La recherche universitaire en Calcul Formel

Marie-Françoise Roy
IRMAR
Université de Rennes I-35043 Rennes CEDEX

1. Introduction

Utiliser les systèmes de Calcul Formel existants pour mener à bien des calculs symboliques est une activité de plus en plus répandue dans les laboratoires de mathématiques pures ou appliquées et dans de nombreuses autres disciplines. C'est un sujet très intéressant car, grâce au calcul symbolique, toute la chaîne du calcul scientifique peut être amenée à être modifiée.

Mais ce n'est pas le sujet de mon intervention aujourd'hui.

La recherche universitaire en Calcul Formel ne consiste pas à faire des calculs avec les systèmes déjà existants. Elle consiste bien plus en une recherche portant sur les points suivants:

- *formulation précise de problèmes*. Ce point est essentiel car il arrive qu'une très petite modification de la formulation d'une question rende un problème qui était impossible à traiter abordable,
- *effectivité*. Y a-t-il une méthode effective pour résoudre le problème ?
- *complexité*. Quelle est la complexité des algorithmes résolvant ce problème ? Y a-t-il des arguments permettant de donner des bornes inférieures pour la complexité du problème ?
- *efficacité*. Peut on résoudre le problème efficacement ? Ce dernier point

nécessite souvent la mise en place d'outils logiciels ad hoc.

Prenons quelques exemples de problèmes de recherche actuels :

- *la théorie de Galois*. On donne un polynôme à coefficients entiers et on veut connaître le groupe de permutation de ses racines. Un algorithme non efficace a été donné par E. Galois lui-même. Des travaux récents d'A. Vallibouze et J.-M. Arnaudiès donnent des algorithmes pratiques qui permettent de traiter le problème jusqu'au degré 11 [1].
- *la démonstration automatique en géométrie*. La formulation du problème est essentielle. S'il s'agit de trouver toutes les conséquences vraies des axiomes, on ne va pas très loin. Si au contraire, il s'agit de savoir si telle conclusion est conséquence de telles hypothèses, des méthodes basées sur l'algèbre se révèlent êtres très efficaces [2].
- *la résolution des systèmes polynomiaux*. Là encore il convient de préciser. Décider si un système d'équations polynomiales a un nombre fini de racines est un premier problème qui se résout plus facilement que le calcul explicite des racines. Calculer explicitement les racines doit être précisé aussi. Il peut s'agir d'un calcul symbolique, où l'on calcule à partir du système de polynômes de départ de nouvelles équations plus simples, où les solutions seront données, par exemple, sous forme de fonction polynomiale des solutions d'un polynôme en une seule variable. Il peut aussi s'agir d'un calcul numérique où l'on demande des garanties sur les approximations obtenues.

Les difficultés pour résoudre les systèmes polynomiaux sont très surprenantes. A titre d'exemple le système "Cyclic 7" semble très simple. Ses équations sont les suivantes

$$x_1 + \ldots + x_7 = 0$$
$$x_1x_2 + x_2x_3 + \ldots + x_7x_1 = 0$$
$$\vdots$$
$$x_1 \ldots x_7 = 1$$

Mais les calculs pour le résoudre sont gigantesques. C'est seulement depuis quelques années qu'on a pu en dire quelque chose, et on commence à s'attaquer maitenant a Cyclic 8, 9 10 ... Les systèmes de calculs formels existants ne peuvent résoudre ces problèmes et des programmes spécifiques doivent être développés.

- *le cas réel*. Etant donné un polynôme à coefficients entiers, on veut déterminer rapidement le nombre de ses racines réelles. De même pour les systèmes polynomiaux, quel est le nombre de racines réelles ? Qu'est ce qu'un

nombre réel et comment le représenter en machine ? De nombreuses applications à la vision, à la robotique, à la démonstration automatique concernent le cas réel.

2. Structures

Depuis les années 1980 les recherches en calcul formel ont été encouragées par le CNRS au travers de diverses structures (GRECO de Calcul Formel, GDR Medicis, GDR Mathématique-Informatique) ainsi que par l'INRIA. Des équipes se sont développées (Bordeaux, Grenoble, Limoges, Nice, Palaiseau (Ecole Polytechnique), Paris, Rennes).

L'enseignement du calcul formel s'est aussi développé. A. Paugam à Rennes a fait un document donnant la liste des enseignements existants. A Rennes par exemple depuis 1985 , un enseignement de DEA, concernant environ 5 étudiants a été mis en place, puis un module de maîtrise concernant une trentaine d'étudiants puis récemment un module optionnel de licence concernant plus de cent étudiants.

