

Deflation and Certified Isolation of Singular Zeros of Polynomial Systems

Angelos Mantzaflaris, Bernard Mourrain

► **To cite this version:**

Angelos Mantzaflaris, Bernard Mourrain. Deflation and Certified Isolation of Singular Zeros of Polynomial Systems. A. Leykin. International Symposium on Symbolic and Algebraic Computation (ISSAC), Jun 2011, San Jose, CA, United States. ACM New York, pp.249-256, 2011, Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation. <10.1145/1993886.1993925>. <inria-00556021>

HAL Id: inria-00556021

<https://hal.inria.fr/inria-00556021>

Submitted on 14 Jan 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Deflation and Certified Isolation of Singular Zeros of Polynomial Systems

Angelos Mantzaflaris and Bernard Mourrain
GALAAD, INRIA Méditerranée
BP 93, 06902 Sophia Antipolis, France
[FirstName.LastName]@inria.fr

ABSTRACT

We develop a new symbolic-numeric algorithm for the certification of singular isolated points, using their associated local ring structure and certified numerical computations. An improvement of an existing method to compute inverse systems is presented, which avoids redundant computation and reduces the size of the intermediate linear systems to solve. We derive a one-step deflation technique, from the description of the multiplicity structure in terms of differentials. The deflated system can be used in Newton-based iterative schemes with quadratic convergence. Starting from a polynomial system and a small-enough neighborhood, we obtain a criterion for the existence and uniqueness of a singular root of a given multiplicity structure, applying a well-chosen symbolic perturbation. Standard verification methods, based eg. on interval arithmetic and a fixed point theorem, are employed to certify that there exists a unique perturbed system with a singular root in the domain. Applications to topological degree computation and to the analysis of real branches of an implicit curve illustrate the method.

Categories and Subject Descriptors

G.1.5 [Mathematics of Computing]: Roots of Nonlinear Equations; I.1.2 [Computing Methodologies]: Symbolic and Algebraic Manipulation—*Algebraic algorithms*

General Terms

Algorithms, Theory

Keywords

root deflation, multiplicity structure, dual space, inverse system, isolated point

1. INTRODUCTION

A main challenge in algebraic and geometric computing is singular point identification and treatment. Such problems naturally occur when computing the topology of implicit curves or surfaces [1], the intersection of parametric

surfaces in geometric modeling. When algebraic representations are used, this reduces to solving polynomial systems. Several approaches are available: algebraic techniques such as Gröbner bases or border bases, resultants, subdivision algorithms [10], [13], homotopies, and so on. At the end of the day, a numerical approximation or a box of isolation is usually computed to characterize the (real) roots of the polynomial system. But we often need to improve the numerical approximation of the roots. Numerical methods such that Newton's iteration can be used to improve the quality of the approximation, provided that we have a simple root. In the presence of a multiple root, the difficulties are significantly increasing. The numerical approximation can be of very bad quality, and the methods used to compute this approximation are converging slowly (or not converging). The situation in practical problems, as encountered in CAGD for instance, is even worse, since the coefficients of the input equations are known, with some incertitude. Computing multiple roots of approximate polynomial systems seems to be an ill-posed problem, since changing slightly the coefficients may transform a multiple root into a cluster of simple roots (or even make it disappear).

To tackle this difficult problem, we adopt the following strategy. We try to find a (small) perturbation of the input system such that the root we compute is an exact multiple root of this perturbed system. In this way, we identify the multiplicity structure and we are able to setup deflation techniques which restore the quadratic convergence of the Newton system. The certification of the multiple root is also possible on the symbolically perturbed system by applying a fixed point theorem, based eg. on interval arithmetic [16] or α -theorems [17].

Related work. In order to be develop Newton-type methods that converge to multiple roots, deflation techniques which consist in adding new equations in order to reduce the multiplicity have already been considered. In [14], by applying a triangulation preprocessing step on the Jacobian matrix at the approximate root, minors of the Jacobian matrix are added to the system to reduce the multiplicity.

In [6], a presentation of the ideal in a triangular form in a good position and derivations with respect to the leading variables are used to iteratively reduce the multiplicity. This process is applied for p-adic lifting with exact computation.

In [7, 8], instead of triangulating the Jacobian matrix, the number of variables is doubled and new equations are introduced, which are linear in the new variables. They describe the kernel of the Jacobian matrix at the multiple root.

In [3], this construction is related to the construction of

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 200X ACM X-XXXXX-XX-X/XX/XX ...\$5.00.

the inverse system. The dialytic method of F.S. Macaulay [9] is revisited for this purpose. These deflation methods are applied iteratively until the root becomes regular, doubling each time the number of variables.

More recent algorithms for the construction of inverse systems are described eg. in [11], reducing the size of the intermediate linear systems (and exploited in [18]), or in [12] using an integration method.

In [15], a minimization approach is used to reduce the value of the equations and their derivatives at the approximate root, assuming a basis of the inverse system is known.

In [20], the inverse system is constructed via Macaulay's method; tables of multiplications are deduced and their eigenvalues are used to improve the approximated root. It is proved that the convergence is quadratic when the Jacobian has corank 1 at the multiple root.

Verification of multiple roots of (approximate) polynomial equations is a difficult task. The approach proposed in [16] consists in introducing perturbation parameters and to certifying the multiple root of nearby system by using a fixed point theorem, based on interval arithmetic. It applies only to cases where the Jacobian has corank equal to 1.

The univariate case. In preparation for the multivariate case, we review some techniques used to treat singular zeros of univariate polynomials, and we present our method on a univariate instance.

Let $g(x) \in \mathbb{K}[x]$ be a polynomial which attains at $x = 0$ a root of multiplicity $\mu > 1$. The latter is defined as the smallest positive integer μ such that $d^\mu g(0) \neq 0$ whereas $g(0) = dg(0) = \dots = d^{\mu-1}g(0) = 0$. Here we denote $d^k g(x) = \frac{d^k}{dx^k} g(x)/k!$ the normalized k -th order derivative.

We see that $\mathcal{D}_0 = \langle 1, d^1, \dots, d^{\mu-1} \rangle$ is the maximal space of differentials which is stable under derivation, that vanish when applied to members of \mathcal{Q}_0 , the $\langle x \rangle$ -primary component of $\langle g \rangle$ at $x = 0$. Consider now the symbolically perturbed equation

$$f_1(x, \varepsilon) = g(x) + \varepsilon_1 + \varepsilon_2 x + \dots + \varepsilon_{\mu-2} x^{\mu-2} \quad (1)$$

and apply every basis element of \mathcal{D}_0 to arrive to the new system $\mathbf{f}(x, \varepsilon) = (f_1, d_1 f_1, \dots, d^{\mu-1} f_1)$ in $\mu-1$ variables. The i -th equation shall be $f_i = d^{i-1} f_1 = d^{i-1} g + \sum_{k=i}^{\mu-2} x^{k-i+1} \varepsilon_k$, i.e. linear in ε , the last one being $f_\mu = d^{\mu-1} g(x)$. This system deflates the root, as we see that the determinant of its Jacobian matrix at $(0, \mathbf{0})$ is

$$\det J_{\mathbf{f}}(0, \mathbf{0}) = \left| \begin{array}{c|cc} \frac{d}{dx} f_1 & 1 & 0 \\ \vdots & \ddots & \\ \frac{d}{dx} f_{\mu-1} & 0 & 1 \\ \hline \frac{d}{dx} f_\mu & 0 & 0 \end{array} \right| = -\mu d f_\mu(0, \mathbf{0}) = -\mu d^\mu g(0) \neq 0.$$

Now suppose that ζ^* is an approximate zero, close to $x = \zeta$. We can still compute \mathcal{D}_ζ by evaluating $g(x)$ and the derivatives up to a threshold relative to the error in ζ^* . Then we can form (1) and use verification techniques to certify the root. Checking that the Newton operator is contracting shows the existence and unicity of a multiple root in a neighborhood of the input data. We are going to extend this approach, described in [16], to multi-dimensional isolated multiple roots.

Our approach. It consists of the following steps:

(a) Compute a basis for the dual space and of the local quotient ring at a given (approximate) singular point.

(b) Deflate the system by augmenting it with new equations derived from the dual basis, introducing adequate perturbation terms.

(c) Certify the singular point and its multiplicity structure for the perturbed system checking the contraction property of Newton iteration (eg. via interval arithmetic).

