INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Action GALAAD

Géométrie, ALgèbre, Algorithmes, Approximation et Développements

Sophia Antipolis

THÈME 2B

Table des matières

1. Composition de l'équipe **1**
2. Présentation et objectifs généraux du projet **2**
2.1. (Sans titre) 2
3. Fondements scientifiques **2**
3.1. (Sans titre) 2
3.2. Géométrie 2
3.2.1. Géométrie des variétés algébriques 2
3.2.2. Géométrie discrète 2
3.2.3. Algorithmes géométriques pour les arcs de courbes et carreaux de surfaces 3
3.2.4. Géométrie, groupes et invariants 3
3.2.5. Géométrie des singularités et topologie 3
3.3. Résolution des systèmes d'équations algébriques 3
3.3.1. Méthodes algébriques et structure quotient 3
3.3.2. Dualité, résidus, interpolation 3
3.3.3. Algèbre linéaire structurée et polynômes 3
3.3.4. Décomposition et factorisation 4
3.3.5. Déformation et homotopie 4
3.4. Liens symbolique-numérique 4
3.4.1. Certification 4
3.4.2. Approximation 4
3.4.3. Dégénérescence et arithmétique 4
4. Domaines d'application **4**
4.1. (Sans titre) 4
4.2. CAO 5
4.3. Vision et robotique 5
4.4. Applications prospectives 5
4.4.1. Biologie moléculaire et structures géométriques 5
4.4.2. Traitement du signal 5
5. Logiciels **5**
5.1. alp : Un environnement pour le calcul symbolique et numérique 5
5.2. multires, un module pour la résolution algébrique en Maple 6
5.3. Module courbes et surfaces 6
5.4. Module de factorisation 7
6. Résultats nouveaux **7**
6.1. Géométrie 7
6.1.1. Résultant résiduel 7
6.1.2. Résultant torique 7
6.1.3. Géométrie discrète 8
6.1.4. Degré de la courbe déplacée d'une courbe algébrique 8
6.2. Résolution des systèmes d'équations algébriques 8
6.2.1. Calcul de formes normales dans une algèbre quotient 8
6.2.2. Formules rationnelles pour le résultant 9
6.2.3. Méthode de Weierstrass multivariée 9
6.2.4. Perturbations linéaires 9
6.2.5. Résultant et problèmes de vecteurs propres généralisés 10
6.3. Liens symboliques-numériques 10
6.3.1. PGCD approché de plusieurs polynômes en une variable 10

6.3.2. Factorisation approchée de polynômes à plusieurs variables 10
6.3.3. Certification 10
6.3.4. Approximation 10
6.3.5. Prédicats et cgal 11
6.4. Applications 11
6.4.1. Étalonnage de robots parallèles 11
6.4.2. Conformations moléculaires et géométrie de distances 11
6.4.3. Vision et modélisation géométrique 12
6.4.4. Cryptanalyse, codes et réseaux arithmétiques 12
8. Actions régionales, nationales et internationales 13
8.1. Actions régionales 13
8.1.1. Action Colors 13
8.2. Actions nationales 13
8.2.1. Action de recherche coopérative INRIA costic 13
8.3. Actions internationales 13
8.3.1. ecg : Effective Computational Geometry for Curves and Surfaces 13
8.3.2. gaia 14
8.3.3. Actions bilatérales 14
9. Diffusion des résultats 14
9.1. Animation de la Communauté scientifique 14
9.1.1. Organisation de seminaire 14
9.1.2. Participation aux comités 14
9.1.3. Serveur WWW 15
9.2. Participation à des colloques et invitations 15
9.3. Enseignement universitaire 16
9.4. Thèses en cours 16
9.5. Stages 16
10. Bibliographie 16

1. Composition de l'équipe

Responsable scientifique
Bernard Mourrain [CR1 Inria]

Responsable permanent
Monique Teillaud [CR1 Inria, à 80% (et à 20% dans le projet PRISME)]

Personnel Inria
Ioannis Emiris [CR1, Inria]

Personnel UNSA
Mohamed Elkadi [Maître de Conférence]
André Galligo [Professeur]
Michel Merle [Professeur, à 20% dans le projet]

Assistante du projet
Irène Urso [1er septembre-5 novembre, à temps partiel]
Aurélie Richard [à partir du 5 novembre, à temps partiel]

Chercheurs doctorants
François Anton [en commun avec PRISME, en collaboration avec l'Univ. de British Columbia, jusqu'au 31 août, bourse canadienne BGF]
Laurent Busé [boursier MESR]
Guillaume Chèze [boursier MESR, ED Math. UNSA, à partir du 1er septembre]
Jean-Pascal Pavone [boursier Inria]
Olivier Ruatta [boursier MESR, ED Marseille]
Philippe Trébuchet [boursier MESR]

Personnel en délégation
Alexis Bonnecaze [Maître de Conférence, Univ. de Toulon, jusqu'au 31 août]

Professeur invité
Alicia Dickenstein [Professeur, Univ. de Buenos Aires, Argentine, du 25 mars au 7 avril]
Michael Stillman [Professeur, Cornell Univ., jusqu'au 23 mai]
Mark Van Barel [Professeur, Univ. Leuven, Belgique, du 15 au 22 octobre]

Post-Doctorants
Carlos D'Andrea [INRIA, à partir du 4 septembre]
David Rupprecht [UNSA, jusqu'au 31 juillet]

Collaborateurs extérieurs
Pierre Comon [DR, CNRS-I3S]
Patrick Solé [DR, CNRS-I3S]

Stagiaires
Lamyaa Amane [ENSIAS, Rabat, Maroc, jusqu'au 31 mai]
Alexandro Artola [MIT, du 10 juin au 10 août]
David Binns [Stanford Univ., du 20 juin au 20 août]
Maud Comboul [UNSA, du 14 juin au 14 août]
Vaibhav Gupta [Inst. Indien de Technologie, New Delhi, du 1er juin au 31 juillet]
Anne-Laure Nicoli [UNSA, du 14 juin au 14 août]
Tina Ong [Stanford Univ., du 25 juin au 25 septembre]
Paul Palakel [Inst. Indien de Technologie, New Delhi, du 1er juin au 31 juillet]
Abhishek Pandey [Inst. Indien de Technologie, Kanpur, du 15 mai au 15 juillet]
Raphaël Vandebril [Kath. Univ. Leuven, Belgique, du 15 octobre au 14 novembre]

2. Présentation et objectifs généraux du projet

2.1. (Sans titre)

Action créée le 15 février 2001.

Notre programme de recherche s'articule autour de la géométrie algébrique effective et de ses applications. Notre objectif est de développer des méthodes algorithmiques permettant de résoudre efficacement et de manière fiable les problèmes géométriques et algébriques, rencontrés dans des domaines tels que la CAO, la robotique, la vision par ordinateur, la biologie moléculaire,.... Nous nous intéressons à l'analyse de ces méthodes tant du point de vue de la complexité arithmétique que des aspects qualitatifs, des interactions entre le calcul symbolique et le calcul numérique.

La géométrie est un des thèmes fédérateurs de notre activité. Ce thème inclut la géométrie algébrique effective, la géométrie discrète et combinatoire ou encore la géométrie algorithmique des objets semi-algébriques. Nous nous intéressons plus spécifiquement aux problèmes (intersection, singularité, topologie) en petites dimensions, et considérons avec attention les questions liées aux courbes et surfaces algébriques.

L'algèbre et plus particulièrement les problèmes de résolution sont également au centre de nos préoccupations. Ils apparaissent dès l'origine des mathématiques et ont évolué sous des formes très diverses. Nous nous intéressons à la conception et à l'analyse de méthodes permettant de traiter ces problèmes sur ordinateur et à leurs aspects algorithmiques. Constituants de ce qui est appelé la géométrie algébrique effective, ces développements sont centraux et souvent critiques dans beaucoup de problèmes concrets.

Les calculs numériques approchés, souvent opposés aux calculs formels, et les problèmes de certification sont également au coeur de notre démarche. Nous voulons explorer ces liens entre la géométrie, l'algèbre et l'analyse, qui connaissent actuellement un essor important. Les objectifs sont à la fois théoriques et pratiques, avec le développement de méthodes permettant de contrôler, vérifier et certifier les résultats et leurs utilisations dans des problèmes où les données sont connues avec une précision limitée.

Enfin ces travaux sont accompagnés de développements logiciels. Une attention particulière est donnée aux problèmes de généricité, de modularité et d'efficacité, propres à l'écriture de codes algébriques et géométriques. Les applications et la validation de ces outils dans des domaines spécifiques forment également une composante importante de notre activité.

3. Fondements scientifiques

3.1. (Sans titre)

Notre activité scientifique se décline suivant trois grands thèmes : la géométrie, la résolution des systèmes d'équations algébriques et les liens symbolique-numérique.

3.2. Géométrie

3.2.1. Géométrie des variétés algébriques

Afin de pouvoir résoudre efficacement un problème algébrique, il est important de bien analyser la géométrie de ses solutions. De cette étude, nous pourrons alors déduire la méthode de résolution la mieux adaptée et ainsi produire un solveur efficace, dédié à cette classe de systèmes. La géométrie algébrique effective nous fournit des outils d'analyse permettant de comprendre la géométrie de ces variétés algébriques. Nous les utilisons par exemple pour développer de nouvelles formulations de résultants permettant de produire des solveurs basés sur des outils d'algèbre linéaire et adaptés aux solutions que l'on cherche à approcher.

