Chapter 8
Zero-Dimensional Systems of Multivariate Polynomials

We have previously emphasized that an indispensable prerequisite for the numerical treatment of an algebraic problem is its *embedding into analysis*. This is a straightforward matter for individual polynomials, univariate or multivariate: We can immediately see them as elements of a linear space, with the monomials of their support as basis elements; in this linear space, a topology is generated through the natural topology of the complex coefficients. Thus, as long as the structure of an algebraic task is determined by only *one* polynomial, its analytic embedding is so natural that we have often not bothered to display it explicitly. For univariate problems with several data polynomials (like g.c.d.), we have also been able to extend this approach.

For multivariate algebraic problems with several data polynomials, we have a different situation: The topology of the coefficients does not generally establish a suitable analytic embedding for the algebraic problem. In *linear* algebra, this is well known for singular or near-singular systems of linear polynomials. In polynomial algebra there are many more ways how an algebraic structure may change its character through (arbitrarily) small changes of its data. This is aggravated by the fact that many multivariate algebraic structures are commonly described in an *overdetermined* fashion: For example, the reduced Groebner basis of a polynomial ideal in s variables has, generally, more than s elements. This makes it impossible to define the "neighborhood of an ideal" naively by a neighborhood of its Groebner basis.

Fortunately, for a wide and meaningful class of multivariate polynomial systems, the *zeros* remain continuous functions of the coefficients in the system, like it is well-known for regular systems of linear equations. Therefore, in this chapter, we will consider the analog of *regular* systems of linear multivariate equations, viz. systems of multivariate polynomials with a finite, positive number of real or complex isolated zeros. Like in numerical linear algebra, we interpret *regularity* of a polynomial system to imply that it is sufficiently removed from systems which are either inconsistent or which possess a positive-dimensional zero manifold so that all sufficiently close neighboring systems are also consistent and 0-dimensional. A necessary but not sufficient prerequisite for this is that the system contains equally many polynomials as there are variables.

The considerations in this chapter will elaborate aspects of regular polynomial systems which are fundamental for their computational solution. Numerical aspects in the proper sense will be delayed to Chapter 9.

8.1 Quotient Rings and Border Bases of 0-Dimensional Ideals

Algebraically, a system P of polynomials specifies a polynomial *ideal* $\mathcal{I} = \langle P \rangle$ which defines a *quotient ring* $\mathcal{R}[\mathcal{I}]$ and a *dual space* $\mathcal{D}[\mathcal{I}]$; cf. Chapter 2. There, we have seen that—in our restricted context—all the defining relations in the diagram

$$\begin{array}{ccccc} & & \mathcal{I} & & \\ & \swarrow\nearrow & & \searrow\nwarrow & \\ \mathcal{R}[\mathcal{I}] & & \rightleftarrows & & \mathcal{D}[\mathcal{I}] \end{array}$$

may be read both ways, i.e. any member of the set $\{\mathcal{I},\ \mathcal{R}[\mathcal{I}],\ \mathcal{D}[\mathcal{I}]\}$ defines the other two; cf. Theorems 2.7 and 2.21 etc. In sections 2.4 and 2.5, we have established how all information about the m zeros (counting multiplicities) of a 0-dimensional polynomial ideal $\mathcal{I}$ in $\mathcal{P}^s(m)$ can be determined—by numerical linear algebra techniques—from the multiplicative structure of the quotient ring $\mathcal{R}[\mathcal{I}]$, specified with respect to a suitable basis of $\mathcal{R}$ as an m-dimensional linear space over $\mathbb{C}$. A *normal set representation* of $\mathcal{I}$ specifies these data; cf. Definition 2.23.

In this section, we will continue our considerations of Chapter 2 and consider various aspects of the specification of a quotient ring in more detail. Remember that the elements proper of a quotient ring $\mathcal{R}[\mathcal{I}]$ are *residue classes* mod $\mathcal{I}$, but that—for a simpler notation and in agreement with common practice (cf. section 2.2)—we will generally formulate relations in $\mathcal{R}$ in terms of particular member polynomials of these residue classes. This implies that such relations must be interpreted as *equivalences* mod $\mathcal{I}$. A typical example is the representation of multiplication in $\mathcal{R}[\mathcal{I}]$ by the formulation (cf. (2.20))

$$p(x) \cdot \mathbf{b}(x) \ = \ p(A)\, \mathbf{b}(x)$$

which—as a relation in $\mathcal{P}^s$—is to be read as

$$p(x) \cdot \mathbf{b}(x) \ \equiv \ p(A)\, \mathbf{b}(x) \bmod \mathcal{I} \qquad \text{or} \qquad p(x) \cdot \mathbf{b}(x) - p(A)\, \mathbf{b}(x) \ \in \ \mathcal{I}\,.$$