In step (a), a dual basis at the singular point is computed by means of linear algebra, based on the integration approach of [12]. We describe an improvement of this method, which yields directly a triangular dual basis with no redundant computation. This method has the advantage to reduce significantly the size of the linear systems to solve at each step, compared to Macaulay's type methods [9, 7, 8, 3]. In the case of an approximate singular point, errors are introduced in the coefficients of the basis elements. Yet a successful computation is feasible. In particular, the support of the basis elements is revealed by this approximate process.

In the deflation step (b), new equations and new variables are introduced in order to arrive to a new polynomial system where the singularity is obviated. The new variables correspond to perturbations of the initial equations along specific polynomials, which form a dual counterpart to the basis of the dual space. One of the deflated systems that we compute from the dual system is a square $n \times n$ system with a simple root. This improves the deflation techniques described in [7, 8, 3], which require additional variables and possibly several deflation steps. New variables are introduced only in the case where we want to certify the multiplicity structure. The perturbation techniques that we use extend the approach of [16] to general cases where the co-rank of the Jacobian matrix could be bigger than one. The verification step (c) is mostly a contraction condition, using eg. techniques as in [16]. This step acts on the (approximate) deflated system, since verifying a simple solution of the deflated system induces a certificate of an exact singular point of (a nearby to) the initial system.

We are going to detail the different steps in the following sections, starting with notations in Sect. 2, dual basis in Sect. 3, deflation in Sect. 4, and certification in Sect. 5. In the last section, we will show examples and applications to the topology analysis of curves.

2. PRELIMINARIES AND MAIN RESULTS

We denote by $R = \mathbb{K}[\mathbf{x}]$ a polynomial ring over the field \mathbb{K} of characteristic zero. Also, the *dual ring* R^* is the space of linear functionals $\Lambda : R \rightarrow \mathbb{K}$. It is commonly identified as the space of formal series $\mathbb{K}[[\partial]]$ where $\partial = (\partial_1, \dots, \partial_n)$ are formal variables. Thus we view dual elements as formal series in differential operators at a point $\zeta \in \mathbb{K}^n$. To specify that we use the point ζ , we also denote these differentials ∂_ζ . When applying $\Lambda(\partial_\zeta) \in \mathbb{K}[[\partial_\zeta]]$ to a polynomial $g(\mathbf{x}) \in R$ we will denote by $\Lambda^\zeta[g] = \Lambda^\zeta g = \Lambda(\partial_\zeta)[g(\mathbf{x})]$ the operation

$$\Lambda^\zeta[g] = \sum_{\alpha \in \mathbb{N}^n} \frac{\lambda_\alpha}{\alpha_1! \dots \alpha_n!} \cdot \frac{d^{|\alpha|} g}{d_1^{\alpha_1} \dots d_n^{\alpha_n}}(\zeta), \quad (2)$$

for $\Lambda(\partial_\zeta) = \sum \lambda_\alpha \frac{1}{\alpha!} \partial_\zeta^\alpha \in \mathbb{K}[[\partial_\zeta]]$. Extending this definition to an ordered set $\mathcal{D} = (\Lambda_1, \dots, \Lambda_\mu) \in \mathbb{K}[[\partial]]^\mu$, we shall denote $\mathcal{D}^\zeta[g] = (\Lambda_1^\zeta g, \dots, \Lambda_\mu^\zeta g)$. In some cases, it is convenient to use normalized differentials instead of ∂ : for any $\alpha \in \mathbb{N}^n$, we denote $d_\zeta^\alpha = \frac{1}{\alpha!} \partial_\zeta^\alpha$. When $\zeta = \mathbf{0}$, we have $d_\mathbf{0}^\alpha \mathbf{x}^\beta = 1$

if $\alpha = \beta$ and 0 otherwise. More generally, $(\mathbf{d}_\zeta^\alpha)_{\alpha \in \mathbb{N}^n}$ is the dual basis of $((\mathbf{x} - \zeta)^\alpha)_{\alpha \in \mathbb{N}^n}$.

For $\Lambda \in R^*$ and $p \in R$, let $p \cdot \Lambda : q \mapsto \Lambda(pq)$. We check that

$$(x_i - \zeta_i) \cdot \partial_\zeta^\alpha = \frac{d}{d\partial_{i,\zeta}}(\partial_\zeta^\alpha). \quad (3)$$

This property shall be useful in the sequel.

2.1 Isolated points and differentials

Let $\langle \mathbf{f} \rangle = \langle f_1, \dots, f_s \rangle$ be an ideal of R , $\zeta \in \mathbb{K}$ a root of \mathbf{f} and $m_\zeta = \langle x_1 - \zeta_1, \dots, x_n - \zeta_n \rangle$ the maximal ideal at ζ . Suppose that ζ is an isolated root of \mathbf{f} , then a minimal primary decomposition of $\mathcal{I} = \bigcap_{\mathcal{Q} \text{ prim. } \supset \mathcal{I}} \mathcal{Q}$ contains a primary

component \mathcal{Q}_ζ such that $\sqrt{\mathcal{Q}_\zeta} = m_\zeta$ and $\sqrt{\mathcal{Q}'} \not\subset m_\zeta$ for the other primary components \mathcal{Q}' associated to \mathcal{I} [2].

As $\sqrt{\mathcal{Q}_\zeta} = m_\zeta$, R/\mathcal{Q}_ζ is a finite dimensional vector space. The multiplicity μ_ζ of ζ is defined as the dimension of R/\mathcal{Q}_ζ . A point of multiplicity one is called regular point, or simple root, otherwise we say that ζ is a singular isolated point, or multiple root of \mathbf{f} . In the latter case we have $J_{\mathbf{f}}(\zeta) = 0$.

We can now define the dual space of an isolated point.

DEFINITION 2.1. *The dual space of \mathcal{I} is the subspace of elements of $\mathbb{K}[[\partial_\zeta]]$ that vanish on all the elements of \mathcal{I} . It is also called the orthogonal of \mathcal{I} and denoted by \mathcal{I}^\perp .*

Consider now the orthogonal of \mathcal{Q}_ζ , i.e. the subspace \mathcal{D}_ζ of elements of R^* that vanish on members of \mathcal{Q}_ζ , namely

$$\mathcal{Q}_\zeta^\perp = \mathcal{D}_\zeta = \{\Lambda \in R^* : \Lambda^\zeta[p] = 0, \forall p \in \mathcal{Q}_\zeta\}.$$

The following lemma is an essential property that allows extraction of the local structure \mathcal{D}_ζ directly from the ‘‘global’’ ideal $\mathcal{I} = \langle \mathbf{f} \rangle$, notably by matrix methods outlined in Sect. 3.

PROPOSITION 2.2 ([12, Th. 8]). *For any isolated point $\zeta \in \mathbb{K}$ of \mathbf{f} , we have $\langle \mathbf{f} \rangle^\perp \cap \mathbb{K}[[\partial_\zeta]] = \mathcal{D}_\zeta$.*

In other words, we can identify $\mathcal{D}_\zeta = \mathcal{Q}_\zeta^\perp$ with the space of polynomial differential operators that vanish at ζ on every element of \mathcal{I} .

The space \mathcal{D}_ζ is a vector space of polynomials in ∂_ζ dimension μ_ζ , the multiplicity of ζ . As the variables $(x_i - \zeta_i)$ act on R^* as derivations (see (3)), \mathcal{D}_ζ is a space of differential polynomials in ∂_ζ , which is stable by derivation. This property will be used explicitly in constructing \mathcal{D}_ζ (Sec. 3).

DEFINITION 2.3. *The nilindex of \mathcal{Q}_ζ is the maximal integer $N \in \mathbb{N}$ s.t. $m_\zeta^N \not\subset \mathcal{Q}_\zeta$.*

It is directly seen that the maximal degree of an element of \mathcal{D}_ζ has to be equal to N , also known as the *depth* of \mathcal{D}_ζ .

2.2 Quotient ring and dual structure

In this section we explore the relation between the dual ring and the quotient R/\mathcal{Q}_ζ where \mathcal{Q}_ζ is the primary component of the isolated point ζ . We show how to extract a basis of this quotient ring from the support of the elements of \mathcal{D}_ζ and how \mathcal{D}_ζ can be used to reduce any polynomial modulo \mathcal{Q}_ζ .

It is convenient in terms of notation to make the assumption $\zeta = \mathbf{0}$. This saves some indices, while it poses no constraint (since it implies a linear change of coordinates), and shall be adopted hereafter and in the next section.

