Journées Nationales de Calcul Formel

Rencontre organisée par :
Jean-Guillaume Dumas, Grégoire Lecerf, Delphine Boucher et Thomas Cluzeau

2010

Jean-Guillaume Dumas, Grégoire Lecerf, Delphine Boucher, et Thomas Cluzeau

Informations sur les Journées
Vol. 1, n° 2 (2010), p. 1-30.
<http://ccirm.cedram.org/item?id=CCIRM_2010__1_2_1_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Les cours du C.I.R.M.
Vol. **1** n° 2 (2010) 1-30

Informations sur les Journées

Jean-Guillaume Dumas, Grégoire Lecerf, Delphine Boucher, et Thomas Cluzeau

Comité scientifique

Table des matières

1. Liste des orateurs

1. *Daniel Augot :* Décodage des codes géométriques et algorithmes de Guruswami-Sudan
2. *Alin Bostan :* Algorithmes rapides pour les polynômes et matrices
3. *Jean-Pierre Dedieu :* Complexité et conditionnement
4. *Alban Quadrat :* Une introduction à l'analyse algébrique constructive et à ses applications
5. *Ainhoa Aparicio-Monforte :* Reconstruction d'intégrales premières formelles le long de solutions non ponctuelles d'un système différentiel.
6. *Philippe Aubry :* Calcul algébrique efficace de résolvantes relatives.
7. *Skander Belhaj :* Diagonalisation par blocs approchée d'une matrice de Hankel à coefficients complexes : application à l'algorithme d'Euclide.
8. *Jérémy Berthomieu :* Algorithmique détentue pour les entiers p-adiques.
9. *Luk Bettale :* Résolution de systèmes polynomiaux dans les corps finis.
10. *Brice Boyer :* Multiplication matrice creuse – vecteur dense sur des corps finis pour architectures GPU et multicœurs.
11. *Jérome Brachat :* Le schéma de Hilbert.
12. *Laurent Busé :* Sur les singularités d'une courbe algébrique plane rationnelle.
13. *Christophe Chabot :* Codes quasi-cycliques et polynômes à coefficients matriciels.
14. *Guillaume Chèze :* Un algorithme quasi-optimal pour la décomposition des fractions rationnelles en plusieurs variables.
15. *Carole El Bacha :* Régularisation et solutions régulières de systèmes différentiels linéaires
16. *Joris van der Hoeven :* Arithmétique de boules.
17. *Jean-Gabriel Kammerer :* Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time
18. *Pierre-Vincent Koseleff :* Paramétrisation polynomiale des nœuds à deux ponts.
19. *Romain Lebreton :* Algorithmique dans les algèbres d'invariants polynomiaux sous un groupe fini.
20. *J. van der Hoeven, B. Mourrain, G. Lecerf, O. Ruatta, Ph. Trébuchet :* Mathemagix : langage, fonctionnalités et performances
21. *Marc Mezzaroba :* NumGfun : calcul efficace en Maple des solutions analytiques d'équations différentielles linéaires à coefficients polynomiaux.
22. *Marc Moreno Maza :* Triangular Decomposition of Semi-Algebraic Systems
23. *Guillaume Moroz :* Étude des solutions stables et chaotiques d'un modèle biologique.
24. *Bernard Mourrain :* Décomposition de tenseurs, matrices de moments et polynômes
25. *François Ollivier :* Borne de Jacobi et calcul de l'index pour toutes les composantes quasi-régulières d'un système d'EDO
26. *Clément Pernet :* Décodage adaptatif pour les systèmes multimodulaires redondants
27. *Michel Petitot :* Réseaux de Pétri stochastiques
28. *Adrien Poteaux :* Composition modulaire multivariée et applications.
29. *Xavier Pujol :* Algorithmes de crible pour le calcul d'un plus court vecteur dans un réseau
30. *Guènaël Renault :* Implicit Factoring with Shared Most Significant and Middle Bits
31. *Marie-Françoise Roy :* Sous-résultants et doubles sommes de Sylvester
32. *Mohab Safey El Din :* Algorithmique "diviser-pour-régner" pour le calcul de cartes routières
33. *Jan Sliwka :* Résolution relaxée d'un système d'équations et application dans le domaine de la robotique
34. *Pierre-Jean Spaenlehauer :* Systèmes Bilinéaires et Variétés Déterminantielles : Algorithmes, Complexité et Applications.
35. *Martin Weimann :* Factorisation polynomiale torique

2. Résumés des cours

1. Décodage des codes géométriques et algorithmes de Guruswami-Sudan

Daniel Augot (INRIA, Saclay)

Le premier exposé reprend les algorithmes classiques de décodage des codes géométriques, basés sur l'algorithme de Berlekamp-Massey et ses généralisations multivariées (Berlekamp-Massey-Sakata). Toutefois, avant de présenter ces algorithmes, je rappelerai les bases de la théorie des codes : codes linéaires, borne de Singleton, codes de Reed-Solomon, borne de Hamming. Ensuite, j'introduirai de manière motivée la famille des codes géométriques, comme généralisation des codes de Reed-Solomon, après un bref rappel de la théorie des courbes algébriques sur les corps finis. Le cadre sera alors en place pour introduire le décodage par syndrômes, qui est le décodage classique des codes géométriques. Le deuxième exposé est consacré aux progrès récents dans le domaine du codage algébrique, qui reposent sur le décodage par interpolation. Ces progrès sont dus à Guruswami-Sudan, et reposent sur une vision duale des codes de Reed-Solomon et des codes géométriques. Je présenterai dans l'ordre les algorithmes de Berlekamp-Welsh, Sudan et Guruswami-Sudan, dans le contexte des codes de Reed-Solomon et dans le contexte des codes géométriques. On verra finalement comment l'algorithme de Berlekamp-Massey-Sakata peut être recyclé dans ce contexte.

2. Algorithmes rapides pour les polynômes et matrices

Alin Bostan (INRIA Rocquencourt)

Les principaux thèmes de cet exposé sont la conception et l'analyse d'algorithmes pour deux types spécifiques de calculs algébriques : avec des polynômes et des séries formelles à une variable, d'une part, et avec des matrices denses et des matrices structurées, d'autre part. De nombreuses applications seront décrites, concernant la manipulation rapide des fonctions rationnelles, des matrices polynomiales, des nombres algébriques, des fonctions algébriques, des récurrences et des opérateurs différentiels. L'accent sera mis principalement sur la complexité asymptotique, et sur l'illustration des paradigmes fondamentaux (diviser-pour-régner, pas de bébé/pas de géant, principe de transposition) et des techniques (exponentiation binaire, itération de Newton, évaluation-interpolation), utilisées dans la conception et l'analyse des algorithmes. Dans la première partie de l'exposé, nous montrerons comment, en utilisant de telles techniques, une multitude d'opérations sur les polynômes et les séries (division, logarithme, exponentielle, évaluation, interpolation, changement de base, composition, plus grand commun diviseur, résultant, approximants de Padé et de Padé-Hermite,...) peuvent être ramenées ultimement à la multiplication polynomiale, et héritent ainsi de sa bonne complexité. Dans la deuxième partie de l'exposé, nous examinerons d'abord la complexité des calculs avec les matrices denses (inversion, décomposition LU, calcul du déterminant et du polynôme caractéristique,...), en les ramenant à la multiplication de matrices. Puis, nous présenterons un traitement unifié des calculs avec les matrices structurées (Toeplitz, Hankel, Vandermonde, Cauchy, Sylvester, et leurs généralisations), montrerons leurs liens avec les calculs polynomiaux, et exploiterons ces corrélations pour obtenir des accélérations significatives par rapport au cas des matrices denses. Une liste de problèmes ouverts conclura l'exposé.

3. Complexité et conditionnement

Jean-Pierre Dedieu (Université Toulouse)

Peut-on facilement calculer, de façon approchée, un zéro d'un système de n équations polynomiales en n inconnues à coefficients complexes ? Quelle est la complexité d'un tel calcul ? L'approche que nous présentons au cours de ces exposés utilise un modèle de calcul sur les nombres réels et privilégie les méthodes homotopiques. Nous verrons comment relier la complexité d'un tel calcul au conditionnement des systèmes rencontrés lors du parcours homotopique et nous montrerons comment rechercher des trajectoires optimales.

4. Une introduction à l'analyse algébrique constructive et à ses applications

Alban Quadrat (INRIA Sophia Antipolis)

Le but de ce mini-cours est de présenter une introduction à l'analyse algébrique constructive et à certaines de ses applications récentes en théorie des systèmes, théorie du contrôle et physique

mathématique. L'analyse algébrique est une branche récente des mathématiques qui étudie les systèmes linéaires d'équations aux dérivées partielles à l'aide de techniques venant de la théorie des modules, de l'algèbre homologique et de la théorie des faisceaux. Elle a été développée dans les annnées soixante par Malgrange, Palamodov, Bernstein, Sato, Kashiwara... Certaines des idées et techniques développées pour les systèmes différentiels se généralisent à d'autres classes de systèmes linéaires fonctionnels telles que les systèmes d'équations aux différences, systèmes d'équations différentiels à retards... Nous montrons comment les techniques de l'algèbre constructive (e.g., bases de Gröbner ou Janet pour des anneaux d'opérateurs non-commutatifs tels que des algèbres de Ore) permettent de développer une approche constructive de la théorie des modules et de l'algèbre homologique. Nous interpréterons alors certaines propriétés des modules dans le langage des systèmes et nous montrerons comment des problèmes classiques en théorie des systèmes (e.g., existence de paramétrisations, équivalences, symétries, factorisations, réductions, décompositions, lois de conservation) trouvent alors des réponses simples et constructives. Nous illustrerons ces nouvelles techniques à l'aide de nombreux systèmes classiques venant de la physique mathématique et de la théorie du contrôle à l'aide des packages OreModules, OreMorphisms, QuillenSuslin, Stafford, Serre et Homalg.

3. Exposés courts

5. Reconstruction d'intégrales premières formelles le long de solutions non ponctuelles d'un système différentiel.

Ainhoa Aparicio-Monforte (Université de Limoges ; CNRS ; XLIM UMR 6172 ; DMI)

Le problème de reconstruire des intégrales premières formelles au voisinnage de points d'équilibre a été abondamment traité dans la littérature. Dans notre cas, nous ne considérons pas ce problème autour d'un point d'équilibre mais le long de solutions non ponctuelles. Notre approche est une technique de prolongement qui nous permet de calculer des candidats de jets d'intégrales premières (inconnues) le long d'une solution en nous servant des équations variationnelles. Cette méthode nous permet de réduire l'ordre des équations variationnelles ce qui est utile autant du point de vue calcul formel que du point de vue du calcul numérique si on souhaite appliquer le théorème de Morales-Ramis-Simó. Nous proposons un algorithme permettant d'obtenir des prolongements d'intégrales premières formelles de long de solutions non ponctuelles de systèmes différentiels. Cette technique donne des pistes pour une version effective du Théorème de Morales-Ramis-Simó. C'est un travail en collaboration avec S. Simon Estrada et Jacques-Arthur Weil.

6. Calcul algébrique efficace de résolvantes relatives.

Philippe Aubry (LIP6 - Université Pierre et Marie Curie)

Travail commun avec Annick Valibouze.
La résolvante est un élément central du calcul algébrique ; en particulier pour déterminer le groupe de Galois d'un polynôme univarié, construire une représentation du corps de ses racines, calculer des polynômes minimaux de certains endomorphismes multiplicatifs ou d'éléments algébriques et construire également des polynômes univariés de groupe de Galois donné (problème de Galois inverse). Historiquement, J.-L. Lagrange a introduit la résolvante dite absolue d'un polynôme univarié f afin d'unifier les méthodes de résolution par radicaux jusqu'en degré 4 et tenter de prouver qu'à partir du degré 5 le phénomène d'abaissement du degré n'étant plus systématique, le polynôme f n'est alors pas nécessairement résoluble par radicaux. Alors que le calcul d'une résolvante absolue était somme toute assez simple, deux siècles plus tard, R. P. Stauduhar introduisit la résolvante relative à un sous-groupe L du groupe symétrique contenant le groupe de Galois G du polynôme f ([6]). Deux des théorèmes fondamentaux de l'algèbre sont le théorème fondamental des fonctions symétriques et le théorème de Galois ; sous leur aspect non effectif, ces théorèmes sont en fait les mêmes puisqu'ils expriment tous deux que si un polynôme est invariant par le groupe L contenant le groupe de Galois G, alors son évaluation en les racines de f appartient au corps k des coefficients de f. Dans un cas $L = S_n$, le groupe symétrique de degré $n = \deg(f)$, et dans l'autre $L = G$, le groupe de Galois. Pour réaliser des calculs algébriques avec les racines de f, il s'agit de rendre effectif ce théorème. Lorsque $L = S_n$, nous disposons de nombreuses méthodes effectives du théorème fondamental des fonctions symétriques. Ce sont ces diverses méthodes auxquelles viennent s'ajouter parfois des formules combinatoires qui sont utilisées pour calculer les résolvantes absolues (voir par exemple [3],[5]). Une des raisons qui fait de la résolvante (absolue ou non) un élément central du calcul algébrique est que sa factorisation sur le corps k permet d'aboutir à une forme effective du théorème de Galois. Mais se pose alors le problème de sa factorisation lorsque son degré est élevé. L'exemple le plus édifiant étant celui de la résolvante absolue de Galois dont le degré est $\deg(f)!$; pourtant seul suffit un quelconque de ses facteurs irréductibles sur k, nécessairement de degré l'ordre du groupe de Galois. Lorsque $G \neq S_n$, le recours à la résolvante relative à un sous-groupe strict L de S_n est attractif pour les deux raisons suivantes : d'une part, elle est un facteur strict de la résolvante absolue (de degré le stabilisateur de l'invariant considéré dans L et non plus dans S_n) et, d'autre part, au regard de l'ordonnancement des racines, elle porte en elle des informations plus précises qu'en tant que facteur de la résolvante absolue. Par exemple, la résolvante de Galois relative au groupe de Galois (i.e. $L = G$) est de degré l'ordre du groupe de Galois et les conjugués d'une de ses racines sont obtenus par ses permutations par le groupe de Galois en tant que groupe de permutations dont l'action sur les racines est déterminée (et non à un isomorphisme près comme pour la résolvante absolue). Toutefois, le calcul algébrique des résolvantes relatives a longtemps été considéré comme infaisable puis ardu (voir [1] où une méthode est proposée). Hormis la méthode numérique restreinte au cas $k = \mathbb{Z}$ ([6]) et quelques méthodes

combinatoires adaptées à des multi-résolvantes absolues particulières, jusqu'à l'algorithme de [2] aucune méthode algébrique générale ne venait concurrencer les diverses méthodes efficaces adaptées aux seules absolues. Nous proposons un algorithme algébrique de calcul de résolvantes relatives améliorant celui de [2] et s'inspirant en partie de celui de Lehobey destiné aux résolvantes absolues (voir [4]). Nous montrons en quoi l'algorithme de F. Lehobey est cependant propre aux résolvantes absolues.

[1] J. M. Arnaudiès and A. Valibouze. Résolvantes de lagrange. Technical Report 93.61, LITP, 1993.

[2] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6) :635–651, 2000.

[3] J.-L. Lagrange. Réflexions sur la résolution algébrique des équations. *Prussian Academy*, 1770.

[4] F. Lehobey. Resolvent computations by resultants without extraneous powers. In *ISSAC*, pages 85–92, 1997.

[5] L. Soicher and J. McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3) :273–281, 1985.

[6] R. P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27 :981–996, 1973.

