JNCF '2003

Journées Nationales de Calcul Formel

20-24 Janvier 2003

Ce colloque a pour objectif de faire une photographie des travaux en calcul formel, principalement dans la communauté française. Le terme "calcul formel" s'entend au sens large, i.e. au sens d'algorithmique sur les objets mathématiques.

Le "calcul formel" est à l'heure actuelle un ensemble de disciplines qui se trouvent à cheval entre informatique (thème 2B de l'INRIA) et mathématiques, le distinguo s'effectuant généralement davantage pour des raisons historiques que proprement thématiques.

Il y a 5 à 10 ans, les personnes que nous souhaitons toucher par cette conférence s'organisaient au sein du PRC Math-Info du CNRS, qui a plus ou moins disparu sous cette forme (son "successeur", le GDR ALP, fait partie des "sponsors" de ces journées). En tant que doctorants en mathématiques ou en informatique à l'époque, nous avons le souvenir de ces journées comme d'une possibilité d'ouverture disciplinaire et de discussions entre communautés dont les objectifs sont proches mais dont les contacts sont parfois rares.

Nous espérons donc en particulier que ce congrès sera l'occasion de discuter l'organisation du calcul formel en France, et de réfléchir à sa structuration.

En outre, une session s'intéressera aux applications du calcul formel, et une session à la cryptologie. Nous espérons que ces sessions contribueront à élargir le champ d'applications du calcul formel et à sensibiliser les chercheurs aux applications potentielles de leurs travaux.

Delphine Boucher, Guillaume Hanrot, Fabrice Rouillier, Éric Schost.

Table des matières

Exposés Pléniers

Algèbre linéaire [Jean-Guillaume Dumas]

Algorithmique Géométrique [Michel Pocchiola]

Applications du calcul formel [Jean-Pierre Merlet]

Calcul Symbolique/Numérique [André Galligo]

Contrôlabilité [Michel Fliess]

Cryptologie [Nicolas Sendrier]

Équations différentielles I: résolution [Jacques-Arthur Weil]

Équations différentielles II: autres points de vue [Bruno Salvy et Jacques-Arthur Weil]

Session Ouverte []

Systèmes polynomiaux I [Jean-Charles Faugère]

Systèmes polynomiaux II [Bernard Mourrain]

Fonctions spéciales et finitude différentielle [Bruno Salvy]

Théorie algorithmique des nombres [Karim Belabas]

Annexes

Exposés Pléniers

Quelques résultats récents sur les diagrammes de Voronoi

Jean-Daniel Boissonnat
projet PRISME, INRIA Sophia-Antipolis

Les diagrammes de Voronoï affines sont bien compris. En se placant dans l'espace des sphères, leur calcul se ramène à celui d'un polytope pour lequel des algorithmes optimaux sont connus. L'analyse des diagrammes non affines est beaucoup moins avancée et pose des questions combinatoires e t algorithmiques ouvertes depuis plus de vingt ans.

Dans une première partie, l'exposé introduira les diagrammes de Moebius, qui peuvent être définis comme les diagrammes dont les faces sont sphériques. On établira différentes correspondances entre ces diagrammes, les diagrammes affines et les enveloppes convexes et les diagrammes euclidiens de sphères, ce qui conduit à des résultats combinatoires et algorithmiques.

Dans une deuxième partie, on contournera la difficulté et on montrera qu'on peut approcher le diagramme euclidien d'objets complexes en calculant le diagramme de Voronoï d'un échantillon de points pris sur ces objets.

Cryptologie, algorithmes et calcul formel

François Morain
LIX, École polytechnique

La cryptologie moderne utilise des problèmes difficiles au coeur des systèmes de chiffrement, signature, etc. Le but est ici de relier la sécurité d'un système à la difficulté de résolution d'un problème de calcul. Les exemples les plus connus sont ceux de RSA et de la factorisation d'entiers, de l'échange de clefs et du logarithme discret.

Il faut alors fabriquer des instances sûres de ces problèmes. L'exposé passera en revue quelques objets utilisés en cryptologie moderne, et de leur algorithmique associée. On s'intéressera surtout aux échanges entre ce domaine et le calcul formel.

Aspects non commutatifs de la théorie des équations différentielles : apports du calcul sur machine

Michel Petitot
LIFL,Université de Lille 1

Le calcul non commutatif est beaucoup plus agréable sur machine et pratiquement impossible à la main, ce qui explique qu'il soit peu enseigné.

- en physique quantique: on étudie des opérateurs ou des séries formelles en variables non commutatives qui sont solutions d'équations différentielles. Ces travaux anciens (Heisenberg, Feynmann etc.) sont toujours d'actualité comme le montrent des résultats plus récents en théorie des noeuds, dans la régularisation des diagrammes de Feynmann, le lien profond avec les fonctions spéciales (polylogarithmes), certaines questions d'arithmétique (Multiple Zeta Values) ou le traitement des séries divergentes.
- on montrera, sur un exemple, comment l'utilisation de dérivations (ayant un sens géométrique) qui ne commutent pas entre elles, permet une économie substantielle de calculs dans la résolution du problème posé.

Complexité de calculs sur les matrices polynomiales et entières

Gilles Villard
LIP, CNRS, ENS Lyon

Dans la mesure où l'exposant ω du produit de matrice est l'exposant de bien d'autres problèmes, on peut considérer que la complexité des calculs de base en algèbre linéaire sur un corps K abstrait est bien connue. On pense par exemple au calcul du déterminant, du rang, du polynôme caractéristique, de la matrice inverse ou de la forme de Frobenius qui se réalisent tous en $\tilde{O}(n^\omega)$ opérations dans K. Pour des domaines de coefficients plus concrets et plus intéressants en calcul exact tels que $\mathsf{K}[x]$ ou $\mathbb{Z}$, on ne connaît pas vraiment la répercussion des tailles des données sur les exposants des complexités. On a même longtemps considéré qu'un facteur n (la dimension) supplémentaire était induit par ces tailles, menant typiquement à des coûts algébriques en $\tilde{O}(n^\omega \times nd) = \tilde{O}(n^{\omega+1}d)$ ou binaires en $\tilde{O}(n^{\omega+1} \log \|A\|)$. Ici, d et $\log \|A\|$ sont le degré ou la taille des coefficients de la matrice en entrée. On sait depuis peu qu'il n'en n'est rien. Pour plusieurs problèmes sur $\mathsf{K}[x]$, le surcoût en la dimension peut même n'être que logarithmique.

Après un tour d'horizon des progrès des deux dernières années dans le domaine, nous présentons quelques résultats récents pour les matrices polynomiales. L'étude des matrices sur $\mathsf{K}[x]$ étant considérée comme préliminaire à celle des matrices sur $\mathbb{Z}$.

Les matrices polynomiales que l'on considère sont $n \times n$ de degré d. Nous nous intéressons au lien entre la complexité du produit de matrices polynomiales et celle d'autres problèmes comme le calcul d'approximants matriciels, la colonne réduction (réduction de base de modules sur $\mathsf{K}[x]$) et le calcul du déterminant. Nous montrons, en modèle *straight-line*, que de calculer le produit de matrices se réduit à calculer le terme de degré d du déterminant. Inversement les problèmes cités peuvent se résoudre en temps $\tilde{O}(n^\omega d)$, c'est-à-dire « aussi rapidement » que pour actuellement multiplier deux matrices de degré d. Ces derniers travaux ont été menés avec P. Giorgi et C.P. Jeannerod (Lip).

Une question se soulève naturellement. Si $\mathsf{MM}(n,d)$ est le coût du produit de deux matrices de degré d, quels sont les problèmes qui peuvent se résoudre en $\tilde{O}(\mathsf{MM}(n,d))$ opérations dans K ou « à peu près »? L'analogue binaire étant: quels sont les problèmes qui peuvent se résoudre en $\tilde{O}(\mathsf{MM}(n, \log \|A\|))$ opérations binaires ou « à peu près »?

De Rouché à Newton : application à l'existence et au calcul des racines multiples d'un système d'équations

Jean-Claude Yakoubsohn
MIP, Université Paul Sabatier, Toulouse

Ce travail est le fruit d'une collaboration avec Marc Giusti, Grégoire Lecerf et Bruno Salvy. Dans une premièr temps, cet exopsé présente des résultats nouveaux concernant l'existence d'une grappe de racine pour des systèmes d'équations algébriques.

Ensuite on présentera un algorithme pour approcher quadratiquement cette grappe de racines.

Références Bibliographiques.

- J.-P. Dedieu, M. Shub, On Simple Double Zeros and Badly Conditioned Zeros of Analytic Functions of n Variables. Mathematics of Computation, 70 (2001) 319-327.
- J.-P. Dedieu, Newton's method and some complexity aspects of the zero finding problem. Proceedings of the "FoCM Conference, Oxford, 1999". Cambridge University Press. 2001.
- J.C. Yakoubsohn, Finding cluster of zeros of univariate polynomial. Complexity theory, real machi nes and homotopy (Oxford, 1999), Journal of complexity, 16, (2000), 3, 603-638.

Symposium

Algèbre linéaire

Organisation : Jean-Guillaume Dumas - Université Joseph Fourier, Grenoble

Présentation

En calcul formel comme en calcul numérique, l'algèbre linéaire est souvent un point majeur pour la résolution efficace des problèmes. Ces quinze dernières années, les progrès non négligeables des machines et considérables de l'algorithmique formelle ont permis au domaine de devenir abordable en pratique. En effet, en calcul numérique, le modèle algébrique de complexité associé à l'étude de la stabilité et à une utilisation optimale des différentes ressources réelles des machines permet souvent de conclure sur l'efficacité d'une méthode. Différemment, en calcul formel, si la stabilité des algorithmes n'est plus un problème, les coefficients des matrices appartiennent à des domaines a priori moins naturels à manipuler de manière pratique: il s'agit par exemple des entiers, de corps ou de groupes finis, d'anneaux de polynômes, etc. Tout d'abord, il apparaît qu'il peut être tout aussi rapide de calculer des routines de bases d'algèbre linéaire avec une arithmétique numérique qu'avec une arithmétique exacte simple (par exemple sur des corps finis). Ensuite, et plus étonnamment sans doute, il s'avère que les complexités binaires de nombreux problèmes (par exemple le déterminant de matrices polynomiales) peuvent n'être qu'à un facteur poly-logarithmique des complexités algébriques (i.e. le surcoût dû au grossissement des coefficients peut n'être que logarithmique en la taille des entrées) ! Enfin, des approches probabilistes et même heuristiques sont combinées aux algorithmes déterministes classiques par des techniques algorithmiques de haut-niveau dans une floraison de bibliothèques de programmes dédiés afin de permettre une utilisation efficace de ces objets complexes.

Cette session aborde une bonne partie de ces aspects et des nouvelles questions qui en découlent, tout comme l'application efficace de ces techniques sur plusieurs problèmes précis. Pour l'algèbre linéaire "pure" tout d'abord, Jounaïdi Abdeljaoued étudie le problème du calcul uniforme du rang et un algorithme quasi-optimal pour l'inversion de matrices polynomiales est proposé par Claude-Pierre Jeannerod. Ensuite, le côté algorithmique est présenté par Pascal Giorgi à travers la conception de la bibliothèque LinBox et la résolution de plusieurs problèmes théoriques posés par une implantation à la fois générique (réutilisation de code, modularité) et efficace. Luis M. Pardo, de son côté, effectue une comparaison entre les complexités de l'analyse numérique et du calcul symbolique de problèmes d'algèbre linéaire intervenant dans la résolution de systèmes polynomiaux multivariés, linéaires ou non. Enfin, l'utilisation d'algèbre linéaire exacte pour la topologie algébrique est détaillée par Philippe Elbaz-Vincent pour des calculs de groupes de cohomologies qui pouvaient être jusqu'alors hors d'atteinte.

Résolution uniforme des systèmes linéaires

Jounaïdi Abdeljaoued
École Supérieure de Sciences Techniques de Tunisie

Il s'agit de résoudre de manière uniforme le problème du rang, de la compatibilité d'un système de n équations linéaires à p inconnues sur un corps quelconque (on traitera plus particulièrement le cas réel ou complexe pour comprendre ce qui se passe) et de donner la solution du système à l'aide de formules généralisant les formules de Cramer. On utilise pour cela une extension de l'algorithme de Mulmuley (1987) pour le calcul du rang d'une matrice et on fait appel aux coefficients de Gram généralisés qui permettent de montrer que l'on arrive à contrôler le rang à l'aide de la somme des carrés d'un "petit nombre" de mineurs de la matrice du système.

Calculs effectifs en cohomologies arithmétiques

Philippe Elbaz-Vincent
Institut de Mathématiques et Modélisation de Montpellier (I3M)

Nous présenterons une approche raisonnablement effective pour le calcul des groupes de cohomologies (et d'homologies) de $GL_N(\mathbb{Z})$ et $SL_N(\mathbb{Z})$ (pour $N = 5{,}6$, les cas $N \leqslant 4$ pouvant se faire à la main) «modulo la petite torsion» et nous mentionnerons les applications de ces résultats en arithmétique. Ces résultats (récents), obtenus en collaboration avec H. Gangl (MPI Bonn) et C. Soulé (IHES), sont basés sur la théorie de Voronoï des réseaux euclidiens parfaits. Le coeur du calcul est la construction d'un complexe homologique (non simplicial) d'origine géométrique. Les calculs et les algorithmes font un usage intensif de l'algèbre linéaire sur $\mathbb{Z}$ (calcul de rang, déterminant, inversion de matrices, forme de Smith, recherche d'isométries). Nous discuterons de l'implémentation actuelle (utilisant PARI/GP et une bibliothèque spécifique écrite en C) et de ses limites, ainsi que des travaux en cours pour $N = 7$. Nous donnerons aussi d'autres exemples de complexes (toujours de nature géométrique), lié à la cohomologie motivique des corps finis et qui cette fois-ci reposent sur des calculs intensifs d'algèbre linéaire sur les corps finis et pouvant conduire à des formes de Smith de matrices de grandes tailles.

LinBox : présentation générale et solutions génériques pour l'algèbre linéaire

Pascal Giorgi
LIP - ÉNS Lyon

LinBox est une bibliothèque logicielle générique efficace pour l'algèbre linéaire, à travers des matrices boîtes noires définies sur des domaines d'entrées symboliques (exactes). Le principe de la généricité logicielle permet d'instancier les procédures sur des domaines de coefficients et de matrices boîtes noires variés, sans sacrifier les performances. Au plus haut niveau, LinBox fournit des algorithmes pour plusieurs problèmes standard de l'algèbre linéaire, tels que la résolution d'équations et les formes normales de matrices. Certains de ces algorithmes sont traités par une approche Lanczos-Krylov et par du préconditionnement algébrique. LinBox fournit aussi une boîte à outils permettant de réutiliser les briques de bases nécessaires à ces approches.

L'implantation générique d'algorithmes de haut niveau dans LinBox ne peut se faire sans une parfaite adéquation avec les interfaces imposées par la bibliothèque. Ces algorithmes peuvent être directement instanciés par l'interface des matrices boîtes noires sans avoir à utiliser le mécanisme *template* du C++ qui peut mener à une explosion de la taille du code compilé. Nous verrons que l'utilisation directe de cette interface pose quelquefois des problèmes de généricité.

Nous verrons par exemple le cas de l'algorithme du polynôme minimal qui nécessite le calcul d'une suite de matrices. Ce calcul étant fait en multipliant la matrice boîte noire par des blocs matriciels, nous verrons que l'on ne peut raisonnablement pas utiliser n'importe quel type de blocs matriciels dans ce calcul. Nous montrerons aussi que les mécanismes d'héritage multiple et d'encapsulation permettent de résoudre certains problèmes dus à l'utilisation de cette interface.

Algèbre linéaire des matrices polynomiales: le problème de l'inversion

Claude-Pierre Jeannerod
Inria, Lip, ÉNS Lyon

On considère ici le problème de l'inversion d'une matrice $n \times n$ dont les éléments sont des polynômes de degré d sur un corps commutatif K. Une telle matrice ne dépend que de $O(n^2 d)$ éléments de K mais représenter son inverse – lorsque celui-ci existe – nécessite en général jusqu'à de l'ordre de $n^3 d$ éléments de K distincts. Du point de vue de la complexité, une cible naturelle est donc un algorithme d'inversion ne nécessitant que $O(n^3 d)$ opérations arithmétiques sur K.

Nous présenterons un algorithme d'inversion dont la complexité "straight-line" – c'est-à-dire lorsque les données d'entrée sont génériques – est égale à $O(n^3 d \log^2(nd) \log\log(nd))$. Par rapport aux méthodes antérieures et pour un produit de matrices sur K en $O(n^3)$, cette complexité représente un gain d'un facteur n; elle est de plus "quasi-optimale" au vu de la cible $O(n^3 d)$, indépendamment de l'algorithme utilisé pour multiplier les matrices sur K.

Pour réduire le coût, nous verrons comment associer un schéma de type "diviser pour régner" à des calculs rapides d'approximants de Padé matriciels. En particulier, l'algorithme utilisé pour calculer ces approximants est dû à Beckermann et Labahn [*SIAM Journal on Matrix Analysis and Applications*, 15:3 (1994), 804–823] et permet de tirer parti du produit de polynômes par FFT. Comme alternative à cette approche à base de FFT, une version exploitant le produit de matrices polynomiales sera aussi évoquée.

Ces résultats ont été obtenus avec Pascal Giorgi et Gilles Villard (Lip).

