# Journées Nationales de Calcul Formel

## École Thématique CNRS
## 14 - 18 novembre 2011, cirm, Luminy

Nous remercions également le **GDR IM** ainsi que le **service formation permanente du CNRS**.

Journées Nationales de Calcul Formel 2011
14 - 18 novembre 2011, CIRM, Luminy

**Organisateurs :**

- Marie-Noëlle Besson (Conseillère Formation CNRS, Délégation Aquitaine-Limousin)
- Guillaume Chèze (MdC, Univ. Toulouse III)
- Thomas Cluzeau (MdC, Univ. Limoges)
- Grégoire Lecerf (CR CNRS, École polytechnique, Palaiseau)
- Clément Pernet (MdC, Univ. Grenoble)

**Comité scientifique :**

- Moulay Barkatou (Prof., Univ. Limoges)
- Delphine Boucher (MdC, Univ. Rennes I)
- François Boulier (Prof., Univ. Lille I)
- Frédéric Chyzak (CR INRIA, Rocquencourt)
- Jean-Guillaume Dumas (MdC, Univ. Grenoble)
- Andreas Enge (DR INRIA, Institut de mathématiques de Bordeaux)
- André Galligo (Prof., Univ. Nice)
- Marc Giusti (DR CNRS, École polytechnique, Palaiseau)
- Bruno Salvy (DR INRIA, Rocquencourt)
- Gilles Villard (DR CNRS, ENS Lyon)
- Jean-Claude Yakoubsohn (Prof., Univ. Toulouse III)

## 1. Liste des orateurs

(1) Karim Belabas : *Théorie algébrique des nombres et calcul formel.*

(2) Loïc Pottier : *Preuves formelles automatiques en géométrie.*

(3) Frédéric Chyzak : *Le télescopage créatif pour l'intégration et la sommation paramétrées.*

(4) Joris van der Hoeven : *Calcul analytique.*

(5) Pierre Castel : *Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation.*

(6) Nicolas Estibals : *Un algorithme pour trouver toutes les formules calculant une application bilinéaire.*

(7) Matthieu Legeay : *Utilisation du groupe de permutations d'un code pour améliorer le décodage.*

(8) Guillaume Quintin : *Recherche de racine dans les Galois ring et application aux codes correcteurs d'erreurs.*

(9) Ludovic Perret : *Polynomials with Error (PWE).*

(10) Louise Huot : *Utilisation des symétries pour la résolution du problème de décomposition de points.*

(11) Bruno Grenet : *Représentations déterminantales symétriques en caractéristique* 2, **ET** *La puissance limitée des puissances : borne supérieure sur les racines des polynômes et borne inférieure pour les circuits arithmétiques.*

(12) Brice Boyer : *Software design in the LinBox library and prototypes for many-cores architectures.*

(13) Martin Weimann : *Factoring bivariate polynomials using singularities.*

(14) Jérémy Berthomieu : *Factorisation de polynômes à deux variables convexe-denses.*

(15) Romain Lebreton : *Algorithmique de l'algèbre de décomposition universelle.*

(16) Christoph Koutschan : *Advanced Computer Algebra for Evaluating Determinants.*

(17) Marc Mezzarobba : *Autour de l'évaluation numérique des fonctions D-finies.*

(18) Alexandre Benoit : *Séries de Fourier généralisées solutions d'équations différentielles.*

(19) Matthieu Deneufchâtel : *Functional coefficients in solutions of non-commutative differential equations.*

(20) Georg Regensburger : *Opérateurs intégro-différentiels, algèbres de Weyl généralisées, et localisations de Ore des anneaux euclidiens.*

(21) Razvan Barbulescu : *Logarithme discret et admissibilité.*

(22) Pierre-Jean Spaenlehauer : *Complexité de résolution de systèmes quadratiques booléens.*

(23) Fabien Monfreda : *Méthode de réduction de l'indice d'équations différentielles algébriques par déflation.*

(24) Mioara Joldes : *Approximations polynomiales rigoureuses à base de séries Chebyshev.*

(25) Guillaume Moroz : *Calcul de distances entre fonctions bivariées linéaires par morceaux.*

## 2. Résumés des cours

(1) **Karim Belabas** (Université de Bordeaux 1) : *Théorie algébrique des nombres et calcul formel.*

La théorie algébrique des nombres est née du désir de résoudre certaines équations diophantiennes en nombres entiers (typiquement, l'équation de Fermat). Elle introduit et étudie des structures algébriques associées aux extensions algébriques de $\mathbb{Q}$ ou de $\mathbb{F}_q(t)$, en y retrouvant la trace des propriétés des entiers ordinaires, par exemple la factorisation unique en produit de nombres premiers, sous une forme affaiblie. Je motiverai l'introduction des objets correspondants (anneaux d'entiers, groupes de classes, unités, groupes de Galois, fonctions $L$), et expliquerai comment les calculer en temps raisonnable. On citera des applications à la résolution algorithmique d'équations diophantiennes concrètes (équations aux normes, équations de Thue).

(2) **Loïc Pottier** (INRIA Sophia Antipolis Méditerranée) : *Preuves formelles automatiques en géométrie.*

De nombreux théorèmes de géométrie élémentaire (Desargues, Pappus, Feuerbach, etc) peuvent être démontrés automatiquement. Il existe différentes méthodes efficaces, dont la plus connue est dans doute celle de Wu, mais qui se prêtent plus ou moins à la formalisation. Nous étudierons une méthode qui consiste à utiliser un calcul incomplet de bases de Gröbner pour produire un certificat de petite taille (un programme sans boucle, ou straightline program), permettant de démontrer ensuite une égalité polynomiale de type Nullstellensatz : si $P_1, \ldots, P_n$ sont des polynômes exprimant les hypothèses du théorème, et $P$ sa conclusion, alors on peut écrire $c\,P^r = Q_1\,P_1 + \cdots + Q_n\,P_n$. Le calcul du certificat représentant $(c, r, Q_1, \ldots, Q_n)$ peut être fait dans n'importe langage (par exemple ocaml ou F7), alors que la preuve du Nullstellensatz est produite par réflexion dans le système d'assistance à la preuve Coq. On montrera sur des exemples dans le système Coq les différentes étapes et principes employés.

