

Méthodes effectives et logiciels de la logique et de l'algèbre pour la géométrie algébrique et la cryptographie

Ecole CIMPA-ICTP-UNESCO-CAMEROUN

## **Objectifs :**

L'algorithmique pour la logique et l'algèbre a fait de gros progrès qui ont permis le développement de logiciels puissants et permettant d'étudier par des méthodes effectives des thématiques autrefois considérées comme abstraites et de traiter de nouvelles applications.

Cette école se propose d'introduire des techniques algorithmiques récentes en logique et en algèbre qui ont un impact important en géométrie algébrique, en cryptographie ou pour le traitement automatique de documents numériques.

Ces résultats ouvrent des perspectives vers des sujets de recherches très appliquées et d'impact grandissant sur l'industrie, mais également vers des thématiques plus théoriques en plein développement et qui devraient prendre de plus en plus d'importance ;

*Directeurs scientifiques et organisateurs :*

L. Goettsche (ICTP, Trieste, Italie), M-F Roy (Université de Rennes I, France), O. Ruatta (Université de Limoges, France), M. Tonga (Université de Yaoundé, Cameroun)

*Date et lieu :*

24 août-4 septembre 2009, Yaoundé, Cameroun

*Programme scientifique :*

– ***Outils formels pour la gestion de documents structurés.***

Eric Badouel (Rennes, France)

Cours de 5 H

Plan

1. Introduction générale (1h)

1.1. Documents structurés : quels usages ?

1.2. Représentations : mots, arbres ou graphes ?

1.3. Interpréter et transformer un document structuré

## 2. Reconnaître : les automates d'arbres (2h)

### 2.1. Cas des mots

### 2.2. Automates d'arbres

### 2.3. Validation de documents par automates d'arbres

### 2.4. Cohérence de vues et mise-à-jour de révisions d'un document

## 3. Transformer : les transducteurs d'arbres (2h)

### 3.1. Les transducteurs d'arbres

### 3.2. Les transducteurs d'arbres à attributs

### 3.3. Les transducteurs d'arbres avec paramètres

### 3.4. La composition de transducteurs

*Esprit* : Les documents structurés (ou semi-structurés) présentent une structure hiérarchique régulière facilitant leur interprétation et leur manipulation par des applications informatiques. Pour cette raison ils sont très largement utilisés pour interfacier des programmes; en particulier des applications distribuées sur l'internet grâce au formalisme XML qui permet la définition de schémas de documents structurés. Dans des applications coopératives un document structuré peut jouer le rôle d'un artefact représentant l'état courant d'une tâche circulant entre les différentes activités du système; il sert à représenter le résultat en cours d'élaboration ainsi que l'information permettant de coordonner les actions des différents intervenants du système. Enfin, une nouvelle façon de concevoir une application à base de composants consiste à développer des langages dédiés; ceux-ci sont implémentés par un jeu de combinateurs (fonctions d'ordres supérieurs); un programme dans un tel langage dédié est un terme (éventuellement récursif) vu comme un document actif : il lui est associé une interprétation. Ces différents usages soulèvent un certain nombre de questions : sait-on reconnaître qu'un document est conforme à un schéma donné ? Comment manipuler des documents partiellement définis (projection, fusion ...) ? Comment définir des transformations de documents (transducteurs) ? Quelle sont les familles de transformations closes par composition ? Nous introduisons des outils formels, basés sur des notions grammaticales, afin d'aborder ces différentes questions.

## Références

[1] J.A. Goguen, J.W. Thatcher, E.G. Wagner, J.B. Wright. Initial Algebra Semantics and Continuous Algebras. Journal of the Association for Computing Machinery, Vol. 24, N°1, January 1977, pp. 68-95.

[2] R. Alur, P. Madhusudan. Visibly pushdown languages. In 36th ACM Symposium on Theory on Computing (STOCS'04), pp. 202-211, 2004

[3] J. Berstel, L. Boasson. Formal Properties of XML Grammars and Languages.

[4] H. Comon, M. Dauchet, R. Gilleron, F. Jacquemard, D. Lugiez, S. Tison, M. Tommasi. Tree automata techniques and applications. <http://www.grappa.univ-lille3.fr/tata>, 2002.