From Continuous to Discrete Estimates in Linear and Non-Linear Polynomial Equation Solving

Luis M. Pardo
Depto. de Matemática Estadística y Computación. Facultad de Ciencias, Universidad de Cantabria Avda

This talk is mainly concerned with the attempt to state precise comparisons between the complexity of numerical analysis and symbolic computation methods that solve either linear or non-linear systems of multivariate polynomial equations. Complexity studies in numerical analysis are usually based on a continuous complexity model (cf. the works of Shub-Smale in the non-linear case or the works by Smale, Edelmann, Trefethen and others in the linear case) whereas complexity studies of symbolic procedures -when available- are based on a discrete model. Numerical Analysis studies usually assume that inputs belong to some continuous space with a probability distribution (usually a Riemannian manifold with a volume form). A basic example is Linear Algebra Condition Number. A central question in this field is the study of the expected value of A. Turing's condition number $\kappa(A)$. Most of these studies (cf. Smale, Edelmann, Trefethen and others) remark that κ is a projective function ($\kappa(A)$ only depends on the projective point defined by the matrix A). As the projective space $\mathbb{P}$ of all $n \times n$ real matrices is a Riemannian manifold, expected values of $\kappa(A)$ are obtained by volume estimates of the set of ill-conditionned matrices in the projective space $\mathbb{P}$. From these studies, numerical analyst aim to deduce complexity estimates of their procedures. However, complexity refers to computing and computing is discrete. A standard input of a real life computer is a finite string of symbols on a finite alphabet. For instance, in the Linear Algebra case, the input may be assumed to be a matrix with bounded bit length rational entries. In Elimination Theory (systems of polynomial equations) the input is a system of multivariate polynomials with rational coefficients of bounded bit length. The question is then whether those volume estimates have some meaning when dealing with inputs of bounded bit length. This leads to a classical problem which goes back to H. Weyl's equidistribution theory and Erdos-Turan discrepancy bounds. In this talk, I shall introduce a new technique from the Geometry of Numbers that yields the following consequences:

1 Rational matrices of bounded bit length in a projective space are equidistributed with respect to condition numbers. In particular, for all $n \times n$ matrices with rational entries such that the bit length of the rational numbers is of order $O(n^2)$, the condition number $\kappa(A)$ is at most $n^{5/2}$ with high probability.

2 Similar estimates can be obtained for the norm of the Moore-Penrose pseudo-inverse of $n \times (n+1)$ matrices whose entries are Gaussian rationals of bounded bit length.

As for the non-linear case, the following results can also be exhibited:

3 The average number of projective real zeros of systems of homogeneous polynomial equations with rational coefficientes of bounded bit length equals a square root of the Bézout number.

4 The condition number (for the non-linear case) of systems of multivariate polynomial equations with rational coefficients of bounded bit length is at most $(NB)^{O(1)}$ with high probability, where N is the total number of coefficients (in dense form) and B is the Bézout number.

5 The output of a numerical analysis polynomial system solver can be linear in the input length with high probability.

Item 5 above addresses to a central question when comparing Numerical Analysis and Elimination Theory. The output of all known symbolic methods that solve systems of polynomial equations is exponential on the input length with high probability. Then we can ask : is there any symbolic procedure that solves systems of multivariate polynomial equations and such that the output length is polynomial in the input length? The answer is known to be negative for universal symbolic solvers. Could the output of a symbolic procedure be polynomial in the input length on the average? Which kind of symbolic solver can it be?

Symposium

Algorithmique Géométrique

Organisation : Michel Pocchiola - ENS, Paris

Présentation

La session est composée de quatre exposés représentatifs de l'activité de recherche actuelle d'une partie de la communauté française géométrie algorithmique (cf. `http://www.geoalgo.unilim.fr/`).

Le premier exposé porte sur la complexité combinatoire de la triangulation de Delaunay d'une famille de points répartis sur une surface : pour une surface lisse générique et sous des conditions d'échantillonnage apropriées une borne linéaire, modulo un facteur logarithmique, est annoncée.

Le deuxième exposé porte sur l'estimation de la courbure d'une surface échantillonnée : une nouvelle définition de la courbure des surfaces polyédriques est proposée, un algorithme efficace de calcul est dessiné dans le cas des approximations de surfaces lisses et une borne d'erreur est donnée dans le cas des triangulations de Delaunay restreintes à la surface.

Le troisième exposé porte sur le calcul d'un système fondamental de lacets d'une surface combinatoire orientable : un algorithme polynomial calculant une système fondamental de longueur minimale homotope à un système donné est présenté. Par contraste calculer un graphe de découpe d'une surface combinatoire de longueur minimale est connu comme un problème NP-difficile.

Le quatrième et dernier exposé présente un nouvel algorithme de calcul des graphes de visibilité basé sur une généralisation des arbres d'horizons aux obstacles convexes. Un nouveau théorème d'horizon ou de zone est établi.

Complexité de la tétraédrisation de Delaunay de points répartis sur une surface

Dominique Attali
LIS, ENSIEG, Grenoble

En collaboration avec Jean-Daniel Boissonnat, INRIA Sophia-Antipolis et André Lieutier, Dassault Systèmes.

La tétraèdrisation de Delaunay de n points dans $\mathbb{R}^3$ comprend dans le pire des cas $\Omega(n^2)$ tétraèdres. Or, le calcul de la tétraèdrisation de Delaunay dans le cas particulier de points répartis sur une surface a de nombreuses applications en modélisation, reconstruction de surfaces, ainsi que pour le calcul du squelette. Typiquemement, en ingénieurie inverse, un grand nombre de méthodes de reconstruction de surfaces sont fondées sur le calcul de la tétraèdrisation de Delaunay de points échantillonnant la frontière des objets.

Pour ces applications, une amélioration de la borne sur la taille de la tétraèdrisation de Delaunay signifie immédiatement une amélioration du temps de calcul.

Dans cet exposé, nous présentons quelques résultats concernant la complexité en taille de la tétraèdrisation de Delaunay de points répartis sur une surface [3, 4, 5, 6]. Puis, nous nous intéressons au cas des *surfaces polyédriques*. Nous montrons que sous certaines conditions d'échantillonnage, la complexité en taille de la tétraèdrisation de Delaunay est $O(n)$ [1]. Le résultat est déterministe et la constante dans le O peut être explicitement donnée en fonction de grandeurs décrivant la surface. Nous considérons ensuite le cas de *surfaces lisses génériques*. La condition de généricité impose que les surfaces considérées ont pour lignes de crêtes un nombre fini de courbes. Ceci exclut en particulier les sphères et les cylindres. Sous certaines conditions d'échantillonnage des surfaces lisses génériques, la complexité de la tétraèdrisation de Delaunay est $O(n \log n)$ [2].

Références

[1] Dominique Attali and Jean-Daniel Boissonnat. A linear bound on the complexity of the Delaunay triangulation of points on polyhedral surfaces. In *Proc. 7th ACM Symposium on Solid Modeling and Applications*, pages 139–145, 2002.

[2] Dominique Attali, Jean-Daniel Boissonnat, and André Lieutier. Complexity of the delaunay triangulation of points on surfaces : the smooth case. In *Proc. of the 19th ACM Sympos. Comput. Geom.*, San Diego, USA, 2003. Submitted.

[3] Jeff Erickson. Nice point sets can have nasty Delaunay triangulations. In *Proc. 17th Annu. ACM Sympos. Comput. Geom.*, pages 96–105, 2001.

[4] Jeff Erickson. Dense point sets have sparse delaunay triangulations. In *Proc. of the 13th Annual ACM-SIAM Symposium on Discrete Algorithms*, 2002. To appear.

[5] Mordecai Golin and HyeonSuk Na. On the average complexity of 3d-voronoi diagrams of random points on convex polytopes. In *Proc. 12th Canad. Conf. Comput. Geom.*, pages 127–135, 2000.

[6] Mordecai J. Golin and Hyeon-Suk Na. The probabilistic complexity of the voronoi diagram of points on a polyhedron. In *Proc. 14th Annu. ACM Sympos. Comput. Geom.*, pages 209–216, 2002.

Restricted Delaunay triangulations and normal cycles

David Cohen-Steiner
INRIA, Sophia-Antipolis

In this talk, we address the problem of estimating the curvature of a surface from a polyhedral approximation of it. We use the theory of normal cycles from differential geometry to define curvature tensors for a general class of surfaces, including smooth and polyhedral ones. More precisely, we associate with each region of a surface a tensor which in the smooth case is the average of the curvature tensor over this region. The curvature tensor of a polyhedral approximation of a smooth surface then provides an estimator of the one of the smooth surface. Our main result is an error bound on our estimation when the polyhedral approximation is chosen to be the Delaunay triangulation of sample points restricted to the surface. In particular, this bound implies the convergence of our estimator under a local uniformity condition on the sampling. This is joint work with Jean-Marie Morvan.

Système de lacets optimal sur une surface orientable

Eric Colin de Verdière
ENS, Paris

Toute surface compacte orientable sans bord est homéomorphe à une sphère ou un g-tore (accolement de g tores, pour un $g > 0$). Dans cet exposé, on considère une surface qui est (à homéomorphisme près) un g-tore, et on cherche à la découper pour en faire un disque topologique. Un tel découpage permet de déterminer une paramétrisation de la surface ; les applications sous-jacentes sont le maillage, le plaquage de textures, ou le calcul explicite d'un homéomorphisme entre deux g-tores donnés.

Cela peut être obtenu en découpant la surface le long de $2g$ lacets simples ayant un point commun v, deux à deux disjoints sauf en v ; on obtient ainsi un $4g$-gone dont les côtés peuvent être identifiés par paires pour

retrouver la surface. Ceci constitue un *système fondamental* de lacets. On dispose d'algorithmes pour calculer un tel système sur une surface triangulée, mais ils ne tiennent pas compte de la géométrie de la surface, et les lacets obtenus sont d'aspect irrégulier et plus longs que nécessaire. Pour les applications mentionnées ci-dessus, il est souvent souhaitable d'avoir des lacets aussi courts que possible.

Nous nous plaçons dans un cadre où la surface est polyédrique, et où son graphe sommets-arêtes est valué ; tous les systèmes de lacets considérés sont tracés sur ce graphe sommets-arêtes. Nous présentons un algorithme polynomial qui calcule un système de longueur minimale parmi tous les systèmes homotopes à un système donné. Cet algorithme permet aussi de déterminer le plus court lacet simple homotope à un lacet simple donné.

Ce travail, en collaboration avec Francis Lazarus, est paru dans *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science* (FOCS'02), novembre 2002, pages 627-636.

Horizon trees revisited and extended

Michel Pocchiola
ENS, Paris

In this talk we generalize to collections of pairwise disjoint disks in the plane the notion of horizon trees introduced by Edelsbrunner and Guibas in [1] to sweep the dual arrangement of a collection of points in the plane. We use this notion to derive an horizon theorem for visibility complexes and to design the first linear time algorithm to compute the horizontal greedy pseudo-triangulation of a collection of disks from its horizontal visibility map and a new optimal algorithm to sweep its visibility complex. Our sweep algorithm is only based on the left-turn predicate for disks and is conceptually simpler than the algorithm developed in [2].

Références

[1] H. Edelsbrunner and L. J. Guibas. Topologically sweeping an arrangement. *J. Comput. Syst. Sci.*, 38:165–194, 1989. Corrigendum in 42 (1991), 249–251.

[2] P. Angelier and M. Pocchiola. A sum of squares theorem for visibility complexes and applications. In B. Aronov, S. Basu, J. Pach, and M. Sharir, editors, *Discrete and Computational Geometry – The Goodman-Pollack Festschrift*, Algorithms and Combinatorics, pages 1–65. Springer-Verlag, 2002/2003? Preliminary version appeared in the ACM-SoCG'01 proceedings. To appear

Symposium

Applications du calcul formel

Organisation : Jean-Pierre Merlet - projet COPRIN, INRIA Sophia-Antipolis

Présentation

Le but des exposés de cette session est de présenter un panel très variés d'applications dans lesquelles le calcul formel au sens large a joué un rôle important et d'identifier quelques problèmes, aussi bien théoriques que pratiques (facilité d'utilisation des outils, adaptation aux besoin des utilisateurs,..) qu'il reste à résoudre.

Les domaines abordés sont:

- synthèse de filtres hyperfréquences
- détermination des paramètres des correcteurs pour une commande robuste
- méthodes de calibration en robotique
- aide à la conception optimale en robotique

On verra que si effectivement les outils de calcul formel ont permis d'apporter, au moins dans certains cas, des éléments de solutions aux problèmes traités il n'en reste pas moins que beaucoup reste à faire:

- sur la facilité d'utilisation par un public scientifique, mais non spécialiste, des outils proposés
- sur leur intégration dans un processus complet complexe de résolution d'un problème scientifique dans lequel l'utilisation des outils formels ne constitue que quelques étapes
- sur les limites des outils (en terme de taille de problèmes pouvant être résolus, de temps de calcul,...)

Élimination de variables, appliquée à l'étalonnage des robots parallèles

David Daney
INRIA Sophia-Antipolis

Les tolérances, associées à la fabrication et à l'assemblage d'un manipulateur, induisent des imprécisions sur la connaissance théorique des paramètres qui définissent sa géométrie. Ainsi, la propagation de ces erreurs à travers la commande du robot détériore la précision de positionnement du robot. Mais un étalonnage géométrique va nous permettre d'identifier ces erreurs de modélisation du robot.

Pour cela, il nous faudra obtenir une information redondante sur l'état interne du manipulateur. Plusieurs solutions peuvent être mises en oeuvre :

- mesurer le positionnement de l'organe terminal,

– ajouter des capteurs proprioceptifs,

– contraindre l'organe terminal ou certaines articulations passives.

Pour une configuration du robot, ces informations supplémentaires (mesures, ou contraintes) seront alors liées aux paramètres géométriques à identifier, à travers des équations de contraintes. Puis la multiplication de ces configurations de mesures nous permettra d'obtenir un système d'équations sur-contraint (plus d'équations que d'inconnues). En effet, cette solution permet de minimiser l'influence des bruits de mesures sur l'identification des paramètres géométriques.

Nous nous intéresserons à un des problèmes fondamental de l'étalonnage. Il est souvent nécessaire d'introduire dans la formalisation des équations de contraintes, des variables que nous ne chercherons pas à identifier. Ces variables doivent être éliminées. Traditionnellement, cette élimination est effectuée indirectement par les procédures numériques ce qui diminue la qualité de la résolution.

Nous montrerons comment le calcul formel permet non seulement d'éliminer ces variables mais aussi de rendre plus robuste la résolution des systèmes sur-contraints, par la simplification des contraintes,.

Méthodes par intervalles, propagation de contraintes et calcul formel: Principes et applications

Luc Jaulin
LISA, Angers

Le calcul par intervalles permet de résoudre numériquement, mais de façon garantie, une grande classe de problèmes non-linéaires, comme par exemple le calcul de toutes les solutions d'un système nonlinéaire de n équations à n inconnues. Contrairement aux méthodes numériques classiques (méthodes de MontéCarlo, par exemple) et tout comme les méthodes de calcul formel, les résultats sont obtenus de façon globale et garantie en un temps fini, même lorsque des fonctions trigonométriques ou non-continues apparaissent dans notre problème. Cependant, les méthodes par intervalles classiques deviennent inapplicables lorsque le nombre de variables devient élevé, (supérieur à 10 par exemple), principalement à cause de la complexité exponentielle des problèmes traités.

L'utilisation de techniques de calcul formel et de propagation de contraintes permet de repousser largement cette barrière de la dimension et autorise ainsi le traitement de problèmes plus grandes tailles.

Le but de cet exposé est de présenter de façon brève et pédagogique les principes de bases du calcul par intervalles et de propagation de contraintes. Il sera montré comment ces techniques peuvent collaborer avec le calcul formel pour une résolution efficace d'une plus grande classe de problèmes nonlinéaires.

Quelques applications en automatique et en robotique seront données. Des outils logiciels de résolution gratuits, illustrant les techniques présentées seront utilisés pour la résolution de problèmes de commande robuste, d'estimation d'état et de planification de chemins.

Utilisation de techniques du calcul formel pour la synthèse de filtres hyperfréquences

Fabrien Seyfert
projet MIAOU, INRIA Sophia-Antipolis

Faire la synthèse d'un filtre analogique c'est déterminer un ensemble de ces caractéristiques physiques afin d'obtenir le comportement fréquentiel désiré (passe-bas, passe-bande etc...). Nous nous intéresserons ici à une gamme de filtres hyperfréquences admettant un modèle électrique constitué d'une suite de résonateurs (L,C) couplés entre eux. Ce modèle est régit par un système différentiel linéaire caractérisé par un quadruplet matriciel (A,B,C,D) appelé réalisation. Lors de la synthèse on souhaite après avoir déterminé une fonction de transfert idéale (ici une matrice rationnelle) pouvoir calculer une réalisation (A,B,C,D) de ce dernier afin d'en extraire les informations pour le dimensionnement. Si la théorie de la réalisation assure l'existence de manière constructive d'un tel quadruplet dans le cas général il n'en est pas de même lorsque des contraintes sont imposées sur la forme des matrices (A,B,C,D). Ces contraintes portent dans notre cas sur la nullité de certains des éléments de A qui est induite par des raisons technologiques de faisabilité du filtre. Nous montrerons comment les outils du calcul formel relatifs à l'analyse de systèmes polynomiaux peuvent être utilisés ici notamment pour ce qui est du calcul exhaustif de réalisations correspondant à un même transfert. Nous indiquerons aussi quelques questions ouvertes quant à l'existence générique de solutions réelles au problème

posé. Enfin nous indiquerons comment ces techniques peuvent servir dans une optique d'identification en vue du réglage de ces filtres.

Optimisation géométrique d'un mécanisme parallèle

Philippe Wenger
IRCCyN, CNRS, Nantes

Nous présentons une démarche de conception de l'Orthoglide, un mécanisme utilisant une architecture cinématique parallèle. L'Orthoglide est optimisé de façon que certains indices de performance demeurent compris entre certaines borne dans un volume de travail cubique de l'outil. Ces indices de performances sont définis à partir des valeurs propres d'une matrice jacobienne qui peuvent s'écrire comme racines d'un polynôme de degré 3. On montre une approche qui a permis d'apporter une solution à ce problème en évitant un balayage du volume de travail. Un prototype de l'Orthoglide a été construit à l'IRCCyN pour de l'usinage à grande vitesse (video si le temps le permet).