(3) **Frédéric Chyzak** (INRIA Rocquencourt) : *Le télescopage créatif pour l'intégration et la sommation paramétrées.*

La théorie des fonctions spéciales, celle des polynômes orthogonaux, ainsi que la combinatoire amènent à de nombreux problèmes d'intégrales et de sommes paramétrées, simples ou multiples, faisant intervenir des fonctions de plusieurs variables, continues ou discrètes. Diverses natures de questions interviennent, selon qu'il s'agit de trouver une expression explicite pour une intégrale ou une somme, ou de valider une identité, et selon que le problème à résoudre est exprimé comme une convolution, une extraction de coefficients, ou encore qu'il s'agit d'une intégrale plus générale.

L'approche algorithmique la plus fructueuse pour traiter ces intégrales et sommes est celle du « télescopage créatif », développée et popularisée depuis les travaux de Zeilberger au début des années 90. Le point de vue gagnant est l'abandon des formes explicites comme structure de donnée, au profit d'une représentation des fonctions à manipuler comme solution d'équations ou de systèmes linéaires, différentiels ou de récurrence. La méthode réalise, sur cette représentation implicite, un calcul qui généralise la dérivation sous le signe « intégrale », et dont la terminaison est justifiée dans les bons cas par une théorie de dimension empruntée à la théorie des D-modules.

Depuis son introduction et son algorithmisation par Zeilberger pour les sommes hypergéométriques de la combinatoire, la méthode a été étendue dans diverses directions : le cas des sommes hypergéométriques correspondant à des récurrences d'ordre 1 a d'abord été transposé au cadre des équations différentielles d'ordre 1 pour les intégrales hyperexponentielles ; l'ensemble de cette algorithmique a été étendu aux solutions de systèmes linéaires d'ordre supérieur, pour la sommation et l'intégration de fonctions intégrales de fonctions spéciales « D-finies » et de polynômes orthogonaux ; les mêmes idées ont été appliquées à des fonctions dépendant d'un nombre infini de variables, pour l'étude de certaines extractions de coefficients de fonctions symétriques de la combinatoire ; enfin, la limitation au cas D-fini, correspondant à une dimension nulle d'un certain idéal non commutatif, a été partiellement levée dans un certain nombre de cas, de sorte à élargir la classe des fonctions spéciales admettant un traitement par télescopage créatif.

Du point de vue algorithmique, le point de départ de la méthode de Zeilberger peut s'interpréter comme une forme d'élimination polynomiale non commutative, entre les représentations polynomiales d'opérateurs linéaires différentiels et de récurrence. La théorie des bases de Gröbner s'étend à ce cadre et a fourni les premiers algorithmes. Une approche plus efficace s'appuie sur la résolution d'équations auxiliaires en leurs solutions fractions rationnelles. Néanmoins, ces deux solutions souffrent de ce qu'ils conservent dans leur sortie une forme de trace du calcul qui, si elle peut servir de certificat au résultat final, est bien souvent inutile dans les applications. C'est pourquoi il est apparu important de tenter de s'affranchir de ces certificats. Dans certains cas, la recherche heuristique d'une équation différentielle vérifiée par un développement en série adéquat à grand ordre peut être validé a posteriori, et fournir une équation sur l'intégrale. Dans le cas de fractions rationnelles bivariées, une approche mêlant l'algorithme de Zeilberger et la réduction de Hermite permet de représenter les certificats dans une taille acceptable.

Dans ce mini-cours, nous nous proposons de traiter des divers cadres d'applications et approches algorithmiques du télescopage créatif, jusqu'à aborder quelques questions de complexité.

(4) **Joris van der Hoeven** (CNRS , École polytechnique) : *Calcul analytique.*

À l'heure actuelle, le calcul formel permet surtout la manipulation exacte d'objets de natures algébrique ou symbolique. Le calcul analytique se propose de généraliser cette démarche de calcul exact à l'analyse. Par rapport au calcul numérique classique, il faut donc être en mesure de certifier les calculs en s'appuyant sur une technologie systématique pour encadrer les erreurs de calcul. Un système de calcul analytique se compose de quatre couches de natures assez différentes.

- Au niveau le plus abstrait, des nombres réels calculables $x \in \mathbb{R}$ sont en réalité des algorithmes qui prennent une tolérance $\epsilon \in \mathbb{Q}^>$ en entrée et qui rendent une $\epsilon$-approximation $\tilde{x} \in \mathbb{Q}$ de $x$ avec $|\tilde{x} - x| \leq \epsilon$. Le domaine qui correspond à ce niveau de calcul est assez proche de la logique et s'appelle *analyse calculable*. Les machines de Turing furent originalement introduite pour montrer qu'il n'existe pas d'algorithme pour tester si un nombre réel calculable vaut zéro.

- La deuxième couche concerne la gestion des erreurs de calcul. On utilisera une variante de l'*arithmétique d'intervalles*, où le type de données central est celui d'une boule. On montrera comment ceci permet de rendre effectif des arguments de type $\epsilon$–$\delta$ et de déformation.

- La troisième couche concerne les algorithmes numériques proprement dits. En double précision, on peut utiliser des méthodes classiques développées par les numériciens. En précision arbitraire, il y a un saut de complexité pratique, dû au fait que l'émulation logicielle de nombres flottants est beaucoup plus lente que le calcul avec des « doubles machine ». Pour cette raison parmi d'autres, des algorithmes spécifiques sont souvent plus appropriés en précision plus élevée.

- Le calcul rapide en haute précision passe généralement par du calcul rapide sur les entiers. Pour tout ce qui est calcul efficace avec des matrices, polynômes, séries, etc. à coefficients entiers, on utilisera le même genre d'algorithmes qu'en calcul formel.

