INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Projet Polka

Polynômes, Combinatoire, Arithmétique

Nancy

THÈME 2B

Table des matières

POLKA *est un projet du LORIA (UMR 7503), commun à l'INRIA, au CNRS, à l'Université Henri Poincaré Nancy 1, à l'Université Nancy 2 et à l'Institut National Polytechnique de Lorraine.*

1 Composition de l'équipe

Responsable scientifique

Paul Zimmermann [DR INRIA]

Responsable permanent

Jean-Luc Rémy [CR CNRS]

Assistantes de projet

Anne Loth [jusqu'au 03/09/99]
Geneviève Pierrelée [depuis le 06/10/99]

Personnel INRIA

Guillaume Hanrot [CR]
Grégory Kucherov [CR]
Fabrice Rouillier [CR]

Personnel CNRS

Gilles Schaeffer [CR, depuis le 01/09/99]

Personnel Université

Isabelle Debled-Rennesson [Maître de conférences IUFM de Lorraine]
Alain Giorgetti [PrAg UHP, jusqu'au 30/08/99]
Jocelyne Rouyer [Maître de conférences UHP]

Chercheur doctorant

Luc Rolland [bourse co-financée Région Lorraine, CMW et INRIA]

Stagiaires

Sylvie Boldo [ENS Lyon, du 01/06/99 au 09/07/99]
Mathieu Giraud [ENS Lyon, du 01/06/99 au 09/07/99]
Éric Queffelec [CNAM, du 10/06/99 au 01/09/99]
Isabelle Sivignon [ENS Lyon, du 07/06/99 au 09/07/99]

Chercheurs invités

Roman Kolpakov [professeur invité, du 01/08/99 au 31/10/99]
Vsévolod Makeev [chercheur invité, du 06/11/99 au 26/11/99]
Tony Scott [chaire industrielle co-financée Région Lorraine et SciFace, jusqu'au 30/08/99]

Collaborateurs extérieurs

Michel Barret [Supélec, campus de Metz]
Jean-Charles Faugère [LIP6, Paris]

2 Présentation et objectifs généraux

L'objectif général du projet POLKA est de développer des méthodes systématiques traitant certaines classes bien définies de problèmes algorithmiques, et d'implanter ces méthodes de façon efficace pour traiter des applications en grandeur nature. Parmi les nombreux domaines couverts, trois axes nous intéressent particulièrement.

Les nombres. C'est un axe de recherche récent au sein du projet, motivé par la participation à une action de recherche coopérative sur le calcul fiable. Les deux sous-axes visés sont d'une part la conception et le développement d'algorithmes pour la résolution d'équations diophantiennes, d'autre part les calculs par intervalles flottants et l'arithmétique en précision arbitraire.

Les polynômes. C'est un domaine dans lequel les membres du projet ont acquis une certaine expérience au cours des six dernières années, notamment grâce aux projets européens PoSSo et FRISCO. Cette compétence dans la résolution des systèmes polynomiaux a déjà porté ses fruits dans des domaines applicatifs réels comme les filtres de compression d'images ou la robotique, et nous envisageons de poursuivre dans cette seconde voie, notamment avec une thèse pluridisciplinaire automatique-informatique débutée en 1998. Parallèlement, des recherches théoriques à long terme sont entreprises en vue d'étendre les méthodes actuelles à des systèmes ayant un nombre infini de solutions.

Les structures combinatoires. C'est un axe de recherche relativement ancien au sein du projet, mais que nous désirons relancer, notamment en ce qui concerne les applications de la recherche combinatoire au génome, via une nouvelle action de recherche coopérative sur la recherche et l'extraction de motifs.

3 Fondements scientifiques

3.1 Les nombres

Les nombres (entiers ou flottants, en précision arbitraire) sont pour nous un moyen de montrer des résultats exacts dans le domaine du calcul symbolique. Sur les nombres entiers, nous

étudions essentiellement des équations diophantiennes algébriques. Comme c'est un domaine très difficile, notre démarche consiste à identifier des classes d'équations résolubles, puis à développer des algorithmes efficaces pour les résoudre. Ces algorithmes combinent l'utilisation de bornes supérieures sur la taille des solutions, et des recherches exhaustives. La difficulté principale – une fois la borne supérieure obtenue, ce qui peut nécessiter une étude théorique non négligeable – consiste à réduire la taille des solutions (en utilisant des arguments numériques), mais aussi à mener à bien beaucoup plus efficacement la recherche exhaustive finale.

En ce qui concerne les nombres flottants, notre objectif à long terme est de développer une bibliothèque portable et fiable de calcul sur de tels nombres en précision arbitraire. Par « fiable » nous entendons entre autres le calcul exact des arrondis dirigés (au plus proche, vers zéro, moins et plus l'infini) comme c'est le cas pour les `double` en C grâce à la norme IEEE-754. Il s'agit aussi de développer ou d'améliorer des algorithmes efficaces de calcul sur les nombres flottants. Ces algorithmes sont bien sûr basés sur les algorithmes calculant sur les entiers, mais des méthodes spécifiques peuvent être développées. Ainsi, pour calculer le produit de deux flottants de n chiffres, seuls les n premiers chiffres du produit entier de $2n$ chiffres sont nécessaires.

3.2 Les polynômes

> *There is also a "reflection" about the "meaning" of solving a system, taking place within some research groups more interested in effective methods for algebraic geometry. The philosophy essentially goes back to Kronecker: a system is solved if each root is represented in such a way as to allow the performance of any arithmetical operations over the arithmetical expressions of its coordinates (the operations include, in the real case, numerical interpolation).*
>
> *M. G. Marinari, H. M. Möller, T. Mora, Trans. of the AMS, vol. 348, n. 8, 1996*

L'étude des zéros réels des systèmes polynomiaux constitue un lien direct entre le calcul formel et les applications. Notre but est de fournir des outils performants en vue d'une utilisation industrielle. Ce travail comporte plusieurs aspects : (i) un aspect théorique en géométrie réelle pour l'élaboration d'algorithmes effectifs : méthodes de comptage avec ou sans contraintes, simplification des systèmes, isolation des racines, traitement des hypersurfaces ; (ii) un aspect algorithmique pour l'optimisation pratique des méthodes effectives : diminution du nombre d'opérations arithmétiques, contrôle de la taille des données en cours de calcul ; (iii) un aspect informatique pour l'implantation efficace de ces méthodes sur un grand nombre de plate-formes.

3.3 Les structures combinatoires

En termes généraux, nos études dans ce domaine portent sur les propriétés combinatoires et algorithmiques de structures discrètes, telles que mots, arbres, graphes, cartes, polyominos. Le but consiste en général à développer des algorithmes efficaces, qui sont cependant souvent basés sur des études théoriques profondes de propriétés combinatoires de ces structures.

Un premier volet de ces travaux concerne l'étude de *motifs* dans les mots et les arbres. Ici, notre spectre d'études est large – à partir d'études théoriques sur la décidabilité et la complexité de problèmes liés aux motifs, en passant par des recherches sur des problèmes « classiques » de la combinatoire du mot, jusqu'au développement et à l'implantation d'algorithmes efficaces de recherche de motifs dans les mots et leur application à l'analyse de séquences génomiques.

Une autre voie de recherche concerne la reconstruction d'ensembles discrets bidimensionnels à partir de leurs projections horizontale et verticale. Ces travaux font appel à des outils de géométrie discrète qui sont en lien étroit avec les propriétés combinatoires des mots, comme la reconnaissance de segments de droites discrètes.

Enfin les propriétés des structures discrètes aléatoires sont étudiées sous différents aspects. Les méthodes énumératives, qui font appel aux combinatoires aussi bien bijective, asymptotique qu'algébrique, servent à aborder théoriquement des questions de pertinence de motifs extraits, ou plus classiquement d'analyse d'algorithmes en moyenne. Le développement d'algorithmes de génération aléatoire permet de venir compléter les résultats théoriques par l'expérimentation.

4 Domaines d'applications

4.1 Robots parallèles

La recherche s'articule autour des diverses étapes de conception d'un mécanisme doté d'une unité de commande. Concrètement, les travaux s'appliquent autant aux domaines de la robotique, de la machine-outil et des suspensions actives, *i.e.* partout où il faut asservir des mécanismes complexes en position, en vitesse ou en accélération. Deux familles de problèmes surgissent : la conception du mécanisme pur et la réalisation des algorithmes de commande.

On définit comme mécanisme complexe une structure mécanique à plusieurs chaînes cinématiques. Chaque chaîne est un ensemble de corps rigides assemblés par des joints mobiles permettant des mouvements linéaires ou rotatifs à un, deux ou trois degrés de liberté.

Les chaînes que nous étudions sont des robots parallèles : elles sont constituées d'une base (corps rigide fixe comprenant six joints) et d'une nacelle (corps rigide mobile contenant six joints).

Les objectifs visés sont :

- la modélisation de mécanismes : la modélisation et la résolution de modèles de mécanismes sont abordés du point de vue de la géométrie afin de produire des équations régissant ces systèmes. S'appuyant sur les méthodes de transformation des systèmes d'équations géométriques en systèmes polynomiaux développées par J.-C. Faugère et F. Rouillier, une solution effective aux divers problèmes de modélisation géométriques (directs, inverses et différentiels) peut être déterminée ;
- la simulation cinématique : les techniques de résolution de problèmes plus complexes issus du calibrage en étudiant les propagations d'erreurs et l'analyse de trajectoires sont abordées dans le domaine plus général de la cinématique ;
- la mise au point d'unités de commande : tout mécanisme commandé nécessite l'élaboration de modèles géométriques qui permettent de représenter de façon adéquate un modèle physique dynamique qui fonctionne en temps réel. L'élaboration de simulateurs de robots

parallèles est favorisée afin d'identifier et de comparer diverses stratégies de commande. Ce travail permettra l'optimisation des paramètres de réglage.

Modèles géométriques. La conception de robots parallèles ou machines-outils nécessite des travaux tels que : l'étude des postures, les modes d'assemblage, le calibrage, la propagation d'erreurs. Ces activités nécessitent l'établissement de modèles géométriques directs (MGD) et inverses (MGI).