7. Diagonalisation par blocs approchée d'une matrice de Hankel à coefficients complexes : application à l'algorithme d'Euclide.

Skander Belhaj (Laboratoire LAMSIN, École Nationale d'Ingénieurs de Tunis, Laboratoire de Mathématiques de Besançon, Université de Franche-Comté)

Les matrices de Hankel à coefficients complexes jouent un rôle important dans le traitement du signal. En effet, les coefficients d'une matrice de Hankel représentent un signal généré par la somme d'un nombre fini r d'exponentielles : $h_k = \sum_{l=1}^{r} \lambda_l^k d_l, k = 1, ..., 2n-1$ où λ_l et d_l sont les sous-jacents modes et poids, respectivement. Lorsque le signal est altéré par un bruit, des matrices de Hankel « perturbées » sont produites. Dans ce travail, nous introduisons le problème de la diagonalisation par blocs de matrices de Hankel « perturbées » et nous étudions le cas complexe [2] en préservant sa relation étroite avec l'algorithme d'Euclide. Bien que l'algorithme décrit dans [1] semble être le premier à étudier le cas approché, il ne préserve pas la taille des blocs dans le cas complexe. Par conséquent, nous reprenons ce problème dans le cas complexe. Nous comparons également l'approche de diagonalisation par blocs approchée de matrices de Hankel à une variante basée sur le complément de Schur adaptée à une matrice de Hankel à coefficients complexes. Nous présentons, enfin, un exemple qui permet de préserver la relation étroite entre l'algorithme d'Euclide et la méthode de diagonalisation par blocs approchée de la matrice de Hankel dans le cas complexe.

[1] S. Belhaj, *A fast method to block-diagonalize a Hankel matrix*, Numer. Algor., 47(2008) pp. 15–34.

[2] S. Belhaj, *Computing the block factorization of complex Hankel matrices*, accepted for publication in Computing.

8. Algorithmique détentue pour les entiers p-adiques.

Jérémy Berthomieu (Ecole Polytechnique)

Classiquement, les nombres p-adiques sont implantés de deux façons différentes. La première, dite zélée ou à précision fixe est très efficace dans le cas où la précision nécessaire est à la fois grande et connue à l'avance. Cependant, elle n'en reste pas moins compliquée pour la programmation de fonctionnalités mathématiques de haut niveau. La seconde implantation est la version paresseuse. On attache à chaque nombre p-adique la suite de ses coefficients et une méthode permettant d'énumérer le prochain coefficient de cette suite. La programmation en devient plus facile, mais le coût des opérations élémentaires telles que la multiplication et la division devient quadratique. L'implantation détendue des séries [1, 2] se généralise aux nombres p-adiques. Nous présenterons

dans cet exposé cette implantation qui a été faite en `C++` pour le logiciel MATHEMAGIX ainsi que quelques applications. La multiplication détendue sera présentée ainsi que son application *via* la méthode des points-fixes pour le calcul de l'inverse ou de la racine carrée d'un nombre. On présentera aussi une méthode de multiplication par blocs. Les techniques de déformation sont très répandues dans le calcul symbolique tel que la factorisation de polynômes, la résolution de systèmes polynomiaux et différentiels. L'utilisation des nombres p-adiques et des séries y est intense. *Il s'agit d'un travail en collaboration avec Grégoire Lecerf et Joris van der Hoeven.*

[1] Joris van der Hoeven. Lazy multiplication of formal power series. In W. W. Küchlin, editor, *Proc. ISSAC '97*, pages 17–20, Maui, Hawaii, July 1997.

[2] Joris van der Hoeven. Relax, but don't be too lazy. *J. Symbolic Comput.*, 34(6) :479–542, 2002.

9. Résolution de systèmes polynomiaux dans les corps finis.

Luk Bettale (DGA/MRIS)

Travail conjoint avec Jean-Charles Faugère et Ludovic Perret.

Dans cet exposé, nous présentons une approche hybride pour calculer les solutions d'un système polynomial à coefficients dans un corps fini. Une méthode bien connue pour résoudre un système polynomial consiste à calculer la base de Gröbner de l'idéal associé. L'algorithme historique de Buchberger, ou des algorithmes plus efficaces comme F_4/F_5[4, 5] permettent de mener à bien ce calcul. Dans de nombreuses applications, notamment en cryptographie, on est amené à étudier des systèmes polynomiaux sur des corps finis, et plus particulièrement, on recherche des solutions de ce système dans le corps des coefficients. Pour obliger les solutions à vivre dans le corps des coefficients, on ajoute au système initial les équations de corps $\{x_1^q - x_1, \ldots, x_n^q - x_n\}$ où q est la taille du corps. Lorsque q est grand devant le degré des équations initiales, l'ajout des équations de corps rend le calcul de base de Gröbner plus difficile et dans certains cas, impossible à réaliser en pratique. D'un autre coté, sur un corps fini, on peut toujours effectuer une recherche exhaustive pour trouver les solutions d'un système polynomial. L'idée de notre approche est de mélanger la recherche exhaustive avec le calcul de bases de Gröbner. Cette méthode consiste à fixer k variables pour calculer les bases de Gröbner de plusieurs systèmes avec moins de variables et qui seront généralement plus faciles à résoudre. Intuitivement, on aimerait que le coût de la recherche exhaustive sur les k variables soit moindre que le gain qu'on aurait en calculant des bases de Gröbner sur de plus petits systèmes. Nous avons étudié la complexité d'une telle approche dans le cadre de systèmes semi-réguliers [3]. Notre travail se base sur les résultats de Bardet [1]. Il est clair que l'efficacité de cette approche dépend du choix du paramètre k. Nous donnons dans cet exposé une analyse du comportement de cette approche hybride. En particulier, il est possible de trouver le meilleur compromis théorique entre la recherche exhaustive et les bases de Gröbner. Pour des corps de taille moyenne, cette méthode améliore la complexité de résolution de systèmes. Cette approche se révèle être efficace en pratique et a été utilisée pour la cryptanalyse de différents cryptosystèmes basés sur des systèmes polynomiaux (TRMS [2], UOV [6]).

[1] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In *Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry*, 2005.

[2] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of the TRMS signature scheme of PKC'05. In *Progress in Cryptology – AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 143–155. Springer, 2008.

[3] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 2009.

[4] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139 :61–88, June 1999.

[5] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In T. Mora, editor, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC*, pages 75–83. ACM Press, July 2002. isbn : 1-58113-484-3.

[6] Jean-Charles Faugère and Ludovic Perret. On the security of UOV. In *SCC 08*, 2008.

10. Multiplication matrice creuse – vecteur dense sur des corps finis pour architectures GPU et multicœurs.

Brice Boyer (LJK, Université de Grenoble)

Introduction. Nous avons implémenté [1] de manière efficace l'opération " Sparse Matrix-Vector multiplication " (en abrégé `spmv`) sur des corps. L'accent a surtout été mis sur des anneaux de type $\mathbb{Z}/m\mathbb{Z}$ avec m plus petit qu'un mot machine. La raison de cet exercice est double. D'une part, les ordinateurs personnels ou même portables comportent de plus en plus de cœurs, souvent sous-utilisés, ainsi que des cartes graphiques de plus en plus performantes, capables d'être programmées assez facilement pour une utilisation purement calculatoire (Nvidia Cuda, Ati Stream, OpenCL). De plus, les cartes graphiques offrent des performances supérieures à prix comparable, d'où, en les parallélisant, une utilisation possible en tant que « super-calculateur » pour certains problèmes. D'autre part, l'opération `spmv` étant une opération de base dans les algorithmes de type « boîte noire » ([6], [3]), les utilisations directes de cette librairie sont donc très vastes.

Généralités sur l'implémentation. L'opération de base est $\mathbf{y} \leftarrow A\mathbf{x}+\mathbf{y}$, permettant d'effectuer plus généralement l'opération $\mathbf{y} \leftarrow \alpha A\mathbf{x} + \beta\mathbf{y}$. Nous avons aussi besoin d'implémenter l'opération transposée ${}^\top\mathbf{y} \leftarrow \alpha\, {}^\top\mathbf{x}A + \beta\, {}^\top\mathbf{y}$. Pour cela, lorsque la mémoire le permet, il est en l'état bien plus efficace (par un ou deux ordres de grandeur) de transposer A et de se reporter au cas de base. L'opération $\mathbf{Y} \leftarrow A\mathbf{X} + \mathbf{Y}$, où $\mathbf{Y}$ est un bloc de vecteurs, est aussi implémentée car nécessaire dans les algorithmes par blocs ([5]). Les formats qui servent de base au stockage des matrices sont COO (`coo`rdinate format), DIA (`dia`gonal format), CSR (`c`ompressed `s`torage `r`ow format), ELL (`Ell`pack), modifiés selon les besoins ([7]). Dans la liste des formats dérivés de ces quatre formats de base figurent notamment ceux pour lesquels les matrices sont constituées uniquement de 1 (ou de -1). En effet, il n'est pas rare que des matrices issues de certaines applications soient riches en ± 1. On en trouve aussi probablement une forte proportion dans des matrices générales sur de petits anneaux. L'intérêt est alors double : l'espace mémoire destiné aux valeurs non nulles de A est inutile et les multiplications sont remplacées par des additions. On crée ainsi des formats hybrides en séparant les ± 1 des autres éléments. Dans le même esprit, on crée aussi des formats hybrides en juxtaposant deux formats simples, par exemple `ELL+CSR` dans le cas d'une matrice qui a un nombre presque constant d'éléments non nul par ligne sauf un certain nombre de lignes. Ensuite une matrice est découpée en sous-matrices stockées selon ces formats. L'utilisateur peut soit choisir les formats hybrides dans lesquels il veut encoder sa matrice, soit laisser le programme découper heuristiquement la matrice et choisir les formats. Les techniques utilisées pour améliorer les performances reposent sur l'utilisation des opérations rapides sur les nombres flottants, de la localité en mémoire des données, de la réduction modulo m différée, de représentations diverses des éléments de l'anneau (voir [4]).

Parallélisation. Nous avons utilisé d'une part OpenMP [2] sur les architectures multicœurs et d'autre part la technologie Cuda [3] de Nvidia sur les cartes graphiques la supportant – la version 2.3 de Cuda ne permettant pas leur utilisation simultanée dans des codes templétés. Nous nous sommes largement inspirés du travail de Bell et Garland (voir [1] et leurs références) pour la partie sur GPU en adaptant leur noyaux à nos problèmes. Pour la plupart des formats simples, la parallélisation est effectuée au niveau des lignes. Le découpage d'une matrice en sous-matrices permet un autre type de parallélisme partiellement exploré dans cette librairie.

Quelques résultats. Le tableau suivant donne une idée des performances sur quelques matrices [4] issues de divers problèmes.
Le gain en performance par rapport à la librairie d'algèbre linéaire LinBox [5] est clair.

Conclusion. Cette librairie donne des résultats performants sur les anneaux de type $\mathbb{Z}/m\mathbb{Z}$ et peut donc être utilisée plus globalement. Nous allons donc en intégrer une partie dans LinBox, et nous allons en profiter pour l'étendre naturellement aux corps finis non premiers. Il sera aussi

1. `https ://ljkforge.imag.fr/projects/ffspmvgpu/`
2. `http ://openmp.org/`
3. `http ://www.nvidia.fr/object/cuda_home_new_fr.html`
4. disponibles sur `http ://ljk.imag.fr/membres/Jean-Guillaume.Dumas/simc.html`
5. `http ://linalg.org`

matrice (dim-#non zéro×10^6)	m133.b3 0,2M-0,8M	GL7d15 0,4M-6M	mpoly2 2,4M-16M	GL7d19 1,9M-37M
Linbox	0,2	0,3	0,2	0,2
1core	0,3	0,4	0,5	0,2
8 core	1,5	1,6	1,9	0,9
GTX	6,6	8,3	4,4	1,1

FIGURE 1: GFlops sur l'opération $\mathbf{y} \leftarrow \mathrm{A}^{20}\mathbf{x} \mod 31$ sur Intel 8c ore 3.2GHz avec Nvidia GTX 280

important d'implémenter l'opération `spmv` sur de petits corps compressés, notamment $\mathbb{Z}/2\mathbb{Z}$. Le travail prochain consistera à donner la possibilité de mieux pré-traîter la matrice, en la partitionnant par exemple avec metis [6] et/ou en choisissant mieux les formats des sous-matrices. Ce travail en amont de `spmv` est utile lorsque A est réutilisée abondamment. Finalement, il sera intéressant de se pencher sur le cas des matrices pour lesquelles A et ${}^{\top}A$ ne peuvent pas être stockées simultanément ([2]).

[1] Nathan Bell and Michael Garland. Implementing sparse matrix-vector multiplication on throughput-oriented processors. In *SC '09 : Proceedings of the Conference on High Performance Computing Networking, Storage and Analysis*, pages 1–11, New York, NY, USA, 2009. ACM.

[2] Aydin Buluç, Jeremy T. Fineman, Matteo Frigo, John R. Gilbert, and Charles E. Leiserson. Parallel sparse matrix-vector and matrix-transpose-vector multiplication using compressed sparse blocks. In *SPAA '09 : Proceedings of the twenty-first annual symposium on Parallelism in algorithms and architectures*, pages 233–244, New York, NY, USA, 2009. ACM.

[3] Li Chen, Wayne Eberly, Erich Kaltofen, B. David, B. David Saunders, William J. Turner, and Gilles Villard. Efficient matrix preconditioners for black box linear algebra. In *Linear Algebra and Applications 343–344 (2002), 119–146. Special issue on Structured and Infinite Systems of Linear Equations*, pages 343–344, 2001.

[4] Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet. Dense linear algebra over word-size prime fields : the fflas and ffpack packages. *ACM Trans. Math. Softw.*, 35(3) :1–42, 2008.

[5] Wayne Eberly. Reliable krylov-based algorithms for matrix null space and rank. In *ISSAC '04 : Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, pages 127–134, New York, NY, USA, 2004. ACM.

[6] William Jonathan Turner. *Black box linear algebra with the linbox library*. PhD thesis, 2002. Chair-Kaltofen, Erich.

[7] F. Vazquez, E. M. Garzon, J. A. Martinez, and J. J. Fernandez. The sparse matrix vector product on gpus. *Technical Report*, June 2009.

11. Le schéma de Hilbert.

Jérome Brachat (Galaad, INRIA Sophia-Antipolis)

Nous nous intéressons dans cet exposé à la représentation effective du schéma de Hilbert 0-dimensionel. Nous donnons ainsi de nouvelles équations plus simples que celles déjà introduites par Bayer et Iarrobino-Kleiman. Ces équations, qui sont du même type que les relations de Plucker, définissent le schéma de Hilbert comme un sous schéma fermé de la Grassmannienne. Elles sont déduites des relations de commutation caractérisant les bases de bord ainsi que des relations de réécriture.

