Systèmes Bilinéaires et Variétés Déterminantielles : Algorithmes, Complexité et Applications.

Pierre-Jean Spaenlehauer

Travail commun avec Jean-Charles Faugère et Mohab Safey El Din

UPMC, Univ Paris 06, LIP6
INRIA, Paris-Rocquencourt Center, SALSA Project
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy-Kennedy
Case 169, 4, Place Jussieu, F-75252 Paris
Pierre-Jean.Spaenlehauer@lip6.fr

Keywords: MinRank, bases de Gröbner, algorithme F_5, FGLM, cryptanalyse algébrique.

Dans cet exposé, nous nous intéressons à un problème fondamental d'algèbre linéaire : le problème *MinRank*. Étant donnés un corps $\mathbb{K}$, un entier r et une matrice linéaire M de taille $m \times n$ (avec $m \leq n$) sur $\mathbb{K}[x_1, \ldots, x_k]$ (i.e. une matrice dont les entrées sont des polynômes affines de degré 1 en k variables), l'objectif est de trouver l'ensemble des points tels que l'évaluation de M est de rang inférieur ou égal à r. Ce problème est prouvé NP-dur quand $\mathbb{K}$ est un corps fini [3] et il est relié à des applications dans des domaines variés : en cryptologie (sécurité des systèmes multivariés [8, 5, 11]), en théorie des codes (décodage en métrique rang [12]), en géométrie (calcul de points critiques de projections [1]), ...

Nous nous concentrons sur deux modélisations du problème MinRank par des systèmes algébriques multivariés. La première modélisation, proposée par Kipnis et Shamir dans le cadre de la cryptanalyse du système HFE, fait apparaître un système *bilinéaire* en introduisant $n-r$ vecteurs indépendants du noyau de M dont les coefficients sont des indéterminées [11, 8]. La seconde modélisation est donnée par le système constitué de l'ensemble des mineurs de taille $r+1$ de la matrice M (ces mineurs s'annulent sur les solutions du problème MinRank).

Ces systèmes sont ensuite résolus en calculant une base de Gröbner pour l'ordre du degré lexicographique inversé à l'aide de l'algorithme F_5 [6] puis en utilisant un algorithme efficace de changement d'ordre (par exemple FGLM [7] si l'idéal est 0-dimensionnel). Notre objectif est d'étudier et d'exploiter les propriétés algébriques de ces modélisations pour en améliorer la résolution. Ceci passe par l'obtention de bornes fines sur la régularité et le degré des idéaux étudiés.

Pour étudier la modélisation de Kipnis-Shamir, nous avons besoin de nouveaux résultats théoriques et pratiques sur la résolution des systèmes bilinéaires. En particulier, nous prouvons une forme explicite de la série de Hilbert des idéaux engendré par des systèmes bilinéaires génériques, ainsi qu'une borne (atteinte sous une hypothèse de généricité) sur le degré de régularité des systèmes bilinéaires affines : pour un système de $n_x + n_y$ équations bilinéaires affines génériques sur $\mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$,

$$\mathsf{d}_{\mathsf{reg}} \leq \min(n_x, n_y) + 1$$

Une conséquence directe de ce résultat est une nouvelle borne sur la complexité de résolution des systèmes bilinéaires affines par des algorithmes de calcul de bases de Gröbner. Nous proposons également une variante dédiée aux systèmes multihomogènes de l'algorithme F_5 qui exploite la structure des matrices de Macaulay pour améliorer la complexité. Dans le cas bilinéaire (i.e. bihomogène de bidegré $(1,1)$), une extension du critère F_5 est proposée, et permet d'éviter toutes les réductions à 0 dans le cas générique. En effet, les syzygies dûes à la structure du système proviennent du noyau de matrices jacobiennes. Par conséquent, les réductions à 0 peuvent être détectées en calculant une base de Gröbner de l'idéal engendré par les mineurs maximaux de ces matrices. Une variante d'un théorème de Sturmfels et Zelevinski [13] montre que le coût de ce calcul est négligeable par rapport au coût global du calcul de base de Gröbner, ce qui est vérifié en pratique.

Du point de vue de la modélisation déterminantielle (i.e. le système constitué des mineurs de taille $r+1$ de la matrice M), nous donnons – sous une hypothèse de généricité – une forme explicite et *exacte* du degré de l'idéal engendré par les mineurs :

$$\prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

Nous prouvons également une forme explicite de sa série de Hilbert, sur laquelle on peut notamment lire le degré de régularité lorsque l'idéal est 0-dimensionnel. Les preuves font intervenir des résultats sur les idéaux engendrés par les mineurs de matrices dont les coefficients sont des indéterminées [4], ainsi que le théorème de Bertini.

Ces nouvelles formules permettent d'obtenir des estimations précises de complexité asymptotique. En particulier, on montre que le problème MinRank générique peut être résolu en temps polynomial quand $n = m$ (la matrice M est carrée), $k = (n-r)^2$ est fixé et n croît : la complexité est alors bornée par $O(n^{3k})$. Cette analyse de complexité va nous guider vers une méthode efficace pour résoudre un challenge issu de la cryptologie pour lequel aucune attaque effective n'était connue jusqu'à présent [5, Challenge C].

Références

[1] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, 21(1) :33–83, 2010.

[2] W. Bruns and U. Vetter. *Determinantal rings*. Springer, 1988.

[3] J. Buss, G. Frandsen, and J. Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3) :572–596, 1999.

[4] A. Conca and J. Herzog. On the Hilbert function of determinantal rings and their canonical module. *Proceedings of the American Mathematical Society*, pages 677–681, 1994.

[5] N. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. *Lecture notes in computer science*, pages 402–421, 2002.

[6] 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*, page 83. ACM, 2002.

[7] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4) :329–344, 1993.

[8] J.-C. Faugère, F. Levy-dit-Vehel, and L. Perret. Cryptanalysis of MinRank. In *Proceedings of the 28th Annual conference on Cryptology : Advances in Cryptology*, page 296. Springer, 2008.

[9] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology. Submitted to ISSAC, 2010.

[10] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1) : Algorithms and complexity. *arXiv :1001.4004v1 [cs.SC]*, 2010.

[11] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. *Lecture Notes in Computer Science*, pages 19–30, 1999.

[12] A. Ourivski and T. Johansson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38(3) :237–246, 2002.

[13] B. Sturmfels and A. Zelevinsky. Maximal minors and their leading terms. *Adv. Math*, 98(1) :65–112, 1993.