AAECC **9**, 433–461 (1999)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing

Solving Zero-Dimensional Systems Through the Rational Univariate Representation

Fabrice Rouillier*

Loria, Inria-Lorraine, 615, rue du Jardin Botanique, B.P. 101, F-54602, Villers-lès-Nancy, France

Received: January 16, 1996; revised version: March 13, 1998

Abstract. This paper is devoted to the *resolution* of zero-dimensional systems in $K[X_1, \ldots X_n]$, where K is a field of characteristic zero (or strictly positive under some conditions). We follow the definition used in [19] and basically due to Kronecker for solving zero-dimensional systems: *A system is solved if each root is represented in such way as to allow the performance of any arithmetical operations over the arithmetical expressions of its coordinates.* We propose new definitions for solving zero-dimensional systems in this sense by introducing the *Univariate Representation* of their roots. We show by this way that the solutions of any zero-dimensional system of polynomials can be expressed through a special kind of univariate representation (*Rational Univariate Representation*):

RUR

$$\left\{ f(T) = 0\ ,\ X_1 = \frac{g_1(T)}{g(T)}\ ,\ \ldots\ ,\ X_n = \frac{g_n(T)}{g(T)} \right\}$$

where $(f, g, g_1, \ldots, g_n)$ are polynomials of $K[X_1, \ldots, X_n]$. A special feature of our Rational Univariate Representation is that we don't lo~~o~~se geometrical information contained in the initial system.

Moreover we propose different efficient algorithms for the computation of the *Rational Univariate Representation*, and we make a comparison with standard known tools.

Keywords: Resolution of polynomial systems, Elimination of variables, Real roots

* Supported partially by the EEC LTR FRISCO 21.024 project

1 Introduction

This paper is devoted to the *resolution* of zero-dimensional systems in $K[X_1, \dots, X_n]$, where K is a field of characteristic zero (or strictly positive under some conditions).

Given any zero dimensional ideal $\mathscr{I} \subset K[X_1, \dots, X_n]$, an Univariate Representation of the roots of $\mathscr{I}$ consists in expressing all the coordinates of the roots as functions of the roots of an univariate polynomial.

When the considered ideal $\mathscr{I}$ is radical, the algebra $\mathscr{A}_K(\mathscr{I}) = K[X_1, \dots, X_n]/\mathscr{I}$ is cyclic and a solution can simply be obtained by computing a primitive element $t \in \mathscr{A}_K(\mathscr{I})$ (see for example [3] or [13]). In practice, this can be easily done by computing, for example, a lexicographic Gröbner basis after a linear change of coordinates, putting the system in generic position.

For the general case, it is in principle possible to compute $\sqrt{\mathscr{I}}$ and proceed as before. In practice, computing $\sqrt{\mathscr{I}}$ is a difficult task (even if a Gröbner basis of $\mathscr{I}$ is known). Moreover, geometric information is lost, for example, the multiplicities of the roots.

Other approaches give the coordinates of the solutions as rational functions at the zeroes of an univariate polynomial. In [5], for the complete intersection case, the computation is done with an u-resultant, through a deformation of the initial system (adding one variable). A similar method can be found in [23], using an infinitesimal arithmetic. Another solution is proposed in [1], starting from a Gröbner basis for any admissible monomial ordering, and valid in all the cases, without any deformation. The representation depends on the multiplicities of the solutions.

The main subject of this paper is to present a new, full and efficient (in practice) algorithm for reducing zero-dimensional polynomial systems to the study of one single univariate polynomial. As above, the coordinates of the solutions of the original system will be rational functions at the zeroes of an univariate polynomial, and the representation will be independent of the multiplicities of the solutions.

After recalling some basic definitions and tools for the study of zero-dimensional systems (Section 1), we first introduce (Section 2) a general definition of univariate representations of zero-dimensional ideals defined by an univariate polynomial with coefficients in $K[T]$ (K is the ground field) such that there exists a bijection between the roots of p (in the algebraic closure of K) and those of the considered ideal. Moreover, we show that this bijection preserves the multiplicities and, when K is ordered, the real roots.

In the second part of Section 2, we define a special kind of univariate representation: the Rational Univariate Representation (RUR) which allows to represent the solutions of any zero-dimensional system of $K[X_1, \dots, X_n]$ in the following way:

$$\begin{aligned} f(T) &= 0 \\ X_1 &= \tfrac{g_1(T)}{g(T)} \\ &\vdots \\ X_n &= \tfrac{g_n(T)}{g(T)} \end{aligned}$$

where $(f, g, g_1, \ldots, g_n)$ are polynomials of $K[X_1, \ldots, X_n]$.

In Section 3 we give a generic algorithm that computes the Rational Univariate Representation in polynomial time from the multiplication tensor of the associated quotient algebra $\mathscr{A}_K(\mathscr{I})$ and we compute precisely its complexity.

In Section 4, some direct applications of the Rational Univariate Representation are studied:

- the link between lexicographic Gröbner basis and Rational Univariate Representation in the shape lemma case (comparisons in terms of computation times and memory allocation will be made), which induces also an algorithm for the computation of the lexicographic Gröbner basis of the radical,
- algorithms for the decomposition of the Rational Univariate Representation including:
  - the primary decomposition of the ideal,
  - the computation of the multiplicities of the roots.

In Section 5, we study the special case of systems with integer coefficients. In particular we will see how to use a modular arithmetic for optimizing the algorithm.

2 Preliminaries

Most of the results presented in this part can be found in [15] and [16] or in the original articles that are mentioned in the text.

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

Since $\mathscr{A}_K(\mathscr{I})$ is a finite dimensional K-vector space, it makes sense to use linear algebra in algorithms for solving zero-dimensional systems. One main result is Stickelberger's theorem:

Theorem 2.1 (*Stickelberger's theorem*) *Let $\mathcal{I} \subset K[X_1, \ldots, X_n]$ a zero-dimensional ideal. For all $h \in K[X_1, \ldots, X_n]$, we denote by $m_h^{\mathcal{A}_K(\mathcal{I})}$ (simply m_h when no confusion is possible) the K-linear map*:

$$\begin{array}{rccc} m_h^{\mathcal{A}_K(\mathcal{I})} : & \mathcal{A}_K(\mathcal{I}) & \longrightarrow & \mathcal{A}_K(\mathcal{I}) \\ & \overline{f} & \longmapsto & \overline{hf} \end{array}$$

where $\overline{p}$ denotes the class in $\mathcal{A}_K(\mathcal{I})$ of any polynomial $p \in K[X_1, \ldots, X_n]$.

The eigenvalues of $m_h^{\mathcal{A}_K(\mathcal{I})}$ are exactly the scalars $h(\alpha)$, $\alpha \in V_C(\mathcal{I}) \subset C^n$, with respective multiplicities $\sum_{\beta \in V_C(\mathcal{I}), h(\beta)=h(\alpha)} \mu(\beta)$.

This theorem has many consequences. Among them the most useful in our case will be:

- $Det\left(m_h^{\mathcal{A}_K(\mathcal{I})}\right) = \prod_{\alpha \in V_C(\mathcal{I})} h(\alpha)^{\mu(\alpha)}$,
- $\text{Trace}\left(m_h^{\mathcal{A}_K(\mathcal{I})}\right) = \sum_{\alpha \in V_C(\mathcal{I})} \mu(\alpha) h(\alpha)$
- the characteristic polynomial of $m_h^{\mathcal{A}_K(\mathcal{I})}$ is (if it is supposed to be monic): $\prod_{\alpha \in V_C(\mathcal{I})} (T - h(\alpha))^{\mu(\alpha)}$.

As an application of this theorem, we can compute the number of distinct complex roots of a polynomial system:

Theorem 2.2 *Let $\mathcal{I}$ be a zero-dimensional ideal and h a polynomial in $K[X_1, \ldots, X_n]$. The Hermite's quadratic form associated to h, defined by*

$$\begin{array}{rccc} q_h^{\mathcal{A}_K(\mathcal{I})} : & \mathcal{A}_K(\mathcal{I}) & \longrightarrow & K \\ & f & \longmapsto & Trace(m_{\overline{hf^2}}^{\mathcal{A}_K(\mathcal{I})}) \end{array}$$

verifies:

$$\sigma(q_h^{\mathcal{A}_K(\mathcal{I})}) = \sharp\{\alpha \in V_C(\mathcal{I}) | h(\alpha) \neq 0\}$$

where $\sigma(q_h^{\mathcal{A}_K(\mathcal{I})})$ denotes the rank of $q_h^{\mathcal{A}_K(\mathcal{I})}$.

Different proofs of this result can be found in (see for example [21, 3, 22]), but we propose here a proof introducing the notion of separating element considered by several authors for different purposes (see [5, 18, 23, 13, 12, 17, 1]), and frequently used in the rest of this paper.

Definition 2.1 *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, given a set of points $V \subset C^n$, we can compute explicitly a finite set of linear forms that contains at least an element that separates V:

Lemma 2.1 *Let V be a finite set in C^n such that $\sharp V = d$. The finite set of linear forms $\mathcal{T} = \{u_i = X_1 + iX_2 + \ldots + i^{n-1}X_n,\ 0 \leq i \leq (n-1)d(d-1)/2\}$ contains at least one element that separates V.*

Proof. Let $u_i(X_1, \ldots, X_n) = X_1 + iX_2 + \ldots + i^{n-1}X_n$ and suppose that $(x, y) = ((x_1, \ldots, x_n), (y_1, \ldots, y_n))$ is a pair of distinct points of V. Since the polynomial $\sum_{j=1}^{n}(x_j - y_j)T^{i-1}$ has at most $n-1$ distinct roots (it is not identically null since $x \neq y$), the set $\{u_0, \ldots, u_{n-1}\}$ contains at least one element u_k such that $u_k(x) \neq u_k(y)$. Since the number of distinct pairs of points in V is $d(d-1)/2$, the set of polynomials $\{X_1 + iX_2 + \ldots + i^{n-1}X_n\ ,\ 0 \leq i \leq (n-1)d(d-1)/2\}$ contains at least one element that separates V. ■

The separating elements have properties which are useful for the study of algebras like $K[X_1, \ldots, X_n]/\mathcal{I}$. In particular:

Lemma 2.2 *Let $\mathcal{I} \subset K[X_1, \ldots, X_n]$ a zero-dimensional ideal and $t \subset K[X_1, \ldots, X_n]$ a polynomial that separates $V_C(\mathcal{I})$. If we denote $d = \sharp V_C(\mathcal{I})$, then $\{1, t, \ldots, t^{d-1}\}$ is a K-linear independent set of $K[X_1, \ldots, X_n]/\mathcal{I}$.*

Proof. Let $a_0, \ldots, a_{d-1}$ be scalars ($\in K$) such that $g(t) = \sum_{i=0}^{d-1} a_i t^i = 0\ mod\ \mathcal{I}$. For all $\alpha \in V(\mathcal{I})$, $t(\alpha)$ is a root of $g(T) = \sum_{i=0}^{d-1} a_i T^i$. Since t separates $V_C(\mathcal{I})$, the polynomial $g(T)$ has also d roots $(t(\alpha)\ ,\ \alpha \in V_C(\mathcal{I}))$ and is also identically null. Consequently, the set $\{1, t, \ldots, t^{d-1}\}$ is K-linear independent in $K[X_1, \ldots, X_n]/\mathcal{I}$. ■