À l'aide du calcul formel, il est possible de résoudre le MGI de manière explicite en calculant la norme entre les points d'attache des chaînes cinématiques à la base et à la nacelle. Le système d'équations du MGI exprime les variables articulaires en fonction des coordonnées généralisées de l'extrémité incluant la position et l'orientation. Le MGI conduit à un système de trois à neuf équations quadratiques à plusieurs variables.

La construction du modèle géométrique direct n'est possible qu'avec le système d'équations du MGI. Il n'y a que rarement une formulation explicite dans des cas simplifiés (le robot Delta). De toutes les méthodes proposées dans la littérature, il n'y en a qu'une qui assure la convergence et qui donne tous les résultats. Il s'agit de transformer le système du MGI en un autre système polynomial à l'aide des bases de Gröbner tel que proposé par J.-C. Faugère avec le logiciel GB. La suite de la méthode consiste à appliquer la représentation univariée telle que réalisée par le logiciel RealSolving de F. Rouillier qui fournit une équation polynomiale univariée — de degré 40 ici — et un ensemble de fonctions qui calculent les variables de départ en fonction des solutions de ladite équation polynomiale univariée. L'isolation des racines réelles s'effectue aussi avec le logiciel RealSolving. La résolution du MGD donne tous les résultats des coordonnées généralisées de l'extrémité en fonction des variables articulaires.

À partir du MGI, il est possible de calculer symboliquement le modèle géométrique différentiel inverse (MDI) qui s'obtient en calculant la matrice jacobienne. Le calcul formel permet de résoudre la matrice jacobienne dite inverse car elle est relative au MDI. Le MDI donne un système d'équations qui permet de calculer : (i) les résolutions de l'extrémité en fonction des résolutions des variables articulaires ; (ii) les forces des actionneurs en fonction d'une force appliquée sur l'extrémité. Le concepteur peut donc dimensionner les couples moteurs en appliquant les forces maximales.

Le calcul du déterminant de la jacobienne inverse donne une équation polynomiale dont les zéros donnent les hypersurfaces du premier type de singularités. Il est aussi possible de calculer le déterminant de la jacobienne (modèle différentiel direct ou MDD) en inversant le déterminant de la jacobienne inverse. L'évaluation des zéros de cette équation polynomiale localise le second type de singularités.

Modèles cinématiques. La notion de MDI permet d'aborder des problèmes de déplacements infinitésimaux qui peuvent être transposés à des études de vitesses instantanées. On peut donc calculer le vecteur de vitesse de l'extrémité en fonction des vitesses des actionneurs.

La modélisation de trajectoires fait intervenir divers scenarii avec l'usage des MGD, MGI et MDI. Cela correspond à construire des algorithmes qui paramètrent les trajectoires (segments de droite, arcs de cercles et *splines*) en équations. Il est possible d'appliquer et d'étudier diverses stratégies : un réglage de position, de vitesse, une combinaison des deux ou toute autre approche jugée pertinente.

Évaluation et optimisation de commandes. La simulation d'un robot parallèle fait intervenir des modèles exacts provenant du MGD étudié avec les outils cités précédemment. Le simulateur interagit avec un simulateur d'unité de commande qui nécessite l'usage d'un système numérique tel que SCILAB. Les approches de commande classiques sont déjà à l'étude : réglage d'axe par rétro-action avec paramètre proportionnel, intégral et dérivatif (PID), suivi *a priori* en position, suivi en vitesse, soit au niveau des actionneurs découplés, soit au niveau de l'organe terminal.

Divers outils sont développés au sein de POLKA et au sein du projet SAGA (INRIA Sophia-Antipolis) qui serviront à l'élaboration du simulateur. J.-P. Merlet a déjà produit des outils numériques d'analyse et de visualisation de robots parallèles de type Hexapode.

4.2 Analyse de génomes

L'analyse de génomes reste un domaine d'application privilégié pour nos travaux sur l'algorithmique combinatoire. POLKA est projet-coordinateur de l'action coopérative de recherche REMAG dont le thème est la recherche et l'extraction de motifs dans les séquences génomiques (cf. aussi les sections 6.3 et 8.1). L'année écoulée a vu une montée considérable d'activité dans la bioinformatique, à la fois au niveau national et régional, qui s'est concrétisée, entre autres, par la création du Génopôle à la fin 1998, suivie par la création de Génopôles régionaux et le lancement de plusieurs programmes. Pour notre part, nous faisons partie du Génopôle Alsace-Lorraine, dans le cadre duquel nous développons un partenariat avec des biologistes de l'Institut de Génétique et de Biologie Moléculaire et Cellulaire (IGBMC) à Strasbourg ainsi qu'avec le Laboratoire d'Enzymologie et de Génie Génétique à l'Université Henri Poincaré de Nancy. Plusieurs réunions de travail ont eu lieu durant l'année 1999 durant lesquelles les participants ont fait des exposés scientifiques sur leur travail. Le but de ces réunions était de dégager des problèmes qui pourraient donner lieu à des collaborations, de faire l'« état des lieux » des méthodes existantes et de repartir les tâches.

Par ailleurs, le contrat de plan État-Région Lorraine prévoit également la mise en place d'un ensemble de travaux sur la bioinformatique. Dans ce cadre, une collaboration débute entre plusieurs groupes de biologistes de Nancy et le LORIA, collaboration à laquelle nous participons.

4.3 Tomographie discrète

L'un des problèmes de la tomographie discrète consiste à reconstruire un ensemble fini de points à partir de rayons X, un rayon X fournissant le nombre de points présents sur un axe donné. Tous les rayons parallèles à un nombre fini de directions sont considérés.
Les applications de la tomographie discrète sont nombreuses en particulier en compression de données, en traitement d'images ou encore en imagerie médicale pour l'aide aux diagnostics médicaux en radiographie. De nouvelles motivations sont apparues plus récemment dans le domaine de l'étude des matériaux. Les techniques développées sont utilisées pour reconstruire des structures cristallines à partir de données obtenues par microscopie électronique. Ceci permet de mettre en relief des propriétés des cristaux au niveau atomique. Des collaborations dans ces directions sont à envisager.

5 Logiciels

5.1 UDX

UDX (Universal Data eXchange) est un nouveau protocole de communication binaire implanté par F. Rouillier et B. Wallrich[1] dont le procédé de base a été breveté en juillet 1999 (Dispositif d'échanges de données entre matériels informatiques, numéro de dépôt 99 08172, auteursJ.-C. Faugère - UPMC[2], F. Rouillier - INRIA).

Les solutions logicielles FGB et RS (voir module REALSOLVING) sont conçues pour permettre une distribution des calculs sur un réseau de machines hétérogènes. Afin de permettre l'échange efficace d'un large volume d'informations, l'échange des données doit se faire en mode binaire.

Le problème habituel à résoudre pour mettre au point ou utiliser un protocole de communication binaire est de déterminer les permutations d'octets nécessaires pour transformer le codage des données scalaires (entiers, flottants) au format d'un processeur donné en un autre format. Par exemple, les octets du codage d'un entier 32 bits sur processeur SPARC sont ordonnés à l'inverse de ceux du codage interne sur processeur PENTIUM.

Sur ces problèmes *usuels* viennent se greffer des problèmes spécifiques dus aux objets manipulés en calcul formel, tels que le codage des entiers multi-précision.

Tous ces paramètres rendent quasi impossible la maintenance d'un code efficace transmettant en mode binaire des entiers multi-précision avec les outils usuels (XDR, PVM, MPI, etc).

UDX est un nouveau protocole de communication binaire qui *détecte* automatiquement et dynamiquement le codage interne des données scalaires (entiers, flottants machine) et des entiers multi-précision sans contenir une seule ligne de code dépendant de l'architecture considérée (et ne faisant évidement appel à aucune implantation dépendant de l'architecture telle que XDR par exemple). Ceci facilite sa maintenance ainsi que celle des programmes l'utilisant.

À noter qu'aucun format d'échange n'est fixé *a priori* dans UDX : le protocole le déterminera également dynamiquement. En particulier, à la différence des protocoles usuels, aucune manipulation et aucune connaissance n'est nécessaire à l'utilisateur pour optimiser la communication. Par exemple, sauf intervention de l'utilisateur, les protocoles usuels utilisent le codage interne des processeurs SPARC comme format d'échange, ce qui ralentit fortement la communication entre deux machines identiques mais dont le codage interne est différent du codage SPARC, compte-tenu des permutations d'octets effectuées. Dans ce genre de situation, UDX détecte automatiquement et dynamiquement la compatibilité des processeurs et n'effectue aucune permutation lors des échanges.

5.2 RealSolving et RS

La majeure partie des algorithmes développés dans POLKA et concernant les systèmes polynomiaux sont intégrés dans le logiciel RS (Real Solutions), dont la version 1.0 a été déposée en juillet 1998 à l'APP (numéro 1998.000.20000).

1. ingénieur de recherche au LORIA
2. Université Pierre et Marie-Curie.

RS est le successeur de RealSolving, logiciel implanté lors du projet PoSSo, maintenu pendant le projet FRISCO mais dont le développement sera arrêté en 2000.

Un travail d'optimisation a été réalisé en 1999 sur l'ensemble des algorithmes implantés dans RS. La gestion de mémoire a été consolidée et des efforts particuliers ont été fournis pour la partie arithmétique (interface avec la bibliothèque MPFR, optimisation de l'arithmétique modulaire, utilisation de la bibliothèque GMP dans sa version de développement).

Les principales nouveautés sont liées aux interfaces. Nous avons mis au point un protocole ASCII commun aux logiciels FGb développé par J.-C. Faugère et RS, mais l'essentiel du travail a été le développement de l'interface *socket-stream* (binaire) qui est à l'origine du protocole UDX. Les logiciels RS et FGb disposent désormais d'interfaces homogènes, solides et performantes permettant d'une part l'exploitation intensive de la distribution des calculs sur un réseau de machines hétérogènes et d'autre part une utilisation transparente à partir de logiciels généralistes tels MuPAD.

Un travail conséquent à par ailleurs été réalisé en collaboration avec le groupe MuPAD pour l'implantation d'un programme de démonstration utilisant l'ensemble de logiciels MuPAD, RS, FGb, connectés grâce au protocole UDX, pour la résolution de quelques problèmes simples en robotique.