3.2.2. Géométrie discrète

Nous nous intéressons ici aux propriétés des solutions d'équations polynomiales, qui se déduisent de la géométrie des monômes apparaissant dans les équations, et basée sur le polytope de Newton associé à chaque polynôme. Cette **théorie de l'élimination torique (ou creuse),** introduite dans les années 1970 par l'équipe

de I. Gelfand [GKZ94] offre des bornes plus précises sur le nombre de racines communes et le degré du résultant, ainsi que des algorithmes plus efficaces pour les systèmes polynomiaux creux. Elle établit des ponts algorithmiques entre la géométrie des points à coordonnées entières (qui représentent des monômes) et la géométrie algébrique effective, et plus particulièrement les résultants.

3.2.3. Algorithmes géométriques pour les arcs de courbes et carreaux de surfaces

Les outils de géométrie algébrique effective mentionnés ci-dessus permettent d'analyser en détail mais isolément les variétés algébriques. A l'opposé, la géométrie algorithmique classique traite des problèmes où les données sont des objets linéaires (points, segments, droites) mais apparaissant en très grand nombre. Fusionnant ces deux démarches, nous nous penchons ici sur des problèmes où interviennent des collections d'objets algébriques définis par morceaux. Les propriétés mathématiques de ces structures géométriques, lorsque les données sont ces objets, sont encore mal connues et les algorithmes habituels de la géométrie algorithmique ne se généralisent pas toujours au cas d'objets courbes.

3.2.4. Géométrie, groupes et invariants

Les objets que l'on est amené à manipuler dans les problèmes géométriques sont souvent des points, des droites, des sphères,... et les grandeurs qui décrivent les propriétés de ces objets sont, par nature, indépendants du repère que l'on choisit pour calculer ces grandeurs. Le groupe des changements de repères laisse invariantes ces quantités géométriques. Nous nous intéressons ici au traitement symbolique de ces objets géométriques exploitant les invariants et permettant une représentation plus synthétique des expressions manipulées.

3.2.5. Géométrie des singularités et topologie

L'analyse des singularités d'un ensemble (semi)-algébrique permet de mieux comprendre sa structure et donc de mieux l'appréhender ou l'approcher. Nous nous intéressons en particulier aux applications de la théorie des singularités aux cas de courbes silhouettes, d'ombres, d'ombres portées, de courbes déplacées, de médiatrices de courbes, d'ensemble d'auto-intersections apparaissant dans des problèmes algorithmiques issus de la CAO.

3.3. Résolution des systèmes d'équations algébriques

3.3.1. Méthodes algébriques et structure quotient

L'approche algébrique que nous suivons consiste à analyser et utiliser la structure du quotient des polynômes en n variables modulo les équations que l'on cherche à résoudre, afin d'en déduire la géométrie des solutions de ce système. Ceci soulève des questions de représentation et de calcul de formes normales dans de telles structures. Des réflexions sur les problèmes numériques et algébriques apparaissant dans ce contexte nous ont conduit récemment à une nouvelle approche du calcul de forme normale, qui généralise les célèbres bases de Gröbner [Mou99].

3.3.2. Dualité, résidus, interpolation

Nous nous intéressons ici à l'utilisation « effective » de la dualité, c'est-à-dire aux propriétés des formes linéaires sur les polynômes ou sur le quotient. Nous avons entrepris une étude détaillée de ces outils d'un point de vue algorithmique, permettant de répondre à des questions de base en géométrie algébrique, tout en nous permettant d'améliorer de manière substantielle la complexité de résolution de ces problèmes. Nous nous intéressons en particulier au calcul effectif du résidu algébrique, à des problèmes d'interpolation et aux relations entre coefficients et racines dans le cas de plusieurs variables.

3.3.3. Algèbre linéaire structurée et polynômes

Les travaux précédents conduisent naturellement à la théorie des matrices structurées. En effet, les matrices issues de problèmes polynomiaux comme les matrices de résultants ou les Bézoutiens, sont structurées. Leurs lignes et colonnes sont naturellement indexées par des monômes (ou points à coordonnées entières), et leurs structures généralisent celles des matrices de Toeplitz au cas multivariable. Nous nous intéressons à des algorithmes exploitant leurs propriétés et à leurs implications dans la résolution d'équations polynomiales [MP00a].

3.3.4. Décomposition et factorisation

Lorsque l'on dispose d'un système d'équations à résoudre, un premier traitement à réaliser est de le transformer si possible en plusieurs sous-systèmes plus simples. Nous nous intéressons ici à de nouveaux types d'algorithmes combinant des aspects numériques et formels, plus efficaces mais également fiables. Le problème (difficile) de factorisation approchée, c'est-à-dire du calcul de perturbations des données permettant de décomposer le problème est également étudié. Plus généralement, nous nous intéressons au problème de décomposition d'une variété en composantes irréductibles.

3.3.5. Déformation et homotopie

Le comportement d'un problème dans un voisinage d'une donnée peut s'interpréter en termes de déformations. Dans cette optique, les méthodes d'homotopie consistent à introduire un nouveau paramètre et à suivre l'évolution des solutions entre une position connue et la configuration que l'on cherche à résoudre. Ce paramètre peut aussi être introduit de manière symbolique, comme dans les techniques de perturbation de situations non-génériques. Nous nous intéressons à ces méthodes en vue de les utiliser dans la résolution d'équations polynomiales ainsi que dans de nouveaux algorithmes de factorisation approchée.

3.4. Liens symbolique-numérique

3.4.1. Certification

Les problèmes numériques sont souvent abordés d'un point de vue local. Or dans beaucoup de problèmes, il est important de donner des réponses globales, permettant de certifier les calculs qui sont faits. L'approche symbolique/numérique que nous suivons combine à la fois des aspects algébriques et analytiques, destinés à pouvoir répondre à ces problèmes. Nous nous intéressons en particulier à la certification de prédicats géométriques essentiels à la cohérence topologique des structures géométriques calculées [FDTM01].

3.4.2. Approximation

L'enchaînement de constructions géométriques, si celles-ci sont traitées de manière exacte, conduit souvent à une complexification rapide des problèmes. Il est alors important de pouvoir approcher ces objets tout en contrôlant la qualité d'approximation. Que ce soit en vue d'approcher une surface par un ensemble de triangles respectant sa topologie ou pour construire une approximation du diagramme de Voronoï d'un ensemble d'arcs de courbes, ce problème combine à la fois des aspects géométriques, algébriques et algorithmiques.

3.4.3. Dégénérescence et arithmétique

Les problèmes de singularités obéissent d'après un ingénieur en CAO, à la règle suivante: moins de 20% des cas traités sont singuliers, mais plus de 80% du temps est nécessaire pour développer un code permettant de les traiter correctement. Les dégénérescences sont donc critiques aussi bien du point de vue théorique que du point de vue de la gestion logicielle. Pour remédier à ces difficultés, nous étudions des méthodes de **perturbations** symboliques ou explicites, ou basées sur une arithmétique exacte mais adaptative. Nous travaillons, par exemple pour le calcul du signe d'expressions, sur des approches combinant des calculs modulaires et approchés, qui allient rapidité et exactitude de la réponse [BEPP99].

4. Domaines d'application

4.1. (Sans titre)

Nous regroupons nos domaines applicatifs en plusieurs pôles. Le premier (la Conception Assistée par Ordinateur) est celui que nous mettons en avant. La deuxième catégorie concerne des thèmes dans lesquels nous nous impliquons en vue de transferts directs de nos méthodes. La dernière catégorie concerne des domaines dans lesquels nous menons une activité prospective.

4.2. CAO

Participants : Laurent Busé, Mohamed Elkadi, Ioannis Emiris, André Galligo, Bernard Mourrain, Olivier Ruatta, Monique Teillaud, Philippe Trébuchet.

Mots clés : *modélisation géométrique, ingénierie assistée par ordinateur*.

La modélisation 3D nous est de plus en plus familière (images de synthèse, architecture, vision par ordinateur, internet, ...). Les objets mathématiques sous-jacents sont souvent de nature algébrique (recollement de courbes et surfaces rationnelles), ceux-ci étant ensuite discrétisés afin de les visualiser ou de les manipuler. De tels objets peuvent ainsi être utilisés dans des processus parfois très complexes nécessitant par exemple des calculs d'intersections ou d'isosurfaces (CSG, simulations numériques, ...). Nous nous proposons de développer des méthodes prenant en compte les spécificités algébriques de ces problèmes. Nous aborderons ces questions dont la réponse dépend fortement du contexte ou de l'application envisagée, en relation directe avec les contacts industriels de la CAO que nous avons.

4.3. Vision et robotique

Participants : Mohamed Elkadi, Ioannis Emiris, Bernard Mourrain, Olivier Ruatta, Monique Teillaud, Philippe Trébuchet.

Mots clés : *ingénierie, reconstruction, étalonnage*.

La robotique et la vision sont des domaines privilégiés d'applications des méthodes de résolution d'équations polynomiales. Que se soit pour l'étalonnage de caméras, de robots, le calcul de configurations, d'espace de travail, la résolution de problèmes algébriques avec des coefficients approchées est omniprésentes.