Proof of theorem 2.2. Let t be a polynomial that separates $V_C(\mathcal{I}) = \{\alpha_1, \ldots, \alpha_d\}$. According to Lemma 2.2, the set $\{1, t, \ldots, t^{d-1}\}$ is K-linear independent in $\mathcal{A}_K(\mathcal{I}) = K[X_1, \ldots, X_n]/\mathcal{I}$. One can find therefore polynomials $\omega_{d+1}, \ldots, \omega_D$ such that $\mathcal{B} = \{\omega_1 = 1, \omega_2 = t, \ldots, \omega_d = t^{d-1}, \omega_{d+1}, \ldots, \omega_D\}$ is a basis of the K-vector space $\mathcal{A}_K(\mathcal{I})$. For a given polynomial $f \in K[X_1, \ldots, X_n]$, let $Y_1, \ldots, Y_D$ denote the coordinates of the class of f in $K[X_1, \ldots, X_n]$, expressed w.r.t. the basis $\mathcal{B}$. According to Theorem 2.1, we have

$$q_h^{\mathcal{A}_K(\mathcal{I})}(f) = \sum_{i=1}^{d} \mu(\alpha_i)h(\alpha_i)\left(\sum_{j=1}^{D} \omega_j(\alpha_i)Y_j\right)^2 .$$

Since $\alpha_1, \ldots, \alpha_d$ are supposed to be distinct elements of C^n and since t separates $V_C(\mathscr{I})$, the matrix

$$\begin{pmatrix} 1 & t(\alpha_1) & \ldots & t(\alpha_1)^{d-1} \\ \vdots & & & \vdots \\ 1 & t(\alpha_d) & \ldots & t(\alpha_d)^{d-1} \end{pmatrix}$$

is a Vandermonde matrix (hence invertible) which is a sub-matrix of the one associated to the linear forms that define the linear change of variables: $Z_i = \sum_{j=1}^{D} \omega_j(\alpha_i) \cdot Y_j, \ i = 1 \ldots d$, which are obviously linearly independent. Consequently, $q_h^{\mathscr{A}_K(\mathscr{I})}(f) = \sum_{i=1}^{d} \mu(\alpha_i) h(\alpha_i) Z_i^2$, and also: $\rho(q_h^{\mathscr{A}_K(\mathscr{I})}) = \sharp\{\alpha \in V(\mathscr{I}) | h(\alpha) \neq 0\}$. ■

3 The Rational Univariate Representation

As we have seen in the previous part, the *trace map* plays an important role in the study of the roots of polynomial systems. In this section, we use it for giving a new definition for the resolution of zero-dimensional systems. We will need to study particular morphisms of algebraic sets. In order to have compact notations, let introduce some definitions:

Definition 3.1 *Let $\mathscr{I} \subset C[X_1, \ldots, X_n]$ and $\mathscr{J} \subset C[Y_1, \ldots, Y_m]$ two ideals, and let $\phi : V_C(\mathscr{I}) \longrightarrow V_C(\mathscr{J})$ a morphism of algebraic sets. We will say that the m-uple $(t_1, \ldots, t_m) \in (K[X_1, \ldots, X_n])^m$ represents ϕ if for any $\alpha \in V_C(\mathscr{I}),\ \phi(\alpha) = (t_1(\alpha), \ldots, t_m(\alpha))$ holds.*

For algorithmic reasons (*see next section*), *most of the morphisms we will have to study will be represented by polynomials with coefficients in K* (*not in its algebraic closure C*). *Such morphisms will be called K-morphisms* (*or K-regular maps*) *of algebraic sets.*

Definition 3.2 *Let $\mathscr{I} \subset K[X_1, \ldots, X_n]$ be a zero-dimensional ideal, $f \in K[T]$ an univariate polynomial and $\phi : V_C(\mathscr{I}) \longrightarrow V_C(f)$ an isomorphism represented by a polynomial $t \in K[T]$. The pair (ϕ, f) is an Univariate Representation of $V_C(\mathscr{I})$ if and only if for any α of $V_C(\mathscr{I}),\ \mu(\alpha) = \mu(\phi(\alpha))$ holds.*

Remark 3.1. Let $\mathscr{I} \subset K[X_1, \ldots, X_n]$ be a zero-dimensional ideal, and suppose that (ϕ, f) is an Univariate Representation of $V_C(\mathscr{I})$. The K-algebras $K[X_1, \ldots, X_n]/\mathscr{I}$ and $K[T]/\langle f \rangle$ are not in general isomorphic.

Let take for example $\mathscr{I} = \langle X_1^2, X_1X_2, X_2^2\rangle$. By defining:

$$\begin{array}{rcl}\phi: V_C(\mathscr{I}) & \longrightarrow & V_C(T^3) \\ (\alpha_1,\alpha_2) & \longmapsto & \alpha_1\end{array},$$

we can easily see that (ϕ, T^3) is an Univariate Representation of $\mathscr{I}$.

Let now suppose that $\psi : K[T]/\langle T^3\rangle \longrightarrow K[X_1, X_2]/\mathscr{I}$ is a morphism of K-algebras and that we have $\psi(\overline{T}) = a\overline{X_1} + b\overline{X_2} + c, a, b, c \in K$. In this case:

$$\psi(\overline{T^2}) = c \cdot \psi(\overline{T}) - c^2,$$

and also psi is not injective.

The following proposition gives a second definition for univariate representations:

Proposition 3.1 *Let $\mathscr{I} \subset K[X_1,\ldots,X_n]$ a zero-dimensional ideal, $f \in K[T]$ an univariate polynomial and $\phi : V_C(\mathscr{I}) \longrightarrow V_C(f)$ a K-isomorphism of algebraic sets (ϕ and ϕ^{-1} are K-regular). The pair (ϕ, f) is said to be a* Univariate Representation *of $V_C(\mathscr{I})$ if there exists a morphism of K-algebras $\Phi^\phi : K[T] \longrightarrow K[X_1,\ldots,X_n]$ such that*

- *$\Phi^\phi(T)$ represents ϕ,*
- *for all $P \in K[T]$, Trace$(m_P^{\mathscr{A}_K(f)})$ = Trace$(m_{\Phi^\phi(P)}^{\mathscr{A}_K(\mathscr{I})})$, where $\mathscr{A}_K(f) = K[T]/\langle f\rangle$ and $\mathscr{A}_{\mathscr{K}}(\mathscr{I}) = K[X_1,\ldots,X_n]/\mathscr{I}$.*

According to the notations of Proposition 3.1, $\Phi^\phi(T)(\alpha) = \phi(\alpha),\ \forall\alpha \in V_C(\mathscr{I})$. Moreover, since Φ^ϕ is a morphism of K-algebras, we have the following result:

Lemma 3.1 *For all $P \in K[T]$, $\Phi^\phi(P)(\alpha) = P(\phi(\alpha))$.*

Proof of Proposition 3.1

- Suppose that (ϕ, f) is an Univariate Representation of $V_C(\mathscr{I})$. Without loss of generality we can suppose that $K = C$ by extending canonically ϕ and Φ^ϕ. Let α be an element of $V_C(f)$. By using Lagrange interpolation, we can construct a polynomial $P_\alpha \in C[T]$ such that $P_\alpha(\alpha) = 1$ and $P_\alpha(\beta) = 0,\ \forall\beta \in V_C(f),\ \beta \neq \alpha$. According to Stickelberger theorem, we have:

$$\text{Trace}\Big(m_{P_\alpha}^{\mathscr{A}_K(f)}\Big) = \sum_{\beta\in V_C(f)} \mu(\beta)P_\alpha(\beta) = \mu(\alpha).$$

  If we suppose that (ϕ, f) is an Univariate Representation of $V_C(\mathscr{I})$, then there exists $\Phi^\phi : C[T] \longrightarrow C[X_1,\ldots,X_n]$ such that:

$$\begin{aligned}\mu(\alpha) = \text{Trace}(m_{\Phi^\phi(P_\alpha)}^{\mathscr{A}_K(\mathscr{I})}) &= \sum_{u\in V_C(\mathscr{I})} \mu(u)\Phi^\phi(P_\alpha)(u) \\ &= \sum_{\beta\in V_C(f)} \mu(\phi^{-1}(\beta))\Phi^\phi(P_\alpha)(\phi^{-1}(\beta)).\end{aligned}$$

Since Φ^ϕ represents ϕ, then, according to Lemma 3.1, $\Phi^\phi(P_\alpha)(\phi^{-1}(\beta)) = P_\alpha(\beta),\ \forall \beta \in V_C(f)$ and

$$\mu(\alpha) = \mathrm{Trace}(m_{\Phi^\phi(P_\alpha)}^{\mathscr{A}_K(\mathscr{I})}) = \mu(\phi^{-1}(\alpha)).$$

- Conversely, let $f \in K[T]$ be an univariate polynomial, $\phi : V_C(\mathscr{I}) \longrightarrow V_C(f)$ an isomorphism of algebraic sets represented by a polynomial $t \in K[X_1, \dots, X_n]$, and let suppose that for any α of $V_C(\mathscr{I})$, we have $\mu(\alpha) = \mu(\phi(\alpha))$. Let $\Phi : K[T] \longrightarrow K[X_1, \dots, X_n]$ be the morphism of K-algebras defined by $\Phi(T) = t$, and P any polynomial in $K[T]$. According to Theorem 2.1 we have: $\mathrm{Trace}(m_P^{\mathscr{A}_K(f)}) = \sum_{\beta \in V_C(f)} \mu(\beta)P(\beta)$. Since $\phi : V_C(\mathscr{I}) \longrightarrow V_C(f)$ is a isomorphism of algebraic sets and $\mathrm{Trace}(m_P^{\mathscr{A}_K(f)}) = \sum_{\alpha \in V_C(\mathscr{I})} \mu(\phi(\alpha))P(\phi(\alpha))$ holds, we deduce from Lemma 3.1, the identity: $\mathrm{Trace}(m_P^{\mathscr{A}_K(f)}) = \sum_{\alpha \in V_C(\mathscr{I})} \mu(\phi(\alpha))\Phi(P)(\phi^{-1}(\phi(\alpha))) = \sum_{\alpha \in V_C(\mathscr{I})} \mu(\phi(\alpha))\Phi(P)(\alpha)$. At last, ϕ preserves the multiplicities, also:

$$\mathrm{Trace}\Big(m_P^{\mathscr{A}_K(f)}\Big) = \sum_{\alpha \in V_C(\mathscr{I})} \mu(\alpha)\Phi(P)(\alpha) = \mathrm{Trace}(m_{\Phi(P)}^{\mathscr{A}_K(\mathscr{I})}).$$

■

In the rest of this section, we will prove that for each zero-dimensional ideal $\mathscr{I} \subset K[X_1, \dots, X_n]$, there exist at least one pair (ϕ, f) that is an Univariate Representation of $V_C(\mathscr{I})$.

