# Fast and rigorous arbitrary-precision evaluation of Legendre polynomials and Gauss-Legendre quadrature nodes

Fredrik Johansson* Marc Mezzarobba†

Gauss-Legendre quadrature requires a nearly minimal number of evaluation points to achieve a given accuracy for numerical integration of functions that are well-approximated by polynomials. However, other quadrature rules (such as the Clenshaw-Curtis and double exponential formulas) have often been favored in high-precision computations due to the cost of generating the quadrature nodes, even in cases where those rules require more evaluation points.

We describe an efficient strategy for rigorous arbitrary-precision evaluation of Legendre polynomials on the unit interval and its application in the generation of Gauss-Legendre quadrature rules.

Our focus is on making the evaluation practical for a wide range of realistic parameters, corresponding to the requirements of numerical integration to an accuracy of about 100 to 100 000 bits. Our evaluation algorithm combines the summation by rectangular splitting of several types of expansions in terms of hypergeometric series with a fixed-point implementation of Bonnet's three-term recurrence relation. We then compute rigorous enclosures of the Gauss-Legendre nodes and weights using the interval Newton method. We provide rigorous error bounds for all steps of the algorithm.

The practicality of the approach is validated by an implementation in the Arb library. Our implementation achieves an order-of-magnitude speedup over previous code for computing Gauss-Legendre nodes with simultaneous high degree and precision, making Gauss-Legendre quadrature viable even at very high precision.

## References

[1] D. H. Bailey and J. M. Borwein. High-precision numerical integration: Progress and challenges. *Journal of Symbolic Computation*, 46(7):741–754, 2011.

[2] I. Bogaert. Iteration-free computation of Gauss–Legendre quadrature nodes and weights. *SIAM Journal on Scientific Computing*, 36(3):A1008–A1026, 2014.

[3] L. Fousse. Accurate multiple-precision Gauss–Legendre quadrature. In *18th IEEE Symposium on Computer Arithmetic*, ARITH'07, pages 150–160. IEEE, 2007.

*Inria Bordeaux, équipe LFANT, fredrik.johansson@gmail.com
†CNRS, LIP6, équipe Pequan, marc@mezzarobba.net

[4] F. Johansson. Arb: efficient arbitrary-precision midpoint-radius interval arithmetic. *IEEE Transactions on Computers*, 66:1281–1292, 2017.

[5] K. Petras. On the computation of the Gauss–Legendre quadrature formula with a given precision. *Journal of Computational and Applied Mathematics*, 112(1):253–267, 1999.

[6] L. N. Trefethen. Is Gauss quadrature better than Clenshaw–Curtis? *SIAM review*, 50(1):67–87, 2008.

[7] J. Wimp. *Computation with Recurrence Relations*. Pitman, Boston, 1984.

# Approximations de Tchebychev certifiées de fonctions D-finies vectorielles

F. Bréhard

Lundi 22 janvier 2018

Les fonctions D-finies, ou holonomes, sont les solutions d'équations différentielles ordinaires linéaires à coefficients polynomiaux. Cette classe de fonctions mathématiques, en dépit de leur apparente simplicité, apparaissent par exemple naturellement dans de nombreux problèmes de physique mathématique et représentent 60% des fonctions répertoriées dans le *Handbook of mathematical functions* [**?**]. Leurs propriétés algébriques riches permettent un traitement purement algébrique de ces objets, au travers notamment de l'équation différentielle satisfaite [**?**]. Par ailleurs, la suite de leurs coefficients pour divers développements en séries (Taylor, Tchebychev, Legendre, Hermite...) [**?**, **?**] vérifie une récurrence linéaire à coefficients polynomiaux.

Néanmoins, il est parfois souhaitable, voire nécessaire, de disposer d'approximations numériques concrètes de ces fonctions, avec une borne certifiée sur l'erreur commise. Cela peut être le cas pour des applications industrielles critiques, comme le contrôle d'un satellite, où avoir une approximation polynomiale certifiée de sa trajectoire permet de la calculer très efficacement, tout en conservant une garantie forte sur la qualité du résultat ainsi obtenu. Cela se révèle également crucial dans le domaine des mathématiques assistées par ordinateur, où une partie des preuves (calcul d'intégrales, vérification d'inégalités, etc.) doit pouvoir être déléguée à l'ordinateur sans compromettre la rigueur mathématique de l'édifice total (voir par exemple [**?**]).

La validation de fonctions D-finies dans la base de Tchebychev a déjà été l'objet de plusieurs travaux. Dans [**?**], l'itération de Picard permet de reformuler le problème comme une équation de point fixe avec opérateur intégral contractant, de sorte à déduire un encadrement certifié de l'erreur d'approximation par le théorème du point fixe de Banach. Dans [**?**], l'utilisation d'une méthode de Newton permet d'obtenir différemment une équation de point fixe pour appliquer le même théorème de Banach. L'objectif de cette présentation est d'étendre cette seconde méthode au cas des équations D-finies vectorielles, en soulignant les difficultés supplémentaires qui apparaissent lors du processus d'obtention d'encadrements fins des erreurs composante par composante. La contribution finale consiste en un algorithme de validation s'insérant dans une chaîne complètement automatisée, partant de l'équation différentielle et produisant des approximations numériques de Tchebychev, dont une borne d'erreur certifiée est calculée *a posteriori* par cette méthode.

Dans un premier temps, nous présenterons une extension du théorème de point fixe de Banach afin d'obtenir une méthode générique de validation *a posteriori* pour des problèmes vectoriels, donnant des encadrements fins compo-

sante par composante de l'erreur d'approximation. Puis, nous appliquerons ce procédé aux équations D-finies vectorielles à l'aide d'une méthode de Newton sur un espace de coefficients bien choisi. Cela nous permettra d'obtenir des approximations polynomiales certifiées en base de Tchebychev pour des fonctions D-finies vectorielles, avec des bornes d'erreur certifiées composante par composante. Pour terminer, un exemple de circuit électrique nous permettra d'illustrer pas à pas le fonctionnement de l'algorithme de validation.

# Rational minimax approximation via adaptive barycentric representations

**S.-I. Filip** Y. Nakatsukasa L. N. Trefethen
B. Beckermann

Rational approximation is historically a core topic in approximation theory with applications in fields such as computer arithmetic, signal processing and model order reduction. In this talk I will discuss about recent work [1] (inspired by [2]) with my collaborators on designing robust algorithms for computing best (in the $L_\infty$ norm) rational approximations to continuous functions over an interval $[a, b]$.

A core aspect of this work is to consider rational functions (of type $(n, n)$) in a *barycentric* representation of the form

$$r(x) = \frac{\sum_{k=0}^{n} \dfrac{\alpha_k}{x - t_k}}{\sum_{k=0}^{n} \dfrac{\beta_k}{x - t_k}},$$

where $\{\alpha_k\}, \{\beta_k\}$ are the barycentric coefficients of $r$ and $\{t_k\}$ are called support nodes which can be freely chosen.

We indicate how these $\{t_k\}$ can be taken in an *adaptive*, problem dependent way that greatly reduces the underlying numerical precision needed to obtain accurate results, in comparison to a more common representation of $r$ involving ratios of polynomials represented in monomial or Chebyshev bases. An example of this is the problem of determining type $(n, n)$ best rational approximations to $f(x) = |x|, x \in [-1, 1]$ up to $n = 80$, for which Varga, Ruttan and Carpenter [3] used 200-digit arithmetic, whereas with our approach we get similar results with standard 16-digit floating point arithmetic.

## References

[1] S.-I. Filip, Y. Nakatsukasa, L.N. Trefethen, and B. Beckermann, Rational minimax approximation via adaptive barycentric representations. *arXiv preprint arXiv:1705.10132* (2017).

[2] Y. Nakatsukasa, O. Sète, and L. N. Trefethen, The AAA algorithm for rational approximation. Technical report, 2016. submitted to *SIAM J. Sci. Comp.*

[3] R. S. Varga, A. Ruttan, and A. D. Carpenter, Numerical results on best uniform rational approximation of $|x|$ on $[-1, +1]$. *Mathematics of the USSR-Sbornik*, 74(2):271, 1993.

# A New Approach for Solving the Permutation Code Equivalence Problem

Magali Bardet, Ayoub Otmani, Mohamed Saeed-Taha

We study the algorithmic problem of deciding whether two linear codes consist of the same codewords up to a permutation on the codeword coordinates. This problem is called Permutation Code Equivalence. Using simple tools from linear algebra, we show that this problem can be solved for many instances in polynomial time. Our approach starts from a new modeling based on a quadratic multivariate polynomial system, $S$, describing the solution set of the problem.

However, since our system involves $n^2$ variables for codes of length $n$, generic algorithms that solve multivariate systems by computing Gröbner bases become very rapidly impractical.

We consider particular instances where the solving can be accelerated by

1. extracting from the system $S$ linear equations involving only a "block" of $n$ variables $x_1, \ldots, x_n$,
2. computing a Gröbner basis of the system obtained by keeping from $S$ only the previous linear equations and the equations depending only on $x_1, \ldots, x_n$,
3. adding this Gröbner basis to the initial system.

The "block" Gröbner bases are easy to compute, and produce many linear equations that permit to solve the initial system.

This is a joint work with Ayoub Otmani and Mohamed Saeed-Taha.

# Regularity and Gröbner bases of the Rees algebra of edge ideals of bipartite graphs

Yairon Cid Ruiz

Let $G = (V(G), E(G))$ be a bipartite graph on the vertex set $V(G) = X \cup Y$ with bipartition $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$. Let $\mathbb{K}$ be a field and let $R$ be the polynomial ring $R = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. The edge ideal $I = I(G)$, associated to $G$, is the ideal of $R$ generated by the set of monomials $x_i y_j$ such that $x_i$ is adjacent to $y_j$.

We study several properties of the Rees algebra of $I$. From a computational point of view we first focus on the universal Gröbner basis of its defining equations, and from a more algebraic standpoint we focus on its total and partial regularities as a bigraded algebra. Applying these ideas, we give an estimation of when $\operatorname{reg}(I^s)$ starts to be a linear function and we find upper bounds for the regularity of the powers of the edge ideal $I$.

Let $\mathcal{R}(I) = \bigoplus_{i=0}^{\infty} I^i t^i \subset R[t]$ be the Rees algebra of the edge ideal $I$. Let $f_1, \ldots, f_q$ be the square free monomials of degree two generating $I$. We can see $\mathcal{R}(I)$ as a quotient of the polynomial ring $S = R[T_1, \ldots, T_q]$ via the map

$$\begin{aligned} S = \mathbb{K}[x_1, \ldots, x_n, y_1 \ldots, y_m, T_1, \ldots, T_q] &\xrightarrow{\psi} \mathcal{R}(I) \subset R[t], \\ \psi(x_i) = x_i, \quad \psi(y_i) = y_i, \quad \psi(T_i) &= f_i t. \end{aligned}$$

Then the presentation of $\mathcal{R}(I)$ is given by $S/\mathcal{K}$ where $\mathcal{K} = \operatorname{Ker}(\psi)$.

The universal Gröbner basis of the ideal $\mathcal{K}$ is defined as the union of all the reduced Gröbner bases $\mathcal{G}_<$ of the ideal $\mathcal{K}$ as $<$ runs over all possible monomial orders ([1]). In our first main result we compute the universal Gröbner basis of the defining equations $\mathcal{K}$ of the Rees algebra $\mathcal{R}(I)$.

