ikenmeyer, Gorav Jindal and Vladimir Lysikov (submitted).

ID de Contribution: **28** Type: **Non spécifié**

Efficient algorithms for Riemann—Roch spaces by Grégoire Lecerf

mardi 26 septembre 2023 15:00 (1 heure)

Abstract. Riemann—Roch spaces are a cornerstone of modern applications of algebra to various areas of computer science: error correcting codes, secret sharing, multi-party computations, zero-knowledge proofs, resilience in distributed storage systems, interactive oracle proofs… Best performances are achieved for specific families of spaces known to be difficult to compute.
We will present a new probabilistic algorithm of Las Vegas type that computes Riemann—Roch spaces of plane projective curves in expected sub-quadratic time whenever the characteristic is zero or positive but sufficiently large. The method relies on the Brill—Noether theory (1874), bivariate polynomial elimination, Puiseux series expansions, and structured polynomial matrices. In case of curves with only ordinary singularities, we will present a faster variant that even supports any characteristic.
This is joint work with Simon Abelard (Thales SIX GTS, France), Elena Berardini (CNRS, University of Bordeaux, France), Alain Couvreur (Inria Saclay, France).

ID de Contribution: **29** Type: **Non spécifié**

Coffee break

mardi 26 septembre 2023 16:00 (30 minutes)

ID de Contribution: **30** Type: **Non spécifié**

Cocktail

mercredi 27 septembre 2023 18:30 (2h 30m)

ID de Contribution: **31** Type: **Non spécifié**

Applications of fast integer and polynomial lattice reduction in cryptography by Nadia Heninger

jeudi 28 septembre 2023 09:30 (1 heure)

Abstract. I will survey some concrete lattice computations that have appeared in the context of some recent papers in applied cryptography that I have been involved with, and pose some open problems and speculative improvements that arose in these contexts.

ID de Contribution: **32** Type: **Non spécifié**

Coffee break

jeudi 28 septembre 2023 10:30 (30 minutes)

ID de Contribution: **33** Type: **Non spécifié**

Interpolating isogenies by Benjamin Wesolowski

jeudi 28 septembre 2023 11:00 (1 heure)

Abstract. In 2011, Jao and De Feo proposed a key exchange based on the presumed hardness of the following problem: given two elliptic curves, and the images of a few points through a secret isogeny, compute this isogeny.
In 2022, a polynomial-time algorithm was discovered. This powerful new tool has broken many cryptosystems, but has also lead to new constructions, and other applications in algorithmic number theory. We will present this algorithm and some of its applications.

ID de Contribution: **34** Type: **Non spécifié**

On the complexity of computing characteristic polynomials by Clément Pernet

jeudi 28 septembre 2023 14:00 (1 heure)

Abstract. : Among the classical problems in computational linear algebra, the computation of the characteristic polynomial is of great relevance for applications as it reflects most invariants of the input matrix. It is a key component in the solution of many other related problems, such as computing eigenvalues, invariant factors and invariant subspace decomposition, testing matrices for similarity, Krylov methods etc. Computing characteristic polynomials efficiently is surprisingly challenging and has lead to a very diverse algorithmic landscape, as it lies in-between scalar linear algebra and modules of polynomial matrices. For instance, finding a deterministic reduction to dense matrix multiplication was an open-problem until recently. We will introduce some of these algorithmic techniques to present recent complexity improvements for the computation of characteristic polynomials: with dense matrices, first, we will present a recent work achieving the first reduction to matrix multiplication, based on polynomial matrix arithmetic. Then, in the context of matrices with a displacement rank structure, we will present algorithms, leading to the first sub-quadratic time cost.
This talk is based on joint work with P. Karpman, V. Neiger, H. Signargout and G. Villard.

ID de Contribution: **35** Type: **Non spécifié**

The practical complexity of arbitrary-precision functions by Fredrik Johansson

jeudi 28 septembre 2023 15:00 (1 heure)

Abstract. Most familiar operations on N-digit real numbers (sum, product, square root, exponential, logarithm, etc.) can be computed in time quasilinear in N. However, this kind of asymptotic statement hides details which can add up to huge differences in practical running times. We will discuss how to think about optimizing arbitrary-precision algorithms, with a detailed look at state-of-the-art methods for transcendental functions.

ID de Contribution: **36** Type: **Non spécifié**

Coffee break

jeudi 28 septembre 2023 16:00 (30 minutes)

ID de Contribution: **37** Type: **Non spécifié**

Computing Sparse Fourier Sum of Squares on Finite Abelian Groups by Lihong Zhi

jeudi 28 septembre 2023 16:30 (1 heure)

Abstract. The non-negativity of a function on a finite abelian group can be certified by its Fourier sum of squares (FSOS). We propose a method of certifying the nonnegativity of an integer valued function by an FSOS certificate, which is defined to be an FSOS with a small error. We prove the existence of exponentially sparse polynomial and rational FSOS certificates and provide two methods to validate them. As a consequence of the aforementioned existence theorems, we propose a semidefinite programming (SDP)-based algorithm to efficiently compute a sparse FSOS certificate. For applications, we consider certificate problems for maximum satisfiability (MAX-SAT) and maximum k-colorable subgraph (MkCS) and demonstrate our theoretical results and algorithm by numerical experiments.
Jointed work with Jianting Yang and Ke Ye.

