Résumés des exposés courts

Journées Nationales de Calcul Formel 2015

ENSAM, Cluny

2-6 Novembre 2015

Liste des exposés

1 - Moulay Barkatou : *On Apparent Singularities of Systems of Linear Differential Equations with Rational Function Coefficients* 3
2 - Jérémy Berthomieu : *Algèbre linéaire pour le calcul de bases de Gröbner de suites multidimensionnelles récurrentes linéaires* 3
3 - Yacine Bouzidi : *Computer algebra methods for testing the structual stability of multidimensional systems* 5
4 - Thomas Camus : *Calcul des isométries de réseaux algébriques* 6
5 - Svyatoslav Covanov : *Multiplication rapide d'entiers utilisant des nombres de Fermat généralisés premiers* 8
6 - Philippe Dumas : *Calcul rapide d'un coefficient d'une série algébrique en caractéristique positive* 10
7 - Bruno Grenet : *Calcul de racines sur un corps fini à l'aide de transformées de Graeffe* 11
8 - Pierre Lairez : *Un algorithme déterministe pour calculer une racine approchée d'un système polynomial en complexité moyenne polynomiale* 13
9 - Bernard Mourrain : *Formules de quadrature, extension plate et optimization convexe* 14
10 - Vincent Neiger : *Computing minimal interpolation bases* 15
11 - François Ollivier : *La borne de Jacobi. Déterminant tropical, ordre et formes normales des systèmes d'EDO* 16
12 - Clément Pernet : *Computing the Rank Profile Matrix* 18
13 - Adrien Poteaux : *Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields* 19
14 - Joelle Saadé : *A short survey on Kantorovich-like theorems for Newton's method* 20
15 - Thomas Sibut-Pinote : *Calculs symboliques sur des algorithmes théoriques de produits de matrices* 22
16 - Pierre-Jean Spaenlehauer : *Sparse Polynomial Systems With Many Positive Solutions From Bipartite Simplicial Complexes* 23
17 - Alexandre Temperville : *Simplification de paramètres* 25
18 - Thibaut Verron : *Classification algébrique associée à l'optimisation de contraste pour l'IRM* 26

1. On Apparent Singularities of Systems of Linear Differential Equations with Rational Function Coefficients

Moulay Barkatou
Université de Limoges ; CNRS ; XLIM UMR 5272 ; DMI
moulay.barkatou@unilim.fr

Let (S) $\frac{dY}{dz} = A(z)Y$ be a system of first order linear differential equations with rational function coefficients. The (finite) singularities of (S) are the poles of the entries of the matrix $A(z)$. A singular point z_0 of (S) is called an apparent singularity for (S) if there is a basis of solutions of (S) which are holomorphic in a neighborhood of z_0. In this talk we shall present a new algorithm which, given a system of the form (S), detects apparent singularities and constructs an equivalent system (S') with rational coefficients, whose singularities coincide with the non apparent singularities of (S). Our method can, in particular, be applied to the companion system of any linear differential equation with arbitrary order n. We thus have an alternative method to the standard methods for removing apparent singularities of linear differential operators. We shall compare our method to the one designed for operators and we shall show some applications and examples of computation. This talk is based on a joint work, with S. Maddah, recently presented at ISSAC 2015.

2. Algèbre linéaire pour le calcul de bases de Gröbner de suites multidimensionnelles récurrentes linéaires

J. Berthomieu, B. Boyer, J.-Ch. Faugère
Sorbonne Universités, UPMC Univ Paris 06,
CNRS, INRIA, LIP6 UMR 7606, Équipe PolSys,
4 place Jussieu, 75005 Paris.
jeremy.berthomieu@lip6.fr, brice.boyer@lip6.fr,
jean-charles.faugere@inria.fr

En 1988, Sakata a généralisé l'algorithme de Berlekamp – Massey [Ber68, Mas69] à la dimension n. Cet algorithme, connu sous le nom de Berlekamp – Massey – Sakata [Sak88,

Sak90], peut être utilisé pour calculer une base de Gröbner de l'idéal, de dimension 0, des relations vérifiées par une table. Nous étudions ce problème en utilisant des techniques d'algèbre linéaire, dans l'esprit de ce qui a été fait pour Berlekamp – Massey [KY13], afin d'améliorer, par exemple, les algorithmes de changement d'ordre [FGLM93].

En dimension 1, les suites récurrentes linéaires à coefficients constants sont des objets classiques. En dimension $n \geq 2$, on peut trouver dans la littérature plusieurs définitions de telles suites qui ne sont pas toutes équivalentes [CN92, SH95]. Nous proposons une définition qui étend les propriétés qu'ont de telles suites en dimension 1. En particulier, cette définition permet de caractériser exactement l'idéal des relations et la série génératrice.

Nous présentons aussi plusieurs algorithmes pour calculer une base de Gröbner de l'idéal des relations. Le premier, requérant beaucoup d'éléments de la table, est l'analogue d'un changement de variables linéaire sur l'idéal des relations. Cette méthode probabiliste permet essentiellement, sous des hypothèses de généricité, de ramener le problème à celui du calcul des relations de récurrence d'une suite de dimension 1 et donc à un unique appel à l'algorithme de Berlekamp – Massey.

Il n'est pas rare que la connaissance d'un élément de la table puisse être coûteuse. C'est pourquoi, nous nous plaçons ensuite dans le modèle *boîte noire* en cherchant à minimiser le nombre d'appels à la table dans notre modèle de complexité. Nous proposons alors un second algorithme effectuant, en général, moins d'appels.

Cet algorithme, à la FGLM, permet de calculer les relations en se ramenant à l'extraction d'une sous-matrice de rang maximal d'une matrice *multi-Hankel* (une généralisation à plusieurs variables d'une matrice de Hankel). De plus, nous présentons une version adaptative de ce second algorithme réduisant d'avantage le nombre de requêtes à la table.

Le nombre d'appels par le second algorithme peut être estimé précisément par le nombre d'éléments distincts d'une matrice multi-Hankel. Ce nombre est aussi lié à la *géométrie* de l'escalier final de la base de Gröbner. Ainsi, dans les cas favorables comme celui où l'escalier est convexe, la complexité est essentiellement linéaire en la taille de la sortie.

Les techniques d'algèbre linéaire permettent aussi d'estimer la complexité du second algorithme. En effet, lorsque l'ordre monomial utilisé pour le calcul est un ordre LEX, les matrices multi-Hankel sont des matrices bloc-Hankel avec des blocs imbriqués, dites *Hankel à plusieurs à niveaux* [FT00]. Nous pouvons alors utiliser l'algorithmique rapide [BJS07] des polynômes comme dans le cas des matrices de Hankel pour l'algorithme de Berlekamp – Massey.

En application directe à ceci, nous décodons des codes cycliques en dimension $n > 1$, une généralisation des codes de Reed Solomon. Nous proposons aussi un algorithme pour le calcul de séries génératrices de suites récurrentes linéaires à coefficients constants.

Bibliographie

[Ber68] Berlekamp, E., 1968. Nonbinary BCH decoding. IEEE Trans. Inform. Theory 14 (2), 242–242.

[BJS07] Bostan, A., Jeannerod, C.-P., Schost, É., 2007. Solving Toeplitz- and

Vandermonde-like Linear Systems with Large Displacement Rank. In: Brown, C. W. (Ed.), ISSAC'07. ACM Press, pp. 33–40.

[CN92] Chabanne, H., Norton, G. H., 1992. On the key equation for n-dimensional cyclic codes: applications to decoding. Tech. report INRIA RR-1796.

[FT00] Fasino, D., Tilli, P., 2000. Spectral clustering properties of block multilevel hankel matrices. Linear Algebra and its Applications 306 (1–3), 155 – 163.

[FGLM93] Faugère, J.-Ch., Gianni, P., Lazard, D., Mora, T., 1993. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. J. Symbolic Comput. 16 (4), 329–344.

[KY13] Kaltofen, E., Yuhasz, G., 2013. On the Matrix Berlekamp-Massey Algorithm. ACM Trans. Algorithms 9 (4), 33:1–33:24.

[Mas69] Massey, J. L., 1969. Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory IT-15, 122–127.

[SH95] Saints, K., Heegard, C., 1995. Algebraic-geometric codes and multi- dimensional cyclic codes: Theory and algorithms for decoding using Gröbner bases. IEEE Trans. Inform. Theory 41 (6), 1733–1751.

[Sak88] Sakata, S., 1988. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. J. Symbolic Comput. 5 (3), 321–337.

