Preuves automatiques d'inégalités entre fonctions spéciales

Stage de M2 en calcul formel

A. Bostan (Inria & U. Paris-Saclay), M. Safey El Din (LIP6, Sorbonne U.) et B. Salvy (Inria, ENS Lyon)

Contexte. Le *calcul formel* est un domaine très dynamique depuis une soixantaine d'années, au carrefour des mathématiques et de l'informatique, visant à rendre effectives et efficaces les parties «algébrisables» des mathématiques [9]. Cette discipline touche plusieurs millions d'utilisateurs par le biais de systèmes comme Maple, Mathematica ou Sage. En tant qu'outils de calcul certifié ou robuste, les logiciels de calcul formel sont utilisés dans divers domaines des mathématiques comme la combinatoire ou la théorie des nombres, mais aussi dans les sciences de l'ingénieur (par exemple en robotique ou biologie) et plus récemment dans les sciences du numérique (par exemple en cryptologie, ou vérification de programmes).

Le sujet de stage développé ici est à la confluence de deux grandes directions de recherche actuelles en calcul formel :

- considérer les équations différentielles et de récurrence non plus comme *à résoudre*, mais comme des structures de données représentant leurs solutions («D-finitude») ;
- prouver des inégalités entre polynômes multivariés et, lorsque cela est possible, fournir des identités algébriques permettant de certifier ces inégalités.

D-finitude. Historiquement, d'importants efforts de recherche en calcul formel ont été consacrés à donner des solutions *en forme close* de divers problèmes. Un exemple spectaculaire est le calcul de primitives, algorithmisé dans les années 1970 à l'aide de théorèmes de structure en algèbre différentielle [30]. Ensuite, de nombreux travaux, notamment ceux de Singer [43], ont étendu la classe des équations différentielles que les logiciels de calcul formel permettent de résoudre explicitement en termes de fonctions dites *liouvilliennes*. Cependant, l'existence de telles solutions est l'exception plutôt que la règle, ce qui réduit l'application de ces algorithmes à des questions de décision, ou à l'initiation aux équations différentielles dans l'enseignement des mathématiques.

Ce sujet de stage s'inscrit dans un effort de développement d'une algorithmique *générale* et *efficace* sur les solutions d'équations différentielles linéaires (dites *différentiellement finies* ou *D-finies*), *représentées implicitement* par une équation différentielle et des conditions initiales. Une série est D-finie si et seulement si la suite de ses coefficients satisfait une relation de récurrence linéaire à coefficients polynomiaux (on dit de cette suite qu'elle est *P-récursive*) [39] ; et là encore, cette récurrence est une structure de données adéquate pour manipuler la suite. Cette classe de fonctions est particulièrement importante du point de vue des applications, puisque de nombreuses fonctions spéciales classiques de physique mathématique ou de mathématiques appliquées sont D-finies [23].

Les principales propriétés mathématiques des fonctions D-finies sont connues depuis le 19-ème siècle. Leur développement moderne en combinatoire et en calcul formel est dû en grande partie à Stanley [38] puis Zeilberger [45], qui ont souligné leur intérêt comme classe de fonctions close par plusieurs opérations importantes et bénéficiant d'une algorithmique riche. L'étude systématique, du point de vue algorithmique, des fonctions D-finies et des suites P-récursives s'est poursuivie depuis [34]. Sur le plan pratique, des logiciels comme le module Maple `gfun` [35] fournissent déjà un grand nombre d'opérations importantes sur cette structure de données.

Preuves d'inégalités polynomiales. La recherche d'algorithmes permettant de prouver des inégalités polynomiales est un sujet ancien qui apparaît déjà dans les travaux de Fourier au début du 19-ème siècle. Quelques années plus tard, les travaux de Sturm et Hermite permettent d'aborder le cas non-linéaire univarié en fournissant des premiers théorèmes « effectifs » pour le comptage de racines réelles.

Le problème général de représentation des polynômes positifs est posé par Hilbert : est-ce que tout polynôme positif sur les réels peut s'écrire comme une somme de carrés de polynômes (fournissant ainsi un certificat de positivité) ? C'est le 17-ème des problèmes posés par Hilbert pour la recherche mathématique au 20-ème siècle. Il trouve une réponse évidemment positive dans le cas univarié. Artin montre que les polynômes positifs sont en fait des sommes de carrés de fractions rationnelles [2]. Des exemples de polynômes positifs qui ne sont pas des sommes de carrés de polynômes sont donnés par la suite (voir par exemple [18]). Ces premiers travaux constituent le socle de l'algèbre réelle dont un résultat central est le Positivstellensatz qui décrit la forme générale des identités algébriques permettant de certifier qu'un système d'inégalités polynomiales n'admet pas de solution réelle [16].