**Theorem 1.** *Let $G$ be a bipartite graph and $\mathcal{K}$ be the defining equations of the Rees algebra $\mathcal{R}(I(G))$. The universal Gröbner basis $\mathcal{U}$ of $\mathcal{K}$ is given by*

$$\begin{aligned} \mathcal{U} = &\{T_w \mid w \text{ is an even cycle}\} \\ &\cup \{v_0 T_{w^+} - v_a T_{w^-} \mid w \text{ is an even path}\} \\ &\cup \{u_0 u_a T_{(w_1,w_2)^+} - v_0 v_b T_{(w_1,w_2)^-} \mid w_1 \text{ and } w_2 \text{ are disjoint odd paths}\}. \end{aligned}$$

Our second main result is computing the total regularity and giving upper bounds for both partial regularities ([2]) of $\mathcal{R}(I)$ as a bigraded $S$-algebra.

**Theorem 2.** *Let $G$ be a bipartite graph. Then we have:*

*(i)* $\operatorname{reg}(\mathcal{R}(I(G))) = \operatorname{match}(G)$,

*(ii)* $\operatorname{reg}_{xy}(\mathcal{R}(I(G))) \leq \operatorname{match}(G) - 1$,

*(iii)* $\operatorname{reg}_T(\mathcal{R}(I(G))) \leq \operatorname{match}(G)$,

*where match*$(G)$ *denotes the matching number of* $G$.

It is a famous result (for a general ideal in a polynomial ring) the asymptotic linearity of $\operatorname{reg}(I^s)$ for $s \gg 0$ ([3]). However, the exact form of this linear function and the exact point where $\operatorname{reg}(I^s)$ starts to be linear, is a problem that continues wide open even in the case of monomial ideals. In recent years, a number of researchers have focused on computing the regularity of powers of edge ideals and on relating these values to combinatorial invariants of the graph.

From the characterization of the universal Gröbner basis and a special monomial order, we get the following results.

**Corollary 3.** *Let* $G$ *be a bipartite graph with bipartition* $V(G) = X \cup Y$. *Then, for all* $s \geq 1$ *we have*

$$\operatorname{reg}(I(G)^s) \leq 2s + \min\big\{|X| - 1,\ |Y| - 1,\ 2b(G) - 1\big\},$$

*where* $b(G)$ *represents the minimum cardinality of the maximal matchings of* $G$. *In the particular case of* $G$ *being a complete bipartite graph we have*

$$\operatorname{reg}(I(G)^s) = 2s.$$

Using the existence of the canonical module for the Rees algebra, we can obtain our last results.

**Corollary 4.** *Let* $G$ *be a bipartite graph. Then, the following statements hold:*

*(i) For all* $s \geq \operatorname{match}(G) + |E(G)| + 1$ *we have*

$$\operatorname{reg}(I(G)^{s+1}) = \operatorname{reg}(I(G)^s) + 2.$$

*(ii) For all* $s \geq 1$ *we have*

$$\operatorname{reg}(I(G)^s) \leq 2s + \operatorname{match}(G) - 1.$$

# References


[1] Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996.

[2] Tim Römer, *Homological properties of bigraded algebras*, IIllinois J. Math. 45 (2001), no. 4, 1361-1376.

[3] S. Dale Cutkosky, Jürgen Herzog, and Ngô Viêt Trung, *Asymptotic behaviour of the Castelnuovo-Mumford regularity*, Compositio Math. 118 (1999), no. 3, 243 - 261.

# A Symbolic Approach for Solving Algebraic Riccati Equations

Yacine Bouzidi*

A classical and thoroughly studied problem in automatic control theory is the $H_\infty$ control of linear systems. Given a linear dynamical system, the objective is to synthesize controllers that achieve stabilization and guarantee some performance criteria according to the $H_\infty$-norm. This problem, which can be expressed as a mathematical optimization problem, is usually reformulated as a problem of solving nonlinear matrix equations known as *Algebraic Riccati Equations*. Such equations are well-known since they arise in various problems of automatic control and signal processing such as optimal control, Kalman filtering, estimation problems, etc. In the case of the $H_\infty$ control problem, this gives rise to an algebraic Riccati equation of the following form

$$X\,A + A^T\,X - X\,B\,B^T\,X + C^T\,C = 0, \tag{1}$$

where $A, B, C \in \mathbb{R}^{n\times n}$ are constant matrices with real entries and $X \in \mathbb{R}^{n\times n}$ is a symmetric matrix one is seeking for. Under certain conditions on the matrices $A, B$ and $C$, the goal is then to compute a positive definite matrix $X$ that is solution of (1).

Most of the existing methods for solving (1) rely on purely numerical routines (see [2] and references therein). However, due to large model uncertainties, these methods are too conservative, and unfixed model parameters shall be considered in certain applications, that is a model with matrices $A, B$ and $C$ with unknown parameters.

In this presentation, following the work given in [1], we propose a new computer algebra approach for the study of algebraic Riccati equations that depend on a set of unknown parameters. More precisely, using classical techniques from real algebraic geometry (Gröbner bases, univariate representations and discriminant varieties), we examine the algebraic systems that stem from these equations. The conducted study allows us to exhibit some interesting properties of these systems while it eases the computation of their solutions (see [3] for details).

The presented symbolic approach, which is interesting in the context of adaptive control, is illustrated through a classical example, where explicit formulas are obtained for the robust controller and whose robust margin depends only on the parameters of the systems.

This work is a collaboration with G. Rance and Ar. Quadrat (Safran Electronics & Defense), F. Rouillier (Ouragan, Inria Paris) and Al. Quadrat (NON-A, Inria Lille–Nord Europe).

*NON-A, Inria Lille–Nord Europe

## References


[1] Hirokazu Anai, Shinji Hara, Masaaki Kanno, and Kazuhiro Yokoyama. Parametric polynomial spectral factorization using the sum of roots and its application to a control design problem. *Journal of Symbolic Computation*, 44(7):703–725, 2009.

[2] Angelika Bunse-Gerstner. Computational solution of the algebraic riccati equation. *Journal of The Society of Instrument and Control Engineers*, 35(8):632–639, 1996.

[3] Rance Guillaume, Yacine Bouzidi, Alban Quadrat, and Arnaud Quadrat. A symbolic-numeric method for the parametric h_infinity loop-shaping design problem. In *22nd International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, page 8, 2016.

# Projection of analytic surfaces

Sény Diatta Guillaume Moroz Marc Pouget

For some robotic problems we need to represent a singular surface that is the projection of a smooth surface embedded in higher dimension.
In this work, we focus on the problem of computing a triangulation of the projection on $\mathbb{R}^3$ of an analytic surface embedded in $\mathbb{R}^4$.

Based on Transversality theory [3] and Singularity Classification [1, 4], we first recall that, under generic assumptions, the set of singularities of the projected surface are generated by only three types of multi-germs: double points, triple points and cross-caps. Then, we will show that how to characterize those singularities as solutions of three systems of equations which are regular under certain assumptions. Finally, using numerical methods [2, 5, 6], we design an algorithm taking as input an analytic surface and returning a triangulation isotopic to its projected surface.

## References

[1] M. Golubistky and V. Guillemin. Stable Mapping and Their Singularities. Springer-Verlag New York, 1973.

[2] A. Neumaier. Interval methods for systems of equations. Cambridge University Press, 1990.

[3] M. Demazure. Bifurcations and catastrophes: geometry of solutions to nonlinear problems. Universitext. Springer, Berlin, New York, 2000. École polytechnique.

[4] C. A. Hobbs and N. P. Kirk. On the classification and bifurcation of multigerms of maps from surfaces to 3-space. Math. Scand., 89(1):57-96, 2001.

[5] B. Martin, A. Goldsztejn, L. Granvilliers and C. Jermann. Certified parallelotope continuation for one-manifolds. SIAM Journal on Numerical Analysis 51(6), 3373- 3401 (2013)

[6] Van Der Hoeven, Joris. Reliable homotopy continuation. Research Report v4 hal-00589948 (Jan-2015). https://hal.archives-ouvertes.fr/hal-00589948/file/homotopy5.pdf.

# Finite fibers of multi-graded dense rational maps on $\mathbb{P}^3$

Nicolas Botbol  Laurent Busé  Marc Chardin
Fatmanur Yıldırım

Finite fibers of rational maps $\Psi$ from $\mathbb{P}^2$ to $\mathbb{P}^3$ and also $\mathbb{P}^1 \times \mathbb{P}^1$ to $\mathbb{P}^3$ have been studied in [2] by Botbol, Busé and Chardin. For both cases, they have assumed that the base locus $\mathcal{B}$ of $\Psi$ is finite and locally complete intersection. Also for the both cases, $\mathcal{B}$ contains only points and multiple of points. Under these assumptions, they write approximation complexes of cycles $\mathcal{Z}_\bullet$ of multi-degree $\nu$ computed according to [1]. They show that for these $\nu$ values, the Hilbert function of the fiber at a point $p \in \mathbb{P}^3$, becomes Hilbert polynomial of the fiber at $p$. From the first arrow of $\mathcal{Z}_\bullet$ giving a family of matrices they chose one and denote it by $\mathcal{M}(\Psi)_\nu$. They study the fibers of dimension 0 and 1. They state a relation between the corank of $\mathcal{M}(\Psi)(p)_\nu$ and degree of the fiber at point $p$.

Our motivation is to compute the distance from a point $p \in \mathbb{R}^3$ to an algebraic rational surface $\mathcal{S} \in \mathbb{R}^3$. For that purpose, firstly, from a parametrization of $\mathcal{S}$, we construct a parametrization of normal lines to $\mathcal{S}$, namely $\psi$ from $\mathbb{R}^3$ into $\mathbb{R}^3$. Secondly, we homogenize $\psi$ in $\mathbb{P}^2 \times \mathbb{P}^1$ or possibly in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ and we obtain a multi-graded multi homogeneous rational map $\Psi$ into $\mathbb{P}^3$.

Our work is an extension of [2]. We present a new method to study the finite fibers of dense multi-graded rational maps $\Psi$ from $\mathbb{P}^2 \times \mathbb{P}^1$ or $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ to $\mathbb{P}^3$. Different from the previous work [2], in this case the base locus $\mathcal{B}$ of $\Psi$ has degree one components, i.e it contains curves. This was the main difficulty to handle and we needed additional hypothesis to control the fiber over a point $p \in \mathbb{P}^3$. For the multi-degree $\nu$ computed again according to [1], we show that Hilbert function of the fiber at point $p \in \mathbb{P}^3$ becomes Hilbert polynomial at $p$ which is equal to the corank of $\mathcal{M}(\Psi)(p)_\nu$. Moreover, at these multi-degree $\nu$, the corank of $\mathcal{M}(\Psi)(p)_\nu$ is equal to degree of the fiber at $p$ and it gives us the number of the orthogonal projections of $p$ onto the surface $\mathcal{S}$ under our construction.

## References

[1] Nicolás Botbol. The implicit equation of a multigraded hypersurface. *Journal of Algebra*, 348(1):381 – 401, 2011.

[2] Nicolàs Botbol, Laurent Busé, and Marc Chardin. Fitting ideals and multiple points of surface parameterizations. *Journal of Algebra*, 420(Supplement C):486 – 508, 2014.