This reveals the second important fact to be remembered about relations in a polynomial quotient ring $\mathcal{R}[\mathcal{I}]$: *At the zeros of* $\mathcal{I}$, relations in $\mathcal{R}$ become proper equations in $\mathbb{C}$ or $\mathbb{R}$, resp.: For $z \in Z[\mathcal{I}]$,

$$p(z) \cdot \mathbf{b}(z) - p(A)\, \mathbf{b}(z) \ = \ 0\,.$$

8.1.1 The Quotient Ring of a Specified Dual Space

Let us, at first, consider the transition from a quotient ring to the zeros of the associated polynomial ideal in the *reverse direction*: In $\mathbb{C}^s$, $s > 1$, we consider sets of m points z_μ, $\mu = 1(1)m$, which we regard as zero sets Z of 0-dimensional ideals $\mathcal{I} \subset \mathcal{P}^s$. If all z_μ are *disjoint*, we interpret them as *simple* zeros of $\mathcal{I}$ and Z defines the dual space $\mathcal{D}[\mathcal{I}]$; cf. Theorem 2.20. To a subset of $m_\mu \geq 2$ *identical* values $z_\mu = z_{\mu+1} = \ldots = z_{\mu+m_\mu-1}$ we assign the multiplicity m_μ and require that the associated $m_\mu - 1$ further basis elements (beyond evaluation at z_μ) of the dual space $\mathcal{D}[\mathcal{I}]$ be specified; cf. Definition 2.14. We will see later (cf. section 8.5) that this amounts essentially to the specification of $m_\mu - 1$ further vectors in $\mathbb{C}^s$. With this interpretation of coinciding points, the elements of $(\mathbb{C}^s)^m$ represent the ideals in $\mathcal{P}^s$ with exactly m zeros.

Definition 8.1. The set of all 0-dimensional ideals in $\mathcal{P}^s$ with exactly m zeros (counting multiplicities) will be denoted by $\mathcal{P}^s(m)$; the set $(\mathbb{C}^s)^m$, with the indicated interpretation of its elements as zero sets of ideals in $\mathcal{P}^s(m)$, will be denoted by $Z^s(m)$. □

The above consideration suggests that the numerical part of the specification of $\mathcal{R}[\mathcal{I}]$ for $\mathcal{I} \in \mathcal{P}^s(m)$ should consist of either m s-tuples or s m-tuples of complex numbers. This is generally obscured by the fact that the form and the numerical data of the specification of a quotient ring depend strongly on the basis chosen for the representation. Even if we restrict our attention to *monomial* bases or *normal sets* (cf. Definition 2.19)—as we will in the following—there is a wide variety of feasible normal sets for nontrivial values of s and m: For the quotient ring of any given ideal in $\mathcal{P}^s(m)$, all or *almost all* elements from $\mathcal{T}^s(m)$ are feasible as a basis; cf. Proposition 2.28. However, the algorithmic and numerical properties of a basis may depend strongly on the particular choice.

To avoid the technical discussion of special cases, we assume that we select only normal sets which contain *all* variables x_σ as elements; obviously, this requires $m \geq s+1$ and excludes some extremely degenerate positions of the zeros z_μ. An extension to these cases is straightforward and will be indicated in examples. We also assume that $1, x_1, \ldots, x_s$ are the *first* $s+1$ components in the normal set *vector* $\mathbf{b}$.

For a particular zero set $Z \in Z^s(m)$, when we have selected a (feasible) normal set $\mathcal{N} \in \mathcal{T}^s(m)$ and arranged the monomials of $\mathcal{N}$ into a basis (column) vector $\mathbf{b}(x) = (x_\mu^{j_\mu},\ \mu = 1(1)m)$, we can immediately specify the multiplicative structure of the associated quotient ring $\mathcal{R}$ with respect to this basis with the aid of Theorem 2.27; cf. (2.50). Let us, at first, assume that all $z_\mu = (\zeta_{\mu,1}, \ldots, \zeta_{\mu,s}) \in Z$ are disjoint. Then (cf. also Theorem 2.23) the multiplication by x_σ in $\mathcal{R}[\mathcal{I}]$, i.e. mod $\mathcal{I}$, is represented by the matrix

$$A_\sigma = X\,\Lambda_\sigma\,X^{-1} \in \mathbb{C}^{m\times m}, \quad \text{with} \quad X := \begin{pmatrix} | & & | \\ \mathbf{b}(z_1) & .. & \mathbf{b}(z_m) \\ | & & | \end{pmatrix},\ \Lambda_\sigma := \begin{pmatrix} \zeta_{1,\sigma} & & 0 \\ & \ddots & \\ 0 & & \zeta_{m,\sigma} \end{pmatrix}. \tag{8.1}$$

The right-hand side of (8.1) shows that all information about Z is in the $m \times m$-matrix X which is the *same* for all σ, and that even X generally contains this information in a redundant form: Except when $m = s+1$ and $\mathbf{b} = (1, x_1, ..x_s)^T$ (cf. our assumption above), the $m-s-1$ last components of the vectors $\mathbf{b}(z_\mu)$ are immediate functions of the components no. 2 through $s+1$: For $b_\nu(x) = x^{j_\nu},\ \nu > s+1$,

$$b_\nu(z_\mu) = z_\mu^{j_\nu} = \zeta_{\mu,1}^{j_{\nu 1}} \ldots \zeta_{\mu,s}^{j_{\nu s}} = (b_2(z_\mu))^{j_{\nu 1}} \ldots (b_{s+1}(z_\mu))^{j_{\nu s}}\,. \tag{8.2}$$

The fact that the complete information in (8.1) about Z, and thus about the ideal $\mathcal{I}$ with the zero set Z, coded with reference to the normal set $\mathcal{N}$, is contained in the 2nd to $(s+1)$st rows of X is in agreement with $Z \in (\mathbb{C}^s)^m$.