5.3 MuPAD-Scilab

Le but de cette action, qui a fait l'objet d'un contrat de recherche avec la société SciFace distribuant MuPAD (Paderborn, Allemagne), est d'établir une interface entre le système de calcul formel MuPAD et le système de calcul numérique Scilab développé en commun par le projet Méta2 de l'INRIA Rocquencourt et l'ENPC (École Nationale des Ponts et Chaussées). À ce projet participent Éric Fleury (projet Résédas), Fabrice Rouillier, Tony Scott et les développeurs de MuPAD à l'Université de Paderborn, la connexion industrielle pour ces derniers étant représentée par la société SciFace. Nous avons accompli les travaux suivants :

1. Une interface MuPAD-Scilab basée sur PVM (*parallel virtual machine*) a été réalisée et fournie à la société SciFace. Cette passerelle permet d'accéder depuis MuPAD à la plupart des fonctionnalités de Scilab, notamment les routines très efficaces d'algèbre linéaire en double précision. La sortie écran suivante compare les capacités de Scilab et de MuPAD ; on compare d'abord les deux sur le calcul d'un déterminant 3×3, puis sur la résolution d'un système linéaire aléatoire de dimension 50 : sur cet exemple Scilab est presque 250 fois plus rapide que les routines `linalg` standard de MuPAD :

```
>> A:=scilab::rand(3,3);
Starting Scilab. This may need some time... Done
           +-                                                -+
           |  2.113248654e-1, 3.303270917e-1, 8.497452358e-1  |
           |                                                  |
           |  7.560438541e-1, 6.653811042e-1, 6.857310198e-1  |
           |                                                  |
           |  2.211346291e-4, 6.283917883e-1, 8.782164813e-1  |
           +-                                                -+
```

```
>> linalg::det(A), scilab::det(A);

                        2.16730554e-1, 2.16730554e-1

>> n:=50: A:=scilab::rand(n, n): b:=scilab::rand(n, 1):
>> time(scilab::linsolve(A, b)), time(linalg::linearSolve(A, b));

                                20, 4850
```

2. Un prototype utilisant le protocole UDX de J.-C. Faugère et F. Rouillier à la place de PVM a été réalisé en octobre 1999. Ce prototype utilise l'implantation d'UDX réalisée par Bertrand Wallrich.

Un contrat a été établi entre SciFace, POLKA et le groupe SCILAB pour la commercialisation de cette interface.

5.4 mpfr

Une première version de la bibliothèque MPFR de calcul flottant en précision arbitraire avec arrondi exact a été réalisée, et est disponible sur le web[3]. Cette version implante les quatre opérations de base ($+$, $-$, $\times$,/), la racine carrée, l'exponentielle, le logarithme et la moyenne arithmético-géométrique. Ces deux dernières opérations ont été implantées par Sylvie Boldo, dans le cadre de son stage de première année à l'ENS Lyon, en suivant les conseils éclairés de Jean-Michel Muller[Mul97] (projet ARÉNAIRE). Cette première version a déjà permis de détecter sur certains couples processeur/système des écarts par rapport à l'arrondi exact allant d'un *ulp* à plusieurs centaines d'*ulps* (*units in last place*). Par exemple pour le calcul de $\log(2454102056365837 \cdot 2^{-51})$ avec l'arrondi vers zéro, Sun/Solaris donne la valeur $6199195486339951 \cdot 2^{-56}$ alors que le résultat exact est $6199195486339950 \cdot 2^{-56}$:

```
mpfr_log differs from libm.a for a=1.089840243102918382 33e+00, rnd=1
 double calculus gives 8.603111953858698368 60e-02
 mpfr_log        gives 8.603111953858696980 82e-02 (1 ulp)
```

Pire encore, pour $\exp(-8388240597389047 \cdot 2^{-44})$, toujours avec l'arrondi vers zéro, un PC sous Linux donne $4825254294033856 \cdot 2^{-740}$ alors que le résultat exact est $4825254294033475 \cdot 2^{-740}$, soit un écart de 381 *ulps* :

```
mpfr_exp differs from libm.a for x=-4.768162737826200441 30e+02, rnd=1
libm.a gave  8.343022494607129343 33e-208,
mpfr_exp got 8.343022494606470581 87e-208
```

En parallèle a débuté un effort global pour améliorer les algorithmes de base utilisés par `mpfr`, en se ramenant à des multiplications : naïves en $O(n^2)$, à la Karatsuba en $O(n^{1.59})$, ou avec FFT en $O(n \log n \log\log n)$. Un premier résultat a été obtenu pour la racine carrée : nous avons montré en effet qu'il est possible de calculer la racine carrée, avec reste, d'un entier de $2n$ bits en $\sim \frac{3}{2}K(n)$ opérations, où $K(n)$ est le coût de la multiplication de deux entiers de n bits

3. `http://www.loria.fr/~zimmerma/fiable/mpfr-0.0.tar.gz`

[Mul97] J.-M. MULLER, *Elementary Functions. Algorithms and Implementation*, Birkhauser, 1997, 232 pages.

par l'algorithme de Karatsuba. Si le reste n'est pas nécessaire, ce qui est le cas dans MFPR, où seuls les premiers bits du reste suffisent à calculer l'arrondi exact, nous avons aussi établi que $\sim K(n)$ opérations suffisent [23].

Ces recherches poursuivent l'effort entrepris dans le cadre de l'action de recherche coopérative « Outils pour un calcul numérique fiable » (1997-1999), et s'inscrivent dans l'axe « Qualité et sûreté du logiciel » du nouveau contrat de plan État-Région, plus précisément dans l'action « plate-forme logicielle » coordonnée par M. Rusinowitch (projet PROTHÉO).

5.5 grappe

`grappe` est un logiciel qui recherche simultanément plusieurs motifs dont chacun est composé d'une suite de fragments (mots) séparés par des espaces de longueur *a priori* non bornée (cf. section 6.3). Par comparaison avec les logiciels de cette famille, tels que `egrep` ou `agrep`, `grappe` permet de rechercher rapidement un grand nombre de ces motifs dans de longs textes. Cette année, ce logiciel a été étendu afin de permettre de spécifier des espaces de longueur bornée par un intervalle. Une description plus détaillée, ainsi que des références, sont données dans la section 6.3.

6 Résultats nouveaux

6.1 Algèbre commutative et résolution de systèmes polynomiaux

Participants : Luc Rolland, Fabrice Rouillier, Paul Zimmermann.

Variétés définies par une unique équation polynomiale. Depuis quelques années, F. Rouillier s'est attaché à l'étude des variétés définies par une unique équation polynomiale (en plusieurs variables). L'idée est de se ramener autant que faire se peut à l'étude de systèmes zéro-dimensionnels. Une collaboration avec M.-F. Coste-Roy (Université de Rennes 1) et Mohab Safey (Laboratoire d'Informatique de Paris 6) a permis d'élaborer un nouvel algorithme utilisant les propriétés de la fonction distance d'un point à une variété définie par une équation polynomiale ([RRS00]).

Le principe de base est simple. Supposons que l'on se donne une variété définie par un unique polynôme $P \in K[X_1,\ldots,X_k]$ où K est un corps de caractéristique nulle, de clôture réelle R et de clôture algébrique C. Si la variété (de C^n) $P = 0$ est lisse, en choisissant un point $O \in R^n$ suffisamment générique, l'ensemble des points M de C^n vérifiant $P = 0$ et $OM//\mathrm{grad}(P)(M)$ est fini et définit au moins un point dans chaque composante connexe (réelle) de $P = 0$. L'essentiel du travail a été de contourner les hypothèses faites sur la variété de départ (variété lisse, point O suffisamment générique) en gardant à l'esprit le côté *implantation efficace* de l'algorithme. La méthode finale a en particulier permis de découvrir de nouvelles propriétés non triviales de la Représentation Univariée Rationnelle dans le cas de certains systèmes d'équations à coefficients dans le corps des séries de Puiseux comme la caractérisation

[RRS00] F. ROUILLIER, M.-F. ROY, M. SAFEY, « Finding at least one point in each connected component of a real algebraic set defined by a single equation », *Journal of Complexity*, 2000.

des points bornés sur R d'une variété algébrique de $(R\langle\epsilon\rangle)^k$. Elle fait appel, entre autres, à l'ensemble des outils développés depuis le début de la thèse de F. Rouillier[Rou96].

Les résultats mis au point se démarquent à la fois des méthodes utilisées jusqu'alors en pratique (décomposition cylindrique), en évitant le traitement récursif du problème (réduisant ainsi la taille de la sortie des algorithmes), et des résultats développés pour les études de complexité théorique, par l'utilisation d'arithmétiques beaucoup plus simples (nombre d'infinitésimaux nécessaires).

Zéros réels de variétés de dimension positive. Nous travaillons en collaboration avec M. Safey (LIP6) depuis 1999 sur une nouvelle génération d'algorithmes permettant de traiter le cas général des systèmes de dimension positive (donner au moins un point par composante connexe). Le but est de se passer définitivement de l'utilisation de déformations infinitésimales pour des raisons d'efficacité évidentes. L'idée de base est très simple : l'utilisation de déformations infinitésimales n'est nécessaire que pour étudier des cas particuliers où la caractérisation algébrique des points critiques de la fonction *distance à un point* n'est pas possible ou n'a pas de sens. Ceci se produit, par exemple, dès lors que les variétés étudiées admettent une infinité de points singuliers.

Nous avons montré deux choses :

- les sous-variétés de la variété initiale dont l'étude nécessite une déformation infinitésimale du système initial sont modélisables comme étant des variétés de dimension strictement inférieure à la dimension de la variété initiale,
- on peut étudier les composantes de la variété initiale ne nécessitant pas de déformation séparément.

Ceci induit une méthode par induction sur la dimension des variétés étudiées. Une partie de ce travail sera soumis pour publication en 2000.

En appliquant cette stratégie au cas particulier de variétés définies par une unique équation, nous avons d'ores et déja amélioré sensiblement ce qui avait été fait. Les premiers résultats expérimentaux montrent que nous dépasserons de très loin les méthodes existantes en terme de temps de calcul mais également en terme de qualité des résultats produits.

