Signature Gröbner Bases in the Free Algebra

Clemens Hofstadler   Thibaut Verron

Gröbner bases are a fundamental tool for solving systems of polynomial equations, and performing arithmetic operations on ideals. The most recent generation of algorithms computing Gröbner bases are computing bases with so-called signatures. Those signatures have proved to be useful far beyond their initial purpose of eliminating reductions to zero : the data of a signature Gröbner basis for a family of polynomials allows to reconstruct a Gröbner basis with certificates (the coordinates in terms of the input polynomials), as well as a Gröbner basis of the module of syzygies.

In the non-commutative case, Gröbner bases are used for proving formulas in abstract algebra : given relations $f_1(\mathbf{x}) = 0, \dots, f_n(\mathbf{x}) = 0, f(\mathbf{x}) = 0$, the question "*does* $f_1(\mathbf{x}) = \cdots = f_n(\mathbf{x}) = 0$ *imply that* $f(\mathbf{x}) = 0$ *?*" is equivalent to asking whether $f \in \langle f_1, \dots, f_n \rangle$, which can be answered with Gröbner bases. A signature Gröbner basis of the ideal, in addition to answering the question, would also give sufficient data to reconstruct a *proof* of the implication.

In this talk, we present signature Gröbner basis algorithms for pure non-commutative polynomials, in the free algebra. A common difficulty with non-commutative Gröbner bases is that the algorithms do not in general terminate. With signatures, we show how signatures allow to work around an obstruction to termination, and we conjecture a characterization of ideals with a finite signature Gröbner basis.