Résumés des exposés courts

Journées Nationales de Calcul Formel 2014

CIRM, Luminy, Marseille

3-7 Novembre 2014

Liste des exposés

1. Algorithme de optimisation polynomiale en utilisant de bases de bord

Marta Abril Bucero, Bernard Mourrain
INRIA Sophia Méditerranée
BP 93, 06902 Sophia Antipolis, France
{Marta.Abril_Bucero,Bernard.Mourrain}@inria.fr

Computing the global minimum of a polynomial function f on a semi-algebraic set is a difficult but important problem, with many applications. A relaxation approach was proposed in [6] which approximates this problem by a sequence of finite dimensional convex optimization problems. These optimization problems can be formulated in terms of linear matrix inequalities on moment matrices associated to the set of monomials of degree $\leq t \in \mathbb{N}$ for increasing values of t. They can be solved by Semi-Definite Programming (SDP) techniques. The sequence of minima converges to the actual minimum f^* of the function under some hypotheses [6]. In some cases, the sequence even reaches the minimum f^* in a finite number of steps [8, 16, 10, 2, 4, 14]. This approach proved to be particularly fruitful in many problems [7]. In contrast with numerical methods such as gradient descent methods, which converge to a local extremum but with no guaranty for the global solution, this relaxation approach can provide certificates for the minimum value f^* in terms of sums of squares representations.

From an algorithmic and computational perspective, some issues need however to be considered.

- *How to reduce the size of the moment matrices ?* The size of the SDP problems to be solved is a bottleneck of the method. This size is related to the number of monomials of degree $\leq t$ and is increasing exponentially with the number of variables and the degree t. Many SDP solvers are based on interior point methods which provide an approximation of the optimal moment sequence within a given precision in a polynomial time [13]. Thus reducing the size of the moment matrices or the number of parameters can improve significantly the performance of these relaxation methods. We address this issue using polynomial reduction with border basis due to their numerical stability [11, 12].
- *When is the minimum reached ?* A new stopping criteria is given to detect when the relaxation sequence reaches the minimum, using a flat extension criteria from [9]. We also provide a new algorithm to reconstruct a finite sum of weighted Dirac measures from a truncated sequence of moments. This reconstruction method can be used in other problems such as tensor decomposition [1] and multivariate sparse interpolation [3]
- *How to recover the minimizer ideal ?* Computing the points where this minimum is reached if they exist, is critical in many applications. Determining when and how these minimizer points can be computed from the relaxation sequence is a problem that has been adressed for instance in [5, 15] using of kernel of full moment matrices

We present a new algorithm to obtain the minimum of a real polynomial function f in a semialgebraic set $G = (G^0, G^+)$ where G^0 is a set of equalities and G^+ is a set of inequalities non negatives and we suppose that the numbers of minimizer points is finite. We compare our algorithm with the full moment matrix relaxation algorithm (implemented in c++ in the same environment that our algorithm) described in [7], which is also implemented in the package Gloptipoly of Matlab developed by D. Henrion and J.B. Lasserre.

When there are equality constraints, the border basis computation reduces the size of the moment matrices, as well as the localization matrices associated to the inequalities. This speeds up the SDP computation. In the case where there are only inequalities, the size of the moments matrices is the same but the algorithm which verifies the flat extension and the algorithm which computes the minimizers are more efficient and quicker than the reconstruction algorithm used in the full moment matrix relaxation approach. The performance is not the only issue : numerical problems can also occur due to the bigger size of the moment matrices in the flat extension test and the reconstruction of minimizers.

The experiments show that when the size of the SDP problems becomes significant, most of the time is spent during `sdpa` computation and the border basis time and reconstruction time are negligible. In all the examples, the new border basis relaxation algorithm outperforms the full moment matrix relaxation method.

Bibliographie

[1] J. Brachat, P. Comon, B. Mourrain, and E. Tsigaridas. Symmetric tensor decomposition. *Linear Algebra and Applications*, 433 :1851–1872, 2010.

[2] J. Demmel, J. Nie, and V. Powers. Representations of positive polynomials on noncompact semialgebraic sets via kkt ideals. *Journal of Pure and Applied Algebra*, 209(1) :189 – 200, 2007.

[3] M. Giesbrecht, G. Labahn, and W.-S. Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. *J. Symb. Comput.*, 44(8) :943–959, August 2009.

[4] H. V. Ha and T.S. Pham. Representation of positive polynomials and optimization on noncompact semialgebraic sets. *SIAM Journal on Optimization*, 20(6) :3082–3103, 2010.

[5] D. Henrion and J.B. Lasserre. *Positive Polynomials in Control*, chapter Detecting Global Optimality and Extracting Solutions in GloptiPoly., pages 293–310. Lectures Notes in Control and Information Sciences. Springer, 2005.

[6] J.B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11 :796–817, 2001.

[7] J.B Lasserre. *Moments, positive polynomials and their applications.* Imperial College Press, 210.

[8] M. Laurent. Semidefinite representations for finite varieties. *Math. Progr*, 109 :1–26, 2007.

[9] M. Laurent and B. Mourrain. A generalized flat extension theorem for moment matrices. *Arch. Math. (Basel)*, 93(1) :87–98, July 2009.

[10] M. Marshall. Representations of non-negative polynomials, degree bounds and applications to optimization. *Can. J. Math.*, 61(1) :205–221, 2009.

[11] B. Mourrain and P. Trébuchet. Generalized normal forms and polynomials system solving. In M. Kauers, editor, *ISSAC : Proceedings of the ACM SIGSAM International Symposium on Symbolic and Algebraic Computation*, pages 253–260, 2005.

[12] B. Mourrain and Ph. Trébuchet. Stable normal forms for polynomial system solving. *Theoretical Computer Science*, 409(2) :229–240, 2008.

[13] Y. Nesterov and A. Nemirovski. *Interior-point polynomial algorithms in convex programming*. SIAM, Philaldelphia, 1994.

[14] J. Nie. An exact jacobian SDP relaxation for polynomial optimization. *Mathematical Programming*, pages 1–31, 2011.

[15] J. Nie. Certifying convergence of Lasserre's hierarchy via flat truncation. *Mathematical Programming*, pages 1–26, 2012.

[16] J. Nie, J. Demmel, and B. Sturmfels. Minimizing polynomials via sum of squares over gradient ideal. *Math. Program.*, 106(3) :587–606, 2006.

2. Un algorithme efficace de calcul de la dimension réelle d'un ensemble algébrique réel.

Ivan Bannwarth, Mohab Safey El Din
Université Pierre et Marie Curie, INRIA - POLSYS team,
LIP6 - CNRS
ivan.bannwarth@lip6.fr, mohab.safey@lip6.fr

Nous nous intéressons au calcul de la dimension réelle d'un ensemble semi-algébrique S. La dimension réelle est le plus grand entier d tel que la projection de S sur un espace affine de dimension d est d'intérieur non vide.

Ce problème est motivé par les travaux de Barone et Basu [6, 7] qui utilisent le calcul de la dimension réelle. Il est également motivé par l'étude des systèmes mécaniques contraints [8] car la dimension réelle exprime le degré de liberté de mouvement de tels systèmes.

Comme l'élimination d'un bloc de quantificateurs sur les réels permet de calculer la projection d'un semi-algébrique, elle a un rôle important dans l'état-de-l'art. À l'aide des formules obtenues par élimination, on peut tester si l'intérieur de la projection est vide.

Le premier algorithme pour l'élimination de quantificateurs est la décomposition cylindrique algébrique dû à Collins [2] en temps doublement exponentiel en n, le nombre de variables. Les techniques récentes d'élimination permettent à Vorobjov [4], Koiran [3], et

Basu, Pollack et Roy [5] de concevoir une famille d'algorithmes déterministes calculant la dimension réelle d en temps simplement exponentiel en $O(d(n-d))$. Mais malgré ce gain de complexité, il n'y a pas d'implémentation efficace connue de ces algorithmes. Une des raisons repose dans la constante de complexité qui n'est pas bien contrôlée. La meilleure implémentation de l'état de l'art semble être aujourd'hui une implémentation de la décomposition cylindrique algébrique.

Notre objectif est de trouver un algorithme qui calcule la dimension réelle d'un semi-algébrique qui soit dans la meilleure classe de complexité connue et qui admette une implémentation plus efficace que l'état de l'art. Pour cela nous cherchons à contrôler la constante dans l'exposant.

Dans cette présentation nous allons parler d'un nouvel algorithme probabiliste qui calcule la dimension réelle d'une *hypersurface* définie par une équation polynomiale à coefficients réels en temps simplement exponentiel en $3d(n-d)$.

Cet algorithme s'inspire des récents travaux de H. Hong et M. Safey El Din [1] mais dans un cadre plus général : nous contournons l'élimination des quantificateurs en utilisant un nouveau moyen de tester si l'intérieur d'une projection est vide. Pour faire cela, nous calculons la frontière de la projection à l'aide de variétés polaires, ensemble des points critiques de la restriction de la projection à l'hypersurface. En calculant un point par composante connexe du complémentaire de la frontière, nous pouvons tester si l'intérieur de la projection est vide. Le cas d'un ensemble algébrique réel sans point régulier est celui qui pose difficulté et qu'il faut traiter avec attention.

La première implémentation, reposant sur des calculs de bases de Gröbner et écrite en Maple est déjà beaucoup plus performante que celles de l'état de l'art. Elle est à la fois plus rapide et permet de traiter des exemples de taille plus grande, hors de portée de l'état-de-l'art.

Bibliographie

[1] H. Hong, M. Safey El Din, *Variant real quantifier elimination*, Journal of Symbolic Computation, 2012, vol. 47, no. 7, p.883-901.

[2] G. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decompostion*, Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20–23, 1975, p. 134–183.

[3] P. Koiran, *The Real Dimension Problem Is NPR-Complete*, Journal of Complexity, 1999, vol. 15, no. 2, p. 227–238.

[4] N. Vorobjov, *Complexity of Computing the Local Dimension of a Semialgebraic Set*, Journal of Symbolic Computation, 1999, vol. 27, no. 6, p. 565–579.

[5] S. Basu and R. Pollack and M.-F. Roy, *Algorithms in real algebraic geometry*, Algorithms and Computation in Mathematics, 2006, vol. 10.

[6] S. Barone, and S. Basu, *Refined Bounds on the Number of Connected Components of Sign Conditions on a Variety*, Discrete & Computational Geometry, 2012, vol. 47, no.3, p.577–597.

[7] S. Barone, and S. Basu, *On a real analogue of Bezout inequality and the number of connected components of sign conditions*, ArXiv e-prints, 2013, 1303.1577.

[8] , Q. Jin, and T. Qiong, *Overconstraint analysis on spatial 6-link loops*, Mechanism and machine theory, 2002, vol. 37, no. 3, p. 267–278.

3. Algorithmes rapides de résolution de systèmes de Toeplitz bandes

S. Belhaj[a,b], M. Dridi [a,c], A. Salam [c]
[a] Université de Tunis El Manar, ENIT-LAMSIN, BP 37, 1002, Tunis, Tunisie.
[b] Université de la Manouba, ISAMM, 2010 Tunis, Tunisie.
[c] Université de Lille, ULCO, LMPA, BP 699, 62228 Calais, France.
Skander.Belhaj@lamsin.rnu.tn

Nous proposons dans ce travail une synthèse sur les méthodes super-rapide pour la résolution des systèmes d'équations linéaires avec matrices de Toeplitz bandes. Des algorithmes basés sur la réduction cyclique [1, 2] et la factorisation spectrale de la fonction génératrice [4,5] associée à la matrice de Toeplitz vont être présentés. Dans le cas où ces dernières échouent, une alternative a été introduite. Cette nouvelle approche est basée sur l'extension de la matrice donnée par plusieurs lignes en dessus et plusieurs colonnes à droite et d'attribuer des zéros et des constantes non nulles dans chacune de ces lignes et colonnes de telle manière la matrice augmentée a une structure de matrice triangulaire inférieure de Toeplitz. La stabilité de l'algorithme est discutée et son rendement est justifié par des expériences numériques.

Bibliographie

[1] D.A. Bini, B. Meini, *Effective methods for solving banded Toeplitz systems*, SIAM J. Matrix Anal. App. 20 (1999), pp. 700–719.

[2] D.A. Bini, B. Meini, *The cyclic reduction algorithm : from Poisson equation to stochastic processes and beyond. In memoriam of Gene H. Golub*, Numer. Algor. 51(1) (2009), pp. 23–60.

[3] A. Malyshev, M. Sadkane, *Using the Sherman-Morrison-Woodbury inversion formula for a fast solution of tridiagonal block Toeplitz systems*, Linear Alg. Appl. 435 (2011) pp. 2693–2707.

[4] A. Malyshev, M. Sadkane, *Fast solution of unsymmetric banded Toeplitz systems by means of spectral factorizations and Woodbury's formula*, Numer. Linear Algebra Appl. 21(1) (2014) pp. 13–23.

4. Algorithmes en temps polynomial pour l'isomorphisme de polynômes quadratiques : le cas régulier

J. Berthomieu, J.-C. Faugère, L. Perret
Sorbonne Universités, UPMC Univ Paris 06,
Équipe PolSys, LIP6, F-75005, Paris
CNRS UMR 7606, LIP6, F-75005, Paris
INRIA, Équipe PolSys, Centre Paris – Rocquencourt
jeremy.berthomieu@lip6.fr,
jean-charles.faugere@inria.fr,
ludovic.perret@lip6.fr

Soient $\mathbb{K}$ un corps et $\mathbf{x} = (x_1, \ldots, x_n)$ des indéterminées. Soient $\mathbf{f} = (f_1, \ldots, f_m)$ et $\mathbf{g} = (g_1, \ldots, g_m)$ deux ensembles de $m \geq 1$ polynômes homogènes dans $\mathbb{K}[\mathbf{x}]$. On considère le problème d'équivalence consistant à calculer une matrice $A \in \mathrm{GL}_n(\mathbb{K})$ telle que $\mathbf{f}(A \cdot \mathbf{x}) = \mathbf{g}(\mathbf{x})$. Ce problème fondamental de part son nombre d'applications est appelé l'*Isomorphisme de Polynômes à un Secret* (IP1S). Parmi ces applications, on peut noter l'*Isomorphisme de Graphes* dont Agrawal et Saxena [1] ont montré qu'il se ramenait à une instance d'IP1S avec f_1, g_1 cubiques et f_2, g_2 quadratiques, des cryptosystèmes en cryptographie multivariée, la réduction de circuits en complexité algébrique... On peut aussi remarquer que si $m = 1$ et f_1, g_1 sont de degré 2, alors IP1S se résout facilement à l'aide de l'algorithme de réduction des formes quadratiques de Gauss. En calcul formel, un problème proche d'IP1S est celui de la simplification d'un système polynomial $\mathbf{f}$: on cherche $A \in \mathrm{GL}_n(\mathbb{K})$ telle que $\mathbf{g}(\mathbf{x}) = \mathbf{f}(A \cdot \mathbf{x})$ est plus simple à résoudre. Dans cette optique, les algorithmes Ridge [3] et MinVar [4] réduisent au maximum le nombre de variables du système considéré. Plus généralement, étant donné $\mathbf{f}$, la *Décomposition fonctionnelle* consiste à calculer $\mathbf{h} = (h_1, \ldots, h_s)$ homogènes et $\mathbf{g}$ tels que $\mathbf{f}(\mathbf{x}) = \mathbf{g}(\mathbf{h}(\mathbf{x}))$.

Dans cet exposé, nous présentons un algorithme probabiliste en temps polynomial pour résoudre les instances quadratiques régulières d'IP1S avec m quelconque [2]. Notons $H_1, \ldots, H_m$ les représentations matricielles des f_i, avec $\mathrm{char}\,\mathbb{K} \neq 2$. Une instance quadratique sera dite *régulière* s'il existe une combinaison linéaire des H_i de rang maximal. Ceci améliore les résultats obtenus par les algorithmes proposés jusqu'à présent qui étaient soit heuristiques, avec une complexité potentiellement non polynomiale, soit dédiés à des cas particuliers comme $m = 2$.