Algorithmiquement, ces problèmes sont souvent encore abordés par le calcul de décomposition en sommes de carrés via une réduction à des problèmes de programmation semi-définie positive [17, 19]. Il faut noter néanmoins que les certificats ainsi calculés sont approchés (les programmes semi-définis positifs sont résolus numériquement) et ils sont difficiles à relever en des certificats exacts en général. Aussi, des problèmes de nature diophantienne se cachent ici : un polynôme à coefficients rationnels peut être une somme de carrés de polynômes à coefficients réels sans pour autant admettre une telle décomposition sur les rationnels [36]. Enfin, il est établi que le ratio entre volume du cône des polynômes de degré d qui sont sommes de carrés et volume du cône des polynômes de degré d positifs tend vers 0 lorsque le nombre de variables augmente [5].

Des méthodes complémentaires de nature géométrique sont donc nécessaires. Elles émergent dans les travaux de Tarski [42] et Seidenberg [37] et débouchent sur des algorithmes de recherche de solutions qui sont ensuite développés par Collins [7] puis sous un angle plus orienté vers la complexité théorique [3]. Ainsi, pour montrer qu'un polynôme est positif sur les réels, ces algorithmes cherchent à calculer un point en lequel il est négatif strictement. Pour cela, la méthode classique, dite *méthode de points critiques*, consiste à identifier une fonction polynomiale qui atteindrait ses extrema en chaque composante connexe de l'ensemble des solutions étudié [31, 32]. Si ces extrema sont atteints en un nombre fini de points critiques, le problème initial est ramené à la résolution de systèmes polynomiaux ayant un nombre fini de solutions et qui peut alors être résolu par des outils fondamentaux du calcul formel, comme les bases de Gröbner.

Objectifs. Le sujet de ce stage est

Preuves automatiques d'inégalités entre fonctions spéciales.

Il s'agit de concevoir et valider des algorithmes efficaces dans le domaine de la D-finitude. Pour focaliser le choix des problèmes à étudier, deux objectifs de long terme serviront de guide :

- fournir des outils clé en main pour les utilisateurs de fonctions spéciales, leur permettant de prouver des inégalités telles que celles que l'on trouve dans des articles de recherche récents, comme l'inégalité [29]
$$\frac{1}{(1+r)^{ab/(a+b)}} < \frac{{}_2\mathrm{F}_1\left(\begin{matrix} a & b \\ a+b \end{matrix}\middle| r^2\right)}{{}_2\mathrm{F}_1\left(\begin{matrix} a & b \\ a+b \end{matrix}\middle| r\right)},$$
où ${}_2\mathrm{F}_1$ désigne la fonction hypergéométrique de Gauss, inégalité valide pour tout $a, b > 0$ et $r \in (0, 1)$, où l'exposant du membre gauche est optimal; ou, encore plus récemment [10],
$$\int_0^x e^{-\gamma t} t^{\nu} \mathrm{I}_{\nu}(t)\, dt > 0, \quad x > 0, \nu > -\frac{1}{2}, 0 < \gamma < 1,$$
où I_ν est une fonction de Bessel modifiée.

  Dans les deux cas, les objets en jeu sont solutions d'équations différentielles linéaires qu'il est facile de calculer automatiquement, et qui seront le point de départ de la preuve automatique visée.
- localiser les racines de solutions d'équations différentielles linéaires pour des conditions initiales données, en fournissant des certificats que certains intervalles ne contiennent pas de racines.

État de l'art. Ce domaine de recherche n'est pas complètement vierge. D'abord, dans le cas d'équations sans paramètres, on dispose désormais d'algorithmes semi-numériques permettant de calculer à précision arbitraire *et en fournissant un intervalle certifié* les valeurs de fonctions D-finies [21]. Ces algorithmes reposent en particulier sur des bornes effectives permettant d'encadrer les restes de troncatures de développements en série de Taylor de ces fonctions [22]. Une première idée est d'étudier comment une partie des analyses effectuées pour obtenir ces bornes peut s'étendre au cas paramétré, où les coefficients deviennent des polynômes, et où il s'agirait de reposer sur des preuves d'inégalités de polynômes pour obtenir des bornes dépendant de paramètres. Dans cette direction, il existe plusieurs travaux de l'équipe autour de Kauers et Pillwein [11, 27, 8, 26, 4, 25, 14, 12] sur des questions d'inégalités de suites solutions de récurrences linéaires qui sont particulièrement pertinentes et pour lesquelles nous envisageons des collaborations avec cette équipe autrichienne. Une autre approche récente et très reliée à ces considérations mèle de l'évaluation numérique certifiée sur une représentation intégrale de Cauchy et des bornes effectives [20].

