

Duality methods for the membership problem

*Alicia M. Dickenstein** and *Carmen Sessa**

Effective methods in algebraic geometry (Castiglioncello, 1990),
 Progr. Math. **94**, Birkhäuser Boston, Boston, MA, (1991), 89–103.

Introduction

The classical problem of deciding membership to arbitrary polynomial ideals is EXPSPACE complete. Moreover, the problem of finding a representation of a polynomial by generators of a given ideal may involve doubly exponential (in the number of variables) degrees ([16]). The same difficulty arises when computing Gröebner bases of arbitrary polynomial ideals ([11]). This means that all known techniques to decide membership and to find representations of polynomials with respect to a given ideal lead to doubly exponential (sequential time) worst case complexities. However, if the geometry of the underlying algebraic variety is particularly simple, e.g. if the given ideal is zero dimensional or complete intersection, algorithms of considerably lower complexity can be found (see e.g. [7], [9]). The improvements are due to recent progress concerning affine versions of the effective Nullstellensatz (compare [18] and the references given there).

Using methods from residual duality theory, we show that some of the algorithmical problems arising frequently in computational algebraic geometry can be solved in simply exponential sequential and polynomial parallel time complexity.

Let K be a subfield of the complex numbers (e.g. $K = \mathbf{Q}$) and let z_1, \dots, z_n be indeterminates over \mathbf{C} . Let be given a finite set of polynomials $f_1, \dots, f_r \in K[z_1, \dots, z_n]$ with degrees bounded by $d \geq 3$, which generate an ideal $I := I(f_1, \dots, f_r)$.

Suppose first that f_1, \dots, f_r form a regular sequence. In this case we associated in [9] to the ideal I and to any natural number $k \in \mathbf{N}$, an $(O(k^n) + d^{O(n^2)}) \times O(k^n)$ matrix $S_{I,k}$ with entries from K which characterizes membership to I up to degree k in the following sense: a polynomial $p \in \mathbf{C}[z_1, \dots, z_n]$ of degree bounded by k belongs to I iff its coefficients vector is a solution of the homogeneous linear equations system corresponding to $S_{I,k}$.

The matrix $S_{I,k}$ can be computed from the inputs f_1, \dots, f_r by means of an arithmetical network over K of size $k^{O(n)} + d^{O(n^2)}$ and of depth $O(n^4 \log^2(k \cdot d))$ (see [10] for the notion of arithmetical network). In a more down to earth language we can say that $S_{I,k}$ is computable in sequential time $k^{O(n)} + d^{O(n^2)}$ and (simultaneously) in parallel time $O(n^4 \log^2(k \cdot d))$. We shall call an algorithm admissible if it is realizable by an arithmetical network within these time bounds. In the same sense we shall also speak about problems solvable and functions computable in admissible time (if necessary, we

* Research supported by CONICET and UBACYT, Argentina.

allow the sequential - and parallel - complexity to depend polynomially - or polylog - on the number r of generators).

In this paper, we compute in admissible time a matrix with entries from K which characterizes membership to the radical of I up to degree k . As a by-product of our method, we are able to compute in admissible time generators for the radical of I if an a priori degree bound of type $d^{O(n)}$ for them is given (this is the case if $r = n$, i.e. if I is a zero dimensional ideal. See Proposition 2.3 below).

Suppose now that I is a zero dimensional ideal (we don't need any more the hypothesis that f_1, \dots, f_r is a regular sequence). In this case, we are able to compute in admissible time matrices with entries from K which characterize membership to I and to its radical up to a given degree bound $k \in \mathbf{N}$. As mentioned, we are able to compute in admissible time generators for the radical of I .

Our algorithms are based on admissible time computations of ideal quotients of certain zero dimensional ideals. This is combined with ideas of "Zariski-Samuel duality" (see § 2 below) in order to transfer our results on complete intersection ideals to arbitrary zero dimensional ideals.

We want to put special emphasis on the method used in [9] and in this paper, which has its origins in the analytical theory of residues developed in [6], [8], [12].

The tools from residual duality theory we need for our computational applications are outlined in section 1. For residues and duality in the context of algebraic geometry we refer to [13], [15], and also to [1], where some applications are given.

There exists already considerably work with respect to simply exponential complexity bounds in computational algebraic geometry. Pioneering work was done e.g. in [14] (non-emptiness testing and dimension determination for projective varieties), in [5] (a sequential algorithm for decomposition of algebraic varieties into irreducible components) and in [4] (non-emptiness testing, dimension determination and zero dimensional equations solving for affine varieties).

In the case of computational commutative algebra much less is done with respect to non-homogeneous ideals and modules. Our aim is to demonstrate the power of residue theory and future possibilities of its application in Computer Algebra by the presentation of some new algorithms in computational commutative algebra obtained by means of this tool.

Let us also point out that the analytical theory of residues is closely connected to the first proof of an affine effective Nullstellensatz (cf. [3]). See also [2] for further applications of this technique).

We are grateful to Joos Heintz for his generosity to share his knowledge with us.

§ 0. Notations

. $\mathbf{C}[z]$ denotes always the polynomial ring in n variables $\mathbf{C}[z_1, \dots, z_n]$ and for any $k \in \mathbf{N}_0$, $\mathbf{C}[z]_k := \{f \in \mathbf{C}[z] / f = 0 \text{ or } \deg(f) \leq k\}$.

. n being fixed, we'll denote $dz = dz_1 \wedge \dots \wedge dz_n$.

. Let $x = (x_1, \dots, x_n) \in \mathbf{C}^n$ and $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbf{N}_0^n$. We denote $|\alpha| := \sum_{i=1}^n \alpha_i$

and $(z - x)^\alpha := \prod_{i=1}^n (z_i - x_i)^{\alpha_i}$.

. Unless otherwise stated, all the ideals considered lie in $\mathbf{C}[z]$. For any ideal I , we denote $Z(I) := \{x \in \mathbf{C}^n / f(x) = 0 \forall f \in I\}$.

. Let $f_1, \dots, f_r \in \mathbf{C}[z]$; $I(f_1, \dots, f_r)$ denotes the generated ideal $\left\{ \sum_{i=1}^r g_i \cdot f_i / g_i \in \mathbf{C}[z], i = 1, \dots, r \right\}$.

