Open access • Journal Article • DOI:10.1137/17M1162433

Solving Polynomial Systems via Truncated Normal Forms — Source link

Simon Telen, Bernard Mourrain, Marc Van Barel

Institutions: Katholieke Universiteit Leuven

Published on: 25 Sep 2018 - SIAM Journal on Matrix Analysis and Applications (Society for Industrial and Applied Mathematics)

Topics: Polynomial, Quotient ring, Affine transformation, Ring (mathematics) and Basis (linear algebra)

Solving Polynomial Systems via Truncated Normal Forms

Simon Telen, Bernard Mourrain, Marc Van Barel*

July 4, 2018

Abstract

We consider the problem of finding the isolated common roots of a set of polynomial functions defining a zero-dimensional ideal I in a ring R of polynomials over $\mathbb{C}$. We propose a general algebraic framework to find the solutions and to compute the structure of the quotient ring R/I from the null space of a Macaulay-type matrix. The affine dense, affine sparse, homogeneous and multi-homogeneous cases are treated. In the presented framework, the concept of a border basis is generalized by relaxing the conditions on the set of basis elements. This allows for algorithms to adapt the choice of basis in order to enhance the numerical stability. We present such an algorithm and show numerical results.

1 Introduction

We consider the zero-dimensional polynomial rootfinding problem. In this section we give an overview of related work, a summary of our contributions and the outline for the rest of the paper. There exist several methods to find all the roots of a set of polynomial equations [40, 6]. The most important classes are homotopy continuation methods [2, 42], subdivision methods [33] and algebraic methods [18, 37, 9, 14, 32, 41]. In this paper, we focus on the latter class of solvers. These methods perform linear algebra operations on vector subspaces of the ideal generated by the set of equations to deduce the algebraic structure of the quotient algebra of the polynomial ring by the ideal. One can find the roots of these techniques in ancient works on resultants by Bézout, Sylvester, Cayley, Macaulay.... Explicit constructions of matrices of polynomial coefficients are exploited to compute projective resultants of polynomial systems (see, e.g., [28]). These matrix constructions have been further investigated to compute other types of resultants such as toric or sparse resultants [9, 18, 10] or residual resultants [5]. See, e.g., [19] for an overview of these techniques. These matrices are also exploited in numerical linear algebra-based methods for finding the solutions of the polynomial equations from their null space [14, 41].

Another well-established approach to describe the quotient algebra structure is by computing Groebner bases for a given monomial ordering [8]. The initial algorithms based on rewriting techniques have been enhanced by introducing linear algebra tools [20, 15]. H-bases, initiated by F. S. Macaulay, have also been investigated to construct ideal bases, with interesting projection properties to compute normal forms and to describe quotient algebras [30]. To reduce the numerical instability induced by monomial orderings in Groebner bases computations, border bases have been developed to combine robustness and efficiency [32, 35, 36]. These methods proceed incrementally by performing linear algebra operations on monomial multiples of polynomials computed at the previous step, until a reduction or a commutation property is satisfied. The sizes of the matrices involved in these computations are usually smaller than the size of resultant matrices (see, e.g., [34]). Because of the incremental nature of these methods, the computed bases describing the quotient algebra structure may not be optimal from a numerical point of view.

The framework we consider in this paper is related to the construction of ideal interpolation (or normal form). In [11, 12], the problem of characterizing when a linear projector is an ideal projector, that

*Supported by the Research Council KU Leuven, C1-project (Numerical Linear Algebra and Polynomial Computations), and by the Fund for Scientific Research–Flanders (Belgium), G.0828.14N (Multivariate polynomial and rational interpolation and approximation), and EOS Project no 30468160.

is when the kernel of the projector is an ideal, is investigated. The conditions of commutation and the connectivity property of the basis proposed in [32] are discussed and compared to some variants.

Let $R = \mathbb{C}[x_1, \ldots, x_n]$ and $I \subset R$ a zero-dimensional ideal. It is well known that $\dim_{\mathbb{C}}(R/I) = \delta < \infty$. It is common practice to identify R/I with a δ-dimensional vector subspace $B \subset R$. An R-map $\mathcal{N} : R \to B$ satisfying $\mathcal{N}(R) = B, \ker \mathcal{N} = I$ and $\mathcal{N}_{|B} = \mathrm{id}_B$ gives all the information needed to compute the $\mathbb{C}$-algebra structure of R/I. Indeed, 'multiplication with x_i' is given by $B \to B : b \mapsto \mathcal{N}(x_i b)$. However, these *multiplication maps* can also be recovered if we know only the restriction of $\mathcal{N}$ to $B \cup x_1 \cdot B \cup \cdots \cup x_n \cdot B$. This restriction gives a linear map between finite dimensional vector spaces. Going the other way around: suppose we have a map $N : V \to \mathbb{C}^\delta$ with $V \subset R$ a finite dimensional $\mathbb{C}$-vector space. What are the conditions that N must satisfy so that we can recover the algebra structure of R/I from it? An answer to this question is given by our main result (Theorem 3.1), which states in a simplified version the following:

Theorem 1.1. *Let $V \subset R$ be a finite dimensional vector space and let $W = \{f \in V : x_i f \in V, i = 1, \ldots, n\}$. If a $\mathbb{C}$-linear map $N : V \to \mathbb{C}^\delta$ is such that*

1. *$\exists u \in V$ such that $u + I$ is a unit in R/I,*
2. *$\ker(N) \subset I \cap V$,*
3. *$N_{|W}$ is onto $\mathbb{C}^\delta$,*

then we can compute the algebra structure of R/I from the map N.

We show how a map N with the right properties can be computed as the cokernel of a resultant map in the case where I is a complete intersection (see for instance [9, Chapter 6] for a definition). If I is zero-dimensional but not a complete intersection, such resultant maps can still be used in a degree bigger than the regularity as shown for the projective case in Proposition 5.2. We also show how the multiplication operators can be computed from N and we characterize all subspaces $B \subset W$ that can be identified with R/I. Implicitly, this generalizes the concept of border bases [32, 35] by relaxing the conditions of connectivity on the basis. The resulting algorithm and variants of it can be used to find roots of generic dense, sparse, homogeneous and multi-homogeneous systems coming from a complete intersection. By 'generic' we mean that the system has the expected number of solutions in the respective solution varieties (affine space, the algebraic torus, projective space or a Segre variety). For homogeneous systems, the results lead to a new criterion of regularity of a homogeneous ideal I (Proposition 5.2), extending the criterion proposed in [3] in the zero-dimensional case.

In [41] it is shown that the choice of basis of the coordinate ring (that is, the choice of the subspace $B \subset W$) is crucial to the numerical stability of algebraic solving methods. In the framework we propose here, an algorithmic 'good' choice of basis can be made. For this we use the same techniques as in [41] and show in the experiments that the results are comparable in the dense, generic case.

The methods we propose in this paper are numerical linear algebra methods using finite precision arithmetic. Groebner bases methods require symbolic computation because they are unstable. This makes these methods unfeasible for large systems. We compare our algorithms to homotopy continuation methods in double precision, because these methods are known to be successful numerical solvers [2, 42]. However, we show in our numerical experiments that these methods do not guarantee that all solutions are found. On the contrary, our methods do find numerical approximations of all solutions under some genericity assumptions, and they are competitive in speed when the number of variables is not too large.

In the case where I defines a positive dimensional algebraic set which decomposes in irreducible components of the same dimension, our techniques may be used to compute so-called *witness sets* of these components [2]. This is beyond the scope of this article.

Throughout the paper, we assume zero-dimensionality of the ideal generated by the input equations. We start with a motivation and some definitions in the next section. We introduce the notion of *Truncated Normal Form* (TNF), which is important for the rest of the paper. In Section 3 we treat the rootfinding problem in affine space. We assume that the number of solutions in $\mathbb{C}^n$ is finite. Theorem 3.1 is the main theorem of the paper, since the results in other sections follow from it. In the case of a dense set of equations, the approach in [14] follows from Theorem 3.1. Section 4 deals with the toric case: we assume a finite number of solutions in the algebraic torus $(\mathbb{C}^*)^n$. In Section 5, we consider the case of dense systems in a projective setting. We use the framework to compute a representation of the degree ρ part of the quotient algebra, where ρ is the regularity of the ideal. We assume a finite number of solutions in $\mathbb{P}^n$. Section 6 treats the multihomogeneous case, where we have δ solutions in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$. In every setting, we present an appropriate Macaulay-type matrix (or *resultant map*) to work with in the case of a complete intersection with the expected number of solutions. In Section 7 we elaborate on how to find the solutions from a representation of the quotient algebra. Finally, in Section 8 we show some numerical examples. We denote the number of solutions, counting multiplicities, by δ and we denote the solutions by $z_i, i = 1, \ldots, \delta \in \star$ where $\star$ is the solution space.

2 Truncated normal forms

This section uses some standard terminology from commutative algebra. An introduction to polynomial rings, ideals and varieties can be found in [8, Chapter 1]. For an introduction to exact sequences the reader may consult [9, 17] or any standard commutative algebra textbook such as [1]. As in the introduction, let $R = \mathbb{C}[x_1, \ldots, x_n]$ be the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in the field $\mathbb{C}$ and take an ideal $I \subset R$ defining $\delta < \infty$ points, counting multiplicities. This is equivalent to the assumption that $\dim_{\mathbb{C}}(R/I) = \delta < \infty$. A *normal form*, which in [11] is also called an ideal projector, is a map characterized by the following properties.

Definition 2.1 (Normal form)**.** *A* normal form *on R w.r.t. I is an R-map $\mathcal{N} : R \to B$ where $B \subset R$ is a vector subspace of dimension δ over $\mathbb{C}$ such that the sequence*

$$0 \longrightarrow I \longrightarrow R \xrightarrow{\mathcal{N}} B \longrightarrow 0$$

is exact and $\mathcal{N}_{|B} = \mathrm{id}_B$.

From this definition, it follows that $B \simeq R/I$ and multiplication modulo I is completely determined by $\mathcal{N}$. Indeed, we have $m_{x_i} : B \to B : b \mapsto \mathcal{N}(x_i b)$. Since we want to find a representation of R/I using numerical linear algebra techniques, we will work with linear maps $\mathcal{N}$ that can be represented by a matrix. That is, we will work with restricted or *truncated* versions of normal form maps.

Definition 2.2 (Truncated normal form)**.** *Let $B \subset V \subset R$ with B, V finite dimensional vector subspaces, $x_i \cdot B \subset V, i = 1, \ldots, n$ and $\dim_{\mathbb{C}}(B) = \delta = \dim(R/I)$. A* Truncated Normal Form (TNF) *on V w.r.t. I is a linear map $\mathcal{N} : V \to B$ such that $\mathcal{N}$ is the restriction to V of a normal form w.r.t. I. That is, the sequence*

$$0 \longrightarrow I \cap V \longrightarrow V \xrightarrow{\mathcal{N}} B \longrightarrow 0$$

is exact and $\mathcal{N}_{|B} = \mathrm{id}_B$.

Let $\mathcal{N}$ be a TNF on $V \subset R$. Since $\mathcal{N}$ is the restriction of a normal form by definition, we have that multiplication by x_i modulo I can still be computed from $\mathcal{N}$. Now, let $P : B \to \mathbb{C}^\delta$ be an isomorphism defining coordinates on B. Denote $N = P \circ \mathcal{N}$ and let $N_i : B \to \mathbb{C}^\delta$ be given by $N_i(b) = N(x_i \cdot b)$, we have the following facts:

1. $\ker(N) = I \cap V$,
2. $N_{|B} = P$,
3. $m_{x_i}(b) = \mathcal{N}(x_i \cdot b) = (P^{-1} \circ N_i)(b)$.

Notice that an N satisfying these properties is of the form $N : f \in V \to N(f) = (\eta_1(f), \ldots, \eta_\delta(f)) \in \mathbb{C}^\delta$ with $\eta_i \in V^* \cap I^\perp = \{\lambda \in V^* \mid \forall p \in I \cap V, \lambda(p) = 0\}$. In other words, N is given by δ linear forms, which vanish on $I \cap V$. Such maps N will help us to recover TNFs. We therefore introduce the following terminology.

Definition 2.3. *If $\mathcal{N} : V \to B$ is a TNF and $N = P \circ \mathcal{N}$ for some isomorphism $P : B \to \mathbb{C}^\delta$, we say that N* covers *the TNF $\mathcal{N}$.*

If $N : V \to \mathbb{C}^\delta$ covers a TNF $\mathcal{N} : V \to B$, the above discussion suggests that $P = N_{|B}$ and $\mathcal{N} = (N_{|B})^{-1} \circ N = P^{-1}N$ for some $B \subset V$ and that $m_{x_i} = (N_{|B})^{-1} \circ N_i = P^{-1}N_i$. This raises the following questions. Let $N : V \to \mathbb{C}^\delta$ be a linear map with $V \subset R$ a finite dimensional subvector space. What are the conditions on N, V such that N covers a TNF $\mathcal{N}$ w.r.t I? Also, which subspaces $B \subset V$ such that $x_i \cdot B \in V, i = 1, \dots, n$ can we identify with R/I? That is, the map $N : V \to \mathbb{C}^\delta$ might cover different TNFs $\mathcal{N} : V \to B$ and $\mathcal{N}' : V \to B'$. Theorem 3.1 gives an answer to these questions.

In some interesting cases, a map $N : V \to \mathbb{C}^\delta$ covering a TNF can be computed as the cokernel of a *resultant map*. Such a map is defined as follows.

