PROGRAMME DES JNCF 2008
(Programme en date du 20 octobre 2008)

Programme de la semaine

Lundi 20 octobre

09h00 Ouverture des journées

09h30 *Laurent Busé :* Résultants : des matrices pour l'élimination (Cours 1/3)

10h30 Pause

11h00 *Romain Cosset :* Factorisation d'entiers à l'aide de courbes de genre 2
11h30 *Clément Dunand :* Utilisation de bases elliptiques pour le paramétrage de tores algébriques
12h00 *Alexandre Benoît :* Développements de fonctions D-finies sur des polynômes de Tchebychev.

12h30 Déjeuner

14h00 *Frédéric Edoukou :* Codes correcteurs d'erreurs sur des surfaces Hermitiennes
14h30 *Gaëtan Bisson :* Multiplication complexe et discriminants
15h00 *Ainhoa Aparicio :* Réduction des équations variationelles des systèmes hamiltoniens à deux degrés de liberté et leur intégrabilité
15h30 *Luca De Feo :* Principe de transposition et algorithmes pour les tours d'Artin–Schreier

16h00 Pause

17h00 *Lionel Chaussade :* Codes tordus dont le rang ou la distance minimale est prescrite
17h30 *Pierre-Vincent Koseleff :* Nœuds toriques polynomiaux
18h00 *Ihsen Yengui :* La conjecture des anneaux de Hermite en dimension 1

19h00 Temps libre pour discussions

19h30 Dîner

Mardi 21 octobre

09h30 *Laurent Busé :* Résultants : des matrices pour l'élimination (Cours 2/3)

10h30 Pause

11h00 *Mohab Safey El Din :* Real Solving Singular Polynomial Systems
11h30 *Marc Giusti :* Variétés polaires et bipolaires
12h00 *Jean-François Biasse :* Index calculus and large prime variation for the DLP on hyperelliptic curves

12h30 Déjeuner

14h00 *Pierre Rouchon :* Systèmes différentiellement plats (Cours 1/2)

15h30 Pause

Session « Géométrie algorithmique »
16h00 *Sylvain Lazard :* Geometrie algorithmique et calcul formel
16h40 *Marc Pouget :* Du calcul de courbes d'extrême de courbure sur une surface au calcul de la topologie de courbes algébriques en général
17h10 *André Lieutier :* Robustesse en calcul géométrique, pratiques industrielles et apport du calcul formel
17h40 *Guillaume Moroz :* Robots et positions cuspidales

18h10 Temps libre pour discussions

19h30 Dîner

Mercredi 22 octobre

09h00 *Guénaël Renault :* Théorie de Galois effective (Cours 2/2)

10h30 Pause

11h00 *Pierre Rouchon :* Systèmes différentiellement plats (Cours 1/2)

12h30 Déjeuner

14h00 *Laurent Busé :* Résultants : des matrices pour l'élimination (Cours 3/3)

15h00 Pause

15h30 *Joris van der Hoeven :* Mathemagix
16h10 *Daouda-Niang Diatta :* Calcul du type topologique d'une surface implicite
16h40 *Adrien Poteaux :* Calcul numérique-symbolique de développements de Puiseux

17h10 Temps libre pour discussions

19h30 Dîner

Jeudi 23 octobre

09h00 *Guénaël Renault :* Théorie de Galois effective (Cours 2/2)

10h30 Pause

11h00 *Sylvie Boldo :* Preuves formelles et équation des ondes
11h30 *Hong Diep Nguyen :* Résoudre et certifier la solution d'un système linéaire
12h00 *Olivier Ruatta :* Automate globalement convergent pour le calcul de toutes les racines d'une équation algébrique

12h30 Déjeuner

14h00 *Jean-Michel Muller :* Calculs « exacts » avec une arithmétique approchée (Cours 1/2)

15h30 Pause

Session « Modélisation en biologie »

16h00 *Hidde de Jong :* Qualitative Modeling and Simulation of Genetic Regulatory Networks
16h40 *Marie-Françoise Roy :* Méthodes semi-algébriques en épidémiologie
17h10 *François Lemaire :* Approximation au premier ordre des variétés lentes
17h40 *Aslı Ürgüplü :* Qualitative Analysis of Dynamical Systems : Application to Biology
18h10 Fin de la session spéciale
18h20 *Michel Petitot :* Le problème d'équivalence du point de vue algébrique
18h50 Temps libre pour discussions

19h30 Dîner

Vendredi 24 octobre

09h00 *Jean-Michel Muller :* Calculs « exacts » avec une arithmétique approchée (Cours 2/2)

10h30 Pause

11h00 *Richard Leroy :* Certificats de positivité et minimisation polynomiale dans la base de Bernstein multivariée
11h30 *Mioara Joldes :* Certified and fast computation of supremum norms of approximation errors
12h00 *Bernard Mourrain :* Dualité, moments et idéaux radicaux

12h30 Déjeuner

14h00 Clôture des journées

Résumés des cours

1. Les codes algébriques et leur décodage

Daniel Augot (INRIA Paris-Rocquencourt, Équipe-projet Secret)

Exposé annulé *Ce cours portera d'abord sur les célèbres codes de Reed-Solomon. Je commencerai par montrer l'optimalité de ces codes en terme combinatoires : ce sont des codes MDS (*maximum distance separable*). Cette optimalité ne répond cependant pas à tous les besoins, notamment lorsque les alphabets considérés sont petits. Je présenterai ensuite deux constructions de ces codes, lesquelles conduisent à deux grandes familles d'algorithmes de décodage : par syndrome (Berlekamp-Massey) et par interpolation (Sudan). Une autre famille de codes, aux propriétés similaires, est celle des codes géométriques introduits par Goppa. Ces derniers utilisent la théorie des courbes algébriques sur les corps finis. De même que pour les codes de Reed-Solomon, deux approches duales permettent de définir les codes de Goppa : l'algorithme de Berlekamp-Massey se généralise en l'algorithme de Berlekamp-Massey-Sakata ; l'algorithme de Sudan en l'algorithme de Shokrollahi-Wasserman, dont l'algorithme de Guruswami-Sudan est une version améliorée. L'intérêt des algorithmes de décodage par interpolation est qu'ils franchissent le mur de la distance minimale, c'est-à-dire qu'ils corrigent beaucoup plus d'erreurs que les algorithmes classiques.*