Le travail restant à faire est maintenant de nature algorithmique. Nous avons identifié clairement les étapes de calcul qui posent problème d'un point de vue pratique. Les améliorations en vue nécessitent un travail concerté avec les chercheurs de l'équipe CALFOR (LIP6) en vue d'améliorer ou d'adapter deux familles d'algorithmes (décomposition primaire - J.C. Faugère - et ensembles triangulaires - P. Aubry et D. Lazard) pour une utilisation efficace.

Méthode d'Uspensky**.** Le résultat le plus remarqué de ces deux dernières années est un travail effectué par F. Rouillier et P. Zimmermann sur l'algorithme d'Uspensky pour l'isolation des zéros réels d'un polynôme en une variable (en cours de rédaction).

L'essentiel du travail fourni cette année a été de proposer un algorithme optimal (pour la méthode d'Uspensky) tant en terme d'occupation mémoire qu'en terme de temps de calcul (en supposant fixées les opérations de base).

[Rou96] F. Rouillier, *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*, Thèse de doctorat, Université de Rennes I, mai 1996.

Ce résultat devrait être soumis pour publication en 2000.

Modèles géométriques pour les robots parallèles. Il est possible de résoudre de manière exacte les MDI (cf section 4.1) de la plupart des robots parallèles. Des instances des modèles géométriques directs de divers robots parallèles ont été calculées et résolues avec des temps de réponse satisfaisants ; les robots étudiés incluent la plupart des robots parallèles proposés par J.-P. Merlet dont le Delta, Tricept, Hexa, Kanuk, Manta, robot plan, Œil-Agile et plusieurs hexapodes. Le problème le plus complexe a été résolu en six minutes et les autres prennent environ 30 secondes sur une machine peu performante (station Sparc 5 sous Solaris).

Il est possible de déterminer symboliquement et rapidement le MDI à partir du MGI pour la plupart des robots parallèles. Cela donne la jacobienne inverse, matrice 6×6 ou 9×9 selon la modélisation utilisée au niveau du MGI. Les termes de la matrice sont linéaires. Les temps de calcul sont de l'ordre de la minute.

À partir de la jacobienne inverse, il est possible d'obtenir symboliquement le déterminant sous forme d'un polynôme en 6 ou 9 variables. Son analyse consiste à étudier un problème avec une infinité de solutions. F. Rouillier cherche à trouver les solutions de ces problèmes qui ne sont pas zéro-dimensionnels.

Partant de ce déterminant, une inversion donne le déterminant symbolique de la jacobienne provenant du MDD. L. Rolland s'efforce de trouver une forme symbolique du MDD, car les paramètres ont tendance à exploser lors de l'inversion de matrice.

L. Rolland et F. Rouillier proposent des solutions exactes aux problèmes d'études de postures, aux analyses de modes d'assemblage et aux problèmes issus d'études de propagation des erreurs liées au calibrage. Ils proposent aussi des solutions exactes aux calculs de résolutions de l'organe terminal en fonction des résolutions des jambes de robots, menant au choix des capteurs, ainsi que pour l'aide au dimensionnement des actionneurs par le calcul des couples maximaux en fonction des forces appliquées à l'organe terminal.

Modèles cinématiques pour les robots parallèles. La résolution des MDI permet de proposer des solutions exactes aux calculs des vitesses de l'organe terminal en fonction des vitesses des actionneurs.

La modélisation de trajectoires fait intervenir divers scenarii qui sont actuellement à l'étude par J.-P. Merlet,L. Rolland et F. Rouillier. Paramétrer la trajectoire nominale théorique permet sa caractérisation. La modélisation des déplacements des actionneurs a été réalisée avec plusieurs approches, dont une équation à vitesse constante et une à deux équations (linéaire et quadratique). L'application de MGD et MGI avec le calcul formel et les outils tels que Gb et RealSolving a permis d'établir le trajet théorique que va accomplir le robot parallèle selon le type de commande appliquée : en position, en vitesse ou en combinaison des deux.

Stabilité des systèmes linéaires. M. Benidir (Professeur à l'université de Paris-Sud) et M. Barret ont écrit un livre de 256 pages : *Stabilité des filtres et des systèmes linéaires* [BB99]. Les critères et algorithmes de tests de stabilité, que ce soit pour des filtres ou des systèmes linéaires, ont fait l'objet de nombreux travaux et publications depuis plus d'un siècle et demi. L'existence

[BB99] M. Benidir, M. Barret, *Stabilité des filtres et des systèmes linéaires*, Dunod, Paris, 1999.

d'un grand nombre d'articles scientifiques et l'absence de synthèse offrant une méthodologie aux ingénieurs sont les principales motivations de la rédaction du livre. L'objectif est de présenter une synthèse aussi complète que possible de travaux anciens et récents sur la stabilité des filtres dynamiques et des systèmes linéaires mono- et multidimensionnels. Comme la majorité des tests de stabilité sont fondés sur l'étude mathématique de la localisation des zéros d'un polynôme dans le plan complexe, une grande partie de l'ouvrage est consacrée à cette étude. Le chapitre 1 donne des éléments de la théorie des signaux et des systèmes utiles à l'introduction des notions de stabilités associées aux filtres et systèmes dynamiques, dans les cas analogique et discret. Le chapitre 2 est une synthèse des outils mathématiques qui sont à la base de l'étude de la localisation des zéros d'un polynôme dans le plan complexe. La présentation de ce chapitre suit l'évolution des connaissances sur le sujet en étudiant en détail les contributions de Cauchy, Sturm, Hermite, Routh, Hurwitz, Liénard, Chipart, Cohn et Fujiwara, puis les travaux postérieurs. Le lien étroit entre résultant, forme quadratique hermitienne et localisation des zéros d'un polynôme est mis en évidence. Le chapitre 3 expose de façon unifiée de nombreux critères avec les algorithmes associés pour tester la stabilité de filtres monodimensionnels, dans les cas analogique et discret. Des indications sont données pour choisir un algorithme parmi tous ceux proposés en fonction des objectifs visés. Le chapitre 4 regroupe des propriétés géométriques du domaine de stabilité des filtres numériques monodimensionnels, dans trois espaces différents. Il commence par la description de ce domaine dans l'espace des coefficients de réflexion, puis dans celui des polynômes unitaires et enfin dans celui des polynômes dont le degré est majoré par un entier naturel fixé. Au chapitre 5, après l'introduction de la notion de stabilité associée à des filtres et systèmes multidimensionnels, les principaux critères de stabilité de filtres numériques récursifs multidimensionnels sont déduits des propriétés géométriques établies au chapitre précédent. Deux algorithmes testant en un nombre fini d'opérations arithmétiques la stabilité de filtres récursifs bidimensionnels réels sont détaillés. Leur comportement face aux erreurs d'arrondi, quand ils sont implantés avec une arithmétique à virgule flottante, est étudié.

6.2 Théorie des nombres

Participants : Guillaume Hanrot, Jean-Luc Rémy.

Autour de la suite auto-décrite de Golomb. L'étude de cette suite, menée dans le projet depuis plusieurs années, s'est poursuivie dans deux directions différentes.

D'une part, Y.-F.S. Pétermann, J.-L. Rémy et I. Vardi ont étudié les solutions croissantes de l'équation différentielle-fonctionnelle $f'(t) = 1/f(f(t))$, qui possède des liens étroits avec la suite de Golomb [8]. Ils montrent qu'une telle solution admet nécessairement un point fixe positif ou nul, et que pour chaque nombre $p \geq 0$ il y a exactement une solution croissante ayant p pour point fixe. Ils montrent également qu'en général une condition initiale ne détermine pas une solution unique : les courbes représentatives de deux solutions croissantes distinctes se croisent en effet une infinité de fois. En fait, ils conjecturent que la différence de deux solutions croissantes se comporte de façon très similaire au terme d'erreur $E(n)$ dans l'expression asymptotique de la suite de Golomb, $F(n) = \phi^{2-\phi} n^{\phi-1} + E(n)$ (où ϕ est le nombre d'or).

D'autre part, J.-L. Rémy a encadré pendant 3 mois deux élèves de seconde année de l'ESIAL, école d'ingénieurs en informatique, dans le cadre de leur projet d'initiation à la recherche. Ceux-ci ont développé des programmes permettant de se faire une idée du comportement asymptotique de généralisées de la suite de Golomb.

Équations diophantiennes. Les travaux accomplis dans cette direction sont dans le prolongement des idées développées par G. Hanrot dans sa thèse[Han97] et ses travaux antérieurs. En particulier, ce dernier a achevé la rédaction d'un article commun avec Yuri Bilu et Paul Voutier [16], qui met un point final à une conjecture célèbre datant du siècle dernier portant sur les diviseurs de nombres de la forme $\alpha^n - \beta^n$; ce résultat repose sur l'utilisation d'idées techniques nouvelles pour mener à bien les calculs intensifs nécessaires. On peut en particulier signaler le travail [5] récemment paru à *Acta Arithmetica*.

Des travaux communs à Yann Bugeaud (Université de Strasbourg) et G. Hanrot tirent profit d'un aspect initialement marginal d'un article écrit en commun avec Yuri Bilu, qui dans certaines circonstances permet d'obtenir des résultats frappants de façon « élémentaire ».

Cette méthode permet, en particulier, d'améliorer les résultats connus sur l'équation de Catalan $x^p - y^q = 1$, ce qui a donné lieu à la rédaction d'un travail [18] soumis pour publication.

Combinée à de nombreux raffinements techniques ainsi qu'à des idées antérieures [4] plus profondes, et en collaboration avec Maurice Mignotte (Strasbourg), cette nouvelle méthode a également permis de faire d'importants progrès sur l'équation de Nagell-Ljunggren $(x^n - 1)/(x - 1) = y^q$, qui est étroitement liée à l'équation de Catalan. Nous avons en particulier montré[17] que pour toute solution autre que celles déjà connues (x,y,n,q), l'entier n n'est divisible ni par 5, ni par 7. Il convient d'insister sur le fait que très rares sont les exemples de résolution complète d'équations diophantiennes exponentielles $f(x) = y^q$ en inconnues x, y, $q \geq 2$, où f est un polynôme à coefficients entiers de degré ≥ 3.