Symposium

Calcul Symbolique/Numérique

Organisation : André Galligo - UNSA, Université de Nice

Présentation

Généralisation de la méthode de Newton pour les racines multiples

Gregoire Lecerf
LAMA, Université de Versailles

L'expose porte sur le thème de la généralisation de la méthode de Newton pour les racines multiples (méthode par déflation). L'exposé contiendra une partie non-archimédienne avec les résultats de ma these mais le but sera de montrer comment la méthode s'adapte numériquement ; Pour cela on utilise des séries à plusieurs variables à coefficients numériques. Il s'agit de travaux en cours avec Marc Giusti, Bruno Salvy et Jean-Claude Yakoubsohn. Les outils numériques sous-jacents sont les gamma et alpha théorèmes et l'utilisation systématique des séries majorantes.

Calcul d'une factorisation exacte à partir d'une factorisation approchée

Guillaume Cheze
Université de Nice

Nous considérons un polynome irréductible dans $\mathbb{Q}[X,Y]$. Nous notons par $P = P_1P_2...P_s$ sa factorisation absolue dans $\mathbb{C}[X,Y]$ où les P_i sont des polynomes irréductibles dans $\mathbb{C}[X,Y]$. De plus nous notons $\mathbb{Q}[\alpha]$ la plus petite extension de $\mathbb{Q}$ qui contient tous les coefficients de P_1.

Soit $P \approx \tilde{P}_1...\tilde{P}_s$ une factorisation approchée de P. Cela signifie que les coefficients de $\tilde{P}_i$ sont des approximations des coefficients de P_i à ϵ prés. Nous considérons les problèmes suivants: Peut on obtenir une factorisation exacte à partir d'une factorisation approchée?

Si cela est possible: Comment trouver le polynome minimal de α sur $\mathbb{Q}$, et comment exprimer les coefficients de P_1 dans $\mathbb{Q}[\alpha]$?

David Rupprecht avait commencé une étude préliminaire de ces problèmes. Ici nous proposons de donner une réponse complète à ceux-ci.

Algorithmique des bulles solitaires dans un tuyau

Gabriel Dosreis
projet GALAAD, INRIA Sophia-Antipolis

Une interface, entre deux milieux, soumise à une différence de pression constante peut être modelisée par une surface à courbure moyenne constante. De telles surfaces sont en correspondance biunivoque avec les applications harmoniques à valeurs dans la sphère unité de $\mathbb{R}^3$; lorqu'elles ne possèdent pas de points ombilics, elles correspondent aussi aux solutions de l'équation sh-Gordon. L'ensemble des solutions de cette équation est naturellement muni de l'action d'habillage de certains groupes de lacets. Nous nous interessons à l'algorithmique de cette action, notamment à l'application des factorisations de Birkoff et d'Iwasawa. Nous illustrons, en particulier, comment cette action coincide avec la transformation classique de Bäcklund lorsqu'on considère des éléments simples ou rationnels.

Résolution stable de systèmes surdétermines dépendant de paramètres approchés

Mohab Safey El Din
projet SPACES, équipe CALFOR, LIP6, Université de Paris VI
En collaboration avec Daniel Lazard

Un melange de lois de probabilite Gaussiennes depend de 5 parametres: les 2 valeurs moyennes, les deux ecarts quadratiques et la proportion du melange. Retrouver ces parametres a partir des moments, jusqu'a l'ordre 6 revient a resoudre un systeme de 6 equations a 5 inconnues.

Theoreme 1 (injectivite): Quelque soient les valeurs des moments, ce systeme a au plus une solution reelle, a la symetrie pres, qui echange les deux lois.

La demonstration de ce theoreme permet de montrer le

Theoreme 2 (stabilite): Il existe une borne d'erreur r, et un algorithme, qui, quelque soient les valeurs approchees a r pres des moments, calcule une solution dont les moments sont a une distance au plus r+epsilon des valeurs vraies, et telle que l'on peut passer continuement de la solution cherchee a la solution calculee sans sortir de cette boule de rayon r+epsilon.

Malheureusement la metrique qui permet de prouver ce theoreme fait intervenir des degres eleves qui rendent l'algorithme impraticable. Cependant les test experimentaux, montrent que la metrique euclidienne classique, non adaptee a la demonstration du theoreme, donne une methode de resolution dont la stabilite est tres satisfaisante.

Étude de prédicats ge'ome'triques

Monique Teillaud
projet Galaad - INRIA Sophia Antipolis

L'étude des prédicats est un problème crucial pour la stabilité et l'efficacité des algorithmes géométriques.

Ces prédicats sont des expressions polynomiales dont le signe doit être évalué de façon exacte pour assurer le bon déroulement de l'algorithme.

L'exemple des arrangements d'arcs de cercle illustre cette problématique assez récente en géométrie algorithmique. L'exposé présentera, sur cet exemple, une introduction motivant l'étude, les diverses voies explorées actuellement (en particulier au sein du projet europeen ECG, Effective Computational Geometry for Curves and Surfaces, `http://www-sop.inria.fr/prisme/ECG/`), et l'implantation en cours pour CGAL (Computational Geometry Algorithms Library, `http://www.cgal.org/`). On s'attardera en particulier sur les types de nombres et les filtres arithmétiques.

Symposium

Contrôlabilité

Organisation : Michel Fliess - CMLA, ENS-Cachan

Présentation

Quoique trois des quatre exposés portent sur la commande de systèmes régis par des équations aux dérivées partielles, les méthodes et les buts diffèrent grandement. Nous essaierons, lors d'une discussion commune, de suggérer quelques pistes pour le futur.

Sur l'inversibilité formelle du comportement entrée/sortie de systèmes dynamiques

Mikhaïl Foursov
IRISA, Université de Rennes I

Dans cet exposé, nous allons parler d'une méthode formelle d'inversion du comportement entrée/sortie de systèmes dynamiques à une entrée avec dérive. La commande est calculée localement, comme un développement en série de Taylor, à partie du développement de Taylor de la sortie.

La démonstration est basée sur les formules explicites des dérivées itérées de la sortie, exprimées en fonction des coefficients de la série génératrice associée à la fonctionnelle causale et aux multi-dérivées de l'entrée. L'idée principale consiste à séparer les systèmes en plusieurs sous-cas, en fonction de leur série génératrice. Nous démontrons que le problème d'inversibilité est formellement résoluble pour toute fonctionnelle causale dépendant effectivement de la commande et de toute sortie réalisable.

Paramétrisations des systèmes linéaires sous-déterminés d'équations aux dérivées partielles: Algorithmes et applications

A. Quadrat
projet CAFE, INRIA Sophia-Antipolis

Le but de cet exposé est de présenter de tests effectifs permettant de reconnaître si les solutions d'un système linéaire sous-déterminé d'équations aux dérivées partielles (EDP) sont *paramétrisables*, c'est à dire s'obtiennent comme l'image d'un certain opérateur différentiel linéaire. Ces résultats sont basés sur la théorie

des modules différentiels (*D-modules*) et sur *l'analyse algébrique* initialement développées dans les années 70 par V. P. Palamodov et M. Kashiwara. Nous illustrerons les algorithmes par différents exemples venant de la physique mathématique dont les équations linéarisées d'Einstein dans le vide.

Le problème de reconnaître si l'on peut paramétriser les solutions d'un système non-linéaire sous-déterminé d'EDP, *problème de Monge*, a été étudié par G. Darboux, D. Hilbert, E. Goursat, P. Zervos ... De nos jours, ce problème est encore ouvert. Dans les années 90, motivé par le suivi de trajectoires des systèmes de contrôle, ce problème a été redécouvert dans le cas des équations différentielles nonlinéaires ainsi que dans le cas des systèmes linéaires différentiels à retards (*platitude*). Dans l'approche comportementale développée par J. C. Willems et son école, ce problème a aussi été étudié pour les systèmes linéaires multidimensionnels (*image representation problem*). Nous montrerons comment les précédents algorithmes se spécialisent pour les systèmes linéaires multidimensionnels (dont les systèmes différentiels à retards incommensurables) et permettent de tester la contrôlabilité, de calculer différentes paramétrisations ou des polynômes libérateurs utiles au suivi de trajectoires.

Nous illustrerons les exemples par des sorties Maple obtenues à l'aide d'une petite boîte à outils, utilisant la bibliothèque *Mfgun*, développée en collaboration avec F. Chyzak (INRIA Rocquencourt, ALGO).

Système d'équations aux dérivées partielles, platitude et discretisation

François Olivier
laboratoire GAGE, École polytechnique

On envisage diverses manières d'étendre la notion de platitude, introduite par Fliess, Lévine, Martin et Rouchon dans le cas de systèmes de dimension finie, donc décrits par des EDO, au cas de systèmes infinis décrits par des équations aux dérivées partielles. Nous nous attacherons ici au cas le plus simple de systèmes monodimensionnel en espace : tiges chauffées ou pliées.

On rappelera brièvement les résultats obtenus dans le cas d'EDP linéaires, à partir du travail de Mounier, grâce à l'utilisation de la théorie de Mikusiński. Une généralisation non linéaire sera ensuite proposée. Celle-ci repose sur une idée élémentaire : se ramener par discrétisation à une suite convergente de systèmes plats, dont la limite est le système étudiés.

On envisagera des procédés élémentaires mais efficaces à partir du découpage de la tige en un nombre croissant de segments. On utilisera aussi d'autres méthodes permettant pour se ramener à un système fini d'EDO, par exemple en considérant un développement tronqué en série de Fourier.

On illustrera la méthode dans le cas d'une tige flexible non linéaire. On s'attachera aussi à montrer que dans le cas linéaire, on retrouve exactement les résultats précédement obtenus.

L'étude d'une tige chauffée par un point intérieur, nous permettra de retrouver, assez simplement, des conditions de contrôlabilité classiques. Enfin, l'étude de l'équation de la chaleur dans la base de Fourier, fait apparaître quelques belles familles d'identités remarquables, incluant des résultats classiques de Wallis et d'Euler et quelques variantes. On montrera ainsi que pour tout i entier positif :

$$\sum_{j\in\mathbb{N}}(-1)^j(2j+1)^{2i-1} = 0\,!$$

Symposium

Cryptologie

Organisation : Nicolas Sendrier - projet CODES, INRIA Rocquencourt

Présentation

Algorithme de Sudan

L'algorithme de Guruswami-Sudan (1998) a constitué une avancée majeure dans le domaine des codes correcteurs, en permettant le décodage des codes de Reed-Solomon (standard du CD et des communications spatiales) au delà des bornes usuelles.

Plus précisément, cet algorithme consiste a trouver un polynôme de degré k à coefficients dans un corps fini à partir de $n > k$ valeurs connues, dont certaines (on ne sait pas lesquelles) peuvent être fausses. Cet algorithme est fondamentalement algébrique, et l'une des phases critique est la génération puis la factorisation d'un polynôme bivarié à coefficient dans le corps.

Si l'on considère l'algorithme de Guruswami-Sudan comme un moyen d'effectuer une interpolation de polynôme avec erreurs, il apparaît évident que son champ d'application dépasse largement la théorie algébrique des codes. En particulier, il a permis de réaliser avec succès la cryptanalyses de systèmes dont la structure algébrique était optimisée pour résister à la plupart des attaques connues, mais qui coïncidait avec une probabilité non négligeable avec un polynôme de (relativement) bas degré.

L'exposé de Daniel Augot passera en revue des éléments importants de cet algorithme et ses liens avec la cryptographie. L'intervention de Lancelot Pecquet détaillera certains problèmes algébriques liés à son implémentation.

Théorie algorithmique des nombres

Ces quelques dernières années, l'évolution de la cryptologie, et en particulier de la cryptologie à clé publique, s'est faite par l'utilisation d'objets mathématiques de plus en plus complexes. On va, par exemple, utiliser aujourd'hui des groupes de points rationnels sur des variétés algébriques plutôt que le groupe multiplicatif des entiers modulo n. Ces nouveaux objets peuvent permettre, à sécurité constante, de diminuer la taille de objets et d'accélérer les opérations de chiffrement, de déchiffrement ou le calcul d'une signature digitale. Le but peut être, par exemple, de mettre en œuvre des fonctionnalités cryptographiques avec les ressources très limitées d'une carte à puce.

Cette complexification des structures mathématiques sous-jacentes entraîne bien évidemment de nouveaux problèmes, dont certains sont liés au calcul formel. On citera par exemple des problèmes, dont l'énoncé semble pourtant simple, comme déterminer une implémentation la plus efficace possible d'une loi de groupe (cf. l'exposé d'Abdolali Basiri) ou bien calculer le cardinal d'un groupe donné (cf. l'exposé de Pierrick Gaudry). Les enjeux ici seront d'obtenir une implémentation efficace des primitives cryptographiques ou de générer rapidement des clés publiques pour ces cryptosystèmes.

Cryptanalyses par les bases de Gröbner

Beaucoup de cryptosystèmes et donc de problèmes de cryptanalyse possèdent une forte structure algébrique que celle-ci soit explicite (par exemple la clé publique d'une instance de HFE est un système polynomial quadratique multivarié sur le corps fini à 2 éléments) ou implicite. Bien entendu tout problème peut s'écrire sous forme d'un système polynomial booléen, une forte structure algébrique peut rendre ce système facile (disons plutôt moins difficile) à résoudre.

Ainsi calculer des bases de Gröbner de systèmes polynomiaux à coefficient dans $\mathbf{F}_2$ constitue sans conteste une nouvelle technique de cryptanalyse. Le premier succès de cette technique date de 2002 avec la résolution par Jean-Charles Faugère du challenge public de HFE. Dans son exposé, Gwenolé Ars nous présentera une application de cette technique aux générateurs pseudo-aléatoires produits par des registres filtrés. Cette application est extrêmement importante, car ces générateurs sont effectivement utilisés en cryptographie lorsque l'on veut atteindre des débits de chiffrement élevés.

Arithmétique des jacobiennes de courbes superélliptiques cubiques

Abdolali Basiri
équipe CALFOR et projet SPACES, LIP6, Université de Paris VI
En collaboration avec Endreas Enge, Jean-Charles Faugere et Nicolas Gurel

A partir d'une courbe plane C définie sur un corps K, on peut construire naturellement un groupe noté $J_K(C)$, appelé la jacobienne de C sur K . Pour une utilisation cryptographique de $J_K(C)$, il est nécessaire d'avoir une représentation unique des éléments de ce groupe et un algorithme, ou des formules explicites, pour réaliser la loi de groupe. Ceci est deja bien étudie pour les courbes elliptiques et hyperélliptiques.

Pour C une courbe cubique superélliptique, nous donnons un critère de réduction explicite pour la représentation typique d'un élément de $J_K(C)$.

Nous présentons deux nouveaux algorithmes de calcul de la loi de groupe dans les courbes cubiques telles que le diviseur à l'infini est totalement ramifié. Le premier algorithme est inspire de la réduction de Cantor dans le cadre des courbes hyperélliptiques. Il présente l'avantage de s'implanter efficacement en quelques lignes de code si on utilise une bibliothèque d'arithmetique de polynômes. La seconde approche fournit une méthode generale pour obtenir des formules explicites. Il est basé sur l'algorithme FGLM qui, à partir d'une base de Gröbner pour un ordre donné, trouve une base de Gröbner pour un autre ordre.

Algorithme de décodage de Sudan et cryptanalyse

Daniel Augot
projet CODES, INRIA Rocquencourt

L'algorithme de décodage des codes de Reed-Solomon et des codes géométriques de Sudan et Guruswami-Sudan est une avancée importante dans le domaine des codes correcteurs d'erreurs. Cet algorithme permet de décoder au delà de la capacité de correction de ces codes, et notamment de corriger un nombre élevé d'erreurs quand le taux de transmission est faible, ce qui offre de nouvelles perspectives.

Dans cet exposé, nous étudierons le cryptosystème de Knudsen et Nyberg, aprés avoir présenté ce qu'est un algorithme de chiffrement symétrique. Nous montrerons une faiblesse de ce système, et comment le problème de l'attaque de ce système se raméne à un problème de codes correcteurs d'erreurs, celui du décodage des codes de Reed-Solomon. Nous rappellerons les performances de l'algorithme de décodage de Berlekamp-Massey. Ensuite nous présenterons l'algorithme de Sudan dans sa première version, ses performances, et les conséquences sur l'algorithme de chiffrement de Knudsen et Nyberg. Nous traiterons ensuite l'algorithme de Sudan sous l'angle de l'implémentation. Bien que les problèmes rencontrés soient des problèmes de calcul formel (interpolation, recherche de racines), nous donnerons deux algorithmes dédiés aux codes correcteurs d'erreurs, pour une plus grande performance.

Enfin nous traiterons le problème du décodage des Reed-Solomon du point de vue négatif, quand le problème devient difficile c'est-à-dire quand le nombre d'erreurs devient supérieur à la capacité de correction de l'algorithme de Sudan. Nous utiliserons cette difficulté pour construire un système de chiffrement à clé publique, basé sur les codes de Reed-Solomon.

Résolution des régistres filtrées par des méthodes polynomiales

Gwenole Ars
CALFOR, Université de Paris VI

Une application de la cryptographie à clé secrète est la modélisation de générateur pseudo aléatoire comme les registres filtrés. Ils permettent la construction d'une longue suite de nombres à partir d'un court germe de k éléments au départ. Le registre filtré est composé de deux éléments : un registre à décalage et une fonction booléenne. Un registre à décalage est simplement un automate linéaire inversible et la fonction booleenne peut s'écrire sous une forme polynomiale à plusieurs variables dans $\mathbb{F}_2$. Chaque sortie du registre peut qlors s'ecrire comme polynôme des k éléments au départ. Ces modèles sont très étudiées et il existe des méthodes de résolution très performantes sur certains registres imposant ainsi des critères dans le choix de ces registres. L'attaque d'un tel générateur consiste à retrouver l'état initial de l'automate à partir d'équations polynomiales sur le corps. Comme tous les calculs sont exacts (corps fini), il est naturel d'utiliser les méthodes de calcul formel. A travers une étude d'un modèle simplifié, nous étudirons les avantages et les facteurs bloquants de l'utilisation de telles méthodes pour ce type de modèle.