4.4. Applications prospectives

Participants : Alexis Bonnecaze, Pierre Comon, Ioannis Emiris, Bernard Mourrain, Olivier Ruatta, Patrick Solé, Philippe Trébuchet.

Mots clés : *biologie, santé, télécommunications, identification*.

4.4.1. Biologie moléculaire et structures géométriques

La biologie moléculaire est un domaine potentiel d'applications de nos méthodes. Les propriétés chimiques de molécules intervenant dans certains médicaments sont liées aux configurations (ou conformations) qu'elles peuvent prendre. Ces molécules sont vues comme des mécanismes de barres et de sphères, autorisant des rotations autour de certaines liaisons, semblables à des robots séries. La **géométrie des distances** y joue ainsi un rôle important comme dans par exemple pour la reconstruction en RMN, ou dans l'analyse de configurations réalisables ou accessibles.

4.4.2. Traitement du signal

En traitement du signal, des problèmes d'identification « aveugle » des sources d'un signal conduisent à la résolution d'équations algébriques. Les coefficients se déduisent de mesures ou d'observations et sont donc par nature entachés d'erreur. Des méthodes de résolution prenant en compte ces données approchées doivent donc être utilisées. Nous nous intéressons ici aux applications directes de nos méthodes et à leur validation expérimentale.

5. Logiciels

5.1. alp : Un environnement pour le calcul symbolique et numérique

Participants : Ioannis Emiris, Bernard Mourrain [correspondant], Olivier Ruatta, Philippe Trébuchet.

Mots clés : *algèbre linéaire, bézoutien, C++, FFT, généricité, géométrie algébrique effective, lien symbolique-numérique, matrice creuse, matrice structurée, méthode itérative, polynômes, résolution, résultant, stabilité, valeur propre*.

Bibliothèque ALP

Les problèmes que nous rencontrons font appel à la fois à des méthodes manipulant des polynômes, des idéaux, des anneaux quotients,... mais aussi à des calculs numériques sur des vecteurs, des matrices, dans des processus itératifs. Ces domaines étaient jusqu'à présent bien séparés, d'un côté, des logiciels manipulant des formules, souvent peu efficaces pour l'algèbre linéaire numérique, de l'autre, des logiciels stables numériquement et efficaces en algèbre linéaire mais peu adaptés au traitement des polynômes.

L'objectif que nous poursuivons dans la conception du logiciel ALP (Algèbre Linéaire pour les Polynômes [MP00b]) est de fournir un environnement performant, dédié aux calculs symboliques et numériques pour les polynômes, en vue d'applications en robotique, vision, ...

Cette bibliothèque comprend un ensemble de structures et de fonctions permettant de manipuler des vecteurs, des matrices, des polynômes en une ou plusieurs variables. Des outils spécialisés tels que LAPACK, GMP, SUPERLU, RS, GB, … y sont également connectés et peuvent y être utilisés de manière transparente. Une attention particulière a été apportée à la généricité des structures sans pour autant perdre en efficacité. Pour cela, nous avons distingué plusieurs niveaux d'implantation. Le premier niveau concerne les conteneurs qui sont des objets mémorisant les données nécessaires au calcul de manière à optimiser les opérations. Le deuxième niveau concerne les vues (vecteur, polynômes, ...) que l'on veut donner à ces conteneurs et les méthodes qui s'y rattachent. Enfin un troisième niveau, correspondant à des modules (`namespace`), regroupent les implémentations génériques associées à une catégorie d'objets et leurs spécialisations. Nous nous basons pour ces développements, sur le langage C++ qui, grâce à la paramétrisation du code (**template**) et au contrôle de leurs instantiations (**traits, expression template**), offre la généricité indispensable dans ce contexte sans perdre en efficacité.

5.2. multires, un module pour la résolution algébrique en Maple

Participants : Laurent Busé, Ioannis Emiris, Bernard Mourrain [correspondant], Olivier Ruatta.

Mots clés : *algorithmique des polynômes, résultants, résidu, valeur propre, interpolation, algèbre linéaire*.

Le logiciel MULTIRES écrit en Maple contient un ensemble de fonctions pour le traitement de problème de résolution d'équations polynomiales. Il sera bientôt disponible sous la forme d'un ensemble de modules indépendants compatibles avec Maple 7.

MULTIRES permet en particulier de construire des matrices dont le déterminant est un multiple du résultant sur une certaine variété et des algorithmes reposant sur ces formulations, pour résoudre des systèmes d'équations polynomiales. Ce module a comme premier objectif d'illustrer les différentes méthodes algébriques de résolutions. Il est ainsi utilisé dans des enseignements en France et à l'étranger : Angleterre, Argentine, ... Il contient en particulier une implantation d'outils de résolution par calcul de valeurs et vecteurs propres, des bézoutiens en plusieurs variables, de la formulation de Macaulay [Mac02] pour le résultant projectif (ainsi que le calcul du mineur permettant de calculer exactement le résultant), de celle de Jouanolou [Jou91] combinant des matrices de type Macaulay et de Bézout et de résultant (creux) sur une variété torique [CP93][CE00].

Nous avons également rajouté la nouvelle construction que nous proposons pour le résultant résiduel d'une intersection complète [BEM01], ainsi que des fonctions de calcul du degré de cette intersection résiduelle. L'algorithme de décomposition géométrique d'une variété algébrique [EM99a] ainsi que les résolutions à partir de valeurs (ou vecteurs) propres y sont également implémentés.

On y trouve aussi la généralisation en plusieurs variables de la méthode de Weierstrass, présentée dans [Rua01], ainsi qu'une méthode de résolution par homotopie, s'appuyant sur cette généralisation. Par ailleurs, des outils liés à la dualité sur les polynômes y ont également été implémentés, en particulier le calcul du résidu dans le cas d'une intersection complète affine générale, en dimension 0.

5.3. Module courbes et surfaces

Participants : Bernard Mourrain, André Galligo, Jean-Pascal Pavone, Monique Teillaud [correspondante], Philippe Trébuchet, Olivier Ruatta.

La bibliothèque CGAL (Geometric Algorithms Library www.cgal.org est développée depuis plusieurs années dans le projet PRISME en partenariat avec d'autres équipes européennes. Cette bibliothèque utilise les possibilités du langage C++ et se caractérise par sa robustesse, sa généricité, sa flexibilité et son efficacité. CGAL contient à présent un grand nombre de classes d'objets géométriques. Nous nous attachons à participer au développement de fonctionnalités liées aux objets courbes, à la fois pour le noyau (classes d'objets de base munis de prédicats et constructions) et la *basic library* (classes de structures géométriques complexes telles que les diagrammes de Voronoï).

Nous développons également des outils liés aux problèmes d'intersection de courbes et surfaces, de calcul de singularités, et d'auto-intersection s'appuyant sur les outils de résolution de la bibliothèque ALP.

5.4. Module de factorisation

Participants : Guillaume Chèze, André Galligo [correspondant], David Rupprecht.

Une première implantation d'un algorithme de factorisation absolue est disponible. Elle fournit d'excellents résultats pour des polynômes à deux variables de degrés inférieurs à 70. Cette implantation est disponible sous la forme d'un pacage Maple ainsi que comme un programme indépendant (écrit en C). Une seconde implantation est en cours de développement. Elle doit inclure les améliorations récentes [GR01] pour la séparation des composantes irréductibles d'une courbe de $\mathbb{C}^3$ (ou en dimensions plus grandes - pour le nombre de variables ou la dimension de la variété).

6. Résultats nouveaux

6.1. Géométrie

6.1.1. Résultant résiduel

Participants : Laurent Busé, Mohamed Elkadi, Bernard Mourrain.

Mots clés : *élimination, résultant, points base.*

Nous avons continué a développer le résultant résiduel que nous avions introduit dans [BEM01]. Ce résultant résiduel est une extension du résultant classique à l'étude des systèmes algébriques dépendant d'un paramètre qui possèdent des points bases, c'est-à-dire des solutions indépendantes du paramètre. Dans [BEM01] nous donnions une définition du résultant résiduel et un algorithme pour le calculer dans le cas où les points base forment une intersection complète. Depuis nous avons travaillé sur l'extension de cet algorithme au cas des systèmes dont les points base sont de codimension 2 et Cohen-Macaulay. Nous avons également travaillé sur les applications de ce résultant résiduel. Nous avons montré qu'il est possible de généraliser les méthodes de vecteurs et valeurs propres basées sur le résultant classique pour résoudre des systèmes algébriques au cas du résultant résiduel. Nous avons aussi établi un lien entre le résultant résiduel et le travail [BEM00] pour montrer que l'on peut toujours résoudre un système résiduel, quel que soit le lieu des points base, à l'aide d'une représentation rationnelle univariée. Enfin nous avons fourni une nouvelle méthode pour résoudre le problème d'implicitisation lorsque la paramétrisation de la surface rationnelle possède des points base qui forment localement une intersection complète [Bus01].

Tout ces résultats ont été implémentés dans la bibliothèque Maple MULTIRES. Une grosse majorité de nos résultats sont aussi implémentés pour le logiciel Macaulay2.

6.1.2. Résultant torique

Participants : David Binns, Carlos D'Andrea, Ioannis Emiris.