. For any ideal I , we denote $\text{rad}(I) := \{f \in \mathbf{C}[z] / f^m \in I \text{ for some } m \in \mathbf{N}\}$.

. Given $k \in \mathbf{N}$, an ideal I and a matrix S such that “ $P \in I \cap \mathbf{C}[z]_k \iff$ The vector of coefficients of P is a solution of $S \cdot \mathbf{X} = 0$ ”, we will say that $S \cdot \mathbf{X} = 0$ is a system of linear equations for $I \cap \mathbf{C}[z]_k$.

§ 1. Residual duality

§ 1.1. Local analytic residues

The local residue is a generalization of the Cauchy formula in several complex variables. It can be given the following analytic definition:

Let $x \in \mathbf{C}^n$ (or in an n -dimensional complex manifold), $f_{1_x}, \dots, f_{n_x} \in \mathcal{O}_x$ and let U be a ball centered at x such that there exist representatives $f_1, \dots, f_n \in \mathcal{O}(\bar{U})$ verifying $\bigcap_{i=1}^n (f_i = 0) = \{x\}$. For any meromorphic n -form ω in U having its poles on $\bigcup_{i=1}^n (f_i = 0)$, the residue of ω at x is the complex number

$$\text{Res}_x(\omega) = \frac{1}{(2\pi i)^n} \int_{\{z \in U / |f_j(z)| = \delta_j, 1 \leq j \leq n\}} \omega \quad (1.1.0)$$

for any $\delta_1 > 0, \dots, \delta_n > 0$ sufficiently small (cf [6]; [12], ch. 5).

This definition is of course independent of the neighborhood U chosen and of the special sequence $\mathbf{f} = \{f_1, \dots, f_n\}$ verifying the above hypotheses.

We can also think the residue of ω as an operator which assigns to any holomorphic germ $g \in \mathcal{O}_x$, the complex number $R_{\mathbf{f},x}[\omega](g) := \text{Res}_x(g \cdot \omega)$; that is, we have a \mathbf{C} -linear operator $R_{\mathbf{f},x} : \mathcal{O}_x \rightarrow \mathbf{C}$.

Suppose $\omega = \frac{h dz}{f_1 \dots f_n}$, $h_x \in \mathcal{O}_x$, and let $\{f'_{1_x}, \dots, f'_{n_x}\}$ be any regular sequence in the generated ideal $I_x := I(f_{1_x}, \dots, f_{n_x})$. The operator $R_{\mathbf{f},x}[\omega]$ can be expressed in terms of a sequence $\mathbf{f}' := \{f'_1, \dots, f'_n\}$ of representatives by means of the following Transformation Law:

$$R_{\mathbf{f},x}[\omega] = R_{\mathbf{f}',x} \left[\frac{\det A \cdot h dz}{f'_1 \dots f'_n} \right] \quad (1.1.1)$$

where $A = (a_{ij}) \in \mathcal{O}_x^{n \times n}$ and $f'_i = \sum_{j=1}^n a_{ij} f_j \quad \forall i = 1, \dots, n$ (for a proof, see [12], ch. 5).

The operator $R_{\mathbf{f},x}[\omega]$ is in fact a linear differential operator acting on \mathcal{O}_x ; more precisely, there exist $n_x \in \mathbf{N}_0$ and complex constants $(c_{\alpha,x}, \alpha \in \mathbf{N}_0^n, 0 \leq |\alpha| \leq n_x)$ such that for every $g \in \mathcal{O}_x$,

$$R_{\mathbf{f},x}[\omega](g) = \sum_{0 \leq |\alpha| \leq n_x} c_{\alpha,x} \cdot \frac{\partial^{|\alpha|}(g)}{\partial z_1^{\alpha_1} \dots \partial z_n^{\alpha_n}}(x) \quad (1.1.2)$$

This assertion can be easily deduced from the n -variable Cauchy formula and (1.1.1) by means of the local analytic Nullstellensatz, as follows: there exist $r = (r_1, \dots, r_n) \in \mathbf{N}^n$ and $A = (a_{ij}) \in \mathcal{O}_x^{n \times n}$ such that $(z_i - x_i)^{r_i} = \sum_{j=1}^n a_{ij} f_j$ for all $i = 1, \dots, n$. Then,

$$\begin{aligned} R_{\mathbf{f},x} \left[\frac{h dz}{f_1 \dots f_n} \right] (g) &= R_{\mathbf{z}-\mathbf{x},x} \left[\frac{\det A \cdot h dz}{(z_1 - x_1)^{r_1} \dots (z_n - x_n)^{r_n}} \right] (g) = \\ &= \frac{1}{\prod_j (r_j - 1)!} \frac{\partial^{|\mathbf{r}|-n}(\det A \cdot h \cdot g)}{\partial z_1^{r_1-1} \dots \partial z_n^{r_n-1}}(x). \end{aligned}$$

And so, the coefficients $c_{\alpha,x}$ can be precisely described in terms of the derivatives of $\det A \cdot h$ at x .

Suppose that $h = h_1 f_1$, $h_{1_x} \in \mathcal{O}_x$. Then, $\text{Res}_x \left(\frac{h dz}{f_1 \dots f_n} \right) = \text{Res}_x \left(\frac{h_1 dz}{f_2 \dots f_n} \right) = 0$ because the path of integration in (1.1.0) may, without crossing a singularity, be shrunk to a lower dimensional cycle by letting $\delta_1 \rightarrow 0$. Thus, by linearity, $\text{Res}_x \left(\frac{h dz}{f_1 \dots f_n} \right) = 0$ if $h_x \in I_x$. As an easy consequence, the operator $R_{\mathbf{f},x} \left[\frac{h dz}{f_1 \dots f_n} \right]$ is identically zero when $h_x \in I_x$. In fact, the converse to the latter statement is also true:

Local duality: Let f_{1_x}, \dots, f_{n_x} be a regular sequence in \mathcal{O}_x . With the above notations, we have the equivalence (cf [8], [12]):

$$h \in I_x \iff R_{\mathbf{f},x} \left[\frac{h dz}{f_1 \dots f_n} \right] \equiv 0 \quad (1.1.3)$$

Denote Ω^n the sheaf of holomorphic differential n -forms. One can compute the \mathcal{O}_x -module $\text{Ext}_{\mathcal{O}_x}^n(\mathcal{O}_x/I_x, \Omega_x^n)$ by means of the Koszul projective resolution of \mathcal{O}_x/I_x given

by the sequence f_{1_x}, \dots, f_{n_x} . So, one verifies that $\text{Ext}_{\mathcal{O}_x}^n(\mathcal{O}_x/I_x, \Omega_x^n) \simeq \Omega_x^n/I_x \cdot \Omega_x^n \simeq \mathcal{O}_x/I_x$.