# Décomposition d'un tenseur symétrique de rang faible: Application à l'identification de modèle statistique

J. Harmouch B. Mourrain H. Khalil

Ce projet a pour objet d'estimer la décomposition minimale affine d'un tenseur symétrique de rang faible à l'aide des mesures d'un modèle statistique lié à ce tenseur. La décomposition d'un tenseur symétrique vient de la décomposition en valeurs singulières des matrices de Hankel multi-variées tronquées associées au tenseur. On exploite des propriétés de la structure des matrices de multiplication associée à l'algèbre quotient ''de Gorenstein" liée au tenseur afin de calculer les poids et les points de la décomposition. L'estimation des paramètres d'un modèle à travers les moments d'une base de données statistique en utilisant la décomposition en valeurs singulières est à la fois un outil numérique efficace et optimal.

L'identification des paramètres d'un modèle statistique à travers des moments du tenseur associé exige la résolution d'un système d'équations polynomiales multi-variées. Dans cette présentation, on remplace la résolution de ce système par l'étude de la structure de l'algèbre quotient associée au dual du tenseur. Alors, les calculs des paramètres du modèle peuvent être obtenus par l'extraction des valeurs réelles des points et des poids la décomposition aussi que leur nombre. Ceci impose la décomposition affine minimale du tenseur multilinéaire associé au modèle en une somme pondérée des formes linéaires associées à ses paramètres et donc la décomposition de son dual en une somme pondérée d'évaluations. La décomposition du dual de tenseur est obtenue à travers la décomposition en valeurs singulières des matrices de Hankel multi-variées tronquées associées au tenseur. Le calcul du nombre des termes dans cette décomposition dérive du rang numérique de la matrice de Hankel inversible tronquée et le calcul des coordonnées en x, y et z des points vient de calcul des vecteurs propres des matrices de multiplication et de leurs transposées dans les bases orthogonaux convenables. Dans les travaux récents développés par [6] on a présenté la correspondance entre la décomposition du tenseur et l'algèbre quotient associée mais non pas trop l'efficacité de calcul numérique des algorithmes développés qui interprètent la structure de l'algèbre quotient. On propose une méthode algébrique stable qui permet de traiter ces instabilités numériques [5] et d'extraire les paramètres d'un modèle statistique à l'aide d'un petit nombre de moments donnés.

Ce problème a beaucoup d'applications dans les domaines des sciences numériques, de l'ingénieur, de l'ordinateur [1], en traitement de signal [7], en neurologie [3], et en statistique [2].

La probabilité de croisement des deux ou trois premiers mots dans un document fixe(ou de n'importe quelle collection de deux ou trois mots) revient à esti-

mer la probabilité conjointe de cette collection des mots sur tous les documents du corpus. Ceci nous permet alors de déterminer les vecteurs de probabilités de chaque mot suivant chaque document en utilisant la décomposition affine minimale d'un tenseur symétrique de rang r équivalent au nombre des topiques dans le corpus. Ce tenseur est associé aux moments modélisant le croisement des mots dans chaque document. On se sert des propriétés de la décomposition d'un tenseur symétrique décrit par [8] afin d'accomplir cet objectif. Des travaux ont été déjà développé par [4] afin de résoudre cette décomposition en utilisant des outils stochastiques.

## Références


[1] T. G. Colda and B. W. Bader. Tensor decompositions and applications. *SIAM review*. 51 (3) :455, 2009.

[2] J. B. Kruskal. Three-way arrays : rank and uniqueness of trilinear decompositions, with application to arithmetic complexity and statistics. *Linear Algebra and Appl., 18(2) :95-138, 1977*.

[3] M. Littman, R. Sutton, and S. Singh. Predictive representations of state. In *Advances in Neural Information Processing Systems 14*, pages 1555-1561, 2001.

[4] A. Anandkumar, R. Ge, D. Hsu, S. M. Kakade, M. Telgarsky . Tensor Decompositions for Learning Latent Variable Models. *Journal of Machine Learning Research 15*, pages 2773-2832, 2014.

[5] J. Harmouch, B. Mourrain, and H. Khalil. Decomposition of Low Rank Multi-Symmetric Tensor. *MACIS 2017, LNCS 10693*, p. 51-66, 2017.

[6] M. Elkadi, B. Mourrain : Introduction a la resolution des systemes polynomiaux. Mathematiques et Applications, vol. 59. Springer, Heidelberg, 2007.

[7] F. E. D. Raimondi, P. Common. *IEEE Signal Processing Letters*. P. 99, March 2017.

[8] B. Mourrain . Polynomial-exponential decomposition from moments. Found. Comput. Math. , Springer Verlag (2017) , September 2016.

# Continuité géométrique : Calculs sur des éléments polynomiaux par morceaux

Ahmed Blidia Bernard Mourrain

La continuité géométrique est un concept très utilisé dans les méthodes de CAD (Computer Aided design). Ce concept est abordé de différentes manières, nous proposons une étude algébrique de l'équation qui définissent cette continuité.

Deux surfaces $f_1, f_2 : [0,1]^2 \to \mathbb{R}^3$ admettent une jonction $G^k$ le long d'un segment $E$ avec $k \in \mathbb{N}$, si elles ont le même développement de Taylor sur $E$ après un changement de coordonées $\phi$, autrement dit $T^{(k)}(f_1) = T^{(k)}(f_2 \circ \phi)$ . La réunion des images de telles paramétrisations est une surface lisse.

Dans ce travail [1], nous étudions l'espace $\mathcal{S}(\mathcal{M})$ des splines à continuité $G^1$ associés à un maillage arbitraire $\mathcal{M}$, nous considérons des éléments polynomiaux par morceaux.

Certains modèles déja construits ont un degré et nombre de noeuds plus élevés. La plupart de ces travaux utilisent des résolutions de systèmes linéaires. Notre objectif est d'exploiter des structures plus sophistiquées, comme les modules, pour obtenir une analyse plus précise de ces espaces de fonctions. Pour cela nous présentons une étude de l'espace de syzygy sur les fonctions univariées polynomiales par morceaux. Les buts sont les suivants :

- Construire des splines avec une bonne répartitions des degrés de liberté.
- Donner des conditions sur les données de recollement pour ne pas générer de singularité.

## Références

[1] Ahmed Blidia, Bernard Mourrain, and Nelly Villamizar, *G1-smooth splines on quad meshes with 4-split macro-patch elements*, Computer Aided Geometric Design **52** (2017), 106 – 125, Geometric Modeling and Processing 2017.

# Singularités des diffiétés algébriques

François Ollivier (CNRS)
LIX UMR 7161, École polytechnique

L'origine de ce travail est l'étude des singularités des systèmes différentiels plat, entreprise avec Jeremy Kaminski et Jean Lévine [2]. Par exemple, un modèle simple de voiture est plat : $y' - \mathrm{tg}\theta x' = 0 \quad (1)$. On peut paramétrer les trajectoires par les coordonnées d'un point de l'essieu arrière, $(x, y)$, ce qui donne : $\theta = \mathrm{arctg}(y'/x')$, pourvu que $x' \neq 0$. On peut montrer qu'un paramétrage plat existe en tout point où $(x', y', \theta') \neq (0, 0, 0)$. Ces points sont des *singularités au sens des systèmes plats*. Ce sont néanmoins des points lisses de la *diffiété*, c'est-à-dire de l'objet géométrique défini par le système (1).

En effet, les diffiétés définies dans les ouvrages de Vinogradov [5] ou Zharinov [6] sont des variétés lisses, munies d'un champs de vecteur. Mais si on prend des diffiétés définies, par exemple, comme sous-espace de l'espace des jets par des équations différentielles algébriques, des points singuliers peuvent apparaître. La littérature sur le sujet est réduite. On trouve un article de Johnson [1], dans le formalisme de l'algèbre différentielle de Ritt [4].

Johnson propose d'abord une définition intuitive informelle utilisant les ensembles caractéristiques, avant de proposer une notion abstraite. On tente de revenir aux ensembles caractéristiques pour parvenir à une caractérisation effective des points singuliers. On reprend essentiellement la définition informelle de Johnson.

Définition. — Un point $\xi$ d'une diffiété définie par un idéal différentiel premier $\mathcal{P}$, associé à un idéal (non différentiel) maximal $\mathfrak{m}$ est *régulier* s'il existe des fonctions coordonnées $y_j$, définies en $\xi$ et telles que $\mathcal{P}$ admette, dans ces coordonnées, pour un ordre admissible convenable, un ensemble caractéristique $\mathcal{A}$ tel que $\forall A \in \mathcal{A}\ S_A(\xi) \neq 0$. (Rappelons que $S_A$ est la dérivée partielle de $A$ par rapport à sa dérivée dominante.)

C'est-à-dire que les dérivées dominantes peuvent localement s'exprimer comme fonction des dérivées inférieures. On montre que l'on retrouve une proposition prouvée par Johnson dans son formalisme.

Proposition. — Si $\xi$, défini par $\mathfrak{m}$, est régulier, alors $\bigcup_{r\in\mathrm{N}} \mathfrak{m}^r = (0)$.

Un exemple, emprunté à Johnson [1, p. 216], permet d'exhiber un point singulier.

Exemple. — On considère la diffiété algébrique $V$ définie par l'idéal différentiel dont un ensemble caractéristique est $yy'' - y'$. Le terme de degré minimal est $y'$, qui n'est pas d'ordre nul, donc $[y]$ n'est pas une composante isolée. On montre que pour tout $r \in \mathrm{N}\ y' \in [y]^r$. En effet la propriété est vraie pour $r = 0, 1$. Si elle est vraie pour $r$, alors $y'' \in [y]^r$ et $y' = yy'' \in [y]^{r+1}$. Ceci montre que le point correspondant à l'idéal $\mathfrak{m} := [t, y]$ est singulier puisque $\bigcup_{r\in\mathrm{N}} \mathfrak{m}^r \neq (0)$.

Désingulariser une variété algébrique consiste à rechercher une variété lisse dont elle soit la projection (ou l'image par un morphisme fini), à laquelle elle soit birationnellement équivalente. On voit que $V$ ne peut être la projection d'une variété lisse $W$, car alors l'intersection des puissances $\mathfrak{m}^r$ serait la projection des puissance d'un idéal maximal $\mathfrak{m} \subset \mathcal{O}(W)$, donc (0). Les tentatives de désingularisation par des moyens classiques semblent donc compromises.

On donnera un aperçu d'une caractérisation de ces singularités au moyens des différentielles de Kähler.

## Références


[1] Johnson (Joseph), « A notion of regularity for differential local algebras », in *Contributions to algebra*, 211–232, Academic Press, New York, 1977.

[2] Kaminski (Yirmeyahu J.), Lévine (Jean) et Ollivier (François), *Intrinsic and Apparent Singularities in Differentially Flat Systems, and Application to Global Motion Planning*, 2017.

[3] Kolchin (Ellis Robert), *Differential algebra and algebraic groups*, Academic Press, New York, 1973.

[4] Ritt, (Joseph Fels), 1950. *Differential Algebra*, Amer. Math. Soc. Colloq. Publ., vol. 33, A.M.S., New-York.

[5] Krasil'shchik (Iosif S.), Lychagin (Valentin V.) et Vinogradov (Alexandre M.), *Geometry of Jet Spaces and Nonlinear Partial Differential Equations*, Gordon and Breach, New York, 1986.

[6] Zharinov (Viktor Viktorovich), *Geometrical aspects of partial differential equations*, Series on Soviet and East European Mathematics, vol. 9, World Scientific, Singapore, 1992.

# Optimisation de portefeuille : modélisation stochastique et optimisation topologique

Mbaye Diouf

On se propose dans cet exposé de présenter l'optimisation de portefeuille par la modélisation stochastique et l'optimisation topologique, un domaine de recherche se situant à l'interface des mathématiques, de l'informatique et de la finance.