Une méthode de Newton-Puiseux sur les corps de fonctions

Lancelot Pecquet
LACL, Université de Paris XII

Soit K/k un corps de fonctions, nous donnons un algorithme pour trouver les racines dans K d'un polynôme quelconque $G(T) = a_0 + \cdots + a_n T^n \in K[T]$. Cet algorithme est une adaptation au cas des corps de fonctions de deux méthodes décrites par Newton dans Methodus Fluxionum et Seriarum infinitarum [5] vers 1671. La première d'entre-elles fut popularisée autour de 1850 par Puiseux [7], et la seconde, généralisée vers 1908 par Hensel [3].

En supposant que k a une arithmétique calculable, qu'il existe un algorithme trouvant toutes les racines dans k d'un polynôme quelconque de $k[x]$ et que K a une théorie de Riemann-Roch effective (c'est le cas si $k = \mathbb{Q}$, ou si $k = \mathbb{F}_q$ est un corps fini par exemple), on peut choisir une place P de degré 1 et une uniformisante π, et disposer dès lors d'un plongement effectif de K dans son complété π-adique $\widehat{K}$ qui est isomorphe au corps $k((t))$ des séries de Laurent sur k (c'est dans ce dernier corps qu'auront lieu les calculs, sur des séries tronquées). Chaque racine de G est caractérisée par un nombre fini de coefficients de son développement π-adique. Notre algorithme calcule le nombre et la valeur de ces coefficients, puis les utilise pour reconstruire les fonctions de K à partir de leur développement π-adique tronqué.

Notre méthode peut être utilisé [6] comme une primitive dans les algorithmes de décodage en liste tels que ceux de Sudan [8] ou de Guruswami-Sudan [2] et dans les cryptanalyses par interpolation probabilistes comme celle de Jakobsen [4]. L'application à l'algorithme de Sudan, comme à ces cryptanalyses d'une variante de l'algorithme décrit ici conduit à la meilleure complexité connue [1].

Références

[1] Daniel Augot et Lancelot Pecquet. A Hensel lifting to replace factorization in list-decoding of algebraic-geometric and Reed-Solomon codes. *IEEE Transactions on Information Theory*, vol. 46, no. 7 pp. 2605–2614, 2000.

[2] Venkatesan Guruswami et Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, vol. 45, no. 6 pp. 1757–1767, 1999.

[3] Kurt Hensel. Theorie der algebraischen zahlen. Teubner, Leipzig, 1908.

[4] Thomas Jakobsen. Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. In *CRYPTO'98*, volume 1462 of LNCS. Springer-Verlag, 1998.

[5] Isaac Newton. La méthode des fluxions et les suites infinies. *Traduction française de Georges de Buffon*, Paris, 1740.

[6] Lancelot Pecquet. Décodage en liste des codes géométriques. *Thèse de doctorat*, Université Paris VI, 2001.

[7] Victor Puiseux. Recherches sur les fonctions algébriques. *Journal de Mathématiques*, vol. 15 pp. 365–480, 1850.

[8] Madhu Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, vol. 13 pp. 180–193, 1997.

Calcul de cardinalité de courbes de genre 2 sur un corps premier

Pierrick Gaudry
LIX, École polytechnique
En collaboration avec Éric Schost, laboratoire gage École polytechnique

Après le succès populaire de RSA, les courbes elliptiques sont désormais présentées comme une alternative crédible pour faire de la cryptographie à clef publique. Leur principal avantage est que pour une sécurité donnée la taille des paramètres (clefs, sigantures) est plus petite que pour RSA. Les courbes de genre supérieur, et parmi celles-ci, les courbes hyperelliptiques de genre 2 peuvent aussi être utilisées dans la plupart des protocoles basés sur le logarithme discret.

Une tâche importante lorsque l'on désire fabriquer un tel cryptosystème à base de courbes de genre 2 est le calcul de la cardinalité de la Jacobienne de cette courbe. En effet, celle-ci constitue le groupe dans lequel on suppose le problème du logarithme discret difficile, et il faut donc absolument s'assurer que son ordre n'est pas friable (idéalement l'ordre est premier).

Lorsque le corps de base est de petite caractéristique, des algorithmes efficaces de comptage de points existent (Kedlaya, Mestre) et permettent de traiter facilement des courbes de taille suffisante. Pour les corps finis premiers, ces techniques p-adiques ne s'appliquent plus, et la méthode de choix reste l'algorithme de Schoof adapté au genre supérieur.

Nous exposerons cet algorithme et notamment des améliorations récentes qui nous ont permis d'atteindre un nouveau record. Le coeur du problème réside dans la manière de représenter des éléments de torsion sous la forme d'un idéal dans une algèbre de polynômes. Il s'agit de contourner au maximum les méthodes génériques comme l'algorithme de Buchberger afin d'accélérer les calculs.

Symposium

Équations différentielles I: résolution

Organisation : Jacques-Arthur Weil - projet CAFE, INRIA Sophia-Antipolis

Présentation

Le terme résolution peut se décomposer en deux sous-catégories: la mise en bonne forme des systèmes, puis la recherche de solutions à proprement parler. Les travaux de cette session sont de nature essentiellement algébrique.

Un premier aspect est la *préparation* des systèmes, c'est à dire leur transformation en un système "plus agréable" pour la résolution ou pour l'analyse qualitative des solutions. Pour les systèmes différentiels non-linéaires, les outils d'algèbre différentielle conduisent à des algorithmes de triangulation des systèmes différentiels polynomiaux. Ces algorithmes sont sous-jacents aux exposés de Nicolas Le Roux et Sylvain Neut. D'autres approches algébriques des EDP non linéaires mènent à des algorithmes de nature plus géométrique (involution, approches semi-numériques, etc, voir aussi la session "automatique").

Dans le cas linéaire, ces algorithmes reviennent à de l'algèbre non commutative (de l'élimination dans des algèbres de Ore, voir aussi la session "fonctions spéciales") et seront utilisés dans l'exposé de Jacques-Arthur Weil pour caractériser des systèmes différentiels sous-déterminés et les préparer à une résolution et paramétrisation.

Pour les systèmes différentiels linéaires, on peut pousser ce processus de réduction plus finement en transformant un système linéaire en un système équivalent dont les singularités ont des ordres de pôle minimaux. Il ressort, par exemple, des travaux menés autour de Grenoble dans les 20 dernières années (méthodes de super-réduction, projet Cathode) que cette forme normale donne un bon point de départ à des algorithmes de recherche de solutions formelles. C'est un algorithme donnant une telle réduction (pour des systèmes à singularités régulières) qui sera présenté par Manuel Bronstein, avec quelques mots sur la résolution à proprement parler.

Une fois un système mis en "bonne forme" se pose la question de la *recherche de solutions*. Là il faut préciser la classe d'objets que l'on recherche.

La première classe naturelle est celle des séries formelles. L'exposé de Nicolas Le Roux montrera comment, pour un système en bonne forme, on peut adapter un algorithme "à la Newton" pour le calcul de solutions formelles de systèmes d'équations aux dérivées partielles.

Les autres classes sont des solutions globales, en "forme finie". Dans l'exposé de Jacques-Arthur Weil, on verra comment paramétrer complètement les solutions d'un système différentiel linéaire dans un module (pour simplifier, disons des solutions rationelles).

Toujours dans le cas linéaire, les propriétés des solutions, en particulier le fait d'être exprimables en forme finie, se lisent dans le groupe de Galois différentiel. Ce groupe est un objet classifiant très puissant, dont on détecte les propriétés par certains objets laissés invariants. Ceci permet de classifier les types de solutions (par exemple, liouvilliennes) d'équations différentielles et d'établir des algorithmes pour les déterminer. Dans l'exposé de Philippe Gaillard, on verra comment une étude fine des groupes de Galois possibles permet de raffiner des algorithmes de résolution des équations différentielles linéaires d'ordre quatre.
Dans le cas non-linéaire, on n'a plus de structure aussi fine. Mentionnons tout de même deux grandes classes de méthodes. L'utilisation de symétries de Lie (qui seront évoquées dans l'exposé d'Olivier Cormier) et les résolutions par transformation (méthodes à la Cartan) qui seront développées dans l'exposé de Sylvain Neut (dans l'autre session différentielle). rationnelles, différences, aux q-différences, etc..

Enfin, un enjeu important, dans ces travaux de mathématique constructives, est le développement de programmes de calcul formel - qui sont sous-jacents à tout ce qui précéde. Les stratégies ont varié. Beaucoup ont choisi d'intégrer leurs travaux comme librairies ou addenda à des systèmes commerciaux (souvent Maple); d'autres ont développé des outils autonomes dédiés (par exemple le serveur Bernina de Bronstein, le logiciel Colombus de van der Hoeven). L'exposé d'Olivier Cormier présentera la problématique du développement de la librairie d'un logiciel de calcul formel (en l'occurence: MuPad). Les divers enjeux, questions, et stratégies du développement d'une librairie de calcul formel pour les équations différentielles devraient ressortir de ce travail.

Résolutions de systèmes différentiels

Jacques-Arthur Weil
projet CAFE, INRIA Sophia-Antipolis
En collaboration avec Frédéric Chyzak, Alban Quadrat, et Bruno Salvy

Après un bref panorama de l'état de l'art quant à la résolution en forme finie de systèmes différentiels ordinaires déterminés (c'est à dire où les solutions ne dépendent pas de fonctions arbirtraires inconnues), nous proposons une méthode de résolution des systèmes différentiels linéaires sous-déterminés (comme on en rencontre, par exemple, en automatique), en montrant en particulier comment obtenir une paramétrisation rationelle complète de l'ensemble des solutions. Après quelques exemples, nous indiquons des généralisations de ces techniques à certains systèmes d'équations aux dérivées partielles linéaires.

Méthode de Newton pour le calcul de séries solution de systèmes d'EDP

Nicolas Le Roux
LACO,universite de Limoges
En collaboration avec Évelyne Hubert

Nous présenterons une nouvelle méthode de calcul des séries formelles solution de système d'EDP réguliers. Cette méthode généralise une méthode de calcul de la série solution d'une EDO d'ordre 1, introduite par Geddes, qui utilise l'opérateur de Newton associé à l'EDO.

Une implantation de cette méthode est en cours. Nous présenterons des résultats comparatifs de cette méthode et de celle implantée dans diffalg (par F.Boulier) et rif (A.Wittkpof)

Un algorithme de réduction des systèmes différentiels réguliers

Manuel Bronstein
projet CAFE, INRIA Sophia-Antipolis
Travail commun avec Barry Trager

Nous proposons une définition de régularité pour des systèmes différentiels linéaires à coefficients dans une extension monomiale d'un corps différentiel. Nous donnons une itération globale, et complètement rationelle,

qui transforme un système dont les singularités finies sont régulières en un système équivalent dont les pôles finis sont simples. Nous appliquons ensuite cette itération aux systèmes différentiels satisfaits par des bases de corps de fonctions algébriques, et en déduisons des algorithmes pour calculer le nombre de composantes irréductibles et le genre de courbes algébriques.

MuPAD et ODE

Olivier Cormier
Université de Paderborn

Nous présentons quelques algorithmes récemment implantés dans la librairie ODE (Ordinary Differential Equations) de MuPAD pour la résolution des équations différentielles. Dans le cas linéaire cela concerne notamment le résolution des équations du second ordre à l'aide de fonctions spéciales, et dans le cas non-linéaire l'implantation de méthodes pour la résolution des équations d'Abel et la recherche de facteurs intégrands pour des équations explicites d'ordre 2. Nous expérimenterons aussi le lien entre MuPAD et Bernina.

Équations différentielles linéaires d'ordre 4

Philippe Gaillard
IRMAR,Universite de Rennes I

On s'intéressera aux équations différentielles linéaires d'ordre 4 de groupe de Galois différentiel imprimitif non monomial; 4 est le plus petit ordre pour lequel de tels groupes apparaissent. Des travaux précédents de M.F. Singer et F. Ulmer donnaient des bornes pour le degré du polynôme minimal des dérivées logarithmiques de telles équations, en fonction du "type" du groupe, notion qui sera introduite au cours de l'exposé. L'objet du travail présenté ici et réalisé par D. Boucher, F. Ulmer et moi-même est de montrer que ces bornes sont optimales, à une exception près.

Symposium

Équations différentielles II : autres points de vue

Organisation : Bruno Salvy et Jacques-Arthur Weil -

Présentation

Cette session traite de questions dont le point commun est d'être liées aux équations différentielles et d'utiliser (outre l'algèbre) également des outils d'analyse et de géométrie.
Le premier exposé de Joris van der Hoeven est un panorama de méthodes concernant le calcul sur des séries formelles et leur manipulation automatique. Si les méthodes de calcul sont algébriques, des considérations d'analyse interviennent dans les questions de prolongement ou l'établissement de certaines méthodes (par exemple pour le test à zéro) - on retrouvera ce genre d'idées dans la session "holonomie et fonctions spéciales". Les techniques présentées ici fournissent aussi un bon cadre à l'asymptotique automatique.
Les séries formelles considérées sont parfois caractérisées comme solutions d'équations différentielles, mais aussi d'autre types d'équations fonctionnelles comme des équations aux différences et aux q-différences. Le deuxième exposé de la session, par Franck Michel, propose (à travers l'étude d'une solution d'une équation aux différences) des méthodes d'analyse de la nature d'une série formelle solution d'une équation fonctionnelle. Une classe très importante de séries est la classe Gevrey, qui regroupe des séries divergentes qui peuvent s'interpréter (par des procédés de resommation, par exemple de Borel-Laplace) comme développements asymptotiques de "vraies fonctions" (analytiques) dans des secteurs du plan complexe. Ces séries divergentes ont la propriété frappante de "converger" beaucoup plus vite que les séries convergentes. La détermination du type Gevrey d'une série donne une forte information sur le comportement de la fonction, et sur la dynamique du système qu'elle satisfait. L'auteur présentera des recherches menées collectivement pour l'établissement d'outils heuristiques de calcul pour aider à cette détermination (le "gevreytiseur").
L'exposé de Hoang Ngoc Minh se tourne plus vers la théorie des nombres. A travers l'étude des Polylogarithmes et des fonctions multizétas, on voit un fort courant de pensée contemporain en théorie des nombres: étudier systématiquement des nombres définis comme valeurs de solutions d'équations fonctionnelles (théorie qui remonte - au moins - à Siegel) ou d'intégrales, ce qui permet de donner des résultats (par exemple de transcendance ou d'indépendance algébrique) sur ces nombres à partir des relations qui les définissent (pour d'autres développements récents: théorie des périodes de Kontsevich et Zagier, nombres "Naturels" d'Ecalle, etc). Une saveur du beau travail présenté par Hoang est que, parti de fonctions pour caractériser des nombres, il nous présente dans cette session un travail qui, en retour, permet de déterminer un groupe de Galois différentiel, donc des propriétés concernant de nouveau des fonctions.

L'outil central de ce travail est la manipulation d'algèbre de mots (non-commutatives). Ces outils et leurs liens avec la théorie des automates apparaissent de nouveau dans le travail de Vincent Houseaux qui présentera des outils de calcul en Maple sur les séries rationnelles en variables non-commutatives.
Enfin, l'exposé de Sylvain Neut montre une interaction entre des outils d'algèbre différentielle et des outils de géométrie. Les calculs menés sur la méthode d'équivalence de Cartan ont un support algébrique pour un résultat géométrique. Ils permettent, via la détermination des invariants fondamentaux de Chern, de classifier des familles d'équations différentielles pouvant se ramener par des transformations (de contact) à des formes simples (par exemple, une linéarisation).

Calcul effectif avec des séries formelles

Joris van der Hoeven
CNRS, Université de Paris XI

Lorsque l'on s'intéresse en calcul formel en des classes de fonctions plus générales que les fonctions algébriques, il est souvent possible de représenter ces fonctions par des séries formelles. On peut alors se poser plusieurs questions : comment calculer rapidement les coefficients, comment savoir si une expression représente la série nulle, comment prolonger analytiquement une fonction, etc. Nous présenterons un survol du progrès récent dans ce domaine.