Par ailleurs, un travail de G. Hanrot, en collaboration avec N. Saradha et T. Shorey, du Tata Institute à Bombay et utilisant lourdement les techniques de résolution effective d'équations diophantiennes a permis de progresser dans l'étude d'une conjecture d'Erdős et Selfridge, qui cherche à déterminer quand un produit d'entiers consécutifs, duquel on peut omettre au plus un terme, est presque une puissance pure. La rédaction de ce travail est en cours d'achèvement.

Un travail effectué il y a deux ans en collaboration avec François Bertault et Olivier Ramaré sur les sommes de sept cubes a été publié dans la revue *Mathematics of Computation* [3].

Factorisation de RSA-140 et RSA-155. Au sein d'un groupe de chercheurs de plusieurs pays, coordonné par Herman te Riele du CWI (Amsterdam), le projet Polka a participé à la factorisation de RSA-140 en février 1999 [12] et de RSA-155 en août 1999 [24].

6.3 Algorithmique combinatoire

Participants : Isabelle Debled-Rennesson, Mathieu Giraud, Roman Kolpakov, Grégory Kucherov, Vsévolod Makeev, Éric Queffelec, Jean-Luc Rémy, Jocelyne Rouyer, Gilles

[Han97] G. Hanrot, *Résolution effective d'équations diophantiennes : algorithmes et applications*, Thèse de doctorat, Université de Bordeaux I, avril 1997.

Schaeffer, Isabelle Sivignon, Paul Zimmermann.

Combinatoire du mot. Un article résumant les travaux antérieurs sur la proportion minimale limite d'une lettre dans les mots binaires sans puissance n, est paru cette année dans la revue *Theoretical Computer Science* [7]. Notons que ces travaux sont un fruit de notre collaboration avec des chercheurs de l'Université de Moscou dans le cadre d'un projet de l'Institut franco-russe A. M. Liapounov d'informatique et de mathématiques appliquées (cf section 8.2.2).

Les travaux sur les répétitions dans les mots, menés en collaboration avec Roman Kolpakov de l'Université de Moscou, ont vu un progrès considérable depuis leur début mi-1998. Ces études portent sur les répétitions dites *maximales* dans un mot, *i.e.* des facteurs répétitifs (formellement, d'un exposant deux ou plus) ne pouvant pas être étendus à droite ni à gauche en préservant leur période minimale. Le premier résultat combinatoire que nous avons prouvé[KK98] affirme que le nombre de répétitions maximales dans un mot est borné linéairement en la longueur du mot. Pour arriver à ce résultat, nous avons d'abord analysé les mots de Fibonacci, qui fournissent souvent un bon exemple pour tester des conjectures sur les propriétés combinatoires des mots. Comme résultat annexe, nous avons obtenu une formule exacte pour le nombre de répétitions maximales dans les mots de Fibonacci.

Ces résultats nous ont conduit à la conjecture d'une propriété encore plus forte des répétitions maximales, à savoir que non seulement le nombre de répétitions maximales est linéaire, mais la somme de leurs exposants est linéaire elle aussi. Nous avons réussi à généraliser la preuve du résultat précédent pour confirmer cette conjecture [21]. Comme dans le cas du nombre de répétitions, nous avons analysé les mots de Fibonacci et obtenu, pour ces mots, une estimation très précise de la somme des exposants.

Ces résultats sont intéressants sous plusieurs aspects. Du point de vue combinatoire, ils montrent que les répétitions maximales sont en effet une représentation compacte de toute la structure répétitive du mot. Cela améliore plusieurs résultats connus et répond à quelques questions ouvertes dans le domaine. Par exemple, le résultat généralisé prouve la conjecture émise par Stoye et Gusfield[SG98] que le nombre de *branching tandem repeats* est linéairement borné.

L'ensemble de ces travaux (voir aussi la section suivante) a donné lieu à deux publications dans des conférences internationales de haut niveau : *12-th International Symposium on Fundamentals of Computation Theory (FCT'99)* [14] et *1999 Symposium on Foundations of Computer Science (FOCS'99)* [2].

Recherche de répétitions. Les résultats combinatoires décrits ci-dessus ont une conséquence algorithmique très intéressante : ils permettent d'obtenir un algorithme qui recherche toutes les répétitions maximales dans un mot en temps linéaire par rapport à la longueur

[KK98] R. Kolpakov, G. Kucherov, « Maximal Repetitions in Words or How to Find all Squares in Linear Time », *Rapport de recherche*, 1998, `http://www.loria.fr/publications/1998/98-R-227/98-R-227.ps`.

[SG98] J. Stoye, D. Gusfield, « Simple and Flexible Detection of Contiguous Repeats Using a Suffix Tree », *in : Proceedings of the 9th Annual Symposium on Combinatorial Pattern Matching*, M. Farach-Colton (éditeur), *Lecture Notes in Computer Science*, 1448, Springer Verlag, p. 140–152, 1998.

du mot. Cet algorithme est basé sur l'algorithme de Main[Mai89] qui permet de trouver, en temps linéaire, toutes les occurrences les plus à gauche des répétitions maximales d'un mot. Le fait que le nombre total de répétitions maximales reste linéaire permet de démontrer qu'elles peuvent toutes être trouvées en temps linéaire par une extension de l'algorithme de Main.

Puisque l'ensemble des répétitions maximales est une représentation de toutes les répétitions dans le mot, cet algorithme, qui représente en soi une avancée importante, permet de résoudre efficacement d'autres problèmes liés. Par exemple, une fois l'ensemble des répétitions maximales trouvé, on peut en extraire tous les carrés (ou tous les cubes, etc.) en temps $O(n+S)$ où S est le nombre des répétitions recherchées. Un autre exemple : l'ensemble des répétitions maximales permet de trouver, en temps linéaire, le nombre de répétitions d'un exposant donné commençant à chaque position du mot.

L'algorithme de recherche des répétitions maximales a été implanté par Mathieu Giraud lors de son stage au LORIA[4]. Le logiciel, appelé `mreps`, s'est avéré très efficace. Des tests sur des séquences d'ADN (de l'ordre de centaines de milliers de paires de base) ont été faits et des répétitions intéressantes ont été trouvées. Une mini-interface graphique `graf` a été réalisée pour permettre d'afficher les répétitions à l'écran de façon visuelle. Actuellement nous continuons des expérimentations afin d'analyser, à l'aide de ce logiciel, les régions de séquences de nucléotides homogènes en distribution. Le but est de distinguer les régions qui ont une structure hautement répétitive et par conséquent une complexité d'information basse. Il est également prévu de généraliser `mreps` à la recherche de répétitions avec erreurs du type substitution.

Recherche de motifs dans les séquences. Cette année, grâce au stage d'Éric Queffelec, nous avons repris le travail sur la recherche de motifs « avec trous », que nous avions entrepris il y a quelques années[KR97] et qui avait donné lieu au logiciel `grappe`[5]. Rappelons que `grappe` permet de rechercher dans une séquence un ensemble de motifs avec des espaces entre des sous-chaînes. Plus exactement, `grappe` recherche simultanément un ensemble de motifs du type $v_1 * v_2 * \ldots * v_m$ où les v_i sont des mots de l'alphabet et $*$ est un symbole spécial qui peut être substitué par n'importe quelle sous-chaîne. L'algorithme de `grappe` est basé sur la structure de données appelée DAWG (*Directed Acyclic Word Graph*) qui peut être vue comme un automate fini qui change dynamiquement au cours de son travail.

Dans son stage dirigé par Grégory Kucherov, Éric Queffelec a étendu ce logiciel pour traiter des motifs avec des espaces dont la taille peut être spécifiée par un intervalle (p,q). Pour cette extension nous avons dû résoudre quelques problèmes algorithmiques, liés en particulier à la gestion de la mémoire. Le logiciel étendu a donné lieu à la version 2 de `grappe`[6] qui est en phase de test. Nous envisageons une future version de ce logiciel permettant des erreurs dans les occurrences de sous-chaînes.

4. `http://www.ens-lyon.fr/~magiraud/work/`
5. `http://www.loria.fr/~kucherov/SOFTWARE/grappe-1.0/grappe.tar`
6. `http://www.loria.fr/~kucherov/SOFTWARE/grappe-2.0/grappe-2.0.tar`

[Mai89] M. G. Main, « Detecting leftmost maximal periodicities », *Discrete Applied Mathematics 25*, 1989, p. 145–153.

[KR97] G. Kucherov, M. Rusinowitch, « Matching a Set of Strings with Variable Length Don't Cares », *Theoretical Computer Science 178*, 1997, p. 129–154.

Notons que les motifs « avec trous » apparaissent naturellement dans les applications biologiques, par exemple dans la modélisation de sites de fixation de protéines dans les zones-promoteurs de séquences d'ADN. Le problème de recherche de promoteurs est un des thèmes centraux de l'action de recherche coopérative REMAG (cf section 8.1).

Motifs dans les arbres. Dans le travail [15], commun avec Michaël Rusinowitch du projet PROTHÉO, nous avons entrepris un survol comparatif de résultats de complexité algorithmique d'un certain nombre de problèmes naturels sur les langages de mots et d'arbres spécifiés par des ensembles de motifs. Ces langages, appelés *langages de motifs*, sont beaucoup étudiés ces derniers années à cause de leurs applications dans les domaines du traitement de textes, de l'analyse de génomes, ou encore de l'apprentissage automatique. Les problèmes envisagés comprennent des questions naturelles sur les langages formels : appartenance, finitude, inclusion etc. À part l'analyse des résultats connus de complexité, nous avons obtenu quelques résultats nouveaux : par exemple, nous avons prouvé que dans le cas de mots la co-finitude de l'ensemble des instances d'un ensemble de motifs est indécidable. Ce travail poursuit logiquement des travaux antérieurs[KR94,KR95].

G. Kucherov, en collaboration avec David Plaisted de l'Université de Caroline de Nord, a obtenu quelques nouveaux résultats sur la complexité du problème du complément d'un ensemble de termes. Il s'agit d'estimer, pour un ensemble S de termes, la taille minimale d'un ensemble $\bar{S}$ dont les instances forment le complément par rapport aux instances de l'ensemble S. Dans le cas général, la taille de l'ensemble $\bar{S}$ est exponentielle par rapport à la taille de S. Dans le travail [22], dont la version journal est parue dans la revue *Information Processing Letters* [9], nous avons étudié certaines classes particulières d'ensembles S, pour lesquels nous avons prouvé que la taille de $\bar{S}$ reste toujours exponentielle dans le pire des cas. D'autre part, nous avons démontré que pour certaines classes naturelles, la taille de $\bar{S}$ est polynomiale.