According to Proposition 3.1, if a pair (ϕ, f) is a Univariate Representation of $V_C(\mathscr{I})$ then $\Phi^\phi(T)$ represents the isomorphism ϕ. This means in particular that the restriction of $\Phi^\phi(T)$ to $V_C(\mathscr{I})$ is injective and also that $\Phi^\phi(T)$ is separating $V_C(\mathscr{I})$. Moreover:

Proposition 3.2 *Let $\mathscr{I} \subset K[X_1, \dots, X_n]$ be a zero-dimensional ideal and suppose that (ϕ, f) that is an Univariate Representation of $V_C(\mathscr{I})$. Then f is the characteristic polynomial of $m_{\Phi^\phi(T)}^{\mathscr{A}_K(f)}$.*

Proof. Let χ_T (resp. $\chi_{\Phi^\phi(T)}$) be the characteristic polynomial of $m_T^{\mathscr{A}_K(f)}$ $\Big($resp. $m_{\Phi^\phi(T)}^{\mathscr{A}_K(\mathscr{I})}\Big)$. We have obviously $\chi_T = f$ (up to multiplication by a scalar). To show that $\chi_{\Phi^\phi(T)} = \chi_T$, it is sufficient to prove that these two polynomials have the same Newton sums. According to Theorem 2.1, $\chi_{\Phi^\phi(T)}(Y) = \prod_{\alpha \in V_C(\mathscr{I})} (Y - \Phi^\phi(T)(\alpha))^{\mu(\alpha)}$. Also, for $i = 0, \dots, \mathrm{Dim}_K(\mathscr{A}_K(\mathscr{I}))$, the ith Newton sum associated to $\chi_{\Phi^\phi(T)}$ is:

$$N_i(\chi_{\Phi^\phi(T)}) = \sum_{\alpha \in V_C(\mathscr{I})} \mu(\alpha)(\Phi^\phi(T))^i(\alpha) = \mathrm{Trace}(m_{(\Phi^\phi(T))^i}^{\mathscr{A}_K(\mathscr{I})})$$
$$= \mathrm{Trace}(m_{T^i}^{\mathscr{A}_K(f)}) = N_i(\chi_T).$$

Since $\mathrm{Dim}_K(\mathscr{A}_K(\mathscr{I})) = \sum_{\alpha \in V_C(\mathscr{I})} \mu(\alpha) = \sum_{\beta \in V_C(f)} \mu(\beta) = \mathrm{Dim}_K(\mathscr{A}_K(f))$, χ_T and $\chi_{\Phi^\phi(T)}$ have the same degrees. This proves that $\chi_{\Phi^\phi(T)}$ and χ_T have the same Newton sums and also that $\chi_{\Phi^\phi(T)} = \chi_T = f$. ■

According to Stickelberger's theorem, if χ_t denotes the characteristic polynomial of $m_t^{\mathscr{A}_K(\mathscr{I})}$ ($t \in K[X_1, \ldots, X_n]$), we have:

$$\chi_t = \prod_{\alpha \in V_C(\mathscr{I})} (Y - t(\alpha))^{\mu(\alpha)}.$$

In particular, if t is separating $V_C(\mathscr{I})$, the K-regular map

$$\begin{array}{rcl} \phi_t : V_C(\mathscr{I}) & \longrightarrow & V_C(\chi_t) \\ \alpha & \longmapsto & t(\alpha) \end{array}$$

defines a bijection that preserves the multiplicities.

Our goal is now to prove that (ϕ_t, χ_t) is an Univariate Representation by computing explicitly a reciprocal regular map ψ_t, represented by a n-uple of polynomials in $(K[T])^n$.

Definition 3.3 (*Rational Univariate Representation*) *Let $\mathscr{I} \subset K[X_1, \ldots, X_n]$ be a zero- dimensional ideal, t any element in $K[X_1, \ldots, X_n]$ and χ_t the characteristic polynomial of $m_t^{\mathscr{A}_K(\mathscr{I})}$.*
For any $v \in K[X_1, \ldots, X_n]$, we define:

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

*For any $t \in K[X_1, \ldots, X_n]$, the t-*representation *of $\mathscr{I}$ is the $(n+2)$-uple*:

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

If t separates $V_C(\mathscr{I})$, the t-representation of $\mathscr{I}$ is call the Rational Univariate Representation *of $\mathscr{I}$ associated to t.*

Theorem 3.1 *Let $\mathscr{I}$ be a zero-dimensional ideal of $K[X_1, \ldots, X_n]$ and $\{\chi_t, g_t(1, T), g_t(X_1, T), \ldots, g_t(X_n, T)\}$ the t-representation of $\mathscr{I}$. The polynomials defining the t-representation of $\mathscr{I}$ are polynomials of $K[T]$. Moreover, if t separates $V_C(\mathscr{I})$, then*:

- *The application* $\psi_t : V_C(\chi_t) \longrightarrow V_C(\mathscr{I})$ *defined by* $\psi_t(T) = \left(\frac{g_t(X_1,T)}{g_t(1,T)}, \ldots, \frac{g_t(X_n,T)}{g_t(1,T)}\right)$ *is a regular map that can be represented by a* n*-uple of polynomials in* $K[T]$.
- *The pair* (ϕ_t, χ_t), *where* $\phi_t : V_C(\mathscr{I}) \longrightarrow V_C(\chi_t)$ *is the regular map defined by* $\phi_t(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$, *is an Univariate Representation of* $V_C(\mathscr{I})$ *that verifies* $\phi_t^{-1} = \psi_t$.

Proof. If $\overline{\chi}_t$ is the square-free part of χ_t, then: $\overline{\chi}_t(T) = \prod_{y \in V_C(\chi_t)} (T - y)$. Also, for any v of $K[X_1, \ldots, X_n]$, we have:

$$\frac{g_t(v,T)}{\overline{\chi}_t(T)} = \sum_{\alpha \in V_C(\mathscr{I})} \frac{\mu(\alpha)v(\alpha)}{T - t(\alpha)} = \sum_{i \geq 0} \frac{\sum_{\alpha \in V_C(\mathscr{I})} \mu(\alpha)v(\alpha)t(\alpha)^i}{T^{i+1}}$$
$$= \sum_{i \geq 0} \frac{\mathrm{Trace}(m_{vt^i}^{\mathscr{A}_K(\mathscr{I})})}{T^{i+1}}.$$

If $\overline{\chi}_t(T) = \sum_{j=0}^{d} a_j T^{d-j}$, multiplying both sides by $\overline{\chi}_t(T)$ and using that $g_t(v,T)$ is a priori a polynomial in $C[T]$ we have: $g_t(v,T) = \sum_{i=0}^{d-1} \sum_{j=0}^{d-i-1} \mathrm{Trace}(m_{vt^i}^{\mathscr{A}_K(\mathscr{I})}) a_j T^{d-i-j-1}$, and also: $g_t(v,T) = \sum_{i=0}^{d-1} \mathrm{Trace}\ (m_{vt^i}^{\mathscr{A}_K(\mathscr{I})})$ $H_{d-i-1}(T)$, where $H_j(T) = \sum_{i=0}^{j} a_i T^{j-i}$ denotes the j-th Horner's polynomial associated to $\overline{\chi_t}$.

One can notice that $\mu(\beta)v(\beta)\left(\prod_{y \in t(V_C(\mathscr{I}))\setminus\{t(\beta)\}} (t(\alpha) - y)\right)$ vanishes if and only if $\exists y \in t(V_C(\mathscr{I}))\setminus\{t(\beta)\}$ such that $y = t(\alpha)$. Also, $g_t(v, t(\alpha))$ can be written:

$$g_t(v, t(\alpha)) = \left(\sum_{\beta \in V_C(\mathscr{I}), t(\beta)=t(\alpha)} \mu(\beta)v(\beta)\right)\left(\prod_{y \in t(V_C(\mathscr{I}))\setminus\{t(\alpha)\}} (t(\alpha) - y)\right).$$

Using this relation, we have: $\frac{g_t(v, t(\alpha))}{g_t(1, t(\alpha))} = \frac{\sum_{\beta \in V_C(\mathscr{I}), t(\beta)=t(\alpha)} \mu(\beta)v(\beta)}{\sum_{\beta \in V_C(\mathscr{I}), t(\beta)=t(\alpha)} \mu(\beta)}$ and also, if t separates $V_C(\mathscr{I})$, then $\{\beta \in V_C(\mathscr{I}), t(\beta) = t(\alpha)\} = \{\alpha\}$ and $v(\alpha) = \frac{g_t(v, t(\alpha))}{g_t(1, t(\alpha))}$.

The applications ϕ_t and ψ_t are reciprocal by construction. We can see that ϕ_t preserves the multiplicities, so that the only thing we have to prove is that ψ_t is a regular map that can be represented by a n-uple of polynomials in $K[T]$. We can notice that $g_t(1,T) = \chi_t'(T)/\gcd(\chi_t'(T), \chi_t(T))$, so that $g_t(1, T)$ and $\chi_t(T)$ are coprime. This means that there exists a polynomial $U_t(T) \in K[T]$ such that $U_t(T)g_t(1, T) = 1 \mod \chi_t(T)$ and in particular that the regular map $\rho_t : V_C(\chi_t) \longrightarrow V_C(\mathscr{I})$ defined by $\rho_t(T) = (U_t(T)g_t(X_1, T), \ldots, U_t(T)g_t(X_n, T))$ coincides with ϕ_t on $V_C(\chi_t)$. ■

Remark 3.2. According to Proposition 3.2, there is a bijection between the classes of polynomials of $K[X_1, \ldots, X_n]$ that separate $V_C(\mathscr{I})$ and the (rational) univariate representations of $V_C(\mathscr{I})$.

4 A Generic Algorithm

In this section, we present a generic algorithm for computing a Rational Univariate Representation of a given zero-dimensional ideal of $K[X_1, \ldots, X_n]$.

From now, given any polynomial p of $K[X_1, \ldots, X_n]$,

- $\overrightarrow{p}$ will denote the class of p in $\mathscr{A}_K(\mathscr{I})$ with respect to a fixed basis $\mathscr{B}$ of $\mathscr{A}_K(\mathscr{I})$,
- $\overline{p}$ will denote the square-free part of p.

As input, for our algorithm, we consider that the quotient algebra $\mathscr{A}_K(\mathscr{I})$ is determined by:

- A basis $\mathscr{B} = \{\omega_1, \ldots, \omega_D\}$,
- the multiplication matrix M_{X_i} of $m_{X_i} = m_{X_i}^{\mathscr{A}_K(\mathscr{I})}$, $\forall i = 1, \ldots, n$.
- the multiplication tensor of $\mathscr{A}_K(\mathscr{I})$: $MT(\mathscr{A}_K(\mathscr{I})) = \{\overrightarrow{\omega_i\omega_j},\ i = 1, \ldots, n,$ $j = 1, \ldots, n\}$.

According to the results of the precedent part, the two key points of the computation of a Rational Univariate Representation are:

- the choice of a separating element including the computation of its characteristic polynomial,
- the computation of the traces needed for the Rational Univariate Representation (see proof of theorem 3.1) associated to a given separating element.

