Dynamic Galois Theory and Gröbner Basis

Gema M. Díaz-Toca[1]

Given a separable polynomial $f(T)$ of degree n over a field $\mathbb{K}$, the purpose of this talk is to present algorithms for computing in the splitting field in an exact way but with the minimum effort, that is, without obtaining the splitting field before. This idea is based on the dynamic evaluation method (see [4]).

We first construct the splitting algebra associated to $f(T)$, denoted by $\mathbf{A}_{\mathbb{K},f}$, where $f(T)$ totally splits. Recall that the splitting algebra is defined by the quotient ring $\mathbb{K}[X_1, \ldots, X_n/\mathcal{J}$ where $\mathcal{J}$ is the ideal generated by the symmetric functions on the roots of $f(T)$.

It is well known that a splitting field is given by an ideal generated by a maximal idempotent of $\mathbf{A}_{\mathbb{K},f}$. Nevertheless it is not possible to compute such an idempotent in the general situation. Therefore we consider the splitting algebra as our first dynamic splitting field, denoted by $\mathcal{C}_d$.

If when calculating, we find an element $z \in \mathcal{C}_d$ indicating that $\mathcal{C}_d$ is not really a field, that is, an element z which verifies at least one of these properties

i) z is a zero divisor (T divides $\mathrm{Min}_z(T)$).

ii) $\mathrm{degree}(\mathrm{Min}_z(T)) < \mathrm{degree}(\mathrm{Rv}(T))$,

iii) $\mathrm{Min}_z(T) = R_1\, R_2$, with $\deg(R_1) \geq 1$ and $\deg(R_2) \geq 1$,

we apply our algorithms to calculate a new dynamic splitting field where z will behave in a correct way. This new dynamic field is a better approximation to a representation of the splitting field of $f(T)$. Furthermore joint with the dynamic splitting field, we also compute a dynamic Galois group which is a better approximation to the Galois group of $f(T)$. Thus, in this new $\mathcal{C}_d$ we go on computing and proceed in the same way such that we only define a new dynamic field if it is necessary.

These new dynamic fields are quotient rings defined by Galois ideals whose stabilizers define our dynamic Galois groups. One of the most important properties of Galois ideals is that their Gröbner basis are triangular. This property independently appears in both [1] and [7]. A generalization of this property appears in [5].

Observe that in our work it is crucial the computing of minimal polynomials. In `Magma` (see [3]), it is done with the function `MinimalPolynomial`. On the other hand, an efficient algorithm based on the Berlekamp Massey Algorithm can be found in [2] and [10]. It is also possible to compute it via Gröbner Basis. Let T be a new variable. Given $z \in \mathcal{C}_d$ and the Galois ideal which defines $\mathcal{C}_d$, denoted by $\mathfrak{b}$, the Gröbner basis of the elimination ideal $(\mathfrak{b} + \langle T - z\rangle) \cap \mathbb{K}[T]$ returns the minimal polynomial of z.

However, we can get more information about $\mathcal{C}_d$ from the Gröbner basis of $\mathfrak{b} + \langle T - z\rangle$. Let Gb =GroebnerBasis($\mathfrak{b} + \langle T - z\rangle$) with $T < X_n < \cdots < X_1$. If Gb is not triangular then $\mathcal{C}_d$ is not a field. Suppose that $P(T, X_n, \ldots, X_i)$ is a polynomial in Gb such that its leading coefficient with respect to the variable X_i is another polynomial in $T, X_n, \ldots, X_{i+1}$. Then this polynomial, the leading coefficient, is a zero divisor of $\mathcal{C}_d$ and that allows us to obtain a new dynamic field where z behaves as in a field.

In the talk, we will illustrate these ideas with some examples.

References

[1] Aubry P. and Valibouze A., *Using Galois Ideals for Computing Relative Resolvents.* J. Symbolic Computation, **30**, 635–651 (2000).

[2] Ben Atti N., Diaz-Toca G.M. and Lombardi H., *The Berlekamp-Massey Algorithm revisited.* AAECC **17** 1, 75–82 (2006).

[3] Bosma, W., Cannon, J. and Playoust, C., *The Magma Algebra System I: The User Language.* J. Symbolic Comput **24** no. 3, 235–265. (1997). URL: `magma.maths.usyd.edu.au`

[4] Della Dora J., Dicrescenzo C. and Duval D., *About a new method for computing in algebraic number fields.* In Caviness B.F. (Ed.) EUROCAL '85. Lecture Notes in Computer Science 204, 289–290. Springer (1985).

[5] Diaz-Toca G.M., Lombardi H. and Quitté C., *Universal Decomposition Algebra.* Proceedings of Transgressive Computing 2006, 169-184 (2006).

[6] Ducos L., *Effectivité en théorie de Galois. Sous-résultants.* Universite de Poitiers, Thèse doctorale. Poitiers (1997).

[7] Ducos L., *Construction de corps de décomposition grâce aux facteurs de résolvantes. (French) [Construction of splitting fields in favour of resolvent factors].* Communications in Algebra **28** no. 2, 903–924 (2000).

[8] Ekedahl E. and Laskov D., *Splitting algebras, symmetric functions and Galois Theory.* Journal of Algebra and its Applications, **4** (1), 59–76, (2005).

[9] Pohst M.E. and Zassenhaus H.J., *Algorithmic Algebraic Number Theory.* ISBN 0521596696. Cambridge University Press (1989).

[10] Shoup V.,*A Computational Introduction to Number Theory and Algebra.* Cambridge University Press (2005)

[11] Steel A.,*A New Scheme for Computing with Algebraically Closed Fields.* Lecture Notes In Computer Science **2369**. Proceedings of the 5th International Symposium on Algorithmic Number Theory, 491–505 (2002).

[12] L. Soicher and J. McKay, *Computing Galois groups over the rationals.* J. Number Theory 20, 273–281, (1985).

[13] Valibouze, A., *Modules de Cauchy, polynômes caractéristiques et résolvantes* . Rapport LITP, 95-62, (1995).

[14] Valibouze, A., *Étude des relations algébriques entre les racines d'un polynôme d'une variable* . Bull. Belg. Math. Soc. **6**, 507-535, (1999).

.

[1]Dpto. de Matemática Aplicada
Fac. de Informática, Univ. de Murcia
Campus de Espinardo, 30100 Murcia, (Spain)
`gemadiaz@um.es`