On the other hand, this shows that the elements of the $m \times m$-matrices A_σ whose joint eigenvectors constitute the matrix X must generally satisfy a number of *restrictions*. Trivially, the *first* row $a_1^{(\sigma)T}$ of A_σ must comply with $x_\sigma\, b_1(x) = x_\sigma = a_1^{(\sigma)T}\mathbf{b}$ or $a_1^{(\sigma)T} = (0..\overset{\sigma+1}{1}..0)$. Similarly, if the x_σ-multiple of some component $b_\nu(x)$ remains in $\mathcal{N}$, then the ν-th row of A_σ must be a unit vector, with the 1 in position $\bar{\nu}$ for $x_\sigma\, b_\nu(x) = b_{\bar{\nu}}(x)$. The remaining rows of

A_σ are nontrivial; they must comply with the relations (8.2) for the eigenvectors $\mathbf{b}(z_\mu)$ of A_σ. Generally there are more than s nontrivial rows while s of them should be sufficient, considering the number of data elements.

Moreover, it appears from (8.1) that *each one* of the A_σ carries the full information about Z in its eigenvectors which are the same for all matrices in the commuting family $\overline{A}$ generated by the A_σ; cf. Proposition 2.8 and Theorem 2.23. Therefore, the specification of *one* A_σ, say A_s, should uniquely specify all other A_σ. However, there is a fine point in Theorem 2.23: It talks about the *joint* eigenvectors of the matrices in the commuting family $\overline{A}$. And by Proposition 2.8, we can only be sure that an eigenvector of a particular A_σ is a joint eigenvector of $\overline{A}$ if the associated eigenvalue of A_σ has geometric multiplicity 1. While the *family* $\overline{A}$ is a nonderogatory commuting family by Corollary 2.26, an individual A_σ may well have a multiple eigenvalue with an eigenspace of a dimension > 1.

This is evident directly from (8.1): When $n > 1$ simple zeros have the *same* σ-component $\zeta_{\mu,\sigma}$, the associated vectors $\mathbf{b}(z_\mu)$ span an n-dimensional eigenspace of A_σ with the eigenvalue $\zeta_{\mu,\sigma}$. Naturally, when we prescribe the $\mathbf{b}(z_\mu)$ there is no harm. But when we compute the eigenvectors from A_σ, the eigenspace may appear as spanned by a different set of linearly independent eigenvectors which are not interpretable as values of $\mathbf{b}(x)$! Sometimes, it is possible to use the relations (8.2) to determine the appropriate basis vectors; cf. Example 8.1. Generally, one has to use a different matrix A_σ or a suitable linear combination of two or more A_σ. Since the projection of a set of disjoint points in $\mathbb{C}^s$ onto a 1-dimensional subspace preserves the disjointness for almost all such subspaces, almost all linear combinations of A_σ are nonderogatory.

The case of true multiple zeros is more delicate. Assume that there is one m_1-fold zero z_1 in Z, while the remaining $z_\mu,\ \mu = m_1 + 1, .., m$, are simple. Let the associated functionals in the dual space $\mathcal{D}(Z)$ be $c_\mu,\ \mu = 1(1)m_1$. Theorem 2.27 tells us that

$$A_\sigma \ \big(X_1 \mid \mathbf{b}(z_{m_1+1}) \dots \mathbf{b}(z_m) \big) \ = \ \big(X_1 \mid \mathbf{b}(z_{m_1+1}) \dots \mathbf{b}(z_m) \big) \begin{pmatrix} T_{\sigma 1} & & \\ & \zeta_{m_1+1,\sigma} & \\ & & \ddots \end{pmatrix}, \tag{8.3}$$

or

$$\big(c_1(x_\sigma \mathbf{b}),\ c_2(x_\sigma \mathbf{b}), \dots,\ c_{m_1}(x_\sigma \mathbf{b}) \big) \ = \ \big(c_1(\mathbf{b}),\ c_2(\mathbf{b}), \dots,\ c_{m_1}(\mathbf{b}) \big)\ T_{\sigma 1}\,; \tag{8.4}$$

thus, the *joint invariant subspace* X_1 of the family $\overline{A}$ is spanned by the vectors $c_1(\mathbf{b})$, $c_2(\mathbf{b})$, $\dots$, $c_{m_1}(\mathbf{b})$, and the elements in the upper triangular $m_1 \times m_1$-matrices $T_{\sigma 1}$ arise from the representation of the vectors $c_\mu\,(x_\sigma \mathbf{b}),\ \mu = 1(1)m_1$, in terms of the vectors in X_1: Since, for $A_\sigma,\ \zeta_{1,\sigma}$ is the eigenvalue associated with the only eigenvector $\mathbf{b}(z_1)$ in X_1, all diagonal elements of $T_{\sigma 1}$ are $\zeta_{1,\sigma}$, and—with an appropriate ordering of the c_μ—there exist unique coefficients $t_{\lambda\mu}^{(\sigma)}$ such that

$$c_\mu\,(x_\sigma \mathbf{b}) \ = \ \zeta_{1,\sigma}\ c_\mu(\mathbf{b}) + \sum_{\lambda=1}^{\mu-1} t_{\lambda\mu}^{(\sigma)}\, c_\lambda(\mathbf{b})\,, \quad \mu = 2(1)m_1\,;$$

cf. section 2.3.2. Now, the information about the differential structure of the multiple zero z_1 is shared by the columns of X_1 and all of the $T_{\sigma 1}$ in a not so transparent way, and there is, generally, no single A_σ which carries the full information about the differential structure of a multiple zero. We delay a detailed analysis to section 8.5.3.