Dans notre cours, nous aborderons en détail ces différents thèmes du calcul analytique, ainsi que quelques autres aspects, comme des techniques d'implantation, ou la démarche « expérimentation, hypothèse, vérification ». On fournira aussi quelques applications comme l'intégration certifiée de systèmes dynamiques ou la résolution de systèmes algébriques par des méthodes d'homotopie certifiées.

## 3. Résumés des exposés

(5) **Pierre Castel** (Laboratoire de Mathématiques Nicolas Oresme, Caen) : *Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation.*

Dans cet exposé, je présente un nouvel algorithme probabiliste pour résoudre des équations quadratiques sur $\mathbb{Z}$ ou $\mathbb{Q}$ en dimension 5 sans utiliser de factorisation. Il est d'une complexité nettement meilleure que les algorithmes existant pour résoudre ce genre d'équations et repose sur deux algorithmes : celui de Simon et celui de Pollard et Schnorr. Après quelques rappels sur la théorie des formes quadratiques, j'explique comment fonctionne cet algorithme. La suite consiste en l'analyse détaillée de cet algorithme pour laquelle j'utiliserai une version effective du théorème de densité de Tchebotarev.

(6) **Nicolas Estibals** (Équipe-projet Caramel, LORIA, Nancy Université / CNRS/ INRIA) : *Un algorithme pour trouver toutes les formules calculant une application bilinéaire.*

Travail commun avec Razvan Barbulescu, Jérémie Detrey et Paul Zimmermann.

La multiplication est une opération arithmétique coûteuse comparativement à l'addition. Aussi il est intéressant, étant donné une application, de minimiser le nombre de produits à effectuer pour la calculer. Dans cette étude, nous nous restreignons au cas des applications bilinéaires.

En effet, parmi les applications bilinéaires, nous étions intéressés en premier lieu par la multiplication polynomiale. Ce problème ancien a déjàă été très étudié. La première découverte fut celle de Karatsuba (1962) qui montra que l'on peut effectuer le produit de deux polynômes de degré 2 en n'utilisant que 3 produits au lieu de 4 avec l'algorithme quadratique. Puis Toom & Cook (1963) montrèrent que 5 multiplications suffisent àă calculer le produit de polynômes de degré 3. En généralisant le problème aux polynômes de degré $n$ fixé, on définit alors $M(n)$ le nombre minimal de produits àă effectuer pour une telle multiplication. Le calcul de $M(n)$ est difficile et on ne dispose bien souvent que de bornes supérieures, de formules sans preuve de leur optimalité. En 2005, Montgomery effectua une recherche exhaustive de formules pour la multiplication de polynômes de degré 5 et trouva de nouvelles formules pour le degré 6 et 7.

Nous avons alors cherché àă généraliser son approche et réduire son coût grâce à une formalisation en terme d'espace vectoriel. Nous présentons ainsi un algorithme permettant d'énumérer toutes les formules contenant exactement $k$ produits calculant une application bilinéaire. Cet algorithme permet de calculer le nombre minimal de produits àă calculer pour certaines applications bilinéaires.

Enfin, notre algorithme ne se restreignant pas au produit de polynômes, nous avons pu appliquer cet algorithme àă d'autres problèmes tels que : le produit court, la multiplication dans une extension de corps ou encore de matrices.

(7) **Matthieu Legeay** (IRMAR - Université de Rennes 1) : *Utilisation du groupe de permutations d'un code pour améliorer le décodage.*

Dans la théorie des codes correcteurs d'erreurs linéaires et binaires, il n'est pas rare de trouver certains codes avec un groupe de permutations non trivial (codes de Reed-Solomon, codes de Reed-Muller, codes quasi-cycliques, codes BCH, etc). Généralement, ces codes ont un algorithme de décodage en temps polynomial.

Dans la cryptographie à clé publique basée sur les codes, également, on peut remarquer l'utilisation de codes dont le groupe de permutations est non trivial :

- ◇ Les codes de Goppa sont utilisés dans le cryptosystème original de McEliece. Lorsque ces codes sont construits à partir d'un polynôme générateur à coefficients dans un sous-corps du support, leurs groupes de permutations sont non triviaux, puisqu'ils possèdent au moins le Frobénius de l'extension.
- ◇ Plus récemment, les codes quasi-cycliques ont été utilisés dans le cryptosystème de McEliece. Ces codes ont également un groupe de permutations non trivial.
- ◇ Quelques fonctions de compression utilisées dans les fonctions de hachage utilisent aussi les codes quasi-cycliques.

Tous ces systèmes peuvent être attaqués par des algorithmes de décodage génériques. Cependant, aucun de ces algorithmes ne prend en compte le fait que le groupe de permutations est non trivial, alors qu'il est possible de retrouver quelques informations sur ce groupe en utilisant le *support splitting algorithm.*

Dans cet exposé, nous présenterons une façon d'utiliser le groupe de permutations pour améliorer l'efficacité des algorithmes de décodage génériques. On s'interessera à un certain type de permutations et on montrera des bornes sur la dimension d'un sous-code du code idempotent, appelé $\sigma$-code. Celui-ci peut avoir une dimension suffisamment basse en pratique ce qui pourrait permettre éventuellement l'utilisation d'une technique de décodage. Nous donnerons quelques exemples et expliquerons quel peut être le gain.

(8) **Guillaume Quintin** (DGA / École polytechnique / INRIA) : *Recherche de racine dans les Galois ring et application aux codes correcteurs d'erreurs.*

Travail en commun avec Jérémy Berthomieu (Université de Versailles / CNRS) et Grégoire Lecerf (CNRS/ École polytechnique).

Dans cette présentation nous donnerons un algorithme pour trouver toutes les racines jusqu'à une précision fixée d'un polynôme univarié dont les coeffcients sont dans un anneaux intègre, local, régulier, complet, non ramifié. Nous en donnerons la complexité et nous en déduirons un algorithme permettant de trouver les racines d'un polynôme dont les coefficients sont dans un anneaux finis local, non ramifié appelé un anneaux de Galois. Nous discuterons ensuite des conséquences de cet algorithme sur les complexités des algorithmes de décodages des codes de Reed-Solomon comme les algorithmes de Welch-Berlekamp, Sudan et Guruswami-Sudan.