Let $\text{supp } \mathcal{D}_\mathbf{0}$ be the set of exponents of monomials appearing in $\mathcal{D}_\mathbf{0}$, with a non-zero coefficient. These are of degree at most N , the nilindex of $\mathcal{Q}_\mathbf{0}$. Since $\forall \Lambda \in \mathcal{D}_\mathbf{0}$, $\Lambda^0[p] = 0$ iff $p \in \mathcal{Q}_\mathbf{0}$, we derive that $\text{supp } \mathcal{D}_\mathbf{0} = \{\alpha : \mathbf{x}^\alpha \notin \mathcal{Q}_\mathbf{0}\}$. In particular, we can find a basis of $R/\mathcal{Q}_\mathbf{0}$ between the monomials $\{\mathbf{x}^\alpha : \alpha \in \text{supp } \mathcal{D}_\mathbf{0}\}$. This is a finite set of monomials, since their degree is bounded by the nilindex of $\mathcal{Q}_\mathbf{0}$.

Given a standard basis $\mathcal{B} = (\mathbf{x}^{\beta_i})_{i=1, \dots, \mu}$ of $R/\mathcal{Q}_\mathbf{0}$ and, for all monomials $x^{\gamma_j} \notin \mathcal{Q}_\mathbf{0}$, $j = 1, \dots, s - \mu$, $s = \#\text{supp } \mathcal{D}_\mathbf{0}$, with $x^{\gamma_j} \notin \mathcal{B}$, the expression (normal form) of

$$x^{\gamma_j} = \sum_{i=1}^{\mu} \lambda_{ij} \mathbf{x}^{\beta_i} \pmod{\mathcal{Q}_\mathbf{0}} \quad (4)$$

in the basis \mathcal{B} then the dual elements [12, Prop. 13]

$$\Lambda_i = \mathbf{d}^{\beta_i} + \sum_{j=1}^{s-\mu} \lambda_{ij} \mathbf{d}^{\gamma_j}, \quad (5)$$

for $i = 1, \dots, \mu$ form a basis of $\mathcal{D}_\mathbf{0}$. We give a proof of this fact in the following lemma.

LEMMA 2.4. *The set of elements $\mathcal{D} = (\Lambda_i)_{i=1, \dots, \mu}$ is a basis of $\mathcal{D}_\mathbf{0}$ and the normal form of any $g(\mathbf{x}) \in R$ with respect to the standard basis $\mathcal{B} = (\mathbf{x}^{\beta_i})_{i=1, \dots, \mu}$ is*

$$\text{NF}(g) = \sum_{i=1}^{\mu} \Lambda_i^0[g] \mathbf{x}^{\beta_i}. \quad (6)$$

PROOF. First note that the elements of \mathcal{D} are linearly independent. Now, by construction, $\sum_{i=1}^{\mu} \Lambda_i^0[\mathbf{x}^\alpha] = \text{NF}(\mathbf{x}^\alpha)$ for all $\mathbf{x}^\alpha \notin \mathcal{Q}_\mathbf{0}$, eg. $\text{NF}(\mathbf{x}^{\beta_i}) = \mathbf{x}^{\beta_i}$. Also, for $\mathbf{x}^\alpha \in \mathcal{Q}_\mathbf{0}$, $\forall i$, $\Lambda_i^0(\mathbf{x}^\alpha) = 0$, since $\alpha \notin \text{supp } \mathcal{D}$. Thus the elements of \mathcal{D} compute $\text{NF}(\cdot)$ on all monomials of R , and (6) follows by linearity. We deduce that \mathcal{D} is a basis of $\mathcal{D}_\mathbf{0}$, as in Def. 2.1. \square

Computing the normal form of the border monomials of \mathcal{B} via (6) also yields the border basis relations and the operators of multiplication in the quotient $R/\mathcal{Q}_\mathbf{0}$ (see eg. [5] for more properties).

If a graded monomial ordering is fixed and $\mathcal{B} = (\mathbf{x}^{\beta_i})_{i=1, \dots, \mu}$ is the corresponding standard basis of $R/\mathcal{Q}_\mathbf{0}$, then \mathbf{d}^{β_i} is the leading term of (5) wrt the opposite ordering [8, Th. 3.1].

Conversely, if we are given a basis \mathcal{D} of $\mathcal{D}_\mathbf{0}$ whose coefficient matrix in the dual monomials basis $(\mathbf{d}^\alpha)_{\alpha \notin \mathcal{Q}_\mathbf{0}}$ is $D \in \mathbb{K}^{\mu \times s}$, we can compute a basis of $R/\mathcal{Q}_\mathbf{0}$ by choosing μ independent columns of D , say those indexed by \mathbf{d}^{β_i} , $i = 1, \dots, \mu$. If $G \in \mathbb{K}^{\mu \times \mu}$ is the (invertible) matrix formed by these columns, then $D' := G^{-1}D$, is

$$D' = \begin{matrix} \Lambda'_1 \\ \vdots \\ \Lambda'_\mu \end{matrix} \begin{bmatrix} \beta_1 & \cdots & \beta_\mu & \gamma_1 & \cdots & \gamma_{s-\mu} \\ 1 & & 0 & \lambda_{1,1} & \cdots & \lambda_{1,s-\mu} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & \lambda_{\mu,1} & \cdots & \lambda_{\mu,s-\mu} \end{bmatrix}, \quad (7)$$

i.e. a basis of the form (5). Note that an arbitrary basis of \mathcal{D} does not have the above diagonal form, nor does it directly provide a basis for $R/\mathcal{Q}_\mathbf{0}$.

For $t \in \mathbb{N}$, \mathcal{D}_t denotes the vector space of polynomials of \mathcal{D} of degree $\leq t$. The Hilbert function $h : \mathbb{N} \rightarrow \mathbb{N}$ is defined by $h(t) = \dim(\mathcal{D}_t)$, $t \geq 0$, hence $h(0) = 1$ and $h(t) = \dim \mathcal{D}$ for $t \geq N$. The integer $h(1) - 1 = \text{corank } J_{\mathbf{f}}$ is known as the *breadth* of \mathcal{D} .

3. COMPUTING LOCAL RING STRUCTURE

The computation of a local basis, given a system and a point, is done essentially by matrix-kernel computations, and consequently it can be carried out numerically, even when the point or even the system is inexact. Throughout the section we suppose $\mathbf{f} \in R^m$ and $\zeta \in \mathbb{K}^n$ with $\mathbf{f}(\zeta) = 0$.

Several matrix constructions have been proposed, that use different conditions to identify the dual space as a null-space. They are based on the *stability property* of the dual basis:

$$\forall \Lambda \in \mathcal{D}_t, \quad \frac{d}{d\partial_i} \Lambda \in \mathcal{D}_{t-1}, \quad i = 1, \dots, n. \quad (8)$$

We list existing algorithms that compute dual-space bases:

- As pointed out in (3), an equivalent form of (8) is: $\forall \Lambda \in \mathcal{D}_t, \Lambda[x_i f_j] = 0, \forall i, j = 1, \dots, n$. Macaulay's method [9] uses it to derive the algorithm that is outlined in Sect. 3.1.

- In [11] they exploit (8) by forming the matrix D_i of the map $\frac{d}{d\partial_i} : \mathbb{K}[\partial]_t \rightarrow \mathbb{K}[\partial]_{t-1}$ for all $i = 1, \dots, n$ and some triangular decomposition of the differential polynomials in terms the differential variables. This approach was used in [18] to reduce the row dimension of Macaulay's matrix, but not the column dimension. The closedness condition is also used in [21] to identify a superset of $\text{supp } \mathcal{D}_{t+1}$.

- The *integration method* in [12] "integrates" elements of a basis of \mathcal{D}_t , and obtains *a priori* knowledge of the form of elements in degree $t + 1$ (Sect. 3.2).

All methods are incremental, in the sense that they start by setting $\mathcal{D}_0 = \langle 1 \rangle$ and continue by computing $\mathcal{D}_i, i = 1, \dots, N, N + 1$. When $\#\mathcal{D}_N = \#\mathcal{D}_{N+1}$ then \mathcal{D}_N is a basis of \mathcal{D} , and N is the nilindex of \mathcal{Q} .

We shall review two of these approaches to compute a basis for \mathcal{D} , and then describe an improvement, that allows simultaneous computation of a quotient ring basis while avoiding redundant computations.

3.1 Macaulay's dialytic matrices

This matrix construction is presented in [9, Ch. 4], a modern introduction is contained in [3], together with an implementation of the method in ApaTools¹.