12. Sur les singularités d'une courbe algébrique plane rationnelle.

Laurent Busé (Galaad, INRIA Sophia-Antipolis)

Soit k un corps algébriquement clos. Dans la lecture 19 de son livre [1], Abhyankar définit le résultant de Taylor de deux polynômes $f(t), g(t) \in k[t]$ comme le résultant éliminant la variable t

6. `http ://glaros.dtc.umn.edu/gkhome/metis/metis/overview`

des polynômes

$$\frac{f(t)-f(s)}{t-s} = f'(s) + \frac{f''(s)}{2!}t + \frac{f'''(s)}{3!}t^2 + \cdots,$$
$$\frac{g(t)-g(s)}{t-s} = g'(s) + \frac{g''(s)}{2!}t + \frac{g'''(s)}{3!}t^2 + \cdots.$$

Comme il l'énonce dans son théorème page 153, sans toutefois le démontrer, ce résultant de Taylor est un générateur du conducteur de $k[f(t), g(t)]$ dans $k[t]$. En particulier, il permet de décider si $k(t) = k(f(t), g(t))$, si $k[t] = k[f(t), g(t)]$ et de « calculer » les points singuliers de la courbe paramétrée par $x = f(t)$, $y = g(t)$. Ce résultat est partiellement démontré dans [7] et interprété en termes de sous-résultants dans [5]. Le théorème d'Abhyankar ne traite que des courbes rationnelles admettant des paramétrisations polynomiales. Il est donc tout naturel de se poser la question de sa généralisation au cas des courbes rationnelles générales, c'est-à-dire au cas où $f(t), g(t) \in k(t)$. L'article [6] propose une généralisation partielle du théorème d'Abhyankar. Si $f = f_n/f_d$ et $g = g_n/g_d$, les auteurs définissent le résultant de Taylor comme le résultant éliminant la variable t des polynômes

$$\frac{f_n(t)f_d(s) - f_d(t)f_n(s)}{t-s}, \quad \frac{g_n(t)g_d(s) - g_d(t)g_n(s)}{t-s}. \tag{1}$$

Si cette généralisation du résultant de Taylor permet de décider si $k(t) = k(f(t), g(t))$ ou bien si $k[t] = k[f(t), g(t)]$, elle ne permet pas de retrouver exactement les points singuliers de la courbe paramétrée par $x = f(t), y = g(t)$ (voir [6, Theorem 3.1]). Le principal problème vient du fait que la formulation (1) introduit une symétrie qui confond les courbes paramétrées par $x = f(t)^{\pm 1}, y = g(t)^{\pm 1}$. Dans la première partie de cet exposé, on se propose de donner une extension fidèle du théorème d'Abhyankar. Elle est obtenue en considérant non plus la paramétrisation de la courbe rationnelle, mais le module des relations de cette paramétrisation dans un cadre projectif. Ce module se trouve être un module libre de rang 2 dont on peut extraire beaucoup d'informations, notamment sur les singularités de la courbe. On obtient ainsi très simplement une famille de courbes adjointes. Ces résultats sont publiés dans [2]. Dans une deuxième partie, on montrera que les facteurs invariants d'une matrice associée à un certain sous-résultant se décrivent complètement à partir du graphe des multiplicités (i.e. des multiplicités obtenues dans une résolution par éclatements successifs) de la courbe rationnelle considérée. Ce résultat, obtenu récemment en collaboration avec Carlos D'Andrea [3], précise et démontre deux conjectures qui ont été énoncées dans [4].

[1] Shreeram S. Abhyankar. *Algebraic geometry for scientists and engineers*, volume 35 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1990.

[2] Laurent Busé. On the equations of the moving curve ideal of a rational algebraic plane curve. *Journal of Algebra*, 321 :2317–2344, 2009.

[3] Laurent Busé and Carlos D'Andrea. Singular factors of rational plane curves. arXiv :0912.2723v1, 2009.

[4] Falai Chen, Wenping Wang, and Yang Liu. Computing singular points of plane rational curves. *J. Symb. Comput.*, 43(2) :92–117, 2008.

[5] M'Hammed El Kahoui. D-resultant and subresultants. *Proc. Amer. Math. Soc.*, 133(8) :2193–2199 (electronic), 2005.

[6] Jaime Gutierrez, Rosario Rubio, and Jie-Tai Yu. D-resultant for rational functions. *Proc. Amer. Math. Soc.*, 130(8) :2237–2246 (electronic), 2002.

[7] Arno van den Essen and Jie-Tai Yu. The D-resultant, singularities and the degree of unfaithfulness. *Proc. Amer. Math. Soc.*, 125(3) :689–695, 1997.

13. Codes quasi-cycliques et polynômes à coefficients matriciels.

Christophe Chabot (IRMAR, Université de Rennes 1)

Les codes ℓ-quasi-cycliques sont des codes stables par l'action du décalage circulaire de ℓ positions. Ils sont en fait une généralisation des codes cycliques ($\ell = 1$). On s'intéresse ici à des codes ℓ-quasi-cycliques de longueur $n = \ell m$ sur $\mathbb{F}_q$. Notre motivation est de généraliser les résultats

obtenus avec les codes cycliques tels que la génération par des polynômes et la caractérisation du code dual. On sait que les codes cycliques peuvent être vus comme engendrés par des polynômes $C = \langle g(X) \rangle$. De plus un des résultats importants est la caractérisation facile du dual. En effet, $C^\perp = \langle h^*(X) \rangle$ si $X^n - 1 = g(X)h(X)$ (où h^* désigne le polynôme réciproque de h).
Tout d'abord, nous faisons agir l'anneau des polynômes à coefficients matriciels $\mathbb{M}_\ell(\mathbb{F}_q)[X]$ sur des suites à coefficients dans $\mathbb{F}_q^\ell$. On peut adapter cette action sur les mots d'un code quasi-cyclique vivant dans $\mathbb{F}_q^{\ell m}$. De cette manière, on construit des codes quasi-cycliques annulés par des polynômes ($C = \Omega(P)$). Il est de plus facile d'expliciter une matrice génératrice du code annulé par un polynôme donné P.
On obtient aussi un résultat analogue à celui des codes cycliques ($\Omega(P)^\perp = \Omega({}^tQ^*)$ dans le cas Euclidien et $\Omega(P)^\perp = \Omega(\theta({}^tQ^*))$ dans le cas Hermitien). Ceci nous permet de construire effectivement des codes autoduaux Euclidiens et Hermitiens et pour la plupart des longueurs, les meilleures distances minimales connues sont atteintes par des codes de ce type.

14. Un algorithme quasi-optimal pour la décomposition des fractions rationnelles en plusieurs variables.

Guillaume Chèze (Institut de Mathématiques de Toulouse, Université Paul Sabatier Toulouse 3)

Dans cet exposé nous allons présenter un algorithme permettant de décomposer les fractions rationnelles de plusieurs variables.
Une fraction rationnelle $f \in \mathbb{K}(X_1, \dots, X_n)$ est dite décomposable lorsqu'elle peut s'écrire $f = u \circ h$, avec $u \in \mathbb{K}(T)$, $h \in \mathbb{K}(X_1, \dots, X_n)$ et $\deg u \geq 2$; sinon f est dite indécomposable. La décomposition est utilisée pour étudier : la version généralisée du théorème de Lüroth (i.e. cas multivarié), la clôture entière de l'anneau $\mathbb{K}[f]$, le spectre des fractions rationnelles ....
Nous présenterons un algorithme probabiliste permettant d'obtenir sous certaines hypothèses la décomposition de $f \in \mathbb{K}(X_1, \dots, X_n)$ avec $\tilde{\mathcal{O}}(d^n)$ opérations arithmétiques dans $\mathbb{K}$ où d est le degré de f et $n \geq 3$ est fixé.
La principale remarque permettant à notre algorithme de fonctionner est la suivante : Si $f = f_1/f_2 \in \mathbb{K}(X_1, \dots, X_n)$ et $f = u \circ h$ avec $u = u_1/u_2$ et $h = h_1/h_2$ alors $f_1 - \lambda f_2 = e \prod_{i=1}^{\deg f} (h_1 - \lambda_i h_2)$ où $e \in \mathbb{K}$, et les λ_i sont les racines de $u_1 - \lambda u_2$.
Cette méthode ramène donc le problème de la décomposition à un problème de factorisation.

15. Régularisation et solutions régulières de systèmes différentiels linéaires

Carole El Bacha (Université de Limoges ; CNRS ; XLIM UMR 6172 ; DMI)

Nous considérons un système de n équations différentielles linéaires d'ordre ℓ

$$\mathcal{L}(x, \vartheta)(y(x)) = A_\ell(x)\, \vartheta^\ell(y(x)) + \cdots + A_1(x)\, \vartheta(y(x)) + A_0(x)\, y(x) = 0, \tag{2}$$

où $\vartheta = x\frac{d}{dx}$ et pour $i = 0, \dots, \ell$, $A_i(x) \in \mathbb{K}[x]^{n \times n}$ ($\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$) est une matrice carrée de taille n à coefficients polynomiaux et nous nous intéressons au calcul de ses solutions régulières formelles, *i. e.*, de la forme $y(x) = x^{\lambda_0}\, z(x)$ où $\lambda_0 \in \overline{\mathbb{K}}$, la clôture algébrique de $\mathbb{K}$, et $z(x) \in \overline{\mathbb{K}}[\ln(x)][[x]]^n$. À un tel système, nous associons la matrice polynomiale

$$\mathcal{L}(0, \lambda) = A_\ell(0)\, \lambda^\ell + \cdots + A_1(0)\, \lambda + A_0(0).$$

Ce problème a été très étudié dans le cas scalaire $n = 1$ où différentes méthodes ont été développées (*e. g.*, celles de Frobenius - 1873, Heffter - 1894 et Poole - 1936). On montre que l'exposant $\lambda_0 \in \overline{\mathbb{K}}$ doit être choisi comme racine du *polynôme indiciel* $\mathcal{L}(0, \lambda)$. La méthode de Heffter a été généralisée au cas des systèmes du premier ordre $\ell = 1$ dans [4] et au cas général, n et ℓ arbitraires, dans [1] où le problème est réduit au calcul de séries formelles solutions de systèmes aux récurrences. Récemment, dans [3], nous avons proposé un algorithme utilisant l'approche de Poole pour calculer une base de l'espace des solutions régulières des systèmes de la forme (2) vérifiant la condition $A_\ell(0)$ inversible. Ici, l'exposant $\lambda_0 \in \overline{\mathbb{K}}$ doit être choisi comme valeur propre de la matrice polynomiale $\mathcal{L}(0, \lambda)$ c'est-à-dire doit vérifier $\det(\mathcal{L}(0, \lambda_0)) = 0$. Ce déterminant joue donc le rôle du polynôme indiciel dans le cas scalaire. Cet algorithme a été implémenté en Maple et nous avons donné une estimation de sa complexité. Dans ce même papier, nous avons aussi indiqué comment généraliser la méthode de Frobenius à ce cas.
Dans la première partie de l'exposé, nous montrons que la méthode décrite dans [3] peut être

appliquée à tout système (2) vérifiant la condition $\det(\mathcal{L}(0,\lambda)) \neq 0$ et que la dimension de l'espace des solutions régulières est égale au degré de $\det(\mathcal{L}(0,\lambda))$. Nous modifions légèrement l'algorithme présenté dans [3] pour qu'il retourne la solution régulière générale du système (2). La deuxième partie est dédiée au cas où le système (2) vérifie la condition $\det(\mathcal{L}(0,\lambda)) \equiv 0$. Nous supposons ici que le coefficient de tête $A_\ell(x)$ est inversible dans $\mathbb{K}(x)^{n\times n}$ ce qui garantit que l'espace des solutions régulières de (2) est de dimension finie. Nous développons un algorithme qui, étant donné un tel système, calcule un système auxiliaire $\overline{\mathcal{L}}(x,\vartheta)(u(x)) = 0$ vérifiant $\det(\overline{\mathcal{L}}(0,\lambda)) \neq 0$. Ainsi, l'algorithme développé dans la première partie peut être appliqué pour calculer la solution régulière générale de $\overline{\mathcal{L}}(x,\vartheta)(u(x)) = 0$ à partir de laquelle nous montrons comment retrouver celle de (2). Dans un premier temps, nous nous intéressons à l'existence d'un changement de variable $y = T\,u$ avec $T \in \mathrm{GL}_n(\mathbb{K}(x))$ réalisant une telle *régularisation*. Notons que le système $\overline{\mathcal{L}}(x,\vartheta)(u(x)) = 0$ obtenu par ce cha ngement de variable est lui aussi d'ordre ℓ et équivalent à (2), dans le sens qu'il existe une bijection entre leurs espaces de solutions respectifs. En utilisant le calcul d'une base minimale (à droite) de la matrice polynomiale $\mathcal{L}(0,\lambda)$ (voir [5]), nous donnons un algorithme permettant de calculer un tel changement de variable lorsqu'il existe, ou de prouver qu'il n'en existe pas. La non-existence d'un changement de variable rendant la matrice polynomiale associée au nouveau système régulière est due à l'existence d'éléments non-constants (*i. e.*, dépendants de λ) dans une base minimale (à droite) de la matrice polynomiale associée à l'un des systèmes différentiels auxiliaires construits par l'algorithme. Lorsqu'un tel changement de variable n'existe pas, nous développons une autre méthode consistant à appliquer au système (2) une succession de transformations élémentaires, *e. g.*, ajouter à une équation une autre multipliée à gauche par un opérateur différentiel scalaire ou bien multiplier une équation à gauche par un opérateur différentiel scalaire non-nul. En suivant cette démarche analogue à celle de l'algorithme *EG'* proposé par Abramov et al dans [2], nous proposons un algorithme, qui étant donné le système (2) avec $A_\ell(x)$ inversible dans $\mathbb{K}(x)^{n\times n}$, calcule un système associé $\overline{\mathcal{L}}(x,\vartheta)(u(x)) = 0$ vérifiant $\det(\overline{\mathcal{L}}(0,\lambda)) \neq 0$. Notons que ce système est en général d'ordre supérieur ou égal à ℓ et n'est pas nécessairement équivalent au système (2) ; cependant la solution régulière générale de (2) peut s'obtenir à partir de celle de $\overline{\mathcal{L}}(x,\vartheta)(u(x)) = 0$. La complexité des différents algorithmes proposés est analysée et ces algorithmes ont été implémentés en Maple.

[1] S. Abramov, M. Bronstein and D. E. Khmelnov. On Regular and Logarithmic Solutions of Ordinary Linear Differential Systems. *Computer Algebra in Scientific Computing, Lecture Notes in Computer Science, Springer Verlag*, 3718 :1-12, 2005.

[2] S. Abramov, M. Bronstein and D.E. Khmelnov. Regularisation of Linear Recurrence Systems. *Transactions of the A.M. Lyapunov Institute*, 4 : 158-171, 2003.

[3] M. Barkatou, T. Cluzeau and C. El Bacha. Algorithms for Regular Solutions of Higher-Order Linear Differential Systems. In *Proceedings of ISSAC'2009*, p. 7-14, ACM Press.

[4] M. Barkatou and E. Pflügel. An Algorithm Computing the Regular Formal Solutions of a System of Linear Differential Equations. *J. Symbolic Computation*, 11 :1-20, 1998.

[5] F. De Terán, F. M. Dopico and D. S. Mackey. Linearizations of Singular Matrix Polynomials and the Recovery of Minimal Indices. *Electronic J. of Linear Algebra ISSN 1081-3810*, 18 :371-402, July 2009.

16. Arithmétique de boules.

Joris van der Hoeven (CNRS, Universitè Paris-Sud)

Dans cet exposé, nous proposons une introduction à l'arithmétique des boules. Il s'agit d'une variante de l'arithmétique d'intervalles, permettant de faire de l'analyse numérique certifiée, tout en étant mieux adapté au calcul vectoriel et en précision multiple. Nous survolerons quelques techniques classiques, et aborderons quelques questions de complexité algorithmique.

17. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time

Jean-Gabriel Kammerer (DGA/MI, IRMAR, Université de Rennes 1)

Joint work with R. Lercier and G. Renault.