According to Definitions 2.1 and 3.3, a polynomial t separates $V_C(\mathscr{I})$ if and only if degree$(\overline{\chi_t}) = \sharp V_C(\mathscr{I})$. On the other hand the set $\mathscr{T} = \{X_1 + iX_2 + \ldots + i^{n-1}X_n\ ,\ 0 \le i \le (n-1)d(d-1)/2\}$ contains at least one element that separates $V_C(\mathscr{I})$. Also the basic idea consists in first computing $\sharp V_C(\mathscr{I})$, then choosing any t in $\mathscr{T}$ such that degree$(\overline{\chi_t}) = \sharp V_C(\mathscr{I})$.

Knowing the multiplication table, one way for computing $\sharp V_C(\mathscr{I})$ consists in constructing the quadratic form $q_1 = q_1^{\mathscr{A}_k(\mathscr{I})}$ (see Theorem 2.2) whose rank is equal to $\sharp V_C(\mathscr{I})$. In practice, we can express q_1 with its matrix Q_1 with respect to the basis $\mathscr{B}$: $Q_1[i, j] = \mathrm{Trace}(m_{\omega_i\omega_j}^{\mathscr{A}_K(\mathscr{I})})$. This construction becomes very costly if it is done in a naive way since it is supposed to require the computation of all the vectors in the form $\overrightarrow{\omega_i\omega_j\omega_k},\ \ k, i, j = 1, \ldots, n$. The following Lemma, whose proof is obvious using the linearity of the Trace map, shows that the construction can be done efficiently when knowing the multiplication tensor of $\mathscr{A}_K(\mathscr{I})$:

Lemma 4.1 *For any S of $K[X_1, \ldots, X_n]$, let denote by $Vtr(S)$ the vector of K^n:*

$$Vtr(S) = [Trace(m_{S\omega_1}^{\mathscr{A}_K(\mathscr{I})}), \ldots, Trace(m_{S\omega_D}^{\mathscr{A}_K(\mathscr{I})})].$$

We have, for any S and any R of $K[X_1, \ldots, X_n]$:

$$Trace(m_{RS}^{\mathscr{A}_K(\mathscr{I})}) = \overrightarrow{R} \cdot Vtr(S).$$

In particular, we have: $Q_1[i, j] = \overrightarrow{\omega_i\omega_j}Vtr(1)$.

Algorithm Compute-Q_1

- **Input:** $MT(\mathscr{A}_K(\mathscr{I}))$
- Computation of $Vtr(1)$ using $\mathrm{Trace}(m_{\omega_i}^{\mathscr{A}_K(\mathscr{I})}) = \sum_{j=1}^{D} \overrightarrow{\omega_i\omega_j}[j]$, where $\overrightarrow{v}[j]$ denotes the j-th coordinate of $\overrightarrow{v}$.
- Computation of Q_1: $Q_1[i, j] = \overrightarrow{\omega_i\omega_j}Vtr(1)$.
- **Output:** Q_1 w.r.t. $\mathscr{B}$.

For computing the characteristic polynomial χ_t of any element $t \in K[X_1, \ldots, X_n]$ one could use classical algorithms, ignoring in this case the informations provided by the multiplication tensor of the quotient algebra $\mathscr{A}_K(\mathscr{I})$.

Let $P = \sum_{i=0}^{D} a_i T^{D-i} \in K[T]$ and denote by $\{\beta_1, \ldots, \beta_D\}$ its roots counted with multiplicities. We define the i-th Newton sum associated to P by: $N_i(P) = \sum_{j=0}^{D} \beta_j^i$, and, according to Newton's formula, we have $(D-i)a_i = \sum_{j=0}^{i} a_{i-j}N_j(P)$. Theorem 2.1 shows that the Newton sums N_i are in fact equal to traces $N_i(P) = \mathrm{Trace}(m_{P^i}^{\mathscr{A}_K(\mathscr{I})})$, and also Newton's formula becomes: $(D-i)a_i = \sum_{j=0}^{i} a_{i-j}\mathrm{Trace}(m_{P^j}^{\mathscr{A}_K(\mathscr{I})})$. At last, using Lemma 4.1 one can provide an efficient algorithm that computes χ_t through Newton's formula and using the multiplication tensor of $\mathscr{A}_K(\mathscr{I})$:

Algorithm Compute-χ_t

- **Input:** $MT(\mathscr{A}_K(\mathscr{I}))$, M_t the matrix of $m_t^{\mathscr{A}_K(\mathscr{I})}$ w.r.t. $\mathscr{B}$.
- Set $N_0(\chi_t) = D$ and $\overrightarrow{v} = [1, 0, \ldots, 0]$.
- Compute $Vtr(1)$ using $\mathrm{Trace}(m_{\omega_i}^{\mathscr{A}_K(\mathscr{I})}) = \sum_{j=1}^{D} \overrightarrow{\omega_i \omega_j}[j]$, where $\overrightarrow{v}[j]$ denotes the j-th coordinate of $\overrightarrow{v}$,
- For $i = 1, \ldots, D$ do:
  - $N_i(\chi_t) = \mathrm{Trace}(m_{t^i}^{\mathscr{A}_K(\mathscr{I})}) = \overrightarrow{v}\, Vtr(1)$,
  - $\overrightarrow{v} = M_t \overrightarrow{v}$,
- Solve the triangular system: $(D-i)a_i = \sum_{j=0}^{i} a_{i-j}\mathrm{Trace}(m_{t^i}^{\mathscr{A}_K(\mathscr{I})})$, $i = 0, \ldots, D$,
- **Output:** $\chi_t(T) = \sum_{i=0}^{D} a_i T^{D-i}$.

The same kind of result can be used for computing the polynomials $g_t(v, T)$, $v = 1, X_1, \ldots, X_n$, that define the t-representation of $V_C(\mathscr{I})$. As shown in the demonstration of theorem 3.1, $g_t(v, T) = \sum_{i=0}^{d-1} \mathrm{Trace}(m_{vt^i}^{\mathscr{A}_K(\mathscr{I})}) H_{d-i-1}(T)$, where $H_j(T)$ denotes the j-th Horner's polynomial associated to $\overline{\chi_t}$ (the characteristic polynomial of the multiplication by t in $\mathscr{A}_K(\mathscr{I})$) and d the degree of $\overline{\chi_t}$. Using the linearity of the Trace map we have equivalently: $g_t(v, T) = \sum_{i=0}^{d-1} \mathrm{Trace}(m_{vH^i(t)}^{\mathscr{A}_K(\mathscr{I})}) T^{d-i-1}$. Assuming that χ_t is computed using algorithm *Compute*-χ_t, the vectors $\overrightarrow{H^i(t)}$ are easily deducible from the vectors $\overrightarrow{t^i}$ that have been already computed. We can follow with the computation of $g_t(v, T)$ that can be done by using Lemma 4.1: $\mathrm{Trace}(m_{vH^i(t)}^{\mathscr{A}_K(\mathscr{I})}) = \overrightarrow{H^i(t)}\, Vtr(v)$. If M_v denotes the matrix of $m_v^{\mathscr{A}_K(\mathscr{I})}$ w.r.t. $\mathscr{B}$ and M_v^T its transposed one have immediately the relation $Vtr(v) = M_v^T Vtr(1)$. Putting together all these results, one can propose an efficient algorithm for computing the $g_t(v, T)$:

Algorithm Compute-$g_t(v, T)$

- **Input:** $\overline{\chi_t} = \sum_{i=0}^{d} a_i T^{d-i}$, $v \in K[X_1, \ldots, X_n]$, M_v, $Vtr(1)$.
- Set $H_i(t) = \sum_{j=0}^{i} a_j t^{i-j}$, $i = 1 \ldots (d-1)$.

- Set $Vtr(v) = M_v^T Vtr(1)$.
- For $i = 1, \ldots, d-1$ do $\mathrm{Trace}(m_{vH_i(t)}^{\mathscr{A}_K(\mathscr{I})}) = \overrightarrow{H_i(t)} Vtr(v)$,
- **Output:** $g_t(v, T) = \sum_{i=0}^{d-1} \mathrm{Trace}(m_{vH_i(t)}^{\mathscr{A}_K(\mathscr{I})}) T^{d-i-1}$.

Finally, by combining the algorithms described above, the computation of a Rational Univariate Representation could be done using the following algorithm:

Algorithm Compute-RUR

- **Input:** $MT(\mathscr{A}_K(\mathscr{I}))$.
- [1] Compute Q_1 and set $d = \mathrm{rank}(Q_1)$.
- [2] Choose $t \in \mathscr{T} = \{X_1 + iX_2 + \cdots + i^{n-1}X_n, i = 1..nD(D-1)/2$,
- [3] Compute χ_t using *Compute-*χ_t,
- [4] if degree$(\overline{\chi_t}) \neq d$ then goto [2],
- [5] compute $g_t(1, T) = \chi_t' / \mathrm{gcd}(\chi_t', \chi_t)$
- [6] Compute $g_t(X_1, T), \ldots, g_t(X_n, T)$ using *Compute-*$g_t(v, T)$,
- **Output:** $\{\chi_t, g_t(1, T), g_t(X_1, T), \ldots, g_t(X_n, T)\}$.

Given the multiplication table associated to any basis of $\mathscr{A}_K(\mathscr{I})$, the complexity, in terms of basic arithmetic operations in K, of this last algorithm is clearly polynomial in $D = \mathrm{Dim}_K(\mathscr{A}_K(\mathscr{I}))$.

As described in [27], the multiplication tensor of $\mathscr{A}_K(\mathscr{I})$: $MT(\mathscr{A}_K(\mathscr{I})) = \{\overrightarrow{\omega_i \omega_j}, \ i = 1, \ldots, n, \ j = 1, \ldots, n\}$, can be computed using $O(D^4)$ basic arithmetic operations with a well controlled growth of the binary sizes of coefficients when dealing with systems with integer coefficients ($O(Dl)$ if l denotes the binary size of the integers that appear in the multiplication matrix). The multiplication tensor will be considered as the input of the algorithms we propose.

We start by studying the case of systems for which a separating element is known (for example systems in the shape lemma case), removing also the steps [1], [2] and [4] in algorithm Compute-RUR.

Proposition 4.1 *Let $\mathscr{I}$ be a zero-dimensional ideal in $K[X_1, \ldots, X_n]$. When a separating element is known, given the multiplication table associated to any monomial basis of $\mathscr{A}_K(\mathscr{I})$, the complexity of the algorithm Compute-RUR is in $O(D^3 + nD^2)$ basic arithmetic operations in K.*

If K denotes the field of rational numbers, the complexity of the algorithm Compute-RUR is in $O((D^3 + nD^2)M(D^2 l))$ binary arithmetic operations, where l denotes the binary size of the coefficients that appear in the matrix of multiplication by one variable in $\mathscr{A}_K(\mathscr{I})$ and $M(l)$ the complexity of the multiplication of two integers of length l.

When $\mathscr{I}$ is radical this complexity is in $O((D^3 + nD^2)M(Dl))$.