Definition 2.4 (Resultant map)**.** *Let $\mathbf{f} = [f_1, \dots, f_s] \in R^s$. A* resultant map *w.r.t.* $\mathbf{f}$ *is a map*

$$M : \quad V_1 \times \cdots \times V_s \longrightarrow \quad V : (q_1, \dots, q_s) \longmapsto \quad q_1 f_1 + \cdots + q_s f_s.$$

with $V_i, V \subset R$ finite dimensional vector subspaces.

Note that all resultant maps with respect to $\mathbf{f}$ share the property that $\mathrm{im}(M) \subset I \cap V$ where $I = \langle f_1, \dots, f_s \rangle$. Hence, if $N = \mathrm{coker}(M)$ (i.e. $\ker(N) = \mathrm{im}(M)$, the cokernel map is defined up to isomorphism), we have $\ker(N) \subset I \cap V$. In the following sections, we show how TNFs are covered by the cokernel of a specific resultant map in the affine, toric, homogeneous and multihomogenous setting when I is a complete intersection.

3 Ideals defining points in $\mathbb{C}^n$

We consider a 0-dimensional ideal $I = \langle f_1, \dots, f_s \rangle \subset R$ generated by s polynomials in n variables with $\delta < \infty$ solutions in $\mathbb{C}^n$, counting multiplicities. For any ideal $J \subset R$ and $p \in R$, we denote $(J : p) = \{q \in R \mid pq \in J\}$ and $(J : p^*) = \{q \in R \mid \exists k \in \mathbb{N} \ s.t. \ p^k q \in J\}$.

3.1 Characterization of TNFs

Theorem 3.1. *Let I be as defined above. Let $V \subset R$ be a finite dimensional subvector space and let $W = \{f \in V : x_i f \in V, i = 1, \dots, n\}$. Suppose we have a $\mathbb{C}$-linear map $N : V \to \mathbb{C}^\delta$ such that*

1. *$\exists u \in V$ such that $u + I$ is a unit in R/I,*
2. *$\ker(N) \subset I \cap V$,*
3. *$N_{|W}$ is onto $\mathbb{C}^\delta$.*

Then for any δ-dimensional vector subspace $B \subset W$ such that $N_{|B}$ is invertible we have:

(i) there is an isomorphism of R-modules $B \simeq R/I$,

(ii) $V = B \oplus (I \cap V)$ and $I = (\langle \ker(N) \rangle : u)$,

(iii) the maps N_i given by

$$N_i : \ B \longrightarrow \mathbb{C}^\delta, \quad b \longrightarrow N(x_i \cdot b)$$

for $i = 1, \dots, n$ can be decomposed as $N_i = N_{|B} \circ m_{x_i}$ where $m_{x_i} : B \to B$ define the multiplications by x_i in B modulo I and are commuting ($m_{x_i} \circ m_{x_j} = m_{x_j} \circ m_{x_i}$ for $1 \le i < j \le n$).

Proof. (i) It follows from the fact that $N_{|B}$ is invertible that $V = B \oplus \ker(N)$. Let $\pi : V \to B$ be the projection onto B along $\ker(N)$ and define

$$\begin{aligned} m_{x_i}: \ & B \longrightarrow B, \\ & b \longrightarrow \pi(x_i \cdot b). \end{aligned}$$

Then $\forall b \in B$,

$$\begin{aligned} m_{x_i}(b) &= x_i \cdot b \mod \ker(N) & (1) \\ &= x_i \cdot b \mod I & (2) \end{aligned}$$

where the last equality follows from $\ker(N) \subset I \cap V$.

For $\alpha \in \mathbb{N}^n$, we write $\mathbf{m}^\alpha = m_{x_1}^{\alpha_1} \circ \cdots \circ m_{x_n}^{\alpha_n}$ and for $f = \sum_{i=1}^p c_i x^{\alpha_i} \in R$ we define

$$f(\mathbf{m}) = \sum_{i=1}^p c_i \mathbf{m}^{\alpha_i} : B \to B.$$

Replacing u by $\pi(u)$ which is also invertible in R/I, we can assume that $u \in B$. We will show that the sequence

$$\begin{array}{c} 0 \longrightarrow J \longrightarrow R \xrightarrow{\ \phi\ } B \longrightarrow 0 \\ f \longrightarrow f(\mathbf{m})(u) \end{array}$$

with $J = \ker(\phi)$ is exact. From (2), we deduce that $\forall f \in R, \phi(f) = f\,u \mod I$ so that $J = \ker\phi \subset I$. If $\pi_I : R \to R/I$ is the map that sends f to its residue class in R/I, we have $\pi_I(\phi(f)) = \pi_I(f\,u)$. Hence $\pi_I(\phi(R)) = \pi_I(R\,u) = R/I$ since u is invertible in R/I and $\dim_{\mathbb{C}}(\phi(R)) \geq \dim_{\mathbb{C}}(R/I) = \delta$. But also $\phi(R) \subset B$ means $\dim_{\mathbb{C}}(\phi(R)) \leq \dim_{\mathbb{C}}(B) = \delta$. We deduce that ϕ is surjective and $\pi_I : B \to R/I$ is an isomorphism. It follows that the induced map $\overline{\phi} : R/J \to B \simeq R/I$ is an isomorphism of $\mathbb{C}$-vector spaces, which implies $J = I$ since $J \subset I$. We conclude that $\overline{\phi}$ is an isomorphism of R-modules between R/I and B and its inverse is $u^{-1} \cdot \pi_I$. This proves the first point.

(ii) Moreover, $B \cap I = \{0\}$ since $\pi_I : B \to R/I$ is an isomorphism; As B is supplementary to $\ker(N)$ in V and $\ker(N) \subset I \cap V$ by hypothesis, we deduce that $I \cap V = \ker(N)$. It follows that $V = B \oplus \ker(N) = B \oplus (I \cap V)$. We have $\ker(N) \subset I$ and thus $\langle \ker(N) \rangle \subset I$. Therefore $(\langle \ker(N) \rangle : u) \subset (I : u) = I$ since u is a unit in R/I. To prove the reverse inclusion, notice that if $f \in I = J = \ker\phi$ then by the relation (1), $f\,u \in \langle \ker(N) \rangle$. This implies that

$$I \subset (\langle \ker(N) \rangle : u) \subset I,$$

which proves the second point.

(iii) From Equation (2) and the isomorphism $\overline{\phi}$ between R/I and B, we deduce that the operators m_{x_i} correspond to the multiplications by the variables x_i in the quotient algebra R/I. Thus they are commuting. By construction, we have $N_i(b) = N(x_i \cdot b) = N(\pi(x_i \cdot b)) = (N_{|B} \circ m_{x_i})(b)$, where the second equality follows from $\ker(\pi) = \ker(N)$. This concludes the proof of the third point. □

Corollary 3.2. *A linear map $N : V \to \mathbb{C}^\delta$ covers a TNF $\mathcal{N}$ with respect to I if and only if N, V satisfy the conditions of Theorem 3.1.*

Proof. For the if direction, take any $B \subset W$ for which $N_{|B}$ is invertible and $(N_{|B})^{-1} \circ N$ is a TNF by Theorem 3.1. For the other implication, if N covers a TNF, then $N = P \circ \mathcal{N}$ for some isomorphism $P : B \to \mathbb{C}^\delta$, $B \subset W$. Hence $N_{|B} = P$ and $N_{|W}$ is onto $\mathbb{C}^\delta$. It is clear from the properties of TNFs that $\ker(N) = I \cap V$. For the first condition, if the isomorphism $R/I \simeq B$ is given by $\overline{\phi}$, we can take $u = \overline{\phi}(1 + I) \in B \subset V$ and we are done. □

It follows from Theorem 3.1 that once we have a matrix representation of $N, N_{|B}$ and the $N_i, i = 1, \ldots, n$, the matrices m_{x_i} are given by $(N_{|B})^{-1} N_i$. The eigenvalues $z_{ji}, j = 1, \ldots, \delta$ of the m_{x_i} can be computed as the generalized eigenvalues of $N_i v = \lambda N_{|B} v$. As detailed in Section 7, computing the eigenvalues and eigenvectors of the operators of multiplication yields the solutions of the polynomial equations.

Consider the map ϕ from the proof of Theorem 3.1. When $u = 1 \in V$, then $\forall b \in B, \phi(b) = b \mod I$. Since $B \cap I = \{0\}$, we have $\forall b \in B$, $\phi(b) = b$ and ϕ is the normal form or ideal projector on B along its kernel I. Moreover, (iii) implies that $\langle \ker(N) \rangle = I$.

By the normal form characterization proved in [32, 35], if the set B is connected to 1 ($1 \in B$ and there exist vector spaces $B_l \subset R$ such that $B_0 = \text{span}(1) = \mathbb{C} \subset B_1 \subset \cdots \subset B_k = B$ with $B_{l+1} \subset B_l^+$ where $B_l^+ = B_l + x_1 B_l + \cdots + x_n B_l$), then the commutation property (point (iv)) implies that $B \simeq R/I$ (point (ii)).

3.2 Constructing N for dense square systems

We now show how the cokernel of a particular resultant map gives a map N and a subspace V satisfying the conditions of Theorem 3.1. Consider a zero-dimensional ideal $I = \langle f_1, \ldots, f_n \rangle \subset R$ such that the f_i define a system of polynomial equations that has no solutions at infinity. That is, denoting $\deg(f_i) = d_i$, we assume that the f_i are generic in the sense that there are $\delta = \prod_{i=1}^n d_i$ solutions, counting multiplicities, in $\mathbb{C}^n$. A classical result in algebraic geometry, called *Bézout's theorem*, tells us that this is indeed what happens generically (see for instance [23, Chapter I, Theorem 7.7] or [17, Chapter 5]). We denote these solutions by $\mathbb{V}(I) = \{z_1, \ldots, z_{\delta_0}\} \subset \mathbb{C}^n$, where $\delta_0 \le \delta$ is the number of distinct solutions. Next, we consider a generic linear polynomial f_0. We use the classical Macaulay resultant matrix construction defined as follows. Let $\rho = \sum_{i=1}^n d_i - n + 1$, let $V = R_{\le \rho}$ be the space of polynomials of degree $\le \rho$ and $V_i = R_{\le \rho - d_i}$. The associated resultant map is

$$\begin{array}{rccl} M_0 : & V_0 \times V_1 \times \cdots \times V_n & \longrightarrow & V \\ & (q_0, q_1, \ldots, q_n) & \longmapsto & q_0 f_0 + q_1 f_1 + \cdots + q_n f_n. \end{array}$$

For convenience, we use the standard monomial basis for V and the V_i and think of M_0 as a matrix. There is a square submatrix M' of the matrix of M_0 such that $\det(M')$ is a nontrivial multiple of the resultant $\text{Res}(f_0, f_1, \ldots, f_n)$ [9, 29]. In the notation of [41], the monomial multiples of f_0 involved in M' have exponents in $\Sigma_0 = \{\alpha \in \mathbb{N}^n : \alpha_i < d_i, i = 1, \ldots, n\}$. The set $\mathcal{B}_0$ of monomials with exponents in Σ_0 corresponds generically to a basis (the so-called Macaulay basis) of R/I: $B_0 = \text{span}(\mathcal{B}_0) \simeq R/I$. The matrix M' decomposes as

$$M' = \begin{bmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{bmatrix}$$

where the rows and columns of the first block M_{00} are indexed by $\mathcal{B}_0$. The matrix $\tilde{M} = \begin{bmatrix} M_{01} \\ M_{11} \end{bmatrix}$ representing monomial multiples of $f_1, \ldots, f_n$ is such that $\text{im}(\tilde{M}) \subset I \cap V$. Since for generic systems $f_1, \ldots, f_n$, the matrix M_{11} is invertible (see [29], [9, Chapter 3]), the rank of $\tilde{M}$ is $\dim V - \delta$. Let N be the coefficient matrix of a basis of the left null-space of $\tilde{M}$ so that $N \tilde{M} = 0$. Then N corresponds to a linear map $V \to \mathbb{C}^\delta$ of rank δ such that its kernel is $\text{im}(\tilde{M}) \subset I$. In fact, denoting $M = (M_0)_{|V_1 \times \cdots \times V_n}$ (i.e. $M(q_1, \ldots, q_n) = q_1 f_1 + \ldots + q_n f_n$) it satisfies

$$\ker(N) = \text{im}(\tilde{M}) = \text{im}(M) = I \cap V = I_{\le \rho},$$

since $B_0 \cap I = \{0\}$ and M_{11} is invertible, so that any element in $\text{im}(M)$ can be projected in $B_0 \cap I$ along $\text{im}(\tilde{M})$ (i.e. $\text{im}(M) \subset \text{im}(\tilde{M}) \subset \text{im}(M)$).

In order to apply Theorem 3.1, we need to restrict N to a subset $W \subset V$, such that $x_i \cdot W \subset V$ and $N_{|W}$ is surjective. Let us take $W = R_{\le \rho - 1}$. Since M_{11} is invertible, N is equivalent to the matrix $\begin{bmatrix} \text{id} & -M_{01} M_{11}^{-1} \end{bmatrix}$ where the columns of the $\delta \times \delta$ identity block are indexed by the monomials in $\mathcal{B}_0$. Since $B_0 \subset W$, we deduce that $N_{|W}$ is surjective.

This leads to Algorithm 1 for computing the algebra structure of R/I. Note that in step 5 of the algorithm we make a choice of monomial basis for R/I. In order to have accurate multiplication matrices, $N_{|B}$ should be 'as invertible as possible'. A good choice here is to use QR with optimal column pivoting on the matrix $N_{|W}$, such that $\mathcal{B}$ corresponds to a well-conditioned submatrix. This technique is used for the choice of basis on M in [41]. We use M instead of $\tilde{M}$ for numerical reasons. It leads to a more accurate computation of the null space.