Soient $H'_1, \ldots, H'_m$ les représentations matricielles de $g_1, \ldots, g_m$. Résoudre le problème d'équivalence entre $\mathbf{f}$ et $\mathbf{g}$ revient à calculer A inversible telle que

$$A^{\mathrm{T}} H_i A = H'_i, \quad \forall i,\ 1 \leqslant i \leqslant m.$$

Nous montrons alors que l'on peut essentiellement *linéariser* le problème en nous ramenant à tester la conjugaison simultanée de matrices symétriques par une matrice orthogonale, c'est-à-dire à résoudre

$$A^{\mathrm{T}} A = \mathrm{Id}_n, \quad H_i A = A H'_i, \quad \forall i,\ 2 \leqslant i \leqslant m.$$

Chistov, Ivanyos et Karpinski [5] ont montré que ce dernier problème est équivalent à calculer une matrice inversible dans un sous-espace de $\mathbb{K}^{n \times n}$ et d'en calculer une racine

carrée. Alors que calculer une racine carrée de matrice peut être effectué efficacement en utilisant des méthodes numériques, il semble difficile de contrôler la complexité binaire de telles méthodes. En effet, si $\mathbb{K} = \mathbb{Q}$, la racine carrée peut n'exister que dans une extension de $\mathbb{K}$ de degré exponentiel en n. Nous présentons ainsi des algorithmes exacts et en temps polynomial pour calculer une représentation d'une racine carrée d'une matrice dans $\mathbb{K}^{n\times n}$ nous permettant de déduire si $\mathbf{f}$ et $\mathbf{g}$ sont équivalents.

Enfin, nous donnons des résultats expérimentaux où nous résolvons des instances dont les tailles dépassent d'un ordre de grandeur les *challenges* cryptographiques.

Bibliographie

[1] M. Agrawal and N. Saxena, 2006. Equivalence of F-Algebras and Cubic Forms. In : B. Durand, W. Thomas (Eds.), STACS. Vol. 3884 of Lecture Notes in Computer Science. Springer, pp. 115–126.

[2] J. Berthomieu, J.-C. Faugère and L. Perret, 2014. Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials : The Regular Case. Preprint, `http://hal.inria.fr/hal-00846041`.

[3] J. Berthomieu, P. Hivert and H. Mourtada, 2010. Computing Hironaka's invariants : Ridge and Directrix. In : Arithmetic, Geometry, Cryptography and Coding Theory 2009. Vol. 521 of Contemp. Math. Amer. Math. Soc., Providence, RI, pp. 9–20.

[4] E. Carlini, 2005. Reducing the number of variables of a polynomial. In : Algebraic geometry and geometric modeling. Springer, pp. 237–247.

[5] A. L. Chistov, G. Ivanyos and M. Karpinski, 1997. Polynomial time algorithms for modules over finite dimensional algebras. In : B. W. Char, P. S. Wang, W. Küchlin (Eds.), ISSAC. ACM, pp. 68–74.

5. Formes libres pour les trajectoires optimales

P. Bonnelie, O. Ruatta
DMI, XLIM UMR 7252 Université de Limoges CNRS
`pierre.bonnelie@xlim.fr,olivier.ruatta@xlim.fr`

Motivations

On présente une approche pour la génération de chemins des méthodes par homotopie pour la résolution d'un système (calcul de racines, calcul de valeurs propres, valeurs singulières, ...). Si l'ensemble des systèmes a une structure d'espace vectoriel, supposons que l'on veuille résoudre un système S_f, on commence à partir d'un système S_i que l'on sait résoudre et on le déforme jusqu'au système S_f. Une solution est l'homotopie linéaire : on suit le segment $[S_i; S_f]$. Cependant on risque de recontrer un problème plus mal conditionné que le système auquel on s'intéresse. L'idée est de ne pas se restreindre à des segments mais à des chemins, de sorte à éviter le plus possible les systèmes mal conditionnés.

Modèle

Soit E un espace vectoriel et Σ un sous-ensemble de E (Σ représentant l'ensemble des systèmes mal conditionnés). On note $\mu(v) = dist(v, \Sigma)$, pour tout $v \in E$. Etant donnés S_i et $S_f \in E$, on cherche une courbe $\Gamma : [0;1] \to E$ telle que

- $\Gamma(0) = S_i$ et $\Gamma(1) = S_f$
- Γ est le minimum de $\int_0^1 \mu(\Gamma(t))dt$ ou $\max_{t\in[0;1]} \mu(\Gamma(t))$ par exemple

Notre approche

Si E est un espace vectoriel de dimension finie, on peut définir des courbes de Bézier dans E. Ainsi un chemin Γ sera représenté par une courbe de Bézier et les variables du problème d'optimisation seront les points de contrôle de sorte à faire de l'optimisation en dimension finie plutôt qu'en dimension infinie.

Formalisme

Considérons toujours un espace vectoriel E de dimension finie. Une courbe de Bézier de degré d, $B([P_0, ..., P_d], t) = \sum_{i=0}^{d} \binom{d}{i} (1-t)^{d-i} t^i P_i$ à valeurs dans E est entièrement déterminée par des points de contrôle $P_0, ..., P_d$ de E.

On peut montrer que l'application qui à $d+1$ points de contrôle $P_0, ..., P_d$ de E associe la courbe de Bézier précédemment définie constitue un isomorphisme entre E^{d+1} et l'espace $\mathcal{B}_{1,d}$ des courbes de Bézier de degré d.
Le problème d'optimisation $\min_{\Gamma} \int_0^1 \mu(\Gamma(t))dt$ s'écrit alors $\min_{P_0,...,P_d\in E} \int_0^1 \mu(B([P_0, ..., P_d], t))dt$.
Si l'espace $\mathcal{B}_{1,d}$ n'offre pas assez de liberté, on peut l'étendre à l'espace $\mathcal{B}_{N,d}$ des courbes de Bézier par morceaux.

Traitement

On a utilisé la fonction *fmincon* MATLAB pour résoudre le problème $\min_{P_0,...,P_d\in E} \int_0^1 \mu(B([P_0, ..., P_d], t))$ en laissant le logiciel calculer le gradient mais on pourrait aussi le calculer formellement et le passer en argument à *fmincon*.

Exemple dans $\mathbb{R}^2$

On a testé cette méthode sur un exemple plan. Σ est un lieu géométrique (un point, une droite, un cercle ...) et on cherche à relier deux points A et B du plan par le plus court chemin tout en restant le plus loin possible de Σ. En prenant la distance euclidienne d_2, le problème d'optimisation est

$$\min_{P_0,...,P_d \epsilon E} \int_0^1 d_2(B([P_0,...,P_d],t),\Sigma)dt$$

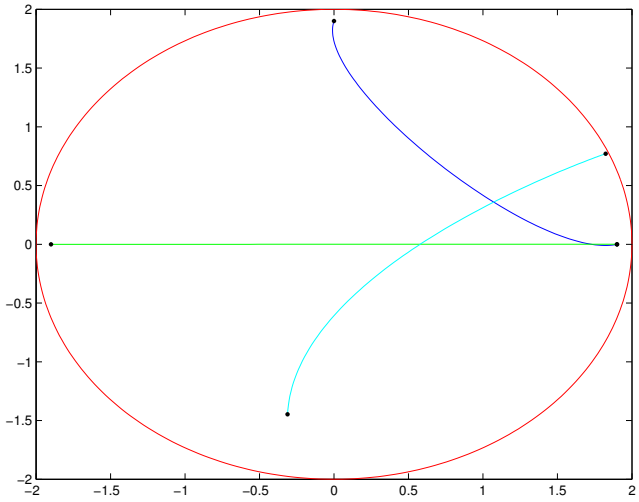

FIGURE 1: Trois trajectoires obtenues pour différents points A et B, lorsque Σ est un cercle.

6. Matrix multiplication over word-size modular rings using Bini's approximate formula

B. Boyer[(a)], J.-G. Dumas[(b)] *a*
[(a)] LIP6, UPMC, Paris, France
[(b)] LJK, Université de Grenoble, Grenoble, France
brice.boyer@lip6fr,jean.guillaume-dumas@imag.fr

a. This material is based on work supported in part by the National Science Foundation under Grant CCF-1115772 (Kaltofen) and Agence Nationale pour la Recherche under Grant ANR-11-BS02-013 HPAC (Dumas).

A fast reliable matrix multiplication implementation over $\mathbf{Z}/p\mathbf{Z}$ is crucial in exact linear algebra. Indeed, many algorithms rely on fast matrix multiplication as a building block.

Bini's approximate formula (or border rank) for matrix multiplication [1] achieves a better complexity than Strassen's matrix multiplication formula [4]. We show a novel way to use the approximate formula in the special case where the ring is $\mathbf{Z}/p\mathbf{Z}$. Besides, we show an implementation à la FFLAS–FFPACK[3], where p is a word-size modulo, that improves on state-of-the-art $\mathbf{Z}/p\mathbf{Z}$ matrix multiplication implementations.

Bini's formula. Bini's approximate formula computes a matrix $C_\epsilon = A \times B + \epsilon D(\epsilon)$, with $A \in \mathbf{K}^{3\times 2}$, $B \in \mathbf{K}^{2\times 2}$ (noted $(3,2,2)$ multiplication), where D is a polynomial in $\mathbf{K}^{3\times 2}[\epsilon]$, and with 10 multiplications.

Application to exact matrix multiplication. We apply a different method than [1], requiring only one call to the approximate multiplication, for the special case $\mathbf{Z}/p\mathbf{Z}$. We are interested in the following two cases. First, we consider $\epsilon = 2^{-27}$ and use `double`floating point machine words; the idea is to store two exact integers in one `double`as $x + \epsilon y$, then any term in ϵ^2 will be neglected, as ϵ^2 approaches the machine precision (a rounding to the nearest will remove the ϵ−approximations). Second, we take $\epsilon = p$, and the p−approximations are removed by a final reduction modulo p.

Proposition 1 (Case $\epsilon = 2^{-27}$) *For $\epsilon = 2^{-27}$ and a (m,k,n) matrix multiplication on $\mathbf{Z}/p\mathbf{Z}$, rounding to the nearest integer the output of one call to Bini $(3,2,2)$−approximate formula with `double`floating point arithmetic, gives the exact result when : $2\lfloor k/2 \rfloor (p-1)^2 < \frac{1}{3}2^{27}$.*

Proposition 2 (Case $\epsilon = p$) *For $\epsilon = p$ and a (m,k,n) matrix multiplication over $\mathbf{Z}/p\mathbf{Z}$, the reduction modulo p of the output C_ϵ of one call to Bini's $(3,2,2)$−approximate formula with `double`floating point arithmetic, gives the exact result when : $\lfloor k/2 \rfloor (p-1)^2 (p+1)^2 < 2^{53}$.*

Remark. These bounds can be improved using a balanced representation.

Memory usage and scheduling We provide schedules requiring less extra memory (temporaries) than Strassen–Winograd's, in a similar fashion to [2], and implement them. We use only two temporaries and can create in-place algorithms by allowing overwriting an operand.

Implementation and Timings. Timings show that our implementation is competitive with Winograd's algorithm implementation, usually providing an $\approx 5\%$ speed-up, and it is always faster than FFLASon `double`. The balanced representation allows to gain an $\approx 10\%$ speed-up on size 3 900 where the standard representation could not be used. The best speed-up of $\approx 15\%$ around sizes 2 700 to 3300 could be explained by optimal size

BLAS block calls. For small moduli, the `float`representation performs better, but this phenomenon is only relevant for small moduli (≈ 400 and less, due to BLAS routines on `float`up to twice as fast as BLAS on `double`.

Bibliography

[1] D. Bini, *Relations between exact and approximate bilinear algorithms. Applications*, Calcolo 17 (1980), pp 87–97, Issue 1.

[2] B. Boyer, J.-G. Dumas, C. Pernet and W. Zhou *Memory efficient scheduling of Strassen-Winograd's matrix multiplication algorithm. Proc. of the 2009 ISSAC* (New York, NY, USA, 2009), ISSAC '09, ACM, pp. 55–62.

[3] J.-G. Dumas, P. Giorgi and C. Pernet *Dense linear algebra over word-size prime fields : the FFLAS and FFPACK packages.* ACM Trans. Math. Softw. 35, 3 (2008), 1–42.

[4] V. Strassen *Gaussian elimination is not optimal.* Numerische Mathematik 13 (1969), 354–356.

7. Structures of polyzetas and the algorithms to express them on algebraic bases on words

V.C. BUI, V. G.H.E. DUCHAMP, HOANG NGOC MINH
LIPN - Paris 13 University
99 avenue Jean-Baptiste Clément, 93430 Villetaneuse
vanchien.bui@lipn.univ-paris13.fr, gheduchamp@gmail.com,
vincel.hoangngocminh@univ-lille2.fr

For any $(s_1, \ldots, s_r) \in (\mathbb{N}^*)^r$ with $s_1 > 1$, the polyzetas (multiple zeta values) $\zeta(s_1, \ldots, s_r)$ is defined by the following sum

$$\zeta(s_1, \ldots, s_r) := \sum_{n_1 > \ldots > n_r > 0} \frac{1}{n_1^{s_1} \ldots n_r^{s_r}} \tag{1}$$

Let $X = \{x_0, x_1\}$ and $Y = \{y_k\}_{k \geq 1}$ be two alphabets of the set of Lyndon words denoted by $\mathcal{L}ynX$ and $\mathcal{L}ynY$ respectively. Let

- $\{P_l\}_{l \in \mathcal{L}ynX}$ be a basis of the Lie algebra $\mathcal{L}ie_{\mathbb{Q}}\langle X\rangle$ and $\{S\}_{l \in \mathcal{L}ynX}$ be the (pure) transcendent basis, in duality with $\{P_l\}_{l \in \mathcal{L}ynX}$ on the Hopf algebra $(\mathbb{Q}\langle X\rangle, ., 1_{X^*}, \Delta_{\sqcup\!\sqcup}, \epsilon_X, \mathcal{S})$ (see [2]),
- $\{\Pi_l\}_{l \in \mathcal{L}ynY}$ be a basis of the primitive elements of the Hopf algebra $(\mathbb{Q}\langle Y\rangle, ., 1_{Y^*}, \Delta_{\sqcup\!\sqcup}), \epsilon_Y, \mathcal{S})$ and $\{\Sigma_l\}_{l \in \mathcal{L}ynY}$ be the (pure) transcendent basis, in duality with $\{\Pi_l\}_{l \in \mathcal{L}ynY}$ (see [1, 4, 5]).

Since, for any multi-index $(s_1, \ldots, s_r)$, the polyzeta $\zeta(s_1, \ldots, s_r)$ can be encoded by the words $x_0^{s_1-1}x_1 \ldots x_0^{s_r-1}x_1 \in X^*$ and $y_{s_1} \ldots y_{s_r} \in Y^*$ (see [3]) then one can define the two following non commutative generating series of polyzetas :

$$Z_{\sqcup\!\sqcup} := \prod_{l \in \mathcal{L}ynX \setminus X}^{\searrow} \exp(\zeta(S_l)\, P_l) \quad \text{and} \quad Z_{\perp\!\!\!\sqcup} := \prod_{w \in \mathcal{L}ynY \setminus \{y_1\}}^{\searrow} \exp(\zeta(\Sigma_l)\, \Pi_l). \tag{2}$$

Let us introduce the following non commutative generating series

$$Z_\gamma = e^{\gamma y_1} Z_{\sqcup\!\sqcup}. \tag{3}$$

Let Γ dedontes the Euler's Gamma function and π_Y stands for the linear projection from $\mathbb{R} \oplus \mathbb{R}\langle\langle X \rangle\rangle x_1$ to $\mathbb{R}\langle\langle Y \rangle\rangle$ mapping $x_0^{s_1-1}x_1 \ldots x_0^{s_r-1}x_1$ to $y_{s_1} \ldots y_{s_r}$. We will base on the following comparison formula

$$Z_\gamma = \Gamma(y_1 + 1)\pi_Y Z_{\sqcup\!\sqcup} \tag{4}$$

to identify the homogeneous polynomials, in weigth, among the local coordinates $\{\zeta(\Sigma_l)\}_{l \in \mathcal{L}ynY \setminus \{y_1\}}$ (and also $\{\zeta(S_l)\}_{l \in \mathcal{L}ynX \setminus X}$) upto weight 12 in Maple.