Génération aléatoire. Des travaux entrepris il y a quelques années avec François Bertault, ex-doctorant du projet, ont donné lieu à une communication à la conférence Ordal'99 [11]. Il s'agit d'un algorithme de calcul du rang inverse de structures combinatoires, *i.e.* étant donnés une taille n et un entier k, générant la k-ème structure de taille n selon un ordre fixé. D'autre part, l'article écrit en 1997 avec Alain Denise sur la génération aléatoire à l'aide de nombres flottants est enfin paru [6].

Avec Dominique Poulalhon, doctorante au LIX (École Polytechnique), G. Schaeffer a obtenu une extension de ses résultats de génération aléatoire [Sch99] à une nouvelle famille de triangulations. Il a ainsi été possible de montrer que ces triangulations tricolores, introduites récemment en physique mathématique, forment en fait une nouvelle famille de plongements de graphes

[KR94] G. KUCHEROV, M. RUSINOWITCH, « The Complexity of Testing Ground Reducibility for Linear Word Rewriting Systems with Variables », *in: Proceedings 4th International Workshop on Conditional and Typed Term Rewriting, Jerusalem (Israel)*, N. Dershowitz, N. Lindenstrauss (éditeurs), *Lecture Notes in Computer Science*, 968, Springer Verlag, p. 262–275, juillet 1994.

[KR95] G. KUCHEROV, M. RUSINOWITCH, « Undecidability of Ground Reducibility for Word Rewriting Systems with Variables », *Information Processing Letters 53*, 1995, p. 209–215.

[Sch99] G. SCHAEFFER, « Random sampling of large planar maps and convex polyhedra », *in: Proceedings of the 31st annual ACM sumposium on theory of computing*, ACM Press, p. 760–769, May 1999.

(ou cartes) « élémentaires » (*i.e.* directement encodées par une famille d'arbres[Sch99]). Alors que de nouvelles familles non élémentaires sont régulièrement découvertes ces dernières années, il convient ici de souligner qu'en dehors de cette famille et de celle des constellations[BMS98], toutes les familles élémentaires sont dues à William Tutte dans les années soixante. Ce résultat vient confirmer la pertinence de l'approche bijective introduite par G. Schaeffer dans sa thèse. L'implantation des algorithmes correspondants est en cours.

Combinatoire énumérative et algébrique. La collaboration suivie de G. Schaeffer avec Alain Goupil du LaCIM (Université du Québec à Montréal) et Dominique Poulalhon, doctorante au LIX (École Polytechnique), sur des aspects de calcul explicite dans l'algèbre du groupe symétrique, continue de porter ses fruits. En particulier une grande partie des conjectures du chimiste Jacob Katriel[KP93,Kat96] ont été démontrées. Ces conjectures portent sur l'obtention de décompositions des caractères du groupe symétrique en terme des fonctions puissances des contenus. Traduisant nos résultats théoriques, des fonctions `Maple` élémentaires (quelques lignes) ont été écrites qui permettent de retrouver en quelques minutes de calculs tous les résultats explicites publiés par Katriel[7]. Ces travaux font l'objet d'un rapport de recherche [20], soumis à publication.

G. Schaeffer collabore avec Mireille Bousquet-Mélou du LaBRI (Université Bordeaux I) à l'étude des équations fonctionnelles aux dérivées discrètes dans les problèmes énumératifs. Ces équations correspondent du point de vue combinatoire à des grammaires étiquetées qui étendent les grammaires algébriques (*i.e.* hors contexte) usuelles. Pour de nombreux exemples d'objets combinatoires énumérés par des séries algébriques, les équations aux différences sont beaucoup plus faciles à écrire que les équations algébriques (qui nécessitent souvent des décompositions sophistiquées). En contrepartie il faut alors comprendre sous quelles conditions les solutions des équations aux dérivées discrètes sont algébriques et comment en déduire effectivement des équations algébriques. L'étude de différents exemples a permis de progresser sur ce problème encore largement mystérieux. En particulier, suite à une question de Richard Kenyon (Université Paris Sud), le cas des chemins du plan évitant une demi-droite a été traité par cette approche. Remarquons que pour terminer les calculs explicites, l'assistance des moyens de calculs formels importants disponibles dans l'équipe a été déterminante. Ces résultats sont en cours de rédaction.

Enfin, signalons la parution du travail de Didier Arquès et Alain Giorgetti sur l'énumération des cartes pointées sur une surface orientable[AG99].

7. `http://www.loria.fr/~schaeffe/Pub/Katriel/`

[BMS98] M. Bousquet-Mélou, G. Schaeffer, « Enumeration of planar constellations », to appear in *Adv. Appl. Math.*, LaBRI report 1214-99, 1998.

[KP93] J. Katriel, R. Pauncz, « Eigenvalues of Single-Cycle Class-Sums in the Symmetric Group II », *Int. J. Quant. Chem. 48*, 1993, p. 125–134.

[Kat96] J. Katriel, « Explicit expressions for the central characters of the symmetric group », *Discrete Applied Math. 67*, 1996, p. 149–156.

[AG99] D. Arques, A. Giorgetti, « Énumération des cartes pointées sur une surface orientable de genre quelconque en fonction des nombres de sommets et de faces », *Journal of Combinatorial Theory série B 77*, 1, 1999, p. 1–24.

Estimations asymptotiques. Suite à une question de Bernard Mourrain (projet SAGA, Sophia-Antipolis), en collaboration avec Isabelle Dutour (LaBRI, Bordeaux) et Laurent Habsieger (A2X, Bordeaux), une estimation asymptotique du nombre de chemins Nord-Est de pente fixée et de largeur bornée a été établie en décembre 1998 [19].

Reconstruction d'ensembles discrets bidimensionnels. Dans le cadre de cette étude, deux classes d'objets discrets ont été étudiées : les droites discrètes épaisses et les polyominos convexes.

La première concerne les droites discrètes épaisses définies par J.P. Reveillès [Rev91]. Une droite discrète de pente $\frac{a}{b}$ avec $b \neq 0$ et pgcd$(a,b)= 1$, de borne inférieure μ, d'épaisseur arithmétique ω, est l'ensemble des points entiers x et y satisfaisant la double inéquation diophantienne :

$$\mu \leq ax - by < \mu + \omega$$

avec tous les paramètres entiers.
Un algorithme très simple de reconstruction de ces objets à partir de leurs projections horizontale et verticale a été élaboré. Il repose sur des propriétés des droites discrètes obtenues antérieurement par I. Debled-Rennesson [DR95b,DR95a]. La rédaction de ce travail est en cours d'achèvement.

La deuxième étude concerne la reconstruction des polyominos convexes à partir des vecteurs de projections horizontale et verticale, problème ouvert jusqu'à présent. Les polyominos sont des objets dans lesquels deux cellules quelconques peuvent être reliées par un chemin ne comportant que des déplacements horizontaux et verticaux (4-connexité). La reconstruction des polyominos est un problème NP-complet [Woe96]. Par contre, si l'on considère des polyominos hv-convexes (à la fois convexes par ligne et par colonne), on dispose aujourd'hui de plusieurs algorithmes de reconstruction polynomiaux. Le meilleur algorithme actuel est celui de Chrobak et Dürr [CD99]. Un polyomino convexe étant hv-convexe, nous avons déterminé deux méthodes de détection de polyominos convexes après reconstruction de polyominos hv-convexes par des méthodes connues. La première se déduit directement d'une définition de la convexité discrète et la seconde fait appel à des outils de géométrie discrète comme la reconnaissance de segments de droites discrètes [DR95b]. Les résultats de ces travaux sont soumis.

Parallèlement, un travail a été réalisé par I. Sivignon, stagiaire ENS Lyon, sur la reconstruction de polyominos convexes en utilisant le langage de programmation par contrainte CHIP. Ce stage a été encadré en collaboration avec A. Bockmayr du projet PROTHÉO.

[Rev91] J.-P. REVEILLÈS, *Géométrie discrète, calculs en nombre entiers et algorithmique*, Thèse d'état, Université Louis Pasteur, Strasbourg, 1991.

[DR95b] I. DEBLED-RENNESSON, J.-P. REVEILLÈS, « A linear algorithm for segmentation of digital curves », *International Journal of Pattern Recognition and Artificial Intelligence*, 1995.

[DR95a] I. DEBLED-RENNESSON, *Étude et reconnaissance de droites et plans discrets*, Thèse de doctorat, Université Louis Pasteur, Strasbourg, Décembre 1995.

[Woe96] G. WOEGINGER, « The reconstruction of polyominoes from their orthogonal projections », *rapport de recherche*, Technische Universität Graz, 1996.

[CD99] M. CHROBAK, C. DÜRR, « Reconstructing hv-Convex Polyominoes from Orthogonal Projections », *Information Processing Letters*, 1999.

7 Contrats industriels (nationaux, européens et internationaux)

Constructions Mécaniques des Vosges Marioni (CMW). Depuis septembre 1998, avec l'arrivée de L. Rolland, le projet POLKA est entré en contact avec la société Constructions Mécaniques des Vosges Marioni. L'objet de ce contrat est l'élaboration d'outils performants pour la mise au point des robots parallèles commercialisés par CMW. Ce contrat concrétise une collaboration étroite entre CMW, le projet POLKA ainsi que le projet SAGA de l'INRIA Sophia-Antipolis.

SciFace. Depuis septembre 1998, le projet POLKA représente l'INRIA dans une négociation avec l'entreprise SciFace (commercialisant le logiciel MUPAD) pour la mise au point d'un environnement de travail pour le calcul scientifique incluant MuPAD, ainsi que d'autres produits INRIA (Scilab, Transfor, etc). Deux contrats ont été signés en 1999 : un contrat de recherche entre SciFace et l'INRIA Lorraine pour le co-financement de la chaire industrielle de T. Scott, et un contrat de commercialisation de la passerelle MuPAD-Scilab entre SciFace, l'INRIA Lorraine et le groupe Scilab (INRIA Rocquencourt et École Nationale des Ponts et Chaussées).