Mots clés : *élimination creuse, polytopes de Newton, subdivision mixte, matrice du résultant.*

Le résultant torique (ou creux) est typiquement exprimé par le biais d'une matrice carrée. Le problème algorithmique qui se pose, est de construire des matrices du résultant torique dont la dimension est la plus petite possible. Pour cela, nous avons proposé des matrices hybrides, se situant entre les matrices de type Sylvester

et Macaulay et celles obtenues par l'approche du Bézoutien. Plus précisément, une ligne de la matrice exprime le Jacobien torique dont les coefficients sont donnés en fonction des coefficients des polynômes d'entrée. Ces matrices étaient introduites dans [CDS98] de façcon abstraite. Nous avons proposé un algorithme explicite et efficace pour construire de telles matrices carrées dans le cas de systèmes de trois polynômes [DE01a]. L'algorithme définit une subdivision mixte de la somme de Minkowski des polytopes de Newton associés aux polynômes donnés. L'implémentation préliminaire en Maple a été suivie par le code développé durant le stage de D. Binns, concernant l'étape critique du relèvement des polytopes de Newton.

6.1.3. Géométrie discrète

Participants : Lamyaa Amane, Ioannis Emiris.

Un calcul important dans la construction d'une matrice du résultant torique concerne l'énumération des points à coordonnées entières à l'intérieur d'une somme de Minkowski de n polytopes convexes et à sommets entiers, en dimension n. En fait, on s'intéresse au calcul d'un sous-ensemble de ces points. Dans [Emi01a] nous avons amélioré l'algorithme utilisé jusqu'à présent et son implémentation en `C` pour obtenir une complexité proportionnelle au produit du nombre de points (qui exprime la taille de la sortie) et d'un polynôme en la dimension et le nombre de sommets, dans la plupart des cas.

L'optimisation linéaire joue un rôle central. Une première amélioration du logiciel existant a été l'objet du stage (co-encadré avec Jean-Pierre Merlet, action COPRIN) de Lamyaa Amane, qui a traité des problèmes avec des contraintes fixes et plusieurs fonctions d'optimisation. La collaboration avec Kyriakos Zervoudakis, étudiant en DEA à l'Université d'Athènes (Grèce) sous la direction de Ioannis Emiris, porte sur des problèmes itérés dont les contraintes diffèrent très peu.

6.1.4. Degré de la courbe déplacée d'une courbe algébrique

Participants : François Anton, Ioannis Emiris, Bernard Mourrain, Monique Teillaud.

Les courbes déplacées (*offsets*) ont été largement étudiées pour leurs applications. Dans le cas où la courbe de départ est algébrique, la courbe déplacée n'est que semi-algébrique, mais la courbe déplacée *généralisée*, qui la contient, est algébrique. Aucune étude du degré de ces courbes n'est actuellement disponible dans la littérature.

Nous avons obtenu des résultats sur le degré de cette courbe déplacée généralisée, résultats beaucoup plus fins que les bornes qui peuvent être déduites par des outils classiques tels que la borne de Bézout, puisque nous tenons compte des composantes parasites induites par les singularités de la courbe de départ, ainsi que des composantes à l'infini.

6.2. Résolution des systèmes d'équations algébriques

6.2.1. Calcul de formes normales dans une algèbre quotient

Participants : Bernard Mourrain, Philippe Trébuchet.

Mots clés : *Polynômes, équations, résolution, algèbre quotient, calcul approchés, formes normales, valeurs et vecteurs propres.*

Coopération avec Daniel Lazard (projet SPACES*)*
Les méthodes algébriques classiques de résolution des systèmes d'équations polynomiales se prêtent mal aux calculs approchés; partant de ce constat, nous avons sur la base d'un nouveau critère de formes normales [Mou99], élaboré un algorithme permettant de calculer la structure de l'algèbre quotient de manière plus robuste numériquement. Sur la base de cet algorithme nous en avons développé une version qui affaiblit le prérequis sur le système de départ. Notre seule hypothèse pour le moment est que le système soit de dimension 0.

Une étude préliminaire de ce genre de méthode est donnée dans [MT01], où la mise en forme de certaines des idées nous permet de décrire un algorithme qui est comparable à l'algorithme F_4 [Fau99] en termes de complexité pratique. Nous nous sommes ensuite penchés sur une méthode unifiant le précédant algorithme et celui décrit dans [MT00]. Il en a résulté un algorithme basé sur des manipulations d'algèbre linéaire.

Un prototype a été implanté en C++ en utilisant la bibliothèque ALP. Il s'avère que la classe d'objets calculables par cet algorithme est plus grande strictement que celle des bases de Gröbner. En fait en introduisant une certaine liberté dans le calcul, on parvient a mieux contrôler la taille des différents coefficients apparaissant. A l'aide de ce prototype nous avons résolu certains problèmes issus de géométrie algorithmique, tels que le calcul des cylindres de rayon fixé ou extrémal passant par 4 ou 5 points donnés de l'espace. Ce travail est décrit dans [DMPT01]. Une autre application de cette méthode à un problème de vision par ordinateur, lié à une variante des équations de Kruppa, est également à l'étude.

Enfin nous étudions actuellement plusieurs voies de développement de ce prototype visant d'une part à affaiblir encore l'hypothèse sur le système polynomial d'entrée, c'est-à-dire de pouvoir traiter le cas d'un système de dimension positive. Nous nous tâchons d'autre part à réduire le temps de calcul en supprimant tous les calculs redondants et aussi en changeant l'anneau sur lequel les calculs sont effectués.

6.2.2. Formules rationnelles pour le résultant

Participant : Carlos D'Andrea.

En généralisant la fameuse formule de Macaulay [Mac02], il est possible d'obtenir une formule rationnelle pour le résultant torique [D'A01b]. Cela offre une réponse partielle à un problème ouvert important, et une conjecture dans [CE00]. Dans le travail [DD01], des formules rationnelles sont spécifiées sur des matrices de type hybride pour le résultant, notamment les matrices étudiées par [Jou97].

De point de vue applicatif, une étude du problème d'implicitisation de surfaces paramétrées a abouti [D'A01c] à une nouvelle preuve du théorème de [CGZ00] concernant la méthode des « quadriques mobiles » (moving quadrics). Cette méthode est ensuite généralisée dans le cas d'une paramétrisation qui n'est pas propre, sous l'hypothèse qu'il n'y a pas de points base.

6.2.3. Méthode de Weierstrass multivariée

Participants : Bernard Mourrain, Olivier Ruatta.

La méthode de Weierstrass est une méthode numérique permettant de calculer simultanément toutes les racines complexes d'un polynôme univarié. A.-M. Bellido a proposé une extension de cette méthode au cas multivarié dans [Bel94], mais sans pouvoir donner de formules réellement explicites. Nous avons donné des formules reposants sur des déterminants de Vandermonde pour exprimer les idempotents d'une algèbre de coordonnées d'un ensemble algébrique de dimension zéro. Ces formules donnent une méthode d'interpolation multivariée analogue à celle de Lagrange dans le cas d'une variable. Il est ainsi possible de construire des ensembles algébriques isomorphes à un ensemble donné. Une telle description donne des extensions naturelles de la méthode de Weierstrass au contexte multivarié [Rua01]. Ainsi, par un prétraitement symbolique, nous obtenons un opérateur local à convergence quadratique pour le calcul simultané de tous les zéros d'un système algébrique. Nous introduisons des méthodes d'homotopie pour concevoir des méthodes à caractère global. Une implantation a été réalisée en C++ en se basant sur les outils disponibles dans la bibliothèque ALP.

6.2.4. Perturbations linéaires

Participants : Carlos D'Andrea, Ioannis Emiris.

Mots clés : *perturbation infinitésimale, matrice du résultant, résolution de systèmes algébriques.*

Nous avons étudié une perturbation symbolique et infinitésimale dans le cadre des matrices du résultant torique (ou creux). Il est possible que ces matrices (ou le résultant torique lui-même) ne fournissent aucune information dans certains cas, dits dégénérés; par exemple, quand le déterminant de la matrice du résultant est identiquement nul, alors qu'il y a des racines isolées qu'il faudrait calculer. C'est la faiblesse principale des méthodes matricielles qui se basent sur le résultant torique. La perturbation infinitésimale linéaire de [DE01b] étend l'idée du « polynôme caractéristique généralisé » de Canny [Can90] mais elle est définie d'après les polytopes de Newton des polynômes, afin de ne pas modifier la structure creuse du système, y compris son volume mixte. Puisqu'il s'agit d'une perturbation linéaire, il est possible de bien borner la complexité de la méthode et d'énoncer des algorithmes pour calculer toutes les racines isolées. Grâce à sa généralité, cette

méthode peut être appliquée au calcul du signe de prédicats. Nous avons implanté ce schéma en Maple, dans le cadre de la librairie MULTIRES.

6.2.5. Résultant et problèmes de vecteurs propres généralisés

Participants : Tina Ong, Bernard Mourrain.

L'utilisation des résultants dans les processus de résolution conduit à un problème de vecteur propre généralisé du type $A(x)\ v = 0$ (où $A(x)$ est une matrice à coefficients des polynômes en x). Durant son stage, T. Ong a ainsi étudié et implémenté un algorithme basé sur un calcul de forme normale de Popov, permettant de résoudre ce problème et étendant un stage précédant de L. Carrot dans notre équipe. Un des gros avantages de cette nouvelle approche est de fournir, une matrice dont la taille est exactement le degré du déterminant de $A(x)$. L'utilisation de ces techniques dans le cas non-générique est à l'étude, dans l'optique de remplacer les perturbations symboliques par des transformations matricielles.