2. Systèmes différentiellement plats

Pierre Rouchon (Mines ParisTech)

Les systèmes différentiellement plats, une sous-classe des systèmes non-linéaires contrôlés, jouent un peu le même rôle que les systèmes intégrables par rapport aux systèmes dynamiques (sans contrôle) : pour ces systèmes contrôlés on dispose aussi d'une description « explicite » de leur trajectoires, i.e., de leur solutions. D'une telle description, on déduit une méthode systématique

pour la planification et le suivi de trajectoires, deux questions de base en contrôle des systèmes. Après des définitions en dimension finie (équations différentielles ordinaires), définitions illustrées par quelques exemples, on aborde des questions ouvertes liées à la caractérisation des systèmes différentiellement plats mais aussi à la planification et au suivi en présence de singularité. L'extension à la dimension infinie, i.e. aux équations aux dérivées partielles avec contrôle frontière, est aussi abordée. Elle s'appuie sur des exemples pour lesquels il peut être nécessaire de faire appel, de manière encore assez mal comprise, à des techniques de re-sommation pour rendre les développements en séries effectifs d'un point de vue numérique.

3. Calculs « exacts » avec une arithmétique approchée

Jean-Michel Muller (CNRS, Laboratoire LIP)

L'arithmétique virgule flottante a été conçue comme une simple approximation de l'arithmétique réelle.Cependant, comme le comportement de chaque opération est complètement spécifié par une norme (la norme IEEE-754), l'arithmétique virgule flottante peut aussi être vue comme une structure mathématique sur laquelle on peut construire des algorithmes et des preuves. C'est ainsi que l'on peut construire des algorithmes arithmétiques nettement plus rapides et précis que ce que l'on pouvait faire auparavant. On donnera quelques exemples montrant l'intérêt de cette approche. On en profitera également pour parler de quelques unes des nouveautés figurant dans la révision de la norme IEEE-754, qui vient d'être adoptée.

4. Théorie de Galois effective

Guénaël Renault (Équipe-projet INRIA / LIP6 Salsa)

La résolution d'équations polynomiales en une variable est le problème qui a fait naître la théorie de Galois. Depuis l'antiquité, les mathématiciens ont toujours voulu pouvoir obtenir les solutions de telles équations sous la forme de formules ne faisant intervenir que les opérations usuelles et des radicaux en les coefficients de l'équation. Pendant longtemps, le problème de savoir si de telles formules existaient resta sans solution. C'est Galois qui édifia la théorie permettant de répondre à cette question et montra, en particulier, que ceci était impossible en toute généralité. Pourtant, l'essence de cette théorie repose sur une construction formelle du plus petit corps contenant les racines du polynôme P entrant dans la définition de l'équation et ainsi permet de résoudre formellement cette dernière. A ce corps, appelé corps de décomposition de P, est associé un groupe qui permet de caractériser des propriétés sur ce corps à partir de propriétés calculées sur le groupe. Dans ce cours, nous présenterons ces objets centraux de la théorie de Galois et nous montrerons des algorithmes efficaces permettant de les calculer.

5. Résultants : des matrices pour l'élimination

Laurent Busé (INRIA Sophia Antipolis - Méditerrannée, Équipe-projet Gallad)

Ce cours est divisé en trois parties. La première partie traite du résultant bien connu de deux polynômes univariés, très souvent appelé résultant de Sylvester. L'objectif principal est ici d'illustrer le contenu géométrique du résultant au travers d'applications concrètes en géométrie et modélisation algébrique : théorème de Bézout, problèmes d'inversion et d'implicitation d'une courbe plane rationelle. Notamment, l'accent sera mis sur deux propriétés fondamentales du résultant qui le distinguent des autres techniques d'élimination : son caractère universel et ses représentations matricielles. La deuxième partie est consacrée à la généralisation du résultant de Sylvester au cas de n polynômes homogènes en n variables, souvent appelé résultant de Macaulay. Après une brève introduction sur le théorème de l'élimination, l'existence et les principales propriétés de ce résultant seront présentés sous l'angle le plus adapté au calcul : les formes d'inerties. Pour finir, on présentera la formule de Poisson que l'on illustrera par quelques applications géométriques.

La dernière partie propose une discussion plus avancée sur l'existence générale des résultants. On montrera qu'il est (presque) toujours possible de donner une définition géométrique pour le résultant d'un système algébrique bien dimensionné. En revanche, il est plus délicat de pouvoir le « calculer », c'est-à-dire d'en trouver une représentation matricielle. En fait, ce calcul nécessite une étude approfondie qui doit bien souvent être menée au cas par cas. Nous l'illustrerons au travers d'un exemple concret.

Sessions d'ouverture

6. Geometrie algorithmique et calcul formel

Sylvain Lazard (INRIA Sophia Antipolis - Méditerrannée, Équipe-projet Vegas)

Je presenterai un ensemble de travaux sur des problemes de geometrie algorithmique ayant des liens avec le calcul formel. Typiquement, les techniques et outils calcul formel peuvent etre utilisees dans les algorithmes geometriques ainsi que pour demontrer des theoremes de geometrie. En particulier, je presenterai des travaux sur des problemes de complexite constante en trois dimensions portant sur les proprietes des droites tangentes a quatre objets, les diagrammes de Voronoi de droites et l'intersection de quadriques.