8 Actions régionales, nationales et internationales

8.1 Actions nationales

L'équipe POLKA a participé à l'action de recherche coopérative INRIA « Outils pour un calcul numérique fiable » coordonnée par Bernard Philippe (projet ALADIN). Deux réunions ont été organisées à Paris, l'une de travail les 9 et 10 mars 1999, et la réunion de clôture du 22 au 24 septembre 1999. M. Barret, S. Boldo, G. Hanrot, F. Rouillier et P. Zimmermann, ont participé à ces réunions et y ont fait plusieurs exposés. POLKA a coordonné les tâches 3 (arithmétique multi-modulaire) et 6 (arithmétique infinitésimale), et a participé activement à la tâche 7 (bibliothèque pour les fonctions élémentaires) avec Jean-Michel Muller (projet ARÉNAIRE) et à la tâche 4 (structure et fiabilité numérique) avec Bernard Mourrain du projet SAGA.

POLKA participe également à l'action de recherche coopérative REMAG (Recherche et Extraction de Motifs pour l'Analyse Génomique) qui a démarré en 1999 (coordinateur G. Kucherov). Remag regroupe cinq sites (projets INRIA POLKA, ALGO et AÏDA, Université Marne-la-Vallée et Institut Pasteur) ; son but est de développer de nouveaux algorithmes d'analyse de séquences génomiques[8]. Trois réunions de travail (17 février, 5 mai et 13 octobre) ont eu lieu durant l'année 1999. Le thème central des travaux dans le cadre de l'action est la recherche et extraction de motifs « à trous », très importants dans la modélisation de certains signaux biologiques, en particulier les promoteurs dans les séquences d'ADN.

Les membres de POLKA font partie du réseau « Informatique et Génomes » qui s'est constitué en 1997 en réponse à l'appel d'offres du CNRS sur le génome[9]. Ce réseau succède au GdR 1029 « Informatique et génomes » et réunit une part importante de la communauté française

8. cf `http://www.loria.fr/projets/REMAG/`
9. `http://genome.liafa.jussieu.fr/`

travaillant dans ce domaine. POLKA participe également à l'action française « Informatique, Mathématiques, Physique pour la Génomique (IMPG) ».

Les 19 et 20 mai 1999, M. Barret a fait un exposé intitulé « Tests de stabilité d'une classe de filtres numériques bidimensionnels », au colloque organisé en l'honneur de Bernard Picinbono, Professeur émérite à l'université de Paris-Sud. Un article est paru dans le numéro spécial de la revue Traitement du Signal [Bar98]. Les 14 et 15 octobre 1999, M. Barret a fait un exposé à la Réunion des Théoriciens des Circuits de Langue Française (RTCLF'99), intitulé « Tests de stabilité des filtres numériques bidimensionnels ».

G. Kucherov et R. Kolpakov ont été invités à faire un exposé au séminaire de l'Institut Gaspard Monge à l'Université de Marne-la-Vallée (octobre 1998). En janvier 1999, G. Kucherov a également fait des exposés au séminaire de l'ENS Cachan et au séminaire algorithmique du LIAFA (Université Paris 7 Denis Diderot). Il a également fait un exposé invité « Combinatoire des mots en génomique » à la 1ère Journée Strasbourgeoise de BioInformatique le 29 novembre 1999.

G. Hanrot a participé aux rencontres du GDR CNRS ALEA à Bordeaux du 15 au 17 mars. Il a été invité à donner un exposé au « séminaire de théorie analytique des nombres et problèmes diophantiens » de l'Université Bordeaux 1 le 18 mars 1999. Il a aussi participé aux rencontres du GDR CNRS « Théorie analytique des nombres » à l'Université de Limoges le 11 octobre 1999, ainsi qu'à un colloque intitulé « Théorie des nombres, bruit des fréquences et télécommunications ». Lors de l'accueil d'une classe de lycéens à l'occasion de la Fête de la Science au LORIA, il a donné un exposé intitulé « Cryptographie et factorisation : comment et pourquoi », qui décrivait en particulier les travaux sur la factorisation de RSA-155 [24].

G. Schaeffer a présenté ses recherches dans le cadre de la journée scientifique du Loria, le 19 novembre 1999. À cette même occasion, F. Rouillier a fait un exposé à la journée des nouveaux arrivants du LORIA décrivant le travail effectué par POLKA en collaboration avec CMW et ayant, pour partie, rapporté au LORIA le prix de la société industrielle de l'Est.

G. Schaeffer a participé à l'action de recherche coopérative Alcophys (Algorithmique, combinatoire et physique statistique), démarrée en 1999 et coordonnée par Ph. Flajolet (projet ALGO).

G. Schaeffer a donné un exposé intitulé « Cartes, triangulations et polyèdres aléatoires » le 7 décembre 1999 au séminaire d'algorithmique du GREYC à l'université de Caen.

G. Schaeffer a reçu le prix de thèse SPECIF 1999, doté de 10.000 francs et décerné à une thèse d'informatique soutenue dans l'année. À cette occasion il a présenté ses travaux devant l'assemblée générale de l'association SPECIF le 2 décembre 1999.

En novembre, F. Rouillier a fait un exposé au séminaire de géométrie algébrique réelle à l'université de Rennes I sur les méthodes effectives pour l'étude des zéros réels des systèmes d'équations polynomiales. Il a en particulier exposé le dernier résultat publié sur la Représentation Univariée Rationnelle [Rou99].

[Bar98] M. BARRET, « Tests de stabilité des filtres numériques récursifs bidimensionnels », *Traitement du Signal 15*, 6, 1998, p. 595–602.

[Rou99] F. ROUILLIER, « Solving zero-dimensional systems through the rational univariate representation », *Journal of Applicable Algebra in Engineering, Communication and Computing 9*, 5, 1999, p. 433–461.

8.2 Actions internationales

G. Kucherov a fait des exposés au *Symposium on Discrete Algorithms (SODA)* à New-York en janvier 1999, à la conférence internationale *Principles of System Programming (PSI)* à Novossibirsk (Russie) en juillet 1999, à la conférence internationale *Fundamentals of Computation Theory (FCT)* à Iaši (Roumanie) en septembre 1999, et au *Symposium on Foundations of Computer Science (FOCS)* en octobre 1999 à New-York. Il a participé, en tant qu'auditeur et membre de comité d'organisation, à la conférence internationale *Computational Molecular Biology (RECOMB)* à Lyon en avril 1999.

G. Kucherov et R. Kolpakov ont rendu visite, lors de leur voyage aux États-Unis, à la société américaine CompuGene où G. Kucherov a présenté les travaux de Polka dans le domaine de la bioinformatique. En juillet, G. Kucherov a fait un exposé à l'Institut Engel'hardt de Biologie Moléculaire à Moscou.

En avril, F. Rouillier a fait un exposé bilan des 3 années de travail au sein du projet Européen Frisco lors du workshop final a Oxford. À cette même occasion, il a également présenté le travail logiciel effectué devant les évaluateurs de la Communauté européenne à Oxford. L. Rolland a pour sa part montré comment exploiter ces logiciels dans le cadre de problèmes de planification de trajectoires de robots parallèles.

En juin, F. Rouillier a fait un exposé lors de la conférence *IMACS* à Madrid sur l'application de méthodes de calcul exact pour la planification des trajectoires de robots parallèles ; un autre exposé a été fait en association avec J.C. Faugère sur l'application de méthodes de calcul exact pour le calcul de bancs de filtres 2D non séparables.

En juillet, M. Kern (INRIA, projet Estime), J.-C. Faugère et F. Rouillier ont fait un exposé lors de la conférence *ICIAM* (*International Congress on Industrial and Applied Mathematics*) à Edinburgh sur un exemple d'utilisation de bases de Gröbner pour le calcul d'éléments finis [KOFR99]. À cette même conférence, F. Rouillier a présenté le logiciel *RS* et ses applications.

En septembre, F. Rouillier a fait un exposé à l'université de Paderborn sur l'utilisation des logiciels *MuPAD* et *RS* pour la résolution du modèle géométrique direct des robots parallèles.

En mai, G. Hanrot a participé au colloque « *Symposium on number theory in memory of Kustaa Inkeri* » à l'université de Turku (Finlande), où il a donné un exposé. En juillet, il a participé aux « $XXI^{èmes}$ *Journées Arithmétiques* » à la cité du Vatican ; il y a donné un exposé sur ses travaux avec Yann Bugeaud sur l'équation de Catalan.

En mars, un travail commun à P. Tellier (LSIIT, Strasbourg) et I. Debled-Rennesson, sur les normales discrètes 3D, a été présenté à la conférence *Digital Geometry for Computer Imagery* qui s'est déroulée à Marne-la-Vallée.

P. Zimmermann a été invité par R. P. Brent et H. Cohen à la session *Computational Number Theory* de la conférence *Foundations of Computer Mathematics (FoCM)* en juillet 1999. Il y a fait un exposé intitulé *GMP-ECM: yet another implementation of the Elliptic Curve Method (or how to find a* 40*-digit prime factor within* $2 \cdot 10^{11}$ *modular multiplications)*. P. Z. a également participé à la réalisation d'un ouvrage collectif sur l'utilisation pratique des systèmes de calcul formel [10] : il a rédigé avec Frank Postel (groupe MuPAD, Paderborn, Allemagne) le chapitre sur la résolution des équations différentielles ordinaires.

[KOFR99] M. Kern, A. Olouy, J.-C. Faugère, F. Rouillier, « Using Groebner bases to compute higher order finite elements for mass lumping », *in : Proceedings of ICIAM'99*, 1999.

8.2.1 Europe

POLKA a fait partie du projet LTR FRISCO 21.042 (*FRamework for Integrating Symbolic and numerical COmputations*) dont le but est de fournir une panoplie d'outils efficaces pour la résolution des systèmes polynomiaux issus de problèmes de type industriel, et qui s'est terminé en mars 1999.

La relation perdure entre POLKA, l'Université de Paderborn en Allemagne qui développe le système de calcul formel MUPAD, et la société SciFace qui le distribue. Après une action intégrée Procope en 1997, ce partenariat s'est renforcé en 1999 avec la chaire industrielle de T. Scott et la réalisation d'une passerelle entre MuPAD et Scilab.