6.3. Liens symboliques-numériques

6.3.1. PGCD approché de plusieurs polynômes en une variable

Participants : André Galligo, David Rupprecht.

Nous avons développé un nouveau point de vue et des algorithmes performants pour calculer des PGCD (Plus Petits Commun Diviseurs) approchés certifiés de polynômes dont les coefficients sont connus avec une précision limitée [Rup00], [GR01][Rup01]. Notre technique étend à ce cas non-linéaire le travail aujourd'hui classique sur le calcul de SVD (Singular Value Decomposition) de matrices approximatives (cf. la bibliothèque LAPACK).

6.3.2. Factorisation approchée de polynômes à plusieurs variables

Participants : Guillaume Chèze, André Galligo.

Nous avons proposé avec nos collaborateurs canadiens de London (Ontario), un nouvel algorithme de factorisation sur les nombres complexes qui procède par calculs approchés avec une grande précision. Il repose sur une nouvelle loi de conservation sur les valeurs discrétisées des graphes de polynômes que nous avons trouvée et sur l'utilisation de la notion de monodromie provenant de la géométrie algébrique. Il semble très efficace. Il s'agit maintenant de l'implémenter pour le tester.

6.3.3. Certification

Participants : Bernard Mourrain, Abhishek Pandey.

Travail effectué en collaboration avec Sylvain Lazard (Projet ISA*).*
Dans le cadre de l'Action de Recherche Coopérative COSTIC, nous nous sommes intéressés aux problèmes de certification intervenant dans les manipulations de quadriques, en particulier à la détection des types d'intersection et à l'arrangement des points sur ces courbes d'intersections. Une synthèse de ce travail entamé durant le stage de A. Pandey, en coencadrement avec S. Lazard, est en préparation.

6.3.4. Approximation

Participant : Bernard Mourrain.

Coopération avec Dimitri Zinoviev du projet PRISME.
Également dans le cadre de l'Action de Recherche Coopérative COSTIC, nous nous sommes intéressés aux approximations de courbes et surfaces, définies par des équations implicites. Pour cela, nous utilisons une méthode d'isolation de racines réelles basée sur une représentation dans la base des polynômes de Bernstein. Dans [MVY01a][MVY01b], nous analysons en détail la complexité de cet algorithme en majorant la hauteur de l'arbre de récursion en fonction du degré et du séparant du polynôme dans le cas de racines simples. Nous utilisons ces résultats pour mettre en place un algorithme de calcul du degré topologique en plusieurs variables.

Par ailleurs, nous étendons cette méthode d'isolation des racines réelles d'un polynôme en une variable au cas 2D et 3D. Les équations sont également représentées dans des bases de Bernstein en deux ou trois variables

et associées à des boîtes ou des simplexes. Ces domaines sont subdivisés suivant la distribution des signes des coefficients afin d'obtenir des représentations polygonales qui décrivent la topologie ou qui approchent à une précision donnée l'objet algébrique. Des expérimentations très satisfaisantes ont été faites avec la bibliothèque ALP, pour le tracé de courbes planes. Les extensions au cas 3D, sont en cours, l'objectif étant d'obtenir un algorithme de triangulation permettant de certifier la topologie et le niveau d'approximation, tout en assurant des propriétés géométriques du maillage (Delaunay). Un article est en cours rédaction.

6.3.5. Prédicats et cgal

Participants : Vaibhav Gupta, Monique Teillaud.

Travail effectué en collaboration avec Sylvain Pion (Projet PRISME*).*

Bibliothèque CGAL *:* `http://www.cgal.org`*.*

Le noyau de la bibliothèque CGAL comprend pour l'instant une grande variété d'opérations sur des objets linéaires (points, segments, etc) mais encore très peu de fonctionnalités concernant des objets courbes.

Dans le cadre du projet européen ECG (Section 8.3.1), nous nous intéressons aux arcs de courbes. Une classe C++ pour représenter des arcs de cercles a été écrite. Le prédicat de comparaison des abscisses de deux points d'intersection entre arcs de cercles, prédicat de base pour le calcul d'arrangements, a été programmé en suivant une méthode combinant l'utilisation de résultants, de techniques algorithmiques et de filtres arithmétiques [FDTM01]. Le travail effectué cette année est la première pierre d'un futur noyau courbe pour CGAL.

6.4. Applications

6.4.1. Étalonnage de robots parallèles

Participant : Ioannis Emiris.

Mots clés : *élimination algébrique, étalonnage robuste, espace de travail.*

Coopération avec David Daney du projet SPACES.

La commande des robots parallèles est dépendante de la connaissance des paramètres qui composent leur modélisation géométrique. Mais les défauts de fabrication et d'assemblage détériorent cette connaissance et ainsi affectent la précision de positionnement. Une procédure d'étalonnage est alors nécessaire à travers la résolution de systèmes surcontraints d'équations. Afin de simplifier la mise en oeuvre expérimentale, nous nous sommes intéressés à des techniques algébriques d'élimination de variables. Le but est ici de supprimer une partie de l'information nécessaire à l'identification des paramètres géométriques. Les techniques utilisées sont basées sur l'obtention d'une matrice du résultant ou de sa généralisation d'après la méthode d'élimination dialytique. Ainsi, nous avons montré comment l'élimination algébrique permet d'obtenir des équations de contraintes qui ne sont dépendantes que de la mesure de la position du robot dans différentes configurations. La mesure de son orientation, plus sensible aux bruits de mesures et plus difficile à réaliser, est algébriquement supprimée. Comparés aux techniques existantes connexes, nous montrons que les systèmes d'équations obtenus par ces techniques sont beaucoup plus stables numériquement, surtout pour des configurations de mesures situées à la frontière de l'espace de travail. Dans ce cas, la fiabilité et la simplicité de l'étalonnage est particulièrement amélioré [DE01c][DE01d].

6.4.2. Conformations moléculaires et géométrie de distances

Participants : Ioannis Emiris, Bernard Mourrain.

Mots clés : *matrice de distances, perturbation matricielle.*

Une partie du travail est effectuée par Théodore Nikitopoulos, étudiant en DEA à l'Université de Crète (Grèce) sous la direction de Ioannis Emiris.

Le problème de calculer toutes les configurations des molécules sous certaines contraintes géométriques est une question cruciale pour la biologie moléculaire et la pharmacologie. Il s'agit d'un problème classique auquel des méthodes de calcul formel ont été appliquées, avec succès dans le cas où le nombre de degré de liberté est petit [EM99b]. Une formulation possible se base sur la **matrice des distances** de la molécule, dont le

rang vaut cinq quand la molécule peut se placer dans l'espace euclidien à trois dimensions. De manière inverse, une molécule de géométrie inconnue peut être spécifiée par une matrice des distances où certaines entrées (voire la majorité) ne sont pas connues exactement. Des expériences (par exemple de Résonance Magnétique Nucléaire) fournissent des bornes inférieures et supérieures sur ces inconnues. Nous avons implémenté une **perturbation structurée** en Matlab et Scilab, appliquée sur les matrices de distances [NE01]. Nous avons calculé des conformations voisines aux données pour les molécules avec, au plus, une trentaine de degrés de liberté. Pour les molécules avec moins de 10 atomes, il est possible d'identifier toutes les conformations possibles dans le cas générique. Notre logiciel enfin explore la variété des conformations afin de borner sa dimension de manière probabiliste.

6.4.3. Vision et modélisation géométrique

Participants : Didier Bondyfalat, Bernard Mourrain.

Coopération avec Théo Papadopoulo du projet ROBOTVIS.

En architecture, en ingénierie civile, en robotique et dans bien d'autres domaines encore, il est important de pouvoir acquérir des informations structurelles sur une scène ou un objet. Les progrès grandissant de la vision artificielle tendent ainsi à construire des modèles virtuels de scènes, directement à partir de simples photographies. L'exploitation des propriétés de ce modèle combinée à l'utilisation d'un plan (type plan cadastral) apporte une connaissance géométrique riche qui peut être mise à profit pour l'étalonnage des caméras. Nous avons développé cette voie et nous avons obtenu des formulations très simples et compactes qui permettent d'exploiter directement certaines propriétés de parallélisme et d'orthogonalité vérifiées par la scène. En fait, ces formulations nous fournissent un algorithme d'étalonnage essentiellement linéaire. Une implémentation a été faite en C++, laissant entrevoir un gros potentiel pour le futur. Ce travail est présenté dans [BMP01].

6.4.4. Cryptanalyse, codes et réseaux arithmétiques

Participants : Alexis Bonnecaze, Patrick Solé, Philippe Trébuchet.

Mots clés : *codage, cryptographie, clé publique, polynôme des poids.*

On s'est intéressé à la cryptanalyse du système NTRU (`http://www.ntru.com`). Nous nous sommes penchés sur différentes approches possibles du problème. La première consiste à le transformer en un problème d'optimisation non linéaire pouvant être résolu par des algorithmes génétiques ou du recuit simulé. Une descente de gradient brute ne permet pas d'obtenir une solution globale car il existe un très grand nombre de minima locaux. Une solution hybride (par exemple, entre algorithmes génétiques et descente de gradient) est envisageable. Pour pouvoir faire fonctionner notre algorithme génétique, nous avons besoin d'une population de génomes et d'une fonction d'énergie qui oriente la reproduction des génomes de manière à sélectionner les meilleurs candidats. Nous cherchons actuellement une bonne configuration en matière de génome, fonction d'énergie et reproduction. Il n'existe malheureusement pas de critère sur la qualité de la configuration choisie. Seuls, des essais sur de petites dimensions (par exemple $N = 11$) peuvent nous guider. Parallèlement, Alexis Bonnecaze s'intéresse avec A. Desideri-Bracco (chercheur doctorant I3S) et P. Solé à une deuxième approche, utilisant des treillis.