Estimations Gevrey de la solution formelle générale d'une équation aux différences

Franck Michel
Université Aix-Marseille III

On s'intéresse à l'équation aux différences

$$u(z+1) - 2u(z) + u(z-1) = -u^2(z)$$

ses solutions permettant d'étudier la scission des séparatrices de l'application de Hénon. Nous présentons des calculs numériques, basés sur l'étude asymptotique de cette équation menée (chronologiquement) par V. Gelfreich et D. Sauzin (travaux publiés dans [1]), puis R. Schäfke, M. Canalis-Durand et F. Michel (travaux en cours).
Nous calculons une solution formelle générale sous forme d'une transérie $\tilde{u}(z,b) = \sum_{n\geq 0} \tilde{u}_n(z)\ b^n$
Chaque $\tilde{u}_n$ se décompose en une partie polynomiale et une partie série, divergente, Gevrey 1, développement asymptotique d'une fonction que l'on peut obtenir par transformée de Borel-Laplace. Une estimation numérique du comportement par rapport à la variable b permet de conclure à une croissance Gevrey 6. Les estimations numériques de la divergence des séries ont fait leurs preuves récemment sur d'autres problèmes, et font l'objet désormais d'un projet de site web, le "Gevreytiseur", que nous présenterons.
La transformée de Borel des $\tilde{u}_n$ possède des singularités aux points $2ik\pi$, $k \in \mathbb{Z}$, $k \neq 0$. Nous nous intéressons au calcul numérique des coefficients de l'équation du pont correspondante.
Les calculs utilisent GMP, Pari, et Maple, avec les moyens de la grappe Médicis.
[1] Borel summation and splitting of separatrices for the Hénon map, [J] Ann. Inst. Fourier 51, No.2, 513-567 (2001)

Differential Galois group & non commutative generating series of polylogarithms

Hoang Ngoc Minh
Universite Lille II

Let us associate to any composition $\mathbf{s} = (s_1, \cdots, s_r)$ (*i.e.* to any finite sequence of strictly positive integers) the polylogarithm function $\mathrm{Li}_{\mathbf{s}}(z)$ (for $|z|$ inside the unit complex circle)

$$\mathrm{Li}_{\mathbf{s}}(z) = \sum_{n_1 > \cdots > n_r > 0} \frac{z^{n_1}}{n_1^{s_1} \cdots n_r^{s_r}} \tag{9.1}$$

and the polyzêta $\zeta(\mathbf{s})$ (for $s_1 > 1$)

$$\zeta(\mathbf{s}) = \mathrm{Li}_{\mathbf{s}}(1) = \sum_{n_1>\cdots>n_r>0} \frac{1}{n_1^{s_1}\cdots n_r^{s_r}}. \tag{9.2}$$

Let us introduce the finite alphabet $X = \{x_0,x_1\}$, and the non commutative free algebra $\mathbb{Q}\langle X\rangle$. We shall identify below the composition $\mathbf{s}$ with its encoding word $w = x_0^{s_1-1}x_1\cdots x_0^{s_r-1}x_1 \in X^*$ over X^*x_1. We obtain so a concatenation isomorphism from the $\mathbb{Q}$-algebra of compositions into the subalgebra $\mathbb{Q}\langle X\rangle x_1$ of $\mathbb{Q}\langle X\rangle$. The polylogarithms can be then indexed in that way by the words w of X^*x_1. But the polyzêtas are well defined only for $s_1 > 1$, and so for the *convergent* words of X^*, *i.e for* $w \in \varepsilon \cup x_0X^*x_1$, and linearly extended to $\mathrm{C}_1 = \mathbb{Q} \oplus x_0\mathbb{Q}\langle X\rangle x_1$.

Let us consider the differential forms

$$\omega_0(z) = \frac{dz}{z} \quad \text{and} \quad \omega_1(z) = \frac{dz}{1-z}. \tag{9.3}$$

One verifies the polylogarithm $\mathrm{Li}_{\mathbf{s}}(z)$ is also the *Chen iterated integral* associated to the word $w = x_0^{s_1-1}x_1\cdots x_0^{s_k-1}x_1$ and with respect to $\omega_0(z)$,$\omega_1(z)$:

$$\mathrm{Li}_{x_0^{s_1-1}x_1\cdots x_0^{s_k-1}x_1}(z) = \int_{0,\gamma}^{z} \omega_0^{s_1-1}\omega_1\cdots\omega_0^{s_k-1}\omega_1. \tag{9.4}$$

This provides an analytic prolongation of $L_{\mathbf{s}}(z) = \mathrm{Li}_w(z)$ over the Riemann surface of $\mathbb{C}\setminus\{0,1\}$.

We can also extend the iterated integral (9.4) over the whole of X^* by putting $L_\epsilon(z) = 1$, where ϵ denotes the empty word over X and, for any integer $n > 0$ and for any word $w \in X^*$,

$$L_{x_0^n}(z) = \frac{\log^n(z)}{n!}, \qquad L_{x_1x_0^n}(z) = \int_{0,\gamma}^{z} \omega_1(t)\frac{\log^n(t)}{n!}, \tag{9.5}$$

$$L_{x_0w}(z) = \int_{0,\gamma}^{z} \omega_0(t)L_w(t), \qquad L_{x_1w}(z) = \int_{0,\gamma}^{z} \omega_1(t)L_w(t). \tag{9.6}$$

This allows to construct the *non commutative generating series* of polylogarithms

$$L(z) = \sum_{w\in X^*} L_w(z)\, w. \tag{9.7}$$

By differentiating it term by term (see (9.4) and (9.5)) we obtain $L(z)$ as the solution of the *Drinfel'd equation*, *i.e.* the following first order differential equation with *non* commuting parameters x_0,x_1

$$dL(z) = [x_0\omega_0(z) + x_1\omega_1(z)]L(z), \tag{9.8}$$

with the boundary condition

$$L(\varepsilon) = e^{x_0\log\varepsilon} + o(\sqrt{\varepsilon}) \quad \text{if} \quad \varepsilon \to 0^+. \tag{9.9}$$

In this work, we prove that the differential Galois group associated to the Drinfel'd equation is the Lie group of the *Lie exponential series* over X :

$$\mathrm{Gal}[x_0\omega_0 + x_1\omega_1] = \{\exp(C) \mid C \in \mathcal{L}ie_{\mathbb{C}}\langle\langle X\rangle\rangle\} \tag{9.10}$$

and it contains the *monodromy* group of $L(z)$. This allows to compute the differential Galois group of the linear differential equation of order n with three simple regular sigularities $z \in \{0,1,\infty\}$

$$a(z)y^{(n)} + \cdots + a_1(z)\dot{y}(z) + a_0(z)y(z) = 0, \tag{9.11}$$

or equivalently, of the differential equation system

$$\left\{\begin{array}{rcl} dq(z) &=& [M_0\omega_0(z) + M_1\omega_1(z)]\, q(z), \\ q(z_0) &=& \eta, \\ y(z) &=& \lambda q(z), \end{array}\right. \tag{9.12}$$

where $\lambda \in \mathcal{M}_{1,n}(\mathbb{C})$,$\eta \in \mathcal{M}_{n,1}(\mathbb{C})$ and M_0,$M_1 \in \mathcal{M}_{n,n}(\mathbb{C})$.

We will show also how to extend this work to the case of more than three singularities.

Méthode de Cartan : équivalence d'équations différentielles

Sylvain Neut
LIFL - Univ. Lille I

La méthode d'équivalence de Cartan permet de décider de l'équivalence d'objets géométriques et, en particulier, de l'équivalence d'équations différentielles. Par exemple, on sait grâce à l'algorithme de Cartan, que les deux équations

$$y'' = x^2 y' + y \quad \text{et} \quad y'' = 0$$

sont équivalentes par une transformation ponctuelle ($x \to \xi(x,y)$, $y \to \eta(x,y)$).
Après une brève description de l'algorithme de Cartan, nous présenterons des résultats d'équivalence nouveaux obtenus grâce à notre programme Maple dédié à cette méthode. Certaines optimisations de ce programme seront évoquées ainsi qu'une methode directe basée sur l'algèbre différentielle. Les principales contributions évoquées portent sur des conditions de linéarisation d'EDO d'ordre 3 et sur l'équivalence de certains systèmes d'EDP.

Séries rationnelles en MAPLE : calcul et applications

Vincent Houseaux
LIFL - Univ. Lille I

Les séries rationnelles forment une classe de séries formelles en variables non-commutatives, classiquement caractérisées par leur propriété d'être reconnues par des automates. Elles sont entre autres utilisées pour coder les systèmes dynamiques dits bilinéaires. D'autre part, le fait que les produits de mélange préservent la rationalité permet de déduire de certaines identités entre séries rationnelles des identités entre poly-logarithmes ou entre valeurs de la fonction ζ de Riemann multi-valuée (*Multiple Zeta Values*). Par exemple, on montre de cette manière que pour tout $n \in \mathbb{N}$, $\zeta(\{4\}^n) = 4^n \zeta(\{3,1\}^n)$.

La librairie *rationalSeries* que nous présentons fournit divers outils de calcul sur les séries rationnelles en MAPLE. Elle utilise une représentation originale des séries rationnelles par un système de ré-écriture et une forme tronquée de la série. Contrairement à la représentation classique par $\mathbb{K}$-automates, cette représentation est unique lorsqu'elle est minimale. Les algorithmes implantés comprennent les opérations rationnelles de base, le produit de mélange et de quasi-mélange (sur l'alphabet des entiers), ainsi que diverses autres opérations (produit de Hadamard, résiduels, minimisation) ce qui permet de prouver le genre d'identités recherchées. Un algorithme d'approximation rationnelle est également inclus, adapté de travaux de C. Hespel et G. Jacob (correspondant à l'approximation bilinéaire d'un système dynamique codé par sa série génératrice).

Symposium

Session Ouverte

Organisation : -

Présentation

La variété des domaines d'application du calcul formel n'a pas permis de tous les prendre en compte ; les propositions d'exposés qui ne trouvaient naturellement leur place dans aucune des sessions ont donc été regroupées au sein d'une "session ouverte".

Dans cette session, on trouve un exposé concernant la théorie des automates, un exposé lié à la géométrie algorithmique qui a dû, faute de place, être intégré à cette session, et un exposé traitant d'applications de techniques de calcul formel pour calculer des groupes de cohomologie de diverses structures algébriques.

Un cadre algébrique pour les problèmes de visibilité 3D

Xavier Goaoc
projet ISA, LORIA Nancy

Les problèmes de visibilité sont omniprésents en infographie et se présentent sous plusieurs forme : lancer de rayon, élimination de surfaces cachées, calcul de facteurs de forme, maillages de discontinuité... Pour pouvoir les traiter de manière uniforme, il est nécessaire de structurer les informations de visibilité de manière globale ; c'est le but du complexe de visibilité, une décomposition de l'espace des rayons suivant les propriétés de visibilité.

Dans cet exposé, nous présentons un cadre algébrique pour l'étude du complexe de visibilité 3D. Nous commençons par représenter ses cellules comme des ensembles semi-algébriques réels. Ensuite, nous décrivons un algorithme de calcul du complexe de visibilité 3D base sur ces représentations, et détaillons les primitives algébriques qu'il utilise.

Élimination Algébrique des ϵ-transitions

Hatem Hadji Kacem
En collaboration avec Éric Laugerotte et Gérard Duchamp

Le but de ce travail est d'aboutir à une méthode algébrique pour éliminer les ϵ-transitions existantes dans un k-ϵ-automate afin d'obtenir un k-automate classique simulant le même comportement. Pour que cette méthode soit définie, il faut que l'étoile de la matrice des ϵ-transitions soit d'éfinie. Ainsi, on enonce un théorème qui va rendre effectif le passage d'un k-ϵ-automate à un k-automate.

Notre travail sera organisé comme suit. On commence par définir la notion d'automate à multiplicités dans un semi-anneau k. Son comportement est un série de $k << \Sigma >>$ ou Σ est un alphabet. Ensuite, on présentera les k-ϵ-automates (structure et comportement) avant d'énoncer et prouver notre résultat principal. Après une discussion sur la validité de l'étoile, on détaillera l'algorithme issu de la méthode algébrique permettant la transformation d'un k-ϵ-automate en k-automate équivalent en terme de comportement.

Ce travail est lié au développement du domaine Automata en cours d'intégration à la bibliothèque MuPAD-Combinat.

Application du calcul formel dans les calculs cohomologiques de structures algébriques

---

A. Makhlouf
LMA, Mulhouse

Dans l'étude des ensembles de lois d'une structure algébrique (algèbre associative, de Lie, de Poisson ou de Hopf), les déformations jouent un rôle fondamental. Les déformations sont intimement liées aux groupes de cohomologie. Le deuxième groupe de cohomologie est le plus important, les premiers termes des déformations sont contenus dans ce groupe et sa nulité indique que l'algèbre est rigide, c'est à dire qu'elle n'admet aucune déformation non triviale. Les groupes de cohomologie sont aussi des invariants de l'algèbre. Ils permettent par exemple de distinguer deux structures algébriques. Les calculs des groupes de cohomologie sont souvent infaisables à la main, les logiciels de calcul formel permettent de surmonter cette difficulté. Le but de mon exposé est de montrer comment est utilisé le calcul formel dans l'étude des ensembles de lois d'une structure algébrique donnée.

Définitions

Afin d'alléger le résumé, on rappelle les définitions dans le cas des algèbres associatives, elles sont analogues pour les autres stuctures algébriques.

Une loi d'algèbre associative sur l'espace vectoriel C^n est une multiplication, elle est donnée par une application bilinéaire $\mu : C^n \times C^n \longrightarrow C^n$ vérifiant

$$\forall X,Y,Z \in C^n \qquad \mu(\mu(X,Y),Z) - \mu(X,\mu(Y,Z)) = 0$$

En fixant une base $\{e_i\}$ de C^n, on identifie μ à ses *constantes de structure* $(C_{ij}^k) : \mu(e_i,e_j) = \sum_{k=1}^n C_{ij}^k e_k$. Les constantes de structure des lois d'algèbres associatives vérifient le système d'équations polynomiales quadratiques suivant :

$$\sum_{l=1}^{n} C_{ij}^l C_{lk}^s - C_{il}^s C_{jk}^l = 0 \quad 1 \leq i,j,k,s \leq n. \qquad (S)$$

Ainsi, l'ensemble des lois d'algèbres associatives, noté A_n, est muni d'une structure de variété algébrique plongée dans C^{n^3}.

L'action du groupe linéaire $GL_n(C)$ sur A_n est définie par :

$$\mu \in A^n,\ f \in GL_n(C) \ : \forall X,Y \in C^n \quad (f \cdot \mu)(X,Y) = f^{-1}(\mu(f(X),f(Y)))$$

Cette action permet de fibrer la variété algébrique. L'ensemble de toutes les lois isomorphes à la loi d'algèbre μ définit l'orbite de μ notée $\vartheta(\mu)$. Deux lois d'algèbres $\mu_1$et μ_2 sont isomorphes s'il existe f de $GL_n(C)$ tel que $\mu_2 = f \cdot \mu_1$ (c'est à dire qu'elles appartiennent à une même orbite).

Une *déformation* d'une loi d'algèbre associative μ_0 sur C^{n^3} est donnée par une famille à un paramètre de lois d'algèbres $\mu_t = \sum_{i \geq 0} t^i \mu_i$ où les μ_i sont des applications bilinéaires et t est un paramètre complexe.

La cohomologie des algèbres associatives, s'appelle *cohomologie de Hochschild*, elle est définit de la manière suivante : on considère l'ensemble des applications p-linéaires sur C^n, $\Omega^p(C^n) = \{\varphi : C^n \times ... \times C^n \to C^n \ p - linéaire\}$. L'opérateur cobord de Hochschild relatif à l'algèbre μ est donné par :

$$\delta^p : \begin{array}{c} \Omega^p(C^n) \to \Omega^{p+1}(C^n) \\ \varphi \to \delta^p \varphi \end{array}$$

avec pour tout $(x_1,...,x_{p+1}) \in (C^n)^{p+1}$

$$\delta^p\varphi(x_1,...,x_{p+1}) = \mu(x_1,\varphi(x_2,...,x_{P+1})) + \sum_{i=1}^{p}(-1)^i\varphi(x_2,...,\mu(x_i,x_{i+1}),...,x_P) + (-1)^{p+1}\mu(\varphi(x_1,...,x_p),x_{p+1})$$

En identifiant les applications 0-linéaires aux éléments de l'algèbre, on définit pour tout p, $0 \leq p \leq n$, les espaces suivants :

Les espaces des cobords sont $B^p(\mu,\mu) = \{\varphi : (C^n)^p \to C^n \ / \ \varphi = \delta^{p-1}f,\ f \in \Omega^{p-1}(C^n)\}$,
les espaces des cocycles sont $Z^p(\mu,\mu) = \{\varphi : (C^n)^p \to C^n \ / \ \delta^p\varphi = 0\}$
et le $p^{ième}$ groupe de cohomologie de Hochschild est le quotient $H^p(\mu,\mu) = Z^p(\mu,\mu)/B^p(\mu,\mu)$.

Problèmes et usage du calcul formel

Un des problèmes fondamentaux concernant ces ensembles consiste à établir des classifications à isomorphisme près. Les résultats ne dépasse pas très souvent les petites dimensions à cause de la complexité des calculs. La deuxième approche est plus topologique, elle utilise les déformations et consiste à déterminer les composantes irréductibles des variétés algébriques de lois d'algèbres.

On montrera dans cet exposé comment déterminer, à l'aide du logiciel Mathematica, les composantes irréductibles des variétés algébriques des lois d'algèbres associatives. On donnera les algorithmes et les procedures qu'on illustrera en petites dimensions. Une autre application concernera les algèbres de Poisson, on construit des déformations de ces algèbres, ce qui permettra de répondre à de nombreux problèmes.

L'usage du calcul formel a permis de résoudre de nombreuses questions ouvertes dans les domaines cités ci-dessus.

Références

Gabriel P. *Finite représentation type is open.* Lecture Notes in Maths N°488, (1974).

Gerstenhaber M. *on the deformations of rings and algebras.* Annals of Math. 79, 84, 88 (1964,1966,1968)

Goze M. et Makhlouf A., *On the rigid complex associative algebras.* Communications in Algebra N18, (1990).

Goze M. et Makhlouf A. *calcul de la cohomologie de Chevalley d'une algèbre de Lie* Publication de l'IREM de Strasbourg (1988)

Mazzola G. *The algebraic and geometric classification of associative algebras of dimension five.* Manuscripta math 27, (1979).

Makhlouf A. On the irreducible component of nilpotent associative algebra, Revista Mathematica de l'Universidad complutence de Madrid, (1993).

Makhlouf A. et Goze M. *Classification of rigid associative algebras in low dimensions.* Dans lois d'algèbres et anneaux Collec. Travaux en cours Hermann (1996).

Makhlouf A., *Algèbres associatives et calcul formel,* Theoretical. Computer Science 187 (1997)

Bordemann M., Makhlouf A., Petit T., *Déformation par quantification des algèbres enveloppantes*, Arxiv (2002).

Symposium

Systèmes polynomiaux I

Organisation : Jean-Charles Faugère - projet SPACES, CNRS - Université de Paris VI - INRIA

Présentation

La résolution des systèmes algébriques est un problème fondamental du Calcul Formel. En effet de nombreux problèmes (voir en particulier les sessions "Applications du calcul formel", "Calcul Symbolique/Numérique" ou "Cryptologie") se ramènent à la résolution d'un système algébrique. Cependant la notion même de ce que l'on entend par *résoudre* un système algébrique va dépendre fortement du contexte. Ainsi la réponse à donner est totalement différente selon :

- que les données du problème sont exactes ou approchées.
- la nature des solutions recherchées: complexe, réelle, corps fini ou extension de corps.
- qu'il y a un nombre fini ou infini de solutions.
- que l'on cherche une solution particulière ou toutes les solutions.
- qu'il existe ou pas des contraintes supplémentaires (inégalités par exemple).