Une autre source d'inspiration provient de la littérature classique sur les équations différentielles linéaires et en particulier le théorème de comparaison de Sturm-Picone [13, 40, 41, 15, 44] qui déduit d'inégalités entre coefficients (polynomiaux) et conditions initiales des inégalités entre solutions. Ces méthodes sont en particulier utilisées classiquement pour comparer les zéros des fonctions de Bessel aux zéros du sinus. L'utilisation de ces méthodes en calcul formel est inédite, et sera une première piste, avant d'aborder les généralisations, notamment aux équations d'ordre supérieur à 2.

Environnement. Ce stage de Master 2 sera co-encadré par Alin Bostan[1], Mohab Safey El Din[2] et Bruno Salvy[3]. Il se déroulera soit dans les locaux du centre Inria Paris-Saclay

[1]Inria & U. Paris-Saclay, alin.bostan@inria.fr
[2]Sorbonne Université, mohab.safey@lip6.fr
[3]Inria & ENS Lyon, bruno.salvy@inria.fr

(Palaiseau), soit au laboratoire d'informatique LIP6 (UMR CNRS 7606) de Sorbonne Université (Paris) soit au laboratoire d'informatique LIP (UMR CNRS 5668) de l'ENS de Lyon. Des rendez-vous hebdomadaires seront organisés en ligne. Le stagiaire sera accueilli dans une équipe dynamique et scientifiquement ambitieuse, et disposera de tous les moyens de calcul nécessaires, qu'ils soient logiciels ou matériels, avec notamment plusieurs serveurs de calculs modernes à disposition.

Les candidatures doivent être envoyées à

alin.bostan@inria.fr, mohab.safey@lip6.fr, bruno.salvy@inria.fr

et contenir un CV, les relevés de notes des deux dernières années scolaires, ainsi qu'une lettre de motivation.

References

[1] A. A. Ahmadi, A. Olshevsky, P. A. Parrilo, and J. N. Tsitsiklis. NP-hardness of deciding convexity of quartic polynomials and related problems. *Math. Program.*, 137(1-2, Ser. A):453–476, 2013.

[2] E. Artin. öUber die Zerlegung definiter Funktionen in Quadrate. *Abh. Math. Sem. Univ. Hamburg*, 5(1):100–115, 1927.

[3] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics).* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[4] J. P. Bell and S. Gerhold. On the positivity set of a linear recurrence sequence. *Israel Journal of Mathematics*, 157:333–345, 2006.

[5] G. Blekherman. There are significantly more nonegative polynomials than sums of squares. *Israel Journal of Mathematics*, 153.1 (2006): 355-380.

[6] F. Boudaoud, F. Caruso, and M.-F. Roy. Certificates of positivity in the Bernstein basis. *Discrete Comput. Geom.*, 39(4):639–655, 2008.

[7] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In *ATFL 2nd GI Conf. Kaiserslautern*, pages 134–183, 1975.

[8] A. Dixit, V. H. Moll, and V. Pillwein. A hypergeometric inequality. *Ann. Comb.*, 20(1):65–72, 2016.

[9] J. von zur Gathen and J. Gerhard. *Modern computer algebra.* Cambridge University Press, New York, 2nd edition, 2003.

[10] R. E. Gaunt. Bounds for an integral of the modified Bessel function of the first kind and expressions involving it. *J. Math. Anal. Appl.*, 502(1):1–16, 2021.

[11] S. Gerhold and M. Kauers. A procedure for proving special function inequalities involving a discrete parameter. In *Proc. of ISSAC'05.* ACM Press, 2005.

[12] S. Gerhold and M. Kauers. A computer proof of Turán's inequality. *Journal of Inequalities in Pure and Applied Mathematics*, 7(2):Article 42, 2006.

[13] E. Kamke. A new proof of Sturm's comparison theorems. *Amer. Math. Monthly*, 46:417–421, 1939.