(9) **Ludovic Perret** (INRIA, Paris-Rocquencourt Center, SALSA Project / UPMC Univ Paris 06, UMR CNRS 7606, LIP6) : *Polynomials with Error (PWE).*

Travail en commun avec Martin R. Albrecht, Jean-Charles Faugère et Dongdai Lin (SKLOIS, Institute of Software, Chinese Academy of Sciences, Beijing, China).

We present in this talk a new problem which consists in solving non-linear equations modulo a prime $q = \text{poly}(n)$ with noise (typically a Gaussian), i.e., some equations of the algebraic system are erroneous. This problem, that we have called *Polynomial With Errors* (PWE), is a non-linear (and rather natural) generalization of the well-known *Learning With Errors* (LWE) problem We recall that LWE is the problem of solving linear equation with noise.

We present in this talk theoretical complexity results on PWE. Note that the hardness of PWE is supported by the hardness of solving algebraic equations without errors ; the PoSSo problem. Solving non-linear system being significantly harder than solving a linear system, it is reasonable to expect that solving PWE will be harder than LWE. However, it can be shown that if the number of equations is $\geq \text{poly}(n)$ ($n$ being the number of variables) then PWE is essentially equivalent to an instance of PWE with bigger parameters. Therefore, the most interesting case to consider is PWE for a fixed and small number $\big(\text{i.e. } < \text{poly}(n)\big)$ of equations. We denote by boundPWE this problem, i.e. PWE with a bounded ($< \text{poly}(n)$) number of samples. We prove that boundPWE has a decision/search equivalence (deciding that a solution exists is equivalent to find a solution) a weak average-case/worst-case reduction. As a by-product, we show that these results also hold for the noiseless version of this problem, i.e. PoSSo.

Finally, we will briefly sketch an algorithm for solving boundPWE/PWE and discuss about the possibly to construct cryptographic schemes based on our new problems.

(10) **Louise Huot** (Équipe projet SALSA : CNRS, INRIA, LIP6, UPMC) : *Utilisation des symétries pour la résolution du problème de décomposition de points.*

Travail en commun avec Jean-Charles Faugère, Pierrick Gaudry (Équipe projet CARAMEL : CNRS, INRIA, LORIA), et Guénaël Renault.

Récemment P. Gaudry a introduit une nouvelle méthode de résolution du DLP sur les courbes elliptiques définies sur un corps fini non premier $\mathbb{F}_{q^n}$. Cet algorithme repose sur le principe général du calcul d'indice dont une étape cruciale nécessite de décomposer des points de la courbe $E(\mathbb{F}_{q^n})$ selon une base de facteurs. C'est à dire, étant donné un point fixé $R$ de $E(\mathbb{F}_{q^n})$ trouver $n$ points $P_i$, $1 \leq i \leq n$, de la base de facteurs $\mathcal{F} \subset E(\mathbb{F}_{q^n})$ tels que

$$R = P_1 \oplus \ldots \oplus P_n \,. \tag{3.1}$$

Une méthode de résolution algébrique de ce problème consiste à modéliser l'équation (3.1) sous forme d'un système polynomial et de le résoudre. À cette fin, Semaev introduit les polynômes de sommation qui projettent le problème de décomposition de points sur l'axe des abscisses. L'application d'une restriction de Weil de $\mathbb{F}_{q^n}$ à $\mathbb{F}_q$ sur un tel polynôme de sommation engendre un système à coefficients dans $\mathbb{F}_q$ à $n$ équations et $n$ inconnues, dont la résolution est équivalente à celle du problème de décomposition de point. Le coût de la résolution de ces systèmes est exponentiel en $n$ et elle devient rapidement impossible. Il est donc nécessaire d'optimiser la résolution de ces systèmes. Un moyen est d'utiliser les symétries du problème de décomposition de points. Une symétrie naturelle de ce problème, lié à la commutativité de la loi de groupe sur les points de la courbe, est l'action du groupe symétrique $\mathfrak{S}_n$. Dans cet exposé, nous mettrons en évidence des symétries supplémentaires. Nous étudierons en particulier deux représentations de courbes – les courbes d'Edwards et les intersections de Jacobi – dont les symétries se propagent sur les polynômes de sommation. Pour ces représentations, nous verrons également comment elles permettent de simplifier les systèmes polynomiaux à résoudre. Finalement nous présenterons quelques résultats pratiques montrant le gain apporté par l'utilisation des symétries.

(11) **Bruno Grenet** (LIP, UMR 5668, ENS de Lyon – CNRS – UCBL – INRIA, Université de Lyon)

– Exposé 1 : *Représentations déterminantales symétriques en caractéristique* 2.

Travail en commun avec Thierry Monteil (LIRMM, UMR 5506 Université de Montpellier 2 – CNRS) et Stéphan Thommasé.

Une *représentation déterminantale symétrique* (RDS) d'un polynôme multivarié $p$ est une matrice symétrique $M$ dont les cœfficients sont soit des éléments du corps de base soit des variables, et telle que le déterminant de $M$ soit égal à $p$. Dans le cas de la caractéristique différente de 2, tout polynôme admet une RDS.
Ce résultat n'est plus vrai en caractéristique 2 : par exemple, $xy + z$ n'admet pas de RDS. Pour prouver ceci, nous donnons une condition nécessaire pour l'existence d'une RDS. Dans le cas des polynômes multilinéaires, nous montrons que cette condition nécessaire est également suffisante, obtenant donc une caractérisation.
Nous fournissons ensuite un algorithme pour décider de l'existence d'une RDS pour les polynômes multilinéaires. Dans le cas où une RDS existe, l'algorithme construit de plus la matrice symétrique $M$. Cet algorithme peut également être appliqué aux polynômes non multilinéaires, mais il ne donne qu'un résultat partiel. Si l'algorithme échoue à construire une RDS, alors on est sûr que le polynôme n'en admet pas. Si l'algorithme retourne une matrice $M$, on doit vérifier si c'est une RDS valide ou non. Cet algorithme est de complexité polynomiale en le nombre de monôme du polynôme.