If we have the quantitative description of a quotient ring with reference to a normal set $\mathcal{N}_1$, the generation of the description with reference to another normal set $\mathcal{N}_2$ (with the same number m of elements, of course) is straightforward, cf. section 2.4.1: Denote the multiplication matrices w.r.t. the basis vectors $\mathbf{b}_i$ of $\mathcal{N}_i$ by $A_\sigma^{(i)}$, $i = 1, 2$. The elements of $\mathcal{N}_2$ are either also in $\mathcal{N}_1$ or they have a nontrivial normal form representation in terms of $\mathbf{b}_1$ which implies

$$\mathbf{b}_2(x) \;=\; M_{21}\,\mathbf{b}_1(x) \mod \mathcal{I}\,.$$

Thus, by Proposition 2.22,

$$A_\sigma^{(2)} \;=\; M_{21}\,A_\sigma^{(1)}\,M_{21}^{-1}\,, \quad \sigma = 1(1)s\,. \tag{8.5}$$

If M_{21} is singular, $\mathcal{N}_2$ is not a feasible normal set for the quotient ring because the singularity of M_{21} implies that span $\mathcal{N}_2$ contains polynomials in $\mathcal{I}$.

Example 8.1: We take $s = 3$ and $m = 7$ and prescribe 7 disjoint points in $\mathbb{C}^3$ "at random," e.g., $Z = \{(2,1,0),\ (0,4,3),\ (2,0,-1),\ (-1,-2,4),\ (0,-1,1),\ (1,\mathrm{i},2+\mathrm{i}),\ (1,-\mathrm{i},2-\mathrm{i})\}$. From $\mathcal{T}^3(7)$, we choose a symmetric normal set $\mathcal{N}_1$ with $\mathbf{b}_1(x) = (1,\ x,\ y,\ z,\ xy,\ xz,\ yz)^T$ and form the vectors $\mathbf{b}_1(z_\mu)$ and the matrices X and Λ_σ of (8.1), where $\sigma = 1, 2, 3$ refers to x, y, z in this order. From $A_\sigma^{(1)} = X\,\Lambda_\sigma\,X^{-1}$, we obtain

$$A_1^{(1)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \frac{-10}{183} & \frac{5}{3} & \frac{10}{183} & \frac{14}{183} & \frac{1}{3} & \frac{-73}{183} & \frac{-2}{61} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \frac{218}{61} & -2 & \frac{148}{61} & \frac{-110}{61} & 1 & \frac{42}{61} & \frac{-40}{61} \\ \frac{454}{183} & \frac{-8}{3} & \frac{644}{183} & \frac{-50}{183} & \frac{-1}{3} & \frac{130}{183} & \frac{-80}{61} \\ \frac{-1213}{183} & \frac{11}{3} & \frac{-983}{183} & \frac{527}{183} & \frac{7}{3} & \frac{-199}{183} & \frac{99}{61} \end{pmatrix},$$

$$A_2^{(1)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \frac{625}{61} & -7 & \frac{534}{61} & \frac{-143}{61} & -2 & \frac{-43}{61} & \frac{-113}{61} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \frac{689}{183} & \frac{-7}{3} & \frac{409}{183} & \frac{-379}{183} & \frac{1}{3} & \frac{107}{183} & \frac{-33}{61} \\ \frac{-1213}{183} & \frac{11}{3} & \frac{-983}{183} & \frac{527}{183} & \frac{7}{3} & \frac{-199}{183} & \frac{99}{61} \\ 27 & -19 & 27 & -5 & -8 & -3 & -6 \end{pmatrix},$$

$$A_3^{(1)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \frac{-643}{61} & 7 & \frac{-455}{61} & \frac{400}{61} & 2 & \frac{-125}{61} & \frac{151}{61} \\ \frac{-1213}{183} & \frac{11}{3} & \frac{-983}{183} & \frac{527}{183} & \frac{7}{3} & \frac{-199}{183} & \frac{99}{61} \\ \frac{-2695}{183} & \frac{35}{3} & \frac{-2795}{183} & \frac{845}{183} & \frac{10}{3} & \frac{182}{183} & \frac{315}{61} \\ \frac{703}{61} & -7 & \frac{395}{61} & \frac{-301}{61} & -2 & \frac{75}{61} & \frac{68}{61} \end{pmatrix}.$$

Each of the matrices has 4 nontrivial rows, which indicates immediately that the information in these rows must be dependent.

When we determine the eigenvectors of the $A_\sigma^{(1)}$, say by the Maple routine `Eigenvectors`, with subsequent normalization for a first component 1, we recover the vectors $\mathbf{b}_1(z_\mu)$ for $\sigma = 2$ and 3. For $\sigma = 1$, however, we have three 2-fold eigenvalues 0, 1, and 2, because each of these values occurs as first coordinate for two different zeros; the associated 2-dimensional eigenspaces are not represented by the corresponding $\mathbf{b}_1(z_\mu)$ but by two other vectors chosen by the routine. This is immediately displayed by the appearance of a first component 0 in one vector of a pair, and by the fact that no complex components appear in the pair for the conjugate-complex zeros. Also it is easily checked that the relations (8.2) are not satisfied for these 3 pairs of eigenvectors. As a remedy, we may try to build linear combinations of the computed vectors which satisfy (8.2).