7. Qualitative Modeling and Simulation of Genetic Regulatory Networks

Hidde de Jong (INRIA Grenoble - Rhône-Alpes)

The adaptation of microorganisms to their environment is controlled at the molecular level by large and complex networks of biochemical reactions involving genes, RNAs, proteins, metabolites, and small signalling molecules. In theory, it is possible to write down mathematical models of these networks, and study these by means of classical analysis and simulation tools. In practice, this is not easy to achieve though, as quantitative data on kinetic parameters are usually absent for most systems of biological interest. Moreover, the models consist of a large number of variables, are strongly nonlinear and include different time-scales, which make them difficult to handle both mathematically and computationally.
We have developed methods for the reduction and approximation of kinetic models of bacterial regulatory networks to simplified, so-called piecewise-linear differential equation models. The qualitative dynamics of the piecewise-linear models can be studied using discrete abstractions from hybrid systems theory. This enables the application of model-checking tools to the formal verification of dynamic properties of the regulatory networks. The above approach has been implemented in the publicly-available computer tool Genetic Network Analyzer (GNA) and has been used to analyze a variety of bacterial regulatory networks.
I will illustrate the application of GNA by means of the network of global transcription regulators controlling the adaptation of the bacterium *Escherichia coli* to environmental stress conditions. Even though *E. coli* is one of the best studied model organisms, it is currently little understood how a stress signal is sensed and propagated through the network of global regulators, and leads the cell to respond in an adequate way. Qualitative modeling and simulation of the network of global regulators has allowed us to identify essential features of the transition between exponential and stationary phase of the bacteria and to make new predictions on the dynamic behavior following a carbon upshift.

8. Robustesse en calcul géométrique, pratiques industrielles et apport du calcul formel

André Lieutier (Dassault - Aix-en-Provence)

Résumé fourni ultérieurement.

9. Du calcul de courbes d'extrême de courbure sur une surface au calcul de la topologie de courbes algébriques en général

Marc Pouget (INRIA Nancy - Grand Est, Équipe-projet Vegas)

Je présenterai un travail en collaboration avec Jean-Charles Faugère et Fabrice Rouillier de l'équipe SALSA. Le problème initial concernait la description de courbes d'extrême de courbure sur une surface connues sous le nom de « ridges ». Pour une surface générique, ces courbes présentent trois types de singularités. Une mise en équation du problème dans le cas d'une surface paramétrée a permis de certifier le calcul de ces points et d'en déduire la topologie de la courbe. Les méthodes de calcul formel utilisées sont la décomposition des systèmes de points singuliers selon leur type, les bases de Groebner et la représentation univariée rationnelle. Ces méthodes, présentant une variante de l'approche de calcul par sous-résultants et arithmétique sur des nombres algébriques réels, ont été généralisées pour le calcul de la topologie d'une courbe algébrique plane quelconque.

Exposés courts

10. Réduction des équations variationelles des systèmes hamiltoniens à deux degrés de liberté et leur intégrabilité

Ainhoa Aparicio (XLIM, Université de Limoges)

Grâce à la théorie de Morales Ramis nous savons qu'un système hamiltonien est non-intégrable si le groupe de Galois de son équation variationelle est non abélien. En utilisant ces connaissances, nous avons développé une méthode de réduction des équations variationelles qui nous permet de décider si un système hamiltonien à deux degrés de liberté est non-intégrable. L'un des intérêts de cette réduction est qu'elle ne réduit pas uniquement les premières équations variationelles mais aussi l'expression de toutes les équations variationelles successives. En illustration de notre méthode nous donnerons une démonstration alternative de la non-intégrabilité du problème de Hill (Morales-Simo-Simon). Travail développé en collaboration avec Jacques-Arthur Weil.

11. Développements de fonctions D-finies sur des polynômes de Tchebychev.

Alexandre Benoît (Équipe-projet Algo, Laboratoire MSR-INRIA)

Une fonction D-finie est une solution d'équation différentielle linéaire à coefficients polynomiaux. Il est bien connu que les développements en série de Taylor de ces fonctions ont des coefficients qui vérifient une récurrence linéaire. La même propriété est vérifiée par les coefficients des développements de ces fonctions en série de Tchebychev (c'est-à-dire sur la base des polynômes de Tchebychev). Ces développements possèdent des propriétés intéressantes du point de vue de l'approximation, ce qui motive leur étude et la recherche d'algorithmes efficaces pour leur calcul. Alors que de tels algorithmes sont classiques dans le cas des séries de Taylor, les méthodes connues pour les séries de Tchebychev n'avaient pas été étudiées du point de vue de la complexité. Dans cet exposé, je décrirai les algorithmes existants et je donnerai un nouvel algorithme plus efficace réalisé lors de mon stage. J'exposerai aussi la théorie mathématique sur laquelle reposent ces algorithmes.

12. Index calculus and large prime variation for the DLP on hyperelliptic curves

Jean-François Biasse (École polytechnique)

Une courbe hyperelliptique $\mathcal{C}$ sur un corps $\mathbb{F}_q$ est la donnée de solutions de l'équation :

$$Y^2 + v(X)Y + u(X) = 0$$

Elle définit une variété algébrique dite "Jacobienne" **Jac** dont les éléments sont appelés des diviseurs. Cette variété est munie d'une structure de groupe, ce qui nous permet par exemple d'y étudier le problème du logarithme discret (DLP). Supposons que P et Q soient deux diviseurs de **Jac**, calculer le logarithme discret de Q en base P, c'est trouver α tel que :

$$Q = \alpha P$$

L'étude du logarithme discret est motivée par l'existence de plusieurs cryptosystèmes reposant sur sa difficulté, notamment le très célèbre protocole d'échange de clef "Diffie-Hellman".Sa difficulté est variable suivant le groupe dans lequel nous l'étudions. Dans le cadre des courbes hyperelliptiques les meilleures attaques connues sont en complexité "sous-exponentielle".
Le calcul d'index est la stratégie permettant d'atteindre une complexité sous-exponentielle. On définit un ensemble de diviseurs $\mathcal{B}$ que l'on appelle la base de friabilité, puis on recherche des relations du type :

$$\alpha P + \beta Q = \sum P_i \quad P_i \in \mathcal{B}$$

Ces relations forment une matrice dont un vecteur du noyau permet de déduire la solution du problème étudié. Le problème qui se pose est que cette matrice est souvent de taille prohibitive. Nous étudierons pendant l'exposé comment réduire la taille de cette matrice afin que la recherche d'un élément de son noyau soit faisable, notamment via la stratégie appelée "large prime variation" ou bien la suppression de colonnes via une élimination du type Gauss structurée.