[Sak90] Sakata, S., 1990. Extension of the Berlekamp-Massey algorithm to N Dimensions. Inform. and Comput. 84 (2), 207–239.

3. Computer algebra methods for testing the structual stability of multidimensional systems

Yacine Bouzidi,Alban Quadrat, Fabrice Rouillier
L2S, Supelec
Gif-sur-Yvette, France
`Prenom.nom@inria.fr`

En théorie des systèmes dynamiques, un système multidimensionnel (ou système n-D) est un système dans lequel l'information se propage dans plus d'une direction indépendante (habituellement, la direction du temps pour les systèmes 1-D classiques). Les systèmes multidimensionnels apparaissent dans l'étude des équations au dérivées partielles, des systèmes avec retard ou dans le traitement d'images.

Un question fondamentale dans l'étude des systèmes multidimensionnels concerne leur stabilité, cette propriété étant une condition nécessaire à leur bon fonctionnement.

Dans ce travail, on s'intéresse au test de stabilité des systèmes multidimensionnels linéaires et discrets à coefficients invariants dans le temps.

Dans le domaine fréquentiel, un système multidimensionnel est décrit au moyen d'une fonction de transfert qui relie la sortie du système à son entrée. Dans le cas des systèmes qui nous intéressent, celle-ci est donnée sous la forme

$$G(z_1, \ldots, z_n) = \frac{N(z_1, \ldots, z_n)}{D(z_1, \ldots, z_n)}, \tag{1}$$

avec N et D des polynômes dans $\mathbb{R}[z_1, \ldots, z_n]$.

Dans la description à base de fonction de transfert, un système est dit *structurellement stable* si et seulement si le dénominateur de la fonction de transfert, $D(z_1, \ldots, z_n)$, est dépourvu de zéros complexes dans le polydisque unité $\mathbb{D}^n := \prod_{k=1}^{n} \{z_k \in \mathbb{C} \mid |z_k| \leq 1\}$ ou, en d'autre termes :

$$D(z_1, \ldots, z_n) \neq 0 \text{ for } |z_1| \leq 1, \ldots, |z_n| \leq 1. \tag{2}$$

Par conséquent, tester qu'un système est structurellement stable revient à tester la condition . La simple formulation de cette condition contraste cependant avec la difficulté de mettre au point des implantations efficaces pour la tester. Les quelques algorithmes proposés dans la littérature [1, 2] sont soit inefficaces, soit ils se contentent d'en tester une formulation plus forte (Une condition de stabilité suffisante mais non nécessaire).

Dans cette présentation, on propose un nouvel algorithme certifié et efficace pour tester la stabilité structurelle d'un système multidimensionnel. Plus précisément, partant de la condition , on montre dans un premier temps que le problème de tester si une hypersurface a des zéros dans le polydisque, est équivalent à celui de décider si un ensemble algébrique à des zéros réels. Ceci permet d'obtenir de nouvelles conditions que l'on teste ensuite à l'aide d'algorithmes classiques de recherche de zéros réels d'ensembles algébriques.

Notre algorithme a été implanté sous la forme d'une routine `Maple`. Celle-ci prend en entrée un polynôme $D(z_1, \ldots, z_n)$ et renvoie vrai si celui-ci n'a pas de zéros à l'intérieur du polydisque et faux sinon. Les nombreux tests et comparaisons effectués ont permis de valider notre approche.

Bibliographie

[1] I. Serban and M. Najim, *Multidimensional systems : Bibo stability test based on functional schur coefficients*, Signal Processing, IEEE Transactions on, 55(11) :5277–5285, 2007.

[2] B. Dumitrescu, *Stability test of multidimensional discrete-time systems via sum-of-squares decomposition*, Circuits and Systems I : Regular Papers, IEEE Transactions on, 53(4) :928–936, April 2006.

4. Calcul des isométries de réseaux algébriques

Thomas Camus[a]
Institut Fourier, UMR 5582 (CNRS-Université Grenoble Alpes),
100 rue des Mathématiques, 38402 Saint Martin d'Hères, France.
thomas.camus@ujf-grenoble.fr

a. Partiellement supporté par le LabEx PERSYVAL-Lab (ANR-11-LABX-0025).

Les réseaux sur un anneau d'entiers algébriques (ou réseaux algébriques) sont une spécialisation de la notion classique de réseau euclidien. Ce sont des objets qui apparaissent naturellement dans des domaines variés tels que la géométrie algorithmique des nombres et la cryptographie. Bien que la théorie englobant les réseaux algébriques soit aujourd'hui mieux comprise, son versant algorithmique demeure encore incomplet.

Nous considérons ici deux des problèmes majeurs en algorithmique des réseaux algébriques :

1. Comment décider si deux réseaux algébriques sont isométriques ?
2. Comment déterminer le groupe des automorphismes d'un réseau algébrique ?

La première question revient à se demander s'il possible de vérifier si deux objets algébriques partagent les mêmes propriétés géométriques. Quant à la seconde, elle concerne la faisabilité du calcul des symétries d'un réseau algébrique.

L'algorithme de Plesken et Souvignier [1] permet aujourd'hui de répondre à ces questions dans le cadre euclidien. On dispose notamment d'implantations effectives de cet algorithme (par exemple dans la librairie PARI/GP [2]).

L'objectif de ce travail est de présenter une adaptation de l'algorithme de Plesken et Souvignier pour les réseaux algébriques. Nous expliquerons notamment comment s'affranchir de l'identification d'un réseau algébrique à un réseau euclidien en travaillant directement sur l'anneau d'entiers algébriques considéré. Ce travail mélange des techniques de calcul exact et de le calcul approché. Cet algorithme a été implantée et testée avec succès en utilisant la libraire PARI/GP.

Ces travaux rentrent dans le cadre de ma thèse dirigée par Ph. Elbaz-Vincent (Institut Fourier) et J.-G. Dumas (Laboratoire Jean Kuntzmann).

Bibliographie

[1] W. Plesken et B. Souvignier, *Computing isometries of lattices*, Journal of Symbolic Computation, 24 (1997), pp. 327–334.
http://www.sciencedirect.com/science/article/pii/S0747717196901303

[2] The PARI Group, *PARI/GP version 2.7.3*, Bordeaux, 2014.
http://pari.math.u-bordeaux.fr/.

[3] K. Okuda et S. Yano, *A generalization of Voronoï's Theorem to algebraic lattices*, Journal de Théorie des Nombres de Bordeaux, 22 (2010), pp. 727–740. https://eudml.org/doc/116430

[4] T. Watanabe, S. Yano et T. Hayashi, *Voronoı's reduction theory of GL_n over a totally real number field*, Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, 587 (2013). p. 213 http://www.math.sci.osaka-u.ac.jp/~twatanabe/voronoireduction.pdf

[5] J. Martinet, *Perfect lattices in Euclidean spaces*, vol. 327, Springer, 2003.

[6] Y. Gan, C. Ling et W.-H. Wai, *Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection*, Signal Processing, IEEE Transactions on, 57-7 (2009), pp. 2701–2710.

5. Multiplication rapide d'entiers utilisant des nombres de Fermat généralisés premiers

Svyatoslav Covanov
Université de Lorraine, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506
Inria, Villers-lès-Nancy, F-54600
CNRS, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506
svyatoslav.covanov@inria.fr

La multiplication d'entiers a et b de n bits est un problème d'algorithmique pour lequel la meilleure complexité connue a été obtenue à travers un effort de 50 ans, passant d'une complexité naïve en $O(n^2)$ à $O(n \log n \cdot 4^{\log^* n})$ [6]. Puisqu'on connaît des algorithmes pour accélerer le produit de polynômes, une première approche pour améliorer la complexité de l'algorithme naïf consiste à transformer a et b en des polynômes A et B tels que $a = A(2^k)$ et $b = B(2^k)$ pour un certain k divisant n.

Il se trouve qu'on peut accélerer le produit de 2 polynômes d'un certain degré N, en évaluant ces polynômes en N points bien choisis, et en multipliant point à point ces N évaluations. Cette observation aboutit à l'exploitation de racines primitives de l'unité comme $e^{\frac{i\pi k}{n}}$ dans $\mathbb{C}$ et de la transformée de Fourier, car on dispose d'un algorithme rapide pour évaluer un polynôme en des racines primitives de l'unité, appelé Fast Fourier Transform (FFT) et dont la forme la plus connue est celle de Cooley-Tukey [1].

Ainsi, en transformant les entiers a et b en des polynômes à coefficients dans $\mathbf{R} = \mathbb{Z}/(2^N + 1)\mathbb{Z}$, dans lequel 2 est une racine primitive $2N$-ème de l'unité, on obtient l'algorithme de Schönhage-Strassen [7], qui fut pendant près de 35 ans l'algorithme de multiplication d'entiers avec la meilleure la complexité connue, dont l'estimation est $O(n \cdot \log n \cdot \log \log n)$.