Proof. Let us study step by step the algorithm Compute-RUR:

- [3] compute χ_t using *Compute-*χ_t. In algorithm *Compute-*χ_t,
  - the computation of $Vtr(1)$ using $\mathrm{Trace}(m_{\omega_i}^{\mathscr{A}_K(\mathscr{I})}) = \sum_{j=1}^{D} \overrightarrow{\omega_i\omega_j}[j]$, requires $O(D^2)$ arithmetic operations. In the case of rational coefficients, since the binary sizes in the expressions $\overrightarrow{\omega_i\omega_j}$ are in $O(Dl)$ (see [27]) the cost in terms of binary operations is in $O(D^2 M(Dl))$.
  - the loop:
    For $i = 1, \ldots, D$ do:
    * $N_i(\chi_t) = \mathrm{Trace}(m_{t^i}^{\mathscr{A}_K(\mathscr{I})}) = \overrightarrow{v}\, Vtr(1)$,
    * $\overrightarrow{v} = M_t \overrightarrow{v}$,

    requires $O(D^3)$ arithmetic operations in K. In the case of rational coefficients, one can observe that if l denotes the binary size of the coefficients that appear in the matrix of multiplication by one variable in $\mathscr{A}_K(\mathscr{I})$, the size of the coefficients in the expression of $\overrightarrow{v}$ is in $O(Dl)$ as in the expression of $Vtr(1)$, so that the binary size of the $N_i(\chi_t)$ is in $O(Dl)$. Hence, this loop requires $O(D^3 M(Dl))$ binary operations.
  - the resolution the triangular system:

$$(D - i)a_i = \sum_{j=0}^{i} a_{i-j} \mathrm{Trace}(m_{t^i}^{\mathscr{A}_K(\mathscr{I})}) \ , \ i = 1, \ldots, D,$$

    needs obviously $O(D^2)$ arithmetic operations in K. One can observe, when using rational numbers, that the order of the binary size in the result is the same than in the $N_i(\chi_t)$, so that the cost of the resolution in terms of binary operations is in $O(D^2 M(Dl))$.
- [6] Compute $g_t(X_1, T), \ldots, g_t(X_n, T)$ using *Compute-*$g_t(v, T)$.
  - given χ_t, the computation of its square-free part $\overline{\chi_t}$, requires $O(D^2)$ ($O(M(D))$ when using FFT) basic arithmetic operations. In the case of rational numbers, since the size of the coefficients in χ_t is in $O(Dl)$, the size of the coefficients of $\overline{\chi_t}$ is in $O(D^2 l)$ in the general case and in $O(Dl)$ if χ_t is square-free (radical ideals). In practice we should assume that the sizes in the result are in $O(Dl)$. Up to the end of the proof we will notice l' this binary size.
  - the expression $H_i(t) = \sum_{j=0}^{i} a_j t^{i-j}, \ i = 1, \ldots, D-1$ can be computed in $O(D^2)$ arithmetic operations. In the case of rational numbers, we have seen that the size of the a_i is in $O(l')$, and that the size of the coefficients in the vectors $\overrightarrow{t^i}$ is in $O(Dl)$ so that all the $H_i(t), \ i = 1, \ldots, D-1$ can be computed in $O(D^3 M(l'))$.

- if v is a variable, the expression $Vtr(v) = M_v^T Vtr(1)$ requires $O(D^2)$ arithmetic operations in K, without a significant growth of coefficients when using rational numbers (also $O(D^2 M(l'))$ binary operations).
- applied for $v = X_1, \ldots, X_n$ the loop

$$For\ i = 1, \ldots, D-1\ do\ \mathrm{Trace}(m_{vH_i(t)}^{\mathscr{A}_K(\mathscr{I})}) = \overrightarrow{H_i(t)} Vtr(v)$$

requires $O(nD^2)$ basic arithmetic operations in K, without a significant growth of coefficients when using rational numbers (hence $O(nD^2 M(l'))$ binary operations).

To summarize, we obtain, for the whole algorithm, a complexity in $O(D^3 + nD^2)$ arithmetic operations in K. In the case of rational numbers, the size of the coefficients that appear during the computations and in the result is in $O(l')$, with $l' = D^2 l$ in general and $l' = Dl$ in practice or in the case of radical ideals. ■

Remark 4.1. The complexity in the case of a radical ideal can be considered as a *practical complexity* for the general case since the size of the coefficients that appear in the gcd of two polynomials is lower, in general, than the size of the coefficients of the polynomials.

In any case, *the size order of the rationals that appear during the computations does not exceed the size order of the rationals that appear in the result*.

A randomly chosen linear form separates $V_C(\mathscr{I})$ with a probability 1, so, the proposition above gives a realistic evaluation of the practical complexity of the algorithm Compute-RUR. The theoretical complexity in the general case is as follows:

Proposition 4.2 *Given the multiplication table associated to any monomial basis of $\mathscr{A}_K(\mathscr{I})$, the complexity of the algorithm Compute-RUR is in $O(nD^5)$ basic arithmetic operations in K.*

If K is the field of rational numbers, the complexity of the algorithm Compute-RUR is in $O(nD^4 M(D^2 l))$ bit-operations, where l denotes the binary size of the coefficients that appear in the matrix of multiplication by one variable in $\mathscr{A}_K(\mathscr{I})$ and $M(l)$ the complexity of the multiplication of two integers of length l.

Moreover, if $\mathscr{I}$ is known to be radical, the bit-complexity, when using rational numbers, is in $O(nD^4 M(Dl))$. In particular, if $\mathscr{I}$ is known to be shape lemma (X_1 separates $V_C(\mathscr{I})$), the complexity is in $O((D^3 + nD^2) M(Dl))$.

Proof. Knowing the number of distinct roots of the system, say d, the algorithm consists in taking potential separating elements in a finite set of linear forms of cardinality $nd(d-1)/2$. This computation needs also $O(nD^2(D^3))$ arithmetic operations in K.

In the case of rational numbers, if l' denotes the binary length of the coefficients in the square-free part of the characteristic polynomials (see the proof of the precedent proposition), this requires $O(n(D^2(D^3M(Dl)+D^2M(l'))))$ binary operations.

For computing the number of roots d of the system one must:

- construct Hermite's quadratic form using the algorithm Compute-Q_1. This requires $O(D^2)$ basic operations in K for computing $Vtr(1)$, and then $O(D^3)$ basic operations in K for computing the expressions $Q_1[i,j] = \overrightarrow{\omega_i\omega_j}Vtr(1)$. In the case of rational numbers the binary size of the coefficients in Q_1 is obviously in $O(Dl)$.
- for reducing the quadratic form Q_1 we may use, in the general case, the Gaussian ortho-normalization which requires $O(D^3)$ basic operations in K. In the case of rational numbers, we may assume that Q_1 has integer entries and also apply the fraction-free algorithm described in [26] which requires $O(D^3)$ basic arithmetic operations in $\mathbb{Z}$ but ensures a well controlled growth of coefficients: $O(D^2l)$ in our case.

In the case of a radical ideal the reduction of Hermite's quadratic form is useless since the characteristic polynomial of any separating element must be square-free. ■

5 Applications of the Rational Univariate Representation

In this part, we suppose that $\{\chi_t(T), g_t(1,T), g_t(X_1,T), \ldots, g_t(X_k,T)\}$ is a Rational Univariate Representation of the elements of a finite affine variety $V_C(\mathscr{I})$, $\mathscr{I} \subset K[X_1,\ldots,X_n]$.

In the first section, we suppose that K is ordered and we study how the Rational Univariate Representation could be used for studying $V_C(\mathscr{I})\bigcap R^n$, where R denotes the real closure of K.

In the second section, we study how the Rational Univariate Representation can be used in order to compute or study radical ideals generated by zero-dimensional systems. In particular we show how the Rational Univariate Representation relies to lexicographic Gröbner basis in the shape lemma case.

In the third section we show how the Rational Univariate Representation can be used for splitting a system by factorizing $\chi_t(T)$ or by computing the multiplicities of the roots.

5.1 Rational Univariate Representation and Real Roots

According to Theorem 3.1, a Rational Univariate Representation of any zero-dimensional ideal induces a K-isomorphism $\psi_t : V_C(\mathscr{I}) \longrightarrow V_C(\chi_t)$.

Since ψ_t and its reciprocal are represented by polynomials with coefficients in the ground field K, then, if K is ordered and if R denotes its real closure, we can see that ψ_t induces an K-isomorphism between $V_R(\mathscr{I}) = V_C(\mathscr{I}) \bigcap R^n$ and $V_R(\chi_t) = V_C(\chi_t) \bigcap R$ that preserves the multiplicities.

Moreover, we can compute a t-representation of $\mathscr{I}$, where the polynomial t separates $V_R(\mathscr{I})$ but not necessarily $V_C(\mathscr{I})$. Such a t-representation will induce a K-isomorphism between $V_R(\mathscr{I}) = V_C(\mathscr{I}) \bigcap R^n$ and $V_R(\chi_t)$ that preserves the multiplicities.

For this purpose we could use the following result (see for example [21, 3, 22]):

Theorem 5.1 *Let $\mathscr{I}$ be a zero-dimensional ideal and h a polynomial in $K[X_1, \ldots, X_n]$. If R denotes the real closure of K* (*when it is defined*) *then the signature of $q_h^{\mathscr{A}_K(\mathscr{I})}$ verifies*:

$$\rho(q_h^{\mathscr{A}_K(\mathscr{I})}) = \sharp\{\alpha \in V_R(\mathscr{I}) | h(\alpha) > 0\} - \sharp\{\alpha \in V_R(\mathscr{I}) | h(\alpha) < 0\}.$$

In particular, the signature of $q_1^{\mathscr{A}_K(\mathscr{I})}$ is exactly equal to the number of elements in $V_R(\mathscr{I})$. Therefore the criterion for searching a element t that separates $V_R(\mathscr{I})$ consists in comparing the signature of $q_1^{\mathscr{A}_K(\mathscr{I})}$ and the number of real roots of χ_t using for example Sturm–Habicht sequences (see [14]) or Uspensky's algorithm (see [4] or [6]).

The algorithm would also become:

Algorithm Compute-RUR-Real

- **Input:** $MT(\mathscr{B})$.
- [1] Compute Q_1 and set $d = signature(Q_1)$.
- [2] Choose $t \in \mathscr{T}$,
- [3] Compute χ_t using *Compute-*χ_t,
- [4] if number of real roots of $\overline{\chi_t} \neq d$ then goto [2],
- [5] compute $g_t(1, T) = \chi_t' / \gcd(\chi_t', \chi_t)$
- [6] Compute $g_t(X_1, T), \ldots, g_t(X_n, T)$ using *Compute-*$g_t(v, T)$,
- **Output:** $\{\chi_t, g_t(1, T), g_t(X_1, T), \ldots, g_t(X_n, T)\}$.

5.2 Rational Univariate Representation and Lexicographic Gröbner Basis in the Case of Radical Ideals

As we have seen in previous parts, the case of radical ideals has to be considered separately especially in the study of the complexity. We will study, in this part, some properties of the Rational Univariate Representation in such cases.

Our first item consists in a relation between the univariate representation introduced above and lexicographic Gröbner basis that provide, in the shape lemma case, a good way for *solving* zero-dimensional systems.