13. Multiplication complexe et discriminants

Gaëtan Bisson (INRIA Nancy - Grand Est)

La théorie de la multiplication complexe décrit les anneaux d'endomorphismes de variétés abéliennes comme ordres dans certains corps de nombres. On l'utilise notamment pour la construction de telles variétés, par exemple dans le cadre d'applications cryptographiques. Nous présenterons cela puis nous intéresserons plus spécifiquement au cas où l'ordre en question n'est pas maximal et aux problèmes que cela induit concernant la réduction modulo des premiers. En particulier, en genre 1, nous expliquerons en quoi cela affecte la construction de courbes elliptiques et comment on cet ordre peut être déterminé.

14. Preuves formelles et équation des ondes

Sylvie Boldo (INRIA Saclay - Île-de-France, Équipe-projet ProVal)

Ce travail a été effectué avec François Clément, Jean-Christophe Filliâtre et Micaela Mayero dans le cadre de l'ANR blanche CerPAN. Nous voulons prouver formellement et complètement (erreur de méthode et erreurs d'arrondi) de vrais programmes numériques. Nous commençons modestement avec la résolution de l'équation des ondes en utilisant un programme C de François Clément et la plateforme Why. La boucle principale de ce programme est :

```
for (k=1 ; k<nk ; k++) {
  p[0][k+1] = 0. ;
  for (i=1 ; i<ni ; i++) {
    dp = p[i+1][k] - 2.*p[i][k] + p[i-1][k] ;
    p[i][k+1] = 2.*p[i][k] - p[i][k-1] + a*dp ;
  }
  p[ni][k+1] = 0. ;
}
```

Borner les erreurs dues aux calculs flottants nécessite une technique originale. En effet, une simple borne de l'erreur d'arrondi de chaque calcul implique une borne d'erreur proportionnelle à 2^k à l'étape k, ce qui est très exagéré. En effet, les erreurs de calcul se compensent de façon assez importante à chaque étape. Pour justifier ce fait, on détermine une erreur analytique, c'est-à-dire une expression mathématique exacte et signée de l'erreur de calcul. Cette erreur analytique est assez compliquée dans ce cas (double sommation pyramidale), mais est démontrable par récurrence. Elle permet de prouver que l'erreur d'arrondi à l'étape k est proportionelle à k^2. Borner l'erreur de méthode est un résultat classique de la littérature. Néanmoins, passer de la littérature à une preuve formelle recèle de nombreux problèmes de définitions et d'imprécisions. Néanmoins, prouver un vrai programme d'analyse numérique s'est révélé bien plus difficile que prévu. Une simple résolution de l'équation des ondes a fait surgir de nombreux problèmes tant au niveau mathématique qu'au niveau formalisation et preuves formelles.

15. Codes tordus dont le rang ou la distance minimale est prescrite

Lionel Chaussade (IRMAR)

Nous étudierons le lien entre les équations aux différences sur un corps fini et un certain anneau de Ore de polynômes. Cette analogie donnera une méthode pour engendrer des codes correcteurs particuliers, dits codes tordus, dont on pourra contrôler le corps de définition et la distance rang. Une approche différente nous permettra de générer des codes BCH tordus dont la distance minimale sera prescrite. Grâce à ces méthodes, on verra que l'on a pu trouver des codes correcteurs augmentant la meilleure distance minimale connue. Travail en commun avec Pierre Loidreau et Félix Ulmer.

16. Factorisation d'entiers à l'aide de courbes de genre 2

Romain Cosset (INRIA Nancy - Grand Est)

L'algorithme ECM (*Elliptic curve method*) introduit par Lenstra dans les années 1980 est un algorithme probabiliste permettant de trouver des facteurs pas trop gros (jusqu'à une soixantaine de chiffres décimaux) d'un nombre entier. Son intérêt est que sa complexité dépend peu de la taille du nombre à factoriser mais de la taille de ses facteurs. L'algorithme ECM est utilisé dans la chaîne de factorisation d'un nombre. Il est possible de généraliser cet algorithme en utilisant des courbes de genre 2 au lieu des courbes elliptiques (de genre 1). Cette généralisation fait apparaître deux difficultés : premièrement, la probabilité de succès est moins bonne et, deuxièmement, les opérations sur ces courbes sont plus lentes que sur les courbes elliptiques. Ces deux problèmes sont résolus séparément. L'utilisation de courbes hyperelliptiques particulières (courbes $(2,2)$-décomposables) améliore la probabilité de succès de l'algorithme. Par ailleurs pour accélérer l'arithmétique, on travaillera sur les surfaces de Kummer. C'est actuellement, la méthode la plus rapide pour calculer sur les courbes de genre 2. La mise en œuvre de ces solutions soulève, cependant, des problèmes techniques. D'un point de vue pratique, on parvient à des paramétrisations permettant d'accélérer l'algorithme. Après avoir décris les algorithme ECM et HECM (*Hyperelliptic curve method*), je présenterai les surfaces de Kummer et notamment leurs propriétés arithmétiques. Finalement j'expliquerai comment avoir une paramétrisation des courbes hyperelliptiques de telle façon que l'algorithme HECM fonctionne. (Travail de thèse sous la direction d'Emmanuel Thomé.)

17. Principe de transposition et algorithmes pour les tours d'Artin–Schreier

Luca De Feo (LIX, École polytechnique)

Le *principe de transposition* est connu sous beaucoup de formes. En voici une formulation proche de l'algorithmique :

« Tout algorithme qui calcule une fonction f peut être transformé en un algorithme qui calcule la fonction *transposée* de f ayant la même complexité à une constante près. »

Le principe se réalise en une technique de transposition d'algorithmes largement répandue dans la communauté du calcul formel. Nous appliquons cette technique dans le cadre des tours d'extension d'Artin–Schreier pour obtenir des algorithmes avec des complexités quasi-optimales. Soit K un corps de caractéristique p, une extension d'Artin–Schreier est une extension algébrique définie par un polynôme de la forme $X^p - X - \alpha$ avec $\alpha \in K$. Nous nous intéressons aux tours d'extensions d'Artin–Schreier sur les corps finis. Nous donnons des algorithmes quasi-optimales pour l'arithmetique de ces tours et nous les appliquons pour la solution de certains problèmes classiques en théorie des nombres.

