Functional Decomposition

Rosario Rubio
Departamento de Industriales
Universidad Antonio de Nebrija
28040 Madrid, Spain

Extended Abstract

During the last years several results has been obtained on univariate decomposition rational function area. However, multivariate decomposition problem has not been studied so much. The problem to compute a decomposition of a univariate rational function is equivalent to compute a proper intermediate subfield in the univariate rational function field $\mathbb{K}(t)$, see for instance [AGR95, Zip91].

The algorithm in [MS99] finds porper intermediate subfields in the multivariate rational function field $\mathbb{K}(x_1, \ldots, x_n)$; among other many requirements, it needs the computation of the primary decomposition of a polynomial ideal in n variables with coefficients in a unirational field and then to check an exponential number of possible candidates.

In this talk we introduce an alternative algorithm to this method. Basically, it requires the computation of Gröbner bases with respect to tag variable orderings and factorization in algebraic extensions, this last part is equivalent to factor a multivariate polynomial with coefficients in the ground field. This method can also be generalized to finite extensions, not necessarily unirational over $\mathbb{K}$.

Our exponential time algorithm is much more effective, in theory and in practice, than the method in [MS99], see the implementation in Maple [Rub01].

On the other hand, generalizing the concept of univariate rational function decomposable by intermediate field theory, we could say that a multivariate rational function f is decomposable if and only if there exists an intermediate field $\mathbb{F}$ such that $\mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(x_1, \ldots, x_n)$. Generally in science, and particularly in mathematics, the methods for solving general problems usually lack of effectively. It seems natural to impose restrictions to the field $\mathbb{F}$ which offer some uniqueness and finiteness –excluding on the one hand the trivial cases and on the other keeping the interesting problem from different points of view–. In fact, this is, overall, one of the other goal in this talk.

We study three concepts of decomposable rational function: uni–multivariate decomposition, generalization of [Gat90] for polynomials; multi–univariate decomposition, motivated by the behavior of reduced Gröbner bases with respect to the composition of polynomials, see [GRub98]; and the single–variable decomposition, decomposition with respect to one variable and which includes the previous ones. These definitions generalize the notions in [GGR99] for polynomials.

We find out the equivalence with field theory and describe algorithms for computing such decompositions. We also present some interesting properties: there exists a finite number of such non–equivalent decompositions, the components of the decomposition are unique, if a polynomial is decomposable as a rational function, its components are polynomials, ...

References

[AGR95] Alonso, C., Gutierrez, J., Recio, T. *A Rational Function decomposition Algorithm by Near-separated Polynomials*. J. Symbolic Comput. **19**, 527–544 (1995).

[Gat90] von zur Gathen, J. *Functional decomposition of polynomials: the tame case*. J. of Symbolic Computation 9, 281–299 (1990).

[GGR99] von zur Gathen, J., Gutierrez, J., Rubio, R. *On multivariate polynomial decomposition*. Computer algebra in scientific computing—CASC'99 (Munich), 463–478, Springer-Verlag, Berlin (1999).

[GRub98] Gutierrez, J., Rubio, R. *Reduced Gröbner Basis Under Composition*. J. of Symbolic Computation, 26, 433–444 (1998).

[MS99] Müller-Quade, J., Steinwandt, R. *Basic Algorithms for Rational Function Fields*. J. Symbolic Comput. **27**, 143–170 (1999).

[Rub01] Rubio, R. *Unirational fields. Theorems, algorithms and applications* Thesis Dissertation, University of Cantabria, Spain, 2001.

[Zip91] Zippel, R. *Rational Function Decomposition* . Proc. of ISSAC-91. ACM press, 1–6 (1991).