En 1989 [4], M. Fürer émet l'idée qu'en utilisant des nombres premiers de Fermat $F_m = 2^{2^m} + 1$, on bénéficie d'un anneau $\mathbf{R}$ dans lequel la multiplication par les racines 2^m-èmes primitives de l'unité sont des multiplications par des puissances de 2, ce qui

s'effectue via un décalage de bits. Bien que peu probable, si on émet l'hypothèse qu'il existe une infinité de nombres premiers de Fermat, on aboutit à une complexité en $O(n \cdot \log n \cdot 2^{O(\log^* n)})$, $\log^* n$ étant le nombre de fois où il faut composer le logarithme avec n pour avoir un nombre plus petit que 1.

En 2007 [5], M. Fürer propose d'utiliser l'anneau $\mathbb{C}[X]/(X^P + 1)$, dans lequel X a des propriétés similaires à 2 dans $\mathbb{Z}/(F_m)\mathbb{Z}$. Cet anneau permet d'aboutir à une complexité en $O(n \cdot \log n \cdot 2^{O(\log^* n)})$, sans dépendre d'une conjecture sur la répartition des nombres premiers de Fermat. Mais on peine à réaliser une implémentation efficace de cet algorithme, c'est-à-dire effectuer de meilleures performances que les implémentations actuelles de l'algorithme de Schönhage-Strassen.

Peu après, Harvey, Van Der Hoeven, and Lecerf publient un rapport [6] dans lequel ils proposent une analyse plus fine de l'algorithme de M. Fürer et obtiennent une estimation en $O(n \cdot \log n \cdot 16^{\log^* n})$ pour une version optimisée de l'algorithme original. Ils proposent par ailleurs d'autres algorithmes dont un en $O(n \cdot \log n \cdot 4^{\log^* n})$, reposant sur une conjecture sur la répartition des nombres premiers de Mersenne.

Cet exposé présentera les travaux réalisés dans [2], proposant un algorithme conjecturel alternatif à celui proposé par Harvey, Van Der Hoeven, and Lecerf, et bénéficiant d'une complexité en $O(n \cdot \log n \cdot 4^{\log^* n})$. On reprend l'idée de Fürer exploitant les nombres premiers de Fermat, mais en utilisant plutôt des nombres généralisés de Fermat, pour lesquels les travaux de Gallot et Dubner [3] permettent de conjecturer qu'on peut en trouver suffisamment pour effectuer une analyse de complexité satisfaisante. L'avantage principal de cet algorithme est sa simplicité en terme d'implémentation, que des travaux futurs vont chercher à mettre en œuvre.

Bibliographie

[1] J. W. Cooley and J. W. Tukey. An algorithm for the machine calculation of complex fourier series. *Math. Comput.*, 19 :297–301, 1965.

[2] S. Covanov and E. Thomé. Fast arithmetic for faster integer multiplication. Jan. 2015.

[3] H. Dubner and Y. Gallot. Distribution of generalized fermat prime numbers. Technical report, Math. Comp, 1999.

[4] M. Fürer. On the complexity of integer multiplication (extended abstract). Technical Report CS-89-17, Pennsylvania State University, 1989.

[5] M. Fürer. Faster integer multiplication. In D. S. Johnson and U. Feige, editors, *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, pages 57–66. ACM, 2007.

[6] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. *CoRR*, abs/1407.3360, 2014.

[7] A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7(3-4) :281–292, 1971.

6. Calcul rapide d'un coefficient d'une série algébrique en caractéristique positive

Alin Bostan	Gilles Christol	**Philippe Dumas**
INRIA	IMJ	INRIA
alin.bostan@inria.fr	gilles.christol@imj-prg.fr	philippe.dumas@inria.fr

Une série algébrique est une série formelle $y = f(x) \in \mathbb{Q}[[x]]$ solution d'une équation algébrique $E(x, y) = 0$, où $E(x, y)$ est un polynôme de $\mathbb{Z}[x, y]$. Par exemple, la série énumérative des arbres 2–3

$$f(x) = 1 + 2\,x + 10\,x^2 + 66\,x^3 + 498\,x^4 + 4066\,x^5 + \cdots$$

est algébrique et satisfait à l'équation algébrique $y = 1 + xy^2 + xy^3$ (il y a soixante-six arbres 2–3 à trois sommets internes, comme le montre le coefficient $[x^3]f$ de x^3 dans f).

Étant donnés un nombre entier N et un nombre premier p, nous nous intéressons dans ce travail au calcul efficace de $[x^N]f \bmod p$, le reste modulo p du coefficient de x^N dans f. En d'autres termes, il s'agit de calculer rapidement le coefficient $[x^N]\bar{f}$ d'une série $\bar{f} \in \mathbb{F}_p[[x]]$, racine d'un polynôme à deux variables $\bar{E}[x, y]$ sur le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Par exemple, nous souhaitons calculer le milliardième coefficient modulo 9001 de la série des arbres 2–3.

Une idée simple est de substituer le développement à l'ordre N de la série dans l'équation et d'identifier à zéro. Cela fait résoudre un système non linéaire dans lequel chaque terme est déterminé par les précédents. Le calcul du N^{e} terme de $\bar{f}$ par cette méthode demande un nombre d'opérations arithmétiques dans $\mathbb{F}_p$ de l'ordre de N^d, où d est le degré de l'équation $\bar{E} = 0$. L'itération formelle de Newton permet d'accélérer ce calcul, en atteignant une complexité $O(N \log N)$, où d n'apparaît que dans la constante du $O(\,)$.

Mais il y a bien plus efficace pour calculer directement le N^{e} terme de $\bar{f} \in \mathbb{F}_p[[x]]$. On utilise pour ce faire l'automaticité des séries algébriques sur un corps fini [1, Cor. 4.5] : l'entier N se décompose en base p et chacun de ses $\log_p N$ chiffres permet d'effectuer une transition dans un automate, à partir de son état initial, ce qui fournit en sortie la valeur du coefficient désiré. Ce calcul demande de l'ordre de $\log_p N$ opérations arithmétiques dans $\mathbb{F}_p$.

Encore faut-il disposer d'un automate, et son précalcul s'avère coûteux. La construction d'un automate à partir de l'équation algébrique [3] passe par l'écriture d'une autre équation algébrique, d'une forme particulière (de Mahler), c'est-à-dire utilisant l'opérateur de Frobenius $g(x) \mapsto g(x^p) = g(x)^p$. Le coût du calcul de cette équation de Mahler à partir d'une équation algébrique $\bar{E}(x, y) = 0$ est en général de l'ordre de $p^{d(d-1)/2}$.

Une meilleure approche repose sur la considération d'une fraction rationnelle dont la série algébrique est la diagonale [5], [2, Cor. 13, p. 6-09]. Par exemple la série des

arbres 2–3 est la diagonale de la fraction rationnelle

$$\frac{3\,xy^4 + 9\,xy^3 + 9\,xy^2 + 5\,xy + 2\,x - y - 1}{xy^3 + 4\,xy^2 + 5\,xy + 2\,x - 1} =$$
$$\underline{1} + y + (\underline{2\,xy}) + (4\,x^2y) + (8\,x^3y + \underline{10\,x^2y^2} - 4\,xy^3)$$
$$+ (16\,x^4y + 40\,x^3y^2 - 2\,xy^4) + (32\,x^5y + 120\,x^4y^2 + \underline{66\,x^3y^3} - 22\,x^2y^4) + \cdots$$

Le précalcul s'effectue dans un espace de polynômes à deux variables dont les degrés partiels sont bornés par ceux de la fraction rationnelle [2, Th. 32]. Nous montrons ainsi que l'utilisation des diagonales comme structure de données permet d'aboutir à une complexité essentiellement quadratique en p pour le précalcul, ce qui constitue déjà une énorme amélioration.

Nous accélérons encore ce calcul : nous montrons, et ceci est notre principale contribution, que l'évaluation du N^{e} coefficient d'une série algébrique de $\mathbb{F}_p[[x]]$ peut se faire en $O(\log_p N + p \log^2 p)$ opérations dans $\mathbb{F}_p$, où la constante du $O(\,)$ ne dépend que du degré d. Ceci est à comparer au calcul de tous les coefficients jusqu'au rang N, qui ne peut pas demander moins de N opérations, ou au calcul direct du N^{e} coefficient dont la meilleure complexité annoncée (mais non explicitée) est $O(p \times \log_p N)$ [4, p. 121].

