Fast Gröbner basis computation and polynomial reduction for generic bivariate ideals

Joris van der Hoeven   Robin Larrieu

Let $A, B \in \mathbb{K}[X, Y]$ be two bivariate polynomials over an effective field $\mathbb{K}$, and let G be the reduced Gröbner basis of the ideal $I := \langle A, B \rangle$ 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 $P \in \mathbb{K}[X, Y]$ 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 $\mathbb{A} := \mathbb{K}[X, Y]/\langle A, B \rangle$, both in quasi-linear time. Moreover, we show that G itself can be computed in quasi-linear time with respect to the output size.

Idea of the algorithm Observe that the major obstruction to quasi-linear reduction algorithms is that the equation

$$P = Q_0 G_0 + Q_1 G_1 + \cdots + Q_n G_n + R \tag{1}$$

is much larger than the input P, A, B : if A, B have degree n, the input takes $\Theta(n^2)$ space, but writing down $G_0, \ldots, G_n$ explicitly requires already $\Theta(n^3)$.

In the generic bivariate setting, we are able to solve this issue by designing a *concise representation* for G that holds all relevant information within $\tilde{O}(n^2)$ space. This representation is based on the following ingredients :

- The reduction is done in such a way that the degrees of the quotients are strictly controlled : most quotients will have a very small degree. We named this ingredient the *dichotomic selection strategy.*
- We reduce modulo a *truncated basis* $G^\#$ where $G_i^\#$ contains only the head terms of G_i. This allows to reduce the size of equation (1) to evaluate it faster.
- We perform *substitutions* in equation (1) during the computation to increase the precision, so that the final result is correct (i.e. it is the reduction modulo G and not $G^\#$).

It is then possible to adapt the fast reduction algorithm from [1] to exploit the concise representation and achieve reduction in $\tilde{O}(n^2)$ time.

Références

[1] Joris van der Hoeven. On the complexity of polynomial reduction. *Proc. Applications of Computer Algebra 2015* pages 447–458. Cham, 2015.

[2] Joris van der Hoeven and Robin Larrieu. Fast Gröbner basis computation and polynomial reduction for generic bivariate ideals. Technical Report, HAL, 2018. `http://hal.archives-ouvertes.fr/hal-01770408`.