Fast Gröbner basis computation and polynomial reduction for generic bivariate ideals

Robin Larrieu* and Joris Van Der Hoeven[1]

[1]INSMI (CNRS) – Centre national de la recherche scientifique - CNRS (France) – France

Résumé

Let A, B ∈ K[X, Y] be two bivariate polynomials over an effective field K, and let G be the reduced Gröbner basis of the ideal I := (A, B) generated by A and B, with respect to the usual degree lexicographic order. Assuming A and B sufficiently generic, we design a quasi-optimal algorithm for the reduction of P ∈ K[X, Y] modulo G, where "quasi-optimal" is meant in terms of the size of the input A, B, P . Immediate applications are an ideal membership test and a multiplication algorithm for the quotient algebra A := K[X, Y] / (A, B), both in quasi-linear time. Moreover, we show that G itself can be computed in quasi-linear time with respect to the output size.

*Intervenant