This gives a more intrinsic formulation of the equivalence (1.1.3):

(1.1.4) The pairing

$$\text{res} : \mathcal{O}_x/I_x \otimes \text{Ext}_{\mathcal{O}_x}^n(\mathcal{O}_x/I_x, \Omega_x^n) \rightarrow \mathbf{C}$$

induced by

$$\text{res}(g, h) = R_{\mathbf{f}, x} \left[\frac{h dz}{f_1 \dots f_n} \right] (g)$$

is non-degenerated, and it is independent of the choice of the regular sequence of generators of I_x .

In the case of holomorphic regular sequences of any codimension p , one still has an explicit definition of a residual operator acting on \mathcal{C}^∞ compactly supported forms (i.e. a residual current) which generalizes the punctual residue ([6]). By computing $\text{Ext}_{\mathcal{O}_x}^p(\mathcal{O}_x/I_x, \Omega_x^n)$ via the injective resolution of the fibers Ω_x^n by means of the $\bar{\partial}$ -complex of currents $'D_x^n'$ for any x , these residual currents provide an explicit generalized local duality (cf. [8]).

§ 1.2. Polynomial residues

a) The 0-dimensional case.

Suppose we are given a regular sequence of n polynomials $\mathbf{q} = \{q_1, \dots, q_n\}$ in $\mathbf{C}[z]$. Denote Q the generated ideal $I(q_1, \dots, q_n)$ with finite zero set $Z(Q)$ in \mathbf{C}^n .

Grothendieck (see Hartshorne [13]) isolated the functorial aspects of the notion of local analytic residue, axiomatizing them and giving a definition of residues in a purely algebraic context. The residue is interpreted (in this particular case) as a morphism

$$\text{res} : \text{Ext}_{\mathbf{C}[z]}^n(\mathbf{C}[z]/Q, \Omega_{\mathbf{C}[z]/\mathbf{C}}^n) \rightarrow \mathbf{C}$$

(where $\Omega_{\mathbf{C}[z]/\mathbf{C}}^n$ denotes the Kähler module of relative differentials). To any $\omega \in \Omega_{\mathbf{C}[z]/\mathbf{C}}^n$ one may associate its Grothendieck residue symbol as follows: by means of the Koszul resolution of $\mathbf{C}[z]/Q$ given by the regular sequence $\{q_1, \dots, q_n\}$, we may identify $\text{Ext}_{\mathbf{C}[z]}^n(\mathbf{C}[z]/Q, \Omega_{\mathbf{C}[z]/\mathbf{C}}^n)$ with $\Omega_{\mathbf{C}[z]/\mathbf{C}}^n/Q \cdot \Omega_{\mathbf{C}[z]/\mathbf{C}}^n$. The symbol $\left[\begin{smallmatrix} \omega \\ q_1 \dots q_n \end{smallmatrix} \right]$ is just the image of ω in this last quotient.

Now we are going to explain how the local analytic residue can be combined with the Grothendieck approach to give an explicit polynomial residual duality.

(1.2.1) Given $p \in \mathbf{C}[z]$, denote $R_{\mathbf{q}}[p] : \mathbf{C}[z] \rightarrow \mathbf{C}$ the \mathbf{C} -linear operator

$$R_{\mathbf{q}}[p](g) := \sum_{x \in Z(Q)} R_{\mathbf{q}, x} \left[\frac{p dz}{q_1 \dots q_n} \right] (g).$$

Then, the residue morphism is explicitly given by

$$\text{res} \left(\begin{bmatrix} p \, dz \\ q_1 \dots q_n \end{bmatrix} \right) = R_{\mathbf{q}}[p](1) .$$

Moreover, the pairing

$$\text{Res} : \mathbf{C}[z]/Q \otimes \text{Ext}_{\mathbf{C}[z]}^n(\mathbf{C}[z]/Q, \Omega_{\mathbf{C}[z]/\mathbf{C}}^n) \longrightarrow \mathbf{C}$$

induced by

$$\left(g, \begin{bmatrix} p \, dz \\ q_1 \dots q_n \end{bmatrix} \right) \longmapsto R_{\mathbf{q}}[p](g)$$

is non-degenerated and independent of the choice of generators q_1, \dots, q_n of \mathbf{Q} .

The non-degeneracy of the bilinear map associated to Res can be deduced from the local analytic duality theory as follows:

Taking into account the description (1.1.2), it is easy to see that $R_{\mathbf{q}}[p] \equiv 0$ is equivalent to $R_{\mathbf{q},x}[p] \equiv 0 \quad \forall x \in Z(Q)$. By (1.1.3), this condition is equivalent to the local analytic membership $p_x \in Q_x \quad \forall x \in Z(Q)$, which by [17] is in turn equivalent to the local algebraic membership for any $x \in Z(Q)$. This is easily seen to be equivalent to the condition $p \in Q$ in $\mathbf{C}[z]$.

We know from (1.2.1) that $p \in Q$ iff $R_{\mathbf{q}}[p] \equiv 0$. Now, this latter condition can be effectively verified taking into account the following facts:

i) Given a polynomial $g \in \mathbf{C}[z]$, $R_{\mathbf{q}}[p][g]$ is effectively computable. (In fact, the resulting sequential time bounds are admissible, in the sense explained in the introduction). Moreover, if the coefficients of p, g and q_1, \dots, q_n lie in some subfield of \mathbf{C} , so does $R_{\mathbf{q}}[p](g)$ (cf. [9]).

ii) $R_{\mathbf{q}}[p] \equiv 0$ iff $R_{\mathbf{q}}[p](g) = 0$ for every $g \in \mathbf{C}[z]$ with $\deg(g) \leq \prod_{i=1}^n \deg(q_i) - 1$ (This can be seen considering the order of the differential operators $R_{\mathbf{q},x}[p]$ (cf.[9])).