We study parametrizations of bivariate polynomial equations, over finite fields. Those equations define plane algebraic curves. More precisely, let $\mathbb{F}_q$ be a finite field of odd characteristic p and $H/\ \mathbb{F}_q : y^2 = f(x)$ where $\deg f = d$ be an elliptic (if $d = 3$ or 4) or hyperelliptic (if $d \geqslant 5$) curve, we consider the problem of computing points on H in deterministic polynomial time.

In the case of elliptic curves, we may remark that it is enough to compute one rational point G, since we can have numerous other points from mG for $m \in \mathbb{Z}$ (at least if G is of large enough order). To compute such a G, one might test random elements $x \in \mathbb{F}_q$ until $f(x)$ is a square. But without assuming GRH, we have no guarantee of finding a suitable x after a small enough number of attempts. Moreover, without assuming GRH, none deterministic algorithm is known for computing square roots when $p \equiv 1 \bmod 4$. Maybe, a more serious attempt in this direction is due to Atkin and Morain [AM93]. They remark that if x_0 is any element of $\mathbb{F}_q$ and $\lambda = f(x_0)$, then the point $(\lambda x_0, \lambda^{(d+1)/2})$ is on the curve $Y^2 = \lambda^d f(X/\lambda)$. But again, the latter can be either isomorphic to the curve or its quadratic twist, following that λ is a quadratic residue or not, and we have no way to control this in deterministic time.

In 2006, Shallue and Woestjine [SvdW06] proposed the first practical deterministic algorithm to encode points into an elliptic curve, quickly generalized by Ulas [Ula07] to the family of hyperelliptic curves defined by the equation $y^2 = x^n + ax + b$ or $y^2 = x^n + ax^2 + bx$. In 2009, Icart proposed a much more efficient encoding for elliptic curves, running in deterministic time $\mathcal{O}(\log^{2+o(1)} q)$ provided that the cubic root function, inverse of $x \mapsto x^3$ on $\mathbb{F}_q$, is an automorphism. Namely, this turns into $q \equiv 2 \bmod 3$ [Ica09]. This encoding uses Cardano's formulae in order to parametrize the points (x, y) on the elliptic curve $E : x^3 + ax + b = y^2$. The main difficulty of finding deterministic parametrizations is that every time we have to compute a square root, we need to ensure that the element is indeed a square: computing roots of solvable polynomials, among them degree 3 polynomials, often begins by computing the square root of a discriminant. Icart annihilates the problem by cleverly parametrizing y such that the resulting equation in x is always solvable without any square rooting algorithm.

We present here for each odd degree d a new family of bivariate equations of the form $y^2 = f(x)$, which admit as nice parametrizing formulae as Icart's ones. Especially, the encoding algorithm runs in deterministic time $\mathcal{O}(\log^{2+o(1)} q)$ too. In terms of algebraic curves, this turns into having, for each genus $g \geqslant 2$, a large family of hyperelliptic curves which admit an efficient deterministic encoding function, provided that $q \equiv 2 \bmod 3$ and, additionally, that $q-1$ and $(2g+1)$ are coprime. This (small) restriction allows to compute efficiently all 3^{th} and $(2g+1)^{\text{th}}$ roots needed by the resolution by radicals. This parametrization essentially works in two steps.

- We first write roots of our polynomials $f(x)$ in terms of radicals.
- We then parametrize auxiliary conics in order to avoid square root computations.

So we get a full parametrization of a large subset of the solutions of any equation in the family.

[AM93] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993), no. 203, 29–68.

[Ica09] Thomas Icart, *How to hash into elliptic curves*, CRYPTO (Shai Halevi, ed.), Lecture Notes in Computer Science, vol. 5677, Springer, 2009, pp. 303–316.

[SvdW06] Andrew Shallue and Christiaan van de Woestijne, *Construction of rational points on elliptic curves over finite fields*, ANTS (Florian Hess, Sebastian Pauli, and Michael E. Pohst, eds.), Lecture Notes in Computer Science, vol. 4076, Springer, 2006, pp. 510–524.

[Ula07] Marciej Ulas, *Rational points on certain hyperellptic curves over finite fields*, Bull. Polish Acad. Sci. Math. (2007), no. 55, 97–104.

18. Algorithmique dans les algèbres d'invariants polynomiaux sous un groupe fini.

Romain Lebreton (LIX, Polytechnique)

Nous allons présenter quelques aspects algorithmiques essentiels pour le calculs dans les algèbres d'invariants polynomiaux sous un groupe fini. Une manipulation rapide de ces objets a des répercutions pour la résolution de systèmes d'équations polynomiales invariantes, pour le calcul de groupes de Galois et autres. La décomposition d'Hironaka d'une algèbre d'invariants permet une réécriture unique et commode de tout invariant. Les algorithmes trouvant une telle décomposition ont pour facteur limitant le calcul de dimension d'une variété algébrique. Nous détaillerons quelques pistes d'améliorations.

19. Paramétrisation polynomiale des nœuds à deux ponts.

Pierre-Vincent Koseleff (Institut de mathèmatiques de Jussieu, UPMC PARIS 6)

Travail commun avec Daniel Pecker (UPMC–Paris 6).
On montre ici comment tout nœud rationnel (ou à deux ponts) à N croisements peut effectivement se paramétrer par une courbe polynomiale $x = T_3(t)$, $y = T_b(t)$, $z = C(t)$, où 3 ne divise pas b, T_n est le polynôme de Chebyshev de degré n, et $b + \deg C = 3N$. On sait que tout nœud non compact peut-être obtenu comme plongement polynomial $\mathbf{R} \to \mathbf{R}^3 \subset \mathbf{S}^3$. L'objet de cet exposé est de donner une méthode effective de paramétrisation des nœuds rationnels par une courbe polynomiale. Un nœud (compact) rationnel (ou à deux ponts) a la propriété qu'il admet un diagramme 4-plat de la forme suivante : Ici les $a_i \in \mathbf{Z}$ désignent le nombre de croisements (positifs ou négatifs). On peut

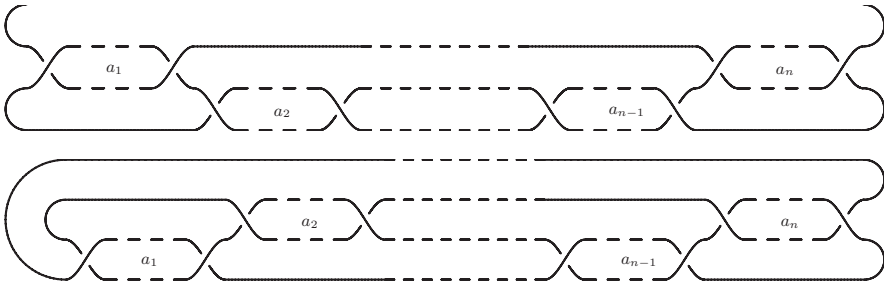
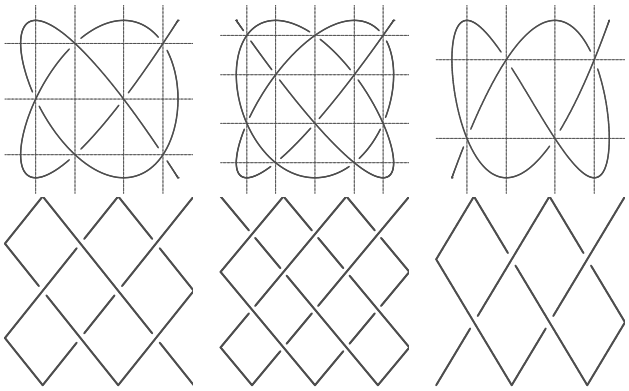


Figure 2: Forme normale de Conway $C(a_1, \ldots, a_n)$, n impair ou pair

identifier (Schubert, 56) les nœuds rationnels grâce à la fraction continue $\dfrac{\alpha}{\beta} = [a_1, \ldots, a_n]$, $\alpha > 0$. Deux fractions de Schubert $\dfrac{\alpha}{\beta}$ et $\dfrac{\alpha'}{\beta'}$ représentent le même nœud (à mirroir près) si et seulement si $\alpha = \alpha'$ et $\beta' = \pm\beta^{\pm 1} \pmod{\alpha}$. On considère ici des nœuds non compacts en envoyant un point à l'infini. Nous traitons deux problèmes :

- Trouver une courbe plane $(x(t), y(t))$ (minimale) qui puisse être la projection du nœud étudié.
- Trouver une hauteur $z(t)$ telle que le courbe gauche obtenue soit effectivement le nœud voulu.

Il est commode de chercher les projections de ces nœuds comme des courbes planes de Chebyshev : $\mathcal{C}(a, b) : x = T_a(t)$, $y = T_b(t)$. Elles ont exactement $\frac{1}{2}(a-1)(b-1)$ points doubles réels, ce qui fait qu'une courbe gauche régulière $x = T_a(t)$, $y = T_b(t)$, $z = C(t)$ est isotope à un "nœud de billiard". Dans le cas où $a = 3$, le diagramme obtenu $\mathcal{C}(3, b)$ est naturellement sous forme de Conway $C(\pm 1, \ldots, \pm 1)$. Nous démontrons tout d'abord : *tout nombre rationnel* $\dfrac{\alpha}{\beta}$ *s'écrit de façon unique comme fraction continue* $[e_1, e_2, \ldots, e_n]$*, où* $e_i = \pm 1$*,* $e_{n-1}e_n > 0$ *et où il n'y a pas deux changements de signe consécutifs.* Cette propriété conduit à mettre en relation le monoïde libre engendré par les homographies $\tau \circ \iota$ et $\iota \circ \tau$ où $\tau : x \mapsto 1 + x$ et $\iota : x \mapsto 1/x$ et l'ensemble des nœuds rationnels, ce qui permet de retrouver de façon élémentaire des résultats classiques de dénombrement des nœuds rationnels. Nous démontrons ensuite : *Tout nœud rationnel à* N *croisements s'obtient comme courbe polynomiale* $x = T_3(t)$, $y = T_b(t)$, $z = C(t)$ *où* $b + \deg C = 3N$. Ces courbes semblent être de degré minimal. On donnera également les paramétrisations explicites



minimales pour des familles infinies de nœuds rationnels, tels que les nœuds toriques où les nœuds de Fibonacci. **Références**

Koseleff, P.-V., Pecker, D, *Chebyshev knots*, à paraître dans Journal of Knot Theory and Ramifications. `arXiv :0812.1089`

Koseleff, P.-V., Pecker, D, *Chebyshev diagrams for two-bridge knots*, 25p., en révision, `arXiv :0909.3281`

20. Mathemagix : langage, fonctionnalités et performances

J. van der Hoeven, B. Mourrain, G. Lecerf, O. Ruatta, Ph. Trébuchet (Mathemagix)

Nous présenterons l'état actuel du système de calcul analytique et symbolique Mathemagix (`www.mathemagix.org`). Nous commencerons par une brève description du langage et de l'état d'avancement du compilateur. Nous présenterons ensuite les fonctionnalités disponibles dans les librairies `C++` : types numériques, polynômes, séries, matrices, etc.

21. NumGfun : calcul efficace en Maple des solutions analytiques d'équations différentielles linéaires à coefficients polynomiaux.

Marc Mezzaroba (INRIA Rocquencourt)

L'objet de cet exposé est de présenter NumGfun, un module Maple consacré à la manipulation « analytique » des solutions d'équations différentielles linéaires à coefficients polynomiaux (fonctions D-finies ou holonomes). Les principales fonctionnalités de NumGfun concernent l'évaluation numérique des fonctions D-finies, et le calcul symbolique de bornes « asymptotiquement fines » qui permettent de contrôler leur comportement. En particulier, NumGfun contient ce qui semble être la seule implémentation générale des algorithmes de prolongement analytique numérique des fonctions D-finies donnés par D.V. et G.V. Chudnovsky à la fin des années 1980. Je ferai une démonstration de l'utilisation de NumGfun, et je reviendrai sur quelques-uns des algorithmes sur lesquels il s'appuie.

22. Triangular Decomposition of Semi-Algebraic Systems

Marc Moreno Maza (University of Western Ontario)

This is joint work with Changbo Chen, James H. Davenport, John P. May, Bican Xia and Rong Xiao.

Regular chains and triangular decompositions are fundamental and well-developed tools for describing the complex solutions of polynomial systems. We propose adaptations of these tools focusing on solutions of the real analogue : systems of equations, inequations and inequalities given by polynomials with rational number coefficients.

We introduce the notion of a regular semi-algebraic system and show that any semi-algebraic system S can be decomposed into finitely many regular semi-algebraic systems, that we call a triangular decomposition of S. We show that under some assumptions, such a decomposition can be computed in singly exponential time w.r.t. the number of variables.

We also propose for this task an algorithm that is suitable for implementation. In this case, we rely

on the notions of *border polynomial* and *fingerprint polynomial set* for real root classification of parametric polynomial systems. We establish singly exponential running time estimates for computing these objects.
We also report on the implementation of this algorithm for triangular decomposition of semi-algebraic systems. Our comparative experimental results illustrate the effectiveness of the presented algorithm.
Changbo Chen
University of Western Ontario
changbo.chen@gmail.com

James H. Davenport
University of Bath
J.H.Davenport@bath.ac.uk

John P. May
Maplesoft
jmay@maplesoft.com

Marc Moreno Maza
University of Western Ontario
moreno@csd.uwo.ca

Bican Xia
Peking University
xbc@math.pku.edu.cn

Rong Xiao
University of Western Ontario
akelux@gmail.com

23. Étude des solutions stables et chaotiques d'un modèle biologique.

Guillaume Moroz (LIP6)

Les impulsions électriques d'un réseau de neurones peuvent se modéliser par un système d'équations différentielles dépendant de paramètres biologiques. En fonction des paramètres, le signal peut être stable ou encore chaotique. Afin de mieux comprendre les différents comportements du signal nerveux observé expérimentalement, il est important de réussir à classer les paramètres biologiques en fonction du caractère stable ou chaotique des solutions du système différentiel correspondant. Je montrerai comment une approche de type calcul formel permet d'obtenir des résultats intéressants pour ce problème.

24. Décomposition de tenseurs, matrices de moments et polynômes

Bernard Mourrain (INRIA Sophia Antipolis - Méditerrannée)

Travail en commun avec J. Brachat, P. Comon, E. Tsigaridas.
Dans des domaines d'applications assez variés (traitement du signal, télécommunication, fouille de données, statistique, chémométrie, complexité, ...) apparaît le problème suivant : à partir d'observations, on mesure des quantités corrélées qui sont regroupées sous formes de tenseurs. On cherche alors à décomposer de manière minimale ce tenseur en une somme de produits tensoriels de vecteurs, afin de déduire des informations sur les sources qui conduisent à ces observations. Dans le cas de tenseurs d'ordre deux (*i. e.* de matrices), ce problème correspond à un calcul de rang et des techniques comme la SVD (Singular Value Decomposition) fournissent des outils numériques efficaces pour calculer de telles décompositions. Ce problème s'étend naturellement à des tenseurs symétriques ou à des polynômes homogènes. Dans ce cas, il est connu sous le nom de problème de Waring. L'analyse de ce problème est beaucoup plus ouverte que pour les tenseurs d'ordre deux, autant sur le plan théorique que pratique. Une première méthode pour calculer le rang et une telle décomposition minimale a été proposée en 1886 par S. S. Sylvester pour des formes binaires.

Dans cet exposé, nous décrirons une généralisation récente de cette approche à des polynômes homogènes quelconques. Des liens avec les problèmes des moments (tronqués) seront exhibés ainsi que des connexions avec les bases de bords et les approximations de Padé.

