Algorithmes en temps polynomial pour l'isomorphisme de polynômes quadratiques : le cas régulier

J. Berthomieu, J.-C. Faugère, L. Perret
Sorbonne Universités, UPMC Univ Paris 06,
Équipe PolSys, LIP6, F-75005, Paris
CNRS UMR 7606, LIP6, F-75005, Paris
INRIA, Équipe PolSys, Centre Paris – Rocquencourt
jeremy.berthomieu@lip6.fr,
jean-charles.faugere@inria.fr,
ludovic.perret@lip6.fr

Soient $\mathbb{K}$ un corps et $\mathbf{x} = (x_1, \ldots, x_n)$ des indéterminées. Soient $\mathbf{f} = (f_1, \ldots, f_m)$ et $\mathbf{g} = (g_1, \ldots, g_m)$ deux ensembles de $m \geq 1$ polynômes homogènes dans $\mathbb{K}[\mathbf{x}]$. On considère le problème d'équivalence consistant à calculer une matrice $A \in \mathrm{GL}_n(\mathbb{K})$ telle que $\mathbf{f}(A \cdot \mathbf{x}) = \mathbf{g}(\mathbf{x})$. Ce problème fondamental de part son nombre d'applications est appelé l'*Isomorphisme de Polynômes à un Secret* (`IP1S`). Parmi ces applications, on peut noter l'*Isomorphisme de Graphes* dont Agrawal et Saxena [1] ont montré qu'il se ramenait à une instance d'`IP1S` avec f_1, g_1 cubiques et f_2, g_2 quadratiques, des cryptosystèmes en cryptographie multivariée, la réduction de circuits en complexité algébrique... On peut aussi remarquer que si $m = 1$ et f_1, g_1 sont de degré 2, alors `IP1S` se résout facilement à l'aide de l'algorithme de réduction des formes quadratiques de Gauss. En calcul formel, un problème proche d'`IP1S` est celui de la simplification d'un système polynomial $\mathbf{f}$: on cherche $A \in \mathrm{GL}_n(\mathbb{K})$ telle que $\mathbf{g}(\mathbf{x}) = \mathbf{f}(A \cdot \mathbf{x})$ est plus simple à résoudre. Dans cette optique, les algorithmes Ridge [3] et MinVar [4] réduisent au maximum le nombre de variables du système considéré. Plus généralement, étant donné $\mathbf{f}$, la *Décomposition fonctionnelle* consiste à calculer $\mathbf{h} = (h_1, \ldots, h_s)$ homogènes et $\mathbf{g}$ tels que $\mathbf{f}(\mathbf{x}) = \mathbf{g}(\mathbf{h}(\mathbf{x}))$.

Dans cet exposé, nous présentons un algorithme probabiliste en temps polynomial pour résoudre les instances quadratiques régulières d'`IP1S` avec

m quelconque [2]. Notons $H_1, \ldots, H_m$ les représentations matricielles des f_i, avec $\operatorname{char} \mathbb{K} \neq 2$. Une instance quadratique sera dite *régulière* s'il existe une combinaison linéaire des H_i de rang maximal. Ceci améliore les résultats obtenus par les algorithmes proposés jusqu'à présent qui étaient soit heuristiques, avec une complexité potentiellement non polynomiale, soit dédiés à des cas particuliers comme $m = 2$.

Soient $H'_1, \ldots, H'_m$ les représentations matricielles de $g_1, \ldots, g_m$. Résoudre le problème d'équivalence entre $\mathbf{f}$ et $\mathbf{g}$ revient à calculer A inversible telle que

$$A^{\mathrm{T}} H_i A = H'_i, \quad \forall i,\ 1 \leqslant i \leqslant m.$$

Nous montrons alors que l'on peut essentiellement *linéariser* le problème en nous ramenant à tester la conjugaison simultanée de matrices symétriques par une matrice orthogonale, c'est-à-dire à résoudre

$$A^{\mathrm{T}} A = \mathrm{Id}_n, \quad H_i A = A H'_i, \quad \forall i,\ 2 \leqslant i \leqslant m.$$

Chistov, Ivanyos et Karpinski [5] ont montré que ce dernier problème est équivalent à calculer une matrice inversible dans un sous-espace de $\mathbb{K}^{n \times n}$ et d'en calculer une racine carrée. Alors que calculer une racine carrée de matrice peut être effectué efficacement en utilisant des méthodes numériques, il semble difficile de contrôler la complexité binaire de telles méthodes. En effet, si $\mathbb{K} = \mathbb{Q}$, la racine carrée peut n'exister que dans une extension de $\mathbb{K}$ de degré exponentiel en n. Nous présentons ainsi des algorithmes exacts et en temps polynomial pour calculer une représentation d'une racine carrée d'une matrice dans $\mathbb{K}^{n \times n}$ nous permettant de déduire si $\mathbf{f}$ et $\mathbf{g}$ sont équivalents.

Enfin, nous donnons des résultats expérimentaux où nous résolvons des instances dont les tailles dépassent d'un ordre de grandeur les *challenges* cryptographiques.

Bibliographie

[1] M. Agrawal and N. Saxena, 2006. Equivalence of F-Algebras and Cubic Forms. In : B. Durand, W. Thomas (Eds.), STACS. Vol. 3884 of Lecture Notes in Computer Science. Springer, pp. 115–126.

[2] J. Berthomieu, J.-C. Faugère and L. Perret, 2014. Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials : The Regular Case. Preprint, `http://hal.inria.fr/hal-00846041`.

[3] J. Berthomieu, P. Hivert and H. Mourtada, 2010. Computing Hironaka's invariants : Ridge and Directrix. In : Arithmetic, Geometry, Cryptography and Coding Theory 2009. Vol. 521 of Contemp. Math. Amer. Math. Soc., Providence, RI, pp. 9–20.

[4] E. Carlini, 2005. Reducing the number of variables of a polynomial. In : Algebraic geometry and geometric modeling. Springer, pp. 237–247.

[5] A. L. Chistov, G. Ivanyos and M. Karpinski, 1997. Polynomial time algorithms for modules over finite dimensional algebras. In : B. W. Char, P. S. Wang, W. Küchlin (Eds.), ISSAC. ACM, pp. 68–74.