Large Multi-Modular RUR

Jean-Charles Faugère, Fabrice Rouillier

Deliverable 3.3.2.3.2

Contents

1 Introduction

The objective of this task is to implement the Rational Univariate Representation for polynomials with integer coefficients. A generic (not multi-modular) version exists and has been fully integrated in the PoSSo-Library.

Since the Multi-modular version of the RUR shares many tools with the Multi-modular version of FGLM (see report task 3.3.2.2.2) that is not fully implemented, the first implementation we describe in this report works only in the case of Radical ideals for the moment. The algorithms are implemented as *servers* that can be called directly from Aldor through a socket stream interface designed by J.C Faugère, M. Moreno and F. Rouillier so that their early versions can be used for applications.

Also, since the experiments made with an early multi-modular version of FGLM (see report task 3.3.2.2.2) shows that we can now hope to be able to compute very efficiently a decomposition into radical triangular systems (see report 3.5.1.3.1), no more general version of the RUR will be needed for solving zero-dimensional systems with integer coefficients.

The rational Univariate Representation of a zero-dimensional system in n variables is a list $(f, g, g_1, \ldots, g_n)$ of univariate polynomials such that :

- For each complex (resp. real) root β of f of multiplicity m, $(g_1(\beta)/g(\beta), \ldots, g_n(\beta)/g(\beta))$ is a root of the system.
- conversely, for each complex (resp.real) root α of multiplicity m of the system, there exist a root β of f (of multiplicity m) such that $\alpha = (g_1(\beta)/g(\beta), \ldots, g_n(\beta)/g(\beta))$

2 Description

Let K be a field of characteristic 0, C its algebraic closure, $\mathcal{I}$ a zero-dimensional ideal of $K[X_1, \ldots X_n]$ and $\mathcal{I}_C$ the canonical image of $\mathcal{I}$ in $C[X_1, \ldots X_n]$. We denote by $\mathcal{A}_K = K[X_1, \ldots X_n]/\mathcal{I}$ (resp. $\mathcal{A}_C = C[X_1, \ldots X_n]/\mathcal{I}_C = C \otimes \mathcal{A}_K$) the finite-dimensional K-algebra (resp. C-algebra), and by $V_C(\mathcal{I}) \subset C^n$ the zeroes of $\mathcal{I}$ in C^n. The localisation $\mathcal{A}_\alpha$ of $\mathcal{A}_C$ at each element $\alpha \in V_C(\mathcal{I})$ defines a finite-dimensional C-vector space whose dimension is the multiplicity $\mu(\alpha)$ of α.

Definition 1 *A polynomial $t \in K[X_1, \ldots, X_n]$ separates $V_C(\mathcal{I})$, if*

$$\forall \alpha, \beta \in V_C(\mathcal{I}) \; , \alpha \neq \beta \Rightarrow t(\alpha) \neq t(\beta).$$

The existence of such polynomials is obvious. The following lemma shows that separating elements can be chosen in a generic and finite (for a fixed finite algebraic set) set of linear forms :

Lemma 1 *Let V be a finite set in C^n such that $\sharp V = d$. The finite set of linear forms $\mathcal{T} = \{X_1 + iX_2 + \ldots + i^{n-1}X_n \; , \; 0 \leq i \leq (n-1)d(d-1)/2\}$ contains at least one element that separates V.*

Let $M_p^{\mathcal{A}_Q}$ denotes the multiplication matrix by any polynomial $p \in \mathbb{Q}[X_1, \ldots, X_n]$ in $\mathcal{A}_Q = \mathbb{Q}[\mathbb{X}_\mathbb{1}, \ldots, \mathbb{X}_\mathbb{n}]/\langle \mathcal{G} \rangle$ (resp. $\mathcal{A}_{GF(p)}$) w.r.t. the canonical monomial basis associated to any Groebner basis $\mathcal{G}$. **Definition :** $t \in K[X_1, \ldots X_n]$, χ_t the characteristic polynomial of $m_t^{\mathcal{A}_K}$ and $\overline{\chi_t}$ its square-free part.