Thus, the membership $p \in Q$ is equivalent to the condition that the vector of coefficients of p is a solution of a certain “residual” homogeneous linear system, which can be effectively computed in admissible time. More precisely, the following two conditions are equivalent for $p = \sum_{|\beta| \leq k} c_{\beta} z^{\beta}$:

- i) $p \in Q$
- ii) The vector of coefficients $(c_{\beta}, \beta \in \mathbf{N}_0^n, |\beta| \leq k)$ verifies the following linear system:

$$\sum_{\beta} c_{\beta} R_{\mathbf{q}}[z^{\beta}](z^{\alpha}) = 0, \quad |\alpha| \leq \prod_{i=1}^n \deg(q_i) - 1$$

Notice that the system has at most $\left(\prod_{i=1}^n \deg(q_i) \right)^n$ equations.

b) Regular sequences of arbitrary dimension.

Let $\mathbf{q} = \{q_1, \dots, q_r\}$, $r \leq n$, be a regular sequence of complex polynomials defining a complete intersection ideal $Q := I(q_1, \dots, q_r)$ in $\mathbf{C}[z]$.

Suppose that the linear projection $\pi : \mathbf{C}^n \rightarrow \mathbf{C}^{n-r}$, $\pi(z) = (z_{r+1}, \dots, z_n)$, restricted to $Z(Q)$ is proper and with finite fibers. Let $z' := (z_1, \dots, z_r)$ and $z'' := (z_{r+1}, \dots, z_n)$ be the vectors of the first r and of the last $n-r$ variables of $z = (z_1, \dots, z_n)$. Let x'' be a point of \mathbf{C}^{n-r} . The specialized polynomials $q_1(z', x''), \dots, q_r(z', x'')$ of $\mathbf{C}[z']$ define a complete intersection in $\pi^{-1}(x'')$, which is isomorphic to \mathbf{C}^r . So, we can apply to this context the punctual residue machinery of section a).

For $p \in \mathbf{C}[z]$, we denote by $R_{\mathbf{q}(z', x'')}[p(z', x'')]$ the residual operator acting on the fiber $\pi^{-1}(x'')$. Now let x'' vary over \mathbf{C}^{n-r} . One can show that for any $g \in \mathbf{C}[z']$, the mapping

$$\begin{aligned} R_{\pi, \mathbf{q}}[p](g) : \mathbf{C}^{n-r} &\longrightarrow \mathbf{C} \\ x'' &\longmapsto R_{\mathbf{q}(z', x'')}[p(z', x'')](g) \end{aligned}$$

is a polynomial function (depending on x'') which can be effectively computed in admissible time (cf. [9]).

If we think now $R_{\pi, \mathbf{q}}[p](g)$ as a polynomial in $\mathbf{C}[z'']$, the Grothendieck residue morphism

$$\text{Ext}_{\mathbf{C}[z]}^r(\mathbf{C}[z]/Q, \Omega_{\mathbf{C}[z]/\mathbf{C}[z'']}^r) \longrightarrow \mathbf{C}[z'']$$

is described by

$$\left[\begin{array}{c} p(z) dz' \\ q_1 \dots q_r \end{array} \right] \longmapsto R_{\pi, \mathbf{q}}[p](1)$$

and the explicit pairing

$$\left(g, \left[\begin{array}{c} p(z) dz' \\ q_1 \dots q_r \end{array} \right] \right) \longmapsto R_{\pi, \mathbf{q}}[p](g)$$

induces a residual pairing

$$R_{\pi} : \mathbf{C}[z]/Q \otimes \text{Ext}_{\mathbf{C}[z]}^r(\mathbf{C}[z]/Q, \Omega_{\mathbf{C}[z]/\mathbf{C}[z'']}^r) \longrightarrow \mathbf{C}[z'']$$

The task of determining whether $p \in Q$ is equivalent to the membership problem arising when we restrict all the polynomials to the fibers of π . Thus, the punctual duality (1.1.4) implies that this pairing R_{π} is also non-degenerated.

Due to the polynomial behaviour of the fibered residue, one can effectively construct, for any $k \in \mathbf{N}$, a system of linear equations for $Q \cap \mathbf{C}[z]_k$ (in the sense of § 0) in admissible time. In fact, the degree of the image polynomial $R_{\pi, \mathbf{q}}[p](g)$ is bounded by $\deg(g) + \deg(p) + rd^n(d^r + 1)$, where $d \in \mathbf{N}_{\geq 3}$ and $d \geq \deg(q_i) \quad \forall i = 1, \dots, r$. Detailed proofs are given in [9].

2. Zariski-Samuel duality

Let \mathcal{I}, \mathcal{Q} be ideals in a ring A . We denote, as usual, $(\mathcal{Q} : \mathcal{I})$ the quotient ideal $\{f \in A / f \cdot h \in \mathcal{Q} \quad \forall h \in \mathcal{I}\}$.

A careful reading of [19], ch.4, §16, reveals the following result: In case A is a local noetherian ring and \mathcal{Q} is an irreducible ideal belonging to the maximal ideal of A , for any ideal \mathcal{I} containing \mathcal{Q} it holds:

$$\mathcal{I} = (\mathcal{Q} : (\mathcal{Q} : \mathcal{I}))$$

We will refer to the above property as Zariski-Samuel local duality.

Proposition 2.1 (N. Coleff): *Let $x \in \mathbf{C}^n$ and let \mathcal{Q} be a complete intersection ideal in the local ring \mathcal{O}_x such that $\text{rad}(\mathcal{Q})$ is the maximal ideal. Then,*

$$(\mathcal{Q} : (\mathcal{Q} : \mathcal{I})) = \mathcal{I}$$

for any ideal \mathcal{I} in \mathcal{O}_x such that $\mathcal{I} \supseteq \mathcal{Q}$.

Proof: In view of the Zariski-Samuel local duality, it will be sufficient to show that \mathcal{Q} is an irreducible ideal in \mathcal{O}_x .