Après un aperçu sur les concepts de base et la terminologie, nous présentons le modèle Moyenne-Variance développé par Harry Markowitz au cours des années 50. Ce modèle est caractérisé par la maximisation du rendement espéré et la minimisation de la variance du rendement ou risque. Un accent est aussi mis sur des applications pour consolider les acquis.

Nous découvrons ensuite le modèle de Black-Scholes considéré comme une avancée fondamentale en Finance et qui propose une formule d'évaluation d'options. Il fut publié en 1973 et est donné par une dynamique du sous-jacent comme mouvement Brownien. Avec sa simplicité d'application, son importante utilisation par les opérateurs financiers, il permet de calculer la volatilité qui mesure la variation moyenne dans le temps d'un actif financier et donne donc une information sur le risque.

Il convient de souligner le lien qui existe entre le calcul d'options et l'équation de la chaleur. On choisit d'utiliser un schéma implicite aux différences finies pour obtenir une approximation de la solution de cette équation.

Nous évoquons aussi la notion de gradient topologique qui pour objectif d'optimiser un domaine $]0, A[$ dans lequel l'équation de la chaleur découlant notamment de l'équation de Black-Scholes est définie afin de minimiser une fonctionnelle $J$ associée. Pour cela on se propose de modifier la topologie de $]0, A[$ en plaçant un trou de rayon $\rho$ en un point $x_0 \in ]0, A[$. Le développement asymptotique de $J$ permet alors d'évaluer le gradient topologique $g(x_0)$ de $J$ en $x_0$ et de construire une famille de points $(\tau, x_0^n, g(x_0^n))$ désignant la frontière efficiente, où $g(x_0^n)$ est proche de 0 et $\tau$ est le temps.

On dispose enfin de graphes pour comprendre la variation de la valeur d'une option en fonction du temps et du sous-jacent. Des schémas numériques permettent de mieux interpréter les équations aux dérivées partielles issues des modèles étudiés.

## Références

[1] F. Aftalion ; *La Nouvelle Finance et la gestion de portefeuille*, Paris, Economica, "Gestion", ($1^{er}$ *Octobre* 2003), 240 *p.*

[2] Philippe Bernard ; *La théorie du portefeuille : une introduction*, Ingénierie Economique et Financière, Université Paris-Dauphine, (*Avril* 2006).

[3] Louis Bachelier ; *Théorie de la spéculation*, Annales scientifiques de l'É.N.S., $3^e$ série, tome 17, (1900), pp. $21 - 86$.

[4] Harry Markowitz ; *Portfolio Selection*, The Journal of Finance, Vol. 7, No. 1, Mar. (1952), pp. $77 - 91$.

[5] Robert Goffin ; *Principes de Finance Moderne*, Paris, Economica, "Finance", $6^{\text{è}}$ éd., (05/01/2012), 664 *p.*

[6] Éric Bayle, Marc Schwartz ; *Fonctionnement des systèmes bancaires et financiers*, Revue d'économie financière, n°81, (2005), pp. $211 - 235$.

[7] Thierry Roncalli ; *La gestion des risques financiers*, Paris, Economica, $2^{\text{è}me}$ édition, (2009), 557 *p.*

[8] David Heath, Robert Jarrow, Andrew Morton ; *Bond Pricing and the Term Structure of Interest Rates : A New Methodology for Contingent Claims Valuation*, Econometrica, The Econometric Society, Vol. 60, No. 1, (Jan., 1992), pp. $77 - 105$.

[9] Fateh Belaid and Daniel De Wolf ; *Sélection du portefeuille de projets d'exploration production en utilisant la méthode de Markowitz*, Nancy, $10^{\text{è}}$ conférence de la Société Française de Recherche Opérationnelle et d'Aide à la Décision, $(10 - fév - 2009)$, 22 *p.*

[10] D. Lamberton and B. Lapeyre ; *Introduction au calcul stochastique appliqué à la finance*, Paris, second ed., Ellipses, "Edition Marketing", (1997), 176 *p.*

[11] François Jubin ; *Outils théoriques du modèle standard*, Paris 9, Witam Patrimoine Finance Actuariat, (2003), 41 *p.*

[12] Patrick Navatte ; *Finance d'Entreprise et Théorie des Options*, Paris, Economica, "Gestion", (1998), 304 *p.*

[13] Nguyen Chi Thanh ; *Priçing d'option financière par la méthode des EDP*, PARIS 6, Université Pierre et Marie CURIE, Paris Universitas, (2007 – 2008).

[14] Jacques-Hervé Saiac ; *Introduction aux méthodes mathématiques et numériques en vue des applications en finance*, CNAM, (3 *avril* 2007), 158 *p.*

[15] Daniel Sevcovic ; *Analysis of the free boundary for the pricing of an American call option*, Euro Jnl of Applied Mathematics, Institute of Applied Mathematics, Faculty of Mathematics & Physics, Comenius University, Slovak Republic, vol. 12, (2001), pp. $25 - 37$.

[16] Jean Cea ; *Conception optimale ou identification de formes, calcul rapide de la dérivée directionnelle de la fonction coût*, RAIRO-Modélisation mathématique et analyse numérique, $n°3$, tome 20, (1986), pp. $371 - 402$.

[17] O. Pantz ; *Topological Gradient*, CMAP, (*January* $28^{th}$, 2015).

[18] Samuel Amstutz, Takéo Takahashi and Boris Vexler ; *Topological sensitivity analysis for time-dependent problems*, ESAIM : Control, Optimisation and Calculus of Variations 14, (2008), pp. $427 - 455$.

[19] J. Sokolowski, A. Zochowski ; *On the topological derivative in shape optimization*, SIAM Journal on Control and Optimization, Vol. 37, $n°4$, (*July* 1999), pp. $1251 - 1272$.

[20] Didier Auroux, Jérôme Fehrenbach ; *Les méthodes de gradient topologique*, Toulouse 3, CNRS, Université Paul Sabatier, Mathématiques pour l'industrie et la physique, $(3 - 4$ *Février* 2005), 17 *p.*

# Problèmes Elliptiques fortement non linéaires dans les Espaces de Sobolev à exposant variable d'ordre infini

M. H. Abdou[1,a], A. Benkirane[1] and S. El Manouni[2]

[1] Département de Mathématiques et Informatique Faculté des sciences Dhar-Mahraz, B.P. 1796 Atlas-Fès, Maroc

[a] Département MPC, Faculté des sciences et techniques, Université des comores, B.P 2585 Rue de la Corniche Moroni Comores

[2] Al-Imam University, Faculty of Sciences, Department of Mathematics P. O. Box 90950, Riyadh 11623, Saudi Arabia.

Dans ce travail, nous nous intéressons à l'existence de solutions pour les problèmes Elliptiques fortement non-linéaires avec des conditions de croissance non-standard dans le cadre des Espaces de Sobolev d'ordre infini anisotropiques avec des exposants variables notés $W_0^{\infty}(a_\alpha, p_\alpha(x))(\Omega)$.
Nous allons tout d'abord traiter le cas fini, c'est à dire dans le cadre des Espaces de Sobolev à exposants variables anisotropiques d'ordre fini $W_0^{m,\vec{p}(x)}(\Omega)$ et ensuite montrer l'existence de solutions dans le cas infini.

**Mots clés.** espaces de Sobolev anisotropique à exposants variables, équations elliptiques fortement non-linéaires d'ordre infini, condition de monotonie, Condition de signe.

## Références

[1] Adams,R., *Sobolev Spaces.* New York : Academic Press 1975.

[2] A. Benkirane M. Chrif and S. El Manouni, *Existence Results for Strongly Nonlinear Equations of Infinite Order*, Z. Anal. Anwend. (J. Anal. Appl.) 26, pp 303- 312 (2007)

[3] H. Brezis, *Analyse fonctionelle. Théorie, Méthodes et Applcations,* Masson, Paris, 1992.

[4] M. Chrif and S. El Manouni, *On a strongly anisotropic equation with L1-data*, Appl. Anal. 87(7), pp 865-871 (2008)

[5] M. Chrif and S. El Manouni, *Anisotropic equations in weighted Sobolev spaces of higher order*, Ricerche mat. DOI 10.1007/s11587-009-0045-1 (2009).

[6] Ju. A. Dubinskii, *Sobolev Spaces of Infinite Order and Differential Equations*, Teubner-Texte Math. Band 87. Leipzig : Teubner, 1986.

[7] Ju. A. Dubinskii, *Sobolev spaces for infinite order and the behavior of solutions of some boundary value problems with unbounded increase of the order of the equation*, Math. USSR-Sb. 27 (1975)(2), pp. 143-162.

[8] O. Kovacik, J. Rakosnik, *On spaces $L^{p(x)}$ and $W^{1,p(x)}$,* Czechoslovak Math. J. 41 (1991) 592-618.

[9] J. L. Lions *Quelque Méthodes de Résolution des Problémes aux Limites Non Linéaires.* Paris : Dunod ; Gauthier-Villars 1969.

[10] X.L. Fan, D. Zhao, *On the generalized Orlicz-Sobolev space $W^{k,p(x)}(\Omega)$*, J. Gansu Educ. College 12 (1) (1998) 1-6.

[11] D. Zhao, W.J. Qiang, X.L. Fan, *On generalized Orlicz spaces $L^{p(x)}$*, J. Gansu Sci. 9 (2) (1996) 1-7.

# Advances in Symbolic Computation in Maple

Jürgen Gerhard*

We will summarize the advances in symbolic computation in Maple that were made over the past years, including polynomial arithmetic, real root isolation and polynomial system solving, series and limit computations, symbolic integration and symbolic summation, and differential equations.

*Senior Director of Research, Maplesoft

# Correcting errors in a matrix inverse

Daniel S. Roche*

We consider the problem of computing the inverse of a matrix $A$, given a matrix $B$ which is close to the inverse of $A$ with a small number of erroneous entries. We show how to recover the true inverse of $A$ in roughly $\tilde{\mathrm{O}}(n^2 + k^w)$ time, where $n$ is the dimension of the matrix, $k$ is the number of errors, and $w$ is the exponent of fast matrix multiplication. With this running time, for sufficiently small number of errors $k$, the time to correct the inverse is linear in the size of the matrix itself, and is therefore worthwhile over the trivial solution of simply recomputing it. This can be seen as a continuation of work by Gasiniec et al on efficiently correcting errors in a matrix product, as well as an extension of recent papers at ISSAC and elsewhere on efficiently verifying the results of linear algebra computations. The main application is to distributed or outsourced computing, where errors can be introduced by a small number of faulty nodes or by network noise.

*U.S. Naval Academy, Annapolis, Maryland, USA; currently at Laboratoire Jean Kuntzmann, Université Grenoble Alpes, Grenoble, France

# A dichotomic Newton-Puiseux algorithm using dynamic evaluation.

Adrien Poteaux

Puiseux series (generalisation of Taylor series above critical points) are a fundamental object in the theory of plane algebraic curves [5]. This talk will focus on the arithmetic complexity of the well-known Newton Puiseux algorithm and its variants. Denoted $D$ the total degree of the input bivariate polynomial, Duval proved a $\mathcal{O}(D^8)$ complexity result [1]. This has been improved to $\tilde{\mathcal{O}}(D^5)$ in [2] by truncating powers of $X$ during the computation and introducing fast multiplication.