Algorithm 1 Computes the structure of the algebra R/I (affine, dense case)

1: **procedure** AlgebraStructure($f_1, \ldots, f_n$)
2: $\quad M \leftarrow$ the resultant map on $V_1 \times \cdots \times V_n$
3: $\quad N \leftarrow \text{null}(M^\top)^\top$
4: $\quad N_{|W} \leftarrow$ columns of N corresponding to monomials of degree $< \rho$
5: $\quad N_{|B} \leftarrow$ columns of $N_{|W}$ corresponding to an invertible submatrix
6: $\quad \mathcal{B} \leftarrow$ monomials corresponding to the columns of $N_{|B}$
7: $\quad$ **for** $i = 1, \ldots, n$ **do**
8: $\quad\quad N_i \leftarrow$ columns of N corresponding to $x_i \cdot \mathcal{B}$
9: $\quad\quad m_{x_i} \leftarrow (N_{|B})^{-1} N_i$
10: $\quad$ **end for**
11: $\quad$ **return** $m_{x_1}, \ldots, m_{x_n}$
12: **end procedure**

Example 3.3. *Consider the ideal* $I = \langle f_1, f_2 \rangle \subset \mathbb{C}[x_1, x_2]$ *given by*

$$\begin{aligned} f_1 &= 7 + 3x_1 - 6x_2 - 4x_1^2 + 2x_1x_2 + 5x_2^2, \\ f_2 &= -1 - 3x_1 + 14x_2 - 2x_1^2 + 2x_1x_2 - 3x_2^2. \end{aligned}$$

As illustrated in Figure 1, the solutions are $z_1 = (-2, 3), z_2 = (3, 2), z_3 = (2, 1), z_4 = (-1, 0)$. *The dense Macaulay matrix* M *of degree* $\rho = d_1 + d_2 - n + 1 = 3$ *is*

$$M^\top = \begin{array}{c} \\ f_1 \\ x_1 f_1 \\ x_2 f_1 \\ f_2 \\ x_1 f_2 \\ x_2 f_2 \end{array} \begin{array}{c} \begin{array}{cccccccccc} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{array} \\ \left[\begin{array}{cccccccccc} 7 & 3 & -6 & -4 & 2 & 5 & & & & \\ & 7 & & 3 & -6 & & -4 & 2 & 5 & \\ & & 7 & & 3 & -6 & & -4 & 2 & 5 \\ -1 & -3 & 14 & -2 & 2 & -3 & & & & \\ & -1 & & -3 & 14 & & -2 & 2 & -3 & \\ & & -1 & & -3 & 14 & & -2 & 2 & -3 \end{array}\right] \end{array}.$$

Since all solutions are simple, a basis for the left null space of M *is given by* $v^{(3)}(z_i), i = 1, \ldots, 4$, *where*

$$v^{(3)}(x_1, x_2) = \begin{bmatrix} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{bmatrix}.$$

These are the linear functionals $\eta_i, i = 1, \ldots, 4$ *in* $V^* \cap I^\perp$ *representing 'evaluation in* z_i*'. We find*

$$N = \begin{array}{c} \\ v^{(3)}(-2,3) \\ v^{(3)}(3,2) \\ v^{(3)}(2,1) \\ v^{(3)}(-1,0) \end{array} \begin{array}{c} \begin{array}{cccccccccc} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{array} \\ \left[\begin{array}{cccccccccc} 1 & -2 & 3 & 4 & -6 & 9 & -8 & 12 & -18 & 27 \\ 1 & 3 & 2 & 9 & 6 & 4 & 27 & 18 & 12 & 8 \\ 1 & 2 & 1 & 4 & 2 & 1 & 8 & 4 & 2 & 1 \\ 1 & -1 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \end{array}\right] \end{array}.$$

For $\mathcal{B} = \{x_1, x_2, x_1^2, x_1x_2\}$, *the submatrices we need are*

$$N_{|B} = \begin{bmatrix} -2 & 3 & 4 & -6 \\ 3 & 2 & 9 & 6 \\ 2 & 1 & 4 & 2 \\ -1 & 0 & 1 & 0 \end{bmatrix}, \quad N_1 = \begin{bmatrix} 4 & -6 & -8 & 12 \\ 9 & 6 & 27 & 18 \\ 4 & 2 & 8 & 4 \\ 1 & 0 & -1 & 0 \end{bmatrix}, \quad N_2 = \begin{bmatrix} -6 & 9 & 12 & -18 \\ 6 & 4 & 18 & 12 \\ 2 & 1 & 4 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

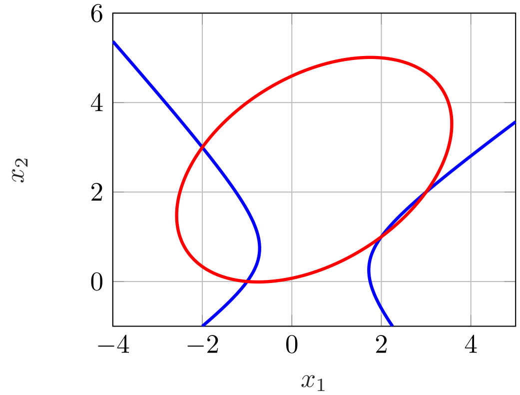

Figure 1: Picture in $\mathbb{R}^2$ of the algebraic curves $\mathbb{V}(f_1)$ (blue) and $\mathbb{V}(f_2)$ (red) from Example 3.3.

corresponding to $\mathcal{B}, x_1 \cdot \mathcal{B}$ and $x_2 \cdot \mathcal{B}$ respectively. The vector space B in this example is the space of polynomials supported in $\mathcal{B}$. One can check that $N_{|B}$ is invertible. Using Matlab, we find the eigenvalues of $N_2 v = \lambda N_{|B} v$ via the command `eig`. The eigenvalues are $0, 1, 2, 3$ as expected. Of course, in practice we do not know the solutions and we cannot construct the nullspace in this way. Any basis will do, since using another basis comes down to left multiplying N and the N_i by an invertible matrix. Note that $\mathcal{B}$ does not correspond to any monomial order and it is not connected to one, so it does not correspond to a Groebner or a border basis.

4 Ideals defining points in $(\mathbb{C}^*)^n$

We now switch to another setting, in which we want to find the roots in the algebraic torus $(\mathbb{C}^*)^n$ of a set of Laurent polynomials. Denote by

$$R_{x_1 \cdots x_n} = \mathbb{C}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}] = \mathbb{C}[x, x^{-1}]$$

the localization of R at $x_1 \cdots x_n$. We consider a zero-dimensional ideal

$$I = \langle f_1, \ldots, f_s \rangle \subset R_{x_1 \cdots x_n}$$

generated by s Laurent polynomials in n variables. Its localization is denoted $I^* = I \cdot R_{x_1 \cdots x_n} \cap R$. Hereafter, we assume that I^* defines δ solutions, counting multiplicities. These are the solutions of I which are in $(\mathbb{C}^*)^n$.

4.1 Characterization of TNFs

Theorem 4.1. *Let I, I^* be as defined above. Let $V \subset R$ be a finite dimensional subvector space and let $W = \{f \in V : x_i f \in V, i = 1, \ldots, n\}$. Suppose we have a $\mathbb{C}$-linear map $N : V \to \mathbb{C}^\delta$ such that*

1. *$\exists u \in V$ such that $u + I$ is a unit in R/I^*,*
2. *$\ker(N) \subset I \cap V$,*
3. *$N_{|W}$ is onto $\mathbb{C}^\delta$.*

Then for any δ-dimensional vector subspace $B \subset W$ such that $N_{|B}$ is invertible we have:

(i) there is an isomorphism of R-modules $B \simeq R/I^*$,

(ii) $V = B \oplus (I^* \cap V)$ and $(\langle \ker(N) \rangle : u) = I^*$ for any monomial $u \in V$.

(iii) the maps N_i given by

$$\begin{aligned} N_i:\ B &\longrightarrow \mathbb{C}^\delta, \\ b &\longrightarrow N(x_i \cdot b) \end{aligned}$$

for $i = 1, \ldots, n$ can be decomposed as $N_i = N_{|B} \circ m_{x_i}$ where $m_{x_i} : B \to B$ define the multiplications by x_i in B modulo I^* and are commuting.

Proof. We apply Theorem 3.1 with $I^* \supset I$. □

Note that if V contains at least one monomial of R, then the first condition is automatically satisfied since the residue class of any monomial is a unit in R/I^*.

Corollary 4.2. *A linear map $N : V \to \mathbb{C}^\delta$ covers a TNF $\mathcal{N}$ with respect to I^* if and only if N, V satisfy the conditions of Theorem 4.1.*

Proof. The proof is analogous to the proof of Corollary 3.2. □

Again, the eigenvalues $z_{ji}, j = 1, \ldots, \delta$ of the m_{x_i} can be computed as the generalized eigenvalues of $N_i v = \lambda N_{|B} v$, once we have a matrix representation of $N_{|B}$ and the $N_i, i = 1, \ldots, n$. The map $(N_{|B})^{-1} \circ N$ is a TNF with respect to I^*.

4.2 Constructing N for square systems

For the construction of N in the toric case we rely on the famous BKK-theorem by Bernstein [4], Kushnirenko [27] and Khovanskii [26] that bounds the number of solutions in the algebraic torus for a sparse, square system. To state it, we need a few definitions. More details can be found in [9, 21, 39]. To any Laurent polynomial in $R_{x_1 \cdots x_n}$ we associate a convex polytope in $\mathbb{R}^n$ in the following way.

Definition 4.3 (Newton polytope)**.** *Let $f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha \in R_{x_1 \cdots x_n}$ be a nonzero Laurent polynomial. The* Newton polytope *P of f is the polytope*

$$P = \mathrm{Conv}(\alpha \in \mathbb{Z}^n : c_\alpha \neq 0) \subset \mathbb{R}^n,$$

where $\mathrm{Conv}(\cdot)$ *takes the convex hull in $\mathbb{R}^n$.*

Definition 4.4 (Minkowski sum)**.** *Let P and Q be polytopes in $\mathbb{R}^n$. The* Minkowski sum *of P and Q is*

$$P + Q = \{p + q : p \in P, q \in Q\}.$$

Definition 4.5 (Mixed volume)**.** *The n-dimensional* mixed volume *of a collection of n polytopes $P_1, \ldots, P_n$ in $\mathbb{R}^n$, denoted by* $\mathrm{MV}(P_1, \ldots, P_n)$*, is the coefficient of the monomial $\lambda_1 \lambda_2 \cdots \lambda_n$ in the homogeneous polynomial* $\mathrm{Vol}_n(\sum_{i=1}^n \lambda_i P_i)$*.*

Theorem 4.6 (Bernstein's Theorem)**.** *Let $I = \langle f_1, \ldots, f_n \rangle \subset R_{x_1 \cdots x_n}$ define a zero-dimensional ideal and let P_i be the Newton polytope of f_i. The number of points in $\mathbb{V}(I) \cap (\mathbb{C}^*)^n$ is bounded above by* $\mathrm{MV}(P_1, \ldots, P_n)$*. Moreover, for generic choices of the coefficients of the f_i, the number of roots in $(\mathbb{C}^*)^n$, counting multiplicities, is exactly equal to* $\mathrm{MV}(P_1, \ldots, P_n)$*.*

Proof. For sketches of the proof we refer to [9, 39]. For details, the reader may consult Bernstein's original paper [4]. A proof based on homotopy continuation is given in [24]. □

The type of genericity we assume in this section is that the number of solutions of I in $(\mathbb{C}^*)^n$, counting multiplicities, is exactly $\mathrm{MV}(P_1, \ldots, P_n)$. Let f_0 be a generic linear polynomial and let $v \in \mathbb{R}^n$ be a generic, small n-tuple. The vector v represents a small displacement vector, which is commonly used in the context of sparse resultants (see for instance [9, Chapter 7, §6] or [19]). We consider the resultant map

$$\begin{array}{rrcl} M_0: & V_0 \times V_1 \times \cdots \times V_n & \longrightarrow & V \\ & (q_0, q_1, \ldots, q_n) & \longmapsto & q_0 f_0 + q_1 f_1 + \cdots + q_n f_n. \end{array}$$

where $V_i = \bigoplus_{\alpha \in \mathcal{S}_i} \mathbb{C} \cdot x^\alpha$, $\mathcal{S}_i = (P_0 + \ldots + \hat{P}_i + \ldots + P_n + v) \cap \mathbb{Z}^n$ (the notation $\hat{P}_i$ means that this term is left out) and $V = \bigoplus_{\alpha \in \mathcal{S}} \mathbb{C} \cdot x^\alpha$, $\mathcal{S} = (\sum_{i=0}^n P_i + v) \cap \mathbb{Z}^n$. We can select a square submatrix M' of this map, so that $\det(M')$ is a nontrivial multiple of the toric resultant of $f_0, f_1, \ldots, f_n$ [18, 9]. We set $W = \{f \in V : x_i \cdot f \in V, i = 1, \ldots, n\}$. As for the Macaulay resultant matrix, we write

$$M' = \begin{bmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{bmatrix}$$

where the rows and columns of M_{00} are indexed by a set $\mathcal{B}_0 \subset W$ of monomials which is a basis of R/I and M_{11} is invertible. Denoting as in Section 3 by $\tilde{M}$ the right block column of M' and by N its cokernel, we have again that $\ker(N) = \operatorname{im}(\tilde{M}) = \operatorname{im}(M) = I \cap V$ with $M = (M_0)_{|V_1 \times \cdots \times V_n}$. Since $\mathcal{B}_0 \subset W$, $N_{|W}$ is surjective and we can apply Theorem 4.1. Algorithm 2 only differs from Algorithm 1 by the construction of M.