18. Calcul du type topologique d'une surface implicite

Daouda-Niang Diatta (XLIM, Université de Limoges)

Nous décrivons un algorithme permettant de calculer un complexe simpliciale isotope à une surface. Cette algorithme est symbolique-numérique, certifié et repose fortement sur l'algorithme de calcul de topologie de courbes gauches implicites présenté lors de la précédente édition des JNCF.

19. Utilisation de bases elliptiques pour le paramétrage de tores algébriques

Clément Dunand (IRMAR)

Le thème de notre travail est le paramétrage des tores algébriques $T_n(F_q)$, de dimension $\varphi(n)$, définis sur un corps fini. La rationalité ou stable rationalité des tores algébriques T_n a donné lieu à plusieurs travaux récents. Parmi eux un articel de Maten van Dijk et David Woodruff (2004), propose une représentation de ces tores. Il s'agit de construire une bijection entre $T_n(F_q) \times \left(\prod_{d|n,\mu(n/d)=-1} F_{q^d}^\times\right)$ et $\prod_{d|n,\mu(n/d)=1} F_{q^d}^\times$. Autrement dit, on identifie tous les points du tore avec des points de $F_{q^n}^\times$ et cette identification est une bijection explicite grâce à l'ajout de quelques composantes complémentaires. L'algorithme présenté pour effectuer ce calcul utilise de nombreuses opérations (multiplication, exponentiation) dans F_{q^n} ou des sous-corps de ce corps fini, ce qui soulève naturellement la question du temps nécessaire à ce calcul. Il s'agit pour nous de raffiner les temps de calcul de ces fonctions en utilisant une nouvelle représentation des extensions de corps mises en jeu : les bases normales elliptiques. Les bases elliptiques ont été introduites très récemment par Jean-Marc Couveignes et Reynald Lercier et peuvent être construites pour toute extension de corps. Leur utilisation permet de réaliser notamment les exponentiations par les puissances de q de manière efficace et peut ainsi accélérer certaines étapes de calcul.

20. Codes correcteurs d'erreurs sur des surfaces Hermitiennes

Frédéric Edoukou (CNRS, Institut de Mathematiques de Luminy)

En 1985, R. Tobias, thésard de I. Chakravati à l'UNC-CH en Caroline du Nord, présenta l'étude des codes construits sur des surfaces hermitiennes sur le corps fini à quatre éléments grâce à un traitement à l'ordinateur. Son travail fut achévé en 1986 par P. Spurr à l'UNC-CH qui par un traitement informatique détermina la distance minimale ainsi que la distribution des poids ce code. En 1991 Sørensen dans sa thèse de doctorat à Aarhus en s'affranchissant de l'outil informatique, donna une approche plus générale et plus géométrique de l'étude ce code construit sur la surface hermitienne. Il formula une conjecture sur sa distance minimale qui suscita plusieurs tentatives de résolutions quelques années plus tard. Dans cet exposé nous allons répondre à cette conjecture. En utilisant des résultats de géométrie finie nous donnerons la distribution des poids et proposerons une généralisation de nos résultats aux codes hermitiens en dimension supérieure.

21. Variétés polaires et bipolaires

Marc Giusti (CNRS / LIX, École polytechnique)

Un algorithme efficace pour trouver un point représentatif algébrique par composante connexe d'une variété algébrique réelle, intersection complète et lisse, a été publié dans des travaux précédents. Cet algorithme est basé sur l'exploitation des variétés polaires génériques et sa complexité est intrinsèque au problème. Il s'agit ici de généraliser ce résultat au cas singulier. Nous introduisons une construction naturelle permettant de nous ramener à une situation en dimension et codimension plus grandes, lisse mais non compacte. (Travail commun avec Bernd Bank, Joos Heintz et Luis Miguel Pardo.)

22. Certified and fast computation of supremum norms of approximation errors

Mioara Joldes (Équipe-projet Arénaire, LIP, École Normale Supérieure de Lyon)

One of the major objectives of the Arenaire team is the design of mathematical libraries and of tools that aim to improve and automate the evaluations of floating-point expressions, to obtain faster a better floating-point code with guarantees on the results quality. For example, various software projects, like CRLibm [1], FloPoCo [2], Metalibm [3] or Sollya [4], focus on the floating-point evaluation of useful functions, on how this process can be automated and on the validation of the obtained numerical accuracy. One of the basic bricks in this automated tool chain consists in computing a fast and certified bounding of approximation errors. In fact, the request is to determine the maximum error between a function $f : R- > R$, such as exp, sin, erf, and a polynomial p, which approximates the function over an interval. The tight, yet certain bounding of this error (relative or absolute) leads to a fast and safe computation of the supremum norm of the error function.
The main difficulty of this problem is due to the fact that this approximation error is very small and the difference $f - p$ is highly cancellating. Specifically, the cancellation effect is due to the subtraction of terms that are very near and is a major source of numerical errors. In consequence, previous approaches for computing the infinity norm in our degenerate case have proven to be either unsafe, not sufficiently tight, or too tedious in manual work.
We present a safe and fast algorithm that offers automatically and certainly a tight lower and upper bound for the infinite norms of error functions. The algorithm is based on a combination of several techniques, including enhanced interval arithmetic, automatic differentiation and polynomial roots isolation. This combination of tools allows us to overcome the cancellation effects and to safely implement this algorithm in our software tool Sollya.
This is a joint work with Sylvain Chevillard (LIP, Arenaire) and Christoph Lauter (LIP, Arenaire).

[1] http ://lipforge.ens-lyon.fr/www/crlibm/
[2] http ://www.ens-lyon.fr/LIP/Arenaire/Ware/FloPoCo/
[3] http ://lipforge.ens-lyon.fr/www/metalibm/
[4] http ://sollya.gforge.inria.fr/

23. Nœuds toriques polynomiaux

Pierre-Vincent Koseleff (Institut de mathématiques de Jussieu, UPMC PARIS6)

Application des approximants de Padé à un problème de géométrie réelle. D'une question de représentation de nœuds par des courbes polynomiales gauches, nous nous ramenons à un problème de construction de courbes planes trigonales. Nous proposons une construction dont la preuve et l'obtention explicite reposent sur des propriétés de certains approximants de Padé. Il semble prouvé à présent (travail en cours avec E. Brugallé et D. Pecker) que cette construction fournit des courbes polynomiales de degré lexicographique minimum.