– Exposé 2 : *La puissance limitée des puissances : borne supérieure sur les racines des polynômes et borne inférieure pour les circuits arithmétiques.*

Travail en commun avec Pascal Koiran, Natacha Portier et Yann Strozecki (Équipe de Logique Mathématique, Université Paris VII).

Le test d'identité polynomiale et les bornes inférieures pour les circuits arithmétiques sont deux questions centrales en complexité algébrique. Il est remarquable que ces questions sont en fait reliées. Cette connexion a récemment amené l'un des auteurs de ce papier à proposer une « conjecture $\tau$ réelle ». Cette conjecture dit que le nombre de racines réelles d'une somme de produits de polynômes creux (univariés) est borné polynomialement. Elle implique une borne inférieure superpolynomiale sur la taille des circuits arithmétiques calculant le permanent.
Dans ce papier, nous prouvons un cas particulier de la conjecture $\tau$ réelle. Nous en déduisons une borne inférieure pour une classe restreinte de circuits de profondeur 4 : nous montrons que le permanent ne peut pas être calculé par des circuits de taille polynomiale de cette classe. Nous donnons également un test d'identité polynomiale déterministe pour ces même circuits.

(12) **Brice Boyer** (LJK, Université de Grenoble) : *Software design in the LinBox library and prototypes for many-cores architectures.*

LinBox is a powerful `C++` linear algebra library. It is very efficient on prime fields linear algebra. We can also do integer and Galois fields computations very well. The library is based on genericity by design and adapts to the user inputs. We will give some examples of actual LinBox performance and code fragments. Then we will also present some recent software design choices and software engineering decisions. Facing new trends in parallelism, we will finally discuss how we could generically do parallelism in LinBox.

(13) **Martin Weimann** (Ricam, Linz, Austria) : *Factoring bivariate polynomials using singularities.*

I will discuss the relations between desingularization and absolute factorization of rational bivariate polynomials. The main result asserts that, given the univariate factorization of $f(x, y)$ modulo $(x)$ and given a basis for the vector space of degree $d-2$ adjoint polynomials of $f$ computed mod $(x)$, one can compute the factorization of $f$ within $\mathcal{O}(d^\omega)$ operations over $\overline{\mathbb{Q}}$, where $\omega$ is the complexity exponent for matrix multiplications. This result leads to new interesting comparisons with the algorithms of Lecerf et al, the usual lifting process being now replaced by the desingularization process. The proof relies on cohomological considerations and on residue theory.

(14) **Jérémy Berthomieu** (Laboratoire de Mathématiques
Université de Versailles – St-Quentin-en-Yvelines) : *Factorisation de polynômes à deux variables convexe-denses.*

Travail en commun avec Grégoire Lecerf (CNRS/ École polytechnique).

Nous présentons un nouvel algorithme pour réduire le problème de la factorisation des polynômes creux à deux variables au cas des polynômes denses. Cette réduction consiste simplement en le calcul d'une transformation monomiale inversible qui rend un polynôme dont la taille dense est du même ordre de grandeur que la taille du polygone de Newton du polynôme donné en entrée. En particulier, si la complexité d'un algorithme de factorisation de polynôme à deux variables s'exprime en le produit des degrés partiels, notre résultat permet de dire que cette même complexité est en fait en la taille du polygone de Newton du polynôme considéré.

(15) **Romain Lebreton** (École Polytechnique, Paris) : *Algorithmique de l'algèbre de décomposition universelle.*

Travail en commun avec Éric Schost (University of Western Ontario, London, Canada).

Fixons un corps effectif $k$ et un polynôme $f \in k[T]$ de degré $n$. Nous appelerons relations symétriques les polynômes symétriques à coefficients dans $k$ qui s'annulent sur les racines de

$f$ dans une extension appropriée. Ces relations forment un idéal $\mathcal{I}$. L'algèbre de décomposition universelle est l'algèbre quotient $\mathbb{A} := k[X_1, \ldots, X_n]/\mathcal{I}$. Cette algèbre est lié au corps de décomposition $L$ de $f$. Par exemple, pour des coefficients de $f$ génériques, le degré de l'extension de corps $L/k$ est $n!$ et alors $L$ s'identifie à $\mathbb{A}$.

Dans cet exposé, nous montrons comment obtenir une algorithmique efficace dans $\mathbb{A}$. Pour cela, on utilise une représentation à une variable de $\mathbb{A}$, *c.-à-d.* un isomorphisme explicite de la forme $\mathbb{A} \simeq k[T]/Q(T)$. Dans cette représentation, les opérations arithmétiques de $\mathbb{A}$ ont naturellement une complexité quasi-optimale.

Nous détaillerons deux algorithmes intrinsèquement liés explicitant d'une part l'isomorphisme et d'autre part calculant le polynôme charactéristique d'un élément $P$ de $\mathbb{A}$.

(16) **Christoph Koutschan** (Centre de Recherche Commun INRIA -Microsoft Research, Orsay, France) : *Advanced Computer Algebra for Evaluating Determinants.*

Travail en commun avec Masao Ishikawa (University of the Ryukyus, Nishihara, Okinawa, Japan) et Thotsaporn Thanatipanonda (RISC, Johannes Kepler University Linz, Austria).

The "holonomic ansatz" for proving and evaluating determinants was recently introduced by Zeilberger. This approach can be applied to matrices whose entries are ($q$-) holonomic sequences in order to establish identities of the form

$$\det(a_{i,j})_{1 \le i,j \le n} = b_n.$$

For example, the holonomic ansatz was used by Kauers, Koutschan, and Zeilberger to prove the $q$-enumeration formula for totally symmetric plane partitions. In this talk we will present some extensions and generalisations of the holonomic ansatz which allow to take the parity of $n$ into account. With these new tools we prove some determinant conjectures that appear in Krattenthaler's prominent collection "Advanced Determinant Calculus : A Complement" (2005). This is joint work of the second and third named author.