After providing the tools of the Newton-Puiseux algorithm and recall the improvments in [2], we will first present results of [3] that enable to reduce the total number of recursive calls of the algorithm from $\mathcal{O}(D^2)$ to $\tilde{\mathcal{O}}(D)$, leading to a complexity in $\tilde{\mathcal{O}}(D^4)$. Finally, we will present a new divide and conquer algorithm that reduces the complexity to $\tilde{\mathcal{O}}(D^3)$ [4].

This work begun during my PhD, under the supervision of Marc Rybowicz ; the recent ameliorations started from a collaboration with Marc in 2011, that led to [3]. The new divide and conquer algorithm [4] is a collaboration with Martin Weimann. This paper is dedicated to Marc Rybowicz, who sadly passed away in November 2016

## Références

[1] D. Duval. Rational Puiseux Expansions. *Compositio Mathematica*, 70 :119–154, 1989.

[2] Adrien Poteaux. *Calcul de développements de Puiseux et application au calcul de groupe de monodromie d'une courbe algébrique plane*. PhD thesis, Université de Limoges, 2008.

[3] A. Poteaux & M. Rybowicz *Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields*. ISSAC 2015.

[4] A. Poteaux & M. Weimann *A dichotomic Newton-Puiseux algorithm using dynamic evaluation*. arXiv :1708.09067.

[5] R. J. Walker. *Algebraic Curves*. Springer-Verlag, 1950.

# Une implémentation de la multiplication rapide des polynômes binaires

Robin Larrieu
Travail en commun avec Joris van der Hoeven et Grégoire Lecerf
Laboratoire d'informatique de l'École polytechnique (LIX)

La multiplication efficace des polynômes dans le corps fini $\mathbb{F}_2$ est un problème fondamental en informatique, avec plusieurs applications pour les codes correcteurs et en cryptographie. Le but de cet exposé est de présenter une solution efficace en pratique pour de grands degrés [5].

Notre implémentation se base sur l'arithmétique efficace dans le corps $\mathbb{F}_{2^{60}}$ [3], mais améliore la librairie précédente grâce à un nouvel algorithme ; plus précisément une variante du *Frobenius FFT* [4]. Ceci permet d'éviter presque entièrement le surcoût lié au travail dans une extension de corps. On arrive ainsi à gagner un facteur 2 par rapport aux librairies de référence [1, 2, 3].

**Article détaillé :** `https://hal.archives-ouvertes.fr/hal-01579863`

**Code source :** Disponible sur le serveur SVN `https://gforge.inria.fr/projects/mmx/` (révision 10681), dans la librairie JUSTINLINE

## Références

[1] R. P. Brent, P. Gaudry, E. Thomé, et P. Zimmermann. Faster multiplication in GF(2)[$x$]. In A. van der Poorten and A. Stein, editors, *Algorithmic Number Theory*, volume 5011 of *Lect. Notes Comput. Sci.*, pages 153–166. Springer Berlin Heidelberg, 2008.

[2] Ming-Shing Chen, Chen-Mou Cheng, Po-Chun Kuo, Wen-Ding Li, et Bo-Yin Yang. Faster multiplication for long binary polynomials. `https://arxiv.org/abs/1708.09746`, 2017.

[3] D. Harvey, J. van der Hoeven, et G. Lecerf. Fast polynomial multiplication over $\mathbb{F}_{2^{60}}$. In M. Rosenkranz, editor, *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 255–262. ACM, 2016.

[4] J. van der Hoeven et R. Larrieu. The Frobenius FFT. In M. Burr, editor, *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 437–444. ACM, 2017.

[5] J. van der Hoeven, R. Larrieu et G. Lecerf. Implementing fast carryless multiplication.. `https://hal.archives-ouvertes.fr/hal-01579863`. Accepté à MACIS 2017.

# Variations autour d'un théorème de Christol

Xavier Caruso

Un célèbre théorème de Christol affirme qu'une série à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ est algébrique sur $\mathbb{Z}/p\mathbb{Z}(x)$ si et seulement si la suite de ses coefficients est $p$-automatique.

L'objectif de cet exposé sera de raconter de jolies mathématiques en lien de ce théorème. Je commencerai par esquisser trois démonstrations différentes de ce résultat, chacune d'entre elles mettant en avant soit des méthodes plutôt analytiques, soit des méthodes plutôt géométriques, soit enfin des méthodes algébriques.

Je présenterai ensuite une question algorithmique directement inspirée par le théorème de Christol, puis expliquerai comment la résoudre de manière efficace en mêlant au mieux les divers ingrédients que l'on a vu apparaître dans chacune des trois démonstrations précédentes.

(Travail en commun avec A. Bostan, G. Christol et Ph. Dumas.)

# A pseudo-matrix approach to Prüfer domains

Gema M. Díaz-Toca* Henri Lombardi†

**Abstract**

In this extended abstract, we present the tools in order to construct an algorithm for computing the Hermite normal form of pseudo-matrices over Prüfer domains. This algorithm allows us to provide constructive proofs of the main theoretical results on finitely presented modules over Prüfer domains and to discuss the resolution of linear systems. We generalize the methodology developed by Henri Cohen for Dedekind domains in [Cohen, Chapter 1]. Finally, we present some results for Prüfer domains of dimension one. A full paper is found on `http://arxiv.org/abs/1508.00345`.

## Introduction

The algorithmic solution of linear systems over fields or over PIDs is classical and it is equivalent to transforming the system via elementary manipulations (and Bezout manipulations for PIDs), in order to obtain a convenient reduced form (Hermite normal form or Smith normal form).

We use here a generalization of this kind of process for arbitrary Prüfer domains.

We adapt for an arbitrary Prüfer domain the generalized matrix computations given by Henri Cohen [Cohen, Chapter 1] for the algorithmics in rings of number fields (number rings).

We obtain a system of generalized matrix computations and as consequences the main "abstract" theorems for Prüfer domains. The generalization consists in replacing when necessary matrices over usual bases by matrices over decompositions of the modules as direct sums of rank one projective modules. These new matrices are called pseudo-matrices.

From a Computer Algebra viewpoint, computing with pseudo-matrices allows us to treat some examples inaccessible for usual methods: since our true computational tool is the inversion of finitely generated ideals, it is possible to work with number rings whose discriminant has no known complete factorization.

For Dedekind domains, and more generally for dimension one Prüfer domains, we obtain more precise results, similar to Smith reduction of usual matrices in PIDs.

General references for the constructive theory of Prüfer domains are found in [ACMC, CACM, Modules]. Many useful constructive proofs are also found in [MRR].

*Departamento de Matemática Aplicada, Universidad de Murcia, 30100 Murcia, Spain. `gemadiaz@um.es`

†Laboratoire de Mathématiques, Université de Franche-Comté, 25030 Besançon, France `henri.lombardi@univ-fcomte.fr`

# 1 Basic facts

## 1.1 Definitions

A ring $\mathbf{A}$ is ***zero-dimensional*** when

$$\forall a \in \mathbf{A},\ \exists n \in \mathbb{N}\ \exists x \in \mathbf{A},\ x^n(1-ax)=0.$$

An integral domain $\mathbf{A}$ is ***of (Krull) dimension*** $\leqslant 1$ if for all $b \neq 0$ in $\mathbf{A}$, the quotient ring $\mathbf{A}/\langle b\rangle$ est zero-dimensional. E.g. number rings have dimension 1 because their quotients are finite, and consequently zero-dimensional.

Over an arbitrary ring $\mathbf{A}$ a finitely generated ideal $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ is ***locally principal*** if there exists $s_1, \ldots, s_n \in \mathbf{A}$ such that $\sum_{i\in[\![1..n]\!]} s_i = 1$ and $s_i\mathfrak{a} \subseteq \langle a_i\rangle$ for each $s_i$.

A ring $\mathbf{A}$ is ***arithmetic*** if all finitely generated ideals are locally principal.

A finitely generated ideal $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ is ***invertible*** if there exists a regular element $c$ and an finitely generated ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \langle c\rangle$. Il other words, $\mathfrak{a}$ is locally principal an contains a regular element.

A ***Prüfer domain*** is an integral arithmetic ring. In other words, it is an integral domain whose all nonzero finitely generated ideal are invertible.

The ***determinantal ideal of order*** $k$ of a matrix $M$ is the ideal $\mathfrak{D}_k(M)$ generated by the minors of order $k$ of $M$.

The ***Fitting ideal of order*** $k$ of a finitely presented module $P$, coker of a matrix $M \in \mathbb{M}_{n,m}(\mathbf{A})$ is defined by $\mathfrak{F}_k(P) := \mathfrak{D}_{n-k}(M)$.

## 1.2 Computations with finitely generated ideals in a Prüfer domain

We work with an explicit Prüfer domain $\mathbf{Z}$. This means that for an arbitrary finitely generated ideal $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle$ we have an algorithm that computes $s_1, \ldots, s_n \in \mathbf{Z}$ such that $\sum_i s_i = 1$ and $s_i\mathfrak{a} \subseteq \langle a_i\rangle$ for each $s_i$. E.g. number rings are explicit Prüfer domains. We assume also that $\mathbf{Z}$ has a divisbility test, giving an $x$ s.t. $ax = b$ when the test gives the answer "Yes" to the question "does $a$ divise $b$?".

From these basic algorithms the following computations are shown to be easy. Note that by "computing an ideal", we mean to compute a generator set and a list $(s_1, \ldots, s_n)$ as in the previous explanation.

- For $\mathfrak{a}$ finitely generated, compute an ideal $\mathfrak{b}$ s.t. $\mathfrak{ab}$ is principal.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, compute $s$, $t$ s.t. $s + t = 1$, $s\mathfrak{a} \subseteq \mathfrak{b}$ and $t\mathfrak{b} \subseteq \mathfrak{a}$.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, compute $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{ab}$, $\mathfrak{a} \cap \mathfrak{b}$ and $(\mathfrak{a} : \mathfrak{b})$.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, test if $\mathfrak{a} \subseteq \mathfrak{b}$.

The following computations are more tricky. We assume that $\mathbf{Z}$ is moreover explicitly of dimension 1.

- For $\mathfrak{a}$ finitely generated and $a$ nonzero in $\mathfrak{a}$, compute $b \in \mathfrak{a}$ s.t. $\mathfrak{a} = \langle a, b \rangle$.
- For $\mathfrak{a}$ and $\mathfrak{b}$ finitely generated, compute an isomorphism between the modules $\mathfrak{a} \oplus \mathfrak{b}$ and $\mathbf{Z} \oplus \mathfrak{a}\mathfrak{b}$.

## 2 Pseudo-bases and pseudo-matrices

We note $\mathbf{K}$ the quotient field of $\mathbf{Z}$ and $\mathrm{Gfr}(\mathbf{Z})$ the (multiplicative) group of ***fractional ideals*** of $\mathbf{K}$. Such a fractional ideal is a sub-$\mathbf{Z}$-module of $\mathbf{K}$ equal to $\frac{\mathfrak{a}}{c}$ for a (usual) finitely generated ideal $\mathfrak{a} \subseteq \mathbf{Z}$ and $c$ nonzero in $\mathbf{Z}$. A $\mathbf{Z}$-module $E$ which is finitely generated and without torsion can be viewed as a sub-$\mathbf{Z}$-module of the $\mathbf{K}$-vector space $E' = \mathbf{K} \otimes_{\mathbf{Z}} E$.