24. Approximation au premier ordre des variétés lentes

François Lemaire (UFR IEEA, Université Lille I)

Une façon de modéliser les systèmes biologiques est d'utiliser des systèmes de réactions chimiques. Ces derniers peuvent être étudiés par équations différentielles. En supposant certaines réactions lentes ou rapides, on peut réduire les systèmes de réactions chimiques en système d'équations différentielles faisant intervenir moins d'inconnues. Cette réduction directement basée sur l'étude des systèmes singulièrement perturbés et sur le théorème de Tikhonov, s'appuie sur des notions techniques, dont l'une est l'approximation de la variété lente (qui est intuitivement une variété le long de laquelle les solutions « glissent » après avoir suivi un transitoire rapide). Nous verrons comment obtenir une approximation au premier ordre de la variété lente dans le contexte de l'étude des systèmes de réactions chimiques, et pourquoi cette approximation est nécessaire sur un exemple tiré de la littérature.

25. Certificats de positivité et minimisation polynomiale dans la base de Bernstein multivariée

Richard Leroy (IRMAR)

Soit $f \in \mathbb{Z}[X_1, \ldots, X_k]$ un polynôme multivarié, et soit

$$\Delta = \left\{ (x_1, \ldots, x_k) | \, \forall i, x_i \geq 0 \text{ et } \sum x_i = 1 \right\}$$

le simplexe unité de $\mathbb{R}^k$. La question de la positivité de f sur Δ est un problème classique en géométrie algébrique réelle et en calcul formel. Deux questions se posent :

1. Déterminer si f est strictement positif sur Δ ou non
2. Le cas échéant, trouver une écriture de f qui rende évidente cette positivité.

Une telle écriture est appelée certificat de positivité de f sur Δ.
Le cas de la dimension 1 a été traité par Boudaoud, Caruso et Roy [BCR]. La généralisation en dimension quelconque fait l'objet de la première partie du présent exposé.
Pour cela, on introduira la base de Bernstein, plus adaptée au problème que la traditionnelle base des monômes. Elle permet notamment de définir le polytope de contrôle de f, fournissant une approximation de son graphe. L'étude précise de la distance entre le polytope de contrôle et le graphe de f sera présentée, permettant l'utilisation de techniques d'élévation de degré et de subdivision. La méthode de subdivision, basée sur l'algorithme de De Calsteljau, se révèle plus efficace. Un algorithme sera alors présenté, décidant si un polynôme donné est strictement positif sur Δ ou non. Il fournit de plus un certificat de positivité le cas échéant. Une borne sur la taille du certificat obtenu sera également donnée.
Dans un second temps, le problème classique ([KLP]) de minimisation de f sur le simplexe Δ sera abordé. Un algorithme de subdivision sera également présenté, basé sur les mêmes techniques que précédemment. L'étude de sa complexité a été menée et sera présentée.

[BCR] Fatima Boudaoud, Fabrizio Caruso, Marie-Françoise Roy, *Certificates of Positivity in the Bernstein Basis*, Discrete and Computational Geometry Volume 39, Number 4 (2008), 639-655.

[KLP] Etienne de Klerk, Monique Laurent, Pablo A. Parrilo, *A PTAS for the minimization of polynomials of fixed degree over the simplex*, Theor. Comput. Sci. Volume 361, Number 2 (2006), 210-225

26. Robots et positions cuspidales

Guillaume Moroz (LIP6)

L'étude de la géométrie des robots est un problème difficile et important pour la planification de trajectoire. Un robot est dit cuspidal si il possède des points cuspidaux. On verra que cette caractéristique est importante pour mesurer la souplesse du robot.
Soit $S(\mathbf{T}, \mathbf{X})$ un système paramétré d'équations modélisant la géométrie d'un robot, où $\mathbf{T}$ représente k variables de contrôle et $\mathbf{X}$ désigne n variables de positions. Chaque solution $(\mathbf{T}_0, \mathbf{X}_0)$ de $S(\mathbf{T}, \mathbf{X})$ correspond a une position admissible du robot. De plus, si $(\mathbf{T}_0, \mathbf{X}_0)$ est une racine de multiplicité 3 de $S(\mathbf{T}_0, \mathbf{X})$, la position correspondante est alors dite cuspidale.
Dans un premier temps, nous verrons les propriétés vérifiées par les robots idaux, ainsi que les différentes méthodes existantes permettant calculer les pitions cuspidales. Nous présenterons ensuite une nouvelle méthode basée sur les propriétés algébriques locales des racines de multiplicité inférieure à 3.
L'application de cette méthode nous a permis d'obtenir la description complète des positions cuspidales des robots parallèles plans de type 3-RPR.

27. Dualité, moments et idéaux radicaux

Bernard Mourrain (INRIA Sophia Antipolis - Méditerrannée)

L'exposé portera sur des travaux récents exploitant le calcul de formes normales pour la résolution de systèmes polynomiaux et la dualité dans les algèbres quotients. Un algorithme de forme normale pour un idéal zérodimensionnel produit des tables de multiplications et par calcul de valeurs et vecteurs propres, il permet d'obtenir toutes les solutions complexes du système avec leur multiplicité. Nous décrirons des extensions de cette approche permettant de calculer le radical de l'idéal, ou même le radical réel, décrivant les solutions réelles sans multiplicité, quand celles-ci sont isolées. Ces nouvelles méthodes exploitent fortement les propriétés des algèbres de Gorenstein et des techniques de programmation semi-définie positive. C'est un travail en commun avec J.B. Lassere, M. Laurent, Ph. Rostalski, Ph. Trébuchet.