Le polynôme des poids est un thème majeur de la théorie des codes en blocs qui a donné lieu à de nombreuses variations : conjoint, coupé, de genre g, ... Si le code est auto-dual, alors ce polynôme à plusieurs variables est un invariant absolu ou relatif d'un certain groupe de matrices, qui reflète non seulement la propriété d'auto-dualité mais encore des propriétés de congruence des poids des mots du code : Type II, Type IV ... Dans [BCDS01] nous étudions les séries théta des deux translatés d'un sous réseau pair d'un réseau unimodulaire impair L. Ces deux translatés constituent le **shadow** de L. Parallèlement, nous nous intéressons au shadow de codes auto-duaux. Nous construisons de nouveaux codes formellement auto-duaux en longueurs $7,\ 15,\ 21,\ 23,\ 31,\ 35$ et 47. Nous nous sommes intéressés aux codes quasi-cycliques et, en particulier, aux codes l-quasi cycliques de longueur $3l$ qui peuvent être obtenus par une construction cubique à partir d'un code binaire et d'un code défini sur F_4, tous deux de longueur l. Dans [BDNS01], nous généralisons la construction

cubique. Nous étudions des codes binaires $l-$quasi-cycliques auto-duaux de longueur $3l$ en tant que codes de longueur l sur $F_2 \times F_4$. Nous obtenons en particulier un nouveau code extrémal en longueur 36.

8. Actions régionales, nationales et internationales

8.1. Actions régionales

8.1.1. Action Colors

Participant : Bernard Mourrain.

Action Colors avec MIAOU (L. Baratchart) et SINUS (J.-A. Désidéri) sur l'utilisation de représentations de courbes et surfaces par spline dans des processus d'optimisation de forme.

8.2. Actions nationales

8.2.1. Action de recherche coopérative INRIA costic

Participants : François Anton, Laurent Busé, Mohamed Elkadi, Ioannis Emiris, André Galligo, Bernard Mourrain [correspondant], Olivier Ruatta, Monique Teillaud, Philippe Trébuchet.

Action COSTIC *:* http://www-sop.inria.fr/galaad/costic
Cette action regroupe quatre équipes : GAMMA (UR-Rocquencourt), ISA (UR-Lorraine), PRISME (UR-Sophia), GALAAD (UR-Sophia).

L'objectif est de regrouper les compétences de différents participants autour des objets tridimensionnels ; en particulier de développer des méthodes d'analyse, de manipulation et de représentation d'objets algébriques, ainsi que des possibilités de visualisation des propriétés de tels objets.

8.3. Actions internationales

8.3.1. ecg : Effective Computational Geometry for Curves and Surfaces

Participants : François Anton, Laurent Busé, Guillaume Chèze, Carlos D'Andrea, Mohamed Elkadi, Ioannis Emiris, André Galligo, Bernard Mourrain, Olivier Ruatta, Monique Teillaud [correspondante], Philippe Trébuchet.

Projet ECG *:* http://www-sop.inria.fr/prisme/ECG/
l'INRIA (PRISME et GALAAD) assure la coordination du projet de recherche communautaire ci-dessous :
– Acronyme : ECG, numéro IST-2000-26473
– Titre : Effective Computational Geometry for Curves and Surfaces.
– Programme spécifique du projet : IST
– Modalité du projet : RTD (FET Open)
– Date de début : 1er mai 2001 - Durée : 3 ans
– Mode de participation de l'Inria : participant via UNSA
– Liste des partenaires :

- ETH Zürich (Suisse),
- Freie Universität Berlin (Allemagne),
- Rijksuniversiteit Groningen (Pays-Bas),
- MPI Sarrebruck (Allemagne),
- Tel Aviv University (Israël)

– Résumé du projet : Traitement effectif des objets courbes en géométrie algorithmique. Algorithmes géométriques pour les courbes et les surfaces, questions algébriques, problèmes de robustesse, approximation.

8.3.2. gaia

Participants : Laurent Busé, Mohamed Elkadi, Ioannis Emiris, André Galligo [correspondant], Bernard Mourrain, Olivier Ruatta.

En relation avec l'université de Nice, l'action GALAAD intervient dans le projet européen GAIA (assessment project) :
– Acronyme : GAIA, numéro IST-1999-29010
– Titre : Applications of approximate algebraic geometry in industrial computer aided geometry
Surfaces.
– Programme spécifique du projet : IST
– Modalité du projet : FET (Assessment project)
– Date de début : Octobre 2000 - Durée : 1 an
– Mode de participation de l'Inria : participant via l'UNSA
– Liste des partenaires :

- Univ. d'Oslo (Suède),
- SINTEF (Suède),
- Think3 (France & Italie),
- UNSA (France)

– Résumé du projet : détection et traitement d'intersections, d'auto-intersections, analyse des singularités, classification, géométrie algébrique approchée et applications à la CAO.

8.3.3. Actions bilatérales

- Collaboration avec le département de Mathématiques de l'Université de Buenos Aires (Argentine), au sein d'une action ECOS-Sud de 3 ans (2001-2003). Elle finance des missions de chercheurs ainsi que des séjours de plus longue durée de thésards et de post-doctorants. Sous le titre « Résolution robuste de systèmes algébriques et applications en la conception assistée par ordinateur », la thématique concerne la théorie de l'élimination, les matrices du résultant, mais aussi de nouveaux sujets de recherche liés aux applications à la modélisation et à la conception assistée par ordinateur. Correspondant : I. Emiris.
- Projet PAI Tournesol avec l'équipe du Prof. M. Van Barel à l'Univ. de Leuven, Belgique, autour des matrices structurées, de l'algèbre des polynômes et de l'analyse numérique, en vue d'étudier, de développer, d'implémenter et de tester sur des problèmes concrets, de nouveaux algorithmes rapides et stables, pour la résolution de systèmes non-linéaires. Correspondant : B. Mourrain.

9. Diffusion des résultats

9.1. Animation de la Communauté scientifique

9.1.1. Organisation de seminaire

Mohamed Elkadi a organisé, avec Evelyne Hubert (projet CAFE) le Seminaire Systèmes Polynomiaux et Différentiels.

9.1.2. Participation aux comités

Ioannis Emiris a participé au comité de programme de la conférence « ACM International Symposium on Symbolic and Algebraic Computation (ISSAC) » et Bernard Mourrain a été l'éditeur des actes de la même conférence.

Bernard Mourrain participe au Comité de pilotage de la Communauté de Calcul Formel.

9.1.3. Serveur WWW

http://www-sop.inria.fr/galaad/ Ce site contient une collection de fiches explicatives sur les sujets présentés dans ce rapport, sur nos publications ainsi que sur les logiciels téléchargeables, que nous développons dans GALAAD.

9.2. Participation à des colloques et invitations

Les membres du projet ont présenté des articles lors de plusieurs conférences : on se reportera à la bibliographie pour en avoir la liste complète.