[5] Z. Fulop, H. Vogler. Syntax-Directed Semantics - Formal Models Based on Tree Transducers. Monographs in Theoretical Computer Science, EATCS Series, Springer Verlag, 1980.

- [6] F. Gecseg, M. Steinby. Tree Automata. Akadémiai Kiadó, Budapest, 1984.
- [7] R. Giegerich. Composition and Evaluation of Attribute Coupled Grammars. Acta Informatica 25, 355-423, 1988.
- [8] J. Paakki. Attribute grammar paradigms - a high level methodology in language implementation. ACM Computing Surveys, 27(2): 196-255, 1995.
- [9] J.-C. Raoult. A Survey of Tree Transductions. In Nivat & Podelski Eds. Tree Automata and Languages pp. 311-326, 1992.

– ***Algorithmiques des nombres, polynômes et séries.***

Olivier Ruatta (Limoges, France)

Cours de 5 H

*Plan :*

1. Introduction générale (1/4 d'heure)
2. Représenter et manipuler des nombres élémentaires en machine (2 heures)
  - 2.1. Entiers multiprécision
  - 2.2. Rationnels
  - 2.3. Flottants et réels effectifs
  - 2.4. Complexités asymptotiques
3. Représenter et manipuler des polynômes (2 heures)
  - 3.1. Arithmétique naïve
  - 3.2. Diviser pour régner (Karatsuba)
  - 3.3. Evaluation et interpolation
  - 3.4. Diviser, c'est toujours multiplier !
  - 3.5. Nombres algébriques et nombres algébriques effectifs
4. Elements sur les séries et les fonctions analytiques effectives (3/4 d'heure)
  - 4.1. Arithmétiques des séries tronquées
  - 4.2. Fonctions analytiques effectives

*Esprit :*

Dans ce cours on donnera des techniques récentes et effectives (implantées) et on essaiera d'en mettre quelques unes en oeuvre à l'aide de Mathemagix. On ne donnera pas forcément les algorithmes les plus performants et on ne sera pas systématiques, mais on décrira des cas où l'apport algorithmique en termes d'efficacité est clair. La programmation joue un rôle important pour comprendre les enjeux de ces questions.

*Références :*

Cours de calcul formel de Bostan et al. au MPRI : <http://algo.inria.fr/salvy/mpri/poly.pdf>

J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge University Press, 1999.

R. P. Brent, P. Zimmermann, Modern Computer Arithmetic, in preparation (<http://www.loria.fr/~zimmerma/mca/mca-0.3.pdf>)

J. van der Hoeven. Effective complex analysis. JSC, 39:433–449, 2005.

– ***Algèbre commutative effective et géométrie algébrique.***

Trois cours de 5 H

## *Cours 1 : Algèbre commutative effective*

Henri Lombardi (Besançon, France)

Plan :

1. Matrices à coefficients entiers (2 heures)
  - 1.1. Réduction de Smith. Complexité algorithmique.
  - 1.2. Systèmes linéaires sur  $\mathbb{Z}$
  - 1.3. Sous  $\mathbb{Z}$ -modules de type fini de  $\mathbb{Z}^n$
  - 1.4.  $\mathbb{Z}$ -modules de présentation finie
  - 1.5. Noéthérianité et cohérence, Généralisation aux anneaux principaux
  
2. Systèmes linéaires sur les anneaux commutatifs (1 heure 30)
  - 2.1. Systèmes de Cramer. Idéaux déterminantiels.
  - 2.2. Anneaux et modules cohérents
  - 2.3. Principe local-global
  - 2.4. Modules libres de rang fini
  - 2.5 Modules de présentation finie
  
3. Anneaux de polynômes sur les corps discrets (1 heure 30)
  - 3.1. Cohérence
  - 3.2. Bases de Gröbner
  - 3.3. Applications des BDG

*Esprit :*

Dans ce cours on donne quelques techniques constructives de base en algèbre commutative. On en profite pour expliquer comment l'exigence d'effectivité modifie le point de vue sur le fonctionnement des démonstrations.