For the zeros (0,4,3), (0,-1,1), e.g., Maple gives us the eigenvectors $\bar{b}_1 = (1, 0, -\frac{7}{2}, 0, 0, 0, -\frac{15}{2})^T$, $\bar{b}_2 = (0, 0, \frac{5}{2}, 1, 0, 0, \frac{13}{2})^T$. When we determine $\gamma_1, \gamma_2 \in \mathbb{C}$ from

$$\gamma_1 \bar{b}_{1,1} + \gamma_2 \bar{b}_{2,1} = 1\,, \quad (\gamma_1 \bar{b}_{1,3} + \gamma_2 \bar{b}_{2,3})\,(\gamma_1 \bar{b}_{1,4} + \gamma_2 \bar{b}_{2,4}) = (\gamma_1 \bar{b}_{1,7} + \gamma_2 \bar{b}_{2,7})\,,$$

we obtain the two (γ_1, γ_2) pairs (1,1), (1,3) yielding the correct eigenvectors $(1, 0, -1, 1, 0, 0, -1)^T$ and $(1, 0, 4, 3, 0, 0, 12)^T$. For the conjugate-complex zero pair, the complex components of the eigenvectors can be recovered from the real representation because the linear combination coefficients are found from a quadratic equation.

When we wish to represent the quotient ring with respect to a basis $\mathbf{b}_2 = (1, x, y, z, x^2, xy, y^2)^T$, we need the normal forms of x^2 and y^2 in the basis $\mathbf{b}_1$. Obviously, their coefficients can be found in the 2nd row of $A_1^{(1)}$ and in the 3rd row of $A_2^{(1)}$, respectively. This yields the transformation matrix

$$M_{21} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{-10}{183} & \frac{5}{3} & \frac{10}{183} & \frac{14}{183} & \frac{1}{3} & \frac{-73}{183} & \frac{-2}{61} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \frac{625}{61} & -7 & \frac{534}{61} & \frac{-143}{61} & -2 & \frac{-43}{61} & \frac{-113}{61} \end{pmatrix},$$

and the multiplication matrices $A_\sigma^{(2)}$ via (8.5) with respect to the basis $\mathbf{b}_2$. □

8.1.2 The Ideal Generated by a Normal Set Ring

In section 2.2.1, we have seen that we can recover a 0-dimensional ideal $\mathcal{I} \subset \mathcal{P}^s$ from its quotient ring $\mathcal{R}[\mathcal{I}] = \mathcal{P}^s/\mathcal{I}$ when we have a basis $\mathbf{b}(x)$ of $\mathcal{R}[\mathcal{I}]$ and generators of the commuting family $\overline{A}$ of matrices which describe the multiplicative structure of the ring with respect to $\mathbf{b}$; cf. Theorem 2.7. This raises the following question: Given an *arbitrary* commutative ring $\mathcal{R}$ on an m-dimensional vector space $\mathcal{V} \subset \mathcal{P}^s$, can it be interpreted as the quotient ring of a polynomial ideal in $\mathcal{P}^s(m)$?

Without essential loss of generality (cf. section 2.5.1), we assume a normal set basis $\mathcal{N} \subset \mathcal{T}^s(m)$ for $\mathcal{R}$, with the associated basis *vector* $\mathbf{b}(x)$. As a ring, $\mathcal{R}$ is closed with respect to multiplication, i.e. all products of elements in $\mathcal{R}$ are in $\mathcal{R}$. But we may also interpret $\mathcal{R}$ as a subset of $\mathcal{P}^s$; then products of elements in $\mathcal{R}$ may well be outside $\mathcal{R}$. In particular, when

we consider multiplication of an element $r \in \mathcal{R}$ by some x_σ, $\sigma = 1(1)s$, the product in the $\mathcal{P}^s$-sense is in $\mathcal{N} \cup B[\mathcal{N}]$; obviously, (2.58) in Definition 2.21 has been chosen to accommodate all products $x_\sigma\, r$ for $r \in \mathcal{R}$. Thus, the multiplicative structure of $\mathcal{R}$ specifies a *linear map* $\mathcal{A}_\mathcal{N}$ from span $\mathcal{N} \cup B[\mathcal{N}]$ into span $\mathcal{N}$ which is a *projection*, i.e. which leaves $\mathcal{N}$ invariant:

$$\mathcal{A}_\mathcal{N}\, x^j \;:=\; \begin{cases} x^j & \text{for } x^j \in \mathcal{N}\,, \\ a_j^T\, \mathbf{b}(x) & \text{for } x^j \in B[\mathcal{N}]\,. \end{cases} \tag{8.6}$$

Then, for $r = c^T[r]\,\mathbf{b}(x) \in \mathcal{R}$, the result in $\mathcal{R}$ of its multiplication by x_σ is

$$x_\sigma r(x) \;=\; c^T[r]\, x_\sigma \mathbf{b}(x) \;=\; c^T[r]\, \mathcal{A}_\mathcal{N}(x_\sigma \mathbf{b}(x)) \;=:\; c^T[r]\, A_\sigma \mathbf{b}(x)\,. \tag{8.7}$$

Obviously, these $m \times m$ matrices A_σ, $\sigma = 1(1)s$, contain trivial μ-th rows (unit vector rows) for components b_μ of $\mathbf{b}$ with $x_\sigma b_\mu \in \mathcal{N}$ and the nontrivial rows a_j^T from (8.6) for b_μ with $x_\sigma b_\mu = x^j \in B[\mathcal{N}]$. Together, the *multiplication matrices* A_σ contain the complete information about $\mathcal{A}_\mathcal{N}$, i.e. about the multiplicative structure of $\mathcal{R}$. Note that we expect $\mathcal{R}$ to specify an ideal with m zeros (with m s components) but that there are $N = |B[\mathcal{N}]| > s$ vectors a_j^T (with N m components) in (8.6).