[1] J. Brachat, P. Comon, B. Mourrain et E. P. Tsigaridas. Symmetric tensor decomposition. In 17th European Signal Processing Conference 2009. (24/08/2009) 525-529.

[2] M. Laurent, B. Mourrain. A Sparse Flat Extension Theorem for Moment Matrices. Archiv der Mathematik 93 (2009) 87-98.

25. Borne de Jacobi et calcul de l'index pour toutes les composantes quasi-régulières d'un système d'EDO

François Ollivier (LIX, Polytechnique)

Avec le soutien du PEPS LÉDA (Logistique des Équations Différentielles Algébriques). Travaux en cours avec Alexandre Sedoglavic.

Introduction

Le principe de moindre action possède au moins deux caractéristiques miraculeuses : une expression aussi élégante que peu intuitive [7] et une efficacité fort précieuse pour la mise en équations d'un système physique. Le lagrangien fournit en effet une forme normale, dont le coût se limite à une inversion de matrices. Le calcul de formes normales pour des systèmes généraux d'équations différentielles peut donc sembler un jeu gratuit. Toutefois, il n'est pas rare en pratique que des simplifications, difficilement évitables lorsque certaines constantes sont extrêmement petites, ne viennent troubler cette belle harmonie. Il faut alors dériver les équations du système un nombre de fois suffisant pour qu'une forme normale ou un ensemble caractéristique puisse être calculés. Cet ordre de dérivation est *l'index* du système et sa connaisance est déterminante pour majorer le coût des calculs. L'automatique fait aussi apparaître naturellement des « systèmes à index », par exemple lorsque l'on veut calculer les paramètres ou l'état d'un système à partir de ses sorties et entrées. Par ailleurs, s'il est naturel d'associer à un problème physique un idéal différentiel premier, il existe en général, si les équations sont non linéaires, des *solutions singulières* : la théorie classique montre que ce sont les enveloppes des solutions régulières. L'index a donc une nature locale : là où une solution régulière est tangeante à une solution singulière, il faut dériver davantage pour discerner les deux solutions et pouvoir intégrer numériquement [8]. Il n'est pas immédiat de majorer l'index local d'une composante régulière en un point singulier, qui correspond à l'index global de la composante singulière qu'elle traverse. Il existe une vaste littérature sur le sujet et de nombreuses notions d'index, en général tous notés σ, qui co'ı ncident génériquement à une unité près, certains auteurs estimant que, si l'équation n'est pas quasi-linéaire, il faut toujours la dériver au moins une fois. Nous considérerons ici l'index de forme normale, c'est-à-dire le nombre minimal de dérivations nécessaire au calcul d'une forme normale ou d'un ensemble caractéristique [9].

1. Définitions

Nous considérons un système d'équations $f_i = 0$, $1 \leq i \leq n$ qui sont des polynômes différentiels en n variables x_j à coefficient dans un corps différentiel k [10]. Le système d'équations f engendre un idéal différentiel $[f]$, qui est le plus petit idéal de $k\{x\}$ contenant les équations de f et toutes

7. Maupertuis y voyait une preuve de l'existence de Dieu. Voir *Les Loix du mouvement et du repos déduites d'un principe métaphysique.*

8. L'équation $x'^2 - 4x = 0$ est l'exemple le plus simple. Les solutions constituent une famille de parabolles dépendant d'un paramètre : $x(t) = (t + c)^2$ et son enveloppe est la courbe $x(t) = 0$. Si l'on dérive l'équation, on obtient $x'(2x'' - 4) = 0$; les solutions régulières satisfont $x'' = 2$ et la courbe singulière $x' = 0$.

9. Nous utilisons ici le formalisme de l'algèbre différentielle[15, 9]. L'article [12] illustre l'utilisation de la borne de Jacobi dans le formalisme des diffiétés, représentées par des formes normales sur des ouverts convenables de l'espace des jets.

10. Par exemple $\mathbf{Q}(t)$ muni de la dérivation d/dt ou $\mathbf{Q}$ muni de la dérivation nulle sont des corps différentiels. L'anneau des polynômes différentiels, noté $k\{x\}$, est l'anneau de polynômes $k[x_i^{(j)}]$, muni de l'unique dérivation δ compatible avec la dérivation de k et $\delta x_i^{(j)} = x_i^{(j+1)}$.

leurs dérivées. Si k est de caractéristique 0, ce que nous supposerons, le radical de $[f]$ est un idéal différentiel, noté $\{f\}$ qui est égal à une intersection finie d'idéaux différentiels premiers, appelé les composantes du système f : $\{f\} = \cap_{i=1}^{s} \mathcal{P}_i$ [11]. Nous allons utiliser une hypothèse de régularité naturelle, qui signifie que l'essentiel des invariants du système sont ceux du système linéarisé [12].

Définition 1. — Une composante $\mathcal{P}$ de f sera dite *(globalement) quasi-régulière* (resp. *quasi régulière en* $\mathcal{I} \subset \mathcal{P}$, où $\mathcal{I}$ est un idéal premier non nécessairement différentiel) si, en désignant par K/k l'extension de corps associée à $\mathcal{P}$ (resp. $\mathcal{I}$), la famille $df_i^{(j)}$, $1 \leq i \leq n$, $j \in \mathbf{N}$ est libre dans $\Omega_{k\{x\}/k} \otimes_k K$.

2. La borne de Jacobi

Ce résultat est contenu dans deux articles posthumes de Jacobi [13]. Bien que non datés, on peut estimer qu'il provient du projet abandonné d'un vaste ouvrage intitulé *Phoronomie*. Il s'agit d'une borne *a priori* sur l'ordre d'un système d'équations différentielles ordinaires, plus précise que « l'analogue différentiel du théorème de Bézout » prouvé par Ritt [14]. Soit A la matrice des ordres, définie par $a_{i,j} := \mathrm{ord}_{x_j} f_i$, la borne de Jacobi est exprimée par le « déterminant tropical » [15]

$$\mathcal{O} := \max_{\sigma \in S_n} \sum_{i=1}^{n} a_{i,\sigma(i)}.$$

Théorème2. — *Soit $\mathcal{P}$ une composante quasi régulière de f, de dimension différentielle* 0*, l'ordre de $\mathcal{P}$* [16] *est au plus $\mathcal{O}$.* [17]. Jacobi a donné une preuve de ce résultat qui peut être rendue parfaitement rigoureuse [13]. Des preuves contemporaines ont été publiées [10, 12], y compris dans le cas des EDP [11], mais la borne de Jacobi demeure conjecturale dans le cas de composantes singulières qui ne sont pas quasi régulières. On trouvera plus de détails dans notre article [13] et la page `www.lix.polytechnique.fr/ char'176ollivier/Borne_Jacobi_I/` Jacobi ne s'est pas contenté d'un résultat théorique, il a également fourni un algorithme permettant de calculer cette borne en temps polynomial. Celui-ci a été réinventé par Kuhn en 1955. L'idée de base est de calculer le *canon minimal*, c'est-à-dire l'unique n-uplet d'entier λ_i telle que la matrice $(a_{i,j} + \lambda_i)$ possèdent des termes maximaux dans chaque colonne, qui soient situés dans des lignes toutes différentes. On conçoit que, sous cette hypothèse, le calcul du déterminant tropical devient aisé. Notons $\Lambda = \max_i \lambda_i$, $\alpha_i = \Lambda - \lambda_i$ et $\beta_j = \max_i a_{i,j} - \alpha_i$. Les n-uplet constituent dans le vocabulaire de Kuhn une *couverture minimale*, c'est-à-dire des n-uplets minimaux tels que $a_{i,j} \leq \alpha_i + \beta_j$. Jacobi affirme en outre que la borne est atteinte ssi le *déterminant tronqué* $|\partial f_i / \partial x_j^{(\alpha_i+\beta_j)}|$ est non nul [4, 12]. Sous cette hypothèse, il montre qu'une forme normale peut être calculée en dérivant l'équation f_i au plus λ_i fois [18] et que l'on peut calculer une résolvante en x_{j_0} [19] en dérivant l'équation f_i un nombre

11. Dans notre exemple, $\{x'^2 - 4x\} = [x'^2 - 4x, x'' - 2] \cap [x]$; on constate que même un polynôme sans facteur peut engendrer un idéal différentiel contenant plusieurs composantes.

12. Cette idée a été explicitement formulée par Jacobi. On la retrouve sous une forme moderne dans les travaux de Johnson, qui l'a utilisée pour la conjecture de Janet [7, 8]. Sur notre exemple, le système linéarisé est $2x'dx' + 4dx$, soit K_i, $i = 1, 2$ les extension de corps différentiel associées aux composantes régulière et singulière de l'équation. Dans $\Omega_{k\{x\}/k} \otimes_k K_2$, l'équation linéarisée devient $4dx = 0$, puisque $x' = 0$ dans K_2 : elle est donc d'ordre nul, égal à celui de la composante $x = 0$.

13. Nous renvoyons aux traductions anglaises [4, 5] ainsi qu'aux traduction françaises et aux textes latin originaux disponible sur la page web http://www.lix.polytechnique.fr/~ollivier/JACOBI/jacobi.htm

14. La borne de Ritt est $\sum_{j=1}^{n} \max_{i=1}^{n} \mathrm{ord}_{x_j} f_i$.

15. La géométrie tropicale s'obtient en remplaçant les produit par des sommes et les sommes par des maxima ou minima. Il est plaisant de songer que le déterminant tropical a été inventé à K'onigsberg : 65 jours de neige et 159 jours de pluie par an en moyenne.

16. La dimension différentielle est le nombre de « fonctions arbitraires » intervenant dans une solution ; l'ordre est le nombre de conditions initiales pouvant être choisies arbitrairement, ou encore le dégré de transcendance algébrique de l'extension de corps K/k associée à une composante $\mathcal{P}$.

17. On peut améliorer le résultat en posant $\mathrm{ord}_{x_j} f_i = -\infty$ si f_i est exempte de x_i et de ses dérivées. C'est la borne *forte*. Par ailleurs, on peut aussi faire dépendre l'expression de l'ordre de la composante $\mathcal{P}$ choisie en posant : $a_{i,j} = {}_{\mathcal{P}}\mathrm{ord}_{x_j} f_i := \max\{\ell | \partial f_i / \partial x_j^{(\ell)} \notin \mathcal{P}\}$.

18. Un résultat redécouvert par Pryce en 2001 [14].

19. C'est-à-dire une équation d'ordre $\mathcal{O}$ ne dépendant que de x_{j_0} et $n-1$ équations exprimant x_j, $j \neq j_0$, en fonction de x_{j_0} et de ses dérivées ; sous réserve que ces expressions existent.

de fois égal au déterminant tropical de la matrice obtenu en remplaçant dans A la ligne i et la colonne j_0 par des 0[5, 13].

3. Index de forme normale

Les résultats de Jacobi incitent à rechercher des bornes plus générales pour l'index en s'inspirant de ses méthodes. C'est ce qu'ont fait avec succès nos collègues argentins Lisi D'Alfonso, Gabriela Jeronimo, Gustavo Massaccesi et Pablo Solernó [2]. La notion d'index qu'ils considèrent est l'ordre de dérivation nécessaire pour mettre en forme normale le système linéarisé. Pour des raisons techniques, ils n'utilisent pas la borne forte et se restreignent à des formes normales pour des ordres respectant l'ordre de dérivation *(orderly orderings)*. Nous considérerons des ordres plus généraux, avec la borne forte, qui a l'avantage d'être compatible avec la réduction à l'ordre 1. Mais surtout, nous montrons que si une composante est *régulière*, leur borne s'étend à la mise en forme normale, ou au calcul d'un ensemble caractéristique pour le système non linéaire f lui-même.

Définition 3. — On appelle *index de forme normale* (resp. *multiindex*) d'une composante $\mathcal{P}$ de f le plus petit entier ${}_{\mathcal{P}}\sigma$ (resp. un n-uplet minimal) [20] tel qu'il existe un ensemble caractéristique $\mathcal{A}$ de $\mathcal{P}$ et un polynôme différentiel g tels que $\mathcal{A} \subset (f_i^{(\ell)} | 1 \leq i \leq n, 0 \leq \ell \leq {}_{\mathcal{P}}\sigma) : g^\infty$ (resp. $\mathcal{A} \subset (f_i^{(\ell)} | 1 \leq i \leq n, 0 \leq \ell \leq {}_{\mathcal{P}}\sigma_i) : g^\infty$. On définira de même des index et multi-index $\overset{\prec}{}_{\mathcal{P}}\sigma$ et $\overset{\circ}{}_{\mathcal{P}}\sigma$, correspondant respectivement au calcul d'un ensemble caractéristique *pour un ordre $\prec$ spécifié sur les dérivées* et au calcul de *tous les ensembles caractéristiques possibles.* Il nous faut maintenant préciser ce qu'il faut entendre par composante régulière. Nous proposons la définition suivante, qui est manifestement compatible avec la théorie classique dans le cas d'une équation unique.

Définition 4. — Nous dirons qu'une composante quasi régulière $\mathcal{P}$ de f est *régulière* si, pour tout ordre, toute composante $\mathcal{Q}$ de f distincte de $\mathcal{P}$ admet un ensemble caractéristique $\mathcal{A} \not\subset \mathcal{P}$.

Théorème5. — *Si $\mathcal{P}$ est une composante régulière, alors*

$$ {}_{\mathcal{P}}\sigma_i \leq \lambda_i + \mathcal{O} - \mathrm{ord}\mathcal{P} \quad et \quad \overset{\circ}{}_{\mathcal{P}}\sigma_i \leq \text{Dét. trop. } {}_iA,$$

où ${}_iA$ désigne la matrice obtenue en remplaçant dans A la ligne i par des zéros [21] Les arguments d'une preuve sont les suivants. On commence par montrer que l'on peut se ramener au cas linéaire, pourvu que $d\mathcal{A} \subset (df_i^\ell | 0 \leq \ell \leq \sigma_i)$ implique $\mathcal{A} \subset (f_i^\ell | 0 \leq \ell \leq \sigma_i) : g^\infty$. Ceci n'est pas toujours vrai, mais la propriété est générique, et l'on peut modifier le système, sans en changer la matrice A, ni l'index ou le multi-index [22], de sorte que ceux du système linéarisé coïncident. Ensuite, pour prouver la majoration de $\overset{\circ}{}_{\mathcal{P}}\sigma_i$ dans le cas linéaire, on peut ajouter des seconds membres génériques $df_i = z_i$. Le multi index σ_i de l'équation i sera l'ordre de z_i dans une forme normale. Si dx_j est la dérivée de tête d'une des équations de $d\mathcal{A}$ où z_i apparaît à l'ordre le plus grand, on peut sans dérivation calculer une forme normale pour un système en $x_1, \ldots, x_{j-1}, z_i, x_{j+1}, \ldots, x_n$ à partir de $d\mathcal{A}$. On conclut en majorant l'ordre de z_i grâce à la borne de Jacobi. Pour la majoration de ${}_{\mathcal{P}}\sigma_i$, on utilise la méthode de Jacobi–Pryce. Si le déterminant tronqué est non nul, on a l'égalité. Sinon, il faut remarquer que toute dérivation supplémentaire d'une équation fait chuter (au moins) d'autant l'ordre du système. Cette majoration correspond en fait à majorer $\overset{\prec}{}_{\mathcal{P}}\sigma_i$ pour un ordre $\prec$ respectant l'ordre de Jacobi ${}^{\mathrm{J}}\mathrm{ord}x_j^{(\ell)} := \ell - \beta_j$. On peut obtenir des résultats semblables pour tous les ordres de ce type, dont ceux respectant l'ordre de dérivation standard.