*Références :*

- 1) Modules sur les anneaux commutatifs (cours de M1). Henri Lombardi  
<http://hlombardi.free.fr/publis/NotesDeCours.html>
- 2) Algèbre Commutative. Méthodes constructives. (livre à paraître)  
Henri Lombardi, Claude Quitté  
<http://hlombardi.free.fr/publis/LivresBrochures.html>
- 3) Cox D., Little J., O'Shea D. Ideals, varieties and algorithms, Second edition.  
New York, Springer-Verlag, 1997.
- 4) The Buchberger Algorithm as a Tool for Ideal Theory of Polynomial Rings in Constructive

Mathematics,

in: Gröbner Bases and Applications (Proc. of the Conference 33 Years of Gröbner Bases),

Cambridge University Press, London Mathematical Society Lecture Notes Series, vol. 251, (1998), 393-407.

Hervé Perdry, Henri Lombardi <http://hlombardi.free.fr/publis/GBPerLom.pdf>

## **Cours 2 : Modules projectifs sur les anneaux de polynômes un point de vue constructif**

Ihsen Yengui (Sfax, Tunisie)

Plan:

1. Théorie constructive des modules projectifs, Preuves de Quillen et Suslin de la conjecture de Serre.
2. Une méthode générale pour rendre l'utilisation des idéaux maximaux constructive.
3. Théorie constructive des anneaux arithmétiques.
4. Comparaison constructive entre les anneaux  $R(X)$  et  $R\langle X \rangle$  et application au théorème d'induction de Lequain-Simis.
5. Nouveau progrès concernant la conjecture des anneaux de Hermite.
6. Bases de Gröbner dynamiques sur les anneaux de Dedekind avec diviseurs de zéro.

*Esprit:*

Tous les résultats classiques ou nouveaux que nous allons voir dans ce cours vont être prouvés constructivement.

*Références:*

- 1) Cox D., Little J., O'Shea D. Ideals, varieties and algorithms, Second edition. New York, Springer-Verlag, 1997.
- 2) Ducos L., Quitté C., Lombardi H., Salou M. Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind. J. Algebra 281 (2004) 604-650.
- 3) Ellouz A., Lombardi H., Yengui I. A constructive comparison of the rings  $R(X)$  and  $R\langle X \rangle$  and application to the Lequain-Simis induction theorem, J. Algebra 320 (2008) 521-533.
- 4) Lam T. Y. Serre's Problem on Projective Modules. Springer Monographs in Mathematics, 2006.
- 5) Lombardi H., Quitté C. Théorie constructive élémentaire des modules projectifs de type fini. 2003. (Preprint).
- 6) Lombardi H., Yengui I. Suslin's algorithms for reduction of unimodular rows. J. Symb. Comp. 39 (2005) 707-717.
- 7) Yengui I. Making the use of maximal ideals constructive. Theoretical Computer Science 392 (2008) 174-178.
- 8) Yengui I. Dynamical Gröbner bases. J. Algebra 301 (2006) 447-458.

9) Yengui I. The Hermite ring conjecture in dimension one. J. Algebra 320 (2008) 437-441.

### **Cours 3 : *Homologie de Koszul et applications.***

Francis Sergerat (Grenoble, France)

#### *Plan:*

1. Notion d'opérateur différentiel et de groupe d'homologie.
2. Notion de «solution du problème homologique» et d'«homologie effective».
3. Complexe de Koszul associé à un module sur un anneau de polynômes.
4. Homologie de Koszul effective de l'anneau des polynômes.
5. Lemme de perturbation homologique.
6. Notion de cône d'un morphisme de complexes.
7. Homologie effective d'un cône.
8. Les théorèmes SES.
9. Homologie de Koszul effective d'un idéal monomial.
10. Le cas général.
11. Application au calcul de résolutions effectives.
12. Le cas des résolutions minimales.

#### *Esprit:*

Le complexe de Koszul intervient dans de multiples questions ; il sert en particulier à analyser la nature homologique locale d'un idéal en un point, plus généralement d'un module sur un anneau local régulier.