Algorithm 2 Computes the algebra structure of R/I^* (generic, sparse case)

procedure AlgebraStructure($f_1, \ldots, f_n$)
  $M \leftarrow$ the toric resultant map on $V_1 \times \cdots \times V_n$
  $N \leftarrow \text{null}(M^\top)^\top$
  $N_{|W} \leftarrow$ columns of N corresponding to monomials x^α such that $x^\alpha \in W$
  Apply Algorithm 1 from step 5 onward.
end procedure

5 Ideals defining points in $\mathbb{P}^n$

Suppose we are interested in finding all projective roots of a system of homogeneous equations. Denote $S = \mathbb{C}[x_0, x_1, \ldots, x_n]$ and let $I = \langle f_1, \ldots, f_s \rangle \subset S$ be a zero-dimensional ideal generated by s homogeneous polynomials in $n+1$ variables with $\delta < \infty$ solutions in $\mathbb{P}^n$, counting multiplicities. We denote $S_d \subset S$ for the subvector space of homogeneous polynomials of degree d and the zero polynomial. Take $h = h_0 x_0 + \ldots + h_n x_n \in S_1 \backslash \{0\}$ such that $h + I$ is not a zero divisor in S/I. We can assume without loss of generality that $h_0 \neq 0$. Let $R = \mathbb{C}[y_1, \ldots, y_n]$ be the ring of polynomials in n variables. We have homogenization isomorphisms

$$\begin{aligned} \sigma_d :\ & R_{\leq d} \longrightarrow S_d, \\ & f \longrightarrow h^d f\left(\frac{x_1}{h}, \ldots, \frac{x_n}{h}\right) \end{aligned}$$

for every $d \in \mathbb{N}$. The inverse dehomogenization map in degree d is given by

$$\begin{aligned} \sigma_d^{-1} :\ & S_d \longrightarrow R_{\leq d}, \\ & f \longrightarrow f\left(\frac{1 - \sum_{i=1}^n h_i y_i}{h_0}, y_1, \ldots, y_n\right). \end{aligned}$$

Its definition is independent of the degree d, so that we can omit d and denote it σ^{-1}. The ideal $\tilde{I} = \langle \sigma^{-1}(f_1), \ldots, \sigma^{-1}(f_n) \rangle \subset R$ has δ solutions in $\mathbb{C}^n$, counting multiplicities.

5.1 Characterization of TNFs and a new criterion for regularity

In this section we show how Theorem 3.1 can be used to compute projective coordinates of the points defined by I. Let $V = S_d, W = S_{d-1}$ and suppose we have a map $N : V \to \mathbb{C}^\delta$ such that $\ker(N) \subset I_d = I \cap V$. We also assume that there exists $h \in S_1$ such that the map

$$N_h : \; W \longrightarrow \mathbb{C}^\delta, \quad f \longrightarrow N(h \cdot f)$$

is surjective. Let

$$N_i : \; W \longrightarrow \mathbb{C}^\delta, \quad f \longrightarrow N(x_i \cdot f).$$

Then $N_h = \sum_{i=1}^n h_i N_i$ where $h = h_0 x_0 + \cdots + h_n x_n, h_0 \neq 0$.

Let $\tilde{V} = R_{\leq d}$ and $\tilde{W} = R_{\leq d-1}$. The map $\tilde{N} : \tilde{V} \to \mathbb{C}^\delta$ given by $\tilde{N} = N \circ \sigma_d$ is surjective and $\ker(\tilde{N}) \subset \tilde{I} \cap \tilde{V}$. Also, $y_i \cdot \tilde{W} \subset \tilde{V}$, $i = 1, \dots, n$. For $f \in \tilde{W}$, $\sigma_d(f) = h \cdot \sigma_{d-1}(f)$. Therefore $\tilde{N}(\tilde{W}) = N(h \cdot W)$ and $\tilde{N}_{|\tilde{W}} = N_h \circ \sigma_{d-1}$ is surjective. It follows from this discussion and from Theorem 3.1 that $\tilde{N}$ covers a TNF w.r.t. $\tilde{I}$. The map N can be used to compute projective coordinates of the solutions. The following theorem shows how that works.

Theorem 5.1. *Let I be as defined above and let $V = S_d, W = S_{d-1}$. Suppose we have a linear map $N : V \to \mathbb{C}^\delta$ and a linear form $h \in S_1$ such that*

1. $\ker(N) \subset I \cap V$,
2. *N_h is onto $\mathbb{C}^\delta$.*

Then for any subspace $B \subset W$ such that $(N_h)_{|B}$ is invertible, we have:

(i) there is an isomorphism of $\mathbb{C}\left[\frac{x_0}{h}, \cdots, \frac{x_n}{h}\right]$-modules $h \cdot B \simeq S_d / I_d$,

(ii) $S_k = h^{k-d+1} \cdot B \oplus I_k$ for $k \geq d$ and $I = (\langle \ker(N) \rangle : h^*)$.

(iii) the maps N_i given by

$$N_i : \; B \longrightarrow \mathbb{C}^\delta, \quad b \longrightarrow N(x_i \cdot b)$$

for $i = 0, \dots, n$ can be decomposed as $N_i = (N_h)_{|B} \circ m_{x_i}$, where m_{x_i} represent the multiplications by x_i/h in $h \cdot B$ modulo I_d and are commuting.

Proof. We apply Theorem 3.1 to $\tilde{N} = R_{\leq d}$ and $\tilde{W} = R_{\leq d-1} \ni 1$. Let B be a supplementary space of $\ker(N_h)$ in S_{d-1}. Then $\tilde{B} = \sigma^{-1}(B)$ is a supplementary vector space of $\ker(\tilde{N}_{|\tilde{W}})$ in $\tilde{W}$.

(i) Theorem 3.1 gives $\tilde{B} \simeq R/\tilde{I}$. Applying σ_d gives $h \cdot B \simeq S_d / I_d$.

(ii) Theorem 3.1 implies that $\tilde{V} = \tilde{B} \oplus (\tilde{I} \cap \tilde{V})$. More generally, we have $\tilde{R}_{\leq k} = \tilde{B} \oplus (\tilde{I} \cap \tilde{R}_{\leq k})$ for $k \geq d$. By applying σ_k for $k \geq d$, we have $S_k = h^{k-d+1} B \oplus I_k$. From Theorem 3.1, we also have $\tilde{I} = \langle \ker(\tilde{N}) \rangle$. By applying σ_k for $k \in \mathbb{N}$, we deduce that $I = (\langle \ker(N) \rangle : h^*)$, which proves the second point.

(iii) Let m_{y_i} be the maps from Theorem 3.1. Consider the induced maps

$$m_{x_i} = \sigma_d \circ m_{y_i} \circ \sigma^{-1}, i = 1, \dots, n$$

and

$$m_{x_0} = \sigma_d \circ \left(\frac{1 - \sum_{i=1}^n h_i y_i}{h_0} \right) (\mathbf{m}) \circ \sigma^{-1},$$

By definition, for $i = 1, \ldots, n$ and $b \in B$, we have $N(x_i \cdot b) = \tilde{N}(\sigma^{-1}(x_i \cdot b)) = \tilde{N}(y_i \cdot \sigma^{-1}(b))$. By Theorem 3.1 this can be written as $\tilde{N}(y_i \cdot \sigma^{-1}(b)) = (\tilde{N}_{|\tilde{B}} \circ m_{y_i})(\sigma^{-1}(b)) = ((N_h)_{|B} \circ \sigma_d \circ m_{y_i})(\sigma^{-1}(b))$. And since $\sigma_d \circ m_{y_i} = m_{x_i} \circ \sigma_d$ we get $N_i(b) = ((N_h)_{|B} \circ m_{x_i})(h \cdot b)$. Analogously, using linearity, for N_0 we have

$$N(x_0 \cdot b) = \tilde{N}\left(\frac{1 - \sum_{i=1}^n h_i y_i}{h_0} \cdot \sigma^{-1}(b)\right) = ((N_h)_{|B} \circ m_{x_0})(h \cdot b).$$

We now show that m_{x_i} represents the multiplication by x_i/h in $h \cdot B \subset h \cdot S_{d-1}$ modulo I_d. For $b \in B$, let $\sigma^{-1}(h \cdot b) = \sigma^{-1}(b) = \tilde{b} \in \tilde{B}$ and $m_{y_i}(\tilde{b}) = y_i \cdot \tilde{b} - p$ with $p \in \tilde{I}$. Then for $i = 1, \ldots, n$,

$$m_{x_i}(h \cdot b) = \sigma_d(y_i \cdot \tilde{b} - p) = x_i \cdot \sigma_{d-1}(\tilde{b}) - \sigma_d(p) = x_i \cdot b \mod I_d.$$

For m_{x_0}, the result follows from $\sigma_1\left(\frac{1-\sum_{i=1}^n h_i y_i}{h_0}\right) = x_0$.

□

It follows that once we have a matrix representation of $(N_h)_{|B}$ and of the N_i, we have that $m_{x_i} = ((N_h)_{|B})^{-1} N_i$ and the matrices $((N_h)_{|B})^{-1} N_i$ commute, so that for an eigenvalue $\lambda_i = \frac{z_{ji}}{h(z_j)}$ of m_{x_i} and $\lambda_k = \frac{z_{jk}}{h(z_j)}$ of m_{x_k} with common eigenvector v:

$$\lambda_k ((N_h)_{|B})^{-1} N_i v = \lambda_k \lambda_i v = \lambda_i ((N_h)_{|B})^{-1} N_k v.$$

Left multiplication by $(N_h)_{|B}$ gives $\lambda_k N_i v = \lambda_i N_k v$ and the generalized eigenvalues of $N_i v = \lambda N_k v$ are the fractions z_{ji}/z_{jk}. This means that we do not need to construct $(N_h)_{|B}$ to find the projective coordinates of the solutions, as long as we have $N_i, i = 0, \ldots, n$ and a generic linear combination of the N_i is invertible.

The following proposition shows that the hypotheses of Theorem 5.1 can be fulfilled for d greater than or equal to the regularity and provides a new criterion for detecting the d-regularity of a projective zero-dimensional ideal. We recall that the regularity $\mathrm{reg}(I)$ of an ideal I is $\min(d_{i,j} - i)$ where $d_{i,j}$ are the degrees of generators of the i^{th}-syzygy module in a minimal resolution of I (see [16]). An ideal is d-regular if $d \geq \mathrm{reg}(I)$.

Proposition 5.2. *Let I be a homogeneous ideal with $\delta < \infty$ solutions in $\mathbb{P}^n$, counting multiplicities. The following statements are equivalent:*

- *(i) There is a linear map $N : S_d \to \mathbb{C}^\delta$ with $\ker(N) \subset I \cap S_d$ and $N_h : S_{d-1} \to \mathbb{C}^\delta$ given by $N_h(f) = N(h \cdot f)$ surjective for a generic $h \in S_1$,*
- *(ii) I is d-regular.*

Proof. (i) ⇒ (ii). From Proposition 5.1 it follows that we can find $B \subset S_{d-1}$ such that $S_d = h \cdot B \oplus I_d$. Therefore $S_d = \langle I, h \rangle_d$. Denote $(I : h) = \{f \in S : fh \in I\}$. Let $f \in (I : h)_d$. Then $f \equiv h \cdot b \mod I_d$ with $b \in B$ and $h^2 \cdot b \in I_{d+1}$. As we have $S_{d+1} = h^2 \cdot B \oplus I_{d+1}$, we deduce that $b = 0$ and $(I : h)_d = I_d$. By [3, Theorem 1.10], I is d-regular.

(ii) ⇒ (i). Assume that I is d-regular. Let $\delta = \dim_{\mathbb{C}}(S_d/I_d)$. By [16, Theorem 4.2 (3)], d is greater or equal to the regularity index of the Hilbert function. Therefore δ is the value of the constant Hilbert polynomial, that is, the number of solutions in $\mathbb{V}(I)$ counting multiplicities. Consider a basis $\{\eta_1, \ldots, \eta_\delta\}$ of $I_d^\perp \subset S_d^*$. Define

$$\begin{aligned} N : \ & S_d \longrightarrow \mathbb{C}^\delta, \\ & f \longrightarrow (\eta_i(f))_{1 \leq i \leq \delta}. \end{aligned}$$

By construction, $\ker(N) = I_d$. By d-regularity, $\langle I, h \rangle_d = S_d$ for a generic $h \in S_1$ (see [3, Theorem 1.10]). For any $f \in S_d$, we can write $f = \tilde{f} + hg$ with $\tilde{f} \in I_d$ and $g \in S_{d-1}$. Therefore $N(f) = N(hg) = N_h(g)$ and $N(S_d) = N_h(S_{d-1})$. □

5.2 Constructing TNFs

We consider first the case of a square system. From the discussion above, $\tilde{N}$ and N have the same matrix representation. We show how the maps $N, (N_h)_{|B}, N_i$ can be constructed from the null space of the resultant map M, used in the affine, dense case: $\rho = \sum_{i=1}^{n} d_i - (n-1)$. For generic $h = h_0x_0 + \ldots + h_nx_n$, $h_0 \neq 0$, a change of coordinates given by

$$\begin{bmatrix} \hat{x}_0 \\ \hat{x}_1 \\ \vdots \\ \hat{x}_n \end{bmatrix} = \begin{bmatrix} h_0 & h_1 & \cdots & h_n \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{bmatrix}$$

does not alter the rank of the resultant map M and the resulting system has δ affine solutions in $\mathbb{P}^n \backslash \{\hat{x}_0 = 0\}$. In the notation from this section, the associated null space map is $\tilde{N} = N \circ \sigma_\rho$ and $\tilde{N}_{|\tilde{W}} = N_h \circ \sigma_{\rho-1}$ with $\tilde{W} = R_{\leq \rho-1}$ and these maps have all the good properties by the results of Section 3. We obtain Algorithm 3, where the 'homogeneous Macaulay matrix' is the matrix from Algorithm 1 with columns corresponding to homogeneous polynomials and rows indexed by monomials of degree ρ. Note that Algorithm 1 is equivalent to Algorithm 3 when we use $h = x_0$.

