Algorithmes élémentaires pour la factorisation des polynômes lacunaires à deux variables

Bruno Grenet *

La représentation lacunaire, ou supercreuse, d'un polynôme multivarié

$$P(X_1, \dots, X_n) = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$

est la donnée de la liste

$$\Big\{(\alpha_{1,1}, \dots, \alpha_{n,1}) : a_1, \dots, (\alpha_{1,k}, \dots, \alpha_{n,k}) : a_k\Big\}.$$

Cette représentation très compacte est adaptée pour des polynômes ayant très peu de monômes par rapport à leur degré. En particulier, le degré d'un polynôme représenté sous forme lacunaire peut être exponentiel en la taille de sa représentation.

On s'intéresse ici au calcul des facteurs irréductibles d'un polynôme donné sous forme lacunaire. L'exemple de la factorisation du polynôme $X^d - 1 = (X-1)(1 + X + \cdots + X^{d-1})$ montre qu'on ne peut calculer tous les facteurs d'un polynôme lacunaire en temps polynomial : alors que la taille de la représentation lacunaire de $X^d - 1$ est de l'ordre de $\log(d)$, la taille de la représentation du second facteur est de l'ordre de d. Ainsi, on doit se restreindre à certains facteurs en fixant une borne sur le degré des facteurs calculés.

La factorisation des polynômes lacunaires a été étudiée dans une série d'articles par Cucker, Koiran et Smale (J. Symb. Comput., 1999), Lenstra (Number Theory in Progress, 1999), et Kaltofen et Koiran (ISSAC 2005 & 2006). Les algorithmes proposés calculent les facteurs de *petit degré* d'un

*LIP (ÉNS Lyon) & IRMAR (U. Rennes 1)

polynôme lacunaire à coefficients dans un corps de nombre. Ces résultats utilisent des techniques non élémentaires issues de la théorie des nombres.

Dans ce travail, nous cherchons à donner des preuves plus élémentaires de ces résultats. Nous nous concentrons sur les résultats de Kaltofen et Koiran concernant les facteurs linéaires des polynômes lacunaires à deux variables. En particulier, nous donnons un algorithme élémentaire de complexité polynomiale pour le calcul des facteurs multilinéaires de polynômes à deux variables et à coefficients dans un corps de nombre. La simplification obtenue nous permet également de donner des résultats similaires en caractéristique positive.

Notre principal outil technique est un borne supérieure sur la valuation de polynômes de la forme $P(X, 1 + X)$ où P est un polynôme lacunaire à deux variables, qui peut être vue comme une généralisation d'un résultat de Hajós.

L'exposé est basé sur un article co-écrit avec Arkadev Chattopdhyay, Pascal Koiran, Natacha Portier et Yann Strozecki, qui sera présenté à la conférence ISSAC 2013.