De plus pour chacune de ces possibilités il existe un ou plusieurs algorithmes. La résolution de systèmes polynomiaux est donc un sujet trop vaste pour être traité intégralement et cette session n'a donc pour objectif que de montrer un échantillon des nouvelles méthodes de résolution.

Lorsque les données sont exactes une méthode, parmi les plus efficaces, constitue à calculer des bases de Gröbner. Des algorithmes de plus en performants ont été proposé pour calculer des bases de Gröbner permettant de traiter des applications en vraie grandeur. C'est le cas en Cryptologie ou plusieurs cryptosystèmes peuvent être cassés par des calculs de bases de Gröbner. La particularité des systèmes algébriques en Cryptologie est qu'ils sont sur-déterminés. À noter que les systèmes sur-déterminés apparaissent aussi lorsqu'on cherche à faire de l'identification de paramètres (exposé de Daniel Lazard). Alors que les études de complexité sur les bases de Gröbner sont nombreuses lorsque le nombre d'équations est inférieur au nombres de variables, peu de résultats étaient disponibles dans le cas contraire; l'exposé de M. Bardet vient ainsi combler cette lacune. Cet exposé donne également un moyen expérimental de distinguer si un système algébrique se comporte comme un système aléatoire ou pas (a priori un système aléatoire est difficile à résoudre). C'est un problème crucial en Cryptologie.

Lorsque que les données du problème sont approchées (mesures) ou que l'on cherche les solutions dans une petite zone de l'espace des solutions les méthodes exactes peuvent devenir inefficaces et inadaptées. Les méthodes par intervalles (exposé de J.P. Merlet) peuvent alors prendre le relais.

Une autre limitation des calculs de base de Gröbner est qu'on obtient ainsi une description des *solutions complexes*, tandis que dans beaucoup d'applications pratiques on cherche uniquement les *solutions réelles*. Si le cas de la dimension zéro (nombre fini de solutions) est maintenant bien traité le cas général (avec paramètres) reste un problème difficile : des algorithmes comme la décomposition algébrique cylindrique (CAD) existe mais sont totalement impraticables sur des problèmes réalistes. Deux approches sont présentées dans cette session: E. Schost donne un algorithme et des bornes de complexité pour le calcul d'un point par composante connexe dans le cas réel; S Corvez présente une CAD spécialisée et simplifiée par des techniques d'éliminination; cet algorithme est beaucoup plus efficace que la CAD originelle et il a été appliquée avec succès pour la classification des robots cuspidaux (en dimension 3).

Le cas d'un système sur-déterminé issu de mesures approchées combinent les difficultés des trois problèmes précédents. C'est pourtant un problème récurrent lorsqu'on cherche à identifier des paramètres ou faire du calibrage (robots, vision, ...). Il est alors nécessaire (exposé de Daniel Lazard) d'utiliser plusieurs algorithmes et logiciels de résolution exacte pour d'abord montrer que la question posé à un sens (ce qui revient à montrer qu'un système algébrique avec contraintes n'admet qu'une solution) puis à dériver un algorithme de calcul numériquement stable (exposé de M Safey dans la session "Calcul Symbolique/Numérique").

Parfois on souhaite pouvoir *manipuler formellement* les solutions d'un système algébrique. Dans le cas de la dimension 0 cela revient essentiellement à manipuler les racines d'un polynôme univarié (irréductible). Alin Bostan présente ainsi un algorithme pour calculer (en particulier) la somme ou le produit de deux nombres algébriques de degré D en temps $D^2 \log(D)$. Un autre problème est de calculer dans le corps défini par *toutes* les racines d'*un* polynôme univarié : les exposés de G. Renault et S. Orange présentent des algorithmes efficaces pour calculer dans le corps de décomposition d'un polynôme sans avoir à calculer un élément primitif.

Analyse par intervalles pour la résolution de systèmes

Jean-Pierre Merlet
projet COPRIN, INRIA Sophia-Antipolis

Les méthodes d'analyse par intervalles semblent être une alternative intéressante pour la résolution pratique de système d'équations/inégalités, de part la souplesse qu'elles apportent (très peu de contraintes sur la structure des systèmes qui peuvent être traités) et le fait qu'elles permettent de focaliser la recherche de solutions dans une zone particulière. Toutefois une application brutale de la méthode "branch and bound" s'avère, en général, peu efficace. Nous montrerons comment une utilisation appropriée d'une combinaison de calcul formel/méhode d'analyse numérique permet des gains de performances très importants. Des exemples dans des domaines très divers (théorie des mécanismes, robotique, automatique, biologie) serviront à illustrer les possibilités et les limites de ces méthodes.

Complexité des systèmes algébriques aléatoires dans un corps fini

Magali Bardet
Projet SPACES
Travail en collaboration avec B. Salvy et J.-C. Faugère.

Nous nous intéressons à la complexité de la résolution d'un système d'équations algébriques avec des bases de Gröbner. Nous établissons des bornes de complexité théorique très précises pour les systèmes algébriques aléatoires dans un corps fini, en tenant compte des degrés d_i de chacune des équations initiales. En particulier nous déterminons un analogue de la borne de Macaulay sur les entiers $1 + \sum_i (d_i - 1)$ (Lazard 83) donnant le degré maximal des polynômes intervenant au cours du calcul. Ces bornes sont valides y compris lorsque le nombre d'équations m est plus grand que le nombre de variables n. On obtient un développement asymptotique de ce degré maximal en calculant des séries génératrices puis en utilisant la méthode des points cols coalescents. Par exemple dans le cas $m = 2n$ et $d_i = d$, la borne de Macaulay devient asymptotiquement $A(d)n + B(d)n^{\frac{1}{3}} + o(1)$ où $A(d)$ est un nombre algébrique et $B(d)$ s'exprime en fonction du plus grand zéro de la fonction Ai

d'Airy. Les deux premiers termes de ce développement asymptotique donnent une approximation quasi exacte de la borne de Macaulay dès que $n \geq 3$.

Ces bornes théoriques sont particulièrement utiles pour faire la distinction en pratique entre un système aléatoire (difficile) et un système provenant d'un problème cryptographique comme HFE (plus facile).

Variétés polaires pour l'étude de variétés réelles non compactes.

Éric Schost
Labratoire GAGE, École polytechnique
Ce travail a été mené en collaboration avec M. Safey el Din

Le calcul d'un point par composante connexe d'une variété algébrique réelle est un problème central pour les questions d'effectivité en géométrie réelle. Ainsi, l'étude d'un ensemble semi-algébrique, c'est-à-dire défini par des égalités et inégalités, peut-il se réduire à l'étude de variétés algébrique réelles.

De ce fait, cette question a fait l'objet de nombreuses contributions. La majeure partie des algorithmes proposés reposent sur la méthode dite des points critiques : le calcul des points critiques d'une fonction f bien choisie donne un point par composante connexe sur la variété V que l'on étudie. Les différentes approches se distinguent alors par le choix de la fonction f, les propriétés de V (compacité, lissitude), l'outil de résolution utilisé pour calculer effectivement les lieux critiques, ...

Le formalisme des variétés polaires a été introduit par Bank, Guisti, Heintz et Mbakop pour ces questions de géométrie réelle effective, pour l'étude d'une variété V supposée lisse, compacte et définie par une suite régulière. Les variétés polaires forment une famille emboîtée de lieux critiques, la dernière d'entre elles donnant les points critiques de la projection sur un axe de coordonnées. En coordonnées génériques, cette dernière variété polaire est réduite à un nombre fini de points, et rencontre toutes les composantes connexes de V, en raison de l'hypothèse de compacité.

Tester la compacité d'un ensemble algébrique réel est une question délicate. Dans cet exposé, on montre comment l'étude de la même suite de variétés polaires permet d'obtenir un point par composante connexe, même si la variété V n'est pas compacte. L'idée est la suivante : les variétés polaires représentent les lieux critiques d'une famille de projections, et ce lieu peut être vide sur une composante connexe non compacte de V. Mais dans ce cas, on montre comment l'étude des fibres de ces projections permet de donner un point sur une telle composante connexe.

On déduit de ce résultat géométrique un algorithme dont la est complexité du même ordre que celui de Bank, Guisti, Heintz et Mbakop. Le système définissant V est supposé donné en évaluation ; la complexité du calcul d'un point par composante connexe est alors polynomiale en la complexité d'évaluation du système, un degré géométrique associé à la suite des variétés polaires, et un nombre combinatoire inhérent à une description determinantielle des variétés polaires.

Utilisation d'outils de calcul formel pour classifier des mécanismes sériels à 3 degrés de liberté

Solen Corvez
projet SPACES, Université de Rennes 1

Les mécanismes sériels à trois degrés de liberté utilisés dans l'industrie ont une géométrie standard et simplifiée. Or la diversité des tâches à effectuer mène à l'étude de nouveaux mécanismes dont il est important d'étudier toutes les possibilités. Comme l'ont montré les roboticiens (travaux de P. Wenger et de J. El Omri) le comportement qualitatif de ces systèmes (possibilités de certains changements de posture) change avec les longueurs des éléments du système articulé, selon qu'il existe ou non des positions de l'espace pour lesquelles un certain polynôme du quatrième degré ait une racine triple.

Avec Fabrice Rouillier nous avons cherché à déterminer des conditions sur ces longueurs pour que le mécanisme présente ce comportement particulier appelé *comportement cuspidal*.

Notre travail, que je vais présenter lors de cet exposé, a d'abord été de modéliser le problème sous forme d'un système d'équations et d'inéquations polynomiales (à l'aide de Bases de Gröbner et de changements de variables adéquates). Puis après élimination des cas particuliers, nous avons obtenu, dans l'esprit de la décomposition algébrique cylindrique, une partition de l'espace des longueurs, telle que dans chaque cellule (de dimension maximale) le comportement d'un mécanisme soit entièrement déterminé (cuspidal ou non).

Injectivité d'applications rationnelles réelles, le cas du mélange de deux lois de probabilité gaussiennes.

Daniel Lazard
projet SPACES, INRIA

De nombreux systèmes physiques peuvent être représentés par un ensemble fini de variables d'état, qui ne sont pas directement accessibles aux mesures. Les variables mesurables sont généralement des fonctions rationnelles ou algébriques des précédentes. Le problème est alors d'inverser ces foncions pour déduire des mesures les valeurs d'état. Cette inversion ne peut se faire sans ambiguïté que s'il y a injectivité de la fonction qui associe les variables mesurées aux états. Comme cette inversion revient à résoudre un système algébrique, on ne peut espérer cette injectivité que si le nombre de variables mesurées est supérieur aux variables d'état, ce qui veut dire que le système à inverser est un système sur-déterminé, dépendant de paramètres approchés (les résultats des mesures).

Pour mettre au point des algorithmes numériquement stables pour calculer les valeurs d'état, un préalable nécessaire est donc de vérifier cette injectivité, et, éventuellement, de déterminer les situations singulières où elle n'est pas vérifiée.

Une telle situation apparaît, en statistique, quand on veut déduire des six premiers moments les cinq paramètres d'un mélange de probabilités gaussiennes (valeurs moyennes, écarts quadratiques et proportion du mélange). Nous montrons que l'application correspondante n'est pas injective d'un point de vue complexe, mais qu'elle le devient si on se restreint aux valeurs admissibles des états (variables réelles, écarts quadratiques positifs et proportion comprise entre 0 et 1). La preuve a nécessité toute la puissance des logiciels Gb et RS.

L'utilisation de cette injectivité pour élaborer un algorithme stable de résolution fait l'objet de l'exposé de Mohab Safey el Din.

Algorithmes rapides pour deux nombres algébriques

Alin Bostan
GAGE, projet Algo INRIA
Ce travail a été mené en collaboration avec P. Flajolet, B. Salvy et É. Schost.

Étant donnés deux polynômes f et g à une variable sur un corps k, on définit leur *somme composée* $f \oplus g$ et leur *produit composé* $f \otimes g$, par les formules suivantes:

$$f \oplus g = \prod_{\alpha,\beta} \big(T - (\alpha + \beta)\big) \text{ et } f \otimes g = \prod_{\alpha,\beta} (T - \alpha\beta),$$

où les produits sont pris sur toutes les racines α de f et β de g, comptées avec multiplicités.

Ces opérations se retrouvent de manière naturelle dans diverses branches des mathématiques concrètes, comme la théorie algébrique des nombres, la théorie de Galois effective, la sommation symbolique, ainsi que pour la construction des polynômes irréductible sur des corps finis et dans l'étude des suites récurrentes linéaires.

Classiquement, les polynômes $f \oplus g$ et $f \otimes g$ sont obtenus via un calcul de résultants bivariés. Nous montrons comment accélérer leur calcul, de manière à obtenir des algorithmes de complexité linéaire en le degré de la sortie, à des facteurs logarithmiques près. Nous proposons également des algorithmes pour le calcul efficace du *produit de diamant* $f \diamond g$, dont la définition généralise celle des sommes et produits composés.

Calcul efficace d'un idéal de Galois maximal

Guenael Renault
CALFOR, Université Paris VI
Travail en collaboration avec Sebastien ORANGE, Annick VALIBOUZE

Soit f un polynôme irréductible de degré n à coefficients rationnels, notons $\alpha_1, \ldots, \alpha_n$ ses racines dans une clôture algébrique de $\mathbb{Q}$. Obtenir le corps de décomposition $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ du polynôme f revient à calculer

un ensemble triangulaire séparable T de $\mathbb{Q}[x_1,\cdots,x_n]$, base de Gröbner d'un idéal maximal $\mathcal{M}$, appelé *idéal des relations* et vérifiant :

$$\mathbb{Q}(\alpha_1,\ldots,\alpha_n) \simeq \mathbb{Q}[x_1,\cdots,x_n]/\mathcal{M}.$$

L'ensemble T est calculable par factorisations successives du polynôme f dans les extensions algébriques $\mathbb{Q}(\alpha_1)$,$\mathbb{Q}(\alpha_1,\alpha_2),\cdots,\mathbb{Q}(\alpha_1,\alpha_2,\cdots,\alpha_n)$. Lorsque l'ordre du groupe de Galois de f est élevé les dernières étapes sont coûteuses et l'algorithme se montre impraticable dans ce cas.

Une autre méthode, proposée par *A. Valibouze* en 1999, est de construire récursivement une chaîne strictement ascendante d'idéaux (triangulaires) dits de *Galois* :

$$I_1 \subset I_2 \subset \cdots \subset I_r = \mathcal{M}$$

Dans cette méthode le calcul de I_n à partir I_{n-1} est d'autant plus couteux que $Card(V(I_{n-1}))$ est grand. En toute généralité I_1 est égal à l'idéal $\mathcal{S}$ des relations symétriques entre les racines du polynôme f. Dans ce cas, $Card(V(I_1)) = n!$ et se sont les premières étapes qui sont les plus coûteuses.

Dans cet exposé nous montrerons comment les premières étapes de la première méthode permettent de construire rapidement un idéal I_1 contenant strictement $\mathcal{S}$. Cet idéal sera alors l'idéal de départ de la seconde méthode. Nous construisons ainsi de manière efficace le corps de décomposition de f.

Calcul du groupe de décomposition d'un idéal triangulaire en dimension 0

Sébastien Orange
CALFOR, Université Paris VI
Travail en collaboration avec Inès ABDELJAOUAD, Guenael RENAULT, Annick VALIBOUZE

Le groupe de décomposition d'un idéal de $k[x_1,\ldots,x_n]$ est l'ensemble des permutations de $x_1,\ldots,x_n$ qui laissent globalement invariant cet idéal.

Nous présenterons un algorithme efficace du calcul du groupe de décomposition d'un idéal engendré par un ensemble triangulaire et nous appliquerons nos résultats aux idéaux de Galois pour le calcul du corps de décomposition d'un polynôme univarié.

Cet exposé sera illustré par des exemples.

Symposium

Systèmes polynomiaux II

Organisation : Bernard Mourrain - projet GALAAD, INRIA Sophian-Antipolis

Présentation

Polynômes multisymétriques des racines de systèmes d'équations polynomiales multivariés

Emmanuel Briand
IGM, Université de Marne-la-Vallée

Soit P un polynôme univarié unitaire de degré n. Les polynômes symétriques en ses n racines sont des polynômes en ses coefficients. On peut aussi définir des polynômes symétriques de n points d'un espace affine de dimension supérieure. Nous considérons, pour certaines familles de systèmes d'équations polynomiales avec un nombre fini, déterminé, n, de racines, les relations entre les coefficients des systèmes et les polynômes symétriques des n racines.

Règle de Descartes, racines virtuelles et polynômes de Bernstein

Marie-Francoise Coste-Roy
IRMAR, Université de Rennes 1

Le théorème des zéros: programmes d'évaluation,degrés et hauteurs

Thérésa Krick
Université de Limoges

Le théorème des zéros est un résultat central en géométrie algébrique. Sous une forme simplifiée son énoncé est le suivant:

Soient $f_1,\ldots,f_s \in \mathbb{Z}[x_1,\ldots,x_n]$ *des polynômes tels que le système d'équations*

$$f_1(x)=0,\ldots,f_s(x)=0$$

n'a aucune solution dans $\mathbb{C}^n$. *Alors il existe* $a \in \mathbb{N}\setminus\{0\}$ *et* $g_1,\ldots,g_s \in \mathbb{Z}[x_1,\ldots,x_n]$ *satisfaisant l'identité de Bézout*

$$a = g_1\,f_1+\cdots+g_s\,f_s. \tag{12.1}$$

Comme beaucoup de résultats en géométrie algébrique et en algèbre commutative, ceci est un énoncé d'existence non effectif. L'estimation des degrés et des hauteurs (maximum des valeurs absolues des coefficients) de polynômes satisfaisant une identité (12.1) est devenue une question largement considérée: des versions effectives du théorème s'appliquent en informatique théorique et en théorie des nombres, en particular, elles décident de la consistance d'un système d'équations donné et sous leur présentation arithmétique elles s'appliquent à des inégalités de Lojasiewicz et à des problèmes de consistance sur des corps finis.