Algorithm 3 Computes the algebra structure of S_ρ / I_ρ

---

procedure ALGEBRASTRUCTURE($f_1, \ldots, f_n$)
    $M \leftarrow$ homogeneous Macaulay matrix of degree $\rho = \sum_{i=1}^{n} d_i - (n-1)$
    $N \leftarrow \text{null}(M^\top)^\top$
    $\mathcal{B}_{\rho-1} \leftarrow$ monomials of degree $\rho - 1$
    for $i = 0, \ldots, n$ **do**
        $N_{|W_i} \leftarrow$ columns of N corresponding to $x_i \cdot \mathcal{B}_{\rho-1}$
    end for
    $h \leftarrow$ generic linear form
    $N_h \leftarrow h(N_{|W_0}, \ldots, N_{|W_n})$
    $(N_h)_{|B} \leftarrow$ columns of N_h corresponding to an invertible submatrix
    for $i = 0, \ldots, n$ **do**
        $N_i \leftarrow$ columns of $N_{|W_i}$ corresponding to the columns of $(N_h)_{|B}$
        $m_{x_i} \leftarrow ((N_h)_{|B})^{-1} N_i$
    end for
    return $m_{x_0}, \ldots, m_{x_n}$
end procedure

Example 5.3. *We give an example of a zero-dimensional system of homogeneous equations coming from an affine system with a solution at infinity. Consider the equations* $f_1 = 2x_1^2 + 5x_1x_2 + 3x_2^2 + 3x_1 - 2 = 0$ *and* $f_2 = -2 + x_1 + x_2 = 0$. *After homogenizing we get*

$$\begin{aligned} f_1^h &= 2x_1^2 + 5x_1x_2 + 3x_2^2 + 3x_0x_1 - 2x_0^2 = 0, \\ f_2^h &= -2x_0 + x_1 + x_2 = 0, \end{aligned}$$

with solutions $z_1 = (0, 1, -1), z_2 = (1, -10, 12) \in \mathbb{P}^2$. *Since* f_2^h *is linear, the system could be solved fairly easily by using substitution, but we use this example nonetheless because the matrices involved are not too large and it illustrates the algorithm nicely. We have* $\rho = 2$ *and we set*

$$w^{(2)}(x_0, x_1, x_2) = \begin{bmatrix} x_0^2 & x_0x_1 & x_0x_2 & x_1^2 & x_1x_2 & x_2^2 \end{bmatrix}.$$

We get a null space matrix

$$N = \begin{array}{c} \\ w^{(2)}(0,1,-1) \\ w^{(2)}(0,-10,12) \end{array} \begin{array}{c} \begin{array}{cccccc} x_0^2 & x_0x_1 & x_0x_2 & x_1^2 & x_1x_2 & x_2^2 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & -1 & 1 \\ 1 & -10 & 12 & 100 & -120 & 144 \end{bmatrix} \end{array}.$$

Note that we cannot apply Algorithm 1, since after dehomogenizing by $x_0 = 1$, there is no invertible submatrix of the degree 1 part of N. The $N_{|W_i}$ are

$$N_{|W_0} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -10 & 12 \end{bmatrix}, \; N_{|W_1} = \begin{bmatrix} 0 & 1 & -1 \\ -10 & 100 & -120 \end{bmatrix}, \; N_{|W_2} = \begin{bmatrix} 0 & -1 & 1 \\ 12 & -120 & 144 \end{bmatrix}.$$

A generic linear combination of the first 2 columns of these matrices is invertible. We set N_i to be the first two colums of $N_{|W_i}$. We find that the pencil $N_1 - \lambda N_0$ has eigenvalues $\infty, -10$, which corresponds to the x_1-values of the solutions in the affine chart $x_0 = 1$. We computed this without constructing $(N_h)_{|B}$. For a generic linear form h, set $(N_h)_{|B} = h(N_0, N_1, N_2)$. The eigenvalues of $((N_h)_{|B})^{-1} N_i$ are the values of the i-th coordinate function at the solutions evaluated at $h(x_0, x_1, x_2) = 1$.

Remark 5.4. *In the case of a homogeneous zero-dimensional ideal I generated by a non-square system $\mathbf{f} = [f_1, \ldots, f_s] \in S^s$ of s homogeneous polynomials, we consider the resultant map M of $\mathbf{f}$ in a degree ρ strictly greater than the regularity of the ideal I. In this degree, we have $\dim(S_\rho / I_\rho) = \delta$ and thus $\dim \ker M^\top = \delta$. Then the cokernel N of M satisfies the conditions of Theorem 5.1 and the projective coordinates of the solutions can be recovered.*

6 Ideals defining points in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$

We want to find all roots in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$ of a system of multihomogeneous equations. Denote $S = \mathbb{C}[x_{10}, \ldots, x_{1n_1}, \ldots, x_{k0}, \ldots, x_{kn_k}]$ and let $I = \langle f_1, \ldots, f_s \rangle \subset S$ be an ideal defined by multihomogeneous equations. Here, we take $x_{i0}, \ldots, x_{in_i}$ to be the projective coordinates on the i-th factor $\mathbb{P}^{n_i}$ in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$. We assume that I has $\delta < \infty$ solutions in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$. By S_ρ, $\rho \in \mathbb{N}^k$ we denote the multidegree ρ part of S. That is, S_ρ consists of the elements of S of degree ρ_i in $x_{ij}, j = 0, \ldots, n_i$ and the zero polynomial. Let $R = \mathbb{C}[y_{11}, \ldots, y_{1n_1}, \ldots, y_{k1}, \ldots, y_{kn_k}]$ be the ring of polynomials in $n = \sum_{i=1}^k n_i$ variables and let $h_i = h_{i0} x_{i0} + \ldots + h_{in_i} x_{in_i} \in S_{e_i}, i = 1, \ldots, k$ be generic linear forms in the disjoint sets of projective variables (the vector $e_i \in \mathbb{N}^k$ has 1 as its i-th entry and zero elsewhere). We can assume $h_{i0} \neq 0, \forall i$. We have homogenization isomorphisms

$$\begin{aligned} \sigma_\rho : \; & R_{\leq \rho} \longrightarrow S_\rho, \\ & f \longrightarrow h_1^{\rho_1} \cdots h_k^{\rho_k} f\left(\frac{x_{11}}{h_1}, \ldots, \frac{x_{1n_1}}{h_1} \ldots, \frac{x_{k1}}{h_k}, \ldots, \frac{x_{kn_k}}{h_k}\right) \end{aligned}$$

for every $\rho \in \mathbb{N}^k$. The inverse dehomogenization map is given by

$$\begin{aligned} \sigma^{-1} : \; & S \longrightarrow R, \\ & f \longrightarrow f\left(\frac{1 - \sum_{i=1}^{n_1} h_{1i} y_{1i}}{h_{10}}, y_{11}, \ldots, y_{1n_1}, \ldots, \frac{1 - \sum_{i=1}^{n_k} h_{ki} y_{ki}}{h_{k0}}, y_{k1}, \ldots, y_{kn_k}\right). \end{aligned}$$

The ideal $\tilde{I} = \langle \sigma^{-1}(f_1), \ldots, \sigma^{-1}(f_n) \rangle$ has δ solutions in $\mathbb{C}^n$, counting multiplicities.

6.1 Characterization of TNFs

We are now going to use a variant of Theorem 3.1 to compute multihomogeneous coordinates of the points on $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$ defined by I. Denoting $\mathbf{1} = \sum_{i=1}^k e_i$, let $V = S_\rho, W = S_{\rho - \mathbf{1}}$ and suppose we have $N : V \to \mathbb{C}^\delta$ surjective and $\ker(N) \subset I_\rho = I \cap V$. We assume that there are linear forms $h_i = h_{i0} x_{i0} + \ldots + h_{in_i} x_{in_i} \in S_{e_i}, i = 1, \ldots, k$ such that

$$\begin{aligned} N_h : \; & W \longrightarrow \mathbb{C}^\delta, \\ & f \longrightarrow N(h_1 \cdots h_k \cdot f) \end{aligned}$$

is surjective. We proceed as in the projective case by using the (de)-homogenization isomorphisms. Let $\tilde{V} = R_{\leq \rho}$ and $\tilde{W} = R_{\leq \rho - 1}$. The map $\tilde{N} : \tilde{V} \to \mathbb{C}^\delta$ given by $\tilde{N} = N \circ \sigma_\rho$ is surjective and $\ker(\tilde{N}) \subset \tilde{I} \cap \tilde{V}$.

Also, $y_{ij} \cdot \tilde{W} \subset \tilde{V}$, $i = 1, \ldots, k, j = 1, \ldots, n_i$. For $f \in \tilde{W}$, $\sigma_\rho(f) = h_1 \cdots h_k \cdot \sigma_{\rho-\mathbf{1}}(f)$. Therefore $\tilde{N}(\tilde{W}) = N(h_1 \cdots h_k \cdot W)$ and $\tilde{N}_{|\tilde{W}} = N_h \circ \sigma_{\rho-\mathbf{1}}$ is surjective. Again, according to Theorem 3.1, the map $\tilde{N}$ covers a TNF w.r.t. $\tilde{I}$. The multihomogeneous coordinates can be found using the following theorem which generalizes Theorem 5.1.

Theorem 6.1. *Let I be as defined above and let $V = S_\rho, W = S_{\rho-\mathbf{1}}$. Suppose we have a linear map $N : V \to \mathbb{C}^\delta$ and linear forms $h_i \in S_{e_i}, i = 1, \ldots, n$ such that*

1. $\ker(N) \subset I \cap V$,
2. *N_h is onto $\mathbb{C}^\delta$.*

Then for any subspace $B \subset W$ such that $(N_h)_{|B}$ is invertible, we have:

(i) there is an isomorphism of $\mathbb{C}\left[\frac{x_{11}}{h_1}, \ldots, \frac{x_{1n_1}}{h_1} \ldots, \frac{x_{k1}}{h_k}, \ldots, \frac{x_{kn_k}}{h_k}\right]$-modules $h_1 \cdots h_k \cdot B \simeq S_\rho / I_\rho$,

(ii) $V = h_1 \cdots h_k \cdot B \oplus I_\rho$ and $I = (\langle \ker(N) \rangle : (h_1 \cdots h_k)^*)$.

(iii) the maps N_{ij} given by

$$\begin{aligned} N_{ij} :\ & B \longrightarrow \mathbb{C}^\delta, \\ & b \longrightarrow N(h_1 \cdots \hat{h}_i \cdots h_k \cdot x_{ij} \cdot b) \end{aligned}$$

for $i = 1, \ldots, k, j = 0, \ldots, n_i$ can be decomposed as $N_{ij} = (N_h)_{|B} \circ m_{x_{ij}}$, where $m_{x_{ij}}$ represent the multiplications by x_{ij}/h_i in $h_1 \cdots h_k \cdot B$ modulo I_ρ and are commuting.

Proof. All statements follow from Theorem 3.1 as in the proof of Theorem 5.1. □

6.2 Constructing N for square systems

We show that the maps $N, (N_h)_{|B}, N_{ij}$ can be constructed from the null space of the toric resultant map M as defined for the affine sparse case. Let $I = \langle f_1, \ldots, f_n \rangle$ be defined by $n = n_1 + \ldots + n_k$ multihomogeneous polynomials of degrees $d_i \in \mathbb{N}^k$. A change of projective coordinates within each factor $\mathbb{P}^{n_i}$ does not alter the rank of the resultant map. Take

$$\begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \vdots \\ \hat{x}_k \end{bmatrix} = \begin{bmatrix} H_1 & & & \\ & H_2 & & \\ & & \ddots & \\ & & & H_k \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}, \quad H_i = \begin{bmatrix} h_{i0} & h_{i1} & \ldots & h_{in_i} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

where $\hat{x}_i, x_i$ are short for $(\hat{x}_{i0}, \ldots, \hat{x}_{in_i})^\top$ and $(x_{i0}, \ldots, x_{in_i})^\top$ respectively. Using the notation in this chapter, the resulting ideal after dehomogenization w.r.t. the $\hat{x}_{i0}$ is $\tilde{I} = \langle \tilde{f}_1, \ldots, \tilde{f}_n \rangle \subset R = \mathbb{C}[\hat{x}_1, \ldots, \hat{x}_k]$ with $\delta = \mathrm{MV}(P_1, \ldots, P_n)$ solutions in $\mathbb{C}^n$, counting multiplicities. We may assume that all δ solutions lie in $(\mathbb{C}^*)^n$, since we can apply another generic block diagonal change of coordinates. Next, we consider a generic polynomial $\tilde{f}_0 \in R_{\leq \mathbf{1}}$, so $d_0 = \mathbf{1}$. We denote $\rho = \sum_{i=0}^n d_i - \mathbf{1}$ and $\rho_i = \rho - d_i, i = 0, \ldots, n$ and we consider the resultant map

$$\begin{array}{rccc} \tilde{M}_0 : & \tilde{V}_0 \times \tilde{V}_1 \times \cdots \times \tilde{V}_n & \longrightarrow & \tilde{V} \\ & (q_0, q_1, \ldots, q_n) & \longmapsto & q_0 \tilde{f}_0 + q_1 \tilde{f}_1 + \cdots + q_n \tilde{f}_n. \end{array}$$

with $\tilde{V}_i = R_{\leq \rho_i}$ and $\tilde{V} = R_{\leq \rho}$. Note that this corresponds to the V_i, V in the affine, sparse case, where we take a vector $v = \epsilon(-1, \ldots, -1) \in \mathbb{R}^n$ with $\epsilon > 0$, small. We denote $\tilde{W} = R_{\leq \rho - \mathbf{1}}$. By the discussion in Section 4, the null space map $\tilde{N}$ associated to $(\tilde{M}_0)_{|\tilde{V}_1 \times \cdots \times \tilde{V}_n}$ and the map $\tilde{N}_{|\tilde{W}}$ have all the good properties. By construction, $\tilde{N} = N \circ \sigma_\rho$ and $\tilde{N}_{|\tilde{W}} = N_h \circ \sigma_{\rho-\mathbf{1}}$ where N is the null space map associated to

$$\begin{array}{rrcl} M: & V_1 \times \cdots \times V_n & \longrightarrow & V \\ & (q_1, \ldots, q_n) & \longmapsto & q_1 f_1 + \cdots + q_n f_n, \end{array}$$

with $V_i = S_{\rho_i}$ and $V = S_\rho$.