Bibliographie

[1] V.C. Bui, G. H. E. Duchamp, Hoang Ngoc Minh, *Schützenberger's factorization on the (completed) Hopf algebra of q−stuffle product*, Journal of Algebra, Number Theory and Applications (2013), 30, No. 2 , pp 191 - 215.

[2] C. Reutenauer.– *Free Lie Algebras*, London Math. Soc. Monographs, New Series-7, Oxford Sc. Pub. (1993).

[3] Hoang Ngoc Minh, M.Petitot.– *Lyndon words, polylogarithms and the Riemann ζ function*, Discrete Mathematics (2000), 273 - 292.

[4] Hoang Ngoc Minh.– *On a conjecture by Pierre Cartier about a group of associators*, in Acta Mathematica Vietnamica, Vol. 3, (2013).

[5] Hoang Ngoc Minh.– *Structure of polyzetas and Lyndon words*, Vietnamese Mathematics Journal (2013), Volume 41 Number 4, pp 409-450.

8. Résultants et sous-résultants de polynômes p-adiques

X. Caruso
IRMAR
Université Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
xavier.caruso@normalesup.org

Soient p un nombre premier et $\mathbb{Z}_p$ l'anneau des entiers p-adiques. À l'origine de ce travail est la volonté d'obtenir des algorithmes à la fois efficaces et stables numériquement pour le calcul du PGCD — ainsi que des coefficients de Bézout — de polynômes à coefficients dans $\mathbb{Z}_p$.

Un premier candidat est, bien entendu, l'algorithme d'Euclide usuel. Malheureusement, s'il est plutôt efficace, on s'aperçoit rapidement qu'il ne fait pas le poids au niveau de la stabilité numérique. En effet, on observe expérimentalement que sur des entrées aléatoires A et B piochées parmi les polynômes unitaires de degré d à coefficients dans $\mathbb{Z}_p$, l'algorithme d'Euclide étendu calcule les coefficients de Bézout correspondants U et V avec une perte moyenne d'un nombre de chiffres significatifs sur chaque coefficient qui croît proportionnellement à d. De surcroît, on obtient fréquemment des exemples pour lesquels on observe une chute importante de la précision alors que le résultant $\mathrm{Rés}(A,B)$ est inversible dans $\mathbb{Z}_p$. Or, avec un algorithme stable, ceci ne devrait pas se produire car la théorie des résultants affirme que les coefficients de U et V s'écrivent comme le quotient d'une expression polynômiale en les coefficient de A et B par $\mathrm{Rés}(A,B)$; ainsi, si $\mathrm{Rés}(A,B)$ est inversible dans $\mathbb{Z}_p$, on s'attend à connaître les coefficients de Bézout avec la même précision que les entrées.

La première partie de mon exposé sera consacrée à l'explication des phénomènes qui viennent d'être décrits. Plus précisément, je montrerai que les pertes de précision qui s'accumulent au cours de l'exécution de l'algorithme d'Euclide valent approximativement :

$$2 \cdot \sum_{j=0}^{d-1} V_j(A,B) \tag{5}$$

où $V_j(A,B)$ désigne la valuation de coefficient dominant du j-ième sous-résultant de (A,B). Cette quantité est à mettre en comparaison avec la valeur $2 \cdot V_0(A,B)$ qui est la perte « théorique » donnée par l'argument des résultants. J'étudierai ensuite les fonctions V_j considérées comme des variables aléatoires : j'énoncerai un théorème qui décrit leur loi et, comme corollaire, en déduirai les résultats descriptifs que voici.

Théorème 1 *Pour tout $j \in \{0, \dots, d-1\}$, on a :*

i) $\frac{1}{p-1} \leq \mathbb{E}[V_j] \leq \frac{p}{(p-1)^2}$;

ii) $\sigma(V_j) = O\big(\frac{1}{\sqrt{p}}\big)$;

iii) $\mathbb{P}[V_j \leq m] = O\big(p^{-m+O(\sqrt{m})}\big)$

où les constantes dans tous les $O(\cdot)$ sont absolues (et, en particulier, ne dépendent ni de j, ni de d).

Il résulte du théorème que l'expression (5) vaut en moyenne $\simeq \frac{2d}{p-1}$, en accord avec ce qui avait été observé initialement. En comparaison, la perte « théorique » $2 \cdot V_0(A,B)$ ne vaut en moyenne que $\simeq \frac{2}{p-1}$. En d'autres termes, l'algorithme d'Euclide surestime les pertes de précision d'un facteur d.

Enfin, dans une deuxième partie de mon exposé, je présenterai une variante « stabilisée » de l'algorithme d'Euclide qui conserve sa complexité mais atteint également la perte de précision donnée par la théorie des résultants. Cette variante repose de façon essentielle sur la théorie de la précision p-adique développée dans [1].

Bibliographie

[1] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*, LMS J. Comput. Math. **17** (Special issue A), 2014, 274–294

9. Calculs de séries génératrices hypergéométriques pour les marches à petits pas dans le quart de plan

A. Bostan[(1)], **F. Chyzak**[(1)], M. van Hoeij[(2)], M. Kauers[(3)], L. Pech[(4)]
[(1)]INRIA, [(2)]Florida State University, [(3)]RISC, [(4)]Google
alin.bostan@inria.fr,frederic.chyzak@inria.fr,
hoeij@mail.math.fsu.edu,mkauers@gmail.com,lucien.pech@gmail.com

Les marches sur un réseau sont des objets combinatoires qui interviennent de façon récurrente en mathématique discrète, en physique statistique, en théorie des probabilités, ou encore en recherche opérationnelle. Les séries génératrices qui les comptent selon certaines contraintes attirent l'attention tant des combinatoriciens que des algorithmiciens du calcul formel. D'abord, leurs propriétés algébriques varient grandement selon la famille de pas admissibles choisie pour les définir, permettant de former des séries génératrices tantôt rationnelles, tantôt algébriques (et donc données par une équation polynomiale), tantôt D-finies (et donc données par une équation différentielle linéaire), tantôt encore sans équation apparente. Ceci suscite depuis quelques années un effort de classification qui a abouti à des caractérisations qui ne sont pas encore suffisamment comprises pour être totalement explicites. Par ailleurs, les propriétés calculatoires des marches sur réseau en font un défi intéressant pour le calcul formel, car leur description selon la classification précédente mène souvent à des équations, qu'elles soient polynomiales ou différentielles, de degrés, ordres et tailles si grandes qu'il devient difficile d'obtenir explicitement ces descriptions, et de les manipuler avec une efficacité raisonnable.

Étant donnée une famille fixée de vecteurs du plan non nuls et de coordonnées ± 1, vecteurs que nous appelerons « pas », une marche à petits pas sur le réseau carré plan est une succession finie de pas mis les uns à la suite des autres. On s'intéresse particulièrement aux marches contraintes à rester dans le quart de plan (à coordonnées entières positives ou nulles), et comptées selon leur longueur (nombre de pas). Dans cet exposé, nous présentons un travail en cours qui fait le pont entre deux travaux antérieurs de natures différentes, sur le sujet des marches à petits pas dans le quart de plan. D'une

part, Bousquet-Mélou et Mishna ont montré [2] que parmi les 79 modèles essentiellement différents, seuls 19 ont une série génératrice qui soit D-finie et transcendante, et correspondent donc à une équation différentielle linéaire, mais ce sans expliciter les équations différentielles dont elles prouvaient l'existence. Presque simultanément, Bostan et Kauers [1] ont obtenu par des calculs non triviaux mais heuristiques des équations différentielles linéaires selon toute vraisemblance vérifiées par ces 19 marches, mais sans prouver formellement la correction de ces équations. Dans le travail en cours, nous donnons la première preuve que ces équations sont bien vérifiées par les séries génératrices correspondantes. L'approche procède en représentant les séries génératrices des marches contraintes comme extractions de coefficients dans des séries rationnelles, et par une validation soignée de l'emploi du procédé de télescopage créatif [3] utilisé pour ces extractions.

Une fois prouvées, les équations différentielles permettent de calculer de façon garantie nombre de formules et propriétés des séries des marches. D'abord, une factorisation appropriée des opérateurs différentiels sous-jacents permet de représenter les séries génératrices de marches comme variations de primitives itérées de fonctions hypergéométriques de Gauss [4]. Il s'ensuit que les propriétés d'algébricité et transcendance des séries énumératives et de spécialisations significatives pour la combinatoire sont accessibles au calcul, de même que des formules asymptotiques complètes pour les nombres de marches en fonction de leur longueur.

Références

[1] Alin Bostan and Manuel Kauers. Automatic classification of restricted lattice walks. In *21st International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2009)*, Discrete Math. Theor. Comput. Sci. Proc., AK, pages 201–215.

[2] Mireille Bousquet-Mélou and Marni Mishna. Walks with small steps in the quarter plane. In *Algorithmic probability and combinatorics*, volume 520 of *Contemp. Math.*, pages 1–39. Amer. Math. Soc., Providence, RI, 2010.

[3] Frédéric Chyzak. An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Math.*, 217(1-3) :115–134, 2000.

[4] Tingting Fang and Mark van Hoeij. 2-descent for second order linear differential equations. In *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, pages 107–114. ACM, New York, 2011.

10. Computing necessary integrability conditions for planar parametrized homogeneous potentials

A. Bostan, **T. Combot**, M. Safey El Din
IMB, Université de Bourgogne
9 avenue Alain Savary 21000 Dijon
Alin.Bostan@inria.fr, thierry.combot@u-bourgogne.fr,
Mohab.Safey@lip6.fr

We consider a potential V, rational homogeneous in dimension 2 with parameters a. We design an algorithm in [1] that computes polynomial necessary conditions on the parameters a such that the dynamical system associated to V is integrable. These conditions originate from those of the Morales-Ramis-Simó integrability criterion [2, 3] near all Darboux points. The implementation of the algorithm allows to treat applications that were out of reach before, as high degree homogeneous polynomials and the non integrability proof of the colinear three body problem.

Bibliographie

[1] A. Bostan, T. Combot, M. Safey El Din, *Computing necessary integrability conditions for planar parametrized homogeneous potentials*, ISSAC 2014

[2] J. J. Morales-Ruiz and J. P. Ramis., *A note on the non-integrability of some Hamiltonian systems with a homogeneous potential*, Methods Appl. Anal., 8(1) :113–120, 2001.

[3] J. J. Morales-Ruiz, J.-P. Ramis, and C. Simó, *Integrability of Hamiltonian systems and differential Galois groups of higher variational equations*, Ann. Sci. École Norm. Sup. (4), 40(6) :845–884, 2007.

11. Équations pour les diagonales, application aux marches unidimensionnelles

A. Bostan, **L. Dumont**, B. Salvy
INRIA Saclay, équipe SpecFun
INRIA Grenoble-Rhône-Alpes, équipe AriC
Alin.Bostan@inria.fr, Louis.Dumont@inria.fr,
Bruno.Salvy@inria.fr

Équations algébriques pour les diagonales de fractions rationnelles bivariées

Si $F(X,Y) = \sum_{n,m\geq 0} a_{n,m} X^n Y^m$ est le développement en série à l'origine d'une fraction rationnelle bivariée, on s'intéresse à la **diagonale** de F, série univariée définie par

$$\Delta F(T) = \sum_{n\geq 0} a_{n,n} T^n.$$

C'est un fait classique, qui remonte au moins à Pólya [4], que ΔF est une fonction algébrique.

Nous apportons une première contribution avec une borne **exponentielle** (en le bidegré du dénominateur de F) sur la taille de l'équation **algébrique** satisfaite par ΔF, et cette borne est fine. Ce résultat est à mettre en regard avec le fait, prouvé dans [2], que ΔF satisfait une équation **différentielle** de taille polynomiale. Nous donnons également un algorithme de calcul en temps quasi-optimal (en la taille de la sortie) de l'équation algébrique, variante additive de l'algorithme « Platypus » proposé dans [1].

Conséquence sur le calcul des séries génératrices de marches unidimensionnelles

À la lumière de ce résultat, nous nous intéressons (dans la lignée de [1]) aux séries génératrices de quatre types de marches **unidimensionnelles**. En s'autorisant un ensemble de pas dans le plan de la forme $(1,u), u \in \mathbb{Z}$ (donc l'abscisse représente le temps), on considère :

- Les marches simples : suites de pas non contraintes ;
- Les ponts : suites de pas qui s'achèvent sur l'axe des abscisses ;
- Les méandres : marches simples confinées au premier quadrant ;
- Les excursions : ponts confinés au premier quadrant.

Notons respectivement $W(X)$, $B(X)$, $M(X)$ et $E(X)$ leurs séries génératrices (le n-ième coefficient est le nombre de marches de longueur n du type choisi). La série W est rationnelle, tandis que les séries B, M, et E sont algébriques [1].

Nous étudions la complexité du développement à l'ordre N de ces trois séries.

(i) La méthode naïve consiste à utiliser la récurrence codée par W, et donne une complexité quadratique en N, sans précalcul.

(ii) Une seconde méthode, présentée dans [1] effectue le calcul en temps linéaire en N, au prix du précalcul de l'équation algébrique.

(iii) Nous exposons une troisième méthode donnant une complexité quasi-linéaire en N, et qui vise à minimiser le coût du précalcul. En effet, le calcul d'une équation algébrique peut dans certains cas être coûteux. Pour E ceci est étudié dans [3]. B quant à elle peut se coder comme une diagonale, rentrant ainsi dans le cadre de l'étude du paragraphe précédent.

Nous proposons donc de s'appuyer sur les méthodes de [2] pour calculer une équation différentielle satisfaite par B sans passer par l'équation algébrique. Ce précalcul est ensuite réutilisé pour calculer E grâce à une relation entre E et B. Une diagonale analogue à B permet d'obtenir le développement de M par la même méthode.

Bibliographie

[1] C. Banderier, P. Flajolet, *Basic analytic combinatorics of directed lattice paths*, Theoretical Computer Science 281 (2002) 37–80.

[2] A. Bostan, S. Chen, F. Chyzak, Z. Li, *Complexity of Creative Telescoping for Bivariate Rational Functions*, Proceedings ISSAC'10, ACM Press (2010) 203–210.

[3] M. Bousquet-Mélou, *Discrete Excursions*, Séminaire Lotharingien de Combinatoire, vol. 57, (2008) 1–23.

[4] G. Pólya, *Sur les séries entières, dont la somme est une fonction algébrique*, L'Enseignement Mathématique, vol. 22, (1921–1922) 38–47.

12. Program certification with computational effects

J.-G. Dumas*, D. Duval*, **B. Ekici***, D. Pous†

*LJK, Université de Grenoble, France

†LIP, ENS Lyon, France

{Jean-Guillaume.Dumas,Dominique.Duval,Burak.Ekici}@imag.fr

Damien.Pous@ens-lyon.fr

Dynamic evaluation is a paradigm in computer algebra which was introduced for computing with algebraic numbers. In linear algebra, for instance, dynamic evaluation can be used to apply programs which have been written for matrices with coefficients modulo some prime number to matrices with coefficients modulo some composite number. A way to implement dynamic evaluation in modern computing languages is to use the *exceptions* mechanism provided by the language. In this paper, we pesent a proof system for exceptions which involves both raising and handling, by extending Moggi's approach based on monads. Moreover, the core part of this proof system is dual to a proof system for the *state effect* in imperative languages, which relies on the categorical notion of comonad [Dumas :12 :duality]. Both proof systems are implemented in the Coq proof assistant, and they are combined in order to deal with both effects at the same time.