The idea behind the algorithm is the following: An element of \mathcal{D} is of the form $\Lambda(\partial) = \sum_{|\alpha| \leq N} \lambda_\alpha \mathbf{d}^\alpha$ under the

condition: Λ^0 evaluates to 0 at any $g \in \langle \mathbf{f} \rangle$, i.e. $\Lambda^0(g) = \Lambda^0(\sum g_i f_i) = 0 \iff \Lambda^0(x^\beta f_i) = 0$ for all monomials x^β . If we apply this condition recursively for $|\alpha| \leq N$ we get a vector of coefficients $(\lambda_\alpha)_{|\alpha| \leq N}$ in the (right) kernel of the matrix with rows indexed by constraints $\Lambda^0[x^\beta f_i] = 0, |\beta| \leq N - 1$.

Note that the only requirement is to be able to perform derivation of the input equations and evaluation at $\zeta = 0$.

EXAMPLE 3.1. Let $f_1 = x_1 - x_2 + x_1^2, f_2 = x_1 - x_2 + x_2^2$. We also refer the reader to [3, Ex. 2] for a detailed demonstration of Macaulay's method on the same instance. The matrices in order 1 and 2 are:

$$\begin{array}{c} \begin{array}{ccc} 1 & d_1 & d_2 \\ f_1 & \begin{bmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \end{bmatrix} \\ f_2 & \begin{bmatrix} 0 & 1 & -1 \end{bmatrix} \end{array}, \quad \begin{array}{cccccc} & 1 & d_1 & d_2 & d_1^2 & d_1 d_2 & d_2^2 \\ f_1 & \begin{bmatrix} 0 & 1 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{bmatrix} \\ x_1 f_1 & \begin{bmatrix} 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \end{bmatrix} \\ x_1 f_2 & \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \\ x_2 f_1 & \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \\ x_2 f_2 & \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \end{array} \end{array}.$$

¹<http://www.neiu.edu/~zzeng/apatools.htm>

The kernel of the left matrix gives $\mathcal{D}_1 = (1, d_1 + d_2)$. Expanding up to order two, we get the matrix on the right, and $\mathcal{D}_2 = (1, d_1 + d_2, -d_1 + d_1^2 + d_1 d_2 + d_2^2)$. If we expand up to depth 3 we get the same null-space, thus $\mathcal{D} = \mathcal{D}_2$. \square

3.2 Integration method

This method is presented in [12]. It is an evolution of Macaulay's method, in the sense that the matrices are not indexed by all differentials, but just by elements based on knowledge of the previous step. This performs a computation adapted to the given input and results in smaller matrices.

For $\Lambda \in \mathbb{K}[\partial]$, we denote by $\int_k \Lambda$ the element $\Phi \in \mathbb{K}[\partial]$ with the property $\frac{d}{d\partial_k} \Phi(\partial) = \Lambda(\partial)$ and with no constant term wrt ∂_k .

THEOREM 3.2 ([12, Th. 15]). *Let $\langle \Lambda_1, \Lambda_2, \dots, \Lambda_s \rangle$ be a basis of \mathcal{D}_{t-1} , that is, the subspace of \mathcal{D} of elements of order at most $t - 1$. An element $\Lambda \in \mathbb{K}[\partial]$ with no constant term lies in \mathcal{D}_t iff it is of the form:*

$$\Lambda(\partial) = \sum_{i=1}^s \sum_{k=1}^n \lambda_{ik} \int_k \Lambda_i(\partial_1, \dots, \partial_k, 0, \dots, 0), \quad (9)$$

for $\lambda_{ik} \in \mathbb{K}$, and the following two conditions hold:

$$(i) \sum_{i=1}^s \lambda_{ik} \frac{d}{d\partial_i} \Lambda_i(\partial) - \sum_{i=1}^s \lambda_{il} \frac{d}{d\partial_k} \Lambda_i(\partial) = 0, \\ \text{for all } 1 \leq k \leq l \leq n.$$

$$(ii) \Lambda^\zeta[f_k] = 0, \text{ for } k = 1, \dots, n.$$

Condition (i) is equivalent to $\frac{d}{d\partial_k} \Lambda \in \mathcal{D}_{t-1}$, for $1 \leq k \leq n$. Thus the two conditions express exactly the fact that \mathcal{D} must be stable by derivation and his members must vanish on $\langle \mathbf{f} \rangle$.

This gives the following algorithm to compute the dual basis: Start with $\mathcal{D}_0 = \langle 1 \rangle$. Given a basis of \mathcal{D}_{t-1} we generate the ns candidate elements $\int_k \Lambda_{i-1}(\partial_1, \dots, \partial_k, 0, \dots, 0)$. Conditions (i) and (ii) give a linear system with unknowns λ_{ik} . The columns of the corresponding matrix are indexed by the candidate elements. Then the kernel of the matrix gives the possible solutions, which we add to \mathcal{D}_{t-1} to obtain \mathcal{D}_t . If for some t there are no further new elements, then $\mathcal{D} = \mathcal{D}_t$ is a basis of \mathcal{D} .

EXAMPLE 3.3. Consider the instance of Ex. 3.1. We have $f_1(\zeta) = f_2(\zeta) = 0$, thus we set $\mathcal{D}_0 = \{1\}$. Equation (9) gives $\Lambda = \lambda_1 d_1 + \lambda_2 d_2$. Condition (i) induces no constraints and (ii) yields the system

$$\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \end{bmatrix} = 0 \quad (10)$$

where the columns are indexed by d_1, d_2 . We get $\lambda_1 = \lambda_2 = 1$ from the kernel of this matrix, thus $\mathcal{D}_1 = \{1, d_1 + d_2\}$.

For the second step, we compute the elements of \mathcal{D}_2 , that must be of the form $\Lambda = \lambda_1 d_1 + \lambda_2 d_2 + \lambda_3 d_1^2 + \lambda_4 (d_1 d_2 + d_2^2)$. Condition (i) yields $\lambda_3 - \lambda_4 = 0$, and together with (ii) we form the system

$$\begin{bmatrix} 0 & 0 & 1 & -1 \\ 1 & -1 & 1 & 0 \\ 1 & -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{bmatrix} = 0, \quad (11)$$

with columns indexed by $d_1, d_1^2, d_2, d_1 d_2 + d_2^2$. We get two vectors in the kernel, the first yielding again $d_1 + d_2$ and a

second one for $\lambda_1 = -1, \lambda_2 = 0, \lambda_3 = \lambda_4 = 1$, so we deduce that $-d_1 + d_1^2 + d_1d_2 + d_2^2$ is a new element of \mathcal{D}_2 .

In the third step we have

$$\Lambda = \lambda_1 d_1 + \lambda_2 d_2 + \lambda_3 d_1^2 + \lambda_4 (d_1 d_2 + d_2^2) + \lambda_5 (d_1^3 - d_1^2) + \lambda_6 (d_1^3 + d_1 d_2^2 + d_1^2 d_2 - d_1 d_2),$$

condition (i) leads to $\lambda_3 - \lambda_4 + (\lambda_5 - \lambda_6)d_1 + (\lambda_5 - \lambda_6)d_2 = 0$, and together with condition (ii) we arrive to

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 1 & -1 & 1 & 0 & -1 & 0 \\ 1 & -1 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \\ \lambda_5 \\ \lambda_6 \end{bmatrix} = 0. \quad (12)$$

Since the kernel of this matrix gives elements that are already in \mathcal{D}_2 , we derive that $\mathcal{D} = \mathcal{D}_2 = \mathcal{D}_3$ and the algorithm terminates.

Note that for this example Macaulay's method ends with a matrix of size 12×10 , instead of 4×6 in this approach. \square

3.3 Computing a primal-dual pair

In this section we provide a process that allows simultaneous computation of a basis pair $(\mathcal{D}, \mathcal{B})$ of \mathcal{D} and R/\mathcal{Q} .

Computing a basis of \mathcal{D} degree by degree involves duplicated computations. The successive spaces computed are $\mathcal{D}_1 \subset \dots \subset \mathcal{D}_N = \mathcal{D}_{N+1}$. It is more efficient to compute only new elements $\Lambda \in \mathcal{D}_t$ which are independent in $\mathcal{D}_t/\mathcal{D}_{t-1}$ at step t .

Also, once dual basis is computed, one has to transform it into the form (5), in order to identify a basis of R/\mathcal{Q} as well. This transformation can be done *a posteriori*, by finding a sub-matrix of full rank and then performing Gauss-Jordan elimination over this sub-matrix, to reach matrix form (7).