Enfin plus récemment, les projets de recherche européens ont permis de mettre en place des projets intégrés en Europe. Par exemple le projet européen d'ESPRIT POSSO (pour POlynomial System SOlving) regroupe sous la direction de C. Traverso de Pisa des équipes d'Allemagne, Angleterre, Autriche, Espagne, France (Limoges, Nice, Palaiseau, Paris , Rennes), Italie, Suède.

3. Exemples tirés du cas réel

Je développerai plus particulièrement quelques exemples concernant le cas réel puisque c'est celui dans lequel je travaille moi-même. J'espère vous convaincre ainsi que la recherche en calcul formel n'est pas une activité ésotérique, et que de nouvelles solutions pour résoudre les problèmes de base sont encore l'objet de recherches actives.

Le comptage des racines réelles est un problème ancien qui a été partiellement résolu par R. Descartes. Descartes a énoncé la règle suivante : le nombre de racines réelles positives d'un polynôme (comptées avec multiplicité) est inférieur ou égal au nombre de changements de signes dans la suite des coefficients non nuls du polynôme. En particulier, un polynôme avec peu de coefficients non nuls a toujours très peu de racines réelles (et donc beaucoup de racines complexes).

Plus tard, vers 1835, C. Sturm a donné une méthode permettant de compter exactement les racines réelles distinctes. Toutefois cette méthode, basée sur la division euclidienne (voir [3]), donne naissance à des polynômes énormes et rend les calculs peu praticables. Une nouvelle méthode, nommée

"suite de Sturm-Habicht", et qui consiste à relier les calculs de divisions euclidiennes à des calculs de déterminants de matrice et de contrôler ainsi la taille des coeffcients produits a été introduite en 1988 par L. Gonzalez Vega, H. Lombardi, T. Recio et moi même et donne d'excellents résultats pratiques [4].

Les nombres réels généraux ne peuvent naturellement pas être codés exactement en machine. Mais qu'en est-il des nombres algébriques réels, qui sont réels et racines d'un polynôme à coefficients entiers ? L'approche la plus naturelle consiste à caractériser la racine par le polynôme qu'elle annule (puisque ses coefficients sont entiers, il peut être codé en machine) et un intervalle d'isolation à extrémités rationnelles (là encore une information finie).

Utilisant un résultat de R. Thom, datant de 1965, Michel Coste et moi avons proposé en 1988 une nouvelle manière de coder un nombre réel algébrique en machine. Le lemme de Thom consiste à remarquer que deux racines réelles distinctes d'un polynôme P donnent des signes différents à la suite des dérivées de P. La démonstration est du niveau terminale et se base sur une récurrence facile sur le degré du polynôme. On peut ainsi caractériser un nombre algébrique réel par une suite de signes, sans aucune information de nature numérique. Il faut bien sûr montrer ensuite que cette information sur les signes des dérivées aux différentes racines réelles peut s'obtenir à partir de P, par un calcul purement algébrique. Ceci se fait grâce à une extension de la suite de Sturm Habicht [4]. Cette méthode a un intérêt pratique dans certains cas mais son véritable intérêt est théorique car ce résultat est valable dans des situation non archimédiennes qui sont intéressantes pour l'étude des déformations.

Disons enfin quelques mots des applications du cas réel à la vision. Si on part d'objets définis par un nombre fini d'équations et inéquations polynomiales dans l'esace, les théorèmes généraux de la géométrie algébrique réelle [5] permettent de voir

- que le nombre d'aspects visuels de l'objet (disons : la topologie de son contour apparent) est en nombre fini,
- que les événements visuels possibles pour lesquels le contour apparent change sont en nombre finis (il y a dix neuf événements possibles de ce type, comme par exemple l'émergence d'une partie cachée),
- qu'on peut décrire explicitement grâce à des calculs symboliques les différents cas possibles.

Le développement de ce point de vue fait l'objet de la thèse de mon étudiant T. van Ellefterre [6].

Bibliographie

[1] A. VALLIBOUZE: *Théorie de Galois constructive*, LITP, Université Paris VI.
[2] SHANG-CHING CHOU: *Mechanical geometry theorem proving*, Reidel.
[3] J.-L. CHABERT et al.: *Histoire d'algorithmes*, Belin.
[4] M.-F. ROY: *Basic algorithms in real algebraic geometry*, en préparation
[5] J. BOCKNAK, M. COSTE, M.-F. ROY, *Géomérie algébrique réelle*, Springer Verlag.
[6] T. VAN EFFELTERRE: *Aspect visuels et géométrie algébrique réelle*.Thèse en préparation, IRMAR, Université de Rennes I.