8.2.2 Russie et Asie Centrale

Dans le cadre de l'Institut franco-russe A. M. Liapounov d'informatique et de mathématiques appliquées, plusieurs membres de POLKA participent au projet « Algorithmique et combinatoire des structures discrètes » (Projet 8) dont G. Kucherov est responsable du côté français. Étant arrivé cette année à la fin de son terme de deux ans, le projet a été évalué et reconduit jusqu'à juin 2000. R. Kolpakov, un des principaux participants russes du projet, a de nouveau rejoint POLKA en 1999 en tant que professeur invité pour un séjour de 3 mois. Les 4-5 février 1999, un séminaire commun du projet a eu lieu à Nancy, centré sur les thèmes de la combinatoire et de l'algorithmique des mots. R. Kolpakov, G. Kucherov, P. Zimmermann y ont présenté leurs travaux.

G. Kucherov participe à une proposition de projet INTAS de la communauté Européenne. Ce projet intitulé « Méthodes, algorithmes et logiciels pour l'annotation fonctionnelle et structurale de génomes complets » regroupe plusieurs laboratoires de bioinformatique en Russie ainsi que des équipes d'Europe occidentale (Allemagne, France, Autriche).

8.3 Visites, et invitations de chercheurs

En 1999, le projet POLKA a invité trois chercheurs étrangers : T. Scott sur une chaire industrielle de 12 mois (septembre 1998 à août 1999) pour la réalisation d'une interface entre MuPAD et Scilab ; R. Kolpakov pour 3 mois comme professeur invité (deux mois sur budget INRIA Lorraine et un mois sur budget du projet) pour la poursuite du travail sur les répétitions maximales ; et V. Makeev pour un mois pour le début d'une collaboration sur l'analyse statistique de génomes.

8.4 Animation scientifique

L'équipe POLKA organise un séminaire, qui a entre autres accueilli cette année Bernard Perrot, Renaud Marlet, Eric Rivals, Vsévolod Makeev.

G. Kucherov est membre du comité de rédaction de la lettre de l'AFIT (Association Française d'Informatique Théorique). Il est également responsable du séminaire d'Informatique Fondamentale du LORIA.

G. Kucherov a fait partie du comité d'organisation de la conférence internationale RECOMB'99 sur informatique et génome, organisé par l'INRIA, qui a réuni plus de 300 spécialistes du domaine du monde entier à Lyon en avril 1999.

I. Debled-Rennesson, G. Kucherov, G. Pierrelée et P. Zimmermann ont fait partie du comité d'organisation du Workshop sur la Tomographie Discrète qui a eu lieu en Lorraine (Domaine de Volkrange, Thionville) en mars 1999.

I. Debled-Rennesson a été responsable pédagogique de l'université d'été « Maîtriser des évolutions de l'informatique pour l'intégration des technologies de l'information et de la communication dans l'enseignement » qui s'est déroulée au Loria du 3 au 5 novembre 1999.

Le projet Polka a organisé du 23 au 25 novembre 1999 à Ventron dans les Vosges des « journées du programme 2B » de l'Inria. À cette occasion se sont retrouvés 27 chercheurs en algorithmique et calcul symbolique, représentant 8 projets (Algo, Arénaire, Café, Codes, Lemme, Polka, Prisme, Saga).

Depuis début 1999, et pour une durée de trois ans, P. Zimmermann est membre élu de la Commission d'Évaluation de l'INRIA, suppléant de Philippe Chartier (INRIA Rennes) sur liste nationale.

8.5 Enseignement

G. Kucherov a enseigné le module de spécialisation « Complexité et analyse d'algorithmes » du DEA d'Informatique de Nancy-Metz.

G. Hanrot occupe des fonctions d'attaché de travaux pratiques à temps partiel à l'École Polytechnique. À ce titre, il a été chargé de co-encadrer des travaux dirigés de dernière année du module « Arithmétique et cryptologie », ainsi que du module « Algorithmes et problèmes NP ». Il participe aussi au cours « Théorie algorithmique des nombres » du D.E.A. d'Algorithmique commun aux Universités de Paris VI, VII, XI, à l'ENS, à l'ENS Cachan, à l'ENST et à l'École Polytechnique.

M. Barret, G. Hanrot et P. Zimmermann ont dispensé un cours de 18h de calcul formel en première année à Supélec.

M. Barret donne un cours de traitement statistique du signal (30h de cours, 18h de TD, polycopié d'environ 130 pages) en troisième année à Supélec, section SIF. Ce cours est également proposé aux étudiants de Georgia Tech Lorraine qui suivent la formation TTI et, comme module optionnel, aux étudiants du DEA de mathématiques appliquées de l'université de Metz. M. Barret donne un cours d'introduction à l'analyse spectrale (9h de cours + 3h de TD) en troisième année à Supélec, dans la section SCO. M. Barret est responsable de travaux de laboratoire (52h) et de projets (32h), en troisième année à Supélec, section SIF et il a donné, en plus de ceux déjà mentionnés des TD (12h) en première et troisième année à Supélec.

9 Bibliographie

Ouvrages et articles de référence de l'équipe

[1] B. Fuchssteiner, K. Drescher, A. Kemper, O. Kluge, K. Morisse, H. Naundorf, G. Oevel, F. Postel, T. Schulze, G. Siek, A. Sorgatz, W. Wiwianka, P. Zimmermann, *MuPAD User's Manual*, Wiley, 1996.

[2] R. Kolpakov, G. Kucherov, « Finding Maximal Repetitions in a Word in Linear Time », *in : Proceedings of the 1999 Symposium on Foundations of Computer Science, New York (USA)*, IEEE Computer Society, p. 596–604, New-York, October 17-19 1999.

Articles et chapitres de livre

[3] F. Bertault, O. Ramaré, P. Zimmermann, « On Sums of Seven Cubes », *Mathematics of Computation*, 68, juillet 1999, p. 1303–1310.

[4] Y. Bilu, G. Hanrot, « Solving superelliptic diophantine equations by Baker's method », *Compositio Math. 112*, 1998, p. 273–312.

[5] Y. Bilu, G. Hanrot, « Thue equations with composite fields », *Acta Arithmetica 58*, 1999, p. 311–326.

[6] A. Denise, P. Zimmermann, « Uniform Random Generation of Decomposable Structures Using Floating-Point Arithmetic », *Theoretical Computer Science 218*, 2, 1999, p. 219–232.

[7] R. Kolpakov, G. Kucherov, Y. Tarannikov, « On repetition-free binary words of minimal density », *Theoretical Computer Science 218*, 1, 1999.

[8] Y.-F. Pétermann, J.-L. Rémy, I. Vardi, « On a functional-differential equation related to Golomb's self-described sequence », *Journal de Théorie des Nombres de Bordeaux 11*, 1, 1999, p. 211–230.

[9] D. Plaisted, G. Kucherov, « The complexity of some complementation problems », *Information Processing Letters 71*, 1999, p. 159–165.

[10] F. Postel, P. Zimmermann, *Computer Algebra Systems: A Practical Guide*, John Wiley & Sons Ltd, 1999, ch. Solving Ordinary Differential Equations.

Communications à des congrès, colloques, etc.

[11] F. Bertault, P. Zimmermann, « Unranking of unlabelled decomposable structures », *in : Proceedings of Ordal'99*, 1999.

[12] S. Cavallar, W. Lioen, H. te Riele, B. Dodson, A. Lenstra, P. Leyland, P. L. Montgomery, B. Murphy, P. Zimmermann, « Factorization of RSA-140 using the Number Field Sieve », *in : Proceedings of Asiacrypt'99*, 1999.

[13] V. Grebinski, G. Kucherov, « Reconstructing Set Partitions », *in : Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'99), Baltimore, Maryland, US*, 1999, `http://www.loria.fr/publications/1999/99-R-012/99-R-012.ps`.

[14] R. Kolpakov, G. Kucherov, « On Maximal Repetitions in Words », *in : Proceedings of the 12-th International Symposium on Fundamentals of Computation Theory, 1999, Iasi (Romania)*, G. Ciobanu, G. Păun (éditeurs), *Lecture Notes in Computer Science, 1684*, Springer Verlag, p. 374 – 385, 30 août - 3 septembre 1999.

[15] G. Kucherov, M. Rusinowitch, « Patterns in words versus patterns in trees : a brief survey and new results », *in : International Conference "Perspectives of Systems Informatics", Novosibirsk, LNCS*, Springer-Verlag, juillet 1999.

Rapports de recherche et publications internes

[16] Y. Bilu, G. Hanrot, P. Voutier, « Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by Maurice Mignotte) », *rapport de recherche*, INRIA, novembre 1999.

[17] Y. Bugeaud, G. Hanrot, M. Mignotte, « Sur l'équation diophantienne $(x^n-1)/(x-1) = y^q$, III », *rapport de recherche n° RR-3808*, INRIA, novembre 1999.

[18] Y. Bugeaud, G. Hanrot, « Un nouveau critère pour l'équation de Catalan », *rapport de recherche*, INRIA, novembre 1999.

[19] I. Dutour, L. Habsieger, P. Zimmermann, « Estimations asymptotiques du nombre de chemins Nord-Est de pente fixée et de largeur bornée », *Rapport de recherche n° RR-3585*, décembre 1998.

[20] A. Goupil, D. Poulalhon, G. Schaeffer, « Central characters and conjugacy classes of the symmetric group », *rapport de recherche*, Loria, novembre 1999.

[21] R. Kolpakov, G. Kucherov, « On the sum of exponents of maximal repetitions in a word », *Rapport de recherche*, LORIA, avril 1999, `http://www.loria.fr/publications/1999/99-R-034/99-R-034.ps`.

[22] D. Plaisted, G. Kucherov, « The Complexity of Some Complementation Problems », *rapport de recherche n° RR-3681*, INRIA, mai 1999, paru dans *Information Processing Letters*.

[23] P. Zimmermann, « Karatsuba Square Root », *Rapport de recherche*, INRIA, novembre 1999.

Divers

[24] S. Cavallar, B. Dodson, A. K. Lenstra, W. Lioen, P. L. Montgomery, B. Murphy, H. te Riele, K. Aardal, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand, F. Morain, A. Muffett, C. Putnam, C. Putnam, P. Zimmermann, « Factorization of a 512–bit RSA Key », soumis à Eurocrypt'2000, 1999, 16 pages.