Calcul des facteurs de petit degré des polynômes lacunaires

B. Grenet
LIRMM - Université Montpellier 2
bruno.grenet@lirmm.fr

La représentation *lacunaire* d'un polynôme est la donnée de la liste de ses monômes non nuls. Une caractéristique de cette représentation est d'être de taille logarithmique en le degré du polynôme. Dans l'exemple de la factorisation

$$1 - X^p = (1 - X) \cdot (1 + X + \cdots + X^{p-1}),$$

le polynôme à factoriser est de taille $O(\log p)$ alors que le second facteur est de taille $O(p)$. Ainsi, il est impossible d'obtenir un algorithme polynomial pour factoriser entièrement un polynôme lacunaire.

Une restriction naturelle pour obtenir un algorithme de complexité polynomiale consiste à ne calculer que les facteurs d'un degré fixé. Cela englobe en particulier le cas important du calcul des racines pour un polynôme à une variable. Une lignée de travaux a conduit à des algorithmes polynomiaux pour le calcul des facteurs de degré borné de polynômes à une variable à coefficients dans un corps de nombres [1, 4], étendus ensuite au cas à plusieurs variables [2, 3].

Dans mon exposé, je présenterai un nouvel algorithme permettant de calculer les facteurs de degré au plus d d'un polynôme lacunaire à plusieurs variables à coefficients dans un corps de nombres, en temps polynomial en la taille du polynôme et en d. Cet algorithme, plus simple et pratique que celui proposé par Kaltofen et Koiran [3], est une réduction du problème au cas de polynômes à une variable d'une part, et au cas de polynômes de petit degré d'autre part. La réduction étant valable pour tout corps de caractéristique 0, l'algorithme permet également de calculer certains facteurs pour des polynômes à coefficients dans d'autres corps, comme les réels ou ou les p-adiques. Les facteurs manquants sont ceux qui peuvent d'écrire $f(X_1^{\alpha_1} \cdots X_n^{\alpha_n})$ où f est un polynôme à une variable et α_1, …, α_n sont des entiers.

La preuve de correction de l'algorithme est basée sur le polygone de Newton et le développement en série de Puiseux du polynôme. En particulier,

elle fait appel à une borne sur la valuation d'une expression de la forme $g(X, \phi(X))$ où g est un polynôme de petit degré et ϕ une série de Puiseux.

Je présenterai également une implantation de cet algorithme qui est en cours dans le logiciel libre `Mathemagix`.

Références

[1] F. Cucker, P. Koiran, and S. Smale. A polynomial time algorithm for Diophantine equations in one variable. *J. Symb. Comput.*, 27(1) :21–30, 1999.

[2] E. Kaltofen and P. Koiran. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In *Proc. ISSAC'05*, pages 208–215. ACM, 2005.

[3] E. Kaltofen and P. Koiran. Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields. In *Proc. ISSAC'06*, pages 162–168. ACM, 2006.

[4] H. Lenstra Jr. On the factorization of lacunary polynomials. In *Number theory in progress*, pages 277–291. De Gruyter, 1999.