Together with Ishikawa we derived a variant of the holonomic ansatz that is suited to deal with Pfaffians. This variant is applied to prove some conjectures that appeared in the article "Pfaffian decomposition and a Pfaffian analogue of $q$-Catalan Hankel determinants" (Ishikawa, Tagawa, Zeng, 2010).

(17) **Marc Mezzarobba** (LIP, INRIA/ENS de Lyon) : *Autour de l'évaluation numérique des fonctions D-finies.*

Certains de ces travaux ont été menés en collaboration avec Alexandre Benoit (UPMC/LIP6/ CNRS/ INRIA Paris-Rocquencourt), Mioara Joldes (CAPA team, Department of Mathematics, Angstrom Laboratory, Uppsala University, Sweden) ou Bruno Salvy (INRIA Paris-Rocquencourt).

Je proposerai une synthèse de mes travaux de thèse, qui ont comme thème commun l'évaluation numérique des fonctions dites D-finies. Les fonctions D-finies sont les solutions d'équations différentielles linéaires à coefficients polynomiaux. Il s'agit de développer des outils pour leur évaluation (et divers problèmes apparentés) qui travaillent à partir d'une équation différentielle accompagnée d'un jeu convenable de conditions initiales.

Le leitmotiv est de proposer des méthodes à la fois générales (couvrant autant que possible toutes les fonctions D-finies), garanties (bornes d'erreur rigoureuse) et efficaces (tant en pratique que du point de vue de la complexité). Les travaux présentés explorent trois principales directions.

(a) Le calcul de *majorants fins* sur les suites solutions de récurrences linéaires à coefficients polynomiaux, qui comprennent comme cas particulier les développements en série entière de fonctions D-finies. Les bornes obtenues interviennent à de multiples reprises pour garantir la précision des calculs numériques.

(b) La mise en pratique d'un algorithme de *prolongement analytique numérique* à grande précision, proposé par Chudnovsky et Chudnovsky à la fin des années 1980 puis étendu par

van der Hoeven. Sans être le plus rapide à petite précision, cet algorithme sert de base à une approche efficace et garantie pour évaluer une fonction D-finie quelconque en n'importe quel point de son domaine de définition et à des précisions pouvant atteindre des millions de chiffres décimaux.

(c) Le calcul de *polynômes d'approximation*. La question est ici d'obtenir à faible coût un polynôme de degré imposé qui approche bien une fonction D-finie donnée, au sens de la norme uniforme sur un segment, ainsi qu'une borne sur l'erreur d'approximation. De tels polynômes sont utiles, par exemple, pour évaluer la fonction à précision modérée en plusieurs points du segment.

La plupart des algorithmes en jeu ont été implémentés (sic), notamment dans le module Maple NumGfun présenté lors de l'édition précédente des JNCF.

(18) **Alexandre Benoit** (UPMC/LIP6/ CNRS/ INRIA Paris-Rocquencourt) : *Séries de Fourier généralisées solutions d'équations différentielles.*

Travail en commun avec Bruno Salvy (INRIA Paris-Rocquencourt).

Les polynômes de Tchebychev, de Hermite ou autres polynômes orthogonaux classiques, les fonctions de Bessel et certaines autres familles de fonctions spéciales, forment des bases d'espaces hilbertiens adaptés. Il est donc utile de pouvoir développer des fonctions sur ces bases, et ces développements s'appellent des séries de Fourier généralisées. Les séries de Taylor sont un cas particulier (base monomiale), mais aussi les séries de Tchebychev ou de Neuman (base des fonctions de Bessel).

Quand une telle série est solution d'une équation différentielle linéaire à coefficients polynomiaux, ses coefficients eux-mêmes satisfont une récurrence linéaire à coefficients polynomiaux. Dans ce travail nous interprétons cette équation comme le numérateur d'une fraction d'opérateurs de récurrence. Cette interprétation nous permet de donner un algorithme général pour calculer de telles récurrences et fournit une vision simple des algorithmes existants pour plusieurs familles de fonctions spécifiques.

(19) **Matthieu Deneufchâtel** (Laboratoire d'Informatique de Paris Nord, CNRS UMR 7030, Université Paris 13) : *Functional coefficients in solutions of non-commutative differential equations.*

Travail en commun avec Gérard H. E. Duchamp et Vincel Hoang Ngoc Minh.

This talk is devoted to the presentation of a theorem [1] giving necessary and sufficient criteria to ensure the linear independance of the coefficients of a series $S$ solution to the non commutative differential equation

$$dS = MS.$$

Here, $S$ belongs to $\mathcal{A}\langle\langle X\rangle\rangle$, where $(\mathcal{A}, d)$ is a differential algebra, and $M$ is a homogeneous series of degree 1 called *multiplier* : $\sum_{x\in X} u_x x$ with coefficients in $\mathcal{A}$.

The tools that we use are mainly those of algebraic combinatorics. One of the reasons why this theorem is interesting is that it allows one to understand the properties of linear independance of the functions with the computation of a small number of them. The theorem also gives a general framework that sums up the previous results.

We also present applications of the theorem to two examples : one the one hand, Drinfeld'd equation,

$$\frac{d}{dz}S = \left(\frac{1}{z}x_0 + \frac{1}{1-z}x_1\right) S$$

1. **Independence of hyperlogarithms over function fields via algebraic combinatorics**, M. D., G. H. E. Duchamp, H. N. Minh and A. Solomon, *CAI 2011*, LNCS 6742, pp. 127–139. Springer, Heidelberg (2011)

which gives birth to *polylogarithms* ; on the other hand, a differential equation with multiplier

$$M = \sum_{x \in X} \frac{\lambda_i}{z - a_i} x_i, \lambda_i \in \mathbb{C}^*,$$

that yields functions called *hyperlogarithms*. In that case, we have to work with fields of functions with variable domains in order to handle the different singularities. That is why we introduce *fields of germs* of analytic functions.

(20) **Georg Regensburger** (INRIA Saclay – Île de France, Projet DISCO, L2S, Supélec, Gif-sur-Yvette) : *Opérateurs intégro-différentiels, algèbres de Weyl généralisées, et localisations de Ore des anneaux euclidiens.*

Ce travail, financé par l'Austrian Science Fund (FWF) : J 3030-N18, est en collaboration avec Alban Quadrat.