We introduce a condition (iii) extending Th. 3.2, that addresses these two issues: It allows the computation of a total of μ independent elements throughout execution, and returns a "triangular basis", e.g. a basis of R/\mathcal{Q} is identified.

LEMMA 3.4. Let $\mathcal{D}_{t-1} = (\Lambda_1, \dots, \Lambda_k)$ be a basis of \mathcal{D}_{t-1} , whose coefficient matrix is

$$\begin{matrix} & \beta_1 & \dots & \beta_k & \gamma_1 & \dots & \gamma_{s-k} \\ \Lambda_1 & \begin{bmatrix} 1 & * & * & * & \dots & * \\ \vdots & & & & & \vdots \\ \Lambda_k & \begin{bmatrix} 0 & 0 & 1 & * & \dots & * \end{bmatrix} \end{matrix} \end{matrix}, \quad (13)$$

yielding the standard basis $\mathcal{B} = (\mathbf{x}^{\beta_i})_{i=1, \dots, k}$. An element $\Lambda \in \mathbb{K}[\mathcal{D}]$ is not zero in $\mathcal{D}_t/\mathcal{D}_{t-1}$ iff in addition to (i), (ii) of Th. 3.2 we impose:

$$(iii) \quad \Lambda[\mathbf{x}^{\beta_i}] = 0, \quad 1 \leq i \leq k.$$

PROOF. Let $\Lambda \in \mathbb{K}[\mathcal{D}]$ be a non-zero functional satisfying (i), (ii) and (iii). Then $\Lambda \in \mathcal{D}_t$ and $\Lambda[\mathbf{x}^{\beta_i}] = 0$ for $i = 1, \dots, k$. If $\Lambda \in \mathcal{D}_{t-1}$, then $\Lambda = \sum_{i=1}^k \lambda_i \Lambda_i$. Take for i_0 the minimal i such that $\lambda_i \neq 0$. Then $\Lambda[\mathbf{x}^{\beta_{i_0}}] = \lambda_{i_0}$, which is in contradiction with condition (iii). Thus, the non-zero solutions of (i), (ii) and (iii) correspond to the elements which are not zero in $\mathcal{D}_t/\mathcal{D}_{t-1}$. \square

The above constraint is easy to realize; it is equivalent to $\forall i, \mathbf{d}_\zeta^{\beta_i} \notin \text{supp } \Lambda^\zeta$, which implies adding a row (linear constraint) for every i . In many cases this constraint is just $\lambda_{ik} = 0$ for some i, k , thus we rather remove the column

corresponding to λ_{ik} instead of adding a row. Either way, this lemma allows to shrink the kernel of the matrix and compute only new dual elements.

Let us explore our running example, to demonstrate the essence of this improvement.

EXAMPLE 3.5. We re-run Ex. 3.3 using Lem. 3.4.

In the initialization step $\mathcal{D}_0 = (1)$ is already in triangular form with respect to $\mathcal{B}_0 = \{1\}$. For the first step, we demand $\Lambda[1] = 0$, thus the matrix is the same as (10), yielding $\mathcal{D}_1 = (1, d_1 + d_2)$. We extend $\mathcal{B}_1 = \{1, x_2\}$, so that \mathcal{D}_1 is triangular with respect to \mathcal{B}_1 .

In the second step we remove from (11) the second column, hence

$$\begin{bmatrix} 0 & 1 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_3 \\ \lambda_4 \end{bmatrix} = 0,$$

yielding a single solution $-d_1 + d_1^2 + d_1d_2 + d_2^2$. We extend \mathcal{B}_1 by adding monomial x_1 : $\mathcal{B}_1 = \{1, x_2, x_1\}$.

For the final step, we search an element with $\Lambda[x_1] = \Lambda[x_2] = 0$ thus (12) loses two columns:

$$\begin{bmatrix} 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \lambda_3 \\ \lambda_4 \\ \lambda_5 \\ \lambda_6 \end{bmatrix} = 0.$$

We find an empty kernel, thus we recover the triangular basis $\mathcal{D} = \mathcal{D}_2$, which is then diagonalized to reach the form:

$$\begin{matrix} & 1 & d_2 & d_1 & d_1^2 & d_1 d_2 & d_2^2 \\ \Lambda_1 & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ \Lambda_2 & \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ \Lambda_3 & \begin{bmatrix} 0 & 0 & 1 & -1 & -1 & -1 \end{bmatrix} \end{matrix} \end{matrix} \end{matrix}.$$

This diagonal basis is dual to the basis $\mathcal{B} = (1, x_2, x_1)$ of the quotient ring and also provides a normal form algorithm (Lem. 2.4) wrt \mathcal{B} . In the final step we generated a 4×4 matrix, size smaller compared to all previous methods. \square

This technique for computing \mathcal{B} can be applied similarly to other the matrix methods, e.g. Macaulay's dialytic method.

If $h(t) - h(t-1) > 1$, ie. there are more than one elements in step t , then the choice of monomials to add to \mathcal{B} is obtained by extracting a non-zero maximal minor from the coefficient matrix in (\mathbf{d}^α) . In practice, we will look first at the monomials of smallest degree.

3.4 Approximate dual basis

In our deflation method, we assume that the multiple point is known approximately and we use implicitly Taylor's expansion of the polynomials at this approximate point to deduce the dual basis, applying the algorithm of the previous section. To handle safely the numerical problems which may occur, we utilize the following techniques:

- At each step, the solutions of linear system (9, i-iii) are computed via Singular Value Decomposition. Using a given threshold, we determine the numerical rank and an orthogonal basis of the solutions from the last singular values and the last columns of the right factor of the SVD.

- For the computation of the monomials which define the equations (3.4, iii) at the next step, we apply QR decomposition on the transpose of the basis to extract a non-zero maximal minor. The monomials indexing this minor are used to determine constraints (9, i-iii). A similar numerical technique is employed in [21], for Macaulay's method.

4. DEFLATION OF A SINGULAR POINT

We consider a system of equations $\mathbf{f} = (f_1, \dots, f_s)$, which has a multiple point at $\mathbf{x} = \zeta$. Also, let $\mathcal{B} = (b_1, \dots, b_\mu)$ be a basis of R/\mathcal{Q}_ζ and $\mathcal{D} = (\Lambda_1, \dots, \Lambda_\mu)$ its dual counterpart, with $\Lambda_1 = \mathbf{1}$.

We introduce a new set of equations starting from \mathbf{f} , as follows: add for every f_i the polynomial $g_k = f_k + p_k$, $p_k = \sum_{i=1}^\mu \varepsilon_{i,k} b_i$ where $\varepsilon_k = (\varepsilon_{1,k}, \dots, \varepsilon_{\mu,k})$ is a new vector of μ variables.

Consider the system

$$\mathcal{D}\mathbf{g}(\mathbf{x}, \varepsilon) = \left(\Lambda_1(\partial_{\mathbf{x}})[\mathbf{g}], \dots, \Lambda_\mu(\partial_{\mathbf{x}})[\mathbf{g}] \right).$$

where $\Lambda^\mathbf{x}[g_k] = \Lambda_i(\partial_{\mathbf{x}})[g_k]$ is defined as in (2) with ζ replaced by \mathbf{x} , ie. we differentiate g_k but we do not evaluate at ζ . This is a system of μs equations, which we shall index $\mathcal{D}\mathbf{g}(\mathbf{x}, \varepsilon) = (g_{1,1}, \dots, g_{\mu,s})$. We have

$$g_{ik}(\mathbf{x}, \varepsilon) = \Lambda_i^\mathbf{x}[f_k + p_k] = \Lambda_i^\mathbf{x}[f_k] + \Lambda_i^\mathbf{x}[p_k] = \Lambda_i^\mathbf{x}[f_k] + p_{ik}(\mathbf{x}, \varepsilon).$$

Notice that $p_{i,k}(\zeta, \varepsilon) = \Lambda_i^\zeta[p_k] = \varepsilon_{i,k}$ because $\mathcal{D} = (\Lambda_1, \dots, \Lambda_\mu)$ is dual to \mathcal{B} .

As the first basis element of \mathcal{D} is $\mathbf{1}$ (the evaluation at the root), the first s equations are $\mathbf{g}(\mathbf{x}, \varepsilon) = 0$.

Note that this system is under-determined, since the number of variables is $\mu s + n$ and the number of equations is μs . We shall provide a systematic way to choose n variables and purge them (or better, set them equal to zero).