4. Index d'une composante singulière quasi régulière

Notre approche repose sur une préparation à la Ritt [15, II 17 p. 63]. On considère une composante singulière quasi-régulière $\mathcal{P}$ de f ; il existera donc une composante régulière $\mathcal{Q}$, dont l'ensemble caractéristique réduit $\mathcal{B}$ (pour un ordre de Jacobi, afin de faciliter le calcul) sera dans $\mathcal{P}$. Soit $\mathcal{A}$ un ensemble caractéristique de $\mathcal{P}$ pour le même ordre. Les éléments B_i de $\mathcal{B}$ seront réécrits

20. Il est à noter que les multi-index minimaux ne sont pas nécessairement uniques. Ceci est sans inconvénient en pratique, l'essentiel étant de disposer des bornes *a priori* les plus fines pour les calculs.

21. Ce résultat est à rapprocher des résultats obtenus par Jacobi pour le calcul des résolvantes, qui consituent naturellement les cas extrêmes.

22. Dans le cas où les multi index ne sont pas unique, un seul peut naturellement être préservé.

sous la forme de polynômes en les éléments A_i de $\mathcal{A}$, dont les coefficients sont irréductibles par $\mathcal{A}$ et où les A_i apparaissent linéairement. On en déduit un système équivalent à $\mathcal{B}$ et de la forme $C_i(x)A_i + R_i(x, A) = 0$, $C_i \notin \mathcal{P}$. Un tel système peut être obtenu en dérivant les f_i un nombre de fois qui correspondà l'index du système linéarisé df dans $\Omega_{k\{x\}/k} \otimes_k K/k$ où K/k est l'extension associéeà $\mathcal{P}$, qui s'obtient donc par la méthode vue précédement. On peut maintenant trouver des combinaisons linéaires L_i $1 \leq i \leq s \leq n$ des A_i et extraire de ce système des équations $L_i + S_i(x, L)$, $1 \leq i \leq s$ où les S_i ne contiennent que des termes de degré au moins 2. Sinon, $\mathcal{P}$ ne serait pas une composante isolée, mais serait incluse dans les singularités de $\mathcal{Q}$. Soit e l'ordre maximal des S_i (borné dans le pire des cas par la borne de Jacobi de f). Pour faire court, nous illustrerons l'idée finale sur un exemple : ${x^{(e)}}^2 = x$. D'ordinaire, on calcule un développement en série en exprimant les termes de degré maximal en fonction des termes de plus bas degré. Mais pour cette équation, il faut exprimer x comme ${x^{(e)}}^2$. La question posée est d'étudier une solution en série dont les premier termes sont nuls et de savoir jusqu'où pousser le développemnt pour que tous le soient. Supposons que l'on aille jusqu'à l'ordre e'. Le developpement de ${x^{(e)}}^2$ est alors nul jusqu'à l'ordre $2(e' - e)$. Si donc $e' > 2e$, le nombre de termes nuls augmente. Il suffit donc d'aller jusqu'à l'ordre $2e + 1$ pour discerner la solution singulière nulle des solutions de la composante régulière. On peut généraliser cette idée pour obtenir une majoration de l'index de forme normale de toute composante singulière quasi régulière : il faut dériver les équations obtenues ci-dessus au plus $2e + 1$ fois, qui s'ajoutentà l'index du linéarisé, pour séparer les solutions de $\mathcal{P}$ et celles de $\mathcal{Q}$. On obtient ainsi une majoration de l'index de forme normale de $\mathcal{P}$ et une majoration de l'index local de $\mathcal{Q}$ en $\mathcal{P}$, défini comme suit.

Définition 6. — Soit $\mathcal{I}$ un idéal premier de $k\{x\}$ (non nécessairement différentiel), on définit un processus de pseudo-réduction local en $\mathcal{I}$ en s'interdisant de multiplier par un initial ou un séparant appartenantà $\sqrt{\mathcal{I} + \mathcal{P}}$. Pour celà, on s'inspire de Denef et Lipschitz [3] [23] Il en résulte des notions d'ensembles autoréduits et d'ensembles caractéristiques locaux en $\mathcal{I}$ d'un idéal différentiel. L'index local en $\mathcal{I}$ de $\mathcal{P}$ est le plus petit entier ${}_{\mathcal{P}}\sigma^{[\mathcal{I}]}$ tel qu'il existe un emsemble caractéristique local $\mathcal{C}$ de $\mathcal{P}$ en $\mathcal{I}$ et un polynôme diférentiel g satisfaisant $\mathcal{C} \subset (f_i^{(\ell)} | \ell \leq {}_{\mathcal{P}}\sigma^{[\mathcal{I}]}) : g^\infty$.

Conclusion

Ces résultats sont partiels, dans la mesure où ils se limitent au cas quasi régulier. Toutefois, cela couvre l'essentiel des exemples pratiques. Le cas général du calcul de l'inverse d'une composante singulière n'est pas immédiat. Cela reviendraitàrésoudre le difficile problème de Ritt : décider l'inclusion de deux idéaux premiers définis par leurs ensembles caractéristiques. Nous ne savons pour l'instant caractériser que les composantes singulières quasi régulières. Denef et Lipschitz on montré que l'existence d'une solution en série est décidable (uniquement pour un système d'EDO), mais qu'on ne peut pas décider l'existence d'une solution n'annulant pas un polynôme donné [3] [24]. Il faut donc limiter nos ambitions et le cas quasi régulier semble un bon cadre. Les majorations de l'index sont directement utiles pour étudier la complexité des calculs d'ensembles caractéristique, mais aussi celles des algorithmes de résolutions inspirées de la méthode TERA [1]. Une dernière notion redoutable, *l'index de base*, qui est le nombre de dérivations des polynômes de f nécessaires pour calculer une *base* Σ d'une composante $\mathcal{P}$ de f, c'est-à-dire un ensemble tel que $\mathcal{P} = \{\Sigma\}$.

[1] D'Alfonso (Lisi), Jeronimo (Gabriela) and Solernó (Pablo), « On the complexity of the resolvent representation of some prime differential ideals », *Journal of Complexity*, **22**, (3), 2006, 396–430.

[2] Lisi D'Alfonso, Gabriela Jeronimo, Gustavo Massaccesi, Pablo Solernó *On the Index and the Order of Quasi-regular Implicit Systems of Differential Equations*, *Linear algebra and its applications*, **430**, (8–9), Elsevier, 2009, 2102–2122.

23. Si les coefficients des termes de tête sont dans $\mathcal{I}$, on peut recourir aux termes suivants. Ainsi, le coefficient de tête est un polynôme en l'ordre de dérivation. Par exemple avec $\mathcal{P} := [{x''}^3 - x] : {x''}^\infty$, on obtient en dérivant 2 fois $x''x^{(4)} + 2{x^{(3)}}^2 - 1$, le terme de tête en gris est nul modulo $\mathcal{P} + (x'')$. Les termes suivants seront de la forme $x''x^{(\ell+2)} + \ell x^{(3)} x^{(\ell+1)} + \cdots$.

24. Le système $t' = 1, tx' = ax, a' = 0$ en (t) ne possède de solution $x(t)$ non nulle que si a est entier ; avec plusieurs systèmes de ce type, on construit un système diophantien. Notons que ce système n'est pas quasi régulier pour a entier.

[3] Denef (Jan) et Lipschitz (Leonard), « Power series solution of algebraic differential equations », *Math. Ann.*, **267**, 213–238, 1984.

[4] Jacobi (Carl Gustav Jacob), « Looking for the order of a system of arbitrary ordinary differential equations », *AAECC* **20**, (1), 7–32, 2009.

[5] Jacobi (Carl Gustav Jacob), « The reduction to normal form of a non-normal system of differential equations », *AAECC* **20**, (1), 33–64, 2009.

[6] Houtain (Louis), « Des solutions singulières des équations différentielles », *Annales des universités de Belgique*, années 1851–1854, 973–1323.

[7] Johnson (Joseph), « Köhler Differentials and Differential Algebra », *The Annals of Mathematics*, 2nd Ser., Vol. 89, No. 1 (Jan., 1969), 92–98.

[8] Johnson (Joseph), « Systems of n partial differential equations in n unknown functions : the conjecture of M. Janet », *Trans. of the AMS*, vol. 242, Aug. 1978.

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

[10] Kondratieva (Marina Vladimirovna), Mikhalev (Aleksandr Vasil'evich), Pankratiev (Evgeniĭ Vasil'evich), « La borne de Jacobi pour des systèmes d'équations polynomiales » (en russe), Algebra. — M. : Moscow University publications, 79–85, 1982.

[11] Kondratieva (Marina Vladimirovna), Mikhalev (Aleksandr Vasil'evich), Pankratiev (Evgeniĭ Vasil'evich), « Jacobi's bound for independent systems of algebraic partial differential equations », *AAECC*, **20**, (1), 65–71, 2009.

[12] Ollivier (François) and Sadik (Brahim), « La borne de Jacobi pour une diffiété définie par un système quasi régulier », *Comptes rendus Mathématique*, **345**, 3, 2007, 139–144.

[13] Ollivier (François), « Jacobi's Bound and Normal Forms Computations », *Differential Algebra and Related Topics*, Li Guo et William Y. Sit éd., World Scientific, Singapour, à paraître en 2010.

[14] Pryce (John D.), « A simple structural analysis method for DAEs », *BIT*, **41**, (2), 364–394, 2001.

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

26. Décodage adaptatif pour les systèmes multimodulaires redondants

Clément Pernet (LIG, Grenoble)

Dans le contexte de calcul distribué sur ressources non-sûres (architectures de calcul globales, pair à pair, ...), des nœuds de calculs malicieux peuvent engendrer des erreurs de type byzantine qu'il faut être capable de détecter et corriger pour assurer la sécurité et la fiabilité d'un calcul par des algorithmes tolérants aux pannes (ABFT : algorithm based fault tolerance). Dans le domaine du calculs exact (dans les anneaux des entiers ou de polynômes à coefficients dans un corps), la parallélisation repose fortement sur l'algorithme des restes chinois où chaque calcul modulaire est une tâche indépendante. En ajoutant quelques calculs modulaires supplémentaires, les codes arithmétiques introduisent une redondance permettant de reconstruire le résultat, malgré des erreurs non localisées dans certains des calculs modulaires. Ces codes peuvent être présentés de manière unifiée pour les systèmes de résidus redondants sur les polynômes et les entiers, et généralisant les codes de Reed-Solomon. Nous présenterons plusieurs variantes de l'application de l'algorithme d'Euclide étendu, rendant le taux de correction adaptatif. Différents critères de terminaison permettent l'utilisation de ces codes sans connaissance a priori de leur paramètres et par conséquent de décoder au mieux avec la redondance disponible. Ils permettent en outre de combiner la tolérance aux pannes avec les approches de terminaison anticipée.

27. Réseaux de Pétri stochastiques

Michel Petitot (LIFL, Universitè de Lille I)

Travail en commun avec S. Vidal

Les réseaux de Pétri sont utilisés dans de nombreux domaines : programmation concurrente, sûreté de fonctionnement, architectures clients–serveurs, conduite d'atelier, réseaux de régulation de

gènes etc. On peut les décrire par des graphes *bipartis* mais il m'a semblé plus intuitif pour l'utilisateur de les voir comme des *systèmes de réactions chimiques*. Si l'on veut étudier les performances d'un réseau de Pétri, il convient d'introduire une *temporisation* des transitions. Ce point est délicat et il existe plusieurs solutions non équivalentes dans la littérature. Pour l'application visée, principalement la modélisation des réseaux de régulation de gènes, la temporisation stochastique retenue est basée sur la loi exponentielle. Techniquement, elle est obtenue en transformant tout réseau de Pétri en une chaîne de Markov en temps continu admettant le même espace d'état. Pour cela, il suffit de définir une *constante cinétique* pour chaque réaction chimique, ce qui est tout à fait naturel pour les chimistes : ils le font déjà pour obtenir un modèle déterministe en utilisant la *loi d'action de masse*. Un tel réseau de Pétri temporisé est dit *stochastique*. L'étude des chaînes de Markov nous amène à revisiter certaines techniques mathématiques utilisées en physique quantique, en particulier l'usage des séries génératrices (en plusieurs variables commutatives) et des propagateurs. On utilise des expressions comme *équation de Schrödinger*, *hamiltonien*, *propagateur* etc. bien que l'on soit très loin de la phylosophie de la physique quantique et de la dualité onde–corpuscule. Par contre, au niveau mathématique, l'analogie est particulièrement frappante. Dans ce travail préliminaire, nous étudions les techniques du calcul symbolique (séries formelles, calcul non commutatif dans les algèbres d'opérateurs etc.) en vue de produire du code numérique efficace pour calculer l'évolution, au cours du temps t, des moments (moyenne, variance, covariance etc.) associés à la variable aléatoire $N(t)$. Cette variable

$$N(t) := (N_1(t), N_2(t), \ldots, N_n(t))$$

compte le nombre de molécules des différentes espèces chimiques présentes à l'instant $t \in \mathbb{R}$. Pour les systèmes complexes, les ingénieurs se limitent le plus souvent à exécuter des simulations, dites Monte–Carlo, car celles–ci sont basées sur l'utilisation de générateurs de nombres aléatoires. Cette méthode est mal adaptée, en particulier dans l'étude des événements qui se produisent avec une faible probabilité. Les simulations Monte–Carlo doivent alors être répétées un si grand nombre de fois que le temps de calcul en devient rédhibitoire. La méthode *mixte* proposée ici (symbolique, numérique) résoud cette question en permettant de traiter correctement les événements rares. Le calcul symbolique est effectué dans l'algèbre de Weyl à n variables. On traitera en détail deux exemples issus de la modélisation des réseaux de régulation de gènes.

