Précision p-adique, échelonnement matriciel et bases de Gröbner

Tristan Vaccon (Univ. Rennes I)

L'avènement de la théorie de Hodge p-adique et ses besoins de calculs explicites, ainsi que les récentes recherches et outils développés en calcul formel p-adiques (voir par exemple le document de Xavier Caruso sur la décomposition LU [2]), ont amené à la question naturelle suivante : quels calculs de bases de Gröbner sur des polynômes à coefficients p-adiques connus de manière approchée sont-ils possibles ?

Par nature, la manipulation sur machine des nombres p-adiques se fait nécessairement de manière approchée, ce qui amène au problème de la définition et du calcul d'une base de Gröbner pour des données connues à précision finie.

En réel, ce type de problème est naturel et a été étudié ces dernières années, entre autres par Shirayanagi et Sweedler, Traverso et Zanoni, Weispfenning, Kondratyev, Stetter et Winkler, Sasaki et Kako, etc... Une excellente introduction aux problèmatiques rencontrées dans ce domaine et vue d'ensemble de celui-ci est l'article [6] de Sasaki et Kako.

Cependant, les résultats obtenus, très orientés sur le point de vue réel, ne s'intéressent pas aux spécificités du calcul en p-adiques.

Tout d'abord, l'une des propriétés les plus remarquables de l'analyse numérique avec $\mathbb{Q}_p$ est que les "erreurs" ne se cumulent pas, tout au contraire de la manipulation de nombres "flottants".

Plus particulièrement, la perte de précision peut être suivie d'opérations élémentaires en opérations élémentaires jusqu'à obtenir le résultat suivant :

Théorème. *Soit M une matrice $n \times m$ dont les coefficients sont des entiers p-adiques connus avec la précision uniforme $O(p^k)$, et telles que son mineur principal $\Delta = det((M_{i,j})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant n})$ vérifie $val(\Delta) < k$.*

Alors, la perte maximale de précision lorsque l'on effectue l'échelonnement de M par l'algorithme de Gauss peut être majorée par $val(\Delta)$ (autrement dit, on peut calculer les coefficients de la forme échelonnée à précision $O(p^{k-val(\Delta)})$.

Maintenant, si l'on fixe un ordre monomial w et k un corps, l'algorithme F5 matriciel (citons [3], [1]) permet de ramener le calcul d'une base de Gröbner à quelques échelonnements matriciels, ceux des matrice de Macaulay en degré d pour ces polynômes, les $Mac_d(f_1, \ldots, f_s)$, pour d plus petit que le degré de régularité, et d'en lire les profils.

Hélas, en précision finie, pour pouvoir certifier le profil d'une matrice échelonnée, il est nécessaire d'avoir une matrice dont le mineur principal est non nul. Les

idéaux vérifiant cette condition sur leurs matrices de Macaulay sont dits être des w-idéaux.

Ceci n'est pas le cas générique, mais on peut voir qu'une notion plus faible est suffisante :

Définition. Soit $(f_1, \ldots, f_s)$ des polynômes homogènes de $k[X_1, \ldots, X_n]$, de degrés $d_1, \ldots, d_s$. On dit que $I = (f_1, \ldots, f_s)$ est faiblement w si pour tout x^α terme de tête d'une base de Gröbner minimale de $(f_1, \ldots, f_s)$ pour l'ordre w, alors tout monôme de degré $|\alpha|$ plus grand que x^α pour cet ordre est dans $LT(I)$.

On a alors le résultat suivant :

Proposition. *Soit $(f_1, \ldots, f_s)$ une suite régulière de $\mathbb{Q}_p[X_1, \ldots, X_n]$ telle que les $I_i = (f_1, \ldots, f_i)$ soit des idéaux faiblement w. On suppose que les f_i sont connus avec une précision suffisante (i.e. plus grande que les valuations des mineurs principaux non nuls maximaux des matrices de Macaulay définis par les f_i). Alors on peut modifier l'algorithme F5 matriciel pour calculer une approximation d'une base de Gröbner de I pour grevlex, et celle-ci est bien définie.*

Enfin, la conjecture de Moreno-Socias (voir [4], [5]) énonce que ce cas particulier est ce qui arrive génériquement dans le cas de l'ordre grevlex, ce qui laisse penser que l'on peut ainsi calculer par un algorithme F5 modifié des approximation des bases de Gröbner d'une assez large part des polynômes à coefficients p-adiques.

Références

[1] Bardet, Magali "Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie", thèse de doctorat, Université Paris VI, Décembre 2004.

[2] Caruso, Xavier Random matrix over a DVR and LU factorization, preprint.

[3] Faugère, Jean-Charles A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In Proceedings of the 2002 international symposium on Symbolic and algebraic computation, ISSAC '02, pages 75-83, New York, NY, USA, 2002. ACM.

[4] Moreno-Socias, Guillermo Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991.

[5] Pardue, Keith Generic Sequences of Polynomials, J. Algebra 324 (2010), no. 4, 579–590

[6] Sasaki,T. & Kako,F. Term cancellations in computing floating-point Gröbner bases. In Proceedings of CASC 2010, volume 6244 of Lecture Notes in Comput. Sci., pages 220–231, Berlin, 2010. Springer.