Due to the projection property of $\mathcal{A}_\mathcal{N}$ and the commutativity of multiplication in $\mathcal{R}$, the A_σ must satisfy

$$\begin{array}{lllll} \text{(i)} & e_j^T\, A_\sigma & = & e_{j'}^T & \text{for } x^{j'} = x_\sigma\, x^j \in \mathcal{N}\,, \\ \text{(ii)} & A_{\sigma_1}\, A_{\sigma_2} & = & A_{\sigma_2}\, A_{\sigma_1} & \text{for all } \sigma_1,\ \sigma_2\,. \end{array} \tag{8.8}$$

By their commutativity, the A_σ define a *commuting family* $\overline{A} := \{A^j := A_1^{j_1} \ldots A_s^{j_s},\ j \in \mathbb{N}_0^s\}$ which contains all matrix polynomials

$$p(A) \;:=\; \sum_{j \in J} \alpha_j\, A^j \;\in\; \mathbb{C}^{m \times m} \qquad \text{for } p \in \mathcal{P}^s\,;$$

cf. section 2.2.2.

Theorem 8.1. Consider a commutative ring $\mathcal{R}$ with a normal set basis $\mathcal{N} \in \mathcal{T}^s(m)$ and basis vector $\mathbf{b}(x)$ and let the multiplication in $\mathcal{R}$ be represented by the $A_\sigma \in \mathbb{C}^{m \times m}$, $\sigma = 1(1)m$, of (8.7). Then

$$\mathcal{I}[\mathcal{R}] \;:=\; \{\, p \in \mathcal{P}^s \;:\; p(A) = 0 \ \text{(zero matrix)}\,\} \;\subset\; \mathcal{P}^s \tag{8.9}$$

is an ideal.

Proof: Trivially, the 0-polynomial is in $\mathcal{I}[\mathcal{R}]$, and so is $p_1 + p_2$ for $p_1, p_2 \in \mathcal{I}[\mathcal{R}]$; for $q \in \mathcal{P}^s$, $p \in \mathcal{I}[\mathcal{R}]$, $q \cdot p \in \mathcal{I}[\mathcal{R}]$ holds because, by commutativity, $(q\, p)(A) = q(A)\, p(A) = 0$. □

Theorem 8.1 is constructive because a basis of $\mathcal{I}[\mathcal{R}]$ can readily be specified:

Proposition 8.2. In the situation of Theorem 8.1, consider the $x^{j'} \in B[\mathcal{N}]$ and the polynomials

$$bb_{j'}(x) \;:=\; x^{j'} - a_{j'}^T\, \mathbf{b}(x)\,, \tag{8.10}$$

with the coefficient vectors $a_{j'}^T$ of (8.6). Then $\mathcal{I}[\mathcal{R}] := \langle bb_{j'}(x),\ \forall j' :\ x^{j'} \in B[\mathcal{N}]\rangle$.

Proof: Let $\mathbf{b}(x) := (x^{j_\mu},\ \mu = 1(1)m\}$ and consider the two possible interpretations of the m-vector $A_\sigma \cdot \mathbf{b}(A)$ of $m \times m$-matrices

$$\begin{pmatrix} \sum_{\mu=1}^{m} (a_{\sigma,1})_\mu\, A^{j_\mu} \\ \vdots \\ \sum_{\mu=1}^{m} (a_{\sigma,m})_\mu\, A^{j_\mu} \end{pmatrix} \;=\; A_\sigma \cdot \mathbf{b}(A) \;=\; \begin{pmatrix} A_\sigma\, A^{j_1} \\ \vdots \\ A_\sigma\, A^{j_m} \end{pmatrix}$$

which follow from linear algebra and (8.7). The identity of the right-hand and left-hand expression implies that $bb_{j'}(A) = 0$ for $\forall\, x^{j'} = x_\sigma x^j \in B[\mathcal{N}],\ x^j \in \mathcal{N}$. How each $p \in \mathcal{I}[\mathcal{R}]$ can be represented as a polynomial combination of $bb_{j'}$ is shown in section 8.2.1. □

Since $|B[\mathcal{N}]| > s$ (often $\gg s$), the basis (8.10) could well be *inconsistent* so that the generated ideal would be trivial (possess no zeros).

Theorem 8.3. In the situation of Theorem 8.1, if the commuting matrix family $\overline{A}$ is nonderogatory (cf. Definition 2.9), then the border basis (8.10) is consistent and $\langle\{bb_{j'}\}\rangle \subset \mathcal{P}^s(m)$.