The *decorated logic* provides a rigorous formalism for proving properties of programs involving computational effects. To start with, let us describe the main features of the *decorated logic for exceptions*. Its syntax is given as follows, where T is any exception name.

$$
\begin{array}{lrcl}
\text{Types :} & t & ::= & A \mid B \mid \ldots \mid t+t \mid \not\vdash \mid V_T \\
\text{Terms :} & f & ::= & id \mid f \circ f \mid [f|f] \mid inl \mid inr \mid [\,] \mid \mathtt{tag}_T \mid \mathtt{untag}_T \\
\text{Decorations :} & (d) & ::= & (0) \mid (1) \mid (2) \\
\text{Equations :} & e & ::= & f \equiv f \mid f \sim f
\end{array}
$$

Here, $\nvdash$ is the empty type while V_T represents the set of values which can be used as arguments for the exceptions with name T. Terms represent functions; they are closed under composition and "copairs" (or case distinction), *inl* and *inr* represent the canonical inclusions into a coproduct (or disjoint union). The basic functions for dealing with exceptions are $\mathtt{tag}_T : V_T \to \nvdash$ and $\mathtt{untag}_T : \nvdash \to V_T$. A fundamental feature of the mechanism of exceptions is the distinction between *ordinary* (or *non-exceptional*) values and *exceptions*. While $\mathtt{tag}_T$ encapsulates its argument (which is an ordinary value) into an exception, $\mathtt{untag}_T$ is applied to an exception for recovering this argument. The usual `throw` and `try/catch` constructions are built from the more basic $\mathtt{tag}_T$ and $\mathtt{untag}_T$ operations [Dumas :14a :coqexc]. We use *decorations* on terms for expressing how they interact with the exceptions. If a term is *pure*, which means that it has nothing to do with exceptions, then it has decoration (0); in particular, $id^{(0)}$, $inl^{(0)}$ and $inr^{(0)}$ are pure. We decorate *throwers* with (1) and *catchers* with (2); clearly $\mathtt{tag}_T^{(1)}$ is a thrower while $\mathtt{untag}_T^{(2)}$ is a catcher. A thrower may throw exceptions and must propagate any given exception, while a catcher may recover from exceptions. Using decorations provides a new schema where term signatures are constructed without any occurrence of a "type of exceptions". Thus, signatures are kept close to the syntax. In addition, decorating terms gives us the flexibility to cope with more than one interpretation of the set of exceptions. This means that with such an approach, any proof in this decorated logic is valid for different implementations of the exceptions. Besides, we have two different kinds of equality between terms : two terms are *weakly equal* if they have the same behavior on ordinary values but may show differences on exceptions, and they are *strongly equal* if they have the same behavior on both ordinary values and exceptions. We respectively use $\sim$ and $\equiv$ symbols to denote weak and strong equalities.

This syntax is enriched with a set of *rules* that are decorated versions of the rules for *equational logic*. The *equivalence* rules ensure that both weak and strong equalities are equivalence relations. The *hierarchy* rules allow to consider any pure term as a thrower, any thrower as a catcher, and any weak equality as a strong one. The "copair" construction $[f, g]$ cannot be used when both f and g are catchers, since this would lead to a conflict when the argument is an exception. But $[f, g]$ can be used when only g is a catcher, it is the catcher $[f, g]^{(2)}$ which is characterized by the equations $[f, g] \circ inl \sim f$ and $[f, g] \circ inr \equiv g$. This means that exceptional arguments are treated by $[f, g]$ as they would be by g. The *substitution* rule for weak equations $f_1^{(2)} \sim f_2^{(2)} \Longrightarrow f_1 \circ g \sim f_2 \circ g$ is valid *only* when the substituted term g is *pure*. The behaviour of the $\mathtt{untag}_T$ functions is given by the rules $\mathtt{untag}_T \circ \mathtt{tag}_T \sim id_T$ and $\mathtt{untag}_T \circ \mathtt{tag}_R \sim [\ ]_R \circ \mathtt{tag}_T$ for all exception names $T \neq R$ (where $[\ ]_R : \nvdash \to R$ is the canonical embedding).

Such a formal system enables us to prove properties of programs involving exceptions. The decorated logic for states and the decorated logic for exceptions, which are mutually dual, are implemented in Coq [Dumas :14a :coqexc]. For instance, we have used these logics for proving the primitive properties of the state effect proposed in [Plotkin :02] and the dual properties of exceptions. To cope with programs including both states and exceptions at the same time, we have composed these Coq implementations, by merging the syntax and the rules. We have also translated the basic imperative programming language IMP in our library, as well as the language IMP_EXC made of IMP extended with exceptions. We have used this implementation to prove some properties of IMP and IMP_EXC programs. For instance, we have checked some simple properties of programs calculating the rank of a (2x2) matrix modulo a composite number using dynamic evaluation [Dumas :14a :coqexc].

We would like to be able to prove more general properties of algorithms for linear algebra using dynamic evaluation implemented through exceptions. For this purpose, we plan to im-

plement Hoare logic for IMP_EXC in decorated terms. We also plan to study other effects (partiality, IO, non-determinism, ...) and to compose them in a systematic way.

Références

[Dumas :14a :coqexc] J.-G. Dumas, D. Duval, B. Ekici, and J.-C. Reynaud. Certified proofs in programs involving exceptions. CICM'14, Coimbra, Portugal, 2014.

[Dumas :14b :coqsts] J.-G. Dumas, D. Duval, B. Ekici, and D. Pous. Formal verification in Coq of program properties involving the global state effect. JFLA, 2014.

[Dumas :12 :duality] J.-G. Dumas, D. Duval, L. Fousse and J.-C. Reynaud. A duality between exceptions and states. Journal of Mathematical Structures in Computer Science 22, p. 719-722(2012).

[Plotkin :02] G.-D. Plotkin, J. Power. Notions of Computation Determine Monads. FoSSaCS 2002. Springer-Verlag Lecture Notes in Computer Science 2303, p.342-356.

13. Efficient algorithms for the design of finite impulse response digital filters

Silviu-Ioan Filip
LIP, ÉNS de Lyon, E.P.I. AriC
46, Allée d'Italie
69364, Lyon, France
silviuioan.filip@ens-lyon.fr

Digital filters represent the foundation for all that is digital signal processing, with widespread applications ranging from data transmission to audio and image processing. A filtering toolchain is comprised of three major steps :

- **derive a concrete mathematical representation for the filter in terms of polynomials or rational functions** ;
- quantization of the filter coefficients using fixed-point or floating-point numerical formats ;
- hardware synthesis of the filter.

We will be concerned with the first step. One of the best known routines for designing digital filters is the Parks-McClellan [4] algorithm. It is an extension of the well known Remez [1] algorithm for minimax polynomial approximation of functions. The problem it tries to solve can be stated in terms of approximating a continuous function on a union of closed intervals over the reals by means of a linear combination of Chebyshev polynomials.

One of the reasons this routine has enjoyed such a wide adoption in the signal processing community is its practical robustness. In this talk we will describe a new implementation of this iterative algorithm which uses recent results related to barycentric

Lagrange interpolation [5] and a numerically stable root finding routine based on determining the eigenvalues of appropriate generalized companion matrices of polynomials [6]. To this end, it shares the same design philosophy as the Remez routine available inside the Chebfun package [2, 3]. To justify the benefits of using our implementation, we will compare it to the de facto one available in Matlab.

We will also try to give some theoretical arguments as to why this filter design routine behaves well in practice, by looking at the numerical stability of the formulas we are using. In particular, our analysis is based on the fact that barycentric Lagrange interpolation is backward stable when a certain Lebesgue constant is small [7].

Bibliography

[1] Remes, E., *Sur le calcul effectif des polynomes d'approximation de Tchebichef. Comptes rendus hebdomadaires des séances de l'Académie des Sciences*, C. P. Paris, 1934.

[2] Driscoll, T.A. ; Hale, N. ; Trefethen, L.N., *Chebfun Guide*, Pafnuty Publications, Oxford, 2014

[3] Pachón, R. ; Trefethen, L.N., *Barycentric-Remez algorithms for best polynomial approximation in the chebfun system*, BIT Numer. Math.,2009

[4] Parks, T. ; McClellan,J., *Chebyshev Approximation for Nonrecursive Digital Filters with Linear Phase*, IEEE Transactions on Circuit Theory 19(2), 1972, pp. 189–194.

[5] Berrut, J-P. ; Trefethen, L.N., *Barycentric Lagrange Interpolation*, SIAM Review, 46, 2004, pp. 501–517.

[6] Boyd, John P., *Finding the Zeros of a Univariate Equation : Proxy Rootfinders, Chebyshev Interpolation, and the Companion Matrix*, SIAM Review, 55(2), 2013, pp. 375–396.

[7] Mascarenhas, W.F. ; Pierro de Camargo, A., *On the backward stability of the second barycentric formula for interpolation*, ArXiv e-prints, 2014, http://arxiv.org/pdf/1310.2516v5.pdf

14. Exploring univariate mixed polynomials

A. Galligo, M. Elkadi
Labo de Mathematiques
Parc Valrose, F-06108 Nice
galligo@unice.fr, elkadi@unice.fr

An expression $P(z,\bar{z}) = \sum_{k=0..n} \sum_{j=0..m} a_{k,j} z^k \bar{z}^j$ where z and $\bar{z}$ are complex conjugated, is called a (univariate) mixed polynomial of bidegree (n,m). We will assume $m \leq n$ and

concentrate on the case where m is small, in particular $m = 1$. Our aim is to study the roots in $\mathbf{C}$ of P. Identifying $\mathbf{C}$ with $\mathbf{R^2}$ and separating real and imaginary parts of P, i.e. writing $P = f(x,y)+ig(x,y)$ with $i^2 = -1$ and $z = x+iy$, we get a pair of real bivariate polynomials of degrees at most $n+m$. Conversely from a pair of bivariate polynomials $(f(x,y), g(x,y))$, letting $x = \frac{z+\bar{z}}{2}$, $y = \frac{z-\bar{z}}{2i}$ and $P = f + ig$, we get a univariate mixed polynomial. However, since the two representations are different, we can investigate interesting roots structures and develop algorithms, intermediate between complex and real algebra. This representation can be also used with several variables $(z_1, .., z_l)$. It received a renewed interest with the works in Algebraic Geometry, authors investigated a new exotic sphere (à la Pham-Brieskorn), more recently Mutsuo Oka [4], thanks to mixed polynomials, answered a question of Milnor on real generalizations of Milnor fibration theorem. Roots of mixed polynomials naturally appear when expressing that a complex polynomial matrix drops rank. It also appears as Taylor expansions of non holomorphic deformations of solutions of wave or elasticity equations. They are central for the study of the complex moment problem. We can also mention the study of real subvarieties of $\mathbf{C^2}$, among others by Moser and his collaborators. Harmonic polynomial and rational maps are important special cases of mixed polynomials ; they have been extensively studied and were applied to the study of gravitational lensing [KN05].

Several techniques developed in Computer algebra are useful for understanding these objects. We revisit, from an algorithmic point of view, the roots study of pairs of real bivariate polynomials (f, g). The case $m = 1$ could be called "almost holomorphic", and we look for properties similar to those of "usual" univariate polynomials. Moreover after simplification it reduces to the study of $\bar{z} = r(z)$, where r is a rational rational map : we will briefly recall recent advances obtained in that field, [3, 5, 1].

One of our tool will be a variant of Vandermonde matrix that we will use to interpolate $P(z, \bar{z})$. Similarly, we will specify a set of roots in $\mathbf{C}$ and investigate the maximum number of other roots in $\mathbf{C}$ admitted by such a constrained mixed polynomial. Unfortunately, the presentation of a univariate polynomial as a product via its roots is not valid in this context. As we will see, although P of bidegree $(n, 1)$ has $2n+2$ coefficients, it may admit more than $2n+2$ roots in $\mathbf{C}$. We will discuss and illustrate this behavior, directly related to bounding the number of zeros of harmonic maps. Beside the case $m = 1$, the results obtained so far on harmonic polynomials, concentrated on m near n, while we are more attracted by small m, see [2]. We will also describe, in small degrees, the partition in semi-algebraic cells of the coefficient spaces corresponding to a given number of roots : their shapes resemble to domains delimited by the generalized "swallow tails" used by R. Thom in his Catastrophes theory.

Another objects of interest are the mixed polynomials, of degrees $(n, 1)$, with given random distribution of coefficients. Experiments with the computer algebra system Maple allowed to observe interesting patterns.

Références

[1] P.M. Bleher, Y. Homma, L.L. Ji and R.K. Roeder, *Counting ze-*

ros of harmonic rational functions and its application to gravitational lensing. arXiv :1206.2273v2 [math.CV] December 2012.

[2] M. Elkadi, A. Galligo, *Exploring univariate mixed polynomials.* Proc. SNC'14 (2014).

[3] D. Khavinson, G.Neumann, *On the number of zeros of certain rational harmonic functions.* Proc. of the AMS, vol 134, 4, pp 1077-85, (2005).

[4] M. Oka , *Non-degenerate mixed functions.* Kodai Math. J. Volume 33, Number 1 (2010), pp. 1-62. arXiv :0909.1904 [math.AG].

[5] S.H. Rhie, *Gravitational lenses with* $5(n-1)$ *images.* arXiv :astro-ph/0305166 (2003).

[6] A. S. Wilmhurst, *The valence of harmonic polynomials.* Proc. Amer. Math. Soc.126, pp 2077–2081 (1998)

15. Calcul des facteurs de petit degré des polynômes lacunaires

B. Grenet
LIRMM - Université Montpellier 2
bruno.grenet@lirmm.fr

La représentation *lacunaire* d'un polynôme est la donnée de la liste de ses monômes non nuls. Une caractéristique de cette représentation est d'être de taille logarithmique en le degré du polynôme. Dans l'exemple de la factorisation

$$1 - X^p = (1 - X) \cdot (1 + X + \cdots + X^{p-1}),$$

le polynôme à factoriser est de taille $O(\log p)$ alors que le second facteur est de taille $O(p)$. Ainsi, il est impossible d'obtenir un algorithme polynomial pour factoriser entièrement un polynôme lacunaire.

Une restriction naturelle pour obtenir un algorithme de complexité polynomiale consiste à ne calculer que les facteurs d'un degré fixé. Cela englobe en particulier le cas important du calcul des racines pour un polynôme à une variable. Une lignée de travaux a conduit à des algorithmes polynomiaux pour le calcul des facteurs de degré borné de polynômes à une variable à coefficients dans un corps de nombres [1, 4], étendus ensuite au cas à plusieurs variables [2, 3].

Dans mon exposé, je présenterai un nouvel algorithme permettant de calculer les facteurs de degré au plus d d'un polynôme lacunaire à plusieurs variables à coefficients dans un corps de nombres, en temps polynomial en la taille du polynôme et en d. Cet algorithme, plus simple et pratique que celui proposé par Kaltofen et Koiran [3], est une réduction du problème au cas de polynômes à une variable d'une part, et au cas de polynômes de petit degré d'autre part. La réduction étant valable pour tout corps de

caractéristique 0, l'algorithme permet également de calculer certains facteurs pour des polynômes à coefficients dans d'autres corps, comme les réels ou ou les p-adiques. Les facteurs manquants sont ceux qui peuvent d'écrire $f(X_1^{\alpha_1} \cdots X_n^{\alpha_n})$ où f est un polynôme à une variable et α_1, ..., α_n sont des entiers.