ID de Contribution: **38** Type: **Non spécifié**

Sparse interpolation and Exponential analysis going hand in hand by Annie Cuyt

vendredi 29 septembre 2023 09:30 (1 heure)

We discuss how sparse interpolation in computer algebra and exponential analysis in digital signal processing can cross-fertilize and lead to new results. The Nyquist constraint [11] is the digital signal processing equivalent of stating that the argument of a complex exponential exp(φΔ) with φ ∈ C and Δ ∈ R+ can only be retrieved uniquely under the condition that |=(φ)|Δ < π. It governs signal processing since the beginning of the 20-th century. In the past two decades this constraint was first broken with the use of randomly collected signal samples [8, 2] and later for use with uniform samples [6].
The latter method closely relates to the original version of the exponential data fitting algorithm published in 1795 by the French mathematician de Prony [7], which is often cited in sparse interpolation research. In engineering applications it is mostly implemented using a structured generalized eigenvalue approach. Besides avoiding the Nyquist constraint, the new result in [6] also solves a number of remaining open problems in exponential analysis, which we plan to discuss.
In the identification, from given values fk ∈ C, of the nonlinear parameters φ1, . . . , φn ∈ C, the linear coefficients α1, . . . , αn ∈ C and the sparsity n ∈ N in the inverse problem
nΣ
j=1
αj exp(φj kΔ) = fk, k = 0, . . . , 2n − 1, . . . fk ∈ C, Δ ∈ R+, (1)
several cases are considered to be hard [6, 1]: When some of the φj cluster, the identification and separation of these clustered φj becomes numerically ill-conditioned. We show how the problem may be reconditioned.
Retrieval of the correct value of n is difficult, and more so in case of clustered φj and noisy samples fk. Here, decimation of the data offers a way to obtain a reliable estimate of n automatically. Such decimation allows to divide and conquer the inverse problem statement. The smaller subproblems are largely independent and can be solved in parallel, leading to an improved complexity and efficiency.
At the same time, the sub-Nyquist Prony method proves to be robust with respect to outliers in the data. Making use of some approximation theory results [9, 10, Kn.Cu:rob:23], we can also validate the computation of the φj and αj .
The Nyquist constraint effectively restricts the bandwidth of the =(φj). Therefore, avoiding the constraint offers so-called superresolution, or the possibility to unearth higher frequency components in the samples. All of the above can be generalized in several ways, to the use of more functions besides the exponential on the one hand, and to the solution of multdimensional inverse problems as in (1) on the other [5].
References
[1] M. Briani, A. Cuyt, F. Knaepkens, and W.-s. Lee. VEXPA: Validated EXPonential Analysis through regular subsampling. Signal Processing, 177: nr. 107722, 2020. (Published online July 17, 2020. Toolbox and experiments downloadable.).
[2] Emmanuel J. Cand‘es, Justin Romberg, and Terence Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inf. Theory, 52(2):489–509, 2006.
[3] Annie Cuyt and Wen-shin Lee. Smart data sampling and data reconstruction. US Patent

9,690,749.
[4] Annie Cuyt and Wen-shin Lee. Smart data sampling and data reconstruction. EP2745404B1.
[5] Annie Cuyt and Wen-shin Lee. Multivariate exponential analysis from the minimal number of samples. Adv. Comput. Math., 44:987–1002, 2018. (Published online
November 16, 2017. Toolbox and experiments downloadable.).
[6] Annie Cuyt and Wen-shin Lee. How to get high resolution results from sparse and coarsely sampled data. Appl. Comput. Harmon. Anal., 48:1066–1087, 2020. (Published online October 11, 2018. Toolbox and experiments downloadable.).
[7] R. de Prony. Essai exp´erimental et analytique sur les lois de la dilatabilite des fluides elastiques et sur celles de la force expansive de la vapeur de l'eau et de la vapeur de l'alkool, a differentes temp´eratures. J. Ec. Poly., 1(22):24–76, 1795.
[8] D. L. Donoho. Compressed sensing. IEEE Transactions on Information Theory, 52(4):1289–1306, 2006.
[9] J. Gilewicz and M. Pindor. Pad´e approximants and noise: a case of geometric series. J. Comput. Appl. Math., 87:199–214, 1997.
[10] J. Gilewicz and M. Pindor. Pad´e approximants and noise: rational functions. J. Comput. Appl. Math., 105:285–297, 1999.
[11] H. Nyquist. Certain topics in telegraph transmission theory. Trans. Am. Inst. Electr. Eng., 47(2):617–644, April 1928

ID de Contribution: **39** Type: **Non spécifié**

Coffee break

vendredi 29 septembre 2023 10:30 (30 minutes)

ID de Contribution: **40** Type: **Non spécifié**

Modulus tricks for integer sparse polynomials by Daniel Roche

vendredi 29 septembre 2023 11:00 (1 heure)

Abstract. Sparse polynomials with integer coefficients are a basic building block in computer algebra systems, as well as an important fundamental object for algorithmic study. Since at least the 1980s, efficient algorithms have been constructed based on the flexibility afforded by changing the integer modulus repeatedly during the computation. This talk will attempt to briefly survey some of the modulus-choosing techniques employed in recent results to achieve faster algorithms. We will also briefly examine when these techniques (fail to) extend to the case of floating point computations and field extensions.

ID de Contribution: **41** Type: **Non spécifié**

Group Photo