Let $\mathcal{J}ac := \det\left(\frac{\partial Q_i}{\partial z_j}\right)$ be the jacobian associated to some system of n generators $\{Q_1, \dots, Q_n\}$ of \mathcal{Q} and denote $\mathcal{J} := \langle \mathcal{Q}, \mathcal{J}ac \rangle$. Then, \mathcal{Q} is irreducible as an easy consequence of the following two statements:

- i) $\mathcal{J} \neq \mathcal{Q}$
- ii) For any ideal $\mathcal{J}' \supseteq \mathcal{Q}$, $\mathcal{J}' \supseteq \mathcal{J}$.

In order to prove i) and ii), we will use the local duality law (1.1.3): “ $\forall \varphi \in \mathcal{O}_x$, $\varphi \in \mathcal{Q} \iff R_{\mathcal{Q},x}[\varphi] \equiv 0$ ”.

For any $h \in \mathcal{O}_x$, $R_{\mathcal{Q},x}[\mathcal{J}ac](h) = c \cdot (2\pi i)^n h(x)$, where $c \in \mathbf{N}$ is the (non-vanishing) intersection number of $(Q_1 = 0), \dots, (Q_n = 0)$ at x (cf. [6], [12]). As $R_{\mathcal{Q},x}[\mathcal{J}ac] \neq 0$, we deduce that $\mathcal{J}ac \notin \mathcal{Q}$, proving i).

In order to see ii), let $f \in \mathcal{J}' - \mathcal{Q}$ and $A = \{g \in \mathcal{O}_x / g \cdot f \notin \mathcal{Q}\}$. Then, A is not empty (because $1 \in A$) and there exists $m \in \mathbf{N}$ such that $(z - x)^\alpha \notin A$, $\forall |\alpha| \geq m$ (because, by the local Hilbert Nullstellensatz, there exists $m \in \mathbf{N}$ such that $(z - x)^\alpha \in \mathcal{Q}$, $\forall |\alpha| \geq m$). Hence, there is an element $g \in A$ such that $(z_i - x_i) \cdot g \notin A$, for all $i = 1, \dots, n$ (i.e. $g \cdot f \notin \mathcal{Q}$ and $(z_i - x_i) \cdot g \cdot f \in \mathcal{Q}$ for all i).

The assumption $g \cdot f \notin \mathcal{Q}$ implies that $R_{\mathcal{Q},x}[g \cdot f] \neq 0$. For any $h \in \mathcal{O}_x$, we have

$$\begin{aligned} R_{\mathcal{Q},x}[g \cdot f](h) &= R_{\mathcal{Q},x}[g \cdot f]\left(h(x) + \sum_{i=1}^n (z_i - x_i) \cdot h_i(z)\right) = \\ &= h(x) \cdot R_{\mathcal{Q},x}[g \cdot f](1), \quad \text{and so } c_1 := R_{\mathcal{Q},x}[g \cdot f](1) \neq 0. \end{aligned}$$

Let's define $\psi := \frac{c}{c_1} \cdot g \cdot f - \mathcal{J}ac$; we deduce, by duality again, that $\psi \in \mathcal{Q}$ since $R_{\mathcal{Q},x}[\psi] \equiv 0$. In particular, $\psi \in \mathcal{J}'$, and so $\mathcal{J}ac \in \mathcal{J}'$. \diamond

Theorem 2.2: *Given a punctual complete intersection ideal $\mathcal{Q} \in \mathbf{C}[z]$,*

$$(\mathcal{Q} : (\mathcal{Q} : I)) = I$$

for any ideal I such that $I \supseteq Q$.

Proof: By the previous proposition, we only need to show that $(Q : I)_x = (Q_x : I_x)$, $\forall x \in \mathbf{C}^n$ (where for any polynomial ideal J , J_x denotes its image in the local ring \mathcal{O}_x).

The inclusion \subseteq is trivial. Suppose now $I = I(g_1, \dots, g_r)$ and $f \in (Q_x : I_x)$. For each $i = 1, \dots, r$, there exists $p_i \in \mathbf{C}[z]$ such that $p_i(x) \neq 0$ and $p_i \cdot f \cdot g_i \in Q$ (because $f \cdot g_i \in Q_x$). Therefore, $\prod_{i=1}^r p_i \cdot f \in (Q : I)$, i.e. $f \in (Q : I)_x$. \diamond

Proposition 2.3 and Remark 2.4 below will be useful in order to obtain an effective membership test for zero dimensional ideals:

Proposition 2.3: *Let Q be a zero dimensional ideal in $\mathbf{C}[z]$ and suppose $\deg(Q) \leq M$. Then, for any ideal J containing Q , there is a system of generators f_1, \dots, f_r of J such that $\deg(f_i) \leq M$, $\forall i = 1, \dots, r$.*

Proof: To avoid cumbersome notation, let's suppose that $Z(Q) = \{a, b\}$ and $\deg_a(Q) = n_a$, $\deg_b(Q) = n_b$ ($n_a + n_b \leq M$). Then, $(z - a)^\alpha \cdot (z - b)^\beta \in Q$, for any pair $\alpha, \beta \in \mathbf{N}_0^n$ such that $|\alpha| \geq n_a$ and $|\beta| \geq n_b$.

Given a polynomial $P \in \mathbf{C}[z]$, by iterated Taylor expansions around a and b , there exists constants c_α , $c_{\alpha\beta}$ and polynomials $P_{\alpha\beta}$ such that

$$\begin{aligned} P &= \sum_{|\alpha| < n_a} c_\alpha (z - a)^\alpha + \sum_{\substack{|\alpha| = n_a \\ |\beta| < n_b}} c_{\alpha\beta} (z - a)^\alpha \cdot (z - b)^\beta + \\ &+ \sum_{\substack{|\alpha| = n_a \\ |\beta| = n_b}} P_{\alpha\beta} \cdot (z - a)^\alpha \cdot (z - b)^\beta. \end{aligned}$$

That is, $P = P_1 + P_2$ with $\deg(P_1) < M$ and $P_2 \in I((z - a)^\alpha \cdot (z - b)^\beta, |\alpha| = n_a$ and $|\beta| = n_b) \subseteq Q \subseteq J$. Then, one can find a (finite) system of generators for J belonging to the set $\{f \in J / \deg(f) < M\} \cup \{(z - a)^\alpha \cdot (z - b)^\beta, |\alpha| = n_a$ and $|\beta| = n_b\} \subseteq \{f \in J / \deg f \leq M\}$. \diamond

Remark 2.4: Let $Q \subseteq \mathbf{C}[z]$ be an ideal. Suppose that for any $m \in \mathbf{N}$ we have a system of linear equations for $Q \cap \mathbf{C}[z]_m$ (in the sense of § 0), given by a matrix S_m .