– **Gène non régulé** La transcription du gène produit des ARN messagers, lesquels sont traduits en protéines, ce qui donne le modèle :

$$\begin{array}{rcll} \text{gène} & \xrightarrow{\lambda_1} & \text{gène} + \text{ARNm} & \text{(transcription)} \quad [1] \\ \text{ARNm} & \xrightarrow{\lambda_1} & \text{ARNm} + \text{protéine} & \text{(traduction)} \quad [2] \\ \text{ARNm} & \xrightarrow{\mu_1} & \emptyset & \text{(dégradation ARNm)} \quad [3] \\ \text{protéine} & \xrightarrow{\mu_2} & \emptyset & \text{(dégradation protéines)} \quad [4] \end{array}$$

– **Gène non régulé** Une protéine peut venir se fixer sur le gène (l'expression du gène est alors bloquée), ce qui revient à compléter le modèle précédent, en ajoutant les deux règles :

$$\begin{array}{rcll} \text{gène} + \text{protéine} & \xrightarrow{c_1} & \text{gène\_bloqué} & \text{(inhibition)} \quad [5] \\ \text{gène\_bloqué} & \xrightarrow{c_2} & \text{gène} + \text{protéine} & \text{(dé-inhibition)} \quad [6] \end{array}$$

28. Composition modulaire multivariée et applications.

Adrien Poteaux (Institute of Applied Geometry Inz, Austria)

Dans cet exposé nous nous intéressons au problème de composition modulaire et ses applications : Soit R un anneau commutatif de caractéristique $p > 0$, et notons $\underline{X} = X_1, \cdots, X_m$ et $\underline{Y} = Y_1, \cdots, Y_s$. Étant donné un polynôme $f \in R[\underline{X}]$ ayant pour degré en X_i au plus $e_i - 1$, un ensemble triangulaire $T = (T_1, \cdots, T_s)$ avec $d_i = \deg_{Y_i}(T_i)$, et des polynôme s $g_1(\underline{Y}), \cdots, g_m(\underline{Y})$ dans $R[\underline{Y}]$ ayant pour degré en Y_i au plus $d_i - 1$, calculer $f(g_1(\underline{Y}), \cdots, g_m(\underline{Y})) \mod < T >$. Ce problème est une généralisation de celui étudié par Kedlaya et Umans [1], qui correspond au cas où $s = 1$ et $e_1 = \cdots = e_m$. Notons $\delta_T = d_1 \cdots d_s$, $\delta_f = e_1 \cdots e_m$ et $\sigma_f = e_1 + \cdots + e_m$. Nous décrirons un algorithme qui, pour tout ϵ, si l'on a accès à $\delta_T \delta_f^{\epsilon}$ éléments de R dont les différences sont des unités, permet de résoudre ce problème dans une complexité $O_{\text{bit}}((\delta_f + \delta_T)^{1+\epsilon} \log^{1+o(1)} q)$, avec

δ_f, δ_T suffisamment grands, et sous l'hypothèse $\sigma_f \leq \delta_f^{\frac{1}{m}(1+o(1))}$. Obtenir une complexité quasi linéaire pour le problème de composition modulaire permet d'améliorer la complexité de nombreux problèmes. Ainsi, nous montrons qu'il est possible de résoudre le problème de projection des puissances en un temps quasi-linéaire en transposant notre algorithme de composition modulaire (toutes les étapes de ce dernier n'étant pas algébriques, l'utilisation du principe de Tellegen ne suffit pas), adaptant pour cela le travail de [1, section 7.2]. De plus, dans le cas bivarié ($m = s = 2$), nous montrons comment traiter les problèmes de composition modulaire et de projection des puissances sans aucune hypothèse sur σ_f, ce qui nous permet de considérer les problèmes déséquilibrés. En utilisant ce dernier résultat pour le problème de projection des puissances dans [2], on obtient un algorithme pour calculer modulo un ensemble triangulaire qui a une complexité quasi-linéaire en la taille de l'ensemble triangulaire. L'ensemble des algorithmes présentés dans cet exposé sont à l'heure actuelle uniquement théoriques. Ceci est un travail effectué en collaboration avec Éric Schost (University of Western Ontario).

[1] Kiran S. Kedlaya and Cristopher Umans. Fast polynomial factorization and modular compostion. Preprint, available at http ://www.cs.caltech.edu/ umans/papers/KU08-final.pdf.

[2] Cyril Pascal and Éric Schost. Change of order for bivariate triangular sets. In *ISSAC '06 : Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 277–284, New York, NY, USA, 2006. ACM.

29. Algorithmes de crible pour le calcul d'un plus court vecteur dans un réseau

Xavier Pujol (ENS Lyon, projet Arenaire)

Un réseau est un sous-groupe discret de R^n, qui peut être décrit comme l'ensemble des combinaisons linéaires entières d'une base d'au plus n vecteurs. Le problème du plus court vecteur (SVP) consiste à calculer un plus court vecteur non nul d'un réseau à partir d'une base de ce réseau. Ce problème est difficile, plus précisément NP-complet sous des réductions randomisées, et a de nombreuses applications en mathématiques et en informatique. En particulier, plusieurs primitives cryptographiques sont fondées sur la difficulté de résoudre SVP. Il existe aujourd'hui trois approches pour résoudre SVP. La première consiste à faire une recherche exhaustive de la solution, mais elle a un coût superexponentiel. La seconde est constituée des algorithmes de crible, non déterministes mais dont la complexité est simplement exponentielle. La dernière est basée sur le calcul de la cellule de Voronoï du réseau, son coût est exponentiel également mais elle ne semble pas utilisable en pratique. Le but de cet exposé est de présenter une amélioration de l'analyse des algorithmes de crible obtenues conjointement avec Damien Stehlé. Nous commencerons par décrire sommairement les différentes familles de méthode, en se concentrant sur les algorithmes de crible, en particulier AKS et ListSieve. Enfin, nous présenterons notre amélioration de l'analyse, reposant sur le paradoxe des anniversaires.

30. Implicit Factoring with Shared Most Significant and Middle Bits

Guènaël Renault (Équipe-projet INRIA / LIP6 Salsa)

Joint work with Jean-Charles Faugère, Raphael Marinier.

We study the problem of integer factoring given *implicit* information of a special kind. The problem is as follows : let $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$ be two RSA moduli of same bit-size, where q_1, q_2 are α-bit primes. We are given the *implicit* information that p_1 and p_2 share t most significant bits. We present a novel and rigorous lattice-based method that leads to the factorization of N_1 and N_2 in polynomial time as soon as $t \geq 2\alpha + 3$. Subsequently, we heuristically generalize the method to k RSA moduli $N_i = p_i q_i$ where the p_i's all share t most significant bits (MSBs) and obtain an improved bound on t that converges to $t \geq \alpha + 3.55\ldots$ as k tends to infinity. We study also the case where the k factors p_i's share t contiguous bits in the middle and find a bound that converges to $2\alpha + 3$ when k tends to infinity. This paper extends the work of May and Ritzenhofen, where similar results were obtained when the p_i's share least significant bits (LSBs). Sarkar and Maitra described an alternative but heuristic method for only two RSA moduli, when the p_i's share LSBs and/or MSBs, or bits in the middle. In the case of shared MSBs or bits in the middle and two RSA moduli, they get better experimental results in some cases, but we use much lower (at least 23

times lower) lattice dimensions and so we obtain a great speedup (at least 10^3 faster). Our results rely on the following surprisingly simple algebraic relation in which the shared MSBs of p_1 and p_2 cancel out : $q_1N_2 - q_2N_1 = q_1q_2(p_2 - p_1)$. This relation allows us to build a lattice whose shortest vector yields the factorization of the N_i's.

31. Sous-résultants et doubles sommes de Sylvester

Marie-Françoise Roy (IRMAR, Université Rennes 1)

Les sous-résultants sont définis par les coefficients de deux polynômes et les doubles sommes de Sylvester par leurs ensembles de racines. Sylvester avait indiqué que ces deux notions sont étroitement liées. Dans ce travail en collaboration avec Aviva Szpirglas nous établissons très simplement les liens entre doubles sommes de Sylvester et sous-résultants qui avaient été étudiés par plusieurs auteurs.

32. Algorithmique "diviser-pour-régner" pour le calcul de cartes routières

Mohab Safey El Din (Équipe-projet INRIA / LIP6 Salsa)

On considère un ensemble semi-algébrique $S \subset \Re^n$ et un couple de points (p, q) dans S. On cherche à répondre aux questions suivantes :

- Les points p et q vivent-ils dans une même composante connexe de S ?
- Si oui, comment exhiber un chemin les reliant ?

Les motivations applicatives de ces questions proviennent de la planification de trajectoires en robotique ; les motivations algorithmiques sont fondamentales en géométrie algébrique réelle effective car les algorithmes permettant de répondre à ces questions sont à la base d'algorithmes permettant de décrire les composantes connexes de S. En 1988, John Canny introduit la notion de carte routière, permettant de réduire ces questions de connectivité au cas de la dimension 1. Il s'agit d'une courbe algébrique ayant une intersection non vide et connexe avec chaque composante connexe du semi-algébrique considéré. Si S est défini par un système de s polynômes de degré borné par D, l'algorithme probabiliste de Canny, ainsi que ses généralisations déterministes obtenues notamment par Basu, Pollack et Roy, est de complexité polynomiale en $(sD^n)^n$. Avec Éric Schost, nous avons étendu cette notion de carte routière (en leur permettant d'être de dimension supérieure à 1) dans le cas des variétés algébriques réelles lisses et compactes. Étant donnée une variété algébrique réelle V compacte, lisse, de dimension d, cette liberté permet d'obtenir un résultat de connectivité plus puissant que celui qui est à la base des algorithmes précédents : il offre la possibilité de construire des cartes routières intermédiaires de dimension inférieure à $d-1$ strictement. Une récursion doit ainsi être effectuée sur les composantes de cette carte routière. Le contrôle de ces dimensions intermédiaires est à la base d'une algorithmique diviser-pour-régner. Dans le cas des hypersurfaces lisses et compactes, nous avons obtenu, avec Éric Schost, un premier algorithme probabiliste de type "pas de bébé/pas de géant" de complexité polynomiale en $(nD^n)^{\sqrt{n}}$. J'exposerais les récentes améliorations de ce résultat que nous avons obtenus. Celles-ci passent par des résultats de lissité sur les variétés polaires (obtenus avec B. Bank, M. Giusti J. Heintz et É. Schost) et la mise en place d'une stratégie diviser-pour régner au problème de calcul de cartes routières. L'objectif est d'obtenir une complexité polynomiale en $(nD^n)^{\log(d)}$ où d est la dimension de la variété étudiée. Si le temps le permet, on présentera aussi des travaux en cours, communs avec S. Basu, M.-F. Roy et É. Schost qui visent à rendre déterministe l'algorithme de type "pas de bébé/pas de géant" tout en le généralisant au cas des variétés algébriques réelles non lisses et non compactes. Cet exposé présente des résultats publiés dans *A baby steps/giant steps Monte Carlo algorithm for computing roadmaps in smooth compact real hypersurfaces, M. Safey El Din, E. Schost Discrete and Computational Geometry, 2010.* Il utilise des résultats montrés dans *On the geometry of polar varieties, B. Bank, M. Giusti, J. Heintz, M. Safey El Din, E. Schost Applicable Algebra in Engineering, Communication and Computing, 21(1) : 33-83, 2010.*

Travaux en commun avec : E. Schost d'un part, et S. Basu, M.-F. Roy et E. Schost d'autre part.

33. Résolution relaxée d'un système d'équations et application dans le domaine de la robotique

Jan Sliwka (ENSIETA)

Mots-clés : Arithmétique d'intervalles, Robotique

1. Introduction

Soit la fonction **f**

$$\begin{array}{l} \mathbb{R}^n \to \mathbb{R}^m \\ \mathbf{x} \mapsto \mathbf{f}(\mathbf{x}) = \begin{pmatrix} f_1(\mathbf{x}) \\ f_2(\mathbf{x}) \\ ... \\ f_m(\mathbf{x}) \end{pmatrix} \end{array} \tag{3}$$

Definition 1. *La résolution q-relaxée d'un système d'équations*

$$\begin{cases} f_1(\mathbf{x}) = 0 \\ f_2(\mathbf{x}) = 0 \\ ... \\ f_m(\mathbf{x}) = 0 \end{cases} \quad \mathbf{x} \in \mathbb{R}^n \tag{4}$$

est la solution du système où $m-q$ équations parmi m équations sont satisfaites i.e.

$$\begin{array}{c} S_q = \{x \in \mathbb{R}^n, \exists \sigma \in \mathbb{S}_m, \\ \forall i \in \{1,..,m-q\}, f_{\sigma(i)}(\mathbf{x}) = 0\} \end{array} \tag{5}$$

S_q étant l'ensemble solution et $\mathbb{S}_m$ étant le groupe des permutations dans $\{1,..,m\}$.

Dans l'exposé, je commencerai par présenter une formalisation mathématique du problème. Ensuite je parlerai de la résolution de ce système en utilisant des méthodes ensemblistes [2]. Finalement, je montrerai un exemple d'application concret dans la robotique.

2. La formalisation du problème en utilisant les polynômes symétriques

2.1. Polynômes symétriques

ϕ est un polynôme symétrique si pour toute permutation σ de $\{1,..,n\}$ on a $\phi(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}) = \phi(X_1, X_2, \ldots, X_n)$ .Par exemple $X_1X_2 + X_1X_3 + X_2X_3$ est symétrique. Dans notre cas nous utiliserons les polynômes symétriques élémentaires défini par

$$\phi_k(X_1,..X_n) = \sum_{1 \le i_0 < ... < i_k \le n} X_{i_1} X_{i_2} ... X_{i_k} \tag{6}$$

par exemple

$$\begin{array}{l} \phi_0(X_1,..,X_3) = X_1 + X_2 + X_3 \\ \phi_1(X_1,..,X_3) = X_1X_2 + X_1X_3 + X_2X_3 \\ \phi_2(X_1,..,X_3) = X_1X_2X_3 \end{array} \tag{7}$$

Proposition 1. *Si pour $\forall i \in \{1,..,n\}, X_i \in [0,+\infty]$, Si $\phi_\kappa(X_1, X_2, .., X_n) = 0$ alors $n-\kappa$ variables parmi $X_1, ..., X_n$ sont égaux à zero .*

Ce qui veut dire aussi que κ variables parmi $X_1, ..., X_n$ peuvent ne pas être égaux à zero. Cette propriété est importante car elle nous permet de traiter le problème de la résolution q-relaxée d'un système d'équations.

2.2 Formalisation

En utilisant la proposition (1) on déduit que la résolution q-relaxée du système (4) reviens à

résoudre le système

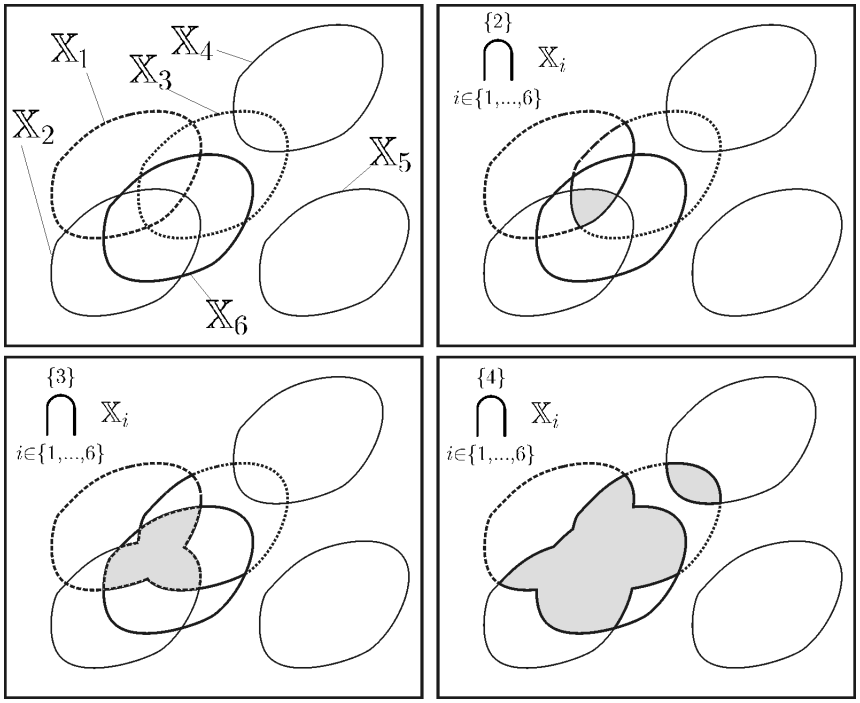
$$\begin{cases} f_1(\mathbf{x}) = z_1 \\ f_2(\mathbf{x}) = z_2 \\ \dots \\ f_m(\mathbf{x}) = z_m \\ \phi_q(\mathbf{z}) = 0 \end{cases} \quad \begin{array}{l} \mathbf{x} \in \mathbb{R}^n \\ \\ \\ \\ z = \begin{pmatrix} z_1 \\ z_2 \\ \dots \\ z_m \end{pmatrix} \in \mathbb{R}^m \end{array}$$