For all $v \in K[X_1, \dots, X_n]$, we define:

$$g_t(v,T) = \sum_{\alpha \in V_C(\mathcal{I})} \mu(\alpha) v(\alpha) \prod_{y \neq t(\alpha), y \in V_C(\chi_t)} (T - y).$$

If t separates $V_C(\mathcal{I})$, the **Rational Univariate Representation** of $\mathcal{I}$ associated to t is the $n+2$-uple :

$$\{\chi_t, g_t(1,T), g_t(X_1,T), \dots, g_t(X_n,T)\}$$

Remark : According to Stickelberger's theorem, $\chi_t(T) = \prod_{\alpha \in V_C(\mathcal{I})} (T - t(\alpha))^{\mu(\alpha)}$.

Proposition : If t separates $V_C(\mathcal{I})$,

- the roots of χ_t are exactly the scalars $t(\alpha)$, $\alpha \in V_C(\mathcal{I})$ with multiplicity $\mu(\alpha)$.
- $v(\alpha) = \frac{g_t(t(\alpha))}{\chi_t(t(\alpha)}$

Consequence : the map :

$$\begin{array}{rccc} \psi_t : & V_C(\chi_t) & \longrightarrow & V_C(\mathcal{I}) \\ & \beta & \longmapsto & \left(\frac{g_t(X_1,\beta)}{g_t(1,\beta)}, \dots, \frac{g_t(X_n,\beta)}{g_t(1,\beta)} \right) \end{array}$$

is a bijection that preserves :

- the multiplicities
- the real roots

The RUR provides an "equivalent" system :

$$\begin{cases} \chi_t(T) = 0 \\ X_{n-1} = \frac{g_{n-1}(T)}{g_t(T)} \\ \vdots \\ X_1 = \frac{g_1(T)}{g_t(T)} \end{cases}$$

In the shape Lemma case, X_n is a separating element and one can switch easily from the RUR to the lexicographic Groebner Basis :

$$RUR : \begin{cases} \chi_t(X_n) = 0 \\ g(X_n)X_{n-1} - g_{n-1}(X_n) = 0 \\ \vdots \\ g(X_n)X_1 - g_1(X_n) = 0 \end{cases}$$

$$LexBasis : \begin{cases} f_n(X_n) = 0 \\ X_{n-1} - f_{n-1}(X_n) = 0 \\ \vdots \\ X_1 - f_1(X_n) = 0 \end{cases}$$

In fact :

- $\chi_t(X_n) = f_n(X_n)$
- $f_i(X_n)g(X_n) = g_i(X_n)$ *modulo* $\chi_t(X_n)$

In the case of radical systems, the difference betwin the algorithm that compute a RUR and the algorithm that compute a lexicographic Groebner basis, in the case of a radical ideal, through the FGLM strategy is the computation of a separating element (a linear form that induces a injection betwin the set of zeroes of the initial system and $\mathbb{C}$) : Once such an element is known, one perform the linear substitution of variables : $X_n -> t(X_1, \ldots, X_n)$ such that the new system is in the shape lemma form.

The situation is obviously similar in the case of multi-modular computations. Once a separating element is known, one can run the algorithm described in report task 3.3.2.2.2 to compute the RUR. As we will see, the verification test can be optimised.

2.1 Separating elements and modular computations

Given any prime number p, $\mathbb{Z}_p$ will denote the localisation of $\mathbb{Q}$ at p, $GF(p)$ the finite field with p elements and $\overline{GF(p)}$ its algebraic closure.

Many basic results used for the computation of a Rational Univariate Representation are working in $GF(p)$ for p sufficiently large. For example, lemma 1 becomes obviously :

Lemma 2 *Let V_p be a finite set in $\overline{GF(p)}^n$ such that $\sharp V_p = d$. If $(n-1)d(d-1)/2 < p$, the finite set of linear forms $\mathcal{T} = \{X_1 + iX_2 + \ldots + i^{n-1}X_n\ ,\ 0 \leq i \leq (n-1)d(d-1)/2\}$ contains at least one element that separates V_p.*

Our goal is to study the link betwin the results obtained by the generic algorithms (working with rational coefficients) and those obtained by computing with coefficients in $GF(p)$.