Une algèbre intégro-différentielle est une algèbre différentielle munie d'une intégrale. Le théorème fondamental de l'analyse montre que l'opérateur intégral doit être un inverse à droite de l'opérateur de dérivation. Cependant, l'opérateur intégral n'est pas un inverse à gauche de la dérivation à cause du terme de bord, mais donne une évaluation multiplicative si l'on exige une version de l'intégration par parties dans l'algèbre intégro-différentielle. Cette approche est à la base d'une étude algébrique des équations différentielles ordinaires avec conditions initiales et conditions aux limites. Un exemple prototypique d'une algèbre intégro-différentielle est l'anneau des polynômes à coefficients dans un corps de caractéristique nulle muni de la dérivation et de l'intégration usuelles.

Dans cet exposé, nous expliquerons la construction de l'algèbre des opérateurs intégro-différentiels à coefficients polynômiaux développée en collaboration avec Markus Rosenkranz. Cette algèbre a aussi été récemment étudiée par V. V. Bavula dans de nombreuses publications basées sur le concept d'algèbres de Weyl généralisées. Nous résumerons cette approche et donnerons quelques propriétés et résultats algébriques.

Dans cette construction, si l'on quotiente cette dernière algèbre par l'idéal bilatère engendré par l'évaluation, l'intégrale devient alors un inverse bilatère de la dérivation. Dans le cas des coefficients fractions rationnelles, nous obtenons un anneau euclidien non commutatif qui s'interprète comme une localisation de Ore de l'anneau des opérateurs différentiels à coefficients dans l'anneau de fractions rationnelles. Nous étudierons quelques aspects algorithmiques de la localisations des anneaux euclidiens (non commutatifs). Finalement, nous indiquerons le calcul de la forme de Jacobson des matrices à coefficients dans une telle localisation, ce qui constitue les premiers pas vers une étude constructive des systèmes linéaires intégro-différentiels.

(21) **Razvan Barbulescu** (LORIA et Université deNancy) : *Logarithme discret et admissibilité.*

Le calcul du logarithme discret (résoudre $T^x = S \mod p$ avec $p$ premier et $T, S \in [1, p-1]$) est un ancien problème de théorie des nombres. Il fut étudié par Bouniakovski et en 1922 Kraitchik créa une technique qui trouve en temps sous-exponentiel en $\log p$ les logarithmes discrets de tous les nombres premiers inférieurs Ãă une certaine borne. Le problème devint ecore plus étudié grâce à son utilisation en cryptographie par Diffie et Hellman.

A présent, le plus rapide algorithme est le crible algébrique (voir par exemple [JL03]), qui reprend les étapes d'un algorithme de 1979, Index Calculus, lui-même inspiré indirectement de la méthode de Kraitchik. Si on note $L_p(s, c) = \exp((\log p)^s (\log \log p)^{1-s})$, la première partie du crible algébrique, qui est commune pour plusieurs $S$, a une complexité $L_p(\frac{1}{3}, k)^{1+o(1)}$ avec $k \approx 1,923$, alors que la deuxième prend un temps inférieur.

Plus précisément, la deuxième partie commence par chercher un $h \in \mathbb{N}$ tel que la décomposition en idéaux premiers de $T^h S$ dans un corps de nombre donné ne contienne que des idéaux de norme inférieure à une borne donnée et qui sont de degré 1. Pour accélérer cette étape on peut utiliser des corps de nombres avec un groupe de Galois d'ordre premier, une reconstruction rationnelle ou on peut introduire un test supplémentaire, dit d'admisibilité.

La technique qui nous intéresse le plus est celle de l'admissibilité car c'est elle qui permet de diminuer la complexité de la deuxième partie de $L_p(\frac{1}{3}, 1)^{1.447+o(1)}$ Ãă $L_p(\frac{1}{3}, 1)^{1.232+o(1)}$. Afin de comprendre pourquoi, on dit, pour tout $B$, qu'un nombre est $B$-friable si tous ses facteurs premiers sont inférieurs à $B$. De même, on appelle test de friabilité un algorithme qui, pour toute borne $B$, teste la $B$-friabilité en temps $L_B(\frac{1}{2}, \sqrt{2})$. La modélisation mathématique de notre problème devient : étant donné un générateur aléatoire de nombres inférieurs à $p$ et un test de friabilité, trouver la plus rapide stratégie de sélection d'un nombre $L_p(\frac{2}{3}, a)$-friable, pour un $a > 0$ à choisir. L'outil de base sera un théorème qui approche la probabilité de friabilité [CEP83].

## Bibliographie


[JL03] A. Joux et R. Lercier, Improvements to the General Number Field for discrete logarithms in prime fields, Mathematics of Computation , 2003

[CEP83] E. Canfield, P. Erdös et C. Pomerance, On a problem of Oppenheim concerning "factoraisatio numerorum", Journal of Number Theory, 1983


(22) **Pierre-Jean Spaenlehauer** (Projet SALSA – INRIA Paris-Rocquencourt/UPMC/LIP6) : *Complexité de résolution de systèmes quadratiques booléens.*

Travail en commun avec Magali Bardet (Université de Rouen), Jean-Charles Faugère et Bruno Salvy (Projet Algorithms – INRIA Paris-Rocquencourt).

La résolution de systèmes quadratiques sur $\mathbb{F}_2$ (Boolean MQ) est un problème naturel qui apparaît dans plusieurs contextes applicatifs. En particulier, la sécurité de plusieurs cryptosystèmes récents repose sur la complexité de résoudre ce problème NP-complet. Dans le cas général, la meilleure borne de complexité connue est $4 \log_2 n 2^n$ et est obtenue en effectuant une recherche exhaustive.

Dans cet exposé, nous proposons un algorithme qui permet, sous des hypothèses algébriques précises, de résoudre des systèmes quadratiques booléens de $n$ équations à $n$ inconnues avec une complexité bornée par :
- $O(2^{0.841n})$ avec une variante déterministe ;
- $O(2^{0.792n})$ avec une variante probabiliste de type Las Vegas.