Bibliographie

[1] Jean-Paul Allouche et Jeffrey Shallit. The ring of k-regular sequences. *Theoret. Comput. Sci.*, 98(2):163–197, 1992.

[2] Gilles Christol. Éléments analytiques uniformes et multiformes. In *Séminaire Delange-Pisot-Poitou (15e année : 1973/74), Théorie des nombres, Fasc. 1, Exp. No. 6*, page 18. Secrétariat Mathématique, Paris, 1975.

[3] Gilles Christol, Teturo Kamae, Michel Mendès-France et Gérard Rauzy. Suites algébriques, automates et substitutions. *Bull. Soc. Math. France*, 108(4):401–419, 1980.

[4] David V. Chudnovsky et Gregory V. Chudnovsky. Computer algebra in the service of mathematical physics and number theory. In *Computers in mathematics (Stanford, CA, 1986)*, volume 125 of *Lecture Notes in Pure and Appl. Math.*, pages 109–232. Dekker, New York, 1990.

[5] Harry Furstenberg. Algebraic functions over finite fields. *J. Algebra*, 7:271–277, 1967.

7. Calcul de racines sur un corps fini à l'aide de transformées de Graeffe

B. Grenet[(a)], J. van der Hoeven[(b)], G. Lecerf[(b)]

[(a)] LIRMM, Université de Montpellier

[(b)] LIX, CNRS – École Polytechnique

bruno.grenet@lirmm.fr

lecerf@lix.polytechnique.fr

vdhoeven@lix.polytechnique.fr

Soit $\mathbb{F}_q$ un corps fini. Nous nous intéressons au calcul des racines de polynômes scindés à racines simples sur $\mathbb{F}_q$. Nous proposons une nouvelle approche pour ce problème, basée sur des transformées de Graeffe généralisées, qui donne lieu à plusieurs algorithmes.

Le calcul des racines d'un polynôme $f \in \mathbb{F}_q[X]$ est un problème important du calcul formel qui sert de brique de base à de nombreux algorithmes du domaine (factorisation, interpolation, ...). Il s'agit également de l'un des rares problèmes que l'on sait résoudre en temps polynomial probabiliste mais pas en temps polynomial déterministe. Une motivation de notre travail vient de l'observation que dans les algorithmes d'interpolation creuse, le calcul de racines de polynômes $f \in \mathbb{F}_q[X]$ représente une part importante du temps de calcul [6]. Dans ces algorithmes, on peut choisir pour q un nombre premier *de type FFT*, c'est-à-dire de la forme $q = M \cdot 2^m + 1$ avec $M = O(\log q)$.

D'une part, nous décrivons un algorithme déterministe. Cet algorithme suppose donnés la factorisation de $(q-1)$ et un élément primitif de $\mathbb{F}_q^\times$. Nous obtenons ainsi une nouvelle borne de complexité déterministe en fonction de $\sqrt{S_1(q-1)}$ où $S_1(q-1)$ est le plus grand diviseur premier de $(q-1)$. Celle-ci améliore légèrement un résultat de von zur Gathen [2]. Dans le cas favorable $S_1(q-1) = O(\log q)$, la complexité de notre algorithme déterministe est équivalente à celle de l'algorithme (probabiliste) de Cantor et Zassenhaus [1], à des facteurs logarithmiques près.

D'autre part, nous donnons des algorithmes probabiliste et heuristique. Ceux-ci sont particulièrement efficaces lorsque le cardinal $(q-1)$ de $\mathbb{F}_q^\times$ est friable, par exemple si q est un nombre premier de type FFT. Pour de telles valeurs de q, notre algorithme probabiliste a une complexité moyenne similaire à celle de l'algorithme de Cantor et Zassenhaus, et l'implantation d'une variante heuristique dans le logiciel libre Mathemagix [5] permet d'obtenir des gains significatifs en pratique. Ces gains permettent une accélération des algorithmes d'interpolation creuse.

Cette exposé est basé sur les deux articles [3, 4].

Bibliographie

[1] D. G. Cantor, H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. 36(154), pp. 587–592, 1981.

[2] J. von zur Gathen, *Factoring polynomials and primitive elements for special primes*, Theoret. Comput. Sci. 52(1-2), pp. 77–89, 1987.

[3] B. Grenet, J. van der Hoeven, G. Lecerf, *Randomized Root Finding over Finite FFT-fields using Tangent Graeffe Transforms*, Proc. issac, pp. 197–204, 2015.

[4] B. Grenet, J. van der Hoeven, G. Lecerf, *Deterministic root finding over finite fields using Graeffe transforms*, Manuscript (submitted), 2015.

[5] J. van der Hoeven, et al, *Mathemagix*, from 2002. http://www.mathemagix.org.

[6] J. van der Hoeven, G. Lecerf, *Sparse Polynomial Interpolation in Practice*, ACM Commun. Comput. Algebra 48(3-4), pp 187–191, 2014.

8. Un algorithme déterministe pour calculer une racine approchée d'un système polynomial en complexité moyenne polynomiale

P. Lairez
TU Berlin, Allemagne
pierre@lairez.fr

Une racine d'un système d'équations polynomiales peut être calculée numériquement par la méthode homotopique : pour résoudre un système f, on part d'un système g dont on connait une racine η, et on le déforme progressivement jusqu'à arriver à f tout en faisant suivre la racine η à l'aide d'itérations de Newton. La complexité de cette méthode est bien comprise en terme du conditionnement des systèmes polynomiaux que l'on rencontre le long du chemin de déformation, mais il est difficile de trouver *a priori* un chemin de déformation efficace.

Shub et Smale [4, p. ex.] ont étudié la complexité *en moyenne* des méthodes homotopiques, où l'on suppose que le système à résoudre est uniformément distribué dans un certain espace. Beltrán et Pardo [1] ont décrit un algorithme probabiliste pour calculer une racine approchée d'un système polynomial dont la complexité est polynomiale par rapport à la taille de l'entrée *en moyenne*, à la fois par rapport à l'entrée de l'algorithme et sa source d'aléa. Bürgisser et Cucker [2] ont eux décrit un algorithme déterministe de complexité $N^{\mathcal{O}(\log\log N)}$, où N est la taille de l'entrée. Tous ces travaux utilisent le modèle BSS : une machine capable d'opérer de manière exacte sur des nombres réels et dotée d'une mémoire à accès direct dont les registres sont capables de stocker des nombres réels à précision infinie.

L'objet de ce travail [3] est de montrer comment supprimer l'aléa dans l'algorithme de Beltràn et Pardo, donnant ainsi un algorithme déterministe de complexité moyenne polynomiale. L'idée principale consiste à exploiter la précision infinie qui nous est donnée dans le modèle BSS : en séparant les bits de poids forts et les bits de poids faible, on décompose le système donné en entrée et on obtient, d'un côté, une approximation de ce système, et de l'autre, des bits aléatoires qu'on peut utiliser pour pourvoir l'algorithme de Beltrán et Pardo.

Références

[1] Carlos Beltrán and Luis Miguel Pardo. Fast linear homotopy to find approximate zeros of polynomial systems. *Found. Comput. Math.*, 11(1) :95–129, 2011.

[2] Peter Bürgisser and Felipe Cucker. On a problem posed by Steve Smale. *Ann. of Math. (2)*, 174(3) :1785–1836, 2011.

[3] Pierre Lairez. A deterministic algorithm to compute approximate roots of polynomial systems in polynomial average time, 2015.

[4] Michael Shub and Steve Smale. Complexity of Bezout's theorem. V. Polynomial time. *Theoret. Comput. Sci.*, 133(1) :141–164, 1994. Selected papers of the Workshop on Continuous Algorithms and Complexity (Barcelona, 1993).

9. Formules de quadrature, extension plate et optimization convexe

B. Mourrain
Inria Méditerranée
2004 route des Lucioles
06902 Sophia Antipolis
bernard.mourrain@inria.fr

Les formules de quadrature jouent un rôle important en calcul scientifique et ont été étudiées depuis de nombreuses années par des mathématiciens célèbres : Gauss, Legendre, Chebyshev, Lobatto, Radau, Radon [3], ... Elles sont aussi reliées à des développements très intéressants autour des polynômes orthogonaux.