Let $I = I(f_1, \dots, f_r)$ with $\deg(f_i) \leq D \quad \forall i = 1, \dots, r$. As $(Q : I) = \bigcap_{i=1}^r (Q : f_i)$, for any fixed $m \in \mathbf{N}$, $h \in (Q : I) \cap \mathbf{C}[z]_m \iff$ The vector of coefficients of $h \cdot f_i$ is a solution of $S_{m+D} \cdot \mathbf{X} = 0 \quad \forall i = 1, \dots, r$.

Now, let's call M_i the associated matrix (in the canonical basis of monomials) to the \mathbf{C} -linear mapping $\mathbf{C}[z]_m \rightarrow \mathbf{C}[z]_{m+D}$ given by $g \mapsto g \cdot f_i$. Therefore, $h \in (Q : I) \cap \mathbf{C}[z]_m \iff$ The vector of coefficients of h is a solution of $S_{m+D} \cdot M_i \cdot \mathbf{X} = 0 \quad \forall i = 1, \dots, r$.

Thus, we have a system of linear equations for $(Q : I) \cap \mathbf{C}[z]_m$. Clearly, the number of equations of this system is r times the number of equations of S_{m+D} .

§ 3. The membership problem in the case of a zero dimensional ideal

In this section, the duality properties of § 1 and § 2 will be our tools to design an admissible algorithm for zero dimensional ideals.

The **inputs** of the algorithm are:

– A set $\{f_1, \dots, f_r\}$ of polynomials in $\mathbf{C}[z]$ such that the generated ideal $I(f_1, \dots, f_r)$ is zero dimensional.

– $d \in \mathbf{N}_{\geq 3}$, $d \geq \deg(f_i) \quad \forall i = 1, \dots, r$.

– $k \in \mathbf{N}$.

The **output** of the algorithm is a matrix S with $\binom{n+k}{n}$ columns and at most $(d+1)^{2n^2}$ rows, satisfying:

– For any complex polynomial $P = \sum_{|\beta| \leq k} c_\beta z^\beta$, $P \in I$ iff the vector of coefficients

(c_β) is a solution of the linear system $S \cdot \mathbf{X} = 0$.

– The entries of S can be computed in simply exponential in n (and polynomial in d and r) time.

– If $f_1, \dots, f_r \in K[X_1, \dots, X_n]$ for some subfield K of \mathbf{C} , the entries of S also belong to K .

The sketch of the algorithm is as follows:

First step: Find $q_1, \dots, q_n \in \mathbf{C}[z]$ such that:

i) $Q := I(q_1, \dots, q_n) \subseteq I$

ii) $\{q_1, \dots, q_n\}$ is a regular sequence

iii) $\deg(q_i) \leq d \quad \forall i = 1, \dots, n$.

The polynomials q_1, \dots, q_n can be effectively found in admissible time, by taking linear combinations of the data f_1, \dots, f_r of the form $f_1 + \gamma f_2 + \gamma^2 f_3 + \dots + \gamma^{r-1} f_r$, with γ varying in any finite set $\Gamma \subseteq \mathbf{C}$ with at least $r \cdot d^n$ elements. A complete proof can be given combining the following three ingredients: a) the proof of Prop. 3 in: Heintz, J.: Definability and Fast Quantifier Elimination in Algebraically Closed Fields. Theoretical Computer Science 24 (1983), 239-277; b) lemma 2.42 in: Giusti, M. and Heintz, J.: Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. Submitted to MEGA 90; and c) Corollary (1.9.1) in [7] (for the bounds in computing the dimension of the ideal generated by a given sequence of linear combinations).

Second step: Find the matrix S' of a system of linear equations for

$Q \cap \mathbf{C}[z]_{d^n + \max\{k, d\}}$.

The matrix S' can be effectively constructed (see § 1.2 a)) since Q is a complete intersection ideal.

Third step: Find the matrix S'' of a system of linear equations for $(Q : I) \cap \mathbf{C}[z]_{d^n}$.

Following Remark 2.4, one can obtain S'' from S' since $Q \subseteq (Q : I)$.

Fourth step: Find a system of generators h_1, \dots, h_s of $(Q : I)$.

By Proposition 2.3, it is enough to find a \mathbf{C} -basis $\{h_1, \dots, h_s\}$ of the space of solutions of the system $S'' \cdot \mathbf{X} = 0$ constructed in the third step.

Notice that $\deg(h_i) \leq d^n \ \forall i = 1, \dots, n$ and $s \leq \dim \mathbf{C}[z]_{d^n} = \binom{d^n+n}{n}$.

Fifth step: Find the matrix S of a system of linear equations for $I \cap \mathbf{C}[z]_k$.

By Theorem 2.2, we know that $I = (Q : (Q : I))$. Moreover, by the fourth step, we have generators $\{h_1, \dots, h_s\}$ of $(Q : I)$ with degrees bounded by d^n . So, we can construct S from S' (obtained in the second step), following again Remark 2.4.

§ 4. Dealing with radicals

4.1. Complete intersections

Given a complete intersection ideal Q in $\mathbf{C}[z]$ and $k \in \mathbf{N}$, we will show how to construct a linear system for $\text{rad}(Q) \cap \mathbf{C}[z]_k$ in admissible time.