A finitely generated projective $\mathbf{Z}$-module $E$ can always be given as a direct sum $E = E_1 \oplus \cdots \oplus E_r$ with isomorphisms $E_i \simeq \mathfrak{e}_i \in \mathrm{Gfr}(\mathbf{A})$: $\mathfrak{e}_i \ni x \mapsto xe_i$ (where $e_i \in E'$). A ***pseudo-basis*** of $E$ is by definition an $r$-tuple

$$\boxed{\big((e_1, \mathfrak{e}_1), \ldots, (e_r, \mathfrak{e}_r)\big)} \text{ s.t. } E = \mathfrak{e}_1 e_1 \oplus \cdots \oplus \mathfrak{e}_r e_r,$$

Note that $(e_1, \ldots, e_r)$ is a basis of the vector space $E'$.

Let $\varphi : E \to H$ a linear map between projective modules with pseudo-bases

$$\mathscr{E} = \big((e_1, \mathfrak{e}_1), \ldots, (e_m, \mathfrak{e}_m)\big) \text{ and } \mathscr{H} = \big((h_1, \mathfrak{h}_1), \ldots, (h_n, \mathfrak{h}_n)\big).$$

Extending the scalars to $\mathbf{K}$ we get a linear map $\varphi' : E' \to H'$ with a matrix $\underline{A}$ over the $\mathbf{K}$-bases $(e_1, \ldots, e_m)$ and $(h_1, \ldots, h_n)$.

- We call ***matrix of $\varphi$ over pseudo-bases $\mathcal{E}$ and $\mathcal{H}$*** the data

  $$A = (\mathfrak{h}_1, \ldots, \mathfrak{h}_n; \mathfrak{e}_1, \ldots, \mathfrak{e}_m; \underline{A}) = (\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A}), \text{ where } \underline{A} = (a_{ij})_{ij} \in \mathbb{M}_{n,m}(\mathbf{K}).$$

  We have the inclusions $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$. We note $\boxed{A = \mathscr{M}_{\mathcal{E},\mathcal{H}}(\varphi)}$.

intuitive visualization:

$$A = \begin{array}{c} \\ \mathfrak{h}_1 \\ \mathfrak{h}_2 \\ \mathfrak{h}_3 \end{array} \begin{array}{c} \begin{array}{cccc} \mathfrak{e}_1 & \mathfrak{e}_2 & \mathfrak{e}_3 & \mathfrak{e}_4 \end{array} \\ \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix} \end{array} \quad a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i.$$

- We call ***pseudo-matrix*** any data $(\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A})$ of this kind, i.e. with inclusions $a_{ij}\mathfrak{e}_j \subseteq \mathfrak{h}_i$. It can be viewed as the matrix of a $\mathbf{Z}$-linear map between sub-$\mathbf{Z}$-modules of $\mathbf{K}^n$ and $\mathbf{K}^m$.
- For fixed lists $\underline{\mathfrak{e}}$ et $\underline{\mathfrak{h}}$, the corresponding pseudo-matrices define a $\mathbf{Z}$-module $\boxed{\mathbb{M}_{\underline{\mathfrak{h}};\underline{\mathfrak{e}}}(\mathbf{A})}$ (isomorphic to the $\mathbf{Z}$-module of $\mathbf{Z}$-linear maps from $E$ to $H$). The product of pseudo-matrices of convenient formats is defined in the natural way and corresponds to the composition of linear maps.

- For a square pseudo-matrix $A = (\underline{\mathfrak{h}}; \underline{\mathfrak{e}}; \underline{A})$ we define its ***determinant (ideal)*** as being
$$\boxed{\mathbf{Z} \supseteq \mathfrak{Det}(A) := \det(\underline{A})\,\mathfrak{e}\,\mathfrak{h}^{-1}}, \text{ where } \mathfrak{e} = \prod_j \mathfrak{e}_j \text{ and } \mathfrak{h} = \prod_i \mathfrak{h}_i.$$
*A square pseudo-matrix $A$ is invertible if and only if $\mathfrak{Det}(A) = \mathbf{Z}$.* For square pseudo-matrices $A$ and $B$ with convenient formats we have $\mathfrak{Det}(AB) = \mathfrak{Det}(A)\,\mathfrak{Det}(B)$.

- Let $\beta = [\beta_1, \ldots, \beta_r] \subseteq [\![1..n]\!]$ et $\alpha = [\alpha_1, \ldots, \alpha_r] \subseteq [\![1..m]\!]$ subsequences in increasing order. We note $A_{\beta,\alpha}$ the pseudo-matrix extracted on the rows $\beta$ and columns $\alpha$.
$$A_{\beta,\alpha} = (\mathfrak{h}_{\beta_1}, \ldots, \mathfrak{h}_{\beta_r}; \mathfrak{e}_{\alpha_1}, \ldots, \mathfrak{e}_{\alpha_r}, \underline{A}_{\beta,\alpha}).$$
The ideal
$$\mathfrak{m}_{\beta,\alpha}(A) := \mathfrak{Det}(A_{\beta,\alpha}) = \det(\underline{A}_{\beta,\alpha})(\textstyle\prod_{i=0}^{r} \mathfrak{e}_{\alpha_i})(\prod_{j=0}^{r} \mathfrak{h}_{\beta_j})^{-1}$$
is called ***the minor (ideal) of order $r$ of $A$ extracted on rows $\beta$ and columns $\alpha$.***

- For an arbitrary pseudo-matrix and $r \leqslant \inf(m, n)$ the ***determinantal ideal of order $r$ of*** $A$, noted $\mathfrak{D}_r(A)$, is the sum of minors of order $r$ of $A$.
*The pseudo-matrix $A$ represents a surjective linear map if and only if $\mathfrak{D}_n(A) = \mathbf{Z}$.*

- Let $s \in \mathbf{Z}^*$ s.t. the modules $E[1/s]$ and $H[1/s]$ are free over $\mathbf{Z}[1/s]$.
Let $\varphi_s : E[1/s] \to H[1/s]$ the extension of $\varphi$ by $\mathbf{Z} \to \mathbf{Z}[1/s]$.
Then for each $r$ we get $\mathfrak{D}_r(\varphi)\mathbf{Z}[1/s] = \mathfrak{D}_r(\varphi_s)$ (usual determinantal ideals).

- Let $(s_1, \ldots, s_n)$ be comaximal in $\mathbf{Z}$. A linear system $AX = B$ (with pseudo-matrices $A, B, X$) admits a solution in $\mathbf{Z}$ if and only if it admits a solution in each $\mathbf{Z}[1/s_i]$.

# 3 Computations with pseudo-matrices

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two finitely generated ideals of $\mathbf{Z}$ and $M$ be a module with pseudo-basis $\mathcal{E} = \big((e_1, \mathfrak{a}), (e_2, \mathfrak{b})\big)$. If $s + t = 1$, $s\mathfrak{a} \subseteq \mathfrak{b}$ and $t\mathfrak{b} \subseteq \mathfrak{a}$, another pseudo-basis of $M$ is $\mathcal{H} = \big((f_1, \mathfrak{a} + \mathfrak{b}), (f_2, \mathfrak{a} \cap \mathfrak{b})\big)$ where $f_1 = te_1 + se_2$ et $f_2 = -e_1 + e_2$. We get the following "Bezout pseudo-matrix " of change of pseudo-bases from $\mathcal{E}$ to $\mathcal{H}$.
$$B = \mathscr{M}_{\mathcal{H},\mathcal{E}}(\mathrm{Id}_M) = \begin{array}{c} \\ \mathfrak{a} \\ \mathfrak{b} \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{a}+\mathfrak{b} & \mathfrak{a}\cap\mathfrak{b} \end{array} \\ \begin{bmatrix} t & -1 \\ s & 1 \end{bmatrix} \end{array},$$
with inverse
$$\mathscr{M}_{\mathcal{E},\mathcal{H}}(\mathrm{Id}_M) = \begin{array}{c} \\ \mathfrak{a}+\mathfrak{b} \\ \mathfrak{a}\cap\mathfrak{b} \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{a} & \mathfrak{b} \end{array} \\ \begin{bmatrix} 1 & 1 \\ -s & t \end{bmatrix} \end{array}.$$

The Bezout pseudo-matrices and the analogues of Gauss pivoting matrices allow us to compute the reduction of pseudo-matrices to convenient "normal forms", analogous to HNF (Hermite normal form) for Prüfer domains and to SNF (Smith normal form) for Prüfer domains of dimension 1.

For dealing with pseudo-matrices over Prüfer domains of dimension 1 we use an algorithm in some zero-dimensional quotient rings: *a zero-dimensional arithmetic ring is a principal ideal ring and a matrix over it can be reduced to a Smith normal form by elementary row and column manipulations.*

Two kinds of easy consequences of these reductions of pseudo-matrices:

- The general discussion of linear systems over Prüfer domains (coefficients and unknowns in $\mathbf{Z}$)
- Theoretical results on the structure of finitely presented modules, finitely generated projective modules and linear maps between these modules: a finitely generated sub-$\mathbf{Z}$-module of $\mathbf{K}^n$ is finitely generated projective, a finitely generated projective module is a direct sum of rank one projective submodules, the kernel of a linear map between finitely generated projective modules is a direct summand, and so on...

# References


[ACMC] Lombardi H. & Quitté C. *Algèbre Commutative. Méthodes constructives.* Calvage&Mounet (2011).

[CACM] Translated, revised and extended english version of [ACMC]. Springer (2015).

[Cohen] Cohen H. *Advanced topics in computational number theory.* Graduate texts in mathematics 193. Springer-Verlag (1999).

[Modules] Díaz-Toca G.-M., Lombardi H. & Quitté C. *Modules sur les anneaux commutatifs.* Calvage&Mounet (2014).

[MRR] Mines R., Richman F. & Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988).

# Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous

Jérémy Marrez Annick Valibouze Philippe Aubry

La théorie des nombres flous est utilisée dans de nombreux domaines où l'information est incomplète ou imprécise pour modéliser des réalités incertaines. Résoudre des systèmes polynomiaux à coefficients flous est l'un des enjeux majeurs dans le champs de la modélisation incertaine car il s'étend à un large spectre d'applications en sciences, comme l'économie, la médecine et l'ingénierie.

Jusque là, deux catégories différentes de méthodes ont été développées pour résoudre des systèmes de polynômes à coefficients flous, l'une reposant sur des calculs approximés, et l'autre sur des calculs exactes. Dans la première catégorie, on retrouve la méthode de Newton et ses extensions comme les réseaux de neurones et d'autres méthodes itératives [1, 2, 5]. Cependant, les résultats de ces approches numériques sont difficiles à évaluer.

Pour faire face à ces problèmes, une autre catégorie de méthodes basées sur du calcul formel a été développée récemment. Contrairement à l'approche numérique, ces techniques algébriques produisent un résultat exact. Nous nous intéressons ici à une nouvelle approche [4] pour résoudre des systèmes de polynômes du type :

$$AX + B = CX + D \tag{1}$$

où $X$ est un vecteur de variables réelles, et $A, B, C, D$ sont des matrices floues, avec la particularité qu'un nombre flou en général n'a pas d'inverse pour l'opération d'addition.

L'idée principale de cette approche est dans un premier temps de convertir le système (1) en un système paramétrique, c'est-à-dire en faisant intervenir la représentation paramétrique des nombres flous. Car si les coefficients sont flous, leur représentation elle, est formelle, ce qui nous permet d'aborder cette représentation dans certain cas. Elle a été étudiée dans le cas des nombres flous dits triangulaires [7, 4] et nous l'étendons ici à celui des nombres flous dits quadratiques. Pour les nombres flous triangulaires, la conversion en système paramétrique donnera 2 fois plus d'équations et un paramètre $r$.