As described in [7] (for example), when an ideal is in the shape lemma position (X_1 is separating and $\mathscr{I}$ is radical) the Gröbner basis for the lexicographic monomial ordering (with $X_1 < \cdots < X_n$) is in the form:

$$\begin{cases} f_1(X_1) \\ X_2 - f_2(X_1) \\ \vdots \\ X_n - f_n(X_1) \end{cases}$$

where $f_1(X_1)$ is a square-free polynomial. In particular it induces an isomorphism of algebraic sets:

$$\begin{array}{rccc} \phi_{lex}: & V_C(\mathscr{I}) & \longrightarrow & V_C(f_1) \\ & (\alpha_1, \ldots, \alpha_n) & \longmapsto & \alpha_1 \end{array}$$

The regular map ϕ_{lex} preserves the multiplicities since the associated pullback mapping induces an isomorphism of K-algebra from $K[X_1]/\langle f_1 \rangle$ onto $K[X_1, \ldots, X_n]/\mathscr{I}$. Also (ϕ_{lex}, f_1) is an univariate resolution of $V_C(\mathscr{I})$.

Proposition 5.1 *Let $\mathscr{I} \subset K[X_1, \ldots, X_n]$ a zero-dimensional ideal in shape lemma position. Since X_1 separates $V_C(\mathscr{I})$, there exists a Rational Univariate Representation associated to X_1: $\{\chi_{X_1}(T), g_{X_1}(1, T), g_{X_1}\ (X_1, T), \ldots, g_{X_1}(X_n, T)\}$. If $\{f_1(X_1), X_2 - f_2(X_2), \ldots, X_n - f_n(X_1)\}$ denotes the lexicographic Gröbner basis of $\mathscr{I}$ for $X_1 < \cdots < X_n$, then:*

- $\chi_{X_1}(T) = f_1(T)$
- $g_{X_1}(1, T)$ *is invertible modulo* $\chi_{X_1}(T)$,
- *for* $i = 2, \ldots, n$, $f_i(T) = g_{X_1}(X_i, T)(g_{X_1}(1, T))^{-1} \bmod \chi_{X_1}(T)$.

Proof. The first item is obvious by construction. The relation $g_{X_1}(1, T) = \chi'_{X_1}/(\mathrm{gcd}(\chi'_{X_1}, \chi_{X_1})$ shows the second item. Since $\mathscr{I}$ is in shape lemma position, $f_1(T)$ is square-free and also $\langle \chi_{X_1} \rangle$ is radical. Noticing that $g_{X_1}(X_i, T)$ $(g_{X_1}(1, T))^{-1}$ and $f_i(T)$ coincide on $V_C(\chi_{X_1})$, the last item is proved. ∎

Remark 5.1. In the case of systems with integer coefficients, we have seen that all the coefficients in all the polynomials defining a Rational Univariate Representation have an equivalent binary size. As we have seen above, one can deduce, in the shape lemma case,a lexicographic Gröbner basis from the Rational Univariate Representation associated to the first variable by inverting the common denominator. In practice, this inversion can be done using Euclide's algorithm inducing a grow of the coefficients, linear in the degree of the polynomial.

The remark above can be illustrated by Fig. 1: we have computed, for a set of 8 examples in the shape lemma case, all the binary sizes of the coefficients

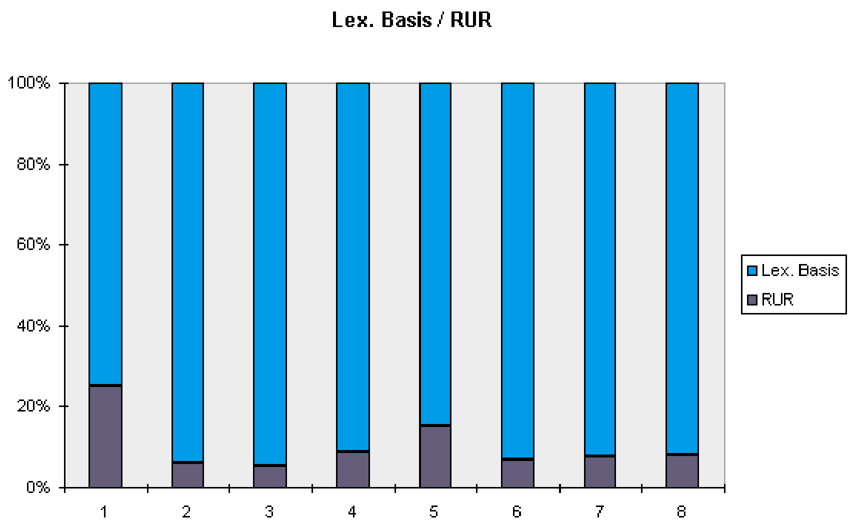

Fig. 1. Coefficient sizes

of the rational Univariate Representation associated to the first variable and the coefficients that appear in the lexicographic Gröbner basis.

Of course this grow of coefficients affects the computation time. Figure 2 compares two methods with a similar number of arithmetic operations:

Both algorithms have been implemented in the library RealSolving (see [24]). The implementation of FGLM is similar to those of Gb (see [8]).

- FGLM (see [11]): computation by change of ordering of a lexicographic Gröbner basis (the algorithm starts with a Gröbner basis computed for any admissible monomial ordering).
- RUR-rat (see next section): computation a Rational Univariate Representation (computing the multiplication tensor from the same Gröbner basis than those used for FGLM).

In the general case of radical ideals, the lexicographic Gröbner basis has the following shape:

$$\begin{cases} f_1(X_1) \\ f_2(X_1, X_2) \\ \vdots \\ f_{k_2}(X_1, X_2) \\ \vdots \\ f_n(X_1, \ldots, X_n) \\ \vdots \\ f_{k_n}(X_1, \ldots, X_n) \end{cases}$$

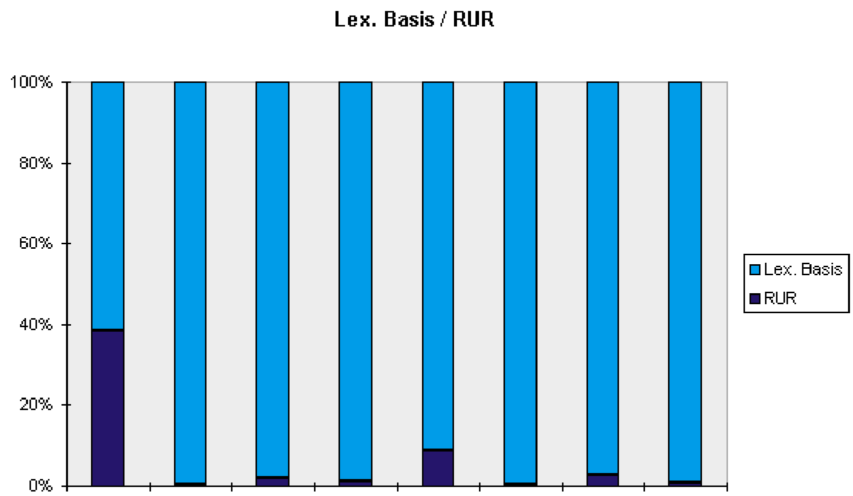

Fig. 2. Computation times

so that Proposition 5.1 can not be extended. The next proposition shows, in particular, that a Rational Univariate Representation of $\sqrt{\mathcal{I}}$ can easily be deduced from a Rational Univariate Representation of $\mathcal{I}$:

Proposition 5.2 *If (ϕ, f) be an Univariate Representation of a zero-dimensional ideal $\mathcal{I}$, then then (ϕ, f_{red}), where f_{red} is the square-free part of f, is an Univariate Representation of $\sqrt{(\mathcal{I})}$.*

Proof. By applying proposition 3.2, f is the characteristic polynomial of $t = \Phi^{\phi}(T)$ in $K[X_1, \ldots, X_n]/\mathcal{I}$. The polynomial t separates $V_C(\mathcal{I})$ and also $V_C(\sqrt{\mathcal{I}})$. ■

5.3 Splitting the Rational Univariate Representation

The main advantage of the Rational Univariate Representation is that we can apply many methods on univariate polynomials in order to study the system. In order to simplify the output, one can for example factorize the first polynomial of the Rational Univariate Representation $\chi_t(T) = \prod_{i=1}^{k} \chi_{t,i}(T)$ and also provide a representation of all the roots by a set of Rational Univariate Representations:

$$\bigcup_{i=1}^{k} \{\chi_{t,i}(T), g_{t,i}(1, T), g_{t,i}(X_1, T), \ldots, g_{t,i}(X_k, T)\}$$

where $g_{t,i}(v, T) = g_t(v, T) \bmod \chi_{t,i}(T)$.

Example 5.1
Consider the following system where none of the variables is separating

$$\begin{aligned} 24uz - u^2 - z^2 - u^2z^2 - 13 &= 0 \\ 24yz - y^2 - z^2 - y^2z^2 - 13 &= 0 \\ 24uy - u^2 - y^2 - u^2y^2 - 13 &= 0 \end{aligned}$$

A Rational Univariate representation is given by:

$$\begin{aligned} \chi_t(x) = {} & x^{16} - 5656x^{14} + 12508972x^{12} - 14213402440x^{10} + 9020869309270x^8 \\ & -3216081009505000x^6 + 606833014754230732x^4 \\ & -51316296630855044152x^2 + 1068130551224672624689 \end{aligned}$$

$$\begin{aligned} g_t(1, x) = {} & x^{15} - 4949x^{13} + 9381729x^{11} - 8883376525x^9 + 4510434654635x^7 \\ & -1206030378564375x^5 + 151708253688557683x^3 \\ & -6414537078856880519x \end{aligned}$$

$$\begin{aligned} g_t(u, x) = {} & 71x^{14} - 355135x^{12} + 673508751x^{10} - 633214359791x^8 \\ & +314815356659869x^6 - 79677638700441717x^4 \\ & +8618491509948092045x^2 - 205956089289536014429 \end{aligned}$$

$$\begin{aligned} g_t(y, x) = {} & 86x^{14} - 418870x^{12} + 759804846x^{10} - 670485664238x^8 \\ & +307445009725282x^6 - 71012402366579778x^4 \\ & +7099657810552674458x^2 - 168190996202566563226 \end{aligned}$$

$$\begin{aligned} g_t(z, x) = {} & 116x^{14} - 483592x^{12} + 784226868x^{10} - 634062241592x^8 \\ & +270086313707548x^6 - 58355579408017944x^4 \\ & +5520988105236180668x^2 - 131448117382500870952 \end{aligned}$$

Noticing that $\chi_t(x)$ equals

$$\begin{aligned} & (x^4 - 1222x^2 + 371293) \cdot (x^4 - 1030x^2 + 190333) \cdot \\ & \cdot (x^4 - 2326x^2 + 484237) \cdot (x^4 - 1078x^2 + 31213), \end{aligned}$$

we can split the rational univariate representation in four components. An example of component:

$$\begin{aligned} \chi_{t,1}(x) &= x^4 - 1222x^2 + 371293 \\ g_{t,1}(1, x) &= -1528597x^3 + 939034343x \\ g_{t,1}(t, x) &= 67229849947 - 104420381x^2 \\ g_{t,1}(y, x) &= 115704058093 - 203404643x^2 \\ g_{t,1}(z, x) &= 67229849947 - 104420381x^2 \end{aligned}$$