This way we arrive to a square system $\mathcal{D}\mathbf{g}(\mathbf{x}, \tilde{\varepsilon})$ (we use $\tilde{\varepsilon}$ for the remaining $\mu s - n$ variables) of size $\mu s \times \mu s$. We shall prove that this system vanishes on $(\zeta, \mathbf{0})$ and that $J_{\mathcal{D}\mathbf{g}}(\zeta, \mathbf{0}) \neq 0$.

By linearity of the Jacobian matrix we have

$$\begin{aligned} J_{\mathcal{D}\mathbf{g}}(\mathbf{x}, \varepsilon) &= J_{\mathcal{D}\mathbf{f}}(\mathbf{x}, \varepsilon) + J_{\mathcal{D}\mathbf{p}}(\mathbf{x}, \varepsilon) \\ &= [J_{\mathcal{D}\mathbf{f}}(\mathbf{x}) | \mathbf{0}] + [J_{\mathcal{D}\mathbf{p}}^\varepsilon(\mathbf{x}, \varepsilon) | J_{\mathcal{D}\mathbf{p}}^\varepsilon(\mathbf{x}, \varepsilon)], \end{aligned}$$

where $J_{\mathcal{D}\mathbf{p}}^\varepsilon(\mathbf{x}, \varepsilon)$ (resp. $J_{\mathcal{D}\mathbf{p}}^\varepsilon(\mathbf{x}, \varepsilon)$) is the Jacobian matrix of $\mathcal{D}\mathbf{p}$ with respect to \mathbf{x} (resp. ε).

LEMMA 4.1. *The Jacobian $J_{\mathcal{D}\mathbf{p}}^\varepsilon(\mathbf{x}, \varepsilon)$ of the linear system $\mathcal{D}\mathbf{p} = (p_{1,1}, \dots, p_{\mu,s})$ with $p_{i,k}(\varepsilon_k) = \Lambda_i^\mathbf{x}[p_k](\mathbf{x}, \varepsilon_k)$ evaluated at $(\mathbf{x}, \varepsilon) = (\zeta, \mathbf{0})$ is the identity matrix in dimension μs .*

PROOF OF LEMMA 4.1. First note that the system is block separated, i.e. every $p_{i,k}$ depends only on variables ε_i and not on all variables $\varepsilon = (\varepsilon_1, \dots, \varepsilon_n)$. This shows that $J_{\mathcal{D}\mathbf{p}}^\varepsilon(\mathbf{x}, \varepsilon)$ is block diagonal,

$$J_{\mathcal{D}\mathbf{p}}^\varepsilon(\mathbf{x}, \varepsilon) = \begin{bmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_\mu \end{bmatrix}.$$

Now we claim that all these blocks are all equal to the identity matrix. To see this, consider their entry $\partial_{\varepsilon_{kj}}[p_{ik}]$ for $i, j = 1, \dots, \mu$, which is

$$\frac{d}{d\varepsilon_{kj}} \Lambda_{i-1}^\mathbf{x}[p_k] = \Lambda_i^\mathbf{x} \left[\frac{d}{d\varepsilon_{jk}} p_k \right] = \Lambda_i[b_j] = \begin{cases} 1 & , i = j \\ 0 & , \text{otherwise} \end{cases},$$

since $\frac{d}{d\varepsilon_{j,k}} p_k = \frac{d}{d\varepsilon_{j,k}} (b_j \varepsilon_{j,k}) = b_j$. \square

LEMMA 4.2. *The $\mu s \times n$ Jacobian matrix $J_{\mathcal{D}\mathbf{f}}(\mathbf{x})$ of the system $\mathcal{D}\mathbf{f}(\mathbf{x}) = (f_1, \dots, f_{\mu n})$ is of full rank n at $\mathbf{x} = \zeta$.*

PROOF OF LEMMA 4.2. Suppose that the matrix is rank-deficient. Then there is a non-trivial vector in its kernel,

$$J_{\mathcal{D}\mathbf{f}}(\zeta) \cdot \mathbf{v} = \mathbf{0}.$$

The entries of \mathbf{v} are indexed by ∂_i . This implies that a non-zero differential $\Delta = v_1 \partial_1 + \dots + v_n \partial_n$ of order one satisfies the following relations: $(\Delta \Lambda_i)^\zeta[f_j] = 0$, $i = 1, \dots, \mu$, $j = 1, \dots, s$. By the standard derivation rules, we have

$$\frac{d}{d\partial_k} (\Delta \Lambda_i) = v_k \Lambda_i + \Delta \frac{d}{d\partial_k} \Lambda_i,$$

for $i = 1, \dots, \mu$, $k = 1, \dots, n$. Since \mathcal{D} is stable by derivation, $\frac{d}{d\partial_k} \Lambda_i \in \mathcal{D}$. We deduce that the vector space spanned by $\langle \mathcal{D}, \Delta \mathcal{D} \rangle$ is stable by derivation and vanishes on \mathbf{f} at ζ . By Proposition 2.2, we deduce that $\Delta \mathcal{D} \subset \mathcal{D}$. This is a contradiction, since Δ is of degree 1 and the elements in \mathcal{D} are of degree $\leq N$. \square

The columns of $J_{\mathcal{D}\mathbf{g}}(\mathbf{x}, \varepsilon)$ are indexed by the variables $(\mathbf{x}, \varepsilon)$, while the rows are indexed by the polynomials g_{ik} . We construct the following systems:

- Let $\mathcal{D}\mathbf{f}^I$ be a subsystem of $\mathcal{D}\mathbf{f}$ such that the corresponding n rows of $J_{\mathcal{D}\mathbf{f}}(\zeta)$ are linearly independent (Lem. 4.2). We denote by $I = \{(i_1, k_1), \dots, (i_n, k_n)\}$ their indices.
- Let $\mathcal{D}\tilde{\mathbf{g}}(\mathbf{x}, \tilde{\varepsilon})$ be the square system formed by removing the variables $\varepsilon_{i_1, k_1}, \dots, \varepsilon_{i_n, k_n}$ from $\mathcal{D}\mathbf{g}(\mathbf{x}, \varepsilon)$. Therefore the Jacobian $J_{\mathcal{D}\tilde{\mathbf{g}}}(\mathbf{x}, \tilde{\varepsilon})$ derives from $J_{\mathcal{D}\mathbf{g}}(\mathbf{x}, \varepsilon)$, after purging the columns indexed by $\varepsilon_{i_1, k_1}, \dots, \varepsilon_{i_n, k_n}$, and it's (i_j, k_j) row becomes $[\nabla(\Lambda_{i_j}^\mathbf{x} \tilde{g}_{i_j, k_j})^T | \mathbf{0}]$.

THEOREM 4.3 (DEFLATION THEOREM 1). *Let $\mathbf{f}(\mathbf{x})$ be a n -variate polynomial system with an μ -fold isolated zero at $\mathbf{x} = \zeta$. Then the $n \times n$ system $\mathcal{D}\mathbf{f}^I(\mathbf{x}) = 0$, defined in (a), has a simple root at $\mathbf{x} = \zeta$.*

PROOF. By construction, ζ is a solution of $\mathcal{D}\mathbf{f}^I(\mathbf{x}) = 0$. Moreover, the indices I are chosen such that $\det J_{\mathcal{D}\mathbf{f}^I}(\zeta) \neq 0$. This shows that ζ is a simple (thus isolated) root of the system $\mathcal{D}\mathbf{f}^I(\mathbf{x}) = 0$. \square

EXAMPLE 4.4. In our running example, we expand the rectangular Jacobian matrix of 6 polynomials in (x_1, x_2) . Choosing the rows corresponding to f_1 and $(d_1 - d_2^2 - d_1 d_2 - d_1^2)[f_1]$, we find a non-singular minor, hence the resulting system $(f_1, 2x_1)$ has a regular root at $\zeta = (0, 0)$. \square

The deflated system $\mathcal{D}\mathbf{f}^I(\mathbf{x}) = 0$ is a square system in n variables. Contrarily to the deflation approach in [7, 3], we do not need to introduce new variables here and one step of deflation is sufficient. In the following theorem, we do introduce new variables to express the condition that the perturbed system has a given multiplicity structure.