Proof: Compare section 2.2.2. We consider, at first, the case of m joint eigenvectors which form the regular matrix $X \in \mathbb{C}^{m\times m}$. By (2.22), the A_σ satisfy $A_\sigma = X\,\Lambda_\sigma\,X^{-1}$; but as we have begun with an arbitrary multiplicative structure, we cannot readily interpret X and the diagonal matrices Λ_σ as in Theorem 2.23. However (cf. section 2.4.1), we can interpret X as a *transformation matrix* from $\mathbf{b}$ to another basis $\mathbf{b}_0(x) = X^{-1}\,\mathbf{b}(x)$ of $\mathcal{R}$ with respect to which multiplication in $\mathcal{R}$ is represented by the matrices

$$A_\sigma^{(0)} \;=\; X^{-1}\,A_\sigma\,X \;=\; \Lambda_\sigma \;=:\; \operatorname{diag}(\lambda_{\sigma\mu})\,, \quad \sigma = 1(1)s\,;$$

cf. Proposition 2.22. Thus, we have in $\mathcal{R}$, for $\sigma = 1(1)s$, $x_\sigma \mathbf{b}_0(x) = \Lambda_\sigma \mathbf{b}_0(x)$ or

$$(x_\sigma - \lambda_{\sigma 1})\, b_{01}(x) = \ldots = (x_\sigma - \lambda_{\sigma\mu})\, b_{0\mu}(x) = \ldots = (x_\sigma - \lambda_{\sigma m})\, b_{0m}(x) = 0\,. \qquad (8.11)$$

These equations in $\mathcal{R}$ must hold in $\mathbb{C}$ at the zeros $z_\mu = (\zeta_{\mu\sigma},\ \sigma = 1(1)s)$ of $\mathcal{I}[\mathcal{R}]$ which requires that, at each z_μ, all $b_{0\sigma}(z_\mu)$ vanish except one, which we call $b_{0\mu}$. $\mathbf{b}_0(z_\mu)$ cannot vanish because this would imply $\mathbf{b}(z_\mu) = X \cdot \mathbf{b}_0(z_\mu) = 0$ while $b_1(x) \equiv 1$. With the normalization $b_{0\mu}(z_\mu) = 1$, $\mathbf{b}_0$ becomes the Lagrange basis for $Z := \{z_\mu,\ \mu = 1(1)m\}$. As in section 2.4.1, this implies that X and Λ_σ are as in section 8.1.1. Now, Theorem 2.27 tells us that, for any $p \in \mathcal{P}^s$, $p(A) = X \operatorname{diag}(p(z_1), .., p(z_m))\, X^{-1}$ whence

$$p(A) \;=\; 0 \qquad \Longrightarrow \qquad p(z_\mu) = 0\,, \quad \mu = 1(1)m\,.$$

There cannot be another $\bar{z} \notin Z$ with $p(\bar{z}) = 0\ \forall\, p \in \mathcal{I}[\mathcal{R}]$ because this would require an $(m+1)$st eigenvalue for the matrices A_σ.

The case of joint invariant subspaces of dimensions > 1 leads to multiple zeros whose differential structure is defined by the associated vectors in X and upper-tridiagonal blocks in the Λ_σ; cf. Proposition 2.8. As above, $p(A) = 0$ implies that all $p \in \mathcal{I}[\mathcal{R}]$ must have a multiple zero z_μ with that particular structure. Details will be explained in section 8.5. □

We have shown that any commutative ring $\mathcal{R}$ with a normal set basis $\mathcal{N} \in \mathcal{T}^s(m)$ and commuting multiplication matrices with the appropriate trivial rows generates a polynomial ideal $\mathcal{I}[\mathcal{R}] \in \mathcal{P}^s(m)$ via the border basis $\mathcal{B}_{\mathcal{N}}[\mathcal{I}[\mathcal{R}]] = \{bb_{j'}(x),\ x^{j'} \in B[\mathcal{N}]\}$ of (8.10). This establishes that the *commutativity of the multiplication matrices* is the essential criterion for the existence of a relation between a ring with a monomial basis and a 0-dimensional ideal. In a concise form, this insight has been pointed out by Mourrain ([8.1]).

For us, an important consequence is the following: Consider a 0-dimensional polynomial system $P \subset \mathcal{P}^s$, with $\langle P\rangle \in \mathcal{P}^s(m)$, with a quotient ring $\mathcal{R}[\langle P\rangle] = \operatorname{span}\mathcal{N}$, $\mathcal{N} \in \mathcal{T}^s(m)$, with multiplication matrices A_σ, $\sigma = 1(1)s$. Consider matrices $\tilde{A}_\sigma \approx A_\sigma$, with the same trivial rows but slightly perturbed nontrivial rows. *If and only if* the $\tilde{A}_\sigma$ *commute*, they define a ring $\widetilde{\mathcal{R}}$ which can be interpreted as the quotient ring of an ideal $\widetilde{\mathcal{I}} \in \mathcal{P}^s(m)$; the zero set $\tilde{Z} \in (\mathbb{C}^s)^m$ is then an approximation of the zero set Z of $\langle P\rangle$. But when we compute *approximate* multiplication matrices $\tilde{A}_\sigma$ from the specification of P by approximate computation, we cannot expect them to commute exactly; thus we cannot follow our standard approach and consider the $\tilde{A}_\sigma$ as *exact* multiplication matrices of a neighboring quotient ring $\widetilde{\mathcal{R}}$. The handling of this dilemma will be discussed in section 9.2.

The following result from linear algebra facilitates the checking of the commutativity of the A_σ:

Proposition 8.4. Consider a family $\overline{A}$ of matrices generated by A_σ, $\sigma = 1(1)s$. If one of the generators (say A_s) is nonderogatory, then $A_\sigma A_s = A_s A_\sigma$, $\sigma \neq s$, implies the commutativity of all matrices in $\overline{A}$.