L'objectif de ces formules est de calculer une bonne approximation d'intégrales de fonctions. Plus précisément, étant donné un domaine Ω de $\mathbb{R}^n$ et une fonction w positive sur Ω, nous voulons remplacer le calcul de

$$I[f] = \int_\Omega w(\mathbf{x}) f(\mathbf{x}) d\mathbf{x}$$

par une formule plus simple à évaluer, de la forme

$$\langle \sigma | f \rangle = \sum_{j=1}^{r} w_j \, f(\zeta_j) \tag{3}$$

où $\zeta_j \in \mathbb{R}^n$ et $w_j \in \mathbb{R}$ sont indépendants de la fonction f. Ils sont choisis de telle manière que

$$\forall f \in V, \ \langle \sigma | f \rangle = I[f],$$

V étant un espace vectoriel de fonctions de dimension finie. Typiquement, V est l'espace vectoriel des polynômes de degré $\leq d$. Ceci permet par exemple de contrôler l'erreur entre $\langle \sigma | f \rangle$ et $I[f]$, par le reste d'un développement de Taylor de la fonction.

De nombreuses méthodes ont été développées au cours du temps [4, 2] pour traiter les cas de petits degrés en petite dimension, avec symétrie, sur des domaines standards, ...Nous présentons une approche algorithmique qui permet de traiter le problème d'un domaine général en dimension quelconque.

Pour cela, nous transformons le problème de quadrature en un problème de complétion de matrices de Hankel tronquées. Nous analysons les propriétés algébriques liées aux

extensions plates de matrices de Hankel, et montrons comment retrouver les points de quadrature et les poids à partir de ces matrices. Nous décrivons ensuite un algorithme de vérification des propriétés d'extensions plates qui permet aussi de calculer la formule de quadrature. Pour construire une formule de quadrature avec un nombre minimal de points, nous proposons une hiérarchie de problèmes d'optimization convexe minimisant la norme nucléaire des matrices de Hankel associées. Nous montrons que pour un ordre assez élevé de la relaxation, une solution du problème d'optimisation convexe fournit une formule de quadrature. Nous illustrons l'approche sur quelques exemples conduisant à de nouvelles formules de quadratures avec un nombre minimal de points.

Pour plus de détails sur ce travail en commun avec M. Abril Bucero, C. Bajaj, voir [1].

Bibliographie

[1] M. Abril Bucero, C. Bajaj, and B. Mourrain. On the construction of general cubature formula by flat extensions. To appear in *Linear Algebra and Applications*. hal.inria.fr/hal-01158099, 2015.

[2] R. Cools. Constructing cubature formulae : the science behind the art. *Acta numerica*, 6 :1–54, 1997.

[3] J. Radon. Zur mechanischen kubatur. *(German) Monatsh. Math*, 52 :286–300, 1948.

[4] A. H. Stroud. Quadrature methods for functions of more than one variable. *Ann. New York Acad. Sci.*, 86 :776–791, 1960.

10. Computing minimal interpolation bases

Vincent Neiger[†‡],

joint work with Claude-Pierre Jeannerod[†], Éric Schost[‡] and Gilles Villard[†]

[†] LIP, ENS de Lyon, France

[‡] University of Waterloo, Ontario, Canada

The first step in Guruswami and Sudan's list decoding algorithm for Reed-Solomon codes [8] amounts to bivariate interpolation with prescribed multiplicities and degree constraints. Later, variants of this problem arose in Koetter and Vardy's soft-decision decoding algorithm [9] (where constraints on the points are weakened), in Guruswami and Rudra's list decoding algorithm for folded Reed-Solomon codes [7] (where more variables are involved), and more recently in Devet, Goldberg, and Heninger's work on Private Information Retrieval [5].

In quest of fast algorithms, essentially two approaches have been proposed so far in the literature : one [3] uses fast structured system solving [2] while the other one [4] uses fast polynomial lattice reduction [6], which itself relies on fast order basis computations [11]. In this talk, we will first introduce the problem, give a quick overview of those

fast algorithms, and discuss possible improvements. Then, noting the analogy between the quadratic iterative algorithms by Kötter [10] and by Beckermann and Labahn [1] respectively for constrained multivariate interpolation and order basis computation, we will present our recent work on a fast divide-and-conquer algorithm which gives a unified solution to these two problems.

Bibliography

[1] B. Beckermann and G. Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM J. Matrix Anal. Appl.*, 15(3) :804–823, July 1994.

[2] A. Bostan, C.-P. Jeannerod, and É. Schost. Solving structured linear systems with large displacement rank. *Theor. Comput. Sci.*, 407(1-3) :155–181, 2008.

[3] M. Chowdhury, C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Faster algorithms for multivariate interpolation with multiplicities and simultaneous polynomial approximations. *IEEE Trans. Inf. Theory*, 61(5) :2370–2387, 2015.

[4] H. Cohn and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. *Adv. Math. Comm.*, 9(3) :311–339, 2015.

[5] Casey Devet, Ian Goldberg, and Nadia Heninger. Optimally robust private information retrieval. Cryptology ePrint Archive, Report 2012/083, 2012. http ://eprint.iacr.org/.

[6] S. Gupta, S. Sarkar, A. Storjohann, and J. Valeriote. Triangular x-basis decompositions and derandomization of linear algebra algorithms over $K[x]$. *J. Symbolic Comput.*, 47(4) :422–453, 2012.

[7] V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity : Error-correction with optimal redundancy. *IEEE Trans. Inf. Theory*, 54(1) :135–150, 2008.

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

[9] R. Koetter and A. Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 49(11) :2809–2825, 2003.

[10] R. Kötter. Fast generalized minimum-distance decoding of algebraic-geometry and Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 42(3) :721–737, 1996.

[11] W. Zhou and G. Labahn. Efficient algorithms for order basis computation. *J. Symbolic Comput.*, 47(7) :793–819, 2012.

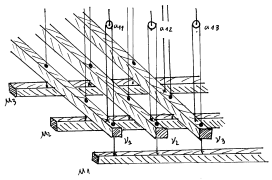
11. La borne de Jacobi. Déterminant tropical, ordre et formes normales des systèmes d'EDO

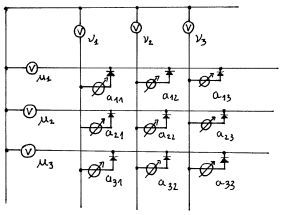
F. Ollivier
LIX, UMR CNRS n° 7161
École polytechnique
F-91128 Palaiseau cedex
francois.ollivier@lix.polytechnique.fr

Jacobi [1, 2] a affirmé que l'ordre d'un système différentiel ordinaire $P_i(x_1, \ldots, x_n) = 0$, $1 \leq i \leq n$, tel que $\mathrm{ord}_{x_j} P_i = a_{i,j}$ était borné par $\max_{\sigma \in S_n} \sum_{i=1}^n a_{i,\sigma(i)}$. Cette expression est le *déterminant tropical* de la matrice $(a_{i,j})$. On obtient une expression *tropicale* en remplaçant les produits par des sommes et les sommes par des maxima [8].

Jacobi a fourni un algorithme polynomial pour calculer le déterminant tropical, qui fut réinventé en 1955 par Kuhn [6, 7] en s'inspirant des travaux de Kőnig [5] et Egerváry [3]. Celui-ci avait montré que si μ_i et ν_j forment une *couverture minimale* de $(a_{i,j})$, c'est-à-dire si $a_{i,j} \leq \mu_i + \nu_j$ et si $\sum_{i=1}^n (\mu_i + \nu_i)$ est minimale, alors cette somme est le déterminant tropical de $(a_{i,j})$.

On illustrera les rapports entre l'algorithme de Jacobi et celui de Kuhn de même que les rapports entre les *canons minimaux* de Jacobi, quantités minimales à ajouter à chaque ligne pour que chacune contienne des maxima (dans leur colonne) placés dans des colonnes toutes différentes, et les couvertures minimales d'Egerváry, en s'aidant d'analogies physiques, comme le système mécanique ou le montage électrique ci-dessous.





On montrera ensuite que la méthode proposée par Jacobi, à partir du canon minimal, pour parvenir dans le cas générique, c'est-à-dire si le *déterminant tropical* est non nul, à une forme normale en dérivant chaque équation un nombre minimal de fois s'étend au cadre plus général des couvertures d'Egerváry.

On illustrera ensuite de quelques exemples la méthode de Jacobi pour rechercher toutes les formes normales d'un système d'EDO, ainsi que sa méthode pour déterminer combien de fois il faut dériver chacune des équations du système pour parvenir à calculer une résolvante, méthode que Jordan a retrouvé pour tenter de prouver la borne de Jacobi [4].

On conclura avec quelques autres possibilités d'emploi du déterminant tropical et des couvertures, comme la recherche d'un décomposition diagonale ou triangulaire par blocs.