- L. Busé s'est rendu à l'Université de Oslo (Norvège, 11 mai) pour la rencontre « midterm » de GAIA et il a participé aux Journées COSTIC à Grasse (15-16 février).
- C. D'Andrea a présenté des exposés à « VII Encuentro de Algebra Computacional y Aplicaciones » à La Rioja (Espagne, septembre), à l'atelier ECG à Leiden (Hollande, 1-5 octobre), au Séminaire d'Algèbre et Géométrie, IRMA, U. L. Pasteur, Strasbourg (30 octobre) et au séminaire sur les singularités, Institut de Mathématique, Paris V (novembre)
- M. Elkadi s'est rendu à l'Université de Oslo (Norvège, 11 mai) pour la rencontre « midterm » de GAIA et il a participé aux Journées COSTIC à Grasse (15-16 février) et GAIA à Bologne (Italie, 12-13 octobre).
- I. Emiris s'est rendu à l'Université de Buenos Aires (Argentine, 15-30 avril) dans le cadre de la collaboration bilatérale ECOS-Sud, il a été invité au département de Mathématiques de l'école polytechnique d'Athènes (Grèce, 19 mars), à l'atelier international sur les Mathématiques de Calcul et de Décisions à l'Université de Patras (Grèce, 25-26 mai), aux Journées de la Société Hollandaise et Flamande d'Analyse Numérique à Woudschoten (Hollande, 12-14 septembre), à l'atelier ECG à Leiden (Hollande, 1-5 octobre), à l'atelier Grec-Israélien sur la modélisation à Athènes (Grèce, 11-12 octobre); et il a participé aux Journées COSTIC à Grasse (15-16 février) et à Paris (10-11 décembre), à la conférence « ACM International Symposium on Symbolic and Algebraic Computation », à London, Ontario (Canada, juillet) et à l'atelier international à Dagstuhl « intégration de logiciels géométriques et algébriques » (Allemagne, 15-19 octobre).
- A. Galligo s'est rendu au « Ontario Research Center for Computer Algebra », London (Canada) pour 8 semaines entre les mois de mai et de juillet, et il a participé aux Journées COSTIC à Grasse (15-16 février), à Paris (10-11 décembre) et GAIA à Bologne (Italie, 12-13 octobre).
- B. Mourrain s'est rendu à l'Université de Buenos Aires (Argentine) (19 novembre - 1 décembre) dans le cadre de la collaboration bilatérale ECOS-Sud; il a donné un exposé dans le séminaire de l'action SPACES (22 octobre). Il a participé aux Journées GAIA à Bologne (Italie, 12-13 octobre); il a donné un cours sur les méthodes de résolutions de systèmes algébriques à l'atelier ECG à Leiden (Hollande, 1-5 octobre); il a participé à la conférence « ACM International Symposium on Symbolic and Algebraic Computation », à London, Ontario (Canada, juillet), aux Journées COSTIC à Grasse (15-16 février), à Nancy (17-18 septembre) et à Paris (10-11 décembre), il a été invité à l'atelier international sur les Mathématiques de Calcul et de Décisions à l'Université de Patras (Grèce, 25-26 mai); et au RISC-Linz (14-16 mars) il a également été invité à donner un cours sur les méthodes de résolutions à Heifei, Chine (19 février-9 mars);
- O. Ruatta s'est rendu à l'Université de Buenos Aires (Argentine, 20 novembre - 20 décembre) dans le cadre de la collaboration bilatérale ECOS-Sud; il a donné un exposé à l'école des Jeunes Chercheur en Informatique et en Calcul Formel à Lyon (29 janvier - 2 février), aux Journées COSTIC à Grasse (15-16 février), et au laboratoire GAGE, École Polytechnique, Paris (24-28 septembre).
- M. Teillaud a présenté un exposé sur les « Prédicats » aux Journées COSTIC à Grasse (15-16 février), à Nancy (17-18 septembre) et à Paris (10-11 décembre),

- P. Trébuchet s'est rendu a Timisoara (Roumanie), pour l'atelier Synasc. Il a présenté à cet occasion l'article [MT01]. Il a aussi présenté un exposé dans le cadre du séminaire de l'action SPACES (22 octobre).

9.3. Enseignement universitaire

- L. Busé : Licence de Mathématiques, UNSA, chargé de TD.
- M. Elkadi : Deug et DEA de Mathématiques, UNSA (30h).
- I. Emiris : DEA MDFI, Université d'Aix-Marseille (6h).
- A. Galligo : Deug et Licence de Mathématique, UNSA.
- B. Mourrain : DEA MDFI, Université d'Aix-Marseille (10h), DEA de Mathématiques, UNSA (30h), DEA d'Algorithmique, LIP6, Paris VI (5h). Maîtrise Math-Info, UNSA (45h).
- M. Teillaud : Maîtrise d'informatique UNSA (8h).

9.4. Thèses en cours

- François Anton, Diagramme de Voronoï et variétés algébriques, University of British Columbia, Vancouver, Canada.
- Guillaume Chèze, Factorisation de polynômes à plusieurs variables, UNSA.
- Laurent Busé, Étude algorithmique des résultants sur une variété algébrique, UNSA.
- Jean-Pascal Pavone, Étude de la géométrie des surfaces paramétrées utilisées en CAO., Inria.
- Olivier Ruatta, Dualité des algèbres et problèmes d'effectivité en géométrie algébrique, Université d'Aix-Marseille II.
- Philippe Trébuchet, Vers des algorithmes de résolution d'équations polynomiales stables et rapides, ENS Cachan.

9.5. Stages

Les sujets de stage proposés peuvent être consultés sur `http://www-sop.inria.fr/galaad/stages`

- Lamyaa Amane, **Programmation linéaire et application à la résolution de systèmes polynomiaux**, ENSIAS, Rabat, Maroc.
- Alexandro Artola, **Resultant matrices in ALP: LU decomposition for sparse matrices**, MIT.
- David Binns, **Implementation of a lifting algorithm to construct sparse resultant matrices in small dimensions**, Stanford Univ.
- Maud Comboul et Anne-Laure Nicoli, **Self-Intersection of Curves and Surfaces**, UNSA.
- Vaibhav Gupta, **Implementation of predicates for circle arcs in CGAL**, Inst. Indien de Technologie, New Delhi.
- Tina Ong, **Generalized eigenvector problem and its application**, Stanford Univ.
- Abhishek Pandey, **Intersection de quadriques**, Inst. Indien de Technologie, Kanpur.
- Raphaël Vandebril, **Polynomial interpolation and numerical structured linear algebra**, Katholieke Universiteit Leuven, Belgique.

10. Bibliographie

Bibliographie de référence

[BEM01] L. BUSÉ, M. ELKADI, B. MOURRAIN. *Residual resultant of complete intersection.* in « J. Pure & Appl. Algebra », volume 164, 2001, pages 35–57.

[CE00] J. CANNY, I. EMIRIS. *A Subdivision-Based Algorithm for the Sparse Resultant.* in « J. ACM », numéro 3, volume 47, mai, 2000, pages 417–451.

[EGL97] I. EMIRIS, A. GALLIGO, H. LOMBARDI. *Certified Approximate Univariate GCDs.* in « J. Pure & Applied Algebra, Special Issue on Algorithms for Algebra », volume 117 & 118, mai, 1997, pages 229–251.

[EM99] I. EMIRIS, B. MOURRAIN. *Matrices in Elimination Theory.* in « J. Symbolic Computation, Special Issue on Elimination », volume 28, 1999, pages 3–44.

[EM00] M. ELKADI, B. MOURRAIN. *Algorithms for residues and Lojasiewicz exponents.* in « J. of Pure and Applied Algebra », volume 153, 2000, pages 27-44.

[Emi00] I. EMIRIS. *Algorithmes Algébriques et Géométriques.* Habilitation à diriger des recherches, Université de Nice – Sophia-Antipolis, École Doctorale des Sciences pour l'Ingénieur, janvier, 2000.

[Gal79] A. GALLIGO. *Théorème de division et stabilité en géométrie analytique locale.* in « Ann. Inst. Fourier », volume 29, 1979, pages 107–184.

[GW97] A. GALLIGO, S. WATT. *A Numerical Absolute Primality Test for Bivariate Polynomials.* in « Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation », pages 217–224, 1997.

[Mou97] B. MOURRAIN. *Algorithmes et Applications en Géométrie Algébrique.* Habilitation à diriger des recherches, Univ. de Nice, septembre, 1997.

[MP00] B. MOURRAIN, V. PAN. *Multivariate Polynomials, Duality and Structured Matrices.* in « J. Complexity », numéro 1, volume 16, 2000, pages 110–180.

Livres et monographies

[Mou01] éditeurs B. MOURRAIN., *Proc. Intern. Symp. on Symbolic and Algebraic Computation, Univ. Western Ontario, Canada.* éditeurs B. MOURRAIN., New-York, ACM Press., 2001.

Articles et chapitres de livre

[BEM01] L. BUSÉ, M. ELKADI, B. MOURRAIN. *Residual resultant of complete intersection.* in « J. Pure and Applied Algebra », 2001, note : à paraître.

[CMS01] Y. CHOIE, B. MOURRAIN, P. SOLÉ. *Rankin Cohen brackets and Invariant Theory.* in « J. Algebraic Combinatorics », numéro 1, volume 13, janvier, 2001, pages 5–13.

[D'A01b] C. D'ANDREA. *Macaulay-style formulas for the sparse resultant.* in « Trans. of the AMS », 2001, note : à paraître.

[D'A01c] C. D'ANDREA. *Resultants and Moving Surfaces.* in « J. Symbolic Computation », volume 31, 2001, pages 585–602.

[DD01] C. D'ANDREA, A. DICKENSTEIN. *Generalized Macaulay formulas for the multivariate resultant.* in « J. Pure Applied Algebra », volume 164, 2001, pages 59–86.

[Emi01a] I. EMIRIS. *Enumerating a Subset of the Integer Points inside a Minkowski Sum.* in « Comp. Geom.: Theory & Appl. », 2001, note : à paraître.

[Emi01b] I. EMIRIS. *Matrix Methods for Solving Algebraic Systems.* éditeurs G. ALEFELD, J. ROHN, S. RUMP, T. YAMAMOTO., in « Symbolic Algebraic Methods and Verification Methods », série Springer Mathematics, Springer-Verlag, address Wien, 2001, pages 69–78.

[EP01] I. EMIRIS, V. PAN. *Symbolic and Numeric Methods for Exploiting Structure in Constructing Resultant Matrices.* in « J. Symbolic Computation », 2001, note : à paraître.

[FDTM01] A. FRONVILLE, O. DEVILLERS, M. TEILLAUD, B. MOURRAIN. *Algebraic Methods and Arithmetic Filtering for Exact Predicates on Circle Arcs.* in « Computational Geometry: Theory and Application », 2001, note : à paraître.

[GGVL01] A. GALLIGO, L. GONZÁLEZ-VEGA, H. LOMBARDI. *Continuity properties for flat families of polynomials (I): Continuous parametrizations.* in « J. Pure & Appl. Algebra », 2001, note : à paraître.

