Factorization of multivariate lacunary polynomials

Martín Avendaño[a]

[a]Departamento de Matemáticas, Universidad de Buenos Aires, Argentina

We present an algorithm that computes all the irreducible factors (with their corresponding multiplicities) of degree bounded by an a priori fixed number d of a given multivariate polynomial f with coefficients in a number field in polynomial time in the "lacunary" size of f and in d. The algorithm also computes the absolute factors of f (up to degree d) having at least three terms within the same time.

The interest of the result is that the lacunary size of a polynomial depends linearly on its number of non-zero terms, on the bit-size of its largest coefficient and on the logarithm of its degree. This can be substantially smaller than the "dense" size.

The strategy used here was introduced by F.Cucker, P.Koiran and S.Smale for finding the integer roots of univariate polynomials with integer coefficients, and first generalized by H.W.Lenstra for finding the low degree factors of univariate polynomials. It is also related to the work of P.Koiran and E. Kaltofen on the subject.

This is joint work with Teresa Krick and Martín Sombra.