In Algorithm 4 we use the notation vec : $S_\rho \to \mathbb{C}^{m_\rho}$, where $m_\rho = \dim_{\mathbb{C}}(V)$ is the number of rows of the matrix M, for the map that sends a multihomogeneous polynomial of degree ρ to its column vector representation corresponding to the monomials in the support of M.

Algorithm 4 Computes the algebra structure of S_ρ / I_ρ

procedure AlgebraStructure($f_1, \ldots, f_n$)
    $M \leftarrow$ the multihomogeneous Macaulay matrix of degree ρ
    $N \leftarrow \text{null}(M)^\top$
    $\mathcal{B}_{\rho-\mathbf{1}} \leftarrow$ monomials of degree $\rho - \mathbf{1}$
    for $i = 1, \ldots, k$ **do**
        $h_i \leftarrow$ generic linear form of degree e_i
    end for
    $K \leftarrow$ empty matrix
    for $m \in \mathcal{B}_{\rho-\mathbf{1}}$ **do**
        $K \leftarrow \begin{bmatrix} K & \text{vec}(h_1 \cdots h_k \cdot m) \end{bmatrix}$
    end for
    $N_h \leftarrow NK$
    $(N_h)_{|B} \leftarrow$ columns of N_h corresponding to an invertible submatrix
    $\mathcal{B} \leftarrow$ monomials in $\mathcal{B}_{\rho-\mathbf{1}}$ corresponding to the columns of $(N_h)_{|B}$
    for $i = 1, \ldots, k$ **do**
        for $j = 0, \ldots, n_i$ **do**
            $K_{ij} \leftarrow$ empty matrix
            for $m \in \mathcal{B}$ **do**
                $K_{ij} \leftarrow \begin{bmatrix} K_{ij} & \text{vec}(h_1 \cdots \hat{h}_i \cdots h_k \cdot x_{ij} \cdot m) \end{bmatrix}$
            end for
            $N_{ij} \leftarrow NK_{ij}$
            $m_{x_{ij}} = ((N_h)_{|B})^{-1} N_{ij}$
        end for
    end for
    return $m_{x_{ij}}, i = 1, \ldots, k, j = 0, \ldots n_i$
end procedure

Example 6.2. *We work out an example in $\mathbb{P}^1 \times \mathbb{P}^1$. We start with the affine equations $f_1 = 2 - x_1 + 2x_2 + 2x_1x_2 = 0$ and $f_2 = 4 - 2x_1 + x_2 + 4x_1x_2 = 0$. Homogenizing we get*

$$\begin{aligned} f_1^h &= 2x_{10}x_{20} - x_{20}x_{11} + 2x_{10}x_{21} + 2x_{11}x_{21}, \\ f_2^h &= 4x_{10}x_{20} - 2x_{20}x_{11} + x_{10}x_{21} + 4x_{11}x_{21} \end{aligned}$$

Using the coordinates $(x_{10}, x_{11}, x_{20}, x_{21})$ on $\mathbb{P}^1 \times \mathbb{P}^1$, the solutions are $z_1 = (1, 2, 1, 0)$, $z_2 = (0, 1, 1, 1/2)$. Note that z_2 corresponds to a solution 'at infinity', in the sense that it lies on the torus invariant divisor $x_{10} = 0$. A null space matrix is

$$N = \begin{bmatrix} 1 & 2 & 4 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & 1/4 & 0 & 0 & 0 & 1/8 \end{bmatrix}$$

where the first row corresponds to z_1 and the second to z_2 and the columns correspond to the monomials

$$x_{10}^3x_{20}^3, x_{10}^2x_{11}x_{20}^3, x_{10}x_{11}^2x_{20}^3, x_{11}^3x_{20}^3, x_{10}^3x_{20}^2x_{21}, x_{10}^2x_{11}x_{20}^2x_{21}, x_{10}x_{11}^2x_{20}^2x_{21}, x_{11}^3x_{20}^2x_{21},$$
$$x_{10}^3x_{20}x_{21}^2, x_{10}^2x_{11}x_{20}x_{21}^2, x_{10}x_{11}^2x_{20}x_{21}^2, x_{11}^3x_{20}x_{21}^2, x_{10}^3x_{21}^3, x_{10}^2x_{11}x_{21}^3, x_{10}x_{11}^2x_{21}^3, x_{11}^3x_{21}^3$$

in that order. In this example, we can take $h_1 = x_{10} + x_{11}$, $h_2 = x_{20} + x_{21}$. For $\mathcal{B} = \{x_{11}^2x_{21}^2, x_{10}x_{11}x_{20}^2\}$, with respect to the same set of monomials, we find

$$\begin{aligned} v_1 = \text{vec}(h_1 \cdot h_2 \cdot x_{11}^2x_{21}^2) &= \begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1\end{bmatrix}^\top, \\ v_2 = \text{vec}(h_1 \cdot h_2 \cdot x_{10}x_{11}x_{20}^2) &= \begin{bmatrix}0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}^\top \end{aligned}$$

and with $\tilde{K} = \begin{bmatrix} v_1 & v_2 \end{bmatrix}$ we find

$$(N_h)_{|B} = N\tilde{K} = \begin{bmatrix} 0 & 6 \\ 3/8 & 0 \end{bmatrix}$$

invertible. Then,

$$K_{10} = \begin{bmatrix}\text{vec}(h_2 \cdot x_{10} \cdot x_{11}^2x_{21}^2) & \text{vec}(h_2 \cdot x_{10} \cdot x_{10}x_{11}x_{20}^2)\end{bmatrix} = \begin{bmatrix} e_{11} + e_{15} & e_2 + e_6 \end{bmatrix}$$

which gives $N_{10} = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$. Analogously,

$$K_{11} = \begin{bmatrix}\text{vec}(h_2 \cdot x_{11} \cdot x_{11}^2x_{21}^2) & \text{vec}(h_2 \cdot x_{11} \cdot x_{10}x_{11}x_{20}^2)\end{bmatrix} = \begin{bmatrix} e_{12} + e_{16} & e_3 + e_7 \end{bmatrix}$$

which gives $N_{11} = \begin{bmatrix} 0 & 4 \\ 3/8 & 0 \end{bmatrix}$. We find that the eigenvalues of $((N_h)_{|B})^{-1}N_{10}$ are 0 and 1/3, corresponding to $\frac{x_{10}}{h_1}(z_i)$. For the generalized eigenvalue problem defined by $N_{11} - \lambda N_{10}$, we find eigenvalues 2 and ∞, corresponding to the x_1-coordinates of the affine solutions of the original system of equations. One can check the corresponding properties of $((N_h)_{|B})^{-1}N_{11}$ and construct the matrices N_{20}, N_{21} in the same way.

7 Finding roots from multiplication tables

Before showing some more experiments, we discuss how to find the δ solutions from the output of the algorithms in this paper using algorithms from numerical linear algebra. To give a general description, suppose $m_{g_i}, i = 1, \ldots, n$ are the matrices corresponding to multiplication by the n generators g_i of a $\mathbb{C}$-algebra A (be it $R/I, R/I^*$ or $S_\rho/I_\rho \sim \mathbb{C}[\frac{x_0}{h}, \ldots, \frac{x_n}{h}]/\tilde{I}$) in some basis. These matrices share a set of δ_0 invariant subspaces, each associated to one of the isolated solutions in $\mathbb{V}(I)$ [17]. We treat the case of simple roots and the case of roots with multiplicities $\mu_i > 1$ separately.

7.1 Simple roots: simultaneous diagonalization

The matrices $m_{g_1}, \ldots, m_{g_n}$ commute and have common eigenvectors. The eigenvalues of m_{g_i} are $g_i(z_j), j = 1, \ldots, \delta$. The m_{g_i} can be diagonalized simultaneously. We can compute the common eigenvectors by diagonalizing a generic linear combination m^* of the m_{g_i}: $m^* = h(m_{g_1}, \ldots, m_{g_n}) = \sum_{i=1}^n h_i m_{g_i}$, such that with probability one, all of the eigenvalues $h(g_1, \ldots, g_n)(z_j), j = 1, \ldots, \delta$ are distinct and the eigenvectors are well separated. Let $g^* = h(g_1, \ldots, g_n)$, we find $Pm^*P^{-1} = J^*$ with $J^* = \text{diag}(g^*(z_1), \ldots, g^*(z_\delta))$. Applying the same transformation to the m_{g_i} gives $Pm_{g_i}P^{-1} = \text{diag}(g_i(z_1), \ldots, g_i(z_\delta))$ where the order of the roots corresponding to the diagonal elements is preserved. If the g_i are coordinate functions, we can read off the coordinates of the δ roots from the diagonals of the $Pm_{g_i}P^{-1}$.

We note that a simultaneous diagonalization of a set of commuting matrices in the non defective case is equivalent to the tensor rank decomposition of a third order tensor [13]. It is possible to use tensor algorithms to refine the solutions obtained by the algorithm described above. The routine `cpd_gevd` in Tensorlab can be used for this computation [43].

An alternative is to compute the complex Schur form of m^*: $Um^*U^H = T^*$, with U orthogonal, T^* upper triangular and $\cdot^H$ denotes the Hermitian transpose. The same transformation makes the m_{g_i} upper triangular: $Um_{g_i}U^H = T_i$ and the solutions can be read off from the diagonals of the T_i.

7.2 Multiple roots: simultaneous block triangularization

We compute the Jordan form of m^*. Let $Pm^*P^{-1} = J^*$ with

$$J^* = \begin{bmatrix} J_1^* & & & \\ & J_2^* & & \\ & & \ddots & \\ & & & J_{\delta_0}^* \end{bmatrix} = \operatorname{diag}(J_1^*, \dots, J_{\delta_0}^*),$$

such that J_i^* is of size $\mu_i \times \mu_i$, upper triangular with diagonal elements all equal to $g^*(z_i)$. Then $Pm_{g_i}P^{-1} = J_i = \operatorname{diag}(J_{i1}, \dots, J_{i\delta_0})$ with J_{ij} of size $\mu_j \times \mu_j$, upper triangular with diagonal elements equal to $g_i(z_j)$.[1] This way, the solutions, along with their multiplicities, can be found from this simultaneous upper triangularization of the m_{g_i}. Unfortunately, the Jordan form of a defective matrix is very ill conditioned and its computation is not possible in finite precision arithmetic.

Since we are interested in numerical methods using finite precision arithmetic, we use the following alternative method [7]. We compute the Schur form of m^*: $\tilde{U}m^*\tilde{U}^H = \tilde{T}^*$, with $\tilde{U}$ orthogonal and $\tilde{T}^*$ upper triangular. If there are solutions with multiplicity > 1, some elements on the diagonal of $\tilde{T}^*$ appear multiple times. Next, we use a clustering of the diagonal elements of $\tilde{T}^*$ and reorder the factorization $Um^*U^H = T^*$ such that U is orthogonal, T^* is upper triangular and the diagonal elements are clustered. The same transformation makes the m_{g_i} block upper triangular with δ_0 diagonal blocks of size $\mu_j \times \mu_j, j = 1, \dots, \delta_0$ corresponding to the clusters on the diagonal of T^*. All of the diagonal blocks only have one eigenvalue, which is $g_i(z_j)$. For more details on this approach we refer to [7]. Another approach based on the intersection of eigenspaces is given in [31] and [22].

8 Numerical examples

We give a few more examples in which we use the algorithms in this paper to solve bigger systems. All computations are performed using Matlab on an 8 GB RAM machine with an intel Core i7-6820HQ CPU working at 2.70 GHz. To measure the quality of the solutions, we use the residual as defined in [41].

8.1 Affine solutions of a sparse 3-variate system

We consider the system given by

$$\begin{aligned} f_1 &= 12x_1x_2x_3^{12} + 7x_1^2x_2^7x_3^6 + 4x_1^{10}x_2^{11}x_3^8 + 4x_1^6x_2^4x_3^7 + 5, & (3)\\ f_2 &= 15x_1^{10}x_2^4x_3^2 + 4x_1^3x_2^6x_3^6 + 10x_1x_2^{10}x_3^8 + 11x_1^6x_2^{11}x_3^8 + 12, & (4)\\ f_3 &= 10x_1^7x_2^4x_3^6 + 4x_1^{10}x_2x_3 + 4x_1^2x_2^{12}x_3^9 + 14x_1^{10}x_2^5x_3 + 2. & (5)\end{aligned}$$

The mixed volume (computed using PHCpack [42]) is 2352. Constructing the Macaulay matrix supported in $\sum_{i=1}^3 P_i + \Delta_3 + v$ where Δ_3 is the simplex in $\mathbb{R}^3$ and v is a random small vector, Algorithm 2 finds 2352 solutions, 2 of which are real. All solutions lie in $(\mathbb{C}^*)^3$, so in this example $I = I^*$. The real solutions are depicted in Figure 2 together with a picture of the surfaces defined by the f_i in $\mathbb{R}^3$. All solutions are simple. They are found by a Schur decomposition of the $m_{x_i}, i = 1, \dots, 3$. Computations with polytopes (except for the mixed volume) are done using polymake [25]. We used QR with optimal column pivoting on $N_{|W}$ for the basis choice [41]. The total computation time is about 294 seconds. All solutions are found with a residual smaller than $3.1 \cdot 10^{-12}$.