28. Résoudre et certifier la solution d'un système linéaire

Hong Diep Nguyen (Équipe-projet Arénaire, LIP, École normale supérieure de Lyon)

Nous proposons une approche pour résoudre un système linéaire et simultanément certifier la solution calculée. Par « certifier », on entend calculer un encadrement garanti de l'erreur. Pour cela, nous passons de l'arithmétique flottante à l'arithmétique par intervalles et nous résolvons le système linéaire satisfait par le résidu. Cela nous donne une borne garantie de l'erreur sur le résultat exact.
L'utilisation du résidu est classique dans les méthodes de raffinement itératif. Nous avons adapté l'une de ces méthodes pour le calcul de la borne d'erreur. La combinaison de ces deux composantes, à savoir la résolution en arithmétique flottante d'un système linéaire et le raffinement itératif de la borne d'erreur en utilisant l'arithmétique par intervalle, produit une solution plus précise dotée d'une borne d'erreur. Cette borne d'erreur nous permet d'estimer en outre le nombre de chiffres corrects de la solution approximative.
Une autre question se pose naturellement : on sait que la précision de la solution ainsi raffiné dépend pour une grande part de la précision utilisée pour le calcul du résidu. Classiquement, une précision doublée sera utilisée pour le calcul du résidu. Notre approche est implantée en utilisant la bibliothèque MPFR, qui offre l'arithmétique flottante de précision arbitraire, et la bibliothèque MPFI pour son homologue par intervalle. Ces bibliothèques nous permettent d'adapter la précision utilisée à chaque étape. Cela nous a permis d'étudier aussi l'effet de la précision utilisée pour le calcul du résidu sur la qualité du résultat calculé.
Les résultats expérimentaux illustrent le gain au niveau de la qualité de la solution et de la borne d'erreur lié à la précision utilisée pour les calculs.
Références :

[1] N.J. Higham ; *Accuracy and Stability of Numerical Algorithms*, 2nd edition, SIAM Press, 2002. Chapter 12 : Iterative Refinement.

[2] A. Neumaier ; *Interval methods for systems of equations*, Cambridge University Press, 1990. Chapter 4 : The solution of square linear systems of equations.

29. Le problème d'équivalence du point de vue algébrique

Michel Petitot (LIFL, Université de Lille I)

Il y a actuellement deux formalismes pour traiter les systèmes d'équations différentielles :

1. Le calcul différentiel extérieur portant sur les formes différentielles utilisés par les géomètres, les physiciens, en théorie du controle etc.
2. L'algèbre différentielle (commutative) portant sur les polynomes différentiels et les opérateurs différentiels linéaires, utilisée par Ritt (1930) dans le cas non linéaire et par Picard et Vessiot (1900) en théorie de Galois des équations linéaires, etc.

Le formalisme 1 (géométrique) permet d'adapter les repères (ce qui réduit la taille des formules) au cours des calculs. C'est le formalisme utilisé par J. Drach (1900) et B. Malgrange (2000) en théorie de Galois des équations non linéaires et par É. Cartan pour traiter du problème d'équivalence (1905).
Le formalisme 2 permet de traiter les inéquations différentielles, les équations différentielles d'ordre 0 (*i.e.* algébriques) et d'éliminer des variables.
Le dictionnaire entre les deux formalismes n'est pas facile. Il semble que le lien passe entre autre par la notion de groupoide développée dans les années 50 par C. Erhesmann, un éléve de É. Cartan puis repris en géometrie algébrique dans les années 60.
Bien que le travail soit loin d'être terminé, nous essayerons de dégager quelques pistes de réflexion.

30. Calcul numérique-symbolique de développements de Puiseux

Adrien Poteaux (INRIA Sophia Antipolis - Méditerrannée)

Étant donné un polynôme $F \in k[x, y]$ et une racine α du discriminant de F en y, il est difficile de calculer numériquement les développements de Puiseux de f au dessus de α (i.e. les séries en $(x - \alpha)$ solutions de F vu comme un polynôme univarié en y). Le calcul symbolique de ces séries peut s'avérer couteux, que ce soit par l'extension de k dans laquelle sont définies les coefficients ou par la croissance de la taille de ces coefficients. De plus, l'évaluation de ces coefficients peut demander une précision non négligeable, de notamment à cette croissance des coefficients.
Néanmoins, en étudiant l'algorithme de Newton-Puiseux, on peut remarquer qu'il n'y a que deux types d'informations exactes nécessaires : les pentes successives des polygones de Newton et les multiplicités des racines des polynômes caractéristiques associés.
Nous détaillerons un algorithme qui calcule numériquement ces développements de Puiseux, en utilisant un calcul préliminaire modulo un nombre premier p bien choisi de ces développements de Puiseux. Le nombre premier p est tel que tous les termes qui introduisent une séparation des racines de f (c'est-à-dire les termes provenant d'une pente non entière ou ceux provenant d'un polynôme caractéristique ayant plus d'une racine) ne soient pas réduit à 0 modulo p. A partir de ces séries calculées modulo p, on reconstruit la suite des polygones et multiplicités dont on a besoin pour nos calculs numériques. Puis cet « arbre de polygones » nous permet de calculer numériquement les séries.
C'est un travail effectué dans le cadre de ma thèse, en collaboration avec Marc Rybowicz.

31. Méthodes semi-algébriques en épidémiologie

Marie-Françoise Roy (IRMAR)

L'exposé présentera le résultat d'un travail en collaboration entre Otto Adamou (doctorant, Niger), Thierry van Ellefterre (modélisateur industrie pharmaceutique, Belgique), M'hamed El Kahoui (professeur, Maroc) et moi-même sur l'étude de la stabilité d'équilibres épidmiologiques sans maliadie ou endémiques, basée sur la notion de bifurcation transcritique.

32. Automate globalement convergent pour le calcul de toutes les racines d'une équation algébrique

Olivier Ruatta (XLIM, Université de Limoges)

On décrit un analogue continu de la méthode de Weierstrass qui conduit à un automate globalement convergent pour la résolution d'une équation univariée. Les principaux outils sont l'analyse effective et un peu de théorie des revêtements différentiels.