The advantage of the Rational Univariate Representation is to keep track of multiplicities of the roots. The polynomials of the Rational Univariate Representation give an easy way to express the multiplicity of each root: the following result can be obtained by a simple computation:

Proposition 5.3 *Let* $\{\chi_t(T), g_t(1, T), g_t(X_1, T), \ldots, g_t(X_n, T)\}$ *a Rational Univariate Representation of any zero dimensional ideal* $\mathcal{I} \subset K[X_1, \ldots, X_n]$. *Then:*

$$\forall \alpha \in V_C(\mathcal{I}) \ , \ \mu(\alpha) = \frac{g_t(1, t(\alpha))}{\overline{\chi}_t'(t(\alpha))}.$$

Using this formula, the square-free factorization of $\overline{\chi}_t(T)$ is obtained by computing the gcd's:

$$\chi_{t,i}(T) = \gcd(g_t(1,T) - i \cdot \overline{\chi}_t'(T), \overline{\chi}_t(T)) \ , \ i = 1, \ldots, \deg(\chi_t(T)).$$

The number of roots with a given multiplicity i is exactly the degree of $\overline{\chi}_{t,i}(T)$. As a direct consequence of these last results, we can define the Rational Univariate Representation of the roots of multiplicity i of $V_C(\chi_t)$, which correspond exactly to the expressions proposed in [1]:

$$\{\chi_{t,i}(T), g_{t,i}(1,T), g_{t,i}(X_1,T), \ldots, g_{t,i}(X_k,T)\}$$

where

$$g_{t,i}(v,T) = g_t(v,T) \bmod \overline{\chi}_{t,i}(T)$$

Example 5.2
Consider the following system

$$\begin{array}{l} 24 - 92a - 92b - 113b^3 + 49a^4 + 49b^4 - 11a^5 - 11b^5 + a^6 + b^6 + 142a^2 + 284ab \\ \quad +142b^2 - 339a^2b - 339ab^2 + 294a^2b^2 + 196ab^3 - 55a^4b - 110a^3b^2 - 110a^2b^3 \\ \quad -55ab^4 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 - 113a^3 + 196a^3b \\ \\ c^3 + 3bc^2 + 3b^2c + b^3 \\ \\ 8b^3 + 12b^2c - 12ab^2 + 6bc^2 - 12cab + 6a^2b + c^3 - 3ac^2 + 3a^2c - a^3 \end{array} .$$

A Rational Univariate Representation is given by:

$$\begin{aligned} \chi_t(x) &= 8x^6 - 44x^5 + 98x^4 - 113x^3 + 71x^2 - 23x + 3 \\ g_t(1,x) &= 24x^2 - 50x + 23 \\ g_t(a,x) &= 24x^3 - 50x^2 + 23x \\ g_t(b,x) &= 22x^2 - 43x + 18 \\ g_t(c,x) &= -22x^2 + 43x - 18 \end{aligned} .$$

Using proposition 5.3 one can compute explicitly the square-free decomposition of χ_t: $\chi_t = (\overline{\chi}_{t,1})(\overline{\chi}_{t,2})^2(\overline{\chi}_{t,3})^3$ with $\overline{\chi}_{t,1}(x) = 2x - 3$, $\overline{\chi}_{t,2}(x) = 2x - 1$ and $\overline{\chi}_{t,3}(x) = x - 1$. Also, there is one root of multiplicity 1, one root of multiplicity 2, and one root of multiplicity 3. The Rational Univariate Representations w.r.t. multiplicities are:

$$\begin{aligned} &[\overline{\chi}_{t,1} = x - 1, g_{t,1}(1,T) = 1, g_{t,1}(X_1,T) = 1, g_{t,1}(X_2,T) = 1, \\ &\quad g_{t,1}(X_3,T) = -1] \\ &[\overline{\chi}_{t,2} = 2x - 1, g_{t,2}(1,T) = 2, g_{t,2}(X_1,T) = 1, g_{t,2}(X_2,T) = 1, \\ &\quad g_{t,2}(X_3,T) = -1] \\ &[\overline{\chi}_{t,3} = 2x - 3, g_{t,3}(1,T) = 2, g_{t,3}(X_1,T) = 3, g_{t,3}(X_2,T) = 3, \\ &\quad g_{t,3}(X_3,T) = -3] \end{aligned}$$

6 The Case of Polynomial Systems with Integer Coefficients

As we have seen in the general case, the search of a separating element is the most costly task in the computation of a Rational Univariate Representation. In this part, we will see how this can be optimized in the case of systems with integer coefficients, when any Gröbner basis is known.

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

6.1 Working in $GF(p)$

Many basic algorithm used for the computation of a Rational Univariate Representation are working in $GF(p)$ for p sufficiently large. For example, lemma 2.1 becomes obviously:

Lemma 6.1 *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 $\mathscr{T} = \{X_1 + iX_2 + \ldots + i^{n-1}X_n\ ,\ 0 \leq i \leq (n-1)d(d-1)/2\}$ contains at least one element that separates V_p.*

In the same way, the demonstration of theorem 2.2 can be easily adapted to give the following result:

Theorem 6.1 *Let $\mathscr{I}_p \subset GF(p)[X_1, \ldots, X_n]$ be a zero-dimensional ideal, h a polynomial in $GF(p)[X_1, \ldots, X_n]$ and $D = \mathrm{Dim}_{GF(p)}(\mathscr{A}_{GF(p)}(\mathscr{I}_p)) = GF(p)[X_1, \ldots, X_n]/\mathscr{I}_p$. If $D < p$, the Hermite's quadratic form associated to h, defined by*

$$\begin{aligned} q_h^{\mathscr{A}_{GF(p)}(\mathscr{I}_p)} : \mathscr{A}_{GF(p)}(\mathscr{I}_p) &\longrightarrow GF(p) \\ f &\longmapsto \mathrm{Trace}(m_{hf^2}^{\mathscr{A}_{GF(p)}(\mathscr{I}_p)}) \end{aligned}$$

verifies:

$$\sigma(q_h^{\mathscr{A}_{GF(p)}(\mathscr{I}_p)}) = \sharp\{\alpha \in V_{GF(p)}(\mathscr{I}_p) | h(\alpha) \neq 0\}$$

where $\sigma\left(q_h^{\mathscr{A}_{GF(p)}(\mathscr{I}_p)}\right)$ denotes the rank of $q_h^{\mathscr{A}_{GF(p)}(\mathscr{I}_p)}$.

Our goal is to study the link between 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 $\mathbb{Z}_p$ to $GF(p)$. Let $\mathscr{G}$ be a Gröbner basis of a zero-dimensional ideal $\mathscr{I} \subset \mathbb{Q}[X_1, \ldots, X_n]$.

Definition 6.1 *A prime number p is said to be $\mathscr{G}$-compatible if p do not divide any of the leading coefficients of $\mathscr{G}$. In such cases we may assume that $\mathscr{G} \subset \mathbb{Z}_p[X_1, \ldots, X_n]$.*

Even if p is a $\mathscr{G}$-compatible prime, $\phi_p(\mathscr{G})$ is not, in general, a Gröbner basis of $\phi_p(\mathscr{I})$, but we have the following property (see [20] or [28]):

Theorem 6.2 *Let $\mathscr{G}$ be a Gröbner basis of a zero-dimensional ideal $\mathscr{I} \subset \mathbb{Q}[X_1, \ldots, X_n]$ for a given admissible monomial ordering $<$. If p is a $\mathscr{G}$-compatible prime then $\phi_p(\mathscr{G})$ is the Gröbner basis for $<$ of any zero-dimensional ideal $\phi_p(\mathscr{I}) \subset GF(p)[X_1, \ldots, X_n]$. Moreover, if $NF(f, \mathscr{G})$ denotes the canonical reduction of any polynomial p modulus a Gröbner basis $\mathscr{G}$ (normal form) then $\forall f \in \mathbb{Z}_p[X_1, \ldots, X_n]$, $\phi_p(NF(f, \mathscr{G})) = NF(\phi_p(f), \phi_p(\mathscr{G}))$.*

This theorem has direct consequences:

Corollary 6.1 *Let $\mathscr{G}$ be a Gröbner basis of a zero-dimensional ideal $\mathscr{I} \subset \mathbb{Q}[X_1, \ldots, X_n]$ and p a $\mathscr{G}$-compatible prime number. Then:*

- *$Dim_{GF(p)}(\mathscr{A}_{GF(p)}(\langle\phi_p(\mathscr{G})\rangle)) = Dim_{\mathbb{Q}}(\mathscr{A}_{\mathbb{Q}}(\mathscr{I}))$, where $\mathscr{A}_{\mathbb{Q}}(\mathscr{I}) = Q[X_1, \ldots, X_n]/\langle\mathscr{G}\rangle$ and $\mathscr{A}_{GF(p)}(\langle\phi_p(\mathscr{G})\rangle) = GF(p)[X_1, \ldots, X_n] / \langle\phi_p (\mathscr{G})\rangle$. Moreover, if $\mathscr{B}$ is the canonical monomial basis of $\mathscr{A}_{\mathbb{Q}}(\mathscr{I})$ associated to $\mathscr{G}$ (the set of monomials that are not reducible modulus $\mathscr{G}$) then $\mathscr{B}$ is also the monomial basis of $\mathscr{A}_{GF(p)}(\langle\phi_p(\mathscr{G})\rangle)$ associated to $\phi_p(\mathscr{G})$.*
- *if M_p (resp. M_{ϕ_p}) denotes the multiplication matrix by any polynomial $p \in \mathbb{Z}_p[X_1, \ldots, X_n]$ in $\mathscr{A}_{\mathbb{Q}}(\mathscr{I})$ (resp. $\mathscr{A}_{GF(p)}(\langle\phi_p(\mathscr{G})\rangle)$) w.r.t. the canonical monomial basis associated to $\mathscr{G}$ (resp. $\phi_p(\mathscr{G})$), then we have:*

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

  and also:
  - $\phi_p(Trace(M_p)) = Trace(M_{\phi_p})$,
  - $\phi_p(Det(M_p)) = Det(M_{\phi_p})$,
  - *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 $V_{\mathbb{C}}(\mathscr{I})$ on can establish the following result:

Proposition 6.1 *Let $\mathscr{I} \subset \mathbb{Q}[X_1, \ldots, X_n]$ a zero-dimensional ideal, $\mathscr{G}$ any Gröbner basis of $\mathscr{I}$. If p is a $\mathscr{G}$-compatible prime number greater than $D = Dim_{\mathbb{Q}}(\mathscr{A}_{\mathbb{Q}}(\mathscr{I}))$, then:*

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

Proof. Let $t \in \mathbb{Z}_p[X_1, \ldots, X_n]$ such that $\phi_p(t)$ separates $V_{\overline{GF(p)}}(\phi_p(\mathscr{G}))$. In such cases, $\sharp V_{\overline{GF(p)}}(\phi_p(\mathscr{G})) = deg(\overline{\chi_t}) = deg(\chi_{\phi(t)}/\mathrm{gcd}(\chi_{\phi(t)}, \chi_{\phi(t)}'))$. Since obviously $\mathrm{gcd}(\chi_{\phi(t)}, \chi_{\phi(t)}') \geq \mathrm{gcd}(\chi_t, \chi_t')$ (χ_t is supposed to be monic) and since $\sharp V_{\mathbb{C}}(\mathscr{G}) \geq deg(\chi_t/\mathrm{gcd}(\chi_t, \chi_t'))$, then $\sharp V_{\mathbb{C}}(\mathscr{G}) \geq \sharp V_{\overline{GF(t)}}(\phi_p(\mathscr{G}))$.