Bibliographie

[1] Jacobi (Carl Gustav Jacob), « De investigando ordine systematis aequationum dif-

ferentialum vulgarium cujuscunque », traduction anglaise, *AAECC*, **20**, (1), 7–32, 2009.

[2] Jacobi (Carl Gustav Jacob), « De aequationum differentialum systemate non normali ad formam normalem revocando », traduction anglaise, *AAECC*, **20**, (1), 33–64, 2009.

[3] Egerváry (Jenő), « Matrixok kombinatorius tulajdonságairól » [En hongrois : Des propriétés cmbinatoires des matrices], *Matematikai és Fizikai Lapok*, vol. 38, 1931., 16–28 ; traduit en américain par H. W. Kuhn, Paper 4, Issue 11 of *Logistik Papers*, Georges Washington University Research Project, 1955.

[4] Jordan (Camille), « Sur l'ordre d'un système d'équations différentielles », *Annales de la société scientifique de Bruxelles*, vol. 7, B., 127–130, 1883.

[5] Kőnig (Dénes), « Gráfok és mátrixok », *Matematikai és Fizikai Lapok* 38 : 116–119, 1931.

[6] Kuhn (Harold H.), « The Hungarian method for the assignment problem », *Naval res. Logist. Quart.* **2** (1955), 83–97.

[7] Kuhn (Harold H.), "A tale of three eras : The discovery and rediscovery of the Hungarian Method", *European Journal of Operational Research*, 219 (2012), 641–651.

[8] Maclagan (Diane) and Sturmfels (Bernd), *Introduction to Tropical Geometry*, preprint, 2015.
https ://homepages.warwick.ac.uk/staff/D.Maclagan/papers/TropicalBook20.4.14.pdf

12. Computing the Rank Profile Matrix

J.G. Dumas, **C. Pernet**, Z. Sultan
Laboratoire de l'Informatique et du Parallélisme
Université Grenoble Alpes, CNRS, Inria, Université de Lyon
jean-guillaume.dumas@imag.fr,clement.pernet@imag.fr,
ziad.sultan@imag.fr

The row (resp. column) rank profile of a matrix describes the stair case shape of its row (resp. column) echelon form. We will first propose a recursive Gaussian elimination algorithm that can compute simultaneously the row and column rank profiles of a matrix, as well as those of all of its leading sub-matrices, in the same time as state of the art Gaussian elimination algorithms. We then propose the definition of a new matrix invariant, the rank profile matrix, summarizing all information on the row and column rank profiles of all the leading sub-matrices. We also explore the conditions for a Gaussian elimination algorithm to compute all or part of this invariant, through the corresponding PLUQ decomposition. As a consequence, we show that the classical iterative CUP decomposition algorithm can actually be adapted to compute the rank profile

matrix. Used, in a Crout variant, as a base-case to the recursive algorithm, it delivers a significant improvement in efficiency. The row (resp. column) echelon form of a matrix are usually computed via various dedicated triangular decompositions. We show here that, from some PLUQ decompositions, it is possible to recover the row and column echelon forms of a matrix and of any of its leading sub-matrices thanks to an elementary post-processing algorithm. Lastly, we will make connections with the recent algorithmic improvements of Storjohann and Yang [3, 4] for the computation of the rank profiles of matrices with small ranks, leading to an $O\tilde{}(r^\omega + mn)$ algorithm computing the rank profile matrix. This work has been presented, for the most part, in [1] and [2].

Bibliographie

[1] Jean-Guillaume Dumas, Clément Pernet, and Ziad Sultan. *Simultaneous computation of the row and column rank profiles.* In Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, ISSAC '13, pages 181–188, New York, NY, USA, 2013. ACM.

[2] Jean-Guillaume Dumas, Clément Pernet, and Ziad Sultan. *Computing the rank profile matrix.* In Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '15, pages 149–156, New York, NY, USA, 2015. ACM.

[3] Arne Storjohann and Shiyun Yang. *Linear Independence Oracles and Applications to Rectangular and Low Rank Linear Systems.* In Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, ISSAC '14, pp 381–388, New York, NY, USA, 2014. ACM.

[4] Arne Storjohann and Shiyun Yang. *A Relaxed Algorithm for Online Matrix Inversion.* In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '15, pp 339–346, New York, NY, USA, 2015. ACM.

13. Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields

Adrien Poteaux[⋆] & Marc Rybowicz[†]

[⋆] CRIStAL-CFHP, université de Lille

adrien.poteaux@univ-lille1.fr

[†] XLIM-DMI, université de Limoges

marc.rybowicz@unilim.fr

Let L be a field of characteristic p with $\mathfrak{q}$ elements and $F \in L[X, Y]$ be a polynomial with $p > \deg_Y(F)$ and total degree d. In [2], we showed that rational Puiseux series

of F above $X = 0$ could be computed with an expected number of $\tilde{O}(d^5 + d^3 \log \mathfrak{q})$ arithmetic operations in L. In this paper, we reduce this bound to $\tilde{O}(d^4 + d^2 \log \mathfrak{q})$ using Hensel lifting and changes of variables in the Newton-Puiseux algorithm that give a better control of the number of steps. The only asymptotically fast algorithm required is polynomial multiplication over finite fields. This approach also allows to test the irreducibility of F in $\overline{L}[[X]][Y]$ with $\tilde{O}(d^3)$ operations in L. Finally, we describe a method based on structured bivariate multiplication [1] that may speed up computations for some input.

This work has been presented at ISSAC'15 [3].

Bibliographie

[1] J. Lebreton, E. Schost, and J. V. der Hoeven. Structured FFT and TFT : symmetric and lattice polynomials. In ACM, editor, *Proc. ISSAC '13*, pages 355–362, 2013.

[2] A. Poteaux and M. Rybowicz. Complexity Bounds for the Rational Newton-Puiseux Algorithm over Finite Fields. *Applicable Algebra in Engineering, Communication and Computing*, 22(3) :187–217, 2011.

[3] Adrien Poteaux, Marc Rybowicz. *Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields.* In Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '15, pages 299–306, New York, NY, USA, 2015. ACM.

14. A short survey on Kantorovich-like theorems for Newton's method

G. Lecerf, **J. Saadé**
Laboratoire d'informatique de l'École polytechnique
LIX, UMR 7161 CNRS
Campus de l'École polytechnique
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau, France
gregoire.lecerf@math.cnrs.fr,saade@lix.polytechnique.fr

Au cours des dernières années, l'opérateur de Newton est devenu omniprésent dans les calculs numérique et symbolique. Sur des fonctions spécifiques comme les polynômes de degré deux dans $\mathbb{R}$, le comportement de l'opérateur de Newton est simple. Mais en général, il est difficile de savoir si une suite de Newton partant d'une valeur initiale va converger ou non vers un zéro. Plus précisement, soit $\phi : \mathbb{R} \to \mathbb{R}$ une fonction réelle de classe C^1, c'est à dire différentiable et ϕ' continue. Dans la théorie, on sait bien que la suite de Newton $(r_k)_{k\geq 0}$ définie par $r_{k+1} = r_k - \frac{\phi(r_k)}{\phi'(r_k)}$ converge quadratiquement si la valeur initiale r_0 est suffisamment proche d'un zéro simple r_- de ϕ, c'est à dire

$\phi'(r_-) \neq 0$. Mais en pratique cette information de distance n'est pas suffisante, et on voudrait savoir ce qu'on entend par "suffisamment proche".

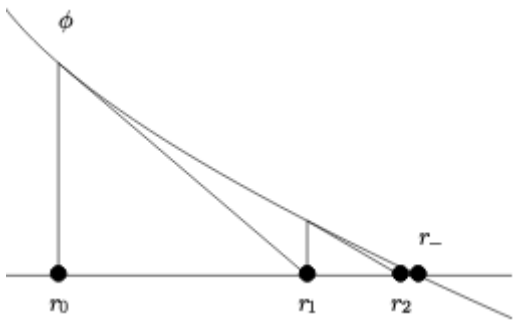


FIGURE 1 – Graphe de ϕ et les premiers itérations de Newton

Dans la Figure 1, on présente le comportement de la suite de Newton au voisinage d'un zéro simple r_-. En effet, c'est un resultat classique si ϕ est décroissante et convexe dans $[r_0, R]$, et $\phi(r_0) > 0$, et $\phi(R) < 0$, alors il existe un unique zéro r_- de ϕ dans $[r_0, R]$, et la suite de Newton $(r_k)_{k\geq 0}$ converge vers r_-. Dans un voisinage de r_-, cette convergence est quadratique.