Ce nouveau système est converti en un système avec une variable de moins appelé le système tranché collecté (collected crisp system). Sur ce nouveau système d'équations intermédiaires, nous utilisons l'algorithme de décomposition triangulaire de Wu Wen Tsun qui nous amène à des systèmes triangulaires fa-

ciles à résoudre [3]. Toutes les solutions peuvent être obtenues simultanément. De plus, il n'est pas nécessaire d'isoler les solutions en fonction de la valeur du paramètre $r$. La variété du système tranché collecté est alors calculée. Cette variété est composée de toutes les solutions exactes du système (1).

La présentation du sujet pourra s'organiser comme suit. Dans un premier temps, la théorie des nombres flous est présentée. Puis les notions de bases nécessaires à l'algorithme de décomposition triangulaire de Wu Wen Tsun sont rappelées et cet algorithme de résolution algébrique de systèmes d'équations polynomiales est introduit. Ensuite, nous nous concentrons sur le passage du flou à l'algébrique pour pouvoir utiliser la méthode de Wu. La procédure principale de résolution de ces systèmes d'équations peut alors être déroulée. Pour finir, nous présentons la bibliothèque Fuzzy résultant de ce travail [6] avec des exemples, et des tests réalisés par son biais. Cette bibliothèque implantée en SageMath basé sur Python décrit l'arithmétique sur les nombres flous et la méthode algébrique de résolution des systèmes de polynômes à coefficients flous.

# Références


[1] Saeid Abbasbandy and B Asady. Newton's method for solving fuzzy nonlinear equations. *Applied Mathematics and Computation*, 159(2) :349–356, 2004.

[2] Saeid Abbasbandy and Mahmood Otadi. Numerical solution of fuzzy polynomials by fuzzy neural network. *Applied Mathematics and Computation*, 181(2) :1084–1089, 2006.

[3] Philippe Aubry. *Ensembles triangulaires de polynomes et resolution de systemes algebriques. Implantation en axiom.* 1999.

[4] Marziyeh Boroujeni, Abdolali Basiri, Sajjad Rahmany, and Annick Valibouze. Finding solutions of fuzzy polynomial equations systems by an algebraic method. *Journal of Intelligent & Fuzzy Systems*, 30(2) :791–800, 2016.

[5] James J Buckley, Thomas Feuring, and Yoichi Hayashi. Solving fuzzy equations using evolutionary algorithms and neural nets. *Soft Computing*, 6(2) :116–123, 2002.

[6] Jeremy Marrez. Étude et implantation d'une méthode algébrique pour résoudre des systèmes à coefficients flous. Master's thesis, UPMC - Pierre and Marie Curie University, France, 2016.

[7] Luciano Stefanini and Laerte Sorini. Fuzzy arithmetic with parametric lr fuzzy numbers. In *IFSA/EUSFLAT Conf.*, pages 600–605, 2009.

# Conversions simultanées entre représentation classique et modulaire à l'aide d'algèbre linéaire

Javad Doliskani Pascal Giorgi Romain Lebreton
Éric Schost

Le système modulaire de représentation des entiers est très utilisé, notamment de par sa capacité à réduire des calculs sur de grandes valeurs à des calculs menés en parallèle sur des nombres de taille choisie. Nous présentons un nouvel algorithme de conversion de représentation d'entiers entre le système positionnel classique et le système modulaire. Cet algorithme ramène le gros des calculs de conversion à de l'algèbre linéaire sur des mots machines.

Notre algorithme est naturellement conçu pour convertir simultanément un certain nombre d'entiers. Dans ce cas, sa complexité théorique améliore celle des méthodes naïves sans toutefois atteindre la quasi-linéarité des algorithmes rapides. Mais c'est en pratique que notre algorithme tire le mieux son épingle du jeu : parce qu'il bénéficie des implémentations optimisées d'algèbre linéaire, notre programme fournit le meilleur temps de calcul des algorithmes de conversions pour une large plage intermédiaire de taille de matrice et d'entiers.

La principale application de notre algorithme est la multiplication de matrices à coefficients entiers. Nos expériences montrent des améliorations de temps de calculs pour une large plage intermédiaire de taille de matrice et d'entiers.

# Finding ECM-friendly curves - A Galois approach

Sudarshan Shinde

The elliptic curve method (ECM) is a factorization algorithm widely used in cryptography. It was proposed in 1985 by Lenstra and improved a couple of months later by Montgomery using well-chosen curves. In order to compare different families of curves, he associated to each elliptic curve $E$ and prime $l$, the mean valuation of $l$ in the cardinality of $E$ modulo random primes. More precisely, we set $\overline{v_l} = \mathbb{E}(v_l(\#(E(\mathbb{F}_p))))$ where the expectation is with respect to random primes $p$.

Montgomery increased $\overline{v_l}$ by forcing curves to have $l$-torsion points over $\mathbb{Q}$. Brier and Clavier further increased $\overline{v_2}$ by imposing torsion points over $\mathbb{Q}(i)$. In 2012, Barbulescu et al (cf [1]) produced families of elliptic curves with better mean valuation without adding any torsion points on $\mathbb{Q}(i)$. Moreover, they showed that it is impossible to change $\overline{v_l}$ without changing the degree of the $l$-torsion field, which has a generic value (cf [2]) in the sense in which the Galois group of an irreducible polynomial of degree $n$ is generically $\mathcal{S}_n$.

In this talk we search families of elliptic curves with a larger valuation for $l = 2$ and $l = 3$ which boils down to searching families with non-generic Galois groups. Initially, we considered the method of Lagrange resolvant but this is not feasible for our polynomials of interest : the degree of division polynomials is quadratic in $l$.

We then present two algorithms which produce a system of polynomial equations characterising every subfamily of elliptic curves having non-generic $\overline{v_3}$ and every subfamily of Montgomery curves having non-generic $\overline{v_2}$.

## Références

[1] Razvan Barbulescu, Joppe Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter Montgomery. Finding ecm-friendly curves through a study of galois properties. *The Open Book Series*, 1(1) :63–86, 2013.

[2] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4) :259–331, 1971.

# Comptage de points de courbes hyperelliptiques en genre 3 et au-delà, théorie et pratique.

Simon Abelard

Le comptage de points d'une courbe algébrique définie sur un corps fini est une primitive essentielle en théorie des nombres, avec des applications en cryptographie, en géométrie arithmétique et pour les codes correcteurs. Étant donné un polynôme bivarié $F \in \mathbb{F}_{p^n}[x, y]$, il s'agit de calculer une série génératrice rationelle associée au nombre de solutions de $F(x, y) = 0$ sur $\mathbb{F}_{p^n}$, $\mathbb{F}_{p^{2n}}$, $\mathbb{F}_{p^{3n}}$, etc. Nous nous intéressons en particulier au cas des courbes hyperelliptiques (i.e. $F(x, y) = y^2 - f(x)$, avec $f$ sans facteur carré) définies sur un corps fini de grande caractéristique. Avec une complexité polynomiale en $\log p$, les algorithmes dérivés de ceux de Schoof [4] et de Pila [3] sont actuellement les plus adaptés pour ce cas de figure. Ils sont d'ailleurs utilisés en genre 1 et 2 pour construire des courbes cryptographiquement sûres. En revanche, la dépendance de leur complexité en le genre $g$ de la courbe est exponentielle, ce qui constitue un obstacle sérieux à l'emploi de ces algorithmes en genre 3 et au-delà.

Du côté théorique, nous nous sommes intéressé à cette dépendance en $g$ et nous avons proposé un algorithme de comptage de points sur des courbes hyperelliptiques dont la complexité est en $f(g)(\log q)^{O(g)}$, avec $f$ une fonction ne dépendant que de $g$, à comparer avec la borne en $(\log q)^{O(g^2)}$ établie dans [1].

L'étape essentielle des algorithmes à la Schoof-Pila consiste à obtenir une représentation efficace de la $\ell$-torsion de la jacobienne de la courbe, afin de réduire au maximum le coût des opérations dans cet espace. Pour ce faire, on décrit la $\ell$-torsion par un système polynomial dont on va ensuite calculer une résolution géométrique. La clé de voûte de notre résultat est que le système est construit de telle sorte qu'il possède naturellement une structure multihomogène qui diminue grandement la complexité d'un tel calcul.

Du côté pratique, la dépendance exponentielle se fait cruellement sentir dès le genre 3, d'où l'intérêt de commencer à étudier le cas d'une sous-famille de courbes dites à multiplication réelle, déjà traité en genre 2 dans [2]. Ces courbes sont munies d'une structure particulière qui permet essentiellement de découper la $\ell$-torsion en somme directe de trois sous-espaces plus petits, qui sont des noyaux de certains endomorphismes. On cherche alors non plus à modéliser directement la $\ell$-torsion, c'est-à-dire le noyau de la multiplication par $\ell$, mais les noyaux des endomorphismes en lesquels $\ell$ se factorise. Cela permet de diminuer fortement les degrés des systèmes polynomiaux, en ne modifiant que très légèrement la modélisation par rapport au cas général. In fine, la structure additionnelle des courbes à multiplication réelle nous permet d'obtenir un algorithme de comptage de points de complexité $\widetilde{O}((n \log p)^6)$.

Travail en commun avec Pierrick Gaudry et Pierre-Jean Spaenlehauer.

## Références


[1] L. M. Adleman and M.-D. Huang. Counting points on curves and Abelian varieties over finite fields. *Journal of Symbolic Computation*, 32(3) :171–189, 2001.

[2] P. Gaudry, D. R. Kohel, and B. A. Smith. Counting points on genus 2 curves with real multiplication. In *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 504–519. Springer, 2011.

[3] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192) :745–763, 1990.

[4] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170) :483–494, 1985.

# Autour de l'arborification et de ses applications

Jordy Palafox

Les structures arborescentes et séries formelles sur des arbres/forêts apparaissent dans de nombreux domaines des mathématiques, en analyse numérique dès les travaux de Butcher sur les shémas de Runge-Kutta (voir [2]), en systèmes dynamiques pour la linéarisation de champs de vecteurs analytiques (voir [5]) ou encore en calcul stochastique avec les équations différentielles conduites par un signal rugueux (voir [6]) ou les équations aux dérivées partielles stochastiques (voir [1]).

Dans les années 70, Jean Ecalle introduit pour des problèmes de normalisation des champs de vecteurs ou difféomorphismes analytiques locaux, le formalisme des moules et la méthode d'arborification (voir [4], [3]). Le formalisme des moules permet d'extraire des coefficients universels des séries formelles normalisantes et la technique d'arborifcation permet de démontrer leur convergence en présence de petits diviseurs.

Dans cet exposé, nous donnerons une présentation de la méthode d'arborification et de ses diverses propriétés. Nous l'illustrerons dans un premier temps sur le théorème de Bruyno de linéarisation analytique des champs de vecteurs vérifiant une condition arithmétique de Bruyno. Nous montrerons aussi comment cette méthode permet de retrouver les résultats de Butcher en analyse numérique et son rôle dans l'étude des équations différentielles stochastiques.

## Références

[1] Y.Bruned, M.Hairer, L.Zambotti, *Algebraic renormalization of regularity structures*, Arxiv préprint : `https://arxiv.org/pdf/1610.08468v2.pdf`, 2017.

[2] J.C.Butcher, *Numerical methods for Ordinary Differential Equations*, Third Edition, Wiley, 2016.