Dans cet exposé on donnera d'abord un aperçu de l'historique du sujet, puis on montrera comment la recherche d'un théorème des zéros effectif du point de vue non traditionnel des programmes d'évaluation permet d'aboutir à un algorithme qui produit une constante a et des polynômes g_i dans une identité de Bézout (12.1) qui vérifient des bornes pour les hauteurs qui sont optimales (et n'avaient pu être obtenues jusque là) alors que les bornes pour les degrés sont comparables aux bornes optimales connues. L'exposé est basé sur un travail en commun avec Martín Sombra et Luis Miguel Pardo.

Méthodes de Weierstrass multivariées

Olivier Ruatta
Université de Pise

La méthode de Weiertrass est une méthode itérative pour le calcul simultané de toutes les solutions d'un système algébrique. Nous montrons comment construire la fonction d'itération dans le cas multivarié. Ensuite nous utilisons cette fonction d'itération comme opérateur de correction dans un processus de suivit de chemin. On obtient un méthode globale, mais dans un context géométrique trop restreint. Cela nous conduit à définir une fonction d'itération pour des systèmes surcontraints. On obtient ainsi une méthode localement quadratiquement convergente. Nous expliquons ensuite nos travaux en cours pour obtenir une méthode globale dans le cas surcontraint.

Hauteur des solutions d'un systeme polynomial

Martin Sombra
Université de Paris VII

Soit $\mathcal{A} := \{a_0,\ldots a_N\} \subset \mathbb{Z}^n$ un ensemble fini de vecteurs entiers. On calcule les minima successifs de la variété torique projective $X_{\mathcal{A}} \subset \mathbb{P}^n$. En utilisant le travail de S. Zhang sur la conjecture de Bogomolov [1], on obtient une estimation pour la hauteur de $X_{\mathcal{A}}$.

Cette estimation nous permet de démontrer l'analogie arithmétique du théorème de Bernstein-Kushnirenko:

Soient $f_1,\ldots,f_n \in \mathbb{Z}[x_1^{\pm1},\ldots,x_n^{\pm1}]$ des polynôems de Laurent à coefficients entiers. Soit $Q_0 \subset \mathbb{R}^n$ un polytope rationnel,e t soit $\mathbb{Q}_i := NP(f_i) \subset \mathbb{R}^n$ le polytope de Nexton de f_i pour $i=1,\ldots,n$. Soit $V(f_1,\ldots,f_n)_0$ l'ensemble des points isolés de $V(f_1,\ldots,f_n) \subset (\mathbb{C}^*)^n$.

Alors:

$$\hat{h}_{Q_0}(V(f_1,\ldots,f_n))_0) \leq \sum_{i=1}^{n} MV(Q_0,\ldots,Q_i,Q_{i+1}\ldots,Q_n)h_1(f_i)$$

Ici, on note $\hat{h}_{Q_0}$ la hauteur induite par l'inclusion $(\mathbb{C}^*)^n \hookrightarrow \bigoplus_{a\in\mathcal{A}}\mathbb{C}^*$, où $\mathcal{A} := Q\bigcap\mathbb{Z}^n$. La hauteur d'un polynôme de Laurent $f=\sum_{a\in\mathcal{A}}$ se définit comme le log de sa 1-norme, c.à.d. $h_1(f) := log||f||_1 = log(\sum_{a\in\mathcal{A}}|f_a|)$.

Ce résultat montre que la bit-complexité de l'ensemble des solutions d'un système d'équations creux est contrôlé par les volumes mixtes des polytopes qui interviennent.

Réferences :

[1] S. Zhang, *Positive line bundles on arithmetic varieties.* J. Amer. Soc. vol. 8 (1995), 187-221

Forme normale et résolution de systemes polynomiaux

Philippe Trébuchet
projet SPACES, CNRS, INRIA, Université de Paris VI

Les systèmes polynomiaux se retrouvent dans de très nombreuses applications industrielles. Ils sont aussi au centre de la géométrie algébrique effective. Un outil important pour leur étude est le calcul de bases de Grœbner. La connaissance de cette base particulière de l'idéal engendré par les polynômes qui composent le système permet de mener des calculs dans l'algèbre quotient $A = \mathbb{K}[x_1 \dots x_n]/I$, ingrédient fondamental lorsque l'on cherche à résoudre. Néanmoins les calculs de bases de Grœbner reposent de manière fondamentale sur la notion d'ordre monomial. Ceci induit une certaine rigidité dans les calculs et une instabilité numérique artificielle. Nous proposons un nouvel algorithme qui permet de remédier à cela. Il généralise les constructions de bases de Grœbner tout en étant moins sensible aux perturbations numériques. Pour ce faire, nous affaiblissons le pré-requis d'ordre monomial et utilisons un nouveau critère de formes normales. Nous donnons ensuite un algorithme et prouvons sa correction lorsque le système de départ est de dimension 0. Ensuite nous comparons notre algorithme avec ceux déjà proposés, et montrons comment il peut en être vu comme une généralisation. Nous détaillons alors comment nous avons implémenté notre algorithme en C++ en utilisant la bibliothèque SYNAPS. Nous décrivons également l'algorithme d'élimination sur les matrices creuses que nous utilisons dans notre programme. Enfin, nous presentons les expérimentations notre programme sur des applications pratiques telles que la vision artificielle, la géométrie algorithmique, la robotique, ou la pharmacologie et nous donnons dans un dernier chapitre le compte-rendu de nos expériences.

Symposium

Fonctions spéciales et finitude différentielle

Organisation : Bruno Salvy - projet ALGO, INRIA Rocquencourt

Introduction aux fonctions D-finies

Bruno Salvy
INRIA Rocquencourt

Les équations différentielles linéaires peuvent être vues comme une structure de donnée pour représenter leurs solutions (les fonctions différentiellement finies ou D-finies), de la même manière que les polynômes univariés permettent le calcul sur des nombres algébriques. Ce point de vue permet de doter de nombreuses fonctions spéciales d'un statut d'objets a part entière du calcul formel (voir l'expose de Ludovic Meunier). L'algorithmique de ces objets dans le cas univarié repose essentiellement sur de l'algèbre linéaire, qui peut se voir comme une extension au cas non commutatif des calculs reposant sur la matrice de Sylvester. Des algorithmes plus rapides sont également en cours de développement, et certains d'entre eux seront présentés dans l'expose d'Alin Bostan. Ce point de vue s'étend au cas multivarié, qui permet de traiter non seulement des fonctions multivariées, mais aussi des familles de fonctions ou de polynômes. Des exemples typiques sont les familles de polynômes orthogonaux classiques ou les fonctions hypergéométriques avec leurs relations de contiguïté. L'algorithmique dans ce cas repose sur des bases de Groebner non-commutatives. Une nouvelle opération très intéressante apparaît en multivarié: le "télescopage créatif", qui permet de calculer des sommes ou des intégrales définies. Nous décrirons des algorithmes permettant d'effectuer cette opération. Enfin, l'extension du cadre D-fini aux fonctions symétriques (c'est-a-dire en quelque sorte le pendant en une infinité de variables de ces notions) fait l'objet de l'expose de Frédéric Chyzak.

The encyclopedia of special functions

Ludovic Meunier
INRIA Rocquencourt

Nous décrivons notre travail en cours sur la production automatique d'une encyclopédie de fonctions spéciales, appelée ESF (http://algo.inria.fr/esf). En exploitant une collection d'algorithmes de calcul formel de manière systématique, nous synthétisons des pages web sur les fonctions spéciales de manière automatique et fournissons un certain niveau d'interactivité.

Algorithmes pour les opérateurs différentiels linéaires

Alin Bostan
laboratoire GAGE

En calcul formel, un grand nombre d'algorithmes sont bases sur la technique d'évaluation-interpolation des polynômes sur un ensemble de points, éléments du corps des coefficients. L'objectif de cet expose est de montrer comment ces techniques, ayant de fortes conséquences en termes d'efficacité algorithmique, peuvent être étendues au cadre non-commutatif des opérateurs différentiels linéaires, nécessaire pour les application aux fonctions spéciales. Dans ce contexte, les "points" sont des series solutions des opérateurs manipules et l'interpolation est faite via des "approximants de Padé-Hermite différentiels". La complexité des algorithmes obtenus repose sur le calcul efficace de ces approximants. Nous proposons plusieurs méthodes pour ce calcul, estimons leur coût et donnons diverses applications au calcul des produits symétriques, des ppcm et des pgcd d'opérateurs différentiels linéaires.

Calcul effectif de fonctions symétriques D-finies

Frédéric Chyzak
Inria Rocquencourt

De nombreuses séries génératrices de la combinatoire s'expriment en termes de fonctions symétriques. Gessel a décrit une grande classe de fonctions symétriques pour lesquelles les séries génératrices extraites sont différentiellement finies (ou D-finies). Nous étendons ce travail de Gessel en donnant des algorithmes qui calculent des équations différentielles satisfaites par ces séries génératrices. Nous donnons des exemples d'application aux graphes k-réguliers et aux tableaux de Young avec entrées répétées.

Symposium

Théorie algorithmique des nombres

Organisation : Karim Belabas - Université de Paris XI

Présentation

La théorie algorithmique des nombres couvre un large spectre : de la théorie élémentaire des nombres (primalité, factorisation), à la géométrie arithmétique (points rationnels des variétés algébriques), en passant par la théorie algébrique des nombres (extensions finies de $\mathbb{Q}$, de $\mathbb{F}_q[T]$, corps locaux, théorie de Galois), et la théorie des formes modulaires ou automorphes (calcul de bases, identification de valeurs spéciales).

Les liens avec les thèmes développés dans les autres sessions de ces journées sont nombreux : *algèbre linéaire* (élimination structurée de matrices de relations pour les problème de log discret ou de factorisation sur $\mathbb{Z}$, ou bien en théorie algébrique des nombres), *calcul symbolique/numérique* et *fonctions spéciales* (calculs sur les plongements en théorie algébrique des nombres, de hauteurs en géométrie arithmétique, valeurs spéciales de fonctions L), *systèmes polynomiaux* (représentations utilisables des variétés algébriques, calculs effectifs sur les groupes de diviseurs), et *cryptographie* bien sûr. Ces liens sont loin d'être à sens unique : la factorisation sur $\mathbb{Z}$ ou sur $\mathbb{Q}[X]$, les calculs sur les corps finis ou les extensions de $\mathbb{Q}_p$ sont des préliminaires indispensables à bien des algorithmes.

Les problèmes traités sont en général du type suivant : calculer un objet de la théorie des nombres, souvent muni de structures algébriques, dans une représentation concrètement utilisable; par exemple, un groupe abélien de type fini se décrit par un système minimal de générateurs, à condition de donner des algorithmes de «logarithme discret» pour exprimer un élément arbitraire sur cette base. Une variante consiste à énumérer les objets de «taille» bornée, de façon à ce que leur nombre soit fini; on exige leur liste, ou bien on se contente éventuellement de son cardinal, voire d'une évaluation asymptotique – on s'éloigne alors du calcul formel pour se rapprocher de la combinatoire ou de la théorie analytique des nombres, disciplines au demeurant cruciales pour l'évaluation de la complexité des algorithmes.

Les exposés de cette session se rattachent tous à ce type de question : directement en ce qui concerne Bill Allombert, Henri Cohen et David Lubicz (respectivement dans les cadres corps finis, corps de nombres, et courbe elliptique sur $\mathbb{F}_q$), dans la variante énumération asymptotique pour Jean-Louis Nicolas, et de façon indirecte pour Jean-François Mestre qui présente un algorithme de calcul de la «taille» d'un point rationnel d'une courbe elliptique (ou de variétés abéliennes plus générales), plus précisément de sa composante archimédienne.

Détermination pratique de polynômes irréductibles sur $\mathbb{F}_p$

Bill Allombert
LORIA, Nancy

Les corps finis, étudiés initialement par E. Galois, jouent un rôle central en Mathématiques, en cryptographie et en arithmétique des ordinateurs. La représentation effective et le calcul algorithmique dans le corps fini $\mathbb{F}_{p^n}$ requiert le calcul d'un polynôme de degré n, irréductible modulo p. Différent algorithmes ont été proposés :

- Tirer un polynôme de degré n au hasard et tester son irréductibilité. En moyenne, un polynôme irréductible sur $\mathbb{F}_p$ est obtenu au bout d'environ n tirages. Ce procédé était connu de Galois, mais de nombreux auteurs ont amélioré le test d'irréductibilité.
- L'utilisation de sous-extensions d'extensions cyclotomiques de degrés premiers. Si l'on admet l'hypothèse de Riemann généralisée, il suffit de calculer dans une extension de degré au plus $O(n\log(n)^{4+\varepsilon})$, d'après la majoration de Lagarias-Odlyzko. Cet algorithme est dû à L. Adleman et H. Lenstra.
- L'utilisation de la théorie de Kummer. C'est une théorie générale pour la construction des extension cycliques des corps. Cette méthode, proposée par V. Shoup, requiert le calcul dans une extension de degré au plus $n-1$.

Je propose une modification de l'algorithme d'Adleman-Lenstra qui remplace le calcul dans une extension de grand degré par un calcul modulo un grand entier dont la taille ne dépend pas de p. En pratique cette approche semble supérieure, même pour des valeurs modestes de p.

Énumération des extensions A_4 de $\mathbb{Q}$

Henri Cohen
Université de Bordeaux I

À tout corps de nombres K (extension finie de $\mathbb{Q}$), on associe son discriminant $\mathrm{disc}(K)$. C'est un entier non nul et le nombre de corps de nombres $K \subset \mathbb{C}$ de discriminant fixé est fini (Hermite). Pour une borne X donnée se pose alors la question de compter les corps K tels que $|\mathrm{disc}(K)| \leq X$, voire de les exhiber. Par exemple, le seul corps de discriminant 1 est $\mathbb{Q}$ (Minkowski), il n'y a pas de corps de discriminant 2, etc.

En fait, il est plus agréable de classer les corps par familles, par exemple suivant leur degré et le type de leur clôture galoisienne. Nous montrons comment la théorie du corps de classe des corps cubiques cycliques et de leurs caractères associés permet d'énumérer efficacement les extensions A_4 de $\mathbb{Q}$ (nous atteignons $X = 10^{16}$). Le calcul de logarithmes discrets dans des groupes relativement petits joue aussi un rôle.

Sur le calcul de cardinalité de courbes hyperelliptiques définies sur un corps fini de petite caractéristique

David Lubicz
CELAR, Rennes

Un pré-requis à l'utilisation des courbes elliptiques définies sur un corps fini en cryptographie est de disposer d'algorithmes efficaces pour en compter le nombre de points rationnels. Soit p un nombre premier, $n \in \mathbb{N}$, $q = p^n$ et E une courbe elliptique donnée définie sur $\mathbb{F}_q$; le précédent problème est équivalent au calcul de la trace du Frobenius à la puissance n puisque $\#E(\mathbb{F}_q) = 1 + q - \mathrm{Tr}(\mathrm{Fr}_q)$.

Dans cet exposé, p est *petit*, et nous présentons un algorithme qui évalue le j-invariant du relevé canonique de E en $O(\log n)$ opérations élémentaires, le temps nécessaire pour calculer une puissance du relevé du Frobenius. Cet algorithme ne nécessite pas de pré-calcul. Soit alors μ la constante telle que le produit de deux entiers de n bits se fasse en $O(n^\mu)$ opérations élémentaires, cela donne un algorithme pour calculer le nombre de points d'une courbe elliptique dont la complexité en temps est en $O(\log(n)n^{2\mu+\frac{1}{2}})$ et $O(n^{\frac{5}{2}})$ en espace. Dans le cas où le corps de base admet une base Gaussienne optimale, nous obtenons un algorithme de complexité $O(\log(n)n^{2\mu})$ en temps et $O(n^2)$ en espace. D'un point de vue pratique, cet algorithme s'avère relativement aisé à implémenter.

Algorithmes quadratiquement convergents de calcul de la hauteur sur une courbe elliptique, et de la capacité de l'union de deux intervalles

Jean-François Mestre
En collaboration avec Jean-Benoît Bost.
Université de Paris VII

Nous décrivons un algorithme quadratiquement convergent pour calculer la hauteur archimédienne d'un point sur une courbe elliptique réelle, ainsi qu'un algorithme quadratiquement convergent pour calculer la capacité de l'union de deux intervalles de la droite réelle. Nous montrons le lien entre les deux notions, et les généralisons en reliant le calcul de la capacité de l'union de $g+1$ intervalles réels à celui de la hauteur de certains points de la jacobienne des courbes hyperelliptiques réelles de genre g.

Sur le nombre de solutions de l'équation diophantienne $A^2 + B^2 = C^2 + C$ avec le même nombre de chiffres binaires

Jean-Louis Nicolas
Université de Lyon I

Soit $Q(N)$ le nombre de solutions de l'équation diophantienne

$$A^2 + B^2 = C^2 + C$$

vérifiant

$$N \leq A \leq B \leq C < 2N.$$

On a

$$\lim_{N\to\infty} \frac{Q(N)}{N} = \frac{1}{6} - \frac{\log(2+\sqrt{3})}{\pi} + \frac{\log(1+\sqrt{2})}{\pi} = 0.02801587455727\ldots$$

La méthode de démonstration utilise les séries de Fourier et les sommes de Kloostermann.