8.2 Affine solutions of a generic dense system

We consider generic dense systems in the sense of [41]. We compute the solution by decomposing the tensor defined by the N_i from Algorithm 1 and choose the basis using QR with pivoting. For this type

[1] Note that the J_i are not necessarily a Jordan form of the m_{g_i}, they may have a different upper triangular nonzero structure than just an upper diagonal of ones [17, 38].

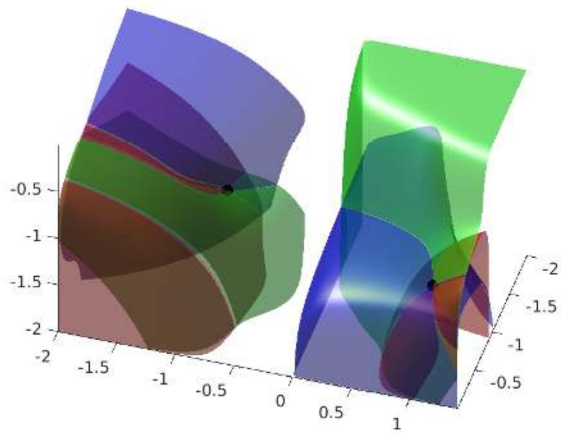

Figure 2: Surfaces in $\mathbb{R}^3$ defined by f_1, f_2 and f_3 (blue, red, green respectively) and the real solutions found using Algorithm 2.

of systems, the basis choice made in Algorithm 1 agrees with the basis chosen in [41]. Also here, the monomials at the border of the support are preferred. Figure 3 shows the basis that is selected for a bivariate system with $d_1 = d_2 = 15$.

8.3 Projective solution of a dense system with a solution at infinity

We use Algorithm 3 to find the projective coordinates of the 77 solutions in $\mathbb{P}^2$ of a bivariate system with $d_1 = 7, d_2 = 11$. There are 7 real solutions, one of which lies at infinity: $(0, 1, 1)$ where the first coordinate corresponds to the homogenization variable. The algorithm returns all of the projective solutions with a residual smaller than $5.24 \cdot 10^{-14}$ within about a tenth of a second. The left part of Figure 4 shows the real solutions in the affine chart $x_0 = 1$ of $\mathbb{P}^2$ (there are 6). The right part of the figure shows all real solutions in $\mathbb{P}^2$ represented as rays connecting the origin in $\mathbb{C}^3$ with a point on the unit sphere. Note that one of the rays (the bold one) is contained in the plane at infinity, and it is also contained in the plane $x_1 - x_2 = 0$, which corresponds to the solution $(0, 1, 1)$.

8.4 An example in $\mathbb{P}^1 \times \mathbb{P}^1$

We consider a system defined by two bivariate affine equations of bidegree $(9, 9)$ and $(9, 9)$, having 6 solutions 'at infinity'. Three of the infinite solutions have an infinite x_1-coordinate and a finite x_2-coordinate (they are on the divisor $x_{10} = 0$), the others have an infinite x_2-coordinate. It takes Algorithm 4 about half a second to find all 162 solutions in $\mathbb{P}^1 \times \mathbb{P}^1$. The residuals are presented in Figure 5, together with the absolute value of the coordinates of the solutions, dehomogenized with respect to x_{10} and x_{20} respectively.

8.5 Comparison with homotopy solvers

We compare the speed and accuracy of our method to that of the homotopy continuation method implemented in PHCpack [42] and Bertini [2]. The current implementation of our method is in Matlab. We have implemented the construction of the matrix M in Fortran. We call the routine from Matlab using a MEX file. An implementation in Julia has also been developed and is accessible at `https://gitlab.inria.fr/AlgebraicGeometricModeling/AlgebraicSolvers.jl`.

We use double precision for all computations and standard settings for Bertini and PHCpack apart from that. By a generic dense system of degree d in n variables we mean a set of n polynomials in

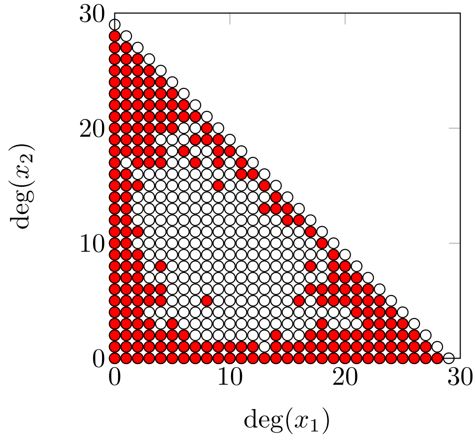

Figure 3: Support of the Macaulay matrix (○) and basis of R/I (●) chosen by Algorithm 1 for a generic dense bivariate system with $d_1 = d_2 = 15$. The bivariate monomials are identified with $\mathbb{Z}^2$ in the usual way.

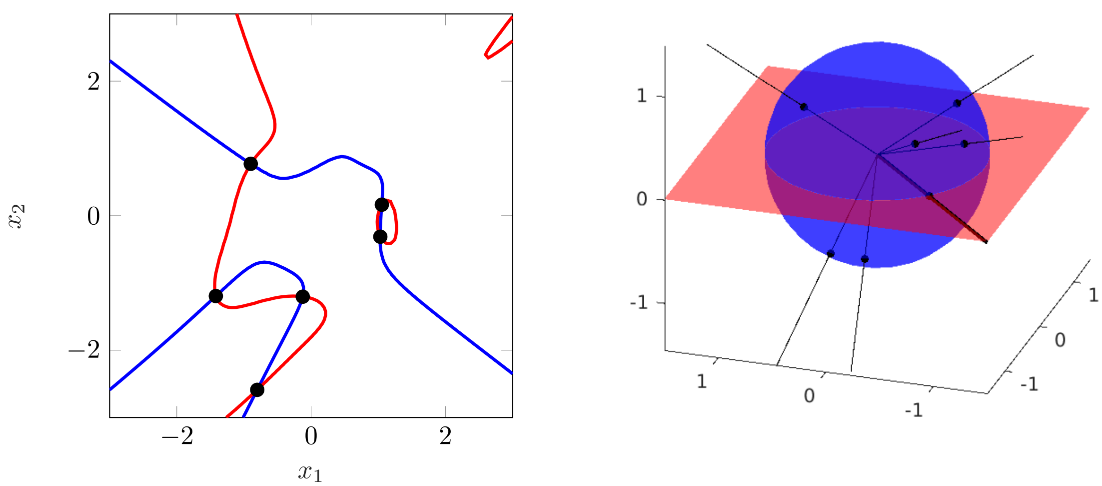

Figure 4: Left: picture in $\mathbb{R}^2$ of the solution set in the affine chart $x_0 = 1$ of $\mathbb{P}^2$ of the system described in Example 8.3. Right: visualization of the real solutions in $\mathbb{P}^2$ with the unit sphere in blue and the plane 'at infinity' in red.

$\mathbb{C}[x_1, \ldots, x_n]$ supported in the monomials x^α of degree $\leq d$ with coefficients drawn from a normal distribution with mean zero and standard deviation 1. For the experiment we fix a value of n and generate generic dense systems of increasing degree d to use as input for the different solvers.

Tables 1 up to 8 give detailed results from the experiment. The following notation is used in the tables. The number of solutions of the input system is δ (in this case, $\delta = d^n$). The numbers $m_1, m_2 = n_1, n_2$

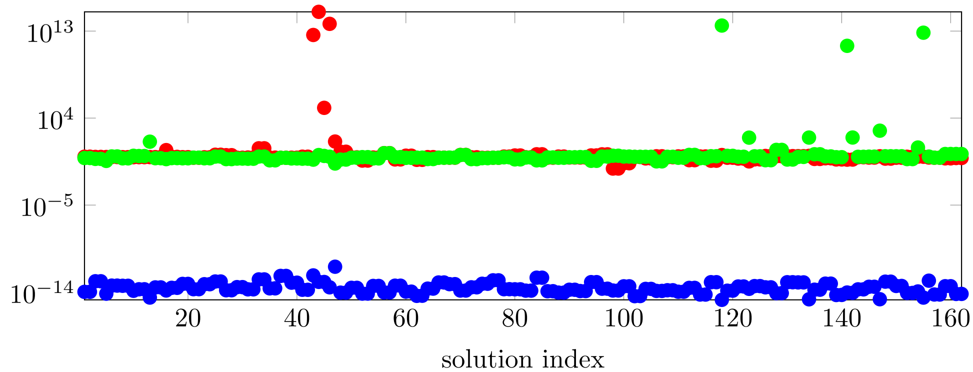

Figure 5: Residual (●), absolute value of the x_1-components (●) and absolute value of the x_2-components (●) of all 162 numerical solutions of the problem described in Example 8.4.

give the sizes of M and N from the algorithms: $M^\top \in \mathbb{C}^{m_1 \times m_2}, N \in \mathbb{C}^{n_1 \times n_2}$. The maximal residual of the solutions computed by the algebraic solver of this paper is denoted by res. The number of solutions found by the different solvers is $\delta_{\text{alg}}, \delta_{\text{phc}}, \delta_{\text{brt}}$ for the algebraic solver, PHCpack and Bertini respectively. Since the homotopy methods use Newton refinement intrinsically, their computed solutions give residuals of the order of the unit roundoff. The values t_M, t_N, t_B, t_S denote the time for the construction of the Macaulay matrix (Fortran), the computation of its null space, the computation of the basis via QR together with the construction of the multiplication matrices and the time to compute the simultaneous Schur decomposition respectively. The total computation times are $t_{\text{alg}}, t_{\text{phc}}$ and t_{brt} for the algebraic solver introduced in this paper ($t_{\text{alg}} = t_M + t_N + t_B + t_S$), PHCpack and Bertini respectively. All timings are in seconds. Tables 1 and 2 present the experiment for $n = 2$ variables, Tables 3 and 4 for $n = 3$, Tables 5 and 6 for $n = 4$ and Tables 7 and 8 for $n = 5$.

We observe that our method has found numerical approximations for *all* d^n roots, with a residual no larger than order 10^{-9}. Due to the quadratic convergence of Newton's iteration, one refining step can be expected to result in a residual of the order of the unit roundoff. Table 1 shows that for 2 variables, up to degree $d = 61$, our method is the fastest. For $n = 3$ this is no longer the case but timings are comparable. For a larger number of variables, the matrix M in the algorithms becomes very large and the null space computation is expensive, which makes the algebraic method slower than the continuation solvers.

d	δ	m_1	$m_2{=}n_1$	n_2	res	δ_{alg}	δ_{phc}	δ_{brt}
1	1	2	3	1	$1.28 \cdot 10^{-16}$	1	1	1
7	49	56	105	49	$2.06 \cdot 10^{-13}$	49	49	49
13	169	182	351	169	$2.18 \cdot 10^{-13}$	169	169	169
19	361	380	741	361	$5.28 \cdot 10^{-13}$	361	361	361
25	625	650	1,275	625	$1.21 \cdot 10^{-10}$	625	614	625
31	961	992	1,953	961	$5.23 \cdot 10^{-9}$	961	951	961
37	1,369	1,406	2,775	1,369	$4.05 \cdot 10^{-12}$	1,369	1,360	1,368
43	1,849	1,892	3,741	1,849	$1.74 \cdot 10^{-11}$	1,849	1,825	1,845
49	2,401	2,450	4,851	2,401	$1.57 \cdot 10^{-10}$	2,401	2,364	2,163
55	3,025	3,080	6,105	3,025	$1.84 \cdot 10^{-11}$	3,025	2,970	2,487
61	3,721	3,782	7,503	3,721	$3.26 \cdot 10^{-11}$	3,721	3,662	2,260

Table 1: Numerical results for PHCpack, Bertini and our method for dense systems in $n = 2$ variables of increasing degree d. The table shows matrix sizes, accuracy and number of solutions.