[3] J.Cresson, D.Manchon, J.Palafox, *Arborifcation, invariance and convergence of normalizing series*, 27p., préprint, 2017.

[4] J.Ecalle, *Singularités non abordables par la géométrie*, Ann.Inst.Fourier, 42(1-2),73-164, 1992.

[5] J.Ecalle et B.Vallet, *Correction and linearization of resonant vector fields and diffeomorphisms*, Math..Z., 229 :249-318, 1998.

[6] M.Gubinelli, *Ramification of rough paths*, Journal of Differential Equations 248, no.4,693-721, 2010.

# A propos d'un groupe d'associateurs

Hoang Ngoc Minh

Partant de l'équation $KZ_3$, *i.e.* l'équation différentielle fuchsienne d'ordre 1 avec les singularités régulières dans $\{0, 1, +\infty\}$ suivante (sans condition initiale) et en les indéterminées non commutatives $\{x_0, x_1\}$ $(= X)$ [3, 5] :

$$(DE) \quad dG = (x_0\omega_0 + x_1\omega_1)G \quad \text{avec} \quad \omega_0(z) = \frac{dz}{z}, \omega_1(z) = \frac{dz}{1-z}$$

et également de son groupe Galois différentiel, *i.e.* le groupe suivant [7]

$$\mathrm{Gal}_{\mathbb{C}}(DE) = \{e^C | C \in \mathcal{L}ie_{\mathbb{C}}\langle\langle X\rangle\rangle\},$$

nous décrivons un groupe d'associateurs contenant l'*associateur de Drinfel'd*, noté $\Phi_{KZ}$, [3, 5] (déterminé de façon unique par cette équation différentielle et des conditions asymptotiques), *i.e.* le groupe suivant [8].

$$\begin{aligned} dm(A) &= \{\Phi_{KZ}e^C | C \in \mathcal{L}ie_A\langle\langle X\rangle\rangle, \langle e^C \mid x_0\rangle = \langle e^C \mid x_1\rangle = 0\} \\ &= \mathrm{Gal}_A^{\geq 2}(DE), \end{aligned}$$

où $A$ est un anneau commutatif contenant $\mathbb{Q}$

Ce groupe $dm(A)$ contient le groupe $DM(A)$ introduit dans [3, 9], *i.e.* et défini par les conditions suivantes : $\Phi \in DM(A)$ si et seulement si

$$\langle \Phi \mid 1_{X^*}\rangle = 1, \quad \langle \Phi \mid x_0\rangle = \langle \Phi \mid x_1\rangle = 0, \quad \Delta_{\sqcup\!\sqcup}\Phi = \Phi \otimes \Phi$$

et, pour tout

$$\Psi = \exp\left(-\sum_{n\geq 2}\langle \pi_Y\Phi \mid y_n\rangle \frac{(-y_1)^n}{n}\right)\pi_Y\Phi \in A\langle\langle Y\rangle\rangle,$$

on a

$$\Delta_{\sqcup\!\sqcup}\Psi = \Psi \otimes \Psi \quad \text{et} \quad \langle \Psi \mid 1_{Y^*}\rangle = 1,$$

$Y$ étant l'aphabet $\{y_k\}_{k\geq 1}$ et $\pi_Y$ est le morphisme de $(\mathbb{C}\langle\langle X\rangle\rangle x_1, ., 1_{X^*})$ dans $(\mathbb{C}\langle\langle Y\rangle\rangle, ., 1_{Y^*})$ défini par

$$\pi_Y x_0^{s_1-1}x_1 \ldots x_0^{s_r-1}x_1 \longmapsto y_{s_1}\ldots y_{s_r}.$$

Nous exhibons également des exemples, non triviaux, de candidats associateurs à coefficients rationnels en régularisant des polyzêtas indexés par des multiindices entiers négatifs [6]. Ces derniers sont des intégrales itérées divergentes, sur $\omega_0, \omega_1$ dans $\Omega = \widetilde{\mathbb{C} \setminus \{0, 1\}}$, et associées à une sous-classe de séries rationnelles en les indeterminées non commutatives dans $X$ et à coefficients complexes [1].

Notons que chaque élément de la forme $\Phi = \Phi_{KZ} e^C$, avec $e^C \in \mathrm{Gal}_{\mathbb{C}}(DE)$, régularise une solution $\bar{\mathrm{L}} \in \mathcal{H}(\Omega)\langle\langle X\rangle\rangle$ de $(DE)$ vérifiant

$$\bar{\mathrm{L}}(z) \sim_0 e^{x_0 \log(z)} e^C \quad \text{et} \quad \bar{\mathrm{L}}(z) \sim_1 e^{-x_1 \log(1-z)} \Phi.$$

En plus, en définissant la série $\Psi \in \mathbb{C}\langle\langle Y\rangle\rangle$ comme suit [8]

$$\forall w \in X^* x_1, \quad \langle \Psi \mid \pi_Y w\rangle = \mathrm{p.f.}_{n\to+\infty} \langle\langle \Phi \mid w\rangle \mid n\rangle, \quad \{n^a \log^b(n)\}_{a\in\mathbb{Z}, b\in\mathbb{N}},$$

les séries $\Phi, \Psi$ vérifient l'identité suivant [4, 8]

$$\prod_{l\in\mathcal{L}ynY}^{\searrow} e^{\langle\Psi|\Sigma_l\rangle\Pi_l} = \exp\left(\gamma y_1 - \sum_{k\geq 2} \zeta(y_k)\frac{(-y_1)^k}{k}\right) \pi_Y \prod_{l\in\mathcal{L}ynX}^{\searrow} e^{\langle\Phi|S_l\rangle P_l},$$

où [8, 10]

- $\mathcal{L}ynX$ (resp. $\mathcal{L}ynY$) est l'ensemble des mots de Lyndon sur $X$ (resp. $Y$),
- $\{S_l\}_{l\in\mathcal{L}ynX}$ (resp. $\{\Sigma_l\}_{l\in\mathcal{L}ynY}$) une base de transcendance pure de l'algèbre $(\mathbb{C}\langle X\rangle, \sqcup\!\sqcup, 1_{X^*})$ (resp. $(\mathbb{C}\langle Y\rangle, \text{⧢}, 1_{Y^*})$),
- $\{P_l\}_{l\in\mathcal{L}ynX}$ (resp. $\{\Pi_l\}_{l\in\mathcal{L}ynY}$) une base de l'algèbre de Lie des éléments primitifs du bigèbre $(\mathbb{C}\langle X\rangle, ., 1_{X^*}, \Delta_{\sqcup\!\sqcup})$ (resp. $(\mathbb{C}\langle Y\rangle, ., 1_{Y^*}, \Delta_{\text{⧢}})$).

En identifiant les coordonnées locales dans cette identié, on obtient un système de relations polynomiales, homogènes en poids, entres les polyzêtas convergents $\{\zeta(S_l)\}_{l\in\mathcal{L}ynX-X}$ (resp. $\{\zeta(\Sigma_l)\}_{l\in\mathcal{L}ynY-\{y_1\}}$) [2, 8].

# Références


[1] J. Berstel & C. Reutenauer.– *Rational series and their languages*, Springer-Verlag, 1988.

[2] V.C. Bui, G.H.E. Duchamp, Hoang Ngoc Minh.– *Structure of Polyzetas and Explicit Representation on Transcendence Bases of Shuffle and Stuffle Algebras*, dans Journal of Symbolic Computation, Volume 83, November–December 2017, Pages 93-111.

[3] P. Cartier– *Fonctions polylogarithmes, nombres polyzetas et groupes prounipotents*– Séminaire BOURBAKI, 53ème, $n°$885, 2000-2001.

[4] Costermans C., Hoang Ngoc Minh.– *Noncommutative algebra, multiple harmonic sums and applications in discrete probability*, J. of Sym. Comp. (2009), 801-817.

[5] V. Drinfel'd– *On quasitriangular quasi-hopf algebra and a group closely connected with Gal($\bar{\mathbb{Q}}/\mathbb{Q}$)*, Leningrad Math. J., 4, 829-860, 1991.

[6] G.H.E. Duchamp, Hoang Ngoc Minh, Q.H. Ngo, *Harmonic sums and polylogarithms at negative multi-indices*, Journal of Symbolic Computation, **83**, 166-186 (2017).

[7] Hoang Ngoc Minh.– Differential Galois groups and noncommutative generating series of polylogarithms, *Automata, Combinatorics & Geometry*, World Multi-conf. on Systemics, Cybernetics & Informatics, Florida, 2003.

[8] Hoang Ngoc Minh.– *On a conjecture by Pierre Cartier about a group of associators*, Acta Math. Vietnamica (2013), 38, Issue 3, 339-398.

[9] G. Racinet.– *Séries génératrices non-commutatives de polyzêtas et associateurs de Drinfel'd*, thèse, Amiens, 2000.

[10] Reutenauer C.– *Free Lie Algebras*, London Math. Soc. Monographs (1993).

# Équations d'évolution et calcul différentiel non commutatifs

Gérard H. E. Duchamp

Nous construisons un calcul différentiel sur les séries non commutatives à coefficients variables [3]. Ce "calculus" est suffisament puissant pour rendre compte des intégrales itérées[7, 2], de l'unicité de leurs solutions avec condition asymptotique (comme celle de Drinfeld pour les polylogarithmes [4, 1]) et pour les construire explicitement [6], les factoriser ainsi que pour établir des algorithmes efficaces sur l'espace des coordonnées et pour donner un cadre effectif aux intégrales de Dyson [5]. Nous donnerons des exemples explicites de ces calculs.

Cet exposé (qui est complémentaire de celui de Hoang Nhoc Minh) s'inscrit dans le projet (maths-info-physique)

Evolution Equations in Combinatorics and Physics.

## Références

[1] P. Cartier–*Jacobiennes généralisées, monodromie unipotente et intégrales itérées*, Séminaire Bourbaki, Volume 30 (1987-1988) , Talk no. 687 , p. 31-52

[2] P. Deligne–*Equations Différentielles à Points Singuliers Réguliers*, Lecture Notes in Math, 163, Springer-Verlag (1970).

[3] M. Deneufchâtel, G. H. E. Duchamp, Hoang Ngoc Minh and A. I. Solomon, Independence of Hyperlogarithms over Function Fields via Algebraic Combinatorics, 4th International Conference on Algebraic Informatics, Linz (2011). Proceedings, Lecture Notes in Computer Science, 6742, Springer.

[4] V. Drinfel'd–*On quasitriangular quasi-hopf algebra and a group closely connected with Gal($\bar{\mathbb{Q}}/\mathbb{Q}$)*, Leningrad Math. J., 4, 829-860, 1991.

[5] G.H.E Duchamp, Hoang Ngoc Minh, Ngo Quoc Hoan, K. A. Penson, P. Simonnet– *Mathematical renormalization in QED via noncommutative generating series*, Springer Proceedings in Mathematics & Statistics, 198, Chapter 6, pp. 59-100, Kotsireas and Martinez- Moro(Eds) : APPLICATIONS OF COMPUTER ALGEBRA, 2017.

[6] Hoang Ngoc Minh, M. Petitot and J. Van der Hoeven.– Polylogarithms and Shuffle Algebra, *Proceedings of FPSAC'98*, 1998.

[7] H. J. Susmann–*A product expansion for Chen Series*, in Theory and Applications of Nonlinear Control Systems, C.I. Byrns and Lindquist (eds). 323-335, 1986.