Let now suppose that $\sharp V_{\mathbb{C}}(\mathcal{G}) = \sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$. According to the precedent results, we have:

$$\sharp V_{\mathbb{C}}(\mathcal{G}) = \sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G})) = deg(\overline{\chi_{\phi(t)}}) \leq deg(\overline{\chi_t}) \leq \sharp V_{\mathbb{C}}(\mathcal{G}).$$

Also $deg(\overline{\chi_t}) = \sharp V_{\mathbb{C}}(\mathcal{G})$ and t separates $V_{\mathbb{C}}(\mathcal{G})$. ■

Finally, 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 6.1 for the modular computation of an element that separates $V_{\mathbb{C}}(\mathcal{G})$. 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 [26], if Q_1 denotes the Hermite's quadratic form associated to 1, it can be written in the form:

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

where D_i are minors extracted from the matrix of Q_1 w.r.t. any basis of $\mathcal{A}_{\mathbb{Q}}$. Also the $\mathcal{G}$-compatible prime numbers such that $\sharp V_{\mathbb{C}}(\mathcal{G}) = \sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$ are exactly the primes that do not divide the minors D_i. In particular, this shows the following result:

Proposition 6.2 *Given any Gröbner basis in $\mathbb{Q}[X_1, \ldots, X_n]$, there exists only a finite number of $\mathcal{G}$-compatible primes such that $\sharp V_{\mathbb{C}}(\mathcal{G}) \neq \sharp V_{\overline{GF(p)}}(\phi_p(\mathcal{G}))$*

6.2 The Algorithm and its Complexity

We describe, in this section, an algorithm for computing the Rational Univariate Representation in the case of zero-dimensional systems of polynomials with rational coefficients, using a modular computation for finding a separating element.

Algorithm Compute-RUR-Rat

- **Input:** $MT(\mathcal{A}_{\mathbb{Q}}(\mathcal{I}))$.
- [1] Set $d = rank(Q_1)$.
- [2] Choose a $\mathcal{G}$-compatible prime number greater than nd^2.
- [3] Compute $d_1 = rank(\phi_p(Q_1))$. If $d_1 \geq d$ goto [2].
- [4] Choose $t \in \phi_p(\mathcal{T})$,
- [5] Compute $\chi_{\phi_p(t)}$ by computing the characteristic polynomial of $m_{\phi_p(t)}^{\mathcal{A}_{GF(p)}(\langle\phi_p(\mathcal{G})\rangle)}$.
- [6] if degree$(\overline{\chi_{\phi_p(t)}}) \neq d$ then goto [4],
- [7] Compute $g_t(1, T) = \chi_t'/\gcd(\chi_t', \chi_t)$
- [8] Compute $g_t(X_1, T), \ldots, g_t(X_n, T)$ using *Compute-$g_t(v, T)$*,
- **Output:** $\{\chi_t, g_t(1, T), g_t(X_1, T), \ldots, g_t(X_n, T)\}$.

The only thing that differs from the generic algorithm *Compute-RUR* is the way of finding an element that separates $V_{\mathbb{C}}(\mathscr{I})$. This is done by steps 2 to 6.

The first stage consists in finding a prime number such that $\sharp V_{\mathbb{C}}(\mathscr{I}) = \sharp V_{\overline{GF(p)}}(\phi_p(\mathscr{G}))$. This operation needs $O(D^2 t)$ (number of primes that divide any coefficient of the reduced form of Q_1) reductions of quadratic forms with coefficients in $GF(p)$, which is not greater than the complexity (in terms of machine operations) of the computations done in step 1.

The second stage (steps 4 to 6) consists in computing a separating element of $V_{\overline{GF(p)}}(\phi_p(\mathscr{G}))$ by comparing the degree of the square-free part of $\chi_{\phi_p(t)}$ with the number of roots of $V_{\overline{GF(p)}}(\phi_p(\mathscr{G}))$. Since t is chosen in a set of cardinality $O(nD^2)$ this stage requires $O(nD^5)$ operations in $GF(p)$ which is less than the number of machine operations needed for steps 7 and 8. Proposition 6.1 ensure us that, after step 6, t separates $V_{\mathbb{C}}(\mathscr{I})$.

To summarize, the use of the modular arithmetic vanish the effect (in terms of computation time) of the search of an element of $\mathbb{Q}[X_1, \ldots, X_n]$ that separate $V_{\mathbb{C}}(\mathscr{I})$.

7 Conclusion

We have introduced, in this article, a new definition for solving zero-dimensional systems of polynomials following Kronecker's philosophy: the Rational Univariate Representation. We have shown that this representation of the solutions can be efficiently computed in practice, especially in the case of systems with integer coefficients.

Since the number of arithmetic operations and the growth of coefficients in intermediate computations are well controlled, this new method allows to solve problems that were not solvable before. It has been used successfully in many applications (see for example [25] or [10]).

As we have seen, the modular arithmetic can be used for optimizing the search of separating elements. We are actually working on a multi-modular version of our algorithm, that give great result in the shape lemma case (the easiest case since no separating element has to be computed) but we would like to extend it to the general case. Our first implementation differs from the one described in [9] only by the addition of the search of a separating element. We observe much better computation times, but the main progress is in terms of memory allocation since no multiplication tensor has to be computed when the ideal is supposed to be radical.

A major application of the Rational Univariate Representation will surely be its use inside algorithms in existential theory of reals or quantifier elimination (see [2]).

Acknowledgments. We would like to thank E. Becker and M.F. Roy for their help in the formulation and in the redaction of the Rational Univariate Representation, and P. Zimmermann for having his help in correcting the final version of this article.

References

1. Alonso, M.-E., Becker, E., Roy, M.-F., Wörmann, T.: Multiplicities and idempotents for zerodimensional systems. In: Algorithms in Algebraic Geometry and Applications, Progress in Mathematics Vol.143 p 1–20 Bosel. Birkhäuser 1996
2. Basu, S., Pollack R., Roy, M.-F.: On the combinatorial and algebraic complexity of quantifier elimination. Proc. 35th IEEE Symp. on Foundations of Computer Science, p 632–641, 1994
3. Becker, E., Wörmann, T.: Radical computations of zero-dimensional ideals and real root counting. Math Comp Simul (1993)
4. Buchberger, B., Collins, G.-E., Loos, R.: Computer Algebra Symbolic and Algebraic Computation. Berlin Heidelberg New York Springer 1982
5. Canny, J.-F.: Some algebraic and geometric computations in pspace. Twentieth ACM Symp. on Theory of Computing, p 460–467, 1988
6. Collins, G., Akritas, A.: Polynomial real root isolation using descartes' rule of signs. In: SYMSAC, p 272–275, 1976
7. Cox, D., Little, J., O'Shea, D.: Ideals, varities, and algorithms an introduction to computational algebraic geometry and commutative algebra. Undergraduate texts in mathematics. New York- Berlin-Paris: Springer 1992
8. Faugère, J.C.: Gb. available on `http : //posso.lip6.fr/~jcf`
9. Faugère, J.C.: Multi-modular fglm. Médicis-PoSSo workshop on polynomial system solving, Toulouse, December 1995
10. Faugère, J.C., Moreau de Saint Martin, F., Rouillier, F.: Design of regular nonseparable bidimensional wavelets using groebner basis techniques. IEEE SP Transactions Special Issue on Theory and Applications of Filter Banks and Wavelets, SP:30, 1997
11. Faugère, J.C., Gainni, P., Lazard, D., Mora, T.: Efficient computation of zero-dimensional gröbner basis by change of ordering. J Sym Comput 16(4):329–344 (1993)
12. Giusti, Heintz, Morais, and Pardo. When polynomial equation systems can be "solved" fast. In: AAECC-11, Lecture Notes in Computer Science, 1995
13. Giusti, M., Heintz, J.: Algorithmes—disons rapides—pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelless. In: Mora, T., Traverso, C. (eds). Proc. Effective Methods in Algebraic Geometry, MEGA '90 Progress in Mathematics, Vol 94 p 169–193. Basel: Birkhäuser 1991
14. González-Vega, L., Lombardi, H., Recio, T., Roy, M-F.: Sturm-habicht sequence. In ISSAC-89 Proceedings, p 136–146. ACM-Press 1989
15. Gonzalez-Vega, L., Rouillier, F., Roy, M.F.: Symbolic Recipes for Polynomial System Solving, chapter 2. Some Tapas of Computer Algebra. Berlin Heidelberg Newyork: Springer 1997
16. Gonzalez-Vega, L., Rouillier, F., Trujillo, G.: Symbolic Recipes for Real Solutions, chapter 6. Some Tapas of Computer Algebra Berlin Heidelberg Newyork: Springer 1997
17. González-Vega, L., Trujillo, G.: Using symmetric functions to describe the solution set of a zero dimensional ideal. In: Cohen, G., Giusti, M., Mora, T. (eds) Applied Algebra and Error Correcting Codes Lecture Notes in Computer Science, Vol 948 p 232–247. Berlin Heidelberg Newyork: Springer 1995
18. Lazard D.: Solving zero-dimensional algebraic systems. J Symbol Comput 13:117–132 (1992)
19. Marinari, M.G., Möller, H.M., Mora, T.: On multiplicities in polynomial system solving. Trans Am Math Soc 348(8):283–321 (1996)
20. Noro, M., Yokoyama, K.: New methods for the change-of- ordering in groebner basis computation. Technical report, Fujutsu, 1995
21. Pedersen, P.: Counting Real Zeros. PhD thesis, New York University, 1991
22. Pedersen, P., Roy, M.-F., Szpirglas, A.: Counting real zeros in the multivariate case. In: Computational Algebraic Geometry, Progress in Mathematics, Vol 109 p 61–76. Basel: Birkhäuser 1993

23. Renegar, J.: On the computational complexity and geometry of the first-order theory of the reals. J Symbol Comput 13:255–352 (1992)
24. Rouillier, F.: RealSolving. available on http : //www.loria.fr/~rouillie
25. Rouillier, F.: Des formules de bareiss à ĺa réduction des formes quadratiques. Notes aux comptes rendus de l'acadmie des sciences 320:1273–1278 (1995)
26. Rouillier, F.: Real root counting for some robotics problems. Solid Mech Appl. 40:73–82 (1995)
27. Rouillier, F.: Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux. PhD thesis, Université de Rennes I, may 1996
28. Traverso, C.: Groebner trace algorithm. Lecture Notes in Computer Science, 8:125–138 (1988)