An important note is that homotopy methods do not guarantee that all solutions are found. In fact, they lose some solutions for large systems. For $n = 2, d = 55$, Bertini gives up on 538 out of 3025 paths, so about 18% of the solutions is not found (using default settings). For the same problem, PHCpack loses 2% of the solutions.

d	t_M	t_N	t_B	t_S	t_{alg}	t_{phc}	t_{brt}
1	$1.48 \cdot 10^{-4}$	$5.5 \cdot 10^{-5}$	$2.96 \cdot 10^{-4}$	$3.6 \cdot 10^{-5}$	$5.35 \cdot 10^{-4}$	$5.6 \cdot 10^{-2}$	$1.41 \cdot 10^{-2}$
7	$7.88 \cdot 10^{-3}$	$1.68 \cdot 10^{-3}$	$3.76 \cdot 10^{-3}$	$2.78 \cdot 10^{-3}$	$1.61 \cdot 10^{-2}$	0.18	$8.65 \cdot 10^{-2}$
13	$4.65 \cdot 10^{-2}$	$1.03 \cdot 10^{-2}$	$1.66 \cdot 10^{-2}$	$2.81 \cdot 10^{-2}$	0.1	0.84	1.14
19	0.13	$5.69 \cdot 10^{-2}$	$5.34 \cdot 10^{-2}$	0.13	0.37	3.29	8.79
25	0.32	0.18	0.15	0.51	1.16	8.79	33.83
31	0.55	0.51	0.55	1.49	3.1	20.25	98.39
37	0.96	1.52	1.5	3.52	7.5	39.92	258.09
43	1.47	4.05	3.8	8.28	17.6	69.1	504.01
49	2.47	10.46	8.78	17.91	39.62	124.47	891.37
55	3.69	20.51	17.85	34.3	76.34	178.55	1,581.77
61	4.85	36.32	31.26	62.87	135.3	283.87	2,115.66

Table 2: Timing results for PHCpack, Bertini and our method for dense systems in $n = 2$ variables of increasing degree d.

d	δ	m_1	$m_2{=}n_1$	n_2	res	δ_{alg}	δ_{phc}	δ_{brt}
1	1	3	4	1	$1.79 \cdot 10^{-16}$	1	1	1
3	27	105	120	27	$1.05 \cdot 10^{-14}$	27	27	27
5	125	495	560	125	$1.29 \cdot 10^{-12}$	125	125	125
7	343	1,365	1,540	343	$6.71 \cdot 10^{-12}$	343	343	343
9	729	2,907	3,276	729	$1.38 \cdot 10^{-10}$	729	726	729
11	1,331	5,313	5,984	1,331	$3.11 \cdot 10^{-11}$	1,331	1,331	1,331
13	2,197	8,775	9,880	2,197	$2.86 \cdot 10^{-11}$	2,197	2,192	2,197

Table 3: Numerical results for PHCpack, Bertini and our method for dense systems in $n = 3$ variables of increasing degree d. The table shows matrix sizes, accuracy and number of solutions.

d	t_M	t_N	t_B	t_S	t_{alg}	t_{phc}	t_{brt}
1	$3.72 \cdot 10^{-4}$	$1.24 \cdot 10^{-4}$	$2.31 \cdot 10^{-3}$	$4.5 \cdot 10^{-5}$	$2.85 \cdot 10^{-3}$	$6.8 \cdot 10^{-2}$	$1.69 \cdot 10^{-2}$
3	$7.91 \cdot 10^{-3}$	$2.42 \cdot 10^{-3}$	$7.06 \cdot 10^{-3}$	$1.08 \cdot 10^{-3}$	$1.85 \cdot 10^{-2}$	0.14	$7.33 \cdot 10^{-2}$
5	$5.66 \cdot 10^{-2}$	$3.93 \cdot 10^{-2}$	$3.31 \cdot 10^{-2}$	$1.17 \cdot 10^{-2}$	0.14	0.68	0.63
7	0.23	1.13	0.12	$9.9 \cdot 10^{-2}$	1.57	3.42	4.11
9	0.68	14.43	0.65	0.63	16.4	12.21	17.29
11	1.77	44.79	3.91	3.98	54.46	39.08	70.66
13	5.81	183.67	16.07	15.35	220.9	97.28	210.34

Table 4: Timing results for PHCpack, Bertini and our method for dense systems in $n = 3$ variables of increasing degree d.

d	δ	m_1	$m_2{=}n_1$	n_2	res	δ_{alg}	δ_{phc}	δ_{brt}
1	1	4	5	1	$1.24 \cdot 10^{-16}$	1	1	1
2	16	140	126	16	$1.13 \cdot 10^{-14}$	16	16	16
3	81	840	715	81	$3.84 \cdot 10^{-14}$	81	81	81
4	256	2,860	2,380	256	$1.52 \cdot 10^{-13}$	256	256	255

Table 5: Numerical results for PHCpack, Bertini and our method for dense systems in $n = 4$ variables of increasing degree d. The table shows matrix sizes, accuracy and number of solutions.

9 Conclusion and future work

We have proposed an algebraic framework for finding a representation of the quotient ring R/I by a zero-dimensional ideal I and we have shown how this leads to a numerical linear algebra method for solving square systems of polynomial equations with the expected number of solutions in $\mathbb{C}^n, (\mathbb{C}^*)^n, \mathbb{P}^n$ or $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_k}$. The choice of basis for the representation of the quotient ring is crucial for the numerical stability of the method. The experiments in Section 8 show that we obtain accurate results. The method guarantees, unlike homotopy solvers, that numerical approximations of all solutions are

d	t_M	t_N	t_B	t_S	t_{alg}	t_{phc}	t_{brt}
1	$1.1 \cdot 10^{-2}$	$2.83 \cdot 10^{-4}$	$1.83 \cdot 10^{-2}$	$8.43 \cdot 10^{-4}$	$3.04 \cdot 10^{-2}$	$6.82 \cdot 10^{-2}$	$1.76 \cdot 10^{-2}$
2	$1.12 \cdot 10^{-2}$	$4.29 \cdot 10^{-3}$	$1.08 \cdot 10^{-2}$	$5.94 \cdot 10^{-4}$	$2.69 \cdot 10^{-2}$	0.12	$6.32 \cdot 10^{-2}$
3	0.11	0.14	$5.76 \cdot 10^{-2}$	$5.55 \cdot 10^{-3}$	0.31	0.52	0.59
4	0.46	8.31	0.23	$5.41 \cdot 10^{-2}$	9.05	2.27	3.62

Table 6: Timing results for PHCpack, Bertini and our method for dense systems in $n = 4$ variables of increasing degree d.

d	δ	m_1	m_2=n_1	n_2	res	δ_{alg}	δ_{phc}	δ_{brt}
1	1	5	6	1	$7.89 \cdot 10^{-17}$	1	1	1
2	32	630	462	32	$4.22 \cdot 10^{-14}$	32	32	32
3	243	6,435	4,368	243	$1.84 \cdot 10^{-12}$	243	243	243

Table 7: Numerical results for PHCpack, Bertini and our method for dense systems in $n = 5$ variables of increasing degree d. The table shows matrix sizes, accuracy and number of solutions.

d	t_M	t_N	t_B	t_S	t_{alg}	t_{phc}	t_{brt}
1	$4.87 \cdot 10^{-4}$	$1.54 \cdot 10^{-4}$	$1.86 \cdot 10^{-3}$	$3 \cdot 10^{-5}$	$2.53 \cdot 10^{-3}$	$6.52 \cdot 10^{-2}$	$1.91 \cdot 10^{-2}$
2	$5.97 \cdot 10^{-2}$	$3.9 \cdot 10^{-2}$	$4.07 \cdot 10^{-2}$	$1.46 \cdot 10^{-3}$	0.14	0.26	0.24
3	1.21	69.38	0.53	$5.5 \cdot 10^{-2}$	71.18	2.42	4.74

Table 8: Timing results for PHCpack, Bertini and our method for dense systems in $n = 5$ variables of increasing degree d.

found under some genericity assumptions. It is competitive in speed with Bertini and PHCpack for a small number of variables. Here are some ideas for future work.

- The submatrix $\tilde{M}$ is generically of full rank, as proved by Macaulay. However, we observe that it has some small singular values for generic, large systems, $n \geq 3$. Therefore it has an ill conditioned null space and it is better to use the larger matrix M. If we can find a subset of the columns of M that leads to a full rank matrix with 'good' singular values, this could speed up the computations.
- Sparse systems lead to a sparse matrix M. It might be useful to exploit this sparsity in the null space computation.
- An implementation in C++, Fortran, ... would speed up the algorithm, exploiting High Performance Computation optimisation.
- The method might be extended to isolated points of varieties defined by non-zero dimensional ideals.
- When the dimension is bigger than $n = 4$, most of the time is spent in computing the null space N. A cheaper construction of the map N can be investigated.

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Pub. Co., 1969.

[2] D. J. Bates, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. *Numerically solving polynomial systems with Bertini*. SIAM, 2013.

[3] D. Bayer and M. Stillman. A criterion for detecting m-regularity. *Inventiones Mathematicae*, 87(1):1–11, 1987.

[4] D. Bernstein. The number of roots of a system of equations. *Functional Anal. Appl.*, 9:1–4, 1975.

[5] L. Busé, M. Elkadi, and B. Mourrain. Resultant over the residual of a complete intersection. *Journal of Pure and Applied Algebra*, 164(1-2):35–57, Oct. 2001.

[6] E. Cattani, D. A. Cox, G. Chèze, A. Dickenstein, M. Elkadi, I. Z. Emiris, A. Galligo, A. Kehrein, M. Kreuzer, and B. Mourrain. *Solving Polynomial equations: foundations, algorithms, and applications (Algorithms and Computation in Mathematics)*. Springer-Verlag New York, Inc., 2005.

[7] R. M. Corless, P. M. Gianni, and B. M. Trager. A reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, pages 133–140. ACM, 1997.

[8] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*, volume 3. Springer, 1992.

[9] D. A. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185. Springer Science & Business Media, 2006.

[10] C. D'Andrea and M. Sombra. A Poisson formula for the sparse resultant. *Proceedings of the London Mathematical Society*, 110(4):932–964, Apr. 2015.

[11] C. De Boor. Ideal interpolation. *Approximation Theory XI: Gatlinburg*, pages 59–91, 2004.

[12] C. de Boor. Ideal interpolation: Mourrain's condition vs. D-invariance. *Banach Center Publications, Institute of Mathematics, Polish Academy of Sciences, Warszawa*, 72:41–47, 2006.

[13] L. De Lathauwer. A link between the canonical decomposition in multilinear algebra and simultaneous matrix diagonalization. *SIAM journal on Matrix Analysis and Applications*, 28(3):642–666, 2006.

[14] P. Dreesen, K. Batselier, and B. De Moor. Back to the roots: Polynomial system solving, linear algebra, systems theory. *IFAC Proceedings Volumes*, 45(16):1203–1208, 2012.

[15] C. Eder and J. E. Perry. Signature-based algorithms to compute Gröbner bases. In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, pages 99–106. ACM, 2011.

[16] D. Eisenbud. *The Geometry of Syzygies: A Second Course in Commutative Algebra and Algebraic Geometry*. Springer, New York, NY, 2005. OCLC: 249751633.

[17] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques et Applications*. Springer, 2007.

[18] I. Z. Emiris and J. Canny. A practical method for the sparse resultant. *Proc. ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 183–192, 1993.

[19] I. Z. Emiris and B. Mourrain. Matrices in Elimination Theory. *Journal of Symbolic Computation*, 28(1-2):3–44, 1999.

[20] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1):61–88, 1999.

[21] W. Fulton. *Introduction to toric varieties*. Number 131. Princeton University Press, 1993.

[22] S. Graillat and P. Trébuchet. A new algorithm for computing certified numerical approximations of the roots of a zero-dimensional system. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 167–174. ACM, 2009.

[23] R. Hartshorne. *Algebraic Geometry*. Springer, 1977.

[24] B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Math. Comp*, 64:1541–1555, 1995.

[25] M. Joswig, B. Müller, and A. Paffenholz. `polymake` and lattice polytopes. In *21st International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2009)*, Discrete Math. Theor. Comput. Sci. Proc., AK, pages 491–502. Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2009.

[26] A. Khovanskii. Newton polytopes and toric varieties. *Functional Anal. Appl.*, 11:289–298, 1977.

[27] A. Kushnirenko. Newton polytopes and the Bézout theorem. *Functional Anal. Appl.*, 10:233–235, 1976.

[28] F. S. Macaulay. Some formulae in elimination. *Proceedings of the London Mathematical Society*, 1(1):3–27, 1902.

[29] F. S. Macaulay. *The algebraic theory of modular systems*. Cambridge University Press, 1994.

[30] H. M. Möller and T. Sauer. H-bases for polynomial interpolation and system solving. *Advances in Computational Mathematics*, 12(4):335–362, 2000.

[31] H. M. Möller and R. Tenberg. Multivariate polynomial system solving using intersections of eigenspaces. *Journal of Symbolic Computation*, 32(5):513–531, 2001.

[32] B. Mourrain. A new criterion for normal form algorithms. In *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LNCS, pages 430–443, London, UK, 1999. Springer-Verlag.

[33] B. Mourrain and J. P. Pavone. Subdivision methods for solving polynomial equations. *Journal of Symbolic Computation*, 44(3):292–306, 2009.

[34] B. Mourrain and P. Trébuchet. Solving projective complete intersection faster. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, pages 234–241. ACM Press, 2000.

[35] B. Mourrain and P. Trébuchet. Generalized normal forms and polynomial system solving. In *Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation*, pages 253–260. ACM, 2005.

[36] B. Mourrain and P. Trébuchet. Stable normal forms for polynomial system solving. *Theoretical Computer Science*, 409(2):229–240, 2008.

[37] L. Sorber, M. Van Barel, and L. De Lathauwer. Numerical solution of bivariate and polyanalytic polynomial systems. *SIAM J. Num. Anal. 52*, pages 1551–1572, 2014.

[38] H. J. Stetter. *Numerical Polynomial Algebra*. Society for Industrial and Applied Mathematics, 2004.

[39] B. Sturmfels. Polynomial equations and convex polytopes. *The American Mathematical Monthly*, 105:907–922, 1998.

[40] B. Sturmfels. *Solving Systems of Polynomial Equations*. Number 97 in CBMS Regional Conferences. Amer. Math. Soc., 2002.

[41] S. Telen and M. Van Barel. A stabilized normal form algorithm for generic systems of polynomial equations. *Journal of Computational and Applied Mathematics*, 342:119–132, 2018.

[42] J. Verschelde. Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation. *ACM Transactions on Mathematical Software (TOMS)*, 25(2):251–276, 1999.

[43] N. Vervliet, O. Debals, L. Sorber, M. Van Barel, and L. De Lathauwer. Tensorlab 3.0. *available online, URL: www.tensorlab.net*, 2016.