La preuve de correction de l'algorithme est basée sur le polygone de Newton et le développement en série de Puiseux du polynôme. En particulier, elle fait appel à une borne sur la valuation d'une expression de la forme $g(X, \phi(X))$ où g est un polynôme de petit degré et ϕ une série de Puiseux.

Je présenterai également une implantation de cet algorithme qui est en cours dans le logiciel libre `Mathemagix`.

Références

[1] F. Cucker, P. Koiran, and S. Smale. A polynomial time algorithm for Diophantine equations in one variable. *J. Symb. Comput.*, 27(1) :21–30, 1999.

[2] E. Kaltofen and P. Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *Proc. ISSAC'05*, pages 208–215. ACM, 2005.

[3] E. Kaltofen and P. Koiran. Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields. In *Proc. ISSAC'06*, pages 162–168. ACM, 2006.

[4] H. Lenstra Jr. On the factorization of lacunary polynomials. In *Number theory in progress*, pages 277–291. De Gruyter, 1999.

16. A New Method to Compute the Probability of Collision for Short-term Space Encounters

R. Serra[1], D. Arzelier[1], **M. Joldes**[1],
J.-B. Lasserre[1], A. Rondepierre[2] and B. Salvy[3],

[1]`LAAS-CNRS, 7 Avenue du Colonel Roche, Toulouse, 31400, France`

[2]`IMT/INSA, 135 Avenue de Rangueil, Toulouse, 31077, France`

[3]`INRIA, LIP-ENS Lyon,46 Allée d'Italie, Lyon, 69000 France`

The increasing number of space debris in Low Earth Orbits constitute a serious hazard for operational satellites. In order to provide adequate collision avoidance strategies, it is important to determine the collision probability between two orbiting objects. Three-dimensional Gaussian probability densities represent the position uncertainties of the objects. With some simplifying assumptions, the problem of computing the collision probability, for short-term encounters between space-borne objects, is, in practice, reduced to a two-dimensional integral of a Gaussian function over a bounded region in a

plane normal to the relative velocity vector (encounter frame). The method presented here is based on an analytical expression for the integral. It has the form of a convergent power series whose coefficients verify a linear recurrence. It is derived using Laplace transform and properties of D-finite functions. We focus on its efficient and reliable numerical evaluation. This talk is based on [1].

Références

[1] R. Serra, D. Arzelier, **M. Joldes**, J.-B. Lasserre, A. Rondepierre and B. Salvy, *A New Method to Compute the Probability of Collision for Short-term Space Encounters*, AIAA/AAS astrodynamics specialist conference, American Institute of Aeronautics and Astronautics, pages 1-7, 2014.

17. Sommes binomiales multiples : structure et calcul

A. Bostan
Inria
alin.bostan@inria.fr

P. Lairez
TU Berlin
lairez@tu-berlin.de

B. Salvy
Inria, ENS Lyon
bruno.salvy@inria.fr

Nous définissons précisément une classe de suites, les *sommes binomiales*, close pour de nombreuses opérations (somme, produit, sommation indéfinie, etc) et contenant les coefficients binomiaux. On y trouve toutes les sommes binomiales, y compris les sommes multiples, au sens usuel du terme, comme

$$\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}\sum_{j=0}^{k}\binom{k}{j}^3 \text{ et } \sum_{i=0}^{n}\sum_{j=0}^{n}\binom{i+j}{j}^2\binom{4n-2i-2j}{2n-2i}.$$

Notre premier résultat montre que les sommes binomiales sont exactement les coefficients des diagonales de fractions rationnelles, donnant ainsi une caractérisation intrinsèque des sommes binomiales. Notre second résultat est un algorithme pour décider de l'égalité dans la classe des sommes binomiales. On peut donc prouver de manière entièrement automatique, et relativement rapide, des identités comme

$$\sum_{r=0}^{n}\sum_{s=0}^{n}(-1)^{n+r+s}\binom{n}{r}\binom{n}{s}\binom{n+r}{r}\binom{n+s}{s}\binom{2n-r-s}{n} = \sum_{k=0}^{n}\binom{n}{k}^4.$$

De nombreux outils existent déjà pour traiter ce genre de sommes, et même des sommes bien plus générales que les sommes binomiales, mais une intervention humaine est souvent nécessaire pour conclure les preuves. Ce que nous apportons est un test d'égalité automatique de bout en bout sur la classe précisément délimitée des sommes binomiales.

Dans les deux cas, le principe est d'éviter la représentation des sommes binomiales par des systèmes d'équations récurrentes pour lui préférer la représentation des *séries génératrices* des sommes binomiales par des intégrales multiples de fractions rationnelles. L'idée n'est pas neuve, elle a notamment été exploitée en profondeur par Egorychev [Ego84] mais nous la systématisons et l'automatisons. Par exemple, nous calculons automatiquement que

$$\sum_{n\geq 0} t^n \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 = \frac{1}{(2i\pi)^3} \oint_\gamma \frac{dx\,dy\,dz}{(1-x)(1-y)(1-z)xyz-t(x+yz-xyz)},$$

pour un certain domaine d'intégration γ. En plus des preuves d'identités, ce type de représentation intégrale permet de calculer des récurrences satisfaites par les sommes binomiales. Et les résultats de complexité obtenus précédemment sur l'intégration des fractions rationnelles [BLS13] peuvent se transférer aux sommes binomiales.

Une procédure, appelée *réduction géométrique*, permet de simplifier grandement les représentations intégrales. Si cette étape n'apporte rien à la théorie, elle est cruciale en pratique pour obtenir des intégrales calculables rapidement. Grâce à un algorithme efficace pour l'intégration rationnelle, on obtient ainsi une méthode efficace en pratique, et compétitive avec les autres approches, pour traiter les sommes binomiales.

Le point fort de la méthode concerne les sommes multiples : parfois malaisées en création télescopique, elles sont traitées indifféremment des sommes simples par cette méthode. La nature des calculs est finalement très différente des approches par création télescopique pour les sommes multiples [Weg97,Chy00], et ce dès les définitions : dans l'approche intégrale, le coefficient binomial $\binom{n}{k}$ est défini comme le coefficient de x^k dans $(1+x)^n$; dans l'approche par création télescopique, il est défini par récurrences linéaires et conditions initiales. Si la création télescopique est beaucoup plus générale, l'approche intégrale évite certains problèmes, comme celui des récurrences singulières (c'est-à-dire les récurrences qui donnent $0 = 0$ pour certaines valeurs des indices), ou celui des certificats difficiles à sommer.

Bibliographie

[1] A. Bostan, P. Lairez & B. Salvy, « Creative telescoping for rational functions using the Griffiths–Dwork method », ISSAC Proceedings (2013), p. 93-100.

[2] F. Chyzak, « An extension of Zeilberger's fast algorithm to general holonomic functions », Discrete Math., 217.1-3 (2000), p. 115-134.

[3] G. P. Egorychev, *Integral representation and the computation of combinatorial sums*, Translations of Mathematical Monographs, t. 59, American Mathematical Society, 1984.

[4] K. Wegshaider, *Computer generated proofs of binomial multi-sum identities*, mémoire de master, J. Kepler Universität, Linz, Autriche, 1997.

18. Algorithmes détendus pour les bases d'ordre et leur impact aux méthodes de Wiedemann par blocs

Romain Lebreton

Les bases d'ordre sont un outil fondamental de l'algèbre linéaire à coefficients polynomiaux. Si l'algorithme de Wiedemann par blocs peut aujourd'hui traiter de grands problèmes d'algèbre linéaire creuse, c'est en bonne partie grâce à l'apport des algorithmes rapides de bases d'ordre.

Toutefois, les algorithmes actuels souffrent de deux défauts : ils ne sont pas conçus pour permettre de la terminaison anticipée et ils nécessitent de connaître plus de coefficients de l'entrée que strictement nécessaire.

Dans cet exposé, nous proposons un algorithme en-ligne pour les bases d'ordre qui permet à la fois la mise en place aisée de terminaison anticipée et de ne nécessiter qu'une connaissance minimale de l'entrée tout en gardant une complexité quasi-optimale. L'utilisation de notre algorithme au sein des méthodes de Wiedemann par blocs mène à une amélioration des performances d'un facteur constant. Travail en collaboration avec Pascal Giorgi.

19. Semidefinite approximations of projections and polynomial images of semialgebraic sets

V. Magron, D. Henrion, J.B. Lasserre
LAAS-CNRS
7 avenue du colonel Roche, F-31400 Toulouse, France
magron@laas.fr, henrion@laas.fr, lasserre@laas.fr

Given a compact semialgebraic set $\mathbf{S} \subseteq \mathbb{R}^n$, a polynomial map $f : \mathbf{S} \to \mathbb{R}^m$, we consider the problem of approximating the image set $\mathbf{F} = f(\mathbf{S})$. This includes in particular the projections of $\mathbf{S}$ on $\mathbb{R}^m$, for $n \geq m$. Assuming that $\mathbf{F} \subseteq \mathbf{B}$, with $\mathbf{B} \subseteq \mathbb{R}^m$ being a "simple" set (box or ellipsoid), we provide two methods (called Method 1 and Method 2) to compute certified outer approximations of $\mathbf{F}$:

- The first approach (Method 1) consists in rewriting $\mathbf{F}$ as a set defined with an existential quantifier. Then, one can outer approximate $\mathbf{F}$ as closely as desired with a hierarchy of superlevel sets of the form $\mathbf{F}_r^1 := \{\mathbf{y} \in \mathbf{B} : q_r(\mathbf{y}) \geq 0\}$, for some polynomials $q_r \in \mathbb{R}[\mathbf{y}]$ of increasing degrees $2r$.
- The second approach (Method 2) consists in building a hierarchy of relaxations for the infinite dimensional moment problem whose optimal value is the volume of $\mathbf{F}$ and whose optimum is the restriction of the Lebesgue measure on $\mathbf{F}$. Then, one can outer approximate $\mathbf{F}$ as closely as desired with a hierarchy of super level sets of the form $\mathbf{F}_r^2 := \{\mathbf{y} \in \mathbf{B} : w_r(\mathbf{y}) \geq 1\}$, for some polynomials $w_r \in \mathbb{R}[\mathbf{y}]$ of increasing degrees $2r$.

These two methods output a sequence of superlevel sets defined with a single polynomial that yield explicit outer approximations of $\mathbf{F}$. Finding the coefficients of this polynomial boils down to compute an optimal solution of a semidefinite program. We provide guarantees of strong convergence to $\mathbf{F}$ in $L_1(\mathbf{B})$-norm, when the degree of the polynomial approximation tends to infinity.

We next present some application examples together with numerical results. In particular, we illustrate that our methodology is a unified framework which can tackle important special cases : semialgebraic set projections and Pareto curves approximations. The framework can be extended to approximate images of semialgebraic sets under semialgebraic applications.

20. Irrationalité de la constante d'Apéry : du calcul formel aux preuves formelles

F. Chyzak*, **A. Mahboubi***, T. Sibut-Pinote*, E. Tassi†
*Inria Saclay – Île-de-France,
†Inria Sophia Antipolis – Méditerranée
frederic.chyzak@inria.fr, assia.mahboubi@inria.fr
thomas.sibut-pinote@inria.fr, enrico.tassi@inria.fr

En 1979, Roger Apéry obtient la première démonstration [2] de l'irrationalité de la constante $\zeta(3)$. Comme détaillé par Alfred Van der Poorten [6], cette preuve est une combinaison astucieuse d'arguments remarquablement élémentaires de théorie des nombres et d'asymptotique. La trame de cette preuve repose de façon cruciale sur la découverte d'une relation de récurrence linéaire d'ordre deux commune aux deux suites suivantes :

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \qquad b_n = a_n \sum_{k=1}^{n} \frac{1}{k^3} + \sum_{k=1}^{n} \sum_{m=1}^{k} \frac{(-1)^{m+1} \binom{n}{k}^2 \binom{n+k}{k}^2}{2m^3 \binom{n}{m} \binom{n+m}{m}}. \tag{6}$$

La suite de la preuve consiste à exploiter l'information donnée par cette récurrence, en particulier sur le comportement asymptotique de ses solutions. On conclut ainsi en construisant une approximation rationnelle de $\zeta(3)$ qui converge trop vite pour que sa limite soit elle-même rationnelle.

À la suite des travaux initiés dans les années 1990 par Doron Zeilberger [8, 9], se développe un appareil d'algorithmes permettant des calculs efficaces sur une large classe de suites, dites ∂-finies [4], qui sont avantageusement représentées par des récurrences linéaires et suffisamment de conditions initiales. Ces algorithmes sont implantés comme bibliothèques de systèmes de calcul formel comme Maple ou Mathematica. Ils permettent par exemple de calculer une récurrence commune aux suites (a_n) et (b_n), à partir des définitions 6. Une feuille de travail Maple écrite par Bruno Salvy [7] montre ainsi comment on peut écrire une variante de la preuve d'Apéry utilisant la bibliothèque Algolib [1] pour découvrir la récurrence cruciale.

L'objectif de ce travail est d'utiliser un assistant de preuve, Coq [5], pour construire une preuve formelle complète de l'irrationalité de $\zeta(3)$ à partir d'une telle preuve algorithmique. Nous utilisons un système de calcul formel pour proposer des énoncés candidats pour certains lemmes de la preuve, à propos des relations de récurrence. Ces énoncés sont ensuite prouvés formellement *a posteriori*, de sorte que la preuve formelle finale ne dépend pas de la façon dont ils ont été proposés et peut être rejouée sans faire appel au système de calcul formel. Nous discuterons la mise en œuvre de cette coopération entre systèmes de calcul formel et de preuves formelles ainsi que les prolongements possibles de cette expérience. Ce travail a fait l'objet d'une publication dans les actes de la conférence Interactive Theorem Proving 2014 [3].

Bibliographie

[1] Algolib. http://algo.inria.fr/libraries/, 2013. Version 17.0. For Maple 17.

[2] R. Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 61, 1979. Société Mathématique de France.

[3] F. Chyzak, A. Mahboubi, T. Sibut-Pinote and E. Tassi. A Computer-Algebra-Based Formal Proof of the Irrationality of $\zeta(3)$ In Ruben Gamboa Gerwin Klein, editor, *Interactive Theorem Proving*, volume 8558 of *Lecture Notes in Computer Science*. Springer, 2014.

[4] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities. *J. Symbolic Comput.*, 26(2) :187–227, 1998.

[5] The Coq Proof Assistant. http://coq.inria.fr/, 2014. Version 8.4pl4.

[6] A. van der Poorten. A proof that Euler missed : Apéry's proof of the irrationality of $\zeta(3)$. *Math. Intelligencer*, 1(4) :195–203, 1979. An informal report.

[7] B. Salvy. An Algolib-aided version of Apéry's proof of the irrationality of $\zeta(3)$. http://algo.inria.fr/libraries/autocomb/Apery2-html/apery.html, 2003.

[8] D. Zeilberger. A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.*, 32(3) :321–368, 1990.

[9] D. Zeilberger. The method of creative telescoping. *J. Symbolic Comput.*, 11(3) :195–204, 1991.

21. Automatic Continued Fractions Expansions by *Guess and Prove*

S. Maulat, B. Salvy
LIP, ENS de Lyon
46 Allée d'Italie, Lyon, 69364 France
sebastien.maulat@ens-lyon.fr, bruno.salvy@inria.fr

Continued Fractions. Continued fractions have been used since Euler's time for their remarkable convergence properties [Eul48]. Among the two-dimensional Padé table formed by the rational approximants P/Q to a given complex series, they form a diagonal staircase. Restricting the approximation to the diagonal is usually preferred because it is formally simple to compute.