Le contexte est élémentaire et très commode pour introduire les diverses notions d'homologie effective. Une méthode très simple est donnée pour calculer l'homologie effective d'un idéal, dont on déduit en particulier une résolution effective du même idéal, inversant le processus usuel «module  $\rightarrow$  résolution  $\rightarrow$  homologie de Koszul»

#### *Référence:*

Chapitres 2-4-5-6 du cours [www-fourier.ujf-grenoble.fr/~sergerat/Papers/Genova-Lecture-Notes.pdf](http://www-fourier.ujf-grenoble.fr/~sergerat/Papers/Genova-Lecture-Notes.pdf)

### **– *Logique et algèbre en géométrie réelle.***

Deux cours de 5 H

#### ***Cours 1: Les outils de l'algèbre réelle et leur utilisation en géométrie et en logique***

Marie-Françoise Roy (Rennes, France)

#### *Plan*

- 1 Les résultats de base de l'algèbre réelle: théorèmes de Descartes et de Sturm (2 heures)

## 2 Ensembles semi-algébriques et élimination des quantificateurs (1h 30)

### 2.1. La démonstration de Tarski

### 2.2. Sous-resultants et élimination des quantificateurs "à la Collins"

## 3. Bases de Bernstein, isolation des racines et certificats de positivité (1H 30)

Des exemples illustratifs et séances de TP proposées en supplément utiliseront la librairie SARAG en MAXIMA.

### *Esprit*

Les deux théorèmes les plus classiques de l'algèbre réelle, dus à Descartes et Sturm continuent à jouer un rôle clef dans le domaine

- le théorème de Sturm et ses améliorations grâce aux sous-résultants est lié à l'élimination des quantificateurs, qui est à la base de la liaison entre la géométrie et une branche de la logique, la théorie des modèles
- le théorème de Descartes joue un rôle clé dans les méthodes efficaces pour l'isolation des racines réelles et les certificats de positivité

### *Références*

Algorithms in real algebraic geometry de S.Basu, R. Pollack et M.-F. Roy, téléchargeable sur <http://perso.univ-rennes1.fr/marie-francoise.roy/bpr-posted1.html>

F. Boudaoud, F. Caruso M.-F. Roy Certificates of positivity in the Bernstein basis, Discrete and Computational Geometry 39 4 639-655 (2008)

## ***Cours 2: Formalisation de mathématiques en théorie des types ou comment utiliser un ordinateur pour faire des démonstrations***

- Assia Mahboubi (Paris, France)

### *Plan :*

#### 1. Introduction à la preuve formelle (1h30)

##### 1.1 Preuves formelles et mathématiques contemporaines

##### 1.2 Assistants à la preuve

##### 1.3 Un peu de théorie des types

#### 2. Premiers pas en Coq (1h)

##### 2.1 Quelques exemples de preuves élémentaires dans le système Coq

##### 2.2 Choix des structures de données

#### 3. Arithmétiques formelles

##### 3.1 Nombres entiers, rationnels, réels en Coq

3.2 Automatisation des preuves, principes

3.3 Exemple de procédures de décision certifiées

4. Polynômes de Bernstein, isolation de racines (1h30)

4.1 Un théorème des valeurs intermédiaires constructif

4.2 Construction d'une formalisation de ce résultat

4.3 Comptage de racines, lemme de Descartes

*Esprit* : La formalisation des mathématiques s'attache à exprimer les énoncés et les preuves de théorèmes dans un langage qui ne laisse aucun détail implicite. La vérification de ces preuves peut ainsi être mécanisée, puisqu'elle obéit à un nombre fini de règles élémentaires. Les assistants à la preuve sont des logiciels qui permettent d'écrire et de vérifier ainsi formellement des résultats mathématiques. Ce cours s'attachera à expliquer l'intérêt croissant suscité par cette démarche de formalisation et à donner un aperçu de la pratique des assistants à la preuve. En particulier on utilisera le système Coq pour énoncer et démontrer certains résultats du cours de géométrie algébrique réelle de Marie-Françoise Roy.

– ***Cryptographie.***

Djiby Sow (Sénégal), cours de 8h 30.

*Plan*

1 Notions de cryptographie

2 Notion de systèmes cryptographiques symétriques

3 Notions de systèmes cryptographiques non-symétriques

4 Cryptographie à clef publique

Des TP seront proposés notamment: implémentation de l'algorithme à clef publique RSA