THEOREM 4.5 (DEFLATION THEOREM 2). *Let $\mathbf{f}(\mathbf{x})$ be a n -variate polynomial system with an μ -fold isolated zero at $\mathbf{x} = \zeta$. The square system $\mathcal{D}\tilde{\mathbf{g}}(\mathbf{x}, \tilde{\varepsilon}) = 0$, as defined in (b), has a regular isolated root at $(\mathbf{x}, \tilde{\varepsilon}) = (\zeta, \mathbf{0})$.*

PROOF. By definition of \mathcal{D} , we have

$$\mathcal{D}\tilde{\mathbf{g}}(\zeta, \mathbf{0}) = (\Lambda_1^\zeta[\mathbf{f}], \dots, \Lambda_\mu^\zeta[\mathbf{f}]) = \mathbf{0}.$$

Moreover, by construction of $\mathcal{D}\tilde{\mathbf{g}}$ we get, up to a row permutation, the determinant:

$$\pm \det J_{\mathcal{D}\tilde{\mathbf{g}}}(\zeta, \mathbf{0}) = \det \begin{bmatrix} J_1 & 0 \\ J_2 & I \end{bmatrix} = \det J_1 \neq 0,$$

where $J_1 = J_{\mathcal{D}\mathbf{f}^I}(\zeta)$. This shows that $(\zeta, \mathbf{0})$ is regular and thus isolated point of the algebraic variety defined by $\mathcal{D}\tilde{\mathbf{g}}(\mathbf{x}, \tilde{\varepsilon}) = 0$. \square

Nevertheless, this deflation does differ from the deflation strategy in [7, 3]. There, new variables are added that correspond to coefficients of differential elements, thus introducing a perturbation in the approximate dual basis, in case of approximate input. Hence the output concerns a deflated root of the given approximate system. In our method, we perturb the equations, keeping an approximate structure of a multiple point. Consequently, the certification of a root concerns a nearby system, within controlled error bounds, as it shall be described in Sect. 5.

We mention that it would also be possible to use the equations (9, i-iii) to construct a deflated system on the differentials and to perturb the approximate dual structure.

5. VERIFYING APPROXIMATE SINGULAR POINTS

In real-life applications it is common to work with approximate inputs. Also, there is the need to (numerically) decide if an (approximate) system possesses a single (real) root in a given domain, notably for use in subdivision-based algorithms, eg. [13, 10].

In the regular case, Smale's α -theory, extending Newton's method, can be used to answer this problem. Another option is Rump's Theorem, also based on Newton theory. In our implementation we choose this latter approach, since it is suitable for inexact data and suits best with the perturbation which is applied. Our perturbation coincides to the numerical scheme of [16] in the univariate case.

The certification test is based on the verification method of Rump [16, Th. 2.1], which we rewrite in our setting:

THEOREM 5.1 ([16] RUMP'S THEOREM). *Let $\mathbf{f} \in R^n$ be a polynomial system and $\zeta^* \in \mathbb{R}^n$ a real point. Given an interval domain $Z \in \mathbb{IR}^n$ containing $\zeta^* \in \mathbb{R}^n$, and an interval matrix $M \in \mathbb{IR}^{n \times n}$ whose i -th column M_i satisfies $\nabla f_i(Z) \subseteq M_i$ for $i = 1 \dots, n$, then the following holds:
If the inclusion*

$$V(\mathbf{f}, Z, \zeta^*) = -J_{\mathbf{f}}(\zeta^*)^{-1} \mathbf{f}(\zeta^*) + (I - J_{\mathbf{f}}(\zeta^*)^{-1} M)Z \subseteq \overset{\circ}{Z} \quad (14)$$

is true, then there is a unique $\zeta \in Z$ with $\mathbf{f}(\zeta) = \mathbf{0}$ and the Jacobian matrix $J_{\mathbf{f}}(\zeta) \in M$ is non-singular.

This theorem is applied on the perturbed system. If the test succeeds, we also get a domain for ε -variables that reflects the distance of the approximate system from a precise system with the computed local structure.

EXAMPLE 5.2. We start with an approximate system: $f_1 = 1.071x_1 - 1.069x_2 + 1.018x_1^2$, $f_2 = 1.024x_1 - 1.016x_2 + 1.058x_2^2$ and the domain: $Z = [-.01, .03] \times [-.03, .01]$. The Jacobian at $\mathbf{x} = (0, 0)$ evaluates to .00652, hence it is close to singular.

We set the tolerance equal to .04, i.e. the size of the domain, and we consider the center of the box as our approximate point, $\zeta^* = (.01, -.01)$.

First we compute approximate multiplicity structure at ζ^* , $\mathcal{D} = (1, d_2 + 1.00016d_2^2 + .99542d_1d_2 + 1.03023d_1^2, d_1 - 1.00492d_2^2 - 1.00016d_1d_2 - 1.03514d_1^2)$ as well as $(1, x_2, x_1)$, a standard basis for the quotient. The latter indicates to perturb up to linear terms.

Now apply the second deflation theorem 4.5 to get the 6×6 system $\mathbf{g} = (1.018x_1^2 + 1.071x_1 + (\varepsilon_{12} - 1.069)x_2, \varepsilon_{12} - .02023, .01723 + 2.036x_1, 1.058x_2^2 + (1.024 + \varepsilon_{23})x_1 + (\varepsilon_{22} -$

$1.016)x_2 + \varepsilon_{21}, .04217 + 2.116x_2 + \varepsilon_{22}, \varepsilon_{23} - .03921)$, which has a regular root for $\zeta \in Z$ and parameters $(\varepsilon_{12}, \varepsilon_{21}, \varepsilon_{22}, \varepsilon_{23})$. Indeed, applying Theorem 5.1 with $Z' = Z \times [-.04, .04]^4$ and $(\zeta^*, 0, \dots, 0)$ we get an inclusion $V(\mathbf{g}, Z', \zeta^*) \subseteq \overset{\circ}{Z}'$. \square

6. GEOMETRY AROUND A SINGULARITY

As a final step in analyzing isolated singularities, we show how the local basis can be used to compute the topological degree around the singular point. If the latter is a self-intersection point of a real algebraic curve, one can deduce the number of curve branches that pass through it.

Topological degree computation. Let $\mathbf{f}(\mathbf{x})$ be a square n -variate system with an μ -fold isolated zero at $\mathbf{x} = \zeta$. To a linear form $\Lambda \in \mathbb{R}[\partial_{\zeta}]$, we associate the quadratic form

$$Q_{\Lambda} : R/\mathcal{Q} \times R/\mathcal{Q} \rightarrow \mathbb{R} \quad , \quad (b_i, b_j) \mapsto \Lambda(b_i b_j) \quad (15)$$

for $R/\mathcal{Q} = \langle b_1, \dots, b_{\mu} \rangle$. The signature of this (symmetric and bi-linear) form is the sum of signs of the diagonal entries of any diagonal matrix representation of it.

PROPOSITION 6.1 ([4, Th. 1.2]). *If Q_{Φ} , $\Phi \in \mathcal{D}$ is any bi-linear symmetric form such that $\Phi^{\zeta}[\det J_{\mathbf{f}}(\mathbf{x})] > 0$, then*

$$tdeg_{\zeta}(\mathbf{f}) = sgn(Q_{\Phi}). \quad (16)$$

This signature is independent of the bi-linear form used.

We can use this result to compute the topological degree at $\mathbf{x} = \zeta$ using the dual structure at ζ . Since a basis \mathcal{D} is available we set $\Phi = \pm \Lambda_i$, for some basis element that is not zero on $\det J_{\mathbf{f}}(\mathbf{x})$. Indeed, such an element can be retrieved among the basis elements, since $\det J_{\mathbf{f}} \notin \langle \mathbf{f} \rangle$, see [5, Ch. 0].


In practice it suffices to generate a random element of \mathcal{D} , compute its matrix representation $[\Phi(b_i b_j)]_{ij}$, and then extract the signature of Q_{Φ} .

Branches around a singularity. In the context of computing with real algebraic curves, the identification of self-intersection points is only the first step of determining the local topology. As a second step, one needs to calculate the number of branches attached to the singular point ζ , hereafter denoted $\text{Br}(\mathbf{f}, \zeta)$. This information is encoded in the topological degree.

An implicit curve in n -space is given by all points satisfying $\mathbf{f}(\mathbf{x}) = 0$, $\mathbf{f} = (f_1, \dots, f_{n-1})$. Consider $p(\mathbf{x}) = (x_1 - \zeta_1)^2 + \dots + (x_n - \zeta_n)^2$, and $\mathbf{g}(\mathbf{x}) = \det J_{(\mathbf{f}, p)}(\mathbf{x})$. Then ([19] and references therein):

$$\text{Br}(\mathbf{f}, \zeta) = 2 tdeg_{\zeta}(\mathbf{f}, \mathbf{g}). \quad (17)$$

This implies an algorithm for $\text{Br}(\mathbf{f}, \zeta)$. First compute the primal-dual structure of (\mathbf{f}, \mathbf{g}) at ζ and then use Prop. 6.1 to get $tdeg_{\zeta}(\mathbf{f}, \mathbf{g})$.