The analytical and numerical properties of continued fractions have been studied extensively since the 60's, as can be seen in numerous reference books on the topic (*e.g.* [JT80]), and we refer to Brezinski for a historical point of view [Bre81]. As an example, the following formal expansion of the natural logarithm as a so-called *C-fraction* provides an analytic continuation to the whole complex plane cut along the negative real axis :

$$\ln(1+z) = \cfrac{z}{1+\cfrac{a_2 z}{1+\cfrac{a_3 z}{1+\ldots}}} \text{ for all } z,\ (1+z) \in \mathbb{C} \setminus \mathbb{R}_-.$$

where $a_{2k} = \frac{k}{2(2k-1)}$ and $a_{2k+1} = \frac{k}{2(2k+1)}$. Compared to the Taylor series, it not only has a wider convergence domain, but also converges faster on the disk $|z| < 1$.

Automation. In many similar cases of interest, simple formulas can be derived for the coefficients of a continued fraction of this shape. As can be seen in a recent compendium on the topic by Cuyt *et alii* [CPV+08], most expansions are obtained by hand, by specializing a number of formulas. We propose here to use data structures from computer algebra, and proof techniques from experimental mathematics, to obtain such formulas automatically, in a unified manner.

Given a power series, our procedure provides a way of :

- detecting instantly if the coefficients of its C-fraction expansion may satisfy a small-order recurrence,
- computing a simple proof for the formal correspondence of this (infinite) expansion to the input series.

Notably, the proofs are obtained in a generic way, using a single procedure, which contrasts with the limits taken coefficient by coefficient in the literature. As such, this work can also be seen as a new direct proof of the expansion for the exponential function for example [Wal48].

The proof is performed using the very general framework of holonomic series as the underlying function representation.

Under the hood. *Holonomic* functions ([Sta80]), cover a wide class of the so–called *special functions* from mathematical physics, combinatorics, *etc.*. It consists of functions which can be implicitely represented using a linear differential equation with polynomial coefficients, along with initial conditions. Equivalently, a holonomic sequence (of coefficients) is represented using a linear recurrence relation with polynomial coefficients. The efficient implementation of these objects and operations in the maple module gfun [SZ94] served as a basis for experimentation and development, to provide reactive tools.

Among others properties, the class of holonomic functions enjoys an algorithmic ring structure. Interestingly, the fact that division does not preserve holonomicity is not an issue here, thanks to a natural approach in the holonomic world : "guess and prove".

Guess and prove. At first, only a finite order expansion is known, providing say the 30 first terms of the continued fraction. A recurrence on its first coefficients can be computed using standard linear algebra — this is the "guessing" step. In a considerable number of examples, the recurrence order is strikingly small (≤ 3).

The "guessed" recurrence then provides a description of an infinite continued fraction, which must be proved equal to the original function. This verification step first involves simple formulas concerning continued fractions, and the algorithmic closure properties of holonomic sequences. But more crucially, another "guess and prove" step is needed, in order to check the differential equation on the conjectured expansion. This last part is the most time-consuming part of the proof, and necessitated optimizations here.

Bibliographie

[Bre81] Claude Brezinski. The long history of continued fractions and padé approximants. In *Padé approximation and its applications, Amsterdam 1980 (Amsterdam, 1980)*, volume 888 of *Lecture Notes in Math.*, pages 1–27. Springer, Berlin-New York, 1981.

[CPV+08] Annie A.M. Cuyt, Vigdis Petersen, Brigitte Verdonk, Haakon Waadeland, and William B. Jones. *Handbook of Continued Fractions for Special Functions*. Springer Publishing Company, Incorporated, 1 edition, 2008.

[Eul48] Leonhard Euler. *Introductio in analysis infinitorum*. apud Marcum-Michaelem Bousquet & socios, 1748.

[JT80] William B. Jones and W. J. Thron. *Continued Fractions: Analytic Theory and Applications*. Cambridge University Press, 1980.

[Sta80] R. P. Stanley. Differentiably finite power series. *European Journal of Combinatorics*, 1(2):175–188, June 1980.

[SZ94] Bruno Salvy and Paul Zimmermann. GFUN: A maple package for the manipulation of generating and holonomic functions in one variable. *ACM Trans. Math. Softw.*, 20(2):163–177, June 1994.

[Wal48] Hubert Stanley Wall. *Analytic Theory of Continued Fractions*. Van Nostrand, 1948.

22. Topologie du discriminant d'une surface

G. Moroz, M. Pouget
INRIA Nancy - Grand Est
615 Rue du Jardin Botanique, 54600 Villers-lès-Nancy
guillaume.moroz@inria.fr,marc.pouget@inria.fr

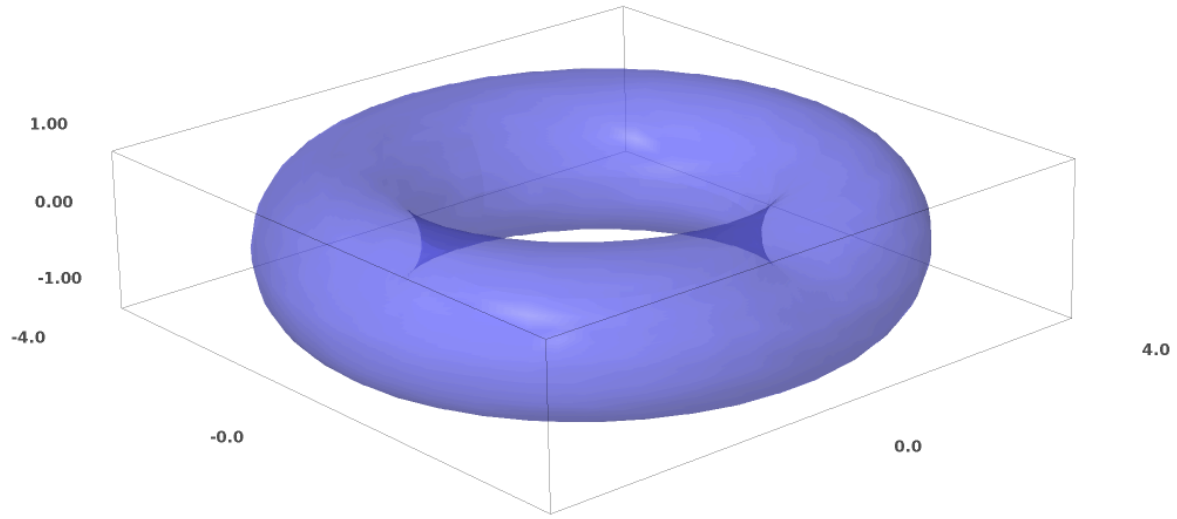

FIGURE 2: Tore et sa silhouette.

Soit S une surface algébrique lisse définie par $f(x, y, z) = 0$. Son discriminant est un polynôme bivarié $\delta(x, y)$. Nous nous intéresserons au calcul de la topologie de la courbe C définie par $\delta(x, y) = 0$, restreinte à une boîte B en x, y. Cette courbe apparait naturellement lorsque l'on cherche à décrire la projection de S sur le plan P_{xy}. La description de C est aussi importante pour classifier les valeurs de (x, y) en fonction du nombre de solutions en z du polynôme $f(x, y, z) = 0$.

Pour décrire la topologie de courbes lisses, on peut distinguer d'une part des méthodes symboliques globales ([MPSTTW06, CLPPPRT10] entre autres) et des méthodes de subdivisions d'autre part (notamment [PV04, LMP08]). L'avantage de l'approche par subdivision est d'être adaptative à la taille de la boîte B dans laquelle on cherche à calculer la topologie.

Cependant, la courbe discriminante C n'est pas nécessairement lisse. En particulier, elle peut contenir des singularités de type nœud ou cusp ordinaire (voir Figure 2 par exemple), qui restent présentes même après perturbation des coefficients de f. Dans ce cas, [BSGY08] est la seule approche par subdivision permettant de calculer la topologie de C. Cette approche n'est malheureusement pas adaptative et pour détecter les singularités de C, elle nécessite de calculer systématiquement des boîtes de diamètre au plus $O(2^{-d^3})$, où d est le degré de $\delta(x, y)$.

Nous présenterons un travail en cours exhibant un critère adaptatif qui permet de

décider si une boîte B contient une singularité de C ainsi que de déterminer la topologie de cette singularité dans B.

Bibliographie

[BSGY08] M. Burr, S.W.Choi, B. Galehouse, and C. Yap. Complete subdivision algorithms, ii : Isotopic meshing of singular algebraic curves. In *International Symposium on Symbolic and Algebraic Computation Symposium - ISSAC*, 2008.

[CLPPPRT10] J. Cheng, S. Lazard, L. Pe naranda, M. Pouget, F. Rouillier, and E. Tsigaridas. On the topology of real algebraic plane curves. *Mathematics in Computer Science*, 4 :113–137, 2010.

[LMP08] C. Liang, B. Mourrain, and J. Pavone. Subdivision methods for 2d and 3d implicit curves. In *Geometric modeling and algebraic geometry*, pages 171–186. Springer, 2008. RR INRIA in 2005.

[MPSTTW06] Bernard Mourrain, Sylvain Pion, Susan Schmitt, Jean-Pierre Técourt, Elias P. Tsigaridas, and Nicola Wolpert. Algebraic issues in Computational Geometry. In J.-D. Boissonnat and M. Teillaud, editors, *Effective Computational Geometry for Curves and Surfaces*, Mathematics and Visualization, chapter 3, pages 117–155. Springer, 2006.

[PV04] S. Plantinga and G. Vegter. Isotopic approximation of implicit curves and surfaces. In *SGP '04 : Eurographics/ACM SIGGRAPH Symposium on Geometry Processing*, pages 245–254, 2004.

23. Computing real points on determinantal varieties and spectrahedra

D. Henrion[1,2,3], **S. Naldi**[1,2,4], M. Safey El Din[4]

[1] CNRS ; LAAS ; 7 avenue du colonel Roche, F-31400 Toulouse ; France.

[2] Université de Toulouse ; LAAS, F-31400 Toulouse, France

[3] Czech Technical University in Prague, Technická 2, CZ-16626 Prague, Czech Republic

[4] Équipe-projet POLSYS (INRIA/UPMC/LIP6)

henrion@laas.fr naldi@laas.fr Mohab.Safey@lip6.fr

Introduction. We are interested in the geometry of real algebraic varieties defined by rank constraints on square matrices whose entries are linear forms with rational coefficients :

$$\mathcal{D} = \left\{ x = (x_1, \ldots, x_n) \in \mathbb{R}^n : A(x) = A_0 + x_1 A_1 + \ldots + x_n A_n \text{ has rank } \leq r \right\}$$

given integers m, n, r and $A_i \in \mathbb{Q}^{m\times m}$ for $i = 0, \ldots, n$. Sets of this type are defined by collections of minors of A and are called *real determinantal varieties*. They are ubiquitous in the mathematical sciences and in applications. If $A_0, \ldots, A_n$ lie in some linear subspace of $\mathbb{Q}^{m\times m}$, so does $A(x)$. In particular, if they are symmetric, then the set

$$\mathcal{S} = \Big\{x \in \mathbb{R}^n : A(x) \text{ is positive semi-definite}\Big\},$$

provided it is full-dimensional, is called the *spectrahedron* associated to A. Spectrahedra are affine sections of the cone of positive semi-definite matrices, and also convex basic semi-algebraic sets (for example, polyhedra are particular examples of spectrahedra, when all the matrices A_i commute, and in particular if they are all diagonal). These are the feasible sets of *semidefinite programming*, whose goal is to minimize linear functions over $\mathcal{S}$. Now, solutions to semidefinite programs are algebraic points lying in the boundary of the set $\mathcal{S}$, which is a subset of the hypersurface defined by $\det A(x) = 0$. In general, the matrix A has rank defects at all points of the boundary of $\mathcal{S}$: this provides a geometric relation between the stratifications of the rank of A and the set $\mathcal{S}$. Hence, it is a problem of primary importance to design exact algorithms solving efficiently what follows :

- decide whether $\mathcal{S}$ is empty or not ;
- compute the smallest rank atteined by $A(x)$ on $\mathcal{S}$;
- compute a point on the boundary of $\mathcal{S}$ where the smallest rank is attained.

Also, in some applications, the matrix $A(x)$ belongs to some fixed subspace of $\mathbb{Q}^{m\times m}$, for example the space of Hankel or Hurwitz matrices. We also consider these *structured* situations which often occur and are interesting in different areas.

Contributions. Our main contribution is the construction of an exact algorithm for finding at least one point in every connected component of the set $\mathcal{D}$. This is a particular instance of the general problem of solving systems of polynomial equations over the real numbers and represents a possible strategy to decide the emptiness of such sets : in fact, if the rank of $A(x)$ is at most r at some real point x, then $\mathcal{D}$ is non-empty and the algorithm is expected to give as output a representation of a finite set of points containing at least one point per connected component of the real set ; otherwise it returns the empty set.

Under genericity assumptions on the entries of $A_0, \ldots, A_n$, the aforementioned algorithm produces a rational parametrization of a finite set intersecting each connected components of $\mathcal{D}$; in case of success its runtime is essentially quadratic on a multihomogeneous Bézout bound on the number of complex solutions, which is strictly upper bounded by $\binom{m(m-r)+n}{n}^3$. In particular, when the size of the matrix is fixed, the complexity is at most polynomial in the number of variables. Moreover, it has a good asymptotic behavior (when both m and n go to infinity). This improves the state of the art since algorithms solving this problem typically require (at most) $d^{\mathcal{O}(N)}$ arithmetic operations when dealing with a polynomial equation of degree d in N variables. This improvement arises from the particular nature of the polynomial system under study, and we will also discuss numerical results supporting this theoretical complexity gain.

The interesting fact is that if the linear matrix has a structure in the sense mentioned above, the bounds on the number of solutions computed by the algorithm are significantly smaller, and the same holds for the computational complexity. For example, the previous Bézout bounds for affine sections of symmetric matrices and Hankel matrices are respectively $\binom{(m-r)(m+r+1)/2+n}{n}^3$ and $\binom{2m-r-1+n}{n}^3$.

Finally, this algorithm can be used to compute points lying on the boundary of a given spectrahedron. This is possible since, in the symmetric case, the boundary of the spectrahedron $\mathcal{S}$ of $A(x)$ contains a connected component of the determinantal variety $\mathcal{D}$ where r is the minimum possible rank appearing on $\mathcal{S}$. This result proves that our algorithm computes a small-rank point lying on the boundary of $\mathcal{S}$ (if $\mathcal{S} \neq \varnothing$) and that it can answer the three questions mentioned above. The complexity of this problem is also a polynomial function of the aforementioned multihomogeneous Bézout bound on the number of complex solutions for symmetric linear matrices. This fact is remarkable because we can derive a complexity estimate for the problem of deciding the emptyness of spectrahedra.

24. List-decoding Reed-Solomon codes : re-encoding techniques and Wu algorithm via simultaneous polynomial approximations

Claude-Pierre Jeannerod[†], Vincent Neiger[†‡], Éric Schost[‡] and Gilles Villard[†]

[†] LIP, ENS de Lyon, France

[‡] University of Western Ontario, London ON, Canada

L'algorithme de Guruswami et Sudan pour le décodage en liste des codes de Reed-Solomon, tel qu'il est présenté dans [6], a un coût élevé et est ainsi difficilement exploitable en pratique y compris pour tailles de codes usuelles et des jeux de paramètres qui ne sont pas très éloignés du cadre du décodage unique. Ainsi, depuis une quinzaine d'années beaucoup de travaux se sont intéressés à réduire la complexité de l'étape la plus coûteuse de cet algorithme, souvent appelée « étape d'interpolation », qui consiste à calculer un polynôme bivarié non trivial qui s'annule en un certain nombre de points avec une multiplicité donnée et des contraintes de degré.

L'algorithme original construit un système linéaire, sous-déterminé par choix des paramètres de décodage, et en calcule une solution non triviale. Il y a essentiellement deux approches qui ont permis d'améliorer la complexité théorique pire-cas de cet algorithme, en résolvant exactement le même problème d'interpolation mais en le reformulant afin de tirer parti d'algorithmes rapides en calcul formel. Une approche, développée d'abord dans un cas particulier dans [9] puis récemment généralisée [12, 4] exploite l'algorithmique des matrices structurées ; l'autre approche [1, 8, 2] exploite la réduction de réseaux

polynomiaux, et est en ce sens une transcription au contexte polynomial des algorithmes de PGCD approché dans le cas entier [5]. Dans cet exposé, nous insisterons d'abord sur le fond commun de ces deux approches : la recherche d'une solution non triviale d'un problème d'approximations polynomiales simultanées avec des contraintes de degrés.

Ensuite, nous aborderons la technique dite de *ré-encodage* [7] qui, par le biais d'une translation du mot reçu, permet de connaître partiellement la solution de l'étape d'interpolation. Nous observerons que cette technique se traduit en une réduction de la taille du problème d'approximation, dans des proportions très intéressantes pour les paramètres pratiques. Tous les algorithmes basés sur ce problème d'approximation semblent pouvoir bénéficier directement de cette technique. Une autre technique, également observable comme une réduction de la taille du problème d'approximation, a été récemment introduite [10] ; si la réduction semble moins spectaculaire, cette technique peut se combiner à la précédente et son intérêt pratique est à étudier.

Une autre grande avancée vers un décodage en liste utilisable en pratique a été réalisée avec l'algorithme de Wu [11]. Cet algorithme commence par transformer le problème de décodage en un autre problème similaire, pour lequel l'étape d'interpolation demande une multiplicité nettement inférieure (dans les cas pratiques où la dimension du code est proche de sa longueur) à celle demandée par l'étape d'interpolation de l'algorithme de Guruswami-Sudan. Nous montrerons comment l'étape d'interpolation de l'algorithme de Wu peut se voir comme un problème d'approximations polynomiales simultanées, de telle manière que les algorithmes rapides développés pour le décodage en liste usuel pourront être réutilisés dans ce cadre. Ceci étend certains résultats présentés dans [3].

References

[1] M. Alekhnovich. Linear diophantine equations over polynomials and soft decoding of Reed-Solomon codes. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS'02, pages 439–448, Washington, DC, USA, 2002. IEEE Computer Society.

[2] P. Beelen and K. Brander. Key equations for list decoding of Reed-Solomon codes and how to solve them. *Journal of Symbolic Computation*, 45(7):773–786, 2010.

[3] P. Beelen, T. Hoholdt, J.S.R. Nielsen, and Yingquan Wu. On rational interpolation-based list-decoding and list-decoding binary Goppa codes. *IEEE Transactions on Information Theory*, 59(6):3269–3281, June 2013.

[4] M. F. I. Chowdhury, C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Faster algorithms for multivariate interpolation with multiplicities and simultaneous polynomial approximations. *http://arxiv.org/abs/1402.0643*, 2014.

[5] H. Cohn and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. In Bernard Chazelle, editor, *ICS*, pages 298–308. Tsinghua University Press, 2011.

[6] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[7] R. Koetter, J. Ma, and A. Vardy. The re-encoding transformation in algebraic list-decoding of Reed-Solomon codes. *Information Theory, IEEE Transactions on*, 57(2):633–647, Feb 2011.

[8] K. Lee and M. E. O'Sullivan. List decoding of Reed-Solomon codes from a Gröbner basis perspective. *Journal of Symbolic Computation*, 43(9):645 – 658, 2008.

[9] R. M. Roth and G. Ruckenstein. Efficient decoding of Reed-Solomon codes beyond half the minimum distance. *IEEE Transactions on Information Theory*, 46(1):246 –257, January 2000.

[10] C. Senger. Prefactor reduction of the Guruswami-Sudan interpolation step. *Information Theory, IEEE Transactions on*, PP(99):1–1, 2014.

[11] Y. Wu. New list decoding algorithms for Reed-Solomon and BCH codes. *IEEE Transactions on Information Theory*, 54(8):3611 –3630, August 2008.

[12] A. Zeh, C. Gentner, and D. Augot. An interpolation procedure for list decoding Reed-Solomon codes based on generalized key equations. *IEEE Transactions on Information Theory*, 57(9):5946–5959, September 2011.

25. Harmonic sums and polylogarithms at non-positive integers

Gerard.H.E. Duchamp, Vincel. Hoang Ngoc Minh, **Quoc Hoan. Ngo**
Universite Paris 13, LIPN
99 avenue Jean-Baptiste Clement, 93430 Villetaneuse.

We are interested in the implementation in Maple of the following objets

$$H_{-s_1,..,-s_r}(N) = \sum_{N\geq n_1>...>n_r>0} n_1^{s_1}...n_r^{s_r}, \forall N \in \mathbb{N}_+, \tag{7}$$

$$Li_{-s_1,...,-s_r}(z) = \sum_{n_1>...>n_r>0} z^{n_1} n_1^{s_1}...n_r^{s_r}, \forall z \in \mathbb{C}, \tag{8}$$

$$\zeta(-s_1,...,-s_k) = \sum_{n_1=0}^{\infty} ... \sum_{n_k=0}^{\infty} (1+n_1)^{s_1} ... (k+n_1+...+n_k)^{s_k}, \tag{9}$$

where $s_1, ..., s_k$ are non-negative integers. [1].

Precisely,

– We prove that $H_{-s_1,..,-s_r}(N)$ is a polynomial of degree $s_1+...+s_r+r$ of N and we give the explicit formula to compute the constants $C_{-s_1,...,-s_r}$ such that

$$\lim_{N\to\infty} \frac{C_{-s_1,...,-s_r} N^{s_1+...+s_r+r}}{H_{-s_1,..,-s_r}(N)} = 1. \tag{10}$$

1. Quantities in eq. 9 are divergent, the aim of this work is to give tools to approach these divergences.

– We prove also that $Li_{-s_1,\ldots,-s_r}(z)$ is a polynomial of degree $s_1+\ldots+s_r+r$ of $(1-z)^{-1}$ and we give the explicit formula to compute the constants $B_{s_1,\ldots,s_r}$ such that

$$\lim_{z\to 1^-} \frac{B_{s_1,\ldots,s_r}(1-z)^{-(s_1+\ldots+s_r+r)}}{Li_{s_1,..,s_r}(z)} = 1. \tag{11}$$

– We give the shuffle structure for (7).
– We study the values of (9) at negative integers, by analytic prolongation.

Bibliographie

[1] Gerard.H.E. Duchamp, V. Hoang Ngoc Minh, A.I. Solomon, S. Goodenough, *An interface between physics and number theory*, in Journal of Physics (2011), 284(1), pp 012 - 023.

[2] Yasushi. Komori, *An integral representation of multiple Hurwitz-Lerch zeta functions and generalized multiple Bernoulli numbers*, Quart. J.Math.61 (2010), 437-496.

[3] Gerard.H.E. Duchamp,L. Poinsot, A.I. Solomon, K.A. Penson, P. Blasiak, A. Horzela, *Ladder Operators and Endomorphisms in Combinatorial Physics*, in Discrete Mathematics and Theoretical Computer Science, Vol 12 :2, 23-46 (2010).

[4] Gerard.H.E. Duchamp,L. Poinsot, A.I. Solomon, K.A. Penson, P. Blasiak, A. Horzela, *Finite polyzetas, Poly- Bernoulli numbers, identities of polyzetas and noncommutative rational power series*, in Proceedings of 4^{th} International Conference on Words, 232- 250 (2003).

[5] S. Goodenough, C. Lavault, , *On subsets of Riordan subgroups and Heisenberg - Weyl algebra*, arXiv :1404.1894v1 [cs.DM] (7 Apr 2014).

26. Computations on symbolic floating point numbers

C.-P. Jeannerod, N. Louvet, J.-M. Muller, **A. Plet**
Département, Laboratoire de l'Informatique du Parallélisme
46 Allée d'Italie, Lyon 69364
antoine.plet@ens-lyon.fr

In a computer, real numbers are often approximated by a finite discrete set called floating point numbers. Therefore, any computation leads to an error we have to care about. When it comes to compute successive basic operations, a naive algorithm can lead to a huge relative error on the result. For example, for an expression as simple as a 2x2 determinant, you can get a relative error bigger than 1 which is not acceptable. Any algorithm computing over floating point numbers should be given with a bound on the possible output error. Such a proof of accuracy can sometimes be independent from the

precision or from the rounding scheme, then covering various standard formats defined in IEEE754-2008 [1].

The next step to achieve a complete analysis of an algorithm is to provide an optimal error bound. Testing the optimality for all the possible inputs does not scale with the increasing precision we are able to compute and the optimality of the error bound in [3] comes from a generic example, parametrized with the precision. Let's call it a symbolic floating point number. However, the computations on such generic examples are done by hand which is time demending and error prone. We propose two methods to compute additions and multiplications followed by a rounding operation on symbolic floating point numbers. Those methods are valid for a subset of floating point numbers which could be called sparse symbolic floating point numbers and for the default rounding scheme "round to nearest ties to even".

The first method relies on the evaluation-interpolation scheme available for polynomial computations. Sparse symbolic floating point numbers can be represented as a polynomial. The dependency on the precision goes all to the evaluation point and none to the polynomial. That is, for every possible precision, the floating point number can be seen as the evaluation of the same polynomial at a different point. Of course, when we add or multiply such numbers with one another, without any rounding operation, we keep the same property. The interesting and non trivial fact is that for the default rounding scheme, the polynomial point of view is still valid after the rounding operation : the result is a new polynomial, evaluated in the same symbolic value. Thus, one can compute the result of a symbolic floating point operation from numerical evaluations of the operation for various precisions and then get the results back to the symbolic word.

The second method is inspired from the natural way to compute on floating point numbers. We first locate the most significant digit and deduce the position of the least significant digit. Then we can decide how to truncate and compensate the initial number to get the right result according to the rounding scheme.

We implemented those two methods which allowed us to instantly check the available examples in [2], [3], [4].

References

[1] IEEE Computer Society, *IEEE Standard for Floating-Point Arithmetic*, Available at http ://ieeexplore.ieee.org/servlet/opac ?punumber=4610933

[2] R. Brent, C. Percival, P. Zimmermann, *Error Bounds on Complex Floating-Point Multiplication*, Mathematics of Computation 76 (2007), pp. 1469–1481

[3] C.-P. Jeannerod, N. Louvet, J.-M. Muller, *On the componentwise accuracy of complex floating-point division with an FMA*, Proceedings of the 21st IEEE Symposium on Computer Arithmetic (2013), pp. 83–93

[4] C.-P. Jeannerod, N. Louvet, J.-M. Muller, *Further analysis of Kahan's algorithm for the accurate computation of* 2×2 *determinants*, Mathematics of Computation 82 (2013), pp. 2245–2264

27. Symbolic Computation for Boundary Problems and Green's Operators

M. Rosenkranz

School of Mathematics, Statistics & Actuarial Science
University of Kent, Canterbury CT2 7NF, Kent, UK

Currently :
Laboratoire d'Informatique Fondamentale de Lille
Université Lille 1, 59000 Lille, France

Classical differential algebra provides powerful methods for analyzing and manipulating differential equations (both linear and nonlinear) but lacks tools for dealing with boundary conditions. In [1, 2] we have introduced a new paradigm for incorporating integral operators (also known as Rota-Baxter operators) into ordinary differential algebras. This allows us to formulate, compute and factor the solution operator (usually called Green's operator) of two-point as well as Stieltjes boundary problems for a linear ordinary differential equation (LODE), relative to a given fundamental system.

In the case of linear partial differential equations (LPDEs), the abstract algebraic framework applies [3], but the formulation of a suitable operator ring over a given partial differential algebra is more subtle (this is work in progress).

We shall give a short survey of the LODE case and some hints about the innovations needed for dealing with LPDEs. A short application in the area of actuarial mathematics illustrates the power of the factorization approach for boundary problems [4, 5]. We round up the talk with a short demo of Anja Korporal's Maple package `IntDiffOp` [6].

Bibliographie

[1] M. Rosenkranz, *A new symbolic method for solving linear two-point boundary value problems on the level of operators*, J. Symbolic Comput. 39/2 (2005), pp. 171–199.

[2] M. Rosenkranz, G. Regensburger, *Solving and factoring boundary problems for linear ordinary differential equations in differential algebras*, J. Symbolic Comput. 43/8 (2008), pp. 515–544.

[3] G. Regensburger, M. Rosenkranz, *An algebraic foundation for factoring linear boundary problems*, Ann. Mat. Pura Appl. (4) 188/1 (2009), pp. 123–151.

[4] H. Albrecher, C. Constantinescu, G. Pirsic, G. Regensburger, M. Rosenkranz, *An algebraic operator approach to the analysis of Gerber-Shiu functions*, Insurance Math. Econom. 46 (2010), pp. 42–51.

[5] H. Albrecher, C. Constantinescu, Z. Palmowski, G. Regensburger, M.

Rosenkranz, *Exact and asymptotic results for insurance risk models with surplus-dependent premiums*, SIAM J. Appl. Math. 73/1 (2012), pp. 47–66.

[6] A. Korporal, G. Regensburger, M. Rosenkranz, *Regular and singular boundary problems in Maple*, Proc. CASC'11, Springer LNCS 6885 (2011).

28. Calcul de bases creuses dans un contexte biologique

François Lemaire, **Alexandre Temperville**
Équipe Calcul Formel, LIFL, Université Lille 1
francois.lemaire@univ-lille1.fr,
a.temperville@ed.univ-lille1.fr

Dans un modèle biologique régi par un système de réactions entre plusieurs espèces, une loi de conservation est une combinaison linéaire constante dans le temps de concentration d'espèces. Le calcul d'une base de lois de conservations revient à calculer une base d'un noyau de matrice.

Il n'y a pas unicité de la base, cependant un utilisateur pourra en préférera une à d'autres, selon ses propres critères. Dans ce contexte biologique, certaines bases sont plus intéressantes que d'autres. Favoriser les bases creuses avec le plus de coefficients positifs semblent être de bons critères. Cependant, combiner ces deux critères n'est pas toujours possible. Nous nous intéresserons ici à calculer une base la plus creuse possible, dans le sens où elle contient le moins de coefficients non-nuls possible. Le problème des coefficients positifs n'est pas traité pour l'instant.

Nous avons développé dans [1] un algorithme glouton qui permet de rechercher une telle base. À chaque étape, l'algorithme améliore un vecteur de la base (par des combinaisons linéaires) jusqu'à obtenir une base la plus creuse possible.

Des temps de calculs effectués sur la base de données BioModels [2] seront présentés.

Bibliographie

[1] François Lemaire and Alexandre Temperville, *On Defining and Computing "Good" Conservation Laws*, P. Mendes et al. (Eds.) : CMSB 2014, LNBI 8859, 2014.

[2] BioModels DataBase, *http ://www.ebi.ac.uk/biomodels-main/publmodels*, Online ; accessed June 16th, 2014.

29. Précision p-adique, application à la résolution d'équations différentielles

P. Lairez, **T. Vaccon**
TU Berlin, Université de Rennes 1
lairez@tu-berlin.de,tristan.vaccon@univ-rennes1.fr

Ces deux dernières décennies ont vu une hausse de la popularité des méthodes p-adiques en calcul formel. Par exemple :

- dans [1], A.Bostan et ses co-auteurs ont utilisé des sommes de Newton pour des polynômes sur les les p-adiques afin de calculer des produits composés de polynômes sur des corps finis ;
- dans [3] P.Gaudry et ses co-auteurs ont utilisé des méthodes de relevés p-adiques pour générer des courbes hyperelliptiques de genre 2 à multiplication complexe ;
- dans [4] K.Kedlaya a utilisé une cohomologie p-adique pour compter des points sur des courbes hyperelliptiques sur des corps finis ;
- dans [5], R.Lercier et T.Sirvent calculent des isogénies entre courbes elliptiques sur des corps finis par la résolution d'équations différentielles dans $\mathbb{Z}_p$.

Cependant, de même que pour les nombres réels, la manipulation sur machine des nombres p-adiques se fait nécessairement de manière approchée, ce qui amène au problème de la gestion de la précision.

Dans [2], X.Caruso, D.Roe et moi-même proposons une manière optimale et géométrique de gérer la précision. Elle repose sur le résultat d'analyse suivant :

Lemme 1 *Soient E et F deux $\mathbb{Q}_p$-espaces vectoriels de dimension finie. Soit $f : E \to F$ une fonction. On suppose que f est différentiable en un certain point $v_0 \subset U$ et que la différentielle $f'(v_0)$ est surjective.*

Alors, il existe un $\delta \in \mathbb{R}_+^*$ tel que pour tout $0 \leq r \leq \delta$:

$$f(v_0 + B(0,r)) = f(v_0) + f'(v_0) \cdot B(0,r). \tag{12}$$

On peut interpréter $B(0,r)$ dans le lemme comme la donnée de précision sur l'entrée v_0 et on voit alors que la précision (optimale) sur la sortie $f(v_0)$ est donnée par $f'(v_0) \cdot B(0,r)$.

De plus, on peut effectivement déterminer un δ comme dans le lemme, via un calcul des normes des différentielles supérieures. Enfin, l'exemple du calcul de la suite SOMOS 4 montre qu'une méthode "de relevés arbitraires" permet d'atteindre la précision optimale même à travers un algorithme qui naïvement perdrait trop de précision.

Nous souhaitons présenter un travail en cours, dans lequel nous calculons la perte de précision optimale pour les équations différentielles étudiées dans [1] et [5]. Celles-ci sont de la forme $y' = g(x)h(y(x))$ avec $g, h \in \mathbb{Z}_p[[x]]$, $g(0) = h(0) = 1$, et en sachant qu'elle admet une solution $y_0 \in \mathbb{Z}_p[[x]]$. [1] et [5] montrent que connaissant g et h à précision $O(p^N)$, on connait le coefficient d'ordre n de y_0 à précision $O(p^{N-\log_p^2 n})$.

Grâce à la méthode différentielle, nous montrons que la précision intrinsèque sur ce n-ème coefficient est $O(p^{N-\log_p n})$. De plus, nous donnons des bornes explicites permettant d'atteindre cette perte de précision : $N > 2\log_p n$.

Enfin, grâce à l'application de la méthode "des relevés arbitraires", nous expliquons comment atteindre cette perte de précision de manière effective et efficace par une méthode de Newton.

Cet exposé sera ainsi l'occasion, à travers l'étude de ces équations différentielles, de présenter et d'illustrer à la fois la précision différentielle en p-adique et la méthode "des relevés arbitraires".

Bibliographie

[1] A. Bostan, L. González-Vega, H. Perdry, É. Schost, *From Newton sums to coefficients : complexity issues in characteristic p*, Proceedings MEGA'05 (2005).

[2] X. Caruso, D. Roe, T. Vaccon *Tracking p-adic precision*, LMS Journal of Computation and Mathematics, volume 17, issue A, pp. 274-294.

[3] P. Gaudry, T. Houtmann, A. Weng, C. Ritzenthaler, D. Kohel, *The* 2*-adic CM method for genus* 2, Asiacrypt 2006, vol. 4284 of Lecture Notes in Comput. Sci. (2006), 114–129

[4] K. Kedlaya, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001)

[5] R. Lercier, T. Sirvent, *On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field*, J. Théorie des Nombres de Bordeaux **20** (2008), 783–797

30. Multiplication rapide d'entiers et de polynômes

Joris van der Hoeven
Laboratoire d'informatique, UMR 7161 CNRS
Campus de l'École polytechnique
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau
Email : vdhoeven@lix.polytechnique.fr
Travail en commun avec David Harvey et Grégoire Lecerf

Résumé

Un problème fondamental en algorithmique est la multiplication rapide de deux entiers de n bits. Soit $\mathsf{I}(n)$ cette complexité, en supposant le modèle des machines de Turing

avec un nombre fini de bandes. Jusqu'à récemment, la meilleure borne asymptotique pour $\mathsf{I}(n)$ était due à Fürer [1, 2]. Plus précisément, il a montré qu'il existe une constante $K > 1$ avec

$$\mathsf{I}(n) \quad = \quad O\left(n \log n K^{\log^* n}\right), \tag{13}$$

où $\log^* x$ (pour $x \in \mathbb{R}$) désigne l'itérateur du logarithme, c.à.d.,

$$\begin{aligned} \log^* x &:= \min\left\{k \in \mathbb{N} : \log^{\circ k} x \leqslant 1\right\}, \\ \log^{\circ k} &:= \log \underset{k\times}{\circ \cdots \circ} \log. \end{aligned} \tag{14}$$

Dans un travail récent [3], nous avons amélioré cette borne. Utilisant un nouveau type d'algorithme, nous avons montré que $K = 8$ (et même $K = 4$ si une certaine conjecture en théorie des nombres est valide). En optimisant l'approche originale de Fürer, il semble que l'on ne peut pas obtenir mieux que $K = 16$.

Dans un deuxième travail [4], nous avons également montré comment adapter notre méthode à la multiplication de polynômes de degré $\leqslant n$ à coefficients dans un corps fini $\mathbb{F}_q$. Plus précisément, désignant par $\mathsf{M}_q(n)$ cette complexité, nous montrons que

$$\mathsf{M}_q(n) \quad = \quad O\left((n \log q) \log(n \log q)\, K^{\log^*(n \log q)}\right),$$

uniformément en q. Ici encore, on peut prendre $K = 8$ (et même $K = 4$ si certaines conjectures en théorie des nombres sont valides). Auparavant, pour q fixé, la meilleure borne connue était $\mathsf{M}_q(n) = O(n \log n \log\log n)$.

Dans notre exposé, nous survolerons les idées principales derrière ces résultats.

Références

[1] M. Fürer. Faster integer multiplication. In *Proceedings of the Thirty-Ninth ACM Symposium on Theory of Computing, STOC 2007*, pages 57–66, New York, NY, USA, 2007. ACM Press.

[2] M. Fürer. Faster integer multiplication. *SIAM J. Comput.*, 39(3) :979–1005, 2009.

[3] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. Technical report, HAL, 2014. .

[4] D. Harvey, J. van der Hoeven, and G. Lecerf. Faster polynomial multiplication over finite fields. Technical report, HAL, 2014. .

31. Complexité du calcul de bases de Gröbner pour des systèmes homogènes avec poids

J.-C. Faugère, M. Safey El Din, **T. Verron**

Équipe PolSys, LIP6, UPMC Sorbonne Universités, INRIA, CNRS

jean-charles.faugere@inria.fr,

mohab.safey@lip6.fr,thibaut.verron@lip6.fr

La résolution de systèmes polynomiaux est un problème important aux applications multiples, et nous nous intéressons ici à sa résolution via le calcul de bases de Gröbner, introduites par Buchberger [1]. Une stratégie de calcul de bases de Gröbner (dite stratégie normale) consiste à réduire des paires de polynômes, en commençant par les paires de plus bas degré. Génériquement, en arrêtant le calcul à un degré d, on obtiendra l'ensemble des polynômes de degré inférieur à d dans la base, et on dispose de bornes de complexité pour estimer *a priori* la difficulté du calcul. En revanche, pour des systèmes structurés provenant d'applications, il arrive que l'on observe des chutes de degré. Ce comportement complique significativement l'obtention de bornes de complexité reflétant la stratégie de calcul.

Ces chutes de degré sont corrélées à la non-régularité des composantes homogènes de plus haut degré du système, c'est-à-dire que le critère $\mathsf{F_5}$ ne permet pas d'éliminer toutes les réductions à zéro entre ces composantes. On peut par conséquent chercher à "modifier" ces composantes homogènes de plus haut degré, de manière à ce qu'elles forment une suite régulière, et qu'ainsi les calculs soient plus prédictibles et plus rapides.

Dans cet exposé, nous étudions une possibilité pour ainsi régulariser le calcul de bases de Gröbner, qui consiste à élargir la définition du degré en affectant des poids arbitraires aux variables. Plus précisément, on s'intéresse à la résolution de systèmes homogènes avec poids (ou quasi-homogènes, [6]), ce qui généralise la notion d'homogénéité. Étant donné un système de poids $W = (w_1, \ldots, w_n) \in \mathbb{Z}_{>0}^n$, on définit le degré pondéré d'un monôme $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ comme la somme pondérée de ses degrés en chaque variable : $\deg_W(X_1^{\alpha_1} \cdots X_n^{\alpha_n}) = \sum_{i=1}^n w_i \alpha_i$. Les polynômes homogènes avec poids sont alors les polynômes constitués uniquement de monômes du même degré pondéré. Hors cas triviaux, un calcul de base de Gröbner pour un système homogène avec poids avec la stratégie normale sans poids aura généralement un comportement irrégulier, avec des chutes de degré.

Soit $\mathbb{K}$ un corps et $(f_1, \ldots, f_m) \subset \mathbb{K}[X_1, \ldots, X_n]$ des polynômes homogènes avec poids, de degrés pondérés $(d_1, \ldots, d_m)$. Les polynômes $f_i(X_1^{w_1}, \ldots, X_n^{w_n})$ sont homogènes, de degrés totaux respectifs $(d_1, \ldots, d_m)$. On peut alors utiliser les algorithmes usuels (Buchberger, $\mathsf{F_4}$ [2], $\mathsf{F_5}$ [3]) pour les systèmes homogènes, et expérimentalement, la stratégie normale redevient régulière génériquement. L'enjeu est alors de justifier ce comportement par la théorie.

Si l'on considère des idéaux zéro-dimensionnels définis par une suite régulière ($m = n$), le nombre de solutions du systèmes est borné par la borne de Bézout, et nous avions proposé ([5]) une borne sur le degré à atteindre dans les réductions de polynômes (borne de Macaulay : $d_{\text{reg}} \leq \sum_{i=1}^n (d_i - w_i) + \max\{w_j\}$), montrant qu'on peut résoudre un tel système en temps polynomial en le nombre de solutions.

Pour la dimension positive ($m < n$), on généralise la borne de Macaulay pondérée pour les systèmes génériques : $d_{\text{reg}} \leq \sum_{i=1}^m (d_i - w_i) + w_m$. Cette borne améliore la précédente pour les systèmes de dimension zéro, et indique qu'il semble plus efficace de choisir les variables de poids les plus faibles comme les plus petites (phénomène confirmé en pratique). Pour les systèmes surdéterminés ($m > n$), sous une hypothèse supplémentaire sur W, on montre que la semi-régularité est caractérisée par la série de Hilbert de l'idéal. Ceci permet de calculer *a priori* le degré de régularité d'un système semi-régulier.

Des expériences menées à la fois avec des systèmes génériques et issus d'applications confirment que prendre en compte la structure homogène avec poids d'un système permet d'accélérer significativement les calculs.

Bibliographie

[1] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bull.*, 10(3) :19–29, 1976.

[2] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3) :61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[3] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In ISSAC '02, pages 75–83 (electronic), New York, 2002. ACM.

[4] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4) :329–344, 1993.

[5] J.-C. Faugère, M. Safey El Din, and T. Verron. On the complexity of computing Gröbner bases for quasi-homogeneous systems. In ISSAC '13, New York, 2013. ACM.

[6] C. Traverso. Hilbert functions and the Buchberger algorithm. *J. Symbolic Comput.*, 22(4) :355 – 376, 1996.

32. Approximation de racines multiples isolées de systèmes polynomiaux

Marc Giusti, **J.-C. Yakoubsohn**
Laboratoire LIX , Bâtiment Alan Turing, École Polytechnique
91120 Palaiseau
Institut de Mathématiques de Toulouse, Université Paul Sabatier
118 route de Narbonne
31062 Toulouse Cedex 9
Marc.Giusti@polytechnique.fr,yak@mip.ups-tlse.fr

Nous proposons une analyse numérique de l'article **Multiplicity hunting and approximating multiple roots of polynomial systems** écrit par les deux auteurs [1]. Nous y expliquions comment déduire un système régulier d'un système singulier, avec la même racine multiple isolée supposée exactement connue. Nous formalisions cette transformation par la notion de systèmes équivalents en un point. Plus précisément, si w est une racine multiple isolée du système polynomial $f(x) = (f_1(x), \ldots, f_m(x)) \in \mathbf{C}[\mathbf{x}]^{\mathbf{m}}$, avec x dans $\mathbf{C}^{\mathbf{n}}$, notre méthode calcule un système admettant la même racine w, mais régulier (et que nous appelions *équivalent*). Notons que ceci est obtenu **sans ajout de variables**, par une combinaison de deux opérations appelées **déflation (exacte)** et **dénoyautage (exact)**. Observons que la matrice Jacobienne $Df(w)$ n'est pas de rang maximum, et que m est supérieur ou égal à n.

L'opération de **déflation** consiste à remplacer un polynôme $g(x)$ par son gradient $\nabla g(x)$ quand nous avons simultanément $g(w) = 0$ et $\nabla(g(w) = 0$. Une fois que nous ne pouvons plus déflater aucune équation du système, la seconde opération que nous appelons **dénoyautage** consiste à ajouter au système les numérateurs des coefficients (non identiquement nuls) d'un complément de Schur de la matrice jacobienne $Df(x)$.

En combinant ces deux opérations, nous obtenons une suite **dégonflante** (F_k) insistons **sans ajout de nouvelles variables**), définie comme suit :

$$\begin{aligned} F_0 &= f \\ F_1 &= déflaté(F_0) \\ F_{k+1} &= déflaté(dénoyauté(F_k)), \quad k \geq 1. \end{aligned}$$

Dans l'article [1] *loc. cit.*, nous avons prouvé que la multiplicité de la racine w du système F_k de la suite dégonflante décroît strictement. En conséquence, cette suite est finie. Il suffit d'extraire du dernier système n équations de rang maximum pour obtenir un système régulier équivalent.

Nous décrivons ensuite ce qui se passe dans le cadre numérique, où bien sûr la racine w n'est connue qu'approximativement, et traitons un exemple pour illustrer la méthode.

Enfin, nous donnons une estimation de la quantité appelé maintenant classiquement γ dans la littérature [2]. Elle représente en fait une sorte de nombre de conditionnement du système régulier obtenu après déflation. Pour un système polynomial F notons $[F]_w$ la quantité $\sum_{k\geq 1} \frac{\|D^k F(w)\|}{k!}$. Nous expliquerons le résultat suivant :

Theorem 1 *Soit d_k le maximum de l'ordre des déflations requises pour passer de F_k à F_{k+1} et r_k le rang de la matrice jacobienne du système $déflaté(F_k)$. Nous définissons $\mu = \max \mu_k$ où μ_k est la norme de la sous-matrice inversible de rang r_k de DF_k. Soient λ_0 et ρ_0 les quantités telles que $[F_0]_w \leq \frac{\lambda_0 t}{1-\rho_0 t}$. Nous avons alors :*

$$\lambda_{k+1} \leq (4(\sqrt{2}+1)\mu)^k (2+\sqrt{2})^{\sum_{j=1}^k j(d_j+1)-1} \prod_{j=0}^{k} (d_j+1) \lambda_0 \rho_0^{k+\sum_{j=0}^k d_j}$$

$$\rho_{k+1} \leq (2+\sqrt{2})^k \prod_{j=0}^{k} \frac{d_j+2}{2} \rho_0.$$

Références

[1] Giusti, M. and Yakoubsohn, J.-C., *Multiplicity hunting and approximating multiple roots of polynomial systems*, Recent Advances in Real Complexity and Computation : UIMP-RSME Lluis Santalo Summer School 2012, July 16-20, Santander (Cantabria), Spain, 604, 105, 2014.

[2] Smale, Steve, *Newton's method estimates from data at one point*, The Merging of Disciplines : New Directions in Pure, Applied, and Computational Mathematics, 185–196, 1986.