Ces résultats se généralisent aux cas des systèmes surdéterminés ($\alpha n$ équations, $n$ variables, avec $\alpha > 1$).

Le principe de l'algorithme est d'effectuer une recherche exhaustive, et d'utiliser de l'algèbre linéaire rapide sur la *matrice de Macaulay* pour détecter des sous-arbres de la recherche qui ne contiennent aucune solution. La variante probabiliste fait intervenir l'algorithme de Wiedemann afin d'exploiter le fait que la matrice de Macaulay est très creuse.

L'analyse de complexité passe par une description de la structure algébrique des idéaux engendrés par des systèmes surdéterminés booléens génériques. Elle est soutenue par une variante de la conjecture de Fröberg, et appuyée par des expérimentations montrant qu'en pratique les hypothèses algébriques sont vérifiées avec forte probabilité.

De plus, la variante probabiliste de l'algorithme proposé est plus efficace que la recherche exhaustive quand $n$ est supérieur à 200, ce qui correspond à l'ordre de grandeur de tailles de systèmes qui apparaissent en Cryptologie.

(23) **Fabien Monfreda** (Univ. Toulouse III) : *Méthode de réduction de l'indice d'équations différentielles algébriques par déflation.*

Travail en commun avec Jean-Claude Yakoubsohn.

Cet exposé a pour but de présenter une nouvelle méthode de résolution concernant les équations différentielles algébriques (EDAs).
Cette méthode itérative, dite de déflation, définit une suite d'équations différentielles algébriques

dont l'indice, que l'on caractérisera, est diminué à chaque étape. Ceci est simultanément mis en oeuvre par des substitutions et des différentiations. A la fin du processus, on obtient au plus une équation différentielle ordinaire et une liste de contraintes algébriques vérifiées par la solution de l'EDA initiale.

Une description complète de la méthode est proposée, aussi bien dans le cadre linéaire que dans le contexte quasi-linéaire. A chaque fois, des hypothèses de régularité sont données.

*Soit $k$ le nombre d'étapes de l'algoritme de déflation.*

- *Cadre linéaire* $E(t)\dot{x}(t) = A(t)x(t) + f(t)$.

On montre que les coordonnées de la solution satisfont une équation différentielle du type :

$$E_k(t)\dot{x}^k(t) = A_k(t)x^k(t) + f_k(t),$$

où $E_k(t)$ est inversible ou nulle ainsi qu'une liste de contraintes algébriques de la forme :

$$x_2^j(t) = -N_j^{-1}(t)M_j(t)x_1^j(t) - N_j^{-1}(t)f_{j,r_j+1:r_{j-1}}(t), \quad 0 \leqslant j \leqslant k-1.$$

- *Cadre quasi-linéaire* $E(x(t))\dot{x}(t) = A(x(t))$.

On généralise le résultat précédent ; on montre que les coordonnées de la solution satisfont une équation différentielle quasi-linéaire ainsi qu'un ensemble de contraintes algébriques non linéaires.

L'accent est également porté sur les notions d'indices ; nous développons en particulier les notions d'indice de Kronecker et de différentiation.
La méthode de déflation est illustrée à travers divers exemples physiques, provenant du domaine de la mécanique ou encore de la théorie des circuits électriques.

(24) **Mioara Joldes** (CAPA team, Department of Mathematics, Angstrom Laboratory, Uppsala University, Sweden) : *Approximations polynomiales rigoureuses à base de séries Chebyshev.*

Travail en commun avec Alexandre Benoît (UPMC/LIP6/ CNRS/ INRIA Paris-Rocquencourt), Nicolas Brisebarre (LIP, INRIA/ENS de Lyon) et Marc Mezzarobba (LIP, INRIA/ENS de Lyon).

Quand on veut évaluer ou manipuler une fonction mathématique $f$, il est fréquent de la remplacer par une approximation polynomiale $p$. On le fait, par exemple, pour implanter des fonctions élémentaires en machine, pour la quadrature ou la résolution d'équations différentielles ordinaires (ODE). De nombreuses méthodes numériques existent pour l'ensemble de ces questions et nous nous proposons de les aborder dans le cadre du calcul rigoureux, au sein duquel on exige des garanties sur la précision des résultats, tant pour l'erreur de méthode que l'erreur d'arrondi.

Une approximation polynomiale rigoureuse (RPA) pour une fonction $f$, définie sur un intervalle $[a, b]$, est un couple $(p, \Delta)$ formé par un polynôme $p$ et un intervalle $\Delta$, tel que $f(x) - p(x) \in \Delta$, pour tout $x \in [a, b]$.

Dans ce travail, nous introduisons des procédés de calcul de RPAs en utilisant les séries tronquées de Chebyshev ou les interpolants de Chebyshev. Nous présentons aussi plusieurs applications : une relative à l'implantation de fonctions standard dans une bibliothèque mathématique (libm) et une portant sur le calcul de développements tronqués en séries de Chebyshev de solutions d'ODE linéaires à coefficients polynômiaux.

(25) **Guillaume Moroz** (INRIA Nancy - Grand Est ) : *Calcul de distances entre fonctions bivariées linéaires par morceaux.*

Travail en commun avec B. Aronov (Polytechnic Institute of NYU).

Soient $f$ et $g$ deux fonctions bivariées linéaires par morceaux, définies sur une région $M$ du plan. Nous nous intéressons au calcul de la distance entre $f$ et $g$ au sens de la norme $L_2$ : $\|f - g\|_2 = \sqrt{\iint_M (f-g)^2}$.

Dans le cas où $f$ et $g$ sont définies sur 2 triangulations distinctes de $n$ triangles chacunes, l'algorithme naif pour calculer leur distance est en $\Theta(n^2)$ opérations arithmétiques.

Nous verrons qu'il est possible de calculer cette distance en $O(n \log(n)^4)$ opérations, en réduisant le problème à un problème d'évaluation multipoint de polynôme.