3. Résolution q-relaxée

3.1. L'intersection q-relaxée

Soit m ensembles $\mathbb{X}_1, \dots, \mathbb{X}_m$ de $\mathbb{R}^n$. L'intersection q-relaxée notée par $\bigcap^{\{q\}} \mathbb{X}_i$ est l'ensemble de tous les $\mathbf{x} \in \mathbb{R}^n$ qui appartiennent à tous les $\mathbb{X}_i$, excepté q au plus. La figure ci-dessous montre ce concept pour $m = 6$ et $q = 2, 3, 4$. Dans cet exemple nous avons :

$$\bigcap^{\{0\}} \mathbb{X}_i = \bigcap^{\{1\}} \mathbb{X}_i = \emptyset, \ \bigcap^{\{5\}} \mathbb{X}_i = \bigcup \mathbb{X}_i \text{ et } \bigcap^{\{6\}} \mathbb{X}_i = \mathbb{R}^2. \tag{8}$$



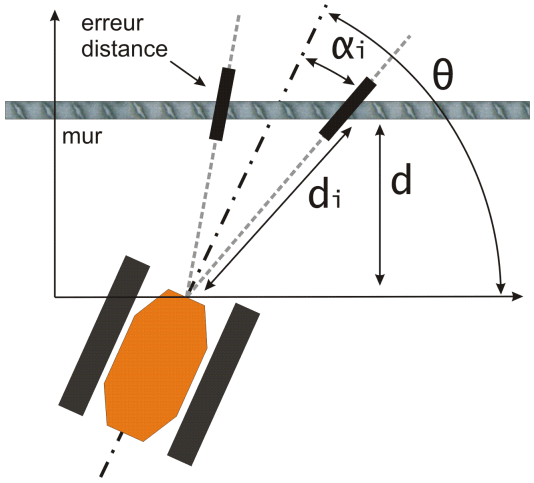
De la même manière, dans le contexte de l'estimation d'ensembles, nous pouvons définir l'ensemble q relaxé des solutions comme

$$\mathbb{P}^{\{q\}} \stackrel{\text{def}}{=} \bigcap_{i\in\{1,\dots,m\}}^{\{q\}} \{\mathbf{x} \in \mathbb{R}^n, f_i(\mathbf{x}) = 0\}. \tag{9}$$

$\mathbb{P}^{\{q\}}$ peut être facilement caractérisé en utilisant l'analyse par intervalle.(inversion ensembliste [3][1])

4. Exemple traité

Chaque année notre école participe à un concours de robotique sous-marine appelé SAUCE (Student Autonomous Underwater Challenge Europe). Le but est de construire un petit robot sous-marin intelligent capable d'effectuer les missions du concours en toute autonomie. Pour effectuer les missions, nous sommes souvent confrontés à des problèmes de localisation.



Dans la figure ci-dessus on veut localiser le robot avec des données sonar. En effet, on veut connaître son orientation θ et la distance d par rapport au mur. Une donnée sonar i est composée d'une distance au premier obstacle (au mur) d_i avec une erreur Δd_i et *(ii)* l'angle correspondant α_i du faisceau du sonar par rapport au robot. On a pour chaque mesure correcte

$$d = d_i \cos(\theta + \alpha_i) \tag{10}$$

Si N est le nombre de mesures, résoudre ce problème revient donc à résoudre le système d'équations

$$\begin{cases} d - d_1 \cos(\theta + \alpha_1) = 0 \\ \dots \\ d - d_N \cos(\theta + \alpha_N) = 0 \end{cases} \quad \begin{array}{l} d \in \mathbb{R} \\ \theta \in \mathbb{R} \end{array} \tag{11}$$

Le sonar nous donne souvent des erreurs de distances. Pour ces mesures erronées, l'équation (10) n'est pas satisfaite. Supposant que le nombre d'erreurs ne dépasse pas q, résoudre le problème revient à résoudre le système d'équations (11) d'une manière q-relaxée.

[1] L. Jaulin, M. Kieffer, O. Didrit, and E. Walter. *Applied Interval Analysis, with Examples in Parameter and State Estimation, Robust Control and Robotics*. Springer-Verlag, London, 2001.

[2] R. E. Moore. *Methods and Applications of Interval Analysis*. SIAM, Philadelphia, PA, 1979.

[3] E. Walter and L. Pronzato. *Identification of Parametric Models from Experimental Data*. Springer-Verlag, London, UK, 1997.

34. Systèmes Bilinéaires et Variétés Déterminantielles : Algorithmes, Complexité et Applications.

Pierre-Jean Spaenlehauer (UPMC, Univ Paris 06, LIP6 ; INRIA, Paris-Rocquencourt Center, SALSA)

Travail commun avec Jean-Charles Faugère et Mohab Safey El Din

Keywords: MinRank, bases de Grőbner, algorithme F_5, FGLM, cryptanalyse algébrique.

Dans cet exposé, nous nous intéressons à un problème fondamental d'algèbre linéaire : le problème *MinRank*. Étant donnés un corps $\mathbb{K}$, un entier r et une matrice linéaire M de taille $m \times n$ (avec $m \leq n$) sur $\mathbb{K}[x_1, \dots, x_k]$ (i.e. une matrice dont les entrées sont des polynômes affines de degré 1 en k variables), l'objectif est de trouver l'ensemble des points tels que l'évaluation de M est de rang inférieur ou égal à r. Ce problème est prouvé NP-dur quand $\mathbb{K}$ est un corps fini [3] et il est relié à des applications dans des domaines variés : en cryptologie (sécurité des systèmes multivariés [8, 5, 11]), en théorie des codes (décodage en métrique rang [12]), en géométrie (calcul de points critiques de projections [1]), ... Nous nous concentrons sur deux modélisations du problème MinRank par des systèmes algébriques multivariés. La première modélisation, proposée par Kipnis et Shamir dans le cadre de la cryptanalyse du système HFE, fait apparaître un système *bilinéaire* en introduisant

$n-r$ vecteurs indépendants du noyau de M dont les coefficients sont des indéterminées [11, 8]. La seconde modélisation est donnée par le système constitué de l'ensemble des mineurs de taille $r+1$ de la matrice M (ces mineurs s'annulent sur les solutions du problème MinRank). Ces systèmes sont ensuite résolus en calculant une base de Gröbner pour l'ordre du degré lexicographique inversé à l'aide de l'algorithme F_5 [6] puis en utilisant un algorithme efficace de changement d'ordre (par exemple FGLM [7] si l'idéal est 0-dimensionnel). Notre objectif est d'étudier et d'exploiter les propriétés algébriques de ces modélisations pour en améliorer la résolution. Ceci passe par l'obtention de bornes fines sur la régularité et le degré des idéaux étudiés. Pour étudier la modélisation de Kipnis-Shamir, nous avons besoin de nouveaux résultats théoriques et pratiques sur la résolution des systèmes bilinéaires. En particulier, nous prouvons une forme explicite de la série de Hilbert des idéaux engendré par des systèmes bilinéaires génériques, ainsi qu'une borne (atteinte sous une hypothèse de généricité) sur le degré de régularité des systèmes bilinéaires affines : pour un système de $n_x + n_y$ équations bilinéaires affines génériques sur $\mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$,

$$\mathsf{d}_{\mathsf{reg}} \leq \min(n_x, n_y) + 1$$

Une conséquence directe de ce résultat est une nouvelle borne sur la complexité de résolution des systèmes bilinéaires affines par des algorithmes de calcul de bases de Gröbner. Nous proposons également une variante dédiée aux systèmes multihomogènes de l'algorithme F_5 qui exploite la structure des matrices de Macaulay pour améliorer la complexité. Dans le cas bilinéaire (i.e. bihomogène de bidegré $(1,1)$), une extension du critère F_5 est proposée, et permet d'éviter toutes les réductions à 0 dans le cas générique. En effet, les syzygies dûes à la structure du système proviennent du noyau de matrices jacobiennes. Par conséquent, les réductions à 0 peuvent être détectées en calculant une base de Gröbner de l'idéal engendré par les mineurs maximaux de ces matrices. Une variante d'un théorème de Sturmfels et Zelevinski [13] montre que le coût de ce calcul est négligeable par rapport au coût global du calcul de base de Gröbner, ce qui est vérifié en pratique. Du point de vue de la modélisation déterminantielle (i.e. le système constitué des mineurs de taille $r+1$ de la matrice M), nous donnons – sous une hypothèse de généricité – une forme explicite et *exacte* du degré de l'idéal engendré par les mineurs :

$$\prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

Nous prouvons également une forme explicite de sa série de Hilbert, sur laquelle on peut notamment lire le degré de régularité lorsque l'idéal est 0-dimensionnel. Les preuves font intervenir des résultats sur les idéaux engendrés par les mineurs de matrices dont les coefficients sont des indéterminées [4], ainsi que le théorème de Bertini. Ces nouvelles formules permettent d'obtenir des estimations précises de complexité asymptotique. En particulier, on montre que le problème MinRank générique peut être résolu en temps polynomial quand $n = m$ (la matrice M est carrée), $k = (n-r)^2$ est fixé et n croît : la complexité est alors bornée par $O(n^{3k})$. Cette analyse de complexité va nous guider vers une méthode efficace pour résoudre un challenge issu de la cryptologie pour lequel aucune attaque effective n'était connue jusqu'à présent [5, Challenge C].

[1] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, 21(1) :33–83, 2010.

[2] W. Bruns and U. Vetter. *Determinantal rings*. Springer, 1988.

[3] J. Buss, G. Frandsen, and J. Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3) :572–596, 1999.

[4] A. Conca and J. Herzog. On the Hilbert function of determinantal rings and their canonical module. *Proceedings of the American Mathematical Society*, pages 677–681, 1994.

[5] N. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. *Lecture notes in computer science*, pages 402–421, 2002.

[6] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, page 83. ACM, 2002.

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

[8] J.-C. Faugère, F. Levy-dit-Vehel, and L. Perret. Cryptanalysis of MinRank. In *Proceedings of the 28th Annual conference on Cryptology : Advances in Cryptology*, page 296. Springer, 2008.

[9] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology. Submitted to ISSAC, 2010.

[10] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1) : Algorithms and complexity. *arXiv :1001.4004v1 [cs.SC]*, 2010.

[11] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. *Lecture Notes in Computer Science*, pages 19–30, 1999.

[12] A. Ourivski and T. Johansson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38(3) :237–246, 2002.

[13] B. Sturmfels and A. Zelevinsky. Maximal minors and their leading terms. *Adv. Math*, 98(1) :65–112, 1993.

35. Factorisation polynomiale torique

Martin Weimann (Université de Barcelona)

Dans cet exposé, on prouve l'existence d'un algorithme de factorisation rationnelle des polynômes bivariés de complexité polynomiale en le *volume du polytope de Newton*.

La plupart des algorithmes de factorisation bivariée utilisent un schéma du type *Lifting et Recombinaison* : déduire la factorisation rationnelle de $f \in \mathbb{Q}[x,y]$ à partir de sa factorisation modulo (x^k) pour un $k \geq 0$. Dans le cas où $f(0,y)$ n'est pas réduit de degré $\deg(f)$, cette approche requiert *a priori* un changement préalable de coordonnées affines. Notre objectif est d'éviter ce changement de coordonnées pour profiter de la géométrie du polytope de Newton N_f de f. Pour cela, on va décomposer la courbe C définie par f dans une compactification torique X adéquate du plan affine. On parle d'algorithme de *factorisation torique*. Soient les hypothèses :

(H_1) Le polytope N_f contient le simplexe élémentaire.
(H_2) Les polynômes des facettes extérieures sont réduits.

Soit $2 \leq \omega < 2.35$ l'exposant de multiplication des matrices. On donnera une esquisse de preuve du résultat suivant :

Theorème 1. *Il existe un algorithme qui, étant donné $f \in \mathbb{Q}[t_1,t_2]$ qui obéit à (H_1) et (H_2), et étant donnée la factorisation des polynômes des facettes extérieures, calcule la factorisation de f avec $\mathcal{O}(\mathrm{Vol}(N_f)^\omega)$ opérations arithmétiques dans $\mathbb{Q}$.*
Exemple. Si $N_f = Conv((0,0),(2,0),(0,2),(n,n))$ avec $n >> 0$, l'algorithme rapide dense de Chèze-Lecerf requiert une facto univariée en degré $2n$ et $\mathcal{O}(n^{\omega+1})$ opérations. L'approche torique requiert deux facto univariées en degré 2 et $\mathcal{O}(n^\omega)$ opérations.
Idée de preuve. On veut factoriser f à partir des factorisations des polynômes de facettes remontées par Hensel avec une précision convenable. La traduction géométrique est la suivante. Soit X la surface torique définie par N_f. On veut décomposer la courbe $C \subset X$ définie par f connaissant la décomposition de sa restriction à un diviseur convenable D supporté à l'infini torique $X \setminus \mathbb{A}^2_{\mathbb{Q}}$.

Soit V le $\mathbb{Q}$-espace vectoriel librement engendré par les composantes irréductibles de $C \cap D$. On veut caractériser le sous-espace $W \subset V$ engendré par les restrictions à D des composantes de C. On introduit pour cela le sous-espace intermédiaire $W \subset V(D) \subset V$ engendré par les éléments de V restrictions à D de diviseurs de X.

Théorème 2. *Si $D \geq 2\,\mathrm{div}_\infty(f)$, alors $W = V(D)$.*

Dans le cas dense $X = \mathbb{P}^2$, le Théorème 2 assure que l'on peut déduire la factorisation de f de sa factorisation modulo (x^{2d}) en résolvant un système linéaire. On retrouve un théorème de Lecerf. Il reste à déterminer la matrice de $V(D) \subset V$.

Théorème 3. *On a $V(D) = \ker(A)$ pour A une matrice rationnelle explicite indexée par l'ensemble des facteurs rationnels des polynomes de facettes et par l'ensemble des points entiers intérieurs au polytope de D.*

Le Théorème 3 est conséquence d'un théorème d'extension de fibrés qui permet d'expliciter le conoyau $\mathrm{Pic}(D) \to \mathrm{Pic}(X)$. Il peut se voir comme une réciproque du théorème des résidus. Finalement, on déduit le Théorème 1 des Théorèmes 2 et 3. La complexité de l'algorithme sous-jacent se déduit essentiellement d'un théorème d'Ostrosvki $N_{f_1 f_2} = N_{f_1} + N_{f_2}$ et de l'égalité $C^2 = \mathcal{O}(\mathrm{Vol}(N_f))$. □

Si le temps le permet, on terminera par quelques problèmes ouverts, en discutant notamment le cas des polynômes de facette non réduits.

Références

• G. Chèze et G. Lecerf, *Lifting and recombination techniques for absolute factorization*, J. of Complexity 23, no. 3 (2007), pp. 380-420.

• M. Weimann, *Algebraic osculation and factorization of sparse polynomials*, arXiv : 0904.0178v1.

• M. Weimann, *A lifting and recombination algorithm for rational factorization of sparse polynomials*, arXiv :0912.0895v1.

Université Joseph-Fourier, Laboratoire Jean-Kuntzmann, BP 53 38041 Grenoble cedex, France • Jean-Guillaume.Dumas@imag.fr

UVSQ, LMV, bâtiment Fermat, 45 avenue des États-Unis, 78035 Versailles cedex, France • Gregoire.Lecerf@math.uvsq.fr

Université Rennes 1, IRMAR, Campus de Beaulieu, 35042 Rennes Cedex, France • delphine.boucher@univ-rennes1.fr

Université de Limoges, XLIM, 123 avenue Albert-Thomas, 87068 Limoges cedex, France • cluzeau@ensil.unilim.fr