We first need the following result:

Theorem 4.1.1: Let $Q = I(Q_1, \dots, Q_p)$ be a complete intersection ideal ($\dim Q = n - p$). Let \mathcal{A} denote the set of all increasing sequences A of p indexes $1 \leq A_1 < A_2 < \dots < A_p \leq n$, and for each $A \in \mathcal{A}$, let's call $M_A := \det \left(\frac{\partial Q_i}{\partial z_{A_j}} \right)_{1 \leq i, j \leq p}$. Then, for any $f \in \mathbf{C}[z]$,

$$f \in \text{rad}(Q) \iff f \cdot M_A \in Q, \quad \forall A \in \mathcal{A}.$$

In the particular case $\dim Q = 0$,

$$f \in \text{rad}(Q) \iff f \cdot \text{Jac} \in Q$$

(where $\text{Jac} := \det \left(\frac{\partial Q_i}{\partial z_j} \right)_{1 \leq i, j \leq n}$).

Proof: The proof is based on the two following facts:

i) There is a well defined residual current acting on $(n - p, n - p)$ compactly supported \mathcal{C}^∞ forms

$$\text{Res} \left[\frac{dQ_1 \wedge \dots \wedge dQ_p}{Q_1 \dots Q_p} \right] \equiv \frac{1}{(2\pi i)^p} \int_{[Q^{-1}(0)]} \quad (\text{cf. [6]}),$$

where $[Q^{-1}(0)]$ denotes the intersection cycle (with integer multiplicities along each irreducible component).

ii) The generalized duality results ([8]) give in particular:

$$f \cdot \text{Res} \left[\frac{dQ_1 \wedge \dots \wedge dQ_p}{Q_1 \dots Q_p} \right] \equiv 0 \iff f \cdot dQ_1 \wedge \dots \wedge dQ_p \in Q \cdot \Omega^p(\mathbf{C}^n).$$

Then,

$$\begin{aligned} f \cdot M_A \in Q, \quad \forall A \in \mathcal{A} &\iff f \cdot dQ_1 \wedge \dots \wedge dQ_p \in Q \cdot \Omega^p(\mathbf{C}^n) \\ &\iff f \cdot \text{Res} \left[\frac{dQ_1 \wedge \dots \wedge dQ_p}{Q_1 \dots Q_p} \right] \equiv \frac{1}{(2\pi i)^p} \int_{[Q^{-1}(0)]} f \wedge \cdot \equiv 0 \iff \\ f|_{Z(Q)} &\equiv 0 \iff f \in \text{rad}(Q). \quad \diamond \end{aligned}$$

Remark 4.1.2: Suppose that the linear projection $\pi : Z(Q) \longrightarrow \mathbf{C}^{n-p}$, $\pi(z) = (z_1, \dots, z_{n-p})$ has finite fibers, and let $A_0 := (n-p+1, n-p+2, \dots, n)$. Then, the conditions $f \cdot M_A \in Q$, $\forall A \in \mathcal{A}$ (in the above theorem) can be replaced by the single condition $f \cdot M_{A_0} \in Q$ (cf. [8], §4). In fact, one can always effectively find a system of coordinates x in “Noether position” for Q (for which $\pi' : Z(Q) \longrightarrow \mathbf{C}^{n-p}$, $\pi'(x) = (x_1, \dots, x_{n-p})$ has finite fibers) (cf. [7], §1).

4.1.3. The algorithm

INPUTS:

- $Q_1, \dots, Q_p \in \mathbf{C}[z]$ ($p \leq n$) defining a complete intersection ideal Q .
- $d_1, \dots, d_p \in \mathbf{N}$ verifying $d_i = \deg(Q_i) \quad \forall i = 1, \dots, p$.
- $k \in \mathbf{N}$.

OUTPUTS:

A matrix S verifying:

- i) S is the matrix of a system of linear equations for $\text{rad}(Q) \cap \mathbf{C}[z]_k$.
- ii) S has at most $\left(k + \prod_{i=1}^p d_i + p \cdot d^n (d^p + 1) + \sum_{i=1}^p (d_i - 1) \right)^{n-p} \cdot \left(\prod_{i=1}^p d_i \right)^n$ rows (and $\binom{k+n}{n}$ columns), where $d \in \mathbf{N}_{\geq 3}$ and $d \geq \deg(Q_i) \quad \forall i = 1, \dots, p$.

First step: Find a system of linear equations $S' \cdot \mathbf{X} = 0$ for $Q \cap \mathbf{C}[z]_{k + \sum_{i=1}^p (d_i - 1)}$.

Second step: Find a system of linear equations $S \cdot \mathbf{X} = 0$ for $\text{rad}(Q) \cap \mathbf{C}[z]_k$.

S can be obtained from S' following the Remark 2.4, because by theorem 4.1.1 $\text{rad}(Q) = (Q : I(M_A, A \in \mathcal{A}))$.

We refer to [9] for the construction of S' and the bounds in ii).

4.2. The zero dimensional case

Given an arbitrary zero dimensional ideal $I = I(f_1, \dots, f_r)$ and $k \in \mathbf{N}$, we will show in 4.2.3 how to construct a linear system for $\text{rad}(Q) \cap \mathbf{C}[z]_k$ in admissible time. As a consequence, we will have an effective method to find a system of generators of $\text{rad}(I)$ in admissible time.

Proposition 4.2.1: *Let J be a zero dimensional radical ideal. For any ideal I verifying $J \subseteq \text{rad}(I)$,*

$$\text{rad}(I) = (J : (J : I)) .$$

Proof: Let $x \in \mathbf{C}^n$ and denote \mathcal{M}_x the maximal ideal in \mathcal{O}_x .

In case $x \in Z(I)$, $I_x \subseteq \mathcal{M}_x$ and by the assumptions on J , $J_x = \mathcal{M}_x$. So

$$(J : (J : I))_x = (J_x : (J_x : I_x)) = (\mathcal{M}_x : \mathcal{O}_x) = \mathcal{M}_x = \text{rad}(I)_x .$$

In case $x \notin Z(I)$, $I_x = \mathcal{O}_x$ and so

$$(J_x : (J_x : I_x)) = (J_x : J_x) = \mathcal{O}_x = \text{rad}(I)_x . \quad \diamond$$

Remark 4.2.2: Let $Q = I(Q_1, \dots, Q_n)$ be a zero dimensional complete intersection ideal. By Theorem 4.1.1, $\text{rad}(Q) = (Q : \text{Jac})$. Then, for any ideal $I = I(f_1, \dots, f_r)$, $(\text{rad}(Q) : I) = (Q : I(f_1 \cdot \text{Jac}, \dots, f_r \cdot \text{Jac}))$.