Généralement, pour une fonction complexe $f : \mathbb{C} \to \mathbb{C}$, l'ensemble des valeurs initiales menant à une suite qui converge vers un zéro de f forme une *fractale de Newton*, c'est à dire un ensemble de Julia de la fonction méromorphe $z \mapsto z - \frac{f(z)}{f'(z)}$. En pratique, il est important de donner des critères simples de convergence. Si le critère est satisfait alors on aura convergence dans le voisinage d'un unique zéro ; sinon, on ne peut rien dire. On trouve beaucoup de critères dans la littérature, mais il est difficile de choisir le critère le plus efficace parce que l'on doit faire un compromis entre la vitesse et la précision.

Notre présentation commence par une extension générale du critère de Kantorovich [1]. Après, on montre comment d'autres critères connus [2, 3] se d 'eduisent de ce cas général ; puis on présente une discusion rapide sur la façon de former des critères offrant des compromis alternatifs [4, 5]. Des notes historiques sont incluses à la fin.

Bibliographie

[1] L.V. KANTOROVICH, *Functional analysis and applied mathematics*, Uspehi Matem. Nauk (N.S.) (1948) pp.89–185

[2] S. SMALE, *Newton's method estimates from data at one point*, In The merging of disciplines : new directions in pure, applied, and computational mathematics (1985) pp.185–196

[3] W. B. GRAGG AND R. A. TAPIA, *Optimal error bounds for the Newton-Kantorovich theorem*, SIAM J. Numer. Anal.,(1974) pp.10–13

[4] Z. DA HUANG, *A note on the Kantorovich theorem for Newton iteration*, J. Comput. Appl. Math., (1993) pp.211–217

[5] J.A. EZQUERRO, D.GONZÁLEZ, AND M.Á. HERNÁNDEZ, *On the local convergence of Newton's method under generalized conditions of Kantorovich*, Appl. Math. Lett., (2013) pp.566–570

15. Calculs symboliques sur des algorithmes théoriques de produits de matrices

T. Sibut-Pinote,
Inria, École Polytechnique

É. Schost
University of Western Ontario

thomas.sibut-pinote@inria.fr

eschost@uwo.ca

La complexité optimale du produit matriciel, opération élémentaire fondamentale du calcul formel, est une question cruciale pour des raisons tant pratiques que théoriques. Pourtant, elle est à ce jour un problème ouvert.

Le produit de $A \in \mathcal{M}_{m,n}(\mathbb{K})$ et $B \in \mathcal{M}_{n,p}(\mathbb{K})$, noté (m, n, p), se calcule de manière naïve en mnp multiplications. Strassen [6] fut le premier à introduire un algorithme sous-cubique, qui motiva l'introduction de la constante$\omega = \inf\{\tau | \text{la complexité optimale du calcul de } (m, n, p) \text{ est } \mathcal{O}((mnp)^{\frac{\tau}{3}})\}$. On sait que $2 \leq \omega < 3$ et on conjecture que $\omega = 2$.

De nombreux travaux donnent des bornes inférieures sur ω, la meilleure étant actuellement celle de Le Gall [1] : $\omega < 2.3728639$. Les algorithmes correspondants ne sont pas considérés comme utilisables en pratique : rarement implémentés, ils ne sont parfois pas complètement explicités, voire proviennent d'un argument d'existence non constructif.

Un algorithme de produit de matrices peut s'écrire comme un tenseur

$$t := \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{p} a_{i,k} \otimes b_{k,j} \otimes c_{i,j}$$

La question de sa complexité correspond à la recherche d'une écriture de t avec un nombre minimal r de tenseurs élémentaires : on sait alors en déduire que $\omega \leq \frac{\log(r)}{\log(mnp)}$. Par exemple, Strassen [6] écrit le produit $(2, 2, 2)$ avec 7 tenseurs élémentaires, ce qui donne par un argument récursif $\omega \leq \log_2(7) \simeq 2.81$.

Le τ-théorème de Schönhage [3] permet de déduire des bornes sur ω à partir d'une telle formule calculant *plusieurs* produits de matrices indépendants. On peut le combiner à une autre technique connue qui consiste à calculer non plus dans $\mathcal{K}$, mais dans $\mathcal{K}[\varepsilon]$. Par exemple, si on appelle t_1 le tenseur

$$\sum_{i=0}^{m-1} \sum_{k=0}^{p-1} (x_{i,0} + \varepsilon u_{0,k,i}) \otimes (y_{0,k} + \varepsilon v_{k,i,0}) \otimes (\varepsilon^2 z_{k,i} + w_{0,0}) - \left(\sum_{i=0}^{m-1} x_{i,0} \right) \otimes \left(\sum_{k=0}^{p-1} y_{0,k} \right) \otimes w_{0,0}$$

Il peut s'écrire $t_1 = \varepsilon^2 t_2 + \varepsilon^3 t_3$ où t_2 calcule les produits de matrices indépendants $(m, 1, p)$ et $(1, (m-1)(p-1), 1)$ en seulement $mp+1$ opérations au lieu de $2mp-(m+p-1)$. Cela implique $\omega < 2.55$. Pan [2] présente de nombreux algorithmes de ce type qui produisent

des valeurs de plus en plus petites de ω. Cependant, ces résultats reposent sur le fait que les multiplications de polynômes et la prise de modulo qui permettent de transformer ces tenseurs avec ε en algorithmes effectifs sont asymptotiquement négligeables devant le reste des calculs ; or ce n'est pas le cas pour les petites tailles de matrices.

Notre contribution est de deux natures : en examinant des tenseurs obtenus en composant ceux de Pan puis en extrayant certains termes, nous avons découvert un moyen de produire des tenseurs sans ε [4] ; cela nous a mené à développer une bibliothèque [5] qui permet de parser les algorithmes du type de ceux de Pan sous un format agréable pour l'utilisateur, de les transformer en arbres de syntaxe abstraite, de les manipuler (notamment les composer) et de les extraire vers du code Maple ou C++. Elle est écrite en Ocaml.

L'ambition de cette bibliothèque n'est pas de fournir des algorithmes efficaces "clés en mains", mais plutôt de fournir un environnement pour manipuler les algorithmes de produits de matrices (théoriques ou non) de manière formelle, ce qui peut être utile pour guider la compréhension du comportement de ces algorithmes à la fois dans un cadre de recherche et d'enseignement.

Bibliographie

[1] François Le Gall. Powers of tensors and fast matrix multiplication. *CoRR*, abs/1401.7714, 2014.

[2] Victor Pan. *How to multiply matrices faster*. Springer-Verlag New York, Inc., New York, NY, USA, 1984.

[3] Arnold Schönhage. Partial and total matrix multiplication. *SIAM J. Comput.*, 10(3) :434–455, 1981.

[4] Thomas Sibut-Pinote. Internship report. 2012. Available at http://perso.ens-lyon.fr/thomas.sibutpinote/rapport_matprod.pdf.

[5] Thomas Sibut-Pinote and Eric Schost. Matrix product experiments, 2012. Available at https://gitlab.com/matrix-product-experiments/matrix-product-experiments.

[6] Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 14(3) :354–356, 1969.

16. Sparse Polynomial Systems With Many Positive Solutions From Bipartite Simplicial Complexes

F. Bihan, LAMA, Université de Savoie

P.-J. Spaenlehauer Inria, CNRS, Univ. Lorraine

frederic.bihan@univ-smb.fr
pierre-jean.spaenlehauer@inria.fr

Real solutions of multivariate polynomial systems are ubiquitous in many applications of mathematics, as they often contain relevant information. Positive solutions are often of special interest, for instance when the variables represent physical quantities (*e.g.* in robotics), or if they represent probabilities (*e.g.* in algebraic statistics). Let $f_1, \ldots, f_n \in \mathbb{R}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ be Laurent polynomials. A real solution of $f_1(X_1, \ldots, X_n) = \cdots = f_n(X_1, \ldots, X_n) = 0$ is called positive if all its coordinates are positive. It is non-degenerate if the Jacobian matrix of the system is invertible at the solution. We focus on the following problem :

> Given an integer $n \in \mathbb{N}$ and a finite set $\mathcal{M}$ of Laurent monomials in n variables, construct n polynomials in $\mathbb{R}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ which involve only monomials in $\mathcal{M}$ and such that the system
>
> $$f_1(X_1, \ldots, X_n) = \cdots = f_n(X_1, \ldots, X_n) = 0$$
>
> has many non-degenerate positive solutions.