33. Real Solving Singular Polynomial Systems

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

Je commencerai par présenter divers systèmes d'égalités polynomiales provenant d'applications en mécanique céleste et en géométrie algorithmique. Ces systèmes définissent des variétés singulières. Pour chacun de ces problèmes, la question posée est de *déterminer l'existence de solutions réelles* (qu'elles soient régulières ou singulières) et, si elles existent, de donner *au moins un point sur chacune des composantes connexes* de la variété définie par le système considéré.
Il est aujourd'hui bien connu qu'aborder ce problème sous l'angle de la décomposition cylindrique algébrique contraint à subir une complexité théorique doublement exponentielle en le nombre de variables, y compris dans des situations non pathologiques, ce qui limite considérablement l'utilisation en pratique de cette approche dans les problèmes mentionnés plus haut. Les méthodes de points critiques introduites à la fin des années 80 offrent un cadre permettant d'appréhender ces problèmes avec une complexité théorique dominée par $D^{\mathcal{O}(n)}$ (où D est le degré des polynômes et n le nombre de variables) au prix d'un alourdissement de l'arithmétique (induit par l'introduction d'infinitésimaux) sur laquelle sont effectués les calculs. Sans maîtrise de la constante de complexité (située ici en exposant), il est illusoire de pouvoir produire des implantations efficaces permettant de résoudre les problèmes mentionnés ci-dessus, ce qui constitue notre objectif.
Dans le cas des hypersurfaces singulières, des résultats datant de 2005 ont permis d'obtenir un algorithme de calcul d'au moins un point par composante connexe dont la complexité était à la fois bien maîtrisée (dans de telles situations, la borne de Bézout domine strictement les degrés des objets géométriques représentés algébriquement en cours de calcul) et dont les performances pratiques avaient à l'époque permis la résolution d'applications inatteignables jusqu'alors. La suite de l'exposé sera consacrée à la présentation de la généralisation de cet algorithme au cas des systèmes polynomiaux définissant des variétés singulières (ou engendrant des idéaux non radicaux) — dont une esquisse est décrite dans les notes de cours des JNCF 2007. La complexité obtenue est un produit d'un facteur combinatoire (dépendant du nombre d'équations) et d'un facteur algébrique (élevé à une puissance que nous expliciterons). On verra que ce facteur algébrique est — comme dans le cas des hypersurfaces — strictement dominé par la borne de Bézout. On verra aussi que dans le cas où les équations sont quadratiques, on obtient un algorithme polynomial en le nombre de variables. Au total, la complexité de cet algorithme est dominée par $D^{\mathcal{O}(n)}$.
Une implantation préliminaire de cet algorithme a permis de résoudre les problèmes de mécanique céleste et de géométrie algorithmique mentionnés plus haut. Cette implantation sera prochainement intégrée à la bibliothèque Maple RAGlib (Real Algebraic Geometry Library).

34. Qualitative Analysis of Dynamical Systems : Application to Biology

Aslı Ürgüplü (LIFL, Université des Sciences et Technologies de Lille)

There are many ways to perform qualitative analysis of dynamical systems. However, this is a difficult task because such systems may have many state variables and especially many parameters. Their studies require special reduction techniques. One of the possibilities is to use exact reduction by means of Lie symmetries in order to increase the dimension of the coordinate space. For this issue, the ExpandedLiePointSymmetry package (see [3, 4]) may be used. Another exact reduction method, which is new to our knowledge, consists of using Lie symmetries in order to cylindrify the dynamical system. This means that a change of coordinates is applied in a such way that its fixed points depends on less parameters.
MABSys (Modelization and Analysis of Biological Systems) is a Maple package (see [2]) for gathering, as much as possible, necessary functions to determine the qualitative analysis of a dynamical system, also applicable to models of biological systems.
MABSys has three main parts. Its first part consists of representing chemical reactions and modeling them by means of ODE systems. It may perform quasi-steady state approximations which is an inexact reduction (see [1]) where some chemical reactions are considered faster then the others. The model study is the dynamic of the slow reactions assuming that the fast ones are at quasi-equilibrium. The second part performs a change of coordinates on either algebraic, semi-algebraic or ODE systems. This processus is based on scaling type Lie symmetries of the corresponding algebraic systems but can be used with no prior knowledge of them. The ExpandedLiePointSymmetry package (see [3]) is employed to seek for Lie symmetries. Finally, the third part is composed by several qualitative analysis functions. These two latest parts are complementary, meaning that, in general they are overlapped.
Change of coordinates processus uses only scaling type Lie symmetries. The first reason is the sake of computational simplicity. The second one is linked to biological models properties. For such models, one of the main assumptions is the positivity of its coordinates which is preserved by this kind of Lie symmetries.
(Thèse en cours sous la direction de François Boulier et Alexandre Sedoglavic.)

[1] Boulier, F.; Lefranc, M.; Lemaire, F. and Morant, P.-E. *Model Reduction of Chemical Reaction Systems using Elimination* MACIS 2007 `http://hal.archives-ouvertes.fr/hal-00184558/fr`.

[2] Lemaire, F. and Ürgüplü, A. *MABSys - Modelization and Analysis of Biological Systems* Maple package (available at `www.lifl.fr/~urguplu`), 2008.

[3] Sedoglavic, A. and Ürgüplü, A. *Expanded Lie Point Symmetry* Maple package (available at `www.lifl.fr/~urguplu`) 2007.

[4] Sedoglavic, A. *Reduction of Algebraic Parametric Systems by Rectification of their Affine Expanded Lie Symmetries* Proceedings of Algebraic Biology 2007 – Second International Conference 2007. Vol: 4545, pages: 277-291.

35. Mathemagix

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

Nous faisons la démonstration d'une première version alpha du système Mathemagix (voir aussi `http://www.mathemagix.org`). C'est un nouveau système de calcul formel et analytique, composé des parties suivantes :

1. Une série extensible de paquetages C++ avec des opérations rapides sur des types de base (polynômes, matrices, séries, mais aussi boules et fonctions analytiques).
2. Un langage haut niveau, actuellement inteprété, et avec un compilateur en cours de développement.
3. Un mécanisme de colle, permettant de rajouter de facon souple de nouveaux paquetages C++ à l'interprète/compilateur.

Le système admet GNU TeXmacs comme interface graphique, ainsi que le système Axel pour la visualisation 3D.

36. La conjecture des anneaux de Hermite en dimension 1

Ihsen Yengui (Faculté des Sciences de Sfax)

Je montrerai (constructivement) que pour tout anneau A de dimension de Krull ≤ 1, tous les $A[X]$-modules stablement libres sont libres. Ceci donne une réponse positive à la conjecture des anneaux de Hermite en dimension 1.