Let ϕ_p be the canonical morphism from Z_p to $GF(p)$. Let $\mathcal{G}$ be a Groebner basis of a zero-dimensional ideal $\mathcal{I} \subset \mathbb{Q}[\mathbb{X}_1, \ldots, \mathbb{X}_n]$.

Definition 2 *A prime number p is said to be $\mathcal{G}$-compatible if $\mathcal{G} \subset \mathbb{Z}_p[\mathbb{X}_1, \ldots, \mathbb{X}_n]$.*

Even if p is a $\mathcal{G}$-compatible prime, $\phi_p(\mathcal{G})$ is not, in general, a Groebner basis of $\phi_p(\mathcal{I})$, but we have the following property (see [1] or [2]) :

Theorem 1 *Let $\mathcal{G}$ be a Groebner basis of a zero-dimensional ideal $\mathcal{I} \subset \mathbb{Q}[\mathbb{X}_1, \ldots, \mathbb{X}_n]$ for a given admissible monomial ordering $<$. If p is a $\mathcal{G}$-compatible prime then $\phi_p(\mathcal{G})$ is the Groebner basis for $<$ of any zero-dimensional ideal $\mathcal{I}_p \subset GF(p)[X_1, \ldots, X_n]$. Moreover, if $NF(f, \mathcal{G})$ denotes the canonical reduction of any polynomial p modulus a Groebner basis $\mathcal{G}$ (normal form) then $\forall f \in \mathbb{Z}_p[\mathbb{X}_1, \ldots, \mathbb{X}_n]$, $\phi_p(NF(f, \mathcal{G})) = NF(\phi_p(f), \phi_p(\mathcal{G}))$.*

This theorem has direct consequences :

Corollary 1 *Let $\mathcal{G}$ be a Groebner basis of a zero-dimensional ideal $\mathcal{I} \subset \mathbb{Q}[\mathbb{X}_1, \ldots, \mathbb{X}_n]$ and p a $\mathcal{G}$-compatible prime number. Then :*

- *$Dim_{GF(p)}(\mathcal{A}_{GF(p)}) = Dim_{\mathbb{Q}}(\mathcal{A}_Q)$, where $\mathcal{A}_Q = Q[X_1, \ldots, X_n]/\langle \mathcal{G} \rangle$ and $\mathcal{A}_{GF(p)} = GF(p)[X_1, \ldots, X_n]/\langle \phi_p($ Moreover, if $\mathcal{B}$ is the canonical monomial basis associated to $\mathcal{G}$ (down-stair monomial basis) then $\mathcal{B}$ is also the monomial basis associated to $\phi_p(\mathcal{G})$.*

- *If M_p (resp. M_{ϕ_p}) denotes the multiplication matrix by any polynomial $p \in \mathbb{Z}[X_1, \ldots, X_n]$ in $\mathcal{A}_Q$ (resp. $\mathcal{A}_{GF(p)}$) w.r.t. the canonical monomial basis associated to $\mathcal{G}$, then we have :*

$$\phi_p(M_p) = M_{\phi_p},$$

  and also :

  - $\phi_p(Trace(M_p)) = Trace(M_{\phi_p})$,
  - $\phi_p(Det(M_p)) = Det(M_{\phi_p})$,
  - *and if χ_p (resp. $\chi_{\phi(p)}$ denotes the characteristic polynomial (monic) of M_p (resp. $\phi(p)$) then :*

$$\phi_p(\chi_p) = \chi_{\phi(p)}.$$

Coming back to the problem of the computation of a separating element of $V_C(\mathcal{I})$ on can establish the following result :