Proof: Compare [2.15], p.139, Problem 1. □

Example 8.2: For $\mathcal{N} := \{1, x, y, z\} \in \mathcal{T}^3(4)$, consider the quotient ring $\mathcal{R}$ for the ideal from $\mathcal{P}^3(4)$ with the zero set $Z = \{(1,2,0),\ (-1,-2,0),\ (2,0,-1),\ (0,-1,-2)\}$; for $\mathbf{b}(x) = (1, x, y, z)^T$, the multiplication matrices of $\mathcal{R}$ are

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 2 & -1 & 1 \\ 2 & \frac{-4}{7} & \frac{2}{7} & \frac{6}{7} \\ 0 & \frac{-8}{7} & \frac{4}{7} & \frac{-2}{7} \end{pmatrix},\ A_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 2 & \frac{-4}{7} & \frac{2}{7} & \frac{6}{7} \\ 4 & \frac{-10}{7} & \frac{5}{7} & \frac{8}{7} \\ 0 & \frac{-4}{7} & \frac{2}{7} & \frac{-8}{7} \end{pmatrix},\ A_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & \frac{-8}{7} & \frac{4}{7} & \frac{-2}{7} \\ 0 & \frac{-4}{7} & \frac{2}{7} & \frac{-8}{7} \\ 0 & \frac{-4}{7} & \frac{2}{7} & \frac{-15}{7} \end{pmatrix}.$$

The border set $B[\mathcal{N}]$ has the 6 elements $x^2,\ xy,\ xz,\ y^2,\ yz,\ z^2$; accordingly, the ideal may be defined by the 6 border basis elements $bb_1 = x^2 - (2x - y + z + 1)$, $bb_2 = xy - (-4x + 2y + 6z + 14)/7$, $bb_3 = xz - (-8x + 4y - 2z)/7$, $bb_4 = y^2 - (-10x + 5y + 8z + 28)/7$, $bb_5 = yz - (-4x + 2y - 8z)/7$, $bb_6 = z^2 - (-4x + 2y - 15z)/7$. This basis is consistent and has the joint zero set Z. (Note that A_3 has a 2-fold eigenvalue 0 and the associated eigenspace spanned by $(1,0,0,0)^T$, $(0,1,2,0)^T$ does not permit a determination of the two associated zeros.)

Now we round the elements in the A_σ to 5 *relative* decimal digits and compute the normalized eigenvectors of the individual $\tilde{A}_\sigma$. Each $\tilde{A}_\sigma$ yields a slightly different approximation $\tilde{Z}_\sigma$ of the original zero set Z; rounded to 5 digits after the decimal point we obtain from

$$\tilde{A}_1: \begin{matrix} (.99985, 2.00220, .00150) \\ (-1.00002, -2.00000, .00039) \\ (2.00013, -.00018, -.99992) \\ (-.00026, -.99966, -1.99905) \end{matrix} \qquad \tilde{A}_2: \begin{matrix} (1.00010, 1.99980, -.00010) \\ (-.99971, -1.99967, -.00051) \\ (1.99973, .00040, -.99984) \\ (.00019, -1.00013, -1.99970) \end{matrix}$$

$$\tilde{A}_3: \begin{matrix} (.99996, 2.00001, .00001) \\ \textit{(.00000,.00000,.00000)} \\ (2.00006, -.00006, -1.00006) \\ (.00002, -1.00004, -2.00004) \end{matrix}$$

(The perturbation has also split the 2-fold eigenvalue 0 of A_3, but the "singular" eigenvector $(1, 0, 0, 0)^T$ from the eigenspace representation has persevered, due to the 0-column in A_3.) □

8.1.3 Quasi-Univariate Normal Sets

In the previous section, we have seen that the *overdetermination* which is generally present in the specification of a quotient ring $\mathcal{R}$ by a monomial basis $\mathcal{N}$ and the s multiplication matrices A_σ requires the satisfaction of the *constraints* expressed by (8.8); otherwise there exists no ideal which matches $\mathcal{R}$ (cf. Example 8.2).

In the univariate case, this problem does not arise: A quotient ring $\mathcal{R}$ for a polynomial ideal from $\mathcal{P}^1(m)$ has the unique normal set basis $\mathcal{N} = \{1, x, \ldots, x^{m-1}\}$ and the only multiplication matrix, for the basis vector $\mathbf{b}(x) = (1, x, x^2, \ldots, x^{m-1})^T$, is

$$A = \begin{pmatrix} 0 & 1 & 0 & & \\ & \ddots & 1 & \ddots & \\ 0 & & \ddots & \ddots & 0 \\ & & & 0 & 1 \\ \alpha_0 & \ldots & & \ldots & \alpha_{m-1} \end{pmatrix} \in \mathbb{C}^{m\times m} .$$

Any choice of the m elements α_μ in the only nontrivial row of A defines a multiplication matrix of a proper quotient ring $\mathcal{R}$. The m eigenvalues of A (counting multiplicities) are the m zeros of the ideal $\mathcal{I}[\mathcal{R}]$. This indicates that we may be able to avoid the overdetermination in the multivariate case if we look for a specification of the multiplicative structure by *one* $m \times m$-matrix with *exactly* s nontrivial rows: m zeros in $\mathbb{C}^s$ represent $m\,s$ data and so do s rows of m elements.

The nontrivial rows $a_{\sigma\nu}^T$ of a multiplication matrix A_σ contain the coefficients of the normal forms of the monomials $