EXAMPLE 6.2. Consider the implicit curve $f(x, y) = 0$, in xy -plane, with $f(x, y) = x^4 + 2x^2y^2 + y^4 + 3x^2y - y^3$, that looks like this . We search for the number of branches touching $\zeta = (0, 0)$.

We compute $g(x, y) = J_{(f, x^2+y^2)} = 18xy^2 - 6x^3$, and then the multiplicity structure of (f, g) at ζ , and we arrive to the standard basis $\mathcal{B} = (1, y, x, y^2, xy, x^2, y^3, xy^2, x^2y)$. Among the 9 elements of the dual basis, we find $\Phi = d_y^3 + \frac{3}{8}d_y^4 + \frac{1}{8}d_x^2d_y^2 + \frac{3}{8}d_x^4$, having value $\Phi^0[\det J_{(f, g)}(\mathbf{x})] = 54 > 0$ on the Jacobian determinant.

Using \mathcal{B} and (6), we get the 9×9 matrix representation of Q_Φ (15) with ij -th entry $\Phi[\text{NF}(\mathbf{x}^{\beta_i} \mathbf{x}^{\beta_j})]$, and we compute $\text{tdeg}_\zeta(f, g) = \text{sgn } Q_\Phi = 3$, thus $\text{Br}(f, (0, 0)) = 6$. \square

7. EXPERIMENTATION

Our method is developed in MAPLE. It uses Mourrain's Integration technique to compute (approximate) dual basis and derive the augmented system of Th. 4.5. Then Rump's method is used to verify the root. Macaulay's method is also implemented for testing purposes.

EXAMPLE 7.1. Consider the system [8] of 3 equations in 2 variables $f_1 = x_1^3 + x_1x_2^2$, $f_2 = x_1x_2^2 + x_3^2$, $f_3 = x_1^2x_2 + x_1x_2^2$, and the singular point $(0, 0)$.

Suppose that the point is given. Using 3.2 and 3.4 we derive the primal-dual pair $\mathcal{D} = (1, d_1, d_2, d_1^2, d_1d_2, d_2^2, \underline{d_2^3} + d_1^3 + d_1^2d_2 - d_1d_2^2)$, where d_2^3 is underlined to show that it corresponds to x_2^3 in the primal standard basis \mathcal{B} . The biggest matrix used, in depth 4, was of size 9×8 , while Macaulay's method terminates with a matrix of size 30×15 .

To deflate the root, we construct the augmented system $\mathcal{D}\mathbf{f}$ of 21 equations. The 21×2 Jacobian matrix $J_{\mathcal{D}\mathbf{f}}$ is of rank 2 and a full-rank minor consists of the rows 4 and 5. Consequently find the system $(d_1^2[f_1], d_1d_2[f_1]) = (3x_1, 2x_2)$ which deflates $(0, 0)$. Note that even though both equations of the deflated system derive from f_1 , the functionals used on f_1 are computed using all initial equations. \square

EXAMPLE 7.2. Let, as in [6, 8], $f_1 = 2x_1 + 2x_1^2 + 2x_2 + 2x_2^2 + x_3^2 - 1$, $f_2 = (x_1 + x_2 - x_3 - 1)^3 - x_1^3$, and $f_3 = 2x_1^3 + 2x_2^2 + 10x_3 + 5x_3^2 + 5^3 - 1000x_1^5$.

Point $(0, 0, -1)$ occurs with multiplicity equal to 18, in depth 7. The final matrix size with our method is 206×45 , while Macaulay's method ends with a 360×165 matrix.

If the objective is to deflate as efficiently as possible, then one can go step by step: First compute a basis for \mathcal{D}_1 and stop the process. We get the evaluation 1 and 2 first order functionals, which we apply to f_1 . We arrive to $(1[f_1], (d_2 - d_1)[f_1], (d_1 + d_3)[f_1]) = (f_1, -4x_1 + 4x_2, 2 + 4x_1 + 2x_3)$ and we check that the Jacobian determinant is 64, thus we have a deflated system only with a partial local structure. \square

Table 7 shows computations on the benchmark set of [3]. Multiplicity, matrix sizes at termination step are reported.

Sys.	μ	Integration	Macaulay
cmbs1	11	33×23	105×56
cmbs2	8	21×17	60×35
mth191	4	10×9	30×20
decker2	4	5×5	20×15
Ojika2	2	6×5	12×10
Ojika3	4	24×9	60×35
KSS	16	569×69	630×252
Caprasse	4	34×13	60×35
Cyclic 9	4	369×33	495×33
DZ1	131	1450×524	4004×1365
DZ2	7	73×33	360×165
DZ3	5	14×8	30×21

Table 1: Benchmark systems from [3].

Acknowledgments. This research has received funding from the EU's 7th Framework Programme [FP7/2007-2013], Marie Curie ITN SAGA, grant n^o [PITN-GA-2008-214584].

8. REFERENCES

- [1] L. Alberti, B. Mourrain, & J. Wintz. Topology and arrangement computation of semi-algebraic planar curves. *CAGD*, 25:631–651, November 2008.
- [2] M.F. Atiyah & I.G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.
- [3] B. H. Dayton & Z. Zeng. Computing the multiplicity structure in solving polynomial systems. In *ISSAC '05*, pp. 116–123, 2005. ACM.
- [4] D. Eisenbud & H.I. Levine. An algebraic formula for the degree of a c^∞ map germ. *The Annals of Mathematics*, 106(1):pp. 19–44, 1977.
- [5] M. Elkadi & B. Mourrain. *Introduction à la résolution des systèmes d'équations algébriques*, vol. 59 of *Mathématiques et Applications*. Springer, 2007.
- [6] G. Lecerf. Quadratic newton iteration for systems with multiplicity. *Fo. Comp. Math.*, 2:247–293, 2002.
- [7] A. Leykin, J. Verschelde, & Zhao A. Newton's method with deflation for isolated singularities of polynomial systems. *TCS*, 359(1-3):111 – 122, 2006.
- [8] A. Leykin, J. Verschelde, & A. Zhao. Higher-order deflation for polynomial systems with isolated singular solutions. vol. 146 of *The IMA Volumes in Math. and its Appl.*, pp. 79–97, 2008.
- [9] F.S. Macaulay. *The algebraic theory of modular systems*. Cambridge Univ. Press, 1916.
- [10] A. Mantzaflaris, B. Mourrain, & E. Tsigaridas. Continued fraction expansion of real roots of polynomial systems. In *Proc. of SNC '09*, pp. 85–94, 2009.
- [11] M. G. Marinari, T. Mora, & H.M. Möller. Gröbner duality and multiplicities in polynomial system solving. In *Proc. of ISSAC '95*, pp. 167–179, 1995.
- [12] B. Mourrain. Isolated points, duality and residues. *J. of Pure & App. Alg.*, 117-118:469 – 493, 1997.
- [13] B. Mourrain & J. P. Pavone. Subdivision methods for solving polynomial equations. *J. Symb. Comp.*, 44:292–306, March 2009.
- [14] T. Ojika, S. Watanabe, & T. Mitsui. Deflation algorithm for multiple roots of a system of nonlinear equations. *J. of Math. An. & Appls.*, 96(2):463–479, 1983.
- [15] S.R. Pope & A. Szanto. Nearest multivariate system with given root multiplicities. *JSC*,44(6):606-625,2009.
- [16] S. Rump & S. Graillat. Verified error bounds for multiple roots of systems of nonlinear equations. *Num. Algs.*, 54:359–377, 2010.
- [17] Michael Shub & Steve Smale. Complexity of Bezout's theorem I: Geometric aspects. *J. of the AMS*, 6(2):459–501, 1993.
- [18] H. J. Stetter. Analysis of zero clusters in multivariate polynomial systems. In *Proc. of ISSAC '96*, pp. 127–136, New York, NY, USA, 1996. ACM.
- [19] Zbigniew Szafraniec. Topological degree and quadratic forms. *J. of Pure & App. Alg.*, 141(3):299 – 314, 1999.
- [20] X. Wu & L. Zhi. Computing the multiplicity structure from geometric involutive form. In *Proc. of ISSAC '08*, pp. 325–332, 2008. ACM.
- [21] Z. Zeng. The closedness subspace method for computing the multiplicity structure of a polynomial system. vol. 496 of *Contemporary Mathematics*, pp. 347–362. AMS. Providence, RI, 2009.