Proposition 1 *Let $\mathcal{I} \subset \mathbb{Q}[X_1, \ldots, X_n]$ a zero-dimensional ideal, $\mathcal{G}$ any Groebner basis of $\mathcal{I}$. If p is a $\mathcal{G}$-compatible prime number greater than $nD(D-1)/2$ (D is the dimension of $\mathcal{A}_{\mathbb{Q}}$), then :*

- $\sharp V_C(\mathcal{G}) \geq \sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$
- *moreover, if $\sharp V_C(\mathcal{G}) = \sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$, then every polynomial $t \in \mathbb{Z}[X_1, \ldots, X_n]$ so that $\phi_p(t)$ separates $V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$ separates $V_C(\mathcal{G})$.*

We have to study the $\mathcal{G}$-compatible prime numbers such that $\sharp V_{\mathbb{C}}(\mathcal{G}) = \sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$, in order to use the proposition 2 for the modular computation of an element that separates $\sharp V_{\mathbb{C}}(\mathcal{G})$. For computing $\sharp V_{\mathbb{C}}(\mathcal{G})$ or $\sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$, one have to compute, for example the rank of Hermite's quadratic form associated to 1.

According to [], if Q_1 denotes the Hermite's quadratic form associated to 1, it can be written in the form :

$$\sum_{i=1}^{D} D_i X_i^2$$

where D_i are minors extracted from the matrix of Q_1 w.r.t. any basis of $\mathcal{A}_Q$. Also the *bad prime numbers* for the computation of any separating element are the primes that divide the D_i. Moreover, if t denotes the size of the coefficients that appear in the matrix of Q_1, and if D is the dimension of the algebra, the size of the D_i is in $O(Dt)$ (this gives also a bound for the number of bad primes).

2.2 The multi-modular Algorithm

In the particular case of radical ideals, the joint determination of *good* primes and *separating elements* can be done using the following result.

Proposition 2 *if $\mathcal{I}$ is radical, an element t is separating if and only if the characteristic polynomial of $\mathcal{M}_t$ is square-free.*

Like after the multi-modular computation in FGLM algorithm, the result have to be checked. In our case we can show that it is sufficient to replace the variables in the original system by the coordinates functions we have computed. We thus obtain n univariate polynomials in one variable whose image modulus $\{\chi_t$ must be null.

The proposed algorithm for the multi-modular computation is the following :

Algorithm Compute-RUR

- **Input :** $MTX(\mathcal{B})$: all the reduced values of $X_i\omega_j$ modulo a Groebner Basis $\mathcal{G}$. Les D be the dimension of the finite algebra.
- [1] Choose a prime number p $\mathcal{G}$-compatible,
- [2] Choose $t \in \mathcal{T} = \{X_1 + iX_2 + \ldots + i^{n-1}X_n \ , \ 0 \leq i \leq (n-1)D(D-1)/2\}$,
- [3] if no more elements in $\mathcal{T}$, goto [1],
- [4] Compute $\chi_{\phi_p(t)}$,
- [5] if $degree(\overline{\chi_{\phi_p(t)}}) \neq D$ then goto [2].
- [6] substitute $t(X_1, \ldots, X_n)$ to X_n.
- [7] Compute $\{\chi_{X_n}, g_{X_n}(1, X_n), g_{X_n}(X_1, X_n), \ldots, g_{X_n}(X_{n-1}, X_n)\}$ using the Multi-modular FGLM algorithm.
- [8] Check the result by substituting X_i by $g_{X_n}(X_i, X_n)/g_{X_n}(1, X_n)$ in the initial equations and verify that the corresponding rational fractions are null modulo χ_{X_n}.
- **Output :** $\{\chi_t, g_1(1, T), g_t(X_1, T), \ldots, g_t(X_n, T)\}$.

References

[1] H.G. Graebe, *On Lucky Primes*, J. Symbolic Computation, 15 199-109, 1993

[2] C. Traverso, *Gröbner trace algorithms*, ISSAC '88, Roma, Ed.P. Gianni, Lect. Notes in Comp.Sc, 8, 125–138 , 1988.