Algèbre linéaire pour le calcul de bases de Gröbner de suites multidimensionnelles récurrentes linéaires

J. Berthomieu, B. Boyer, J.-Ch. Faugère
Sorbonne Universités, UPMC Univ Paris 06,
CNRS, INRIA, LIP6 UMR 7606, Équipe PolSys,
4 place Jussieu, 75005 Paris.
jeremy.berthomieu@lip6.fr, brice.boyer@lip6.fr,
jean-charles.faugere@inria.fr

En 1988, Sakata a généralisé l'algorithme de Berlekamp – Massey [Ber68, Mas69] à la dimension n. Cet algorithme, connu sous le nom de Berlekamp – Massey – Sakata [Sak88, Sak90], peut être utilisé pour calculer une base de Gröbner de l'idéal, de dimension 0, des relations vérifiées par une table. Nous étudions ce problème en utilisant des techniques d'algèbre linéaire, dans l'esprit de ce qui a été fait pour Berlekamp – Massey [KY13], afin d'améliorer, par exemple, les algorithmes de changement d'ordre [FGLM93].

En dimension 1, les suites récurrentes linéaires à coefficients constants sont des objets classiques. En dimension $n \geq 2$, on peut trouver dans la littérature plusieurs définitions de telles suites qui ne sont pas toutes équivalentes [CN92, SH95]. Nous proposons une définition qui étend les propriétés qu'ont de telles suites en dimension 1. En particulier, cette définition permet de caractériser exactement l'idéal des relations et la série génératrice.

Nous présentons aussi plusieurs algorithmes pour calculer une base de Gröbner de l'idéal des relations. Le premier, requérant beaucoup d'éléments de la table, est l'analogue d'un changement de variables linéaire sur l'idéal des relations. Cette méthode probabiliste permet essentiellement, sous des hypothèses de généricité, de ramener le problème à celui du calcul des rela-

tions de récurrence d'une suite de dimension 1 et donc à un unique appel à l'algorithme de Berlekamp – Massey.

Il n'est pas rare que la connaissance d'un élément de la table puisse être coûteuse. C'est pourquoi, nous nous plaçons ensuite dans le modèle *boîte noire* en cherchant à minimiser le nombre d'appels à la table dans notre modèle de complexité. Nous proposons alors un second algorithme effectuant, en général, moins d'appels.

Cet algorithme, à la FGLM, permet de calculer les relations en se ramenant à l'extraction d'une sous-matrice de rang maximal d'une matrice *multi-Hankel* (une généralisation à plusieurs variables d'une matrice de Hankel). De plus, nous présentons une version adaptative de ce second algorithme réduisant d'avantage le nombre de requêtes à la table.

Le nombre d'appels par le second algorithme peut être estimé précisément par le nombre d'éléments distincts d'une matrice multi-Hankel. Ce nombre est aussi lié à la *géométrie* de l'escalier final de la base de Gröbner. Ainsi, dans les cas favorables comme celui où l'escalier est convexe, la complexité est essentiellement linéaire en la taille de la sortie.

Les techniques d'algèbre linéaire permettent aussi d'estimer la complexité du second algorithme. En effet, lorsque l'ordre monomial utilisé pour le calcul est un ordre LEX, les matrices multi-Hankel sont des matrices bloc-Hankel avec des blocs imbriqués, dites *Hankel à plusieurs à niveaux* [FT00]. Nous pouvons alors utiliser l'algorithmique rapide [BJS07] des polynômes comme dans le cas des matrices de Hankel pour l'algorithme de Berlekamp – Massey.

En application directe à ceci, nous décodons des codes cycliques en dimension $n > 1$, une généralisation des codes de Reed Solomon. Nous proposons aussi un algorithme pour le calcul de séries génératrices de suites récurrentes linéaires à coefficients constants.

Bibliographie

[Ber68] Berlekamp, E., 1968. Nonbinary BCH decoding. IEEE Trans. Inform. Theory 14 (2), 242–242.

[BJS07] Bostan, A., Jeannerod, C.-P., Schost, É., 2007. Solving Toeplitz- and Vandermonde-like Linear Systems with Large Displacement Rank. In: Brown, C. W. (Ed.), ISSAC'07. ACM Press, pp. 33–40.

[CN92] Chabanne, H., Norton, G. H., 1992. On the key equation for n-dimensional cyclic codes: applications to decoding. Tech. report INRIA RR-1796.

[FT00] Fasino, D., Tilli, P., 2000. Spectral clustering properties of block multilevel hankel matrices. Linear Algebra and its Applications 306 (1–3), 155 – 163.

[FGLM93] Faugère, J.-Ch., Gianni, P., Lazard, D., Mora, T., 1993. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. J. Symbolic Comput. 16 (4), 329–344.

[KY13] Kaltofen, E., Yuhasz, G., 2013. On the Matrix Berlekamp-Massey Algorithm. ACM Trans. Algorithms 9 (4), 33:1–33:24.

[Mas69] Massey, J. L., 1969. Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory IT-15, 122–127.

[SH95] Saints, K., Heegard, C., 1995. Algebraic-geometric codes and multidimensional cyclic codes: Theory and algorithms for decoding using Gröbner bases. IEEE Trans. Inform. Theory 41 (6), 1733–1751.

[Sak88] Sakata, S., 1988. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. J. Symbolic Comput. 5 (3), 321–337.

[Sak90] Sakata, S., 1990. Extension of the Berlekamp-Massey algorithm to N Dimensions. Inform. and Comput. 84 (2), 207–239.