

Factorisation des polynômes bivariés en temps polynomial en le volume du polytope de Newton

Martin Weimann

Séminaire Théorie des Nombres

CAEN, 20 Janvier 2012.

Il existe aujourd'hui des algorithmes de factorisation bivariée de complexité quasi-optimale en le degré total. Cependant, quand le polynôme a peu de monômes, le degré est un indicateur de complexité peu significatif et il est préférable de considérer le polytope de Newton. Je prouve ici l'existence d'un algorithme déterministe qui, donné $f \in \mathbb{Q}[x, y]$ non dégénéré, et donnée la factorisation univariée de certains polynômes de facettes, factorise f sur \mathbb{Q} en temps polynomial en le volume du polytope. Quand le polynôme est suffisamment creux, cet algorithme améliore considérablement les algorithmes denses les plus rapides (Chèze-Lecerf, Gao, Belabas-Van Hoeij-etc). La stratégie est de décomposer la courbe définie par f dans une compactification torique adéquate du plan affine *via* un théorème d'extension des fibrés en droite.

Références

- M. Weimann, *Algebraic osculation and factorization of sparse polynomials*, Foundation of Computational Mathematics (FoCM), à paraître.
- M. Weimann, *A lifting and recombination algorithm for rational factorization of sparse polynomials*, Journal of Complexity, Vol. 26, no. 6 (2010), pp. 608-628.