Our approach is related to a result by Sturmfels [4] which states that if the point configuration given by the exponent vectors of $\mathcal{M}$ admits a regular unimodular triangulation, then there exists a system with support $\mathcal{M}$ whose complex solutions with non-zero coordinate are all real. This is also related to Viro's theorem [6], to its extensions for complete intersections [2, 5] and to constructions of mixed systems based on signed Newton polytopes [3].

We propose a construction whose starting point is to consider a regular simplicial complex in $\mathbb{R}^n$ whose vertices are the exponent vectors of the monomials in $\mathcal{M}$. Next, the goal is to assign a vector in $\mathbb{R}^n$ to each vertex of the simplicial complex under sign constraints on some maximal minors of the matrix recording these vectors. From such an assignment, we construct a polynomial system whose number of positive and non-degenerate solutions is bounded below by the number of simplices in the simplicial complex. Computing this assignment boils down to a positive variant of the low-rank completion problem or, equivalently, to the problem of realizability of some oriented matroids.

We illustrate the construction with various examples and we identify, among classical families, finite sets of monomials $\mathcal{M}$ admitting *maximally positive systems*, *i.e.* systems with support $\mathcal{M}$ all complex toric solutions of which are positive and non-degenerate. These families provide evidence in favor of a conjecture by Bihan [1], which gives a necessary condition on such sets of monomials.

Finally, we discuss the construction of polynomial systems with many positive solutions when only the cardinality of $\mathcal{M}$ is prescribed.

Bibliographie

[1] F. Bihan *Maximally positive polynomial systems supported on circuits*, Journal of Symbolic Computation, 68(20) :61-74, 2015.

[2] F. Bihan. *Viro method for the construction of real complete intersections*. Advances in Mathematics, 169(2) :177-186, 2002.

[3] I. Itenberg and M.-F. Roy. *Multivariate Descartes' rule*. Beitrage Zur Algebra und Geometrie, 37(2) :337-346, 1996.

[4] B. Sturmfels. *On the number of real roots of a sparse polynomial system*. Hamiltonian and Gradient Flows, Algorithms and Control, Fields Inst. Commun., vol. 3, American Mathematical Society, pp. 137–143, 1994.

[5] B. Sturmfels. *Viro's theorem for complete intersections*. Annali della Scuola Normale Superiore di Pisa, 21(3), 377-386, 1994.

[6] O. Viro. *Gluing of algebraic hypersurfaces, smoothing of singularities and construction of curves*. Proc. Leningrad Int. Topological Conf., pp. 149-197, 1983.

Authors' addresses :
Frédéric Bihan, Laboratoire de Mathématiques, Université de Savoie, Campus Scientifique, 73376 Le Bourget-du-Lac Cedex, France, `frederic.bihan@univ-savoie.fr`
Pierre-Jean Spaenlehauer, CARAMEL project, INRIA Grand-Est ; Université de Lorraine ; CNRS, UMR 7503 ; LORIA, Nancy, France, `pierre-jean.spaenlehauer@inria.fr`

17. Simplification de paramètres

F. Lemaire, **A. Temperville**
Département d'Informatique, laboratoire CRIStAL
Université Lille, Villeneuve d'Ascq
`a.temperville@ed.univ-lille1.fr`

L'algorithme CSB (Compute Sparsest Basis), développé dans [1], permet de calculer une base la plus creuse équivalente à une base donnée. Il permet notamment, dans un contexte biologique, d'établir des bases les plus creuses de lois de conservations issus des modèles de base de données Biomodels [2].

Je présenterai une application de l'algorithme CSB permettant de rendre plus creuses des fractions rationnelles, par le biais de changements de variables. J'illustrerai le principe de cette simplification sur quelques exemples.

Bibliographie

[1] F. Lemaire, A. Temperville, *On Defining and Computing "Good" Conservation Laws*, Computational Methods in Systems Biology (2014), pp. 1–19.

[2] *BioModels DataBase*, `http://www.ebi.ac.uk/biomodels-main/publmodels`, Online accessed July 3rd, 2015.

18. Classification algébrique associée à l'optimisation de contraste pour l'IRM

B. Bonnard[1], J.-C. Faugère[2], A. Jacquemard[2],
M. Safey El Din[2], **T. Verron**[2]
[1] Institut de Mathématiques de Bourgogne, UMR CNRS 5584
Dijon, France
[2] Équipe PolSys, LIP6, UPMC Sorbonne Universités, INRIA, CNRS
Paris, France
bernard.bonnard@u-bourgogne.fr,
jean-charles.faugere@inria.fr,
alain.jacquemard@lip6.fr, mohab.safey@lip6.fr,
thibaut.verron@lip6.fr

L'imagerie à résonance magnétique nucléaire (IRMN ou IRM) est un procédé d'imagerie médicale reposant sur la réaction des substances biologiques à l'application d'un champ magnétique. Le contraste de l'image obtenue dépend de plusieurs paramètres régulant cette réaction. Lorsque le contraste est insuffisant, cela signifie que les deux milieux que l'on cherche à distinguer ont des paramètres trop proches. Il est possible de remédier à ce problème en altérant ces paramètres par injection au patient de produits de contraste, mais avec le risque d'effets médicaux indésirables. Nous privilégions une optimisation par l'étude fondamentale d'un modèle physique.

En pratique, la recherche de paramètres donnant un bon contraste est réalisée par des raisonnements qualitatifs. L'influence des paramètres sur le contraste est régie par les équations de Bloch, dont l'inversion permettrait, de manière systématique, de caractériser les paramètres optimisant le contraste.

Dans [3], les auteurs exposent une technique, utilisant la théorie du contrôle optimal, permettant d'obtenir une image dont le contraste est proche de la limite théorique.

Cet algorithme numérique décrit des trajectoires dans l'espace des paramètres. Dans [1], les auteurs s'intéressent aux fondations mathématiques de cette méthode : les points où ces trajectoires peuvent diverger peuvent être décrits comme le lieu singulier d'une variété algébrique. Les auteurs décrivent formellement ce lieu singulier dans plusieurs cas particuliers, à l'aide de bases de Gröbner ([2]).

Dans ce travail, nous cherchons à décrire ce lieu singulier dans le cas général. Plus précisément, on s'intéresse à un sous-ensemble de ces équations, qui s'écrit en termes de singularités d'un déterminant : on considère la matrice M, de taille 4×4, à les coefficients

dans $\mathbb{R}[\gamma_1, \gamma_2, \Gamma_1, \Gamma_2, y_1, y_2, z_1, z_2]$, définie par :

$$M = \begin{pmatrix} -\Gamma_1 y_1 & -z_1 - 1 & -\Gamma_1 + (\gamma_1 - \Gamma_1)\, z_1 & (2, \gamma_1 - 2\,\Gamma_1)\, y_1 \\ -\gamma_1 z_1 & y_1 & (\gamma_1 - \Gamma_1)\, y_1 & 2\,\Gamma_1 - \gamma_1 - (2\,\gamma_1 - 2\,\Gamma_1)\, z_1 \\ -\Gamma_2 y_2 & -z_2 - 1 & -\Gamma_2 + (\gamma_2 - \Gamma_2)\, z_2 & (2\,\gamma_2 - 2\,\Gamma_2)\, y_2 \\ -\gamma_2 z_2 & y_2 & (\gamma_2 - \Gamma_2)\, y_2 & 2\,\Gamma_2 - \gamma_2 - (2\,\gamma_2 - 2\,\Gamma_2)\, z_2 \end{pmatrix}$$

et on note $D(\gamma_1, \gamma_2, \Gamma_1, \Gamma_2, y_1, y_2, z_1, z_2)$ son déterminant. On cherche les valeurs des paramètres (Γ_i, γ_i) au-dessus desquelles existe un point où le déterminant de M est singulier en (y_i, z_i). En théorie, résoudre ce problème revient à calculer une seule base de Gröbner éliminant z_i, y_i du système ci-dessus, mais il s'avère que ce calcul direct est impraticable.

Dans cet exposé, on montrera comment la structure déterminantielle du système nous permet de diriger les calculs : en décomposant ce système par étapes, on parvient à identifier et caractériser différentes composantes de l'espace des paramètres pour lesquels le déterminant D peut être singulier.

Bibliographie

[1] Bernard Bonnard, Monique Chyba, Alain Jacquemard, and John Marriott. Algebraic geometric classification of the singular flow in the contrast imaging problem in nuclear magnetic resonance. *Mathematical Control and Related Fields*, 3(4) :397–432, 2013.

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

[3] Marc Lapert, Yun Zhang, Martin A. Janich, Steffen J. Glaser, and Dominique Sugny. Exploring the physical limits of saturation contrast in magnetic resonance imaging. *Scientific Reports*, 2(589), 2012.