4.2.3. The algorithm

INPUTS:

- $f_1, \dots, f_r \in \mathbf{C}[z]$ defining a zero dimensional ideal I .
- $d \in \mathbf{N}_{\geq 3}$, $d \geq \deg(f_i) \quad \forall i = 1, \dots, r$.
- $k \in \mathbf{N}$.

OUTPUT:

A matrix S verifying:

- i) S is the matrix of a system of linear equations for $\text{rad}(I) \cap \mathbf{C}[z]_k$.
- ii) S has at most $(d+1)^{2n^2}$ rows (and $\binom{k+n}{n}$ columns).

First step: *Same as first step in the algorithm in § 3.*

Second step: *Find the matrix S' of a system of linear equations for $Q \cap \mathbf{C}[z]_{d^n + n(d-1) + \max\{k, d\}}$.*

Third step: Find the matrix S'' of a system of linear equations for $(\text{rad}(Q) : I) \cap \mathbf{C}[z]_{d^n}$.

Following Remark 2.4, one can obtain S'' from S' since $(\text{rad}(Q) : I) = (Q : I(f_1 \cdot \text{Jac}, \dots, f_r \cdot \text{Jac}))$ by Remark 4.2.2.

Fourth step: Find a system of generators h_1, \dots, h_s of $(\text{rad}(Q) : I)$.

As $Q \subseteq (\text{rad}(Q) : I)$ and $\deg(Q) \leq d^n$, it is enough to find a \mathbf{C} -basis h_1, \dots, h_s of solutions of the system $S'' \cdot \mathbf{X} = 0$ constructed in the third step (by Proposition 2.3).

Notice that $\deg(h_i) \leq d^n$ and $s \leq \binom{d^n+n}{n}$.

Fifth step: Find the matrix S of a system of linear equations for $\text{rad}(I) \cap \mathbf{C}[z]_k$.

By Proposition 4.2.1, $\text{rad}(I) = (\text{rad}(Q) : (\text{rad}(Q) : I))$. Moreover, by Remark 4.2.2,

$$\text{rad}(I) = (Q : I(h_1 \cdot \text{Jac}, \dots, h_s \cdot \text{Jac})) .$$

Consequently, S can be constructed from the matrix S' found in the second step, following Remark 2.4.

4.2.4. Generators of $\text{rad}(I)$

In case $I = I(f_1, \dots, f_r)$ is a zero dimensional ideal with $\deg(f_i) \leq d \ \forall i = 1, \dots, r$, there exists (by Proposition 2.3) a system of generators of $\text{rad}(I)$ with degrees bounded by d^n .

Let $k = d^n$ and S the corresponding output of the algorithm described in 4.2.3. Then, a \mathbf{C} -basis of solutions of $S \cdot \mathbf{X} = 0$ provides a system of generators of $\text{rad}(I)$.

References.

- [1] Angeniol, B.: Résidus et Effectivité. Preprint (1983).
- [2] Berenstein, C., Yger, A.: Bounds for the degrees in the division problem. Preprint Univ. of Maryland (1989).
- [3] Brownawell, W.D.: Bounds for the degrees in the Nullstellensatz. Annals of Math. 126 (1987), 577-591.
- [4] Caniglia, L., Galligo, A., Heintz, J.: Some new effectivity bounds in Computational Geometry. Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proc. 6th Int'l Conf., Rome 1988 (Ed. T.Mora), Springer LN Comput. Sci. 357 (1989), 131-151.
- [5] Chistov, A.L., Grigor'ev, D.Yu.: Subexponential time solving systems of algebraic equations. LOMI preprints E-9-83 E-10-83, Leningrad (1983).
- [6] Coleff, N., Herrera, M.: Les Courants Résiduels Associés à une Forme Meromorphe. Springer LN Math. 633 (1978).

- [7] Dickenstein, A., Fitchas, N., Giusti, M., Sessa, C.: The membership problem for unmixed polynomial ideals is solvable in single exponential time. To appear in: Discrete Applied Algebra, Proc. AAEECC-7, Toulouse 1989.
- [8] Dickenstein, A., Sessa, C.: Canonical Representatives in Moderate Cohomology. Invent. Math. 80 (1985), 417-434.
- [9] Dickenstein, A., Sessa, C.: An Effective Residual Criterion for the Membership Problem in $\mathbf{C}[z_1, \dots, z_n]$, Journal of Pure and Applied Algebra (to appear).
- [10] von zur Gathen, J.: Parallel arithmetic computations. A survey. Proc. 13th Symp. MFCS 1986, Springer LN Comput. Sci. 233 (1986), 93-112.
- [11] Giusti, M.: Complexity of standard bases in projective dimension zero. Preprint Ecole Polytechnique Paris (1987).
- [12] Griffiths, P., Harris, J.: Principles of Algebraic Geometry. John Wiley & Sons, 1978.
- [13] Hartshorne, R.: Residues and Duality. Springer L.N. Math. 20 (1966).
- [14] Lazard, D.: Algèbre linéaire sur $K[x_1, \dots, x_n]$ et élimination. Bull. Soc. Math. France 105 (1977), 165-190.
- [15] Lipman, J.: Dualizing sheaves, differentials and residues on algebraic varieties. Astérisque 117 (1984).
- [16] Mayr, E., Meyer, A.: The complexity of the word problem for commutative semigroups and polynomial ideals. Advances in Math. 46 (1982), 305-329.
- [17] Serre, J.P.: G.A.G.A., Annales de l'Institut Fourier, Tome VI (1956), 1-42.
- [18] Teissier, B.: Résultats récents d'algèbre commutative effective. Séminaire Bourbaki, 42ème année, 1989-90, n° 718, 1-19.
- [19] Zariski, O., Samuel, P.: Commutative Algebra, Vol. 1. Van Nostrand, New York, 1958.

Alicia Dickenstein - Carmen Sessa
 Departamento de Matemática - FCEyN
 Universidad de Buenos Aires
 Ciudad Universitaria - Pabellón I
 (1428) Buenos Aires, Argentina.
 alidick@mate.edu.ar
 banyc!atina!dcfcen!mate!pirata@uunet.UU.NET