[MVY01a] B. MOURRAIN, M. VRAHATIS, J. YAKOUKSHON. *Computing with certainty the topological degree in two dimensions using B-splines.* in « J. Complexity », 2001, note : à paraître.

[Rup01] D. RUPPRECHT. *Semi-Numerical Absolute Factorization of Polynomials with Integer Coefficients.* in « J. Symbolic Computation », 2001, note : à paraître.

Communications à des congrès, colloques, etc.

[BMP01] D. BONDYFALAT, B. MOURRAIN, T. PAPADOPOULO. *Using Scene Constraints during the Calibration Procedure.* in « Int. Conf. of Computer Vision », IEEE Computer Society Press., pages 231–238, 2001.

[Bus01] L. BUSÉ. *Residual resultant over the projective plane and the implicitization problem.* in « Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation », pages 48–55, 2001.

[CDH+01a] B. CHAZELLE, O. DEVILLERS, F. HURTADO, M. MORA, V. SACRISTÁN, M. TEILLAUD. *Splitting a Delaunay Triangulation in Linear Time.* in « Proc. 9th. European Symposiun on Algorithms », série Lecture Notes in Computer Science, volume 2161, Springer-Verlag, pages 312–320, 2001.

[D'A01a] C. D'ANDREA. *Explicit Formulas for the Computation of Resultants.* in « Actas VII Encuentro de Algebra Computacional y Aplicaciones », pages 129–133, 2001.

[DE01a] C. D'ANDREA, I. EMIRIS. *Hybrid Resultant Matrices of Bivariate Polynomials.* in « Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation », ACM Press, pages 24–31, address London, Ontario, 2001.

[DE01b] C. D'ANDREA, I. EMIRIS. *Solving Degenerate Polynomial Systems.* in « AMS-IMS-SIAM Conf. on

Symbolic Manipulation », AMS Contemporary Mathematics, address Mt. Holyoke, Massachussetts, 2001, ftp-sop.inria.fr/galaad/emiris/publis/DAnEmi00.ps.gz note : à paraître.

[DE01c] D. DANEY, I. EMIRIS. *Robust Parallel Robot Calibration with Partial Information.* in « Proc. IEEE Intern. Conf. Robotics Automation », pages 3262–3267, address Seoul, S. Korea, 2001.

[DE01d] D. DANEY, I. EMIRIS. *Variable Elimination for Reliable Parallel Robot Calibration.* in « 2nd Intern. Workshop on Computational Kinematics », pages 133–144, address Seoul, S. Korea, 2001.

[DPT01b] O. DEVILLERS, S. PION, M. TEILLAUD. *Walking in a triangulation.* in « Proc. 17th Annu. ACM Sympos. Comput. Geom. », pages 106–114, 2001.

[GR01] A. GALLIGO, D. RUPPRECHT. *Semi-Numerical Determination of Irreducible Branches of a Reduced Space Curve.* in « Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation », ACM Press, pages 137–142, address New York, 2001.

[NE01] T. NIKITOPOULOS, I. EMIRIS. *Structured Eigenvalue Optimization in Distance Geometry.* in « Hellenic European Conf. Computer Math. & Appl. », address Athens, Greece, septembre, 2001, note : à paraître.

[Rua01] O. RUATTA. *A Mutivariate Weierstrass Iterative Rootfinder.* in « Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation », ACM Press, address New York, 2001.

[ZE01] K. ZERVOUDAKIS, I. EMIRIS. *A Comparative Application of Convex Hull Algorithms in Two and Three Dimensions.* in « Hellenic European Conf. Computer Math. & Appl. », address Athens, Greece, septembre, 2001, note : à paraître.

Rapports de recherche et publications internes

[CDH+01b] B. CHAZELLE, O. DEVILLERS, F. HURTADO, M. MORA, V. SACRISTÁN, M. TEILLAUD. *Splitting a Delaunay Triangulation in Linear Time.* Rapport de recherche, numéro 4160, institution INRIA, 2001, http://www.inria.fr/rrrt/rr-4160

[DMPT01] O. DEVILLERS, B. MOURRAIN, F. PREPARATA, P. TRÉBUCHET. *On circular cylinders by four or five points in space.* Rapport de Recherche, numéro 4195, institution INRIA, octobre, 2001, http://www.inria.fr/rrrt/rr-4195

[DPT01a] O. DEVILLERS, S. PION, M. TEILLAUD. *Walking in a triangulation.* Rapport de recherche, numéro 4120, institution INRIA, 2001, http://www.inria.fr/rrrt/rr-4120

[MVY01b] B. MOURRAIN, M. VRAHATIS, J. YAKOUKSHON. *Isolation of real roots and computation of the topological degree.* Rapport de Recherche, institution INRIA, Octobre, 2001, http://www.inria.fr/rrrt/rr-4300.html

Bibliographie générale

[BCDS01] A. BONNECAZE, Y. CHOIE, S. DOUGHERTY, P. SOLÉ. *Splitting the shadow.* in « Discrete Maths », 2001, note : Submitted.

[BDNS01] A. BONNECAZE, S. DOUGHERTY, L. NOCHEFRANCA, P. SOLÉ. *Cubic Self Dual Binary Codes.* in « IEEE Trans. Information Theory », 2001, note : Submitted.

[Bel94] A.-M. BELLIDO. *Construction of iteration functions for the simultaneous computation of the solutions of equations and algebraic systems.* in « Numerical Algorithms », volume 6, 1994, pages 313–351.

[BEM00] L. BUSÉ, M. ELKADI, B. MOURRAIN. *Generalized resultants for unirationnal algebraic varieties.* in « J. Symbolic Computation », volume 59, 2000, pages 515-526.

[BEPP99] H. BRÖNNIMANN, I. EMIRIS, V. PAN, S. PION. *Sign Determination in Residue Number Systems.* in « Theoretical Computer Science, Special Issue on Real Numbers and Computers », numéro 1, volume 210, 1999, pages 173–197.

[Can90] J. CANNY. *Generalised Characteristic Polynomials.* in « J. Symbolic Computation », volume 9, 1990, pages 241–250.

[CDS98] E. CATTANI, A. DICKENSTEIN, B. STURMFELS. *Residues and Resultants.* in « J. Math. Sci. Univ. Tokyo », volume 5, 1998, pages 119–148.

[CE00] J. CANNY, I. EMIRIS. *A Subdivision-Based Algorithm for the Sparse Resultant.* in « J. ACM », numéro 3, volume 47, mai, 2000, pages 417–451.

[CGZ00] D. COX, R. GOLDMAN, M. ZHANG. *On the Validity of Implicitization by Moving Quadrics for Rational Surfaces with No Base Points.* in « J. Symbolic Computation », volume 29, 2000, pages 419–440.

[CP93] J. CANNY, P. PEDERSEN. *An Algorithm for the Newton Resultant.* rapport de recherche, numéro 1394, institution Comp. Science Dept., Cornell University, 1993.

[EM99a] M. ELKADI, B. MOURRAIN. *A new algorithm for the geometric decomposition of a variety.* éditeurs S. DOOLEY., in « Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation », ACM Press, pages 9–16, address New-York, 1999.

[EM99b] I. EMIRIS, B. MOURRAIN. *Computer Algebra Methods for Studying and Computing Molecular Conformations.* in « Algorithmica, Special Issue on Algorithms for Computational Biology », volume 25, 1999, pages 372–402.

[Fau99] J. FAUGÈRE. *A new efficient algorithm for computing Gröbner Basis (F4).* in « J. Pure & Applied Algebra », volume 139, 1999, pages 61–88.

[GKZ94] I. GELFAND, M. KAPRANOV, A. ZELEVINSKY. *Discriminants and Resultants.* Birkhäuser, address Boston, 1994.

[Jou91] J.-P. JOUANOLOU. *Le Formalisme du Résultant.* in « Adv. in Math. », numéro 2, volume 90, 1991.

[Jou97] J.-P. JOUANOLOU. *Formes d'Inertie et Résultant : Un Formulaire.* in « Adv. in Math. », volume 126, 1997, pages 119–250.

[Mac02] F. MACAULAY. *Some Formulae in Elimination.* in « Proc. London Math. Soc. », numéro 33, volume 1, 1902, pages 3–27.

[Mou99] B. MOURRAIN. *A new criterion for normal form algorithms.* éditeurs M. FOSSORIER, H. IMAI, S. LIN, A. POLI., in « Proc. AAECC », série LNCS, volume 1719, Springer, Berlin, pages 430-443, 1999.

[MP00a] B. MOURRAIN, V. Y. PAN. *Multivariate Polynomials, Duality and Structured Matrices.* in « J. of Complexity », numéro 1, volume 16, 2000, pages 110-180.

[MP00b] B. MOURRAIN, H. PRIETO. *A framework for Symbolic and Numeric Computations.* Rapport de Recherche, numéro 4013, institution INRIA, 2000.

[MT00] B. MOURRAIN, P. TRÉBUCHET. *Solving projective complete intersection faster.* éditeurs C. TRAVERSO., in « Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation », ACM Press., pages 231–238, address New-York, 2000.

[MT01] B. MOURRAIN, P. TRÉBUCHET. *Algebraic methods for numerical solving.* 2001, note : Submitted.

[Rup00] D. RUPPRECHT. *Éléments de Géométrie Algébrique Approchée : Étude du PGCD et de la factorisation.* thèse de doctorat, Université de Nice - Sophia Antipolis, janvier, 2000.