Calcul formel

Le calcul formel (ou calcul symbolique) consiste à calculer avec des variables formelles (x, y, ...) ou des données exactes ($1/3, \sqrt{2}, \pi, \ldots$). Ce domaine a été rendu populaire ces dernières années via la diffusion des systèmes de calcul formel comme Mathematica ou Maple. Lorsque Frédérique Bassino m'a demandé d'organiser un cours sur le calcul formel pour l'École Jeunes Chercheurs « Algorithmique et Calcul Formel », j'ai pensé qu'il serait bien d'avoir une présentation synthétique de quelques domaines du calcul formel où des progrès récents ont été réalisés, l'idée étant de montrer les nouveaux algorithmes du domaine, ainsi que les nouvelles applications de ces algorithmes, sans trop rentrer dans les détails techniques.

Éric Schost, chercheur au laboratoire Gage (École Polytechnique), présente le thème « Résolution des systèmes polynomiaux ». Il s'agit là d'un des plus vieux domaines du calcul formel, dont les applications vont du traitement du signal à la vision artificielle, en passant par la cryptographie. Éric montre que le domaine a beaucoup évolué depuis la thèse de Buchberger en 1965, et que le calcul de base de Gröbner n'est plus aujourd'hui un passage obligé pour résoudre ce genre de problème. L'exposé d'Éric convainc du fait que la recherche dans ce domaine est loin d'être terminée. Dans certains cas, on n'a en effet pas encore trouvé quelles sont les bonnes primitives algorithmiques pour résoudre le problème !

Frédéric Chyzak, chercheur du projet Algo (INRIA Rocquencourt), présente le thème « Sommation symbolique ». Là encore, de nombreux progrès récents ont été effectués depuis l'algorithme de Gosper (1978), aussi bien en sommation définie qu'indéfinie. Le cours de Frédéric montre que la recherche d'une forme close n'est pas la seule façon de « calculer » une somme symbolique. Il est souvent plus utile de se ramener à une solution implicite (par exemple sous forme de récurrence), solution qui est parfois mieux adaptée à un traitement ultérieur (développement asymptotique par exemple). Aussi, quand on ne trouve pas de forme close, il est très utile de savoir s'il en existe ou non dans une certaine classe (algorithmes de décision). De nombreux algorithmes sont implantés dans les systèmes de calcul formel comme Maple ou Mathematica ; encore faut-il savoir comment les utiliser... L'exposé de Frédéric, illustré par de nombreux exemples, devrait répondre à cette question.

Guillaume Hanrot, chercheur du projet Spaces (LORIA/LIP6), présente quant à lui le thème « Réduction des réseaux ». Ce thème, un peu moins connu que les deux premiers, a été rendu populaire par l'invention de l'algorithme LLL en 1982. La motivation initiale pour ce nouvel algorithme était de montrer que la factorisation de polynôme s'effectue en temps polynomial. Malheureusement, le « vieil » algorithme exponentiel de Cantor-Zassenhaus restait plus efficace en pratique ! Depuis, de multiples autres applications de la réduction des réseaux ont surgi (reconstruction de nombres algébriques, relations linéaires simultanées, cryptographie, ...) et de nombreuses variantes ont été proposées pour accélérer le calcul de base réduite. Curieusement, il a fallu attendre 2000 et l'algorithme de van Hoeij pour que LLL devienne intéressant en pratique pour l'application initiale de la factorisation ! L'exposé de Guillaume montrera que l'algorithme LLL est un moyen puissant — mais encore assez méconnu — pour résoudre de nombreux problèmes.

Je remercie les trois jeunes chercheurs qui ont accepté de présenter chacun un domaine. Ils ont tous trois réalisé un support de cours de grande qualité, avec des contraintes de temps relativement serrées. Je remercie également les organisateurs de l'EJC « Algorithmique et Calcul Formel » pour leur invitation à présenter le domaine du calcul formel, et surtout je souhaite à tous une excellente école !

Paul Zimmermann
LORIA/INRIA Lorraine