Algorithme de Buchberger-Möller avec signatures pour le calcul de bases de Gröbner à coefficients dans un anneau principal

Maria Francis Thibaut Verron

Depuis leur introduction par Buchberger [2] en 1965, les bases de Gröbner sont devenues un outil fondamental en calcul formel. Pour une algèbre de polynômes à coefficients dans un corps, des algorithmes de plus en plus avancés ont été développés. La génération d'algorithmes la plus récente est formée par les algorithmes "à signatures", qui utilisent la notion de signature pour détecter et éliminer des réductions inutiles ou redondantes. Après des travaux préliminaires [11], le premier algorithme à signatures était l'algorithme F5 [5], qui a démontré que garder la trace des signatures permet de détecter un grand nombre de réductions à zéro via le critère F5. L'algorithme F5 permet de calculer une base de Gröbner d'un système donné par une suite régulière – ce qui est génériquement le cas pour un système non-surdéterminé – sans réduction à zéro. L'invariant crucial qui rend ce calcul possible est que *les signatures augmentent tout au long de l'exécution de l'algorithme*. Les algorithmes à signatures ont vu de nombreuses avancées depuis lors, une comparaison exhaustive en est exposée dans [3].

Les bases de Gröbner peuvent également être définies et calculées pour des polynômes à coefficients dans des anneaux [1, Ch. 1]. Certaines applications requièrent ce cadre, par exemple en cryptographie sur les réseaux [6] (coefficients dans $\mathbb{Z}$), ou comme un outil d'élimination [12] (coefficients dans $K[X_1, \dots, X_k]$).

Le développement d'algorithmes à signatures pour les polynômes à coefficients dans un anneau a été l'intérêt de plusieurs travaux récents. Un premier article [4] en 2017 a présenté une adaptation de l'algorithme de Buchberger pour les anneaux euclidients (dû à Kandri-Rody et Kapur [9]), prenant en compte les signatures. Cet article démontre, en exhibant un contre-exemple, que cette technique ne permet pas de maintenir des signatures croissantes, et que par conséquent la correction et la terminaison de l'algorithme ne peuvent être garanties. Néanmoins, l'algorithme avec signatures peut détecter le moment où il ne garantit plus un résultat correct, et être ainsi utilisé comme une phase de précalcul.

Dans une autre direction [7], les auteurs se sont intéressés à un algorithme dû à Möller [10], permettant de calculer une base de Gröbner dite faible pour des polynômes à coefficients dans un anneau noethérien effectif. En restreignant cet algorithme aux coefficients dans un anneau principal, il est possible de le rendre compatible avec le calcul de signatures. La différence cruciale avec l'algorithme présenté dans [4] est que les signatures sont comparées comme dans le cas des corps, sans attribuer un ordre aux coefficients. Elles ne sont donc que partiellement ordonnées, mais les signatures calculées au cours de l'exécution de

l'algorithme forment une suite croissante (au sens large). Il devient notamment possible d'implanter le critère F5 permettant de calculer une base pour un idéal généré par une suite régulière sans réduction à zéro.

Cependant, l'algorithme de Möller n'a qu'un intérêt théorique, car il fait intervenir une combinatoire qui devient impraticable dès que la base devient moyennement longue. Dans ce travail, on montre comment la même technique peut être utilisée pour adapter l'algorithme de Buchberger à l'utilisation de signatures.

Gebauer et Möller ont présenté en 1988 [8] un ensemble de critères permettant d'éliminer des réductions inutiles dans l'algorithme de Buchberger, et dans le cas des corps, il est connu que ces critères sont compatibles avec l'utilisation de signatures. Dans le cas de l'algorithme de Buchberger sur les anneaux, on montre que ces critères peuvent toujours être implantés de manière compatible avec les signatures.

L'algorithme de Buchberger, ainsi optimisé avec les critères de Gebauer-Möller et le critère F5, permet de calculer une base de Gröbner en considérant moins de S-paires que l'algorithme de Buchberger classique, en calculant moins de réductions, et, pour un système décrit par une suite régulière, sans réduction à zéro. De plus, on a vérifié expérimentalement qu'il calcule moins de S-polynômes que l'algorithme de Möller avec signatures, et que, sans surcoût combinatoire, il est significativement plus rapide.

Références

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*. American Mathematical Society, 7 1994.

[2] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, Austria, 1965.

[3] C. Eder and J.-C. Faugère. A Survey on Signature-based Algorithms for Computing Gröbner Bases. *Journal of Symbolic Computation*, 80 :719–784, 2017.

[4] C. Eder, G. Pfister, and A. Popescu. On Signature-Based Gröbner Bases over Euclidean Rings. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 141–148, New York, NY, USA, 2017. ACM.

[5] J.-C. Faugère. 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.

[6] M. Francis and A. Dukkipati. On Ideal Lattices, Gröbner Bases and Generalized Hash Functions. *Journal of Algebra and Its Applications*, 2017.

[7] M. Francis and T. Verron. Signature-based Criteria for Möller's Algorithm for Computing Gröbner Bases over Principal Ideal Domains. *ArXiv preprint*, abs/1802.01388, 2018.

[8] R. Gebauer and H. M. Möller. On an Installation of Buchberger's Algorithm. *Journal of Symbolic Computation*, 6(2-3) :275–286, 1988.

[9] A. Kandri-Rody and D. Kapur. Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain. *J. Symbolic Comput.*, 6(1) :37–57, 1988.

[10] H. M. Möller. On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation*, 6(2-3) :345–359, 1988.

[11] H. M. Möller, T. Mora, and C. Traverso. GrÖbner bases computation using syzygies. In *Papers from the International Symposium on Symbolic and Algebraic Computation*, ISSAC '92, pages 320–328, New York, NY, USA, 1992. ACM.

[12] K. Nabeshima. Reduced Gröbner Bases in Polynomial Rings over a Polynomial Ring. *Mathematics in Computer Science*, 2(4) :587–599, 2009.