Annexes

Emploi du temps

```
Lundi 20 janvier
----------------

9h00           Accueil des participants.
9h15-12h45     MS   : Équations différentielles I : résolution.
14h30-15h30    PLEN : Michel Petitot
16h-19h30      MS   : Contrôlabilité

Mardi 21 janvier
----------------

9h-10h         PLEN : François Morain
10h30-12h30    MS   : Équations différentielles II : autre point de vue
               //
               MS   : Théorie algorithmique des nombres
14h30-15h30    MS   : Équations différentielles II : autre point de vue (fin)
               //
               MS   : Théorie algorithmique des nombres (fin)
16h-19h30      MS   : Cryptologie
               //
               MS   : Calcul symbolique-numérique.

Mercredi 22 janvier
-------------------

9h-12h30       MS   : Fonctions spéciales et holonomie
               //
               MS   : Applications du calcul formel.
14h-15h        PLEN : Jean-Claude Yakoubsohn

Jeudi 23 janvier
----------------

9h-12h30       MS   : Systèmes polynomiaux I
               //
               MS   : Session ouverte
14h30 - 15h30  PLEN : Jean-Daniel Boissonnat
```

```
16h-19h30      MS   : Algèbre linéaire
               //
               MS   : Algorithmique géométrique.

Vendredi 24 janvier
-------------------

9h-12h30       MS   : Systèmes polynomiaux II
14h-15h        PLEN : Gilles Villard
```

Liste des participants


```
Jounaidi ABDELJAOUED, Université de Tunis
E.S.S.T.T 5, Avenue Taha Hussein, 1008 TUNIS, TUNISIE
jounaidi@esstt.rnu.tn

Bill ALLOMBERT, INRIA Lorraine
LORIA 615, rue du jardin botanique, 54602 Villers-les -Nancy, FRANCE
allomber@loria.fr

Gwénolé ARS, IRMAR
Tour des Mathématiques Campus de Beaulieu Université de Rennes 1 , 35042 Rennes, FRANCE
ars@math.univ-rennes1.fr

Dominique ATTALI, Laboratoire LIS
ENSIEG, Domaine Universitaire BP 46, 38402 Saint Martin d'Heres Cedex, FRANCE
Dominique.Attali@inpg.fr

Daniel AUGOT, INRIA Rocquencourt
Domaine de Voluceau, 78153 Le CHesnay CEDEX, FRANCE
Daniel.Augot@inria.fr

Magali BARDET, Univ. Paris 6
8 rue du capitaine scott, 75015 PARIS, FRANCE
bardet@calfor.lip6.fr

Abdolali BASIRI,
8, rue de capitain scott, 75015 Paris, FRANCE
basiri@calfor.lip6.fr

Karim BELABAS, Univ Paris 11
Universite Pari-Sud Departement de Mathematique (bat 425) , 91405 Orsay, FRANCE
Karim.Belabas@math.u-psud.fr

Jean-Daniel BOISSONNAT, INRIA
2004 Route des Lucioles BP 93, 06902 Sophia-Antipolis, FRANCE
Jean-Daniel.Boissonnat@sophia.inria.fr

Alin BOSTAN, Ecole polytechnique
Laboratoire GAGE, Ecole polytechnique, , 91128 Palaiseau, FRANCE
bostan@gage.polytechnique.fr

Delphine BOUCHER, Universite Rennes
Université de Rennes I UFR Mathématiques, IRMAR Campus de Beaulieu, 35042 Rennes, FRANCE
delphine.boucher@univ-rennes1.fr

Francois BOULIER, LIFL - Univ. Lille I
LIFL - USTL 59655 Villeneuve d'Ascq CEDEX, 59655 Villeneuve d'Ascq, FRANCE
boulier@lifl.fr
```

Emmanuel BRIAND, IGM, Univ. Marne-la-Vallée
IGM, Laboratoire d'informatique, Université de Marne-la-Vallée,
77454 Champs-sur-Marne, FRANCE
ebriand@monge.univ-mlv.fr

Nicolas BRISEBARRE, ENS-Lyon
46, Allée d'Italie, 69364 Lyon, FRANCE
nbriseba@ens-lyon.fr

Manuel BRONSTEIN, INRIA
INRIA - Projet CAFE 2004 route des Lucioles - B.P. 93, 06902 Sophia Antipolis, FRANCE
Manuel.Bronstein@sophia.inria.fr

Guillaume CHEZE, Univ. Nice Sophia-Antipolis
Parc Valrose, 06108 Nice, FRANCE
cheze@math.unice.fr

Frédéric CHYZAK, Inria
(Projet Algorithmes) Inria-Rocquencourt, 78153 Le Chesnay, FRANCE
frederic.chyzak@inria.fr

Henri COHEN, Universite Bordeaux I
Laboratoire A2X, Universite Bordeaux I 351 Cours de la Liberation,
33405 Ce Talence, FRANCE
cohen@math.u-bordeaux.fr

Eric COLIN DE VERDIERE, ENS Paris
45, rue d'Ulm, 75005 Paris, FRANCE
Eric.Colin.de.Verdiere@ens.fr

Elie COMPOINT, Univ.Lille1
Universite Lille1 UFR de Mathematiques, 59655 Villeneuve d ascq, FRANCE
compoint@agat.univ-lille1.fr

Olivier CORMIER, Universite de Paderborn
FB17 - MuPAD Gruppe Universität Paderborn, 33095 Paderborn, ALLEMAGNE
cormier@math.uni-paderborn.de

Solen CORVEZ, Univ. Rennes I
IRMAR Campus de Beaulieu, 35042 Rennes, FRANCE
scorvez@math.univ-rennes1.fr

David DANEY, INRIA Sophia Antipolis
2004 Route des Lucioles, BP 93 06902 Sophia Antipolis Cedex, France,
06902 Sophia Antipolis, FRANCE
David.Daney@sophia.inria.fr

Gabriel DOS REIS, INRIA Sophia Antipolis
2004 route des luciolesBP 93, 06902 Sophia Antipolis, FRANCE
Gabriel.Dos_Reis@sophia.inria.fr

Gérard DUCHAMP, LIFAR, Univ. Rouen
Place Emile Blondel, 76821 Mont-Saint-Aignan, FRANCE
gerard.duchamp@univ-rouen.fr

Jean-Guillaume DUMAS, Univ. Joseph Fourier, Grenoble
Lab. de Modélisation et Calcul 51, avenue des Mathématiques IMAG -- BP53 X,
38041 Grenoble, FRANCE
Jean-Guillaume.Dumas@imag.fr

Philippe ELBAZ-VINCENT, Univ. Montpellier 2
GTA UMR CNRS 5030 U. Montpellier 2 CC51 , 34095 Montpellier, FRANCE
pev@math.univ-montp2.fr

Jean-Charles FAUGERE, CNRS
8 rue du Capitaine Scottt , 75015 Paris, FRANCE
jcf@calfor.lip6.fr

Michel FLIESS, CMLA, ENS-Cachan
61, av. du Président Wilson , 94235 Cachan, FRANCE
fliess@cmla.ens-cachan.fr

Mikhail FOURSOV, Universite de Rennes-I
IRISA, Campus Universitaire de Beaulieu, 35042 Rennes Cedex, FRANCE
foursov@irisa.fr

Philippe GAILLARD, Universite de Rennes I
IRMAR Campus de Beaulieu 35042 RENNES Cedex, 35042 RENNES, FRANCE
philippe.gaillard@math.univ-rennes1.fr

ANDRE GALLIGO, Universite de NICE (UNSA)
Laboratoire de Mathematiques Parc Valrose, 06108 NICE, cedex 02, FRANCE
galligo@unice.fr

Pierrick GAUDRY, Ecole polytechnique
LIX Ecole polytechnique, 91128 Palaiseau, FRANCE
gaudry@lix.polytechnique.fr

Pascal GIORGI, ENS Lyon
LIP 46 Allée d'Italie , 69364 Lyon, FRANCE
pascal.giorgi@ens-lyon.fr

Marc GIUSTI, CNRS-Polytechnique
Laboratoire GAGE Ecole polytechnique, 91128 Palaiseau CEDEX, FRANCE
marc.giusti@gage.polytechnique.fr

Hatem HADJ KACEM, Univ. Rouen
LIFAR, Faculté des Sciences et techniques, 76821 Mont-Saint-Aignan, FRANCE
hatem.hadj-kacem@univ-rouen.fr

Guillaume HANROT, INRIA
LORIA 615, rue du jardin botanique , F-54602 Villers-les-Nancy Cedex, FRANCE
hanrot@loria.fr

HOANG NGOC MINH,
Universite Lille 2 Place Deliot., 59024 Lille, FRANCE
hoang@lifl.fr

Vincent HOUSEAUX, LIFL - Univ. Lille I
LIFL - USTL 59655 Villeneuve d'Ascq CEDEX, 59655 Villeneuve d'Ascq, FRANCE
houseaux@lifl.fr

Luc JAULIN, LISA
LISA, 49000 Angers, FRANCE
jaulin@univ-angers.fr

Claude-pierre JEANNEROD, ENS Lyon
LIP 46 Allee d'Italie , 69364 Lyon, FRANCE
claude-pierre.jeannerod@ens-lyon.fr

Teresa KRICK, Univ. Limoges
LACO 123 Av. Albert Thomas, 87060 Limoges, FRANCE
teresa.krick@unilim.fr

Éric LAUGEROTTE, LIFAR
Faculté des Sciences et des Techniques Place Émile Blondel,

76821 Mont-Saint-Aignan, FRANCE
Eric.Laugerotte@univ-rouen.fr

Daniel LAZARD, Univ. Paris 6
8 rue du Capitaine Scott , 75015 Paris, FRANCE
Daniel.Lazard@lip6.fr

Nicolas LE ROUX, LACO,universite de Limoges
123 avenue Albert Thomas , 87060 CE LIMOGES, FRANCE
nicolas.leroux@unilim.fr

Grégoire LECERF, Université de Versailles St-Qu
LAMA UMR 8100 CNRS Bâtiment Fermat 45, avenue des Etats-Unis, 78035 Versailles, FRANCE
lecerf@math.uvsq.fr

David LUBICZ, Celar
Celar, 35174 Bruz, FRANCE
lubicz@celar.fr

Abdenacer MAKHLOUF, Université de Haute Alsace
Labo de Math 4, rue des frères Lumière, 68093 Mulhouse cedex, FRANCE
N.Makhlouf@uha.fr

Jean-Pierre MERLET, INRIA
2004 route des Lucioles, 06902 Sophia-Antipolis, FRANCE
Jean-Pierre.Merlet@sophia.inria.fr

Jean-Francois MESTRE, paris 7
Universite Paris 7, 2 place Jussieu, 75005 paris, FRANCE
mestre@math.jussieu.fr

Ludovic MEUNIER, INRIA
Projet Algo, INRIA Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay, FRANCE
ludovic.meunier@inria.fr

Franck MICHEL, Université Aix-Marseille III
Lab. de Mathématiques Appliquées 15-19 Allée Claude Forbin,
13627 Aix-en-Provence Cedex 1, FRANCE
Franck.Michel@univ.u-3mrs.fr

Francois MORAIN, Ecole polytechnique
LIX, Ecole polytechnique , 91128 Palaiseau, FRANCE
morain@lix.polytechnique.fr

Bernard MOURRAIN, INRIA
BP 92, 06902 Sophia Antipolis, FRANCE
mourrain@sophia.inria.fr

Sylvain NEUT, LIFL - Univ. Lille I
LIFL - USTL 59655 Villeneuve d'Ascq CEDEX, 59655 Villeneuve d'Ascq, FRANCE
neut@lifl.fr

Jean-Louis NICOLAS, Professeur Emerite a l'Univers
IGD, UMR 5028, Mathematiques Universite Lyon 1, 69622 Villeurbanne, FRANCE
jlnicola@in2p3.fr

Francois OLLIVIER, CNRS
GAGE Ecole polytechnique, 91128 Palaiseau, FRANCE
francois.ollivier@gage.polytecnique.fr

Shea Ming OON, Université Nancy 1
IECNUniversité Nancy 1,BP 239, 54506 Vandoeuvre, FRANCE
oon@iecn.u-nancy.fr

Sébastien ORANGE, Université Paris 6
8, rue du Capitaine Scott, 75015 PARIS, FRANCE
orange@worldonline.fr

Luis M. PARDO,
Depto. de Matematicas, E. y C. Facultad de Ciencias Universidad de Cantabria Avda.
Los Castros s/n, 39071 Santander, ESPAGNE
pardo@matesco.unican.es

Lancelot PECQUET, Univ. Paris 12
87, Quai de la Gare, 75013 Paris, FRANCE
Lancelot.Pecquet@inria.fr

Michel PETITOT, Univ. Lille I, LIFL
Universite Lille I LIFL, Bat M3, 3eme etage, 59655 Villeneuve-d'Ascq, FRANCE
petitot@lifl.fr

Michel POCCHIOLA, ENS-Paris
Dept. Informatique Ecole Nornmale Superieure 45 rue d'ulm, 75230 Paris, FRANCE
Michel.Pocchiola@ens.fr

Alban QUADRAT, INRIA Sophia Antipolis
Projet CAFE, 2004 route des lucioles, BP 93, 06902 Sophia Antipolis cedex, FRANCE
Alban.Quadrat@sophia.inria.fr

Olivier RAMARE, CNRS lille
Laboratoire agat universite Lille 1, 59655 villeneuve d'ascq, FRANCE
ramare@agat.univ-lille1.fr

Guénaël RENAULT, Univ. Paris 6
LIP6 (Po^le MFI) 8 rue du Capitaine Scott, 75015 Paris, FRANCE
renault@calfor.lip6.fr

Joël RIVAT, Université Nancy 1
IECN Université Nancy 1BP239, 54506 Vandoeuvre, FRANCE
rivat@iecn.u-nancy.fr

Fabrice ROUILLIER, INRIA Lorraine
Equipe CALFOR et Projet SPACES, LIP6, 8,rue du capitaine Scott, 75015 Paris, FRANCE
Fabrice.Rouillier@loria.fr

Marie-Francoise ROY, Univ. Rennes I
IRMAR Campus de Beaulieu, 35042 Rennes CEDEX, FRANCE
Marie-Francoise.Roy@univ-rennes1.fr

Olivier RUATTA, université de Pise (Italie)
Les Lavandes E 139 avenue Maurice Jean-pierre, 06110 Le Cannet, FRANCE
oruatta@free.fr

Mohab SAFEY EL DIN, Univ. Paris 6
LIP6 8, rue du Capitaine Scott, 75015 Paris, FRANCE
Mohab.Safey@lip6.fr

Bruno SALVY, Inria
Projet Algorithmes Inria Rocquencourt, 78153 Le Chesnay, FRANCE
Bruno.Salvy@inria.fr

Eric SCHOST, Ecole polytechnique
Laboratoire GAGE, Ecole polytechnique, 91128 Palaiseau, FRANCE
Eric.Schost@polytechnique.fr

Alexandre SEDOGLAVIC, Univ. Lille I

Bat M3 LIFL Univ. Science et Tech. de Lille, 59655 Villeneuve d'ascq cedex, FRANCE
Alexandre.Sedoglavic@polytechnique.fr

Nicolas SENDRIER, INRIA Rocquencourt
INRIA Rocquencourt Domaine de Voluceau, B.P. 105, 78153 Le Chesnay Cedex, FRANCE
Nicolas.Sendrier@inria.fr

Fabien SEYFERT, Inria Sophia-Antipolis
Inria 2004 route des Lucioles BP 93, 06902 Sophia-Antipolis, FRANCE
fabien.seyfert@sophia.inria.fr

Patrick SOLE, CNRS, I3S
ESSI, Route des Colles, 06903 Sophia Antipolis, FRANCE
ps@essi.fr

Martin SOMBRA, Univ. Paris 7
Universite de Paris 7 UFR de Mathematiques Equipe Geometrie et Dynamique
Case 7012 2 place Jussieu 75251 Paris Cedex 05, 75018 Paris, FRANCE
sombra@math.jussieu.fr

Jean-Pierre TECOURT, INRIA sophia-antipolis
2004 route des lucioles BP 93, 06902 Sophia Antipolis, FRANCE
Jean-Pierre.Tecourt@sophia.inria.fr

Monique TEILLAUD, INRIA
INRIA BP 93, 06902 Sophia Antipolis, FRANCE
Monique.Teillaud@sophia.inria.fr

Nicolas M. THIÉRY, Univ. Lyon I / Univ. Marne-la-
LaPCS, Univ. Claude Bernard Lyon I, Bât. recherche [B]50, ave. Tony-Garnier,
Domaine de Gerland, 69366 Lyon Cedex 07, FRANCE
nthiery@users.sf.net

EMMANUEL THOME, Ecole polytechnique
LIX / Ecole polytechnique, 91128 PALAISEAU CEDEX, FRANCE
thome@lix.polytechnique.fr

Joris VAN DER HOEVEN, Paris-XI (CNRS)
Dépt. de Math. (bât. 425) Université Paris-Sud , 91405 Orsay, FRANCE
joris@texmacs.org

Gilles VILLARD, ENS Lyon
LIP CNRS 46, Allée d'Italie, 69364 Lyon Cedex 07, FRANCE
Gilles.Villard@ens-lyon.fr

Jacques-Arthur WEIL, INRIA & Univ. Limoges
Project CAFE INRIA Sophia Antipolis 2004, Route des Lucioles B.P. 93,
F-06902 Sophia Antipolis Cedex , FRANCE
Jacques-Arthur.Weil@inria.fr

Philippe WENGER,
1 rue la Noe BP 92101, 44321 Nantes, FRANCE
Philippe.Wenger@irccyn.ec-nantes.fr

Jean-Claude YAKOUBSOHN, Universté Paul Sabatier
Lab. MIP Univ. Paul Sabatier118,route de Narbonne, 31062 Toulouse Cedex, FRANCE
yak@mip.ups-tlse.fr

Paul ZIMMERMANN, INRIA Lorraine
615 rue du jardin botanique, 54602 Villers-les-Nancy, FRANCE
zimmerma@loria.fr