[14] M. Kauers and V. Pillwein. When can we detect that a P-finite sequence is positive? In *Proceedings of ISSAC '10*, pages 195–201. ACM, New York, 2010.

[15] R. F. King. Improving the Van de Vel root-finding method. *Computing*, 30(4):373–378, 1983.

[16] J.-L. Krivine. Anneaux préordonnés. *J. Analyse Math.*, 12:307–326, 1964.

[17] J.-B. Lasserre. Global Optimization with Polynomials and the Problem of Moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.

[18] M. Laurent. *Sums of squares, moment matrices and optimization over polynomials.* Springer, 2009.

[19] P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization.* PhD thesis, California Inst. Tech., 2000.

[20] S. Melczer and M. Mezzarobba. Sequence positivity through numeric analytic continuation: Uniqueness of the Canham model for biomembranes, 11 2020.

[21] M. Mezzarobba. Rigorous multiple-precision evaluation of D-finite functions in Sagemath. Accepted for publication in the proceedings of ICMS 2016, but withdrawn due to a disagreement with Springer on copyright matters 1607.01967, arXiv, 2016.

[22] M. Mezzarobba and B. Salvy. Effective bounds for P-recursive sequences. *Journal of Symbolic Computation*, 45(10):1075–1096, October 2010.

[23] F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, editors. *NIST Handbook of Mathematical Functions.* Cambridge University Press, 2010.

[24] P. A. Parrilo and B. Sturmfels. Minimizing polynomial functions. In *Algorithmic and quantitative real algebraic geometry (Piscataway, NJ, 2001)*, volume 60 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 83–99. Amer. Math. Soc., Providence, RI, 2003.

[25] V. Pillwein. Positivity of certain sums over Jacobi kernel polynomials. *Advances in Applied Mathematics*, 41(3):365–377, 2008.

[26] V. Pillwein. On the positivity of the Gillis-Reznick-Zeilberger rational function. *Adv. in Appl. Math.*, 104:75–84, 2019.

[27] V. Pillwein and M. Schussler. An efficient procedure deciding positivity for a class of holonomic functions. *ACM Commun. Comput. Algebra*, 49(3):90–93, 2015.

[28] V. Powers. Rational certificates of positivity on compact semialgebraic sets. *Pacific J. Math.*, 251(2):385–391, 2011.

[29] K. C. Richards. A note on inequalities for the ratio of zero-balanced hypergeometric functions. *Proc. Amer. Math. Soc. Ser. B*, 6:15–20, 2019.

[30] R. H. Risch. The solution of the problem of integration in finite terms. *Bulletin of the American Mathematical Society*, 76(3):605–608, 1970.

[31] M. Safey El Din. Computing the global optimum of a multivariate polynomial over the reals. In *Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation*, ISSAC '08, pages 71–78, New York, NY, USA, 2008. ACM.

[32] M. Safey El Din and P.-J. Spaenlehauer. Critical point computations on smooth varieties: Degree and complexity bounds. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 183–190, New York, NY, USA, 2016. ACM.

[33] B. Salvy. D-finiteness: Algorithms and applications. In M. Kauers, editor, *Proc. of ISSAC'05*, pages 2–3. ACM Press, 2005.

[34] B. Salvy. Linear differential equations as a data-structure. *Foundations of Computational Mathematics*, 19(5):1071–1112, 2019.

[35] B. Salvy and P. Zimmermann. Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software*, 20(2):163–177, 1994.

[36] Scheiderer, Claus. Sums of squares of polynomials with rational coefficients. *Journal of the European Mathematical Society*, 18.7 (2016): 1495-1513.

[37] A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, 60:365–374, 1954

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

[39] R. P. Stanley. *Enumerative combinatorics*, volume 2. Cambridge University Press, 1999.

[40] C. A. Swanson. *Comparison and oscillation theory of linear differential equations.* Academic Press, New York-London, 1968.

[41] C. A. Swanson. Picone's identity. *Rend. Mat. (6)*, 8(2):373–397, 1975.

[42] A. Tarski. *A decision method for elementary algebra and geometry.* University of California Press, 1951.

[43] M. van der Put and M. F. Singer. *Galois theory of linear differential equations.* Spinger Verlag, 2003.

[44] W. Walter. A note on Sturm-type comparison theorems for nonlinear operators. *J. Differential Equations*, 135(2):358–365, 1997.

[45] D. Zeilberger. A holonomic systems approach to special functions identities. *Journal of Computational and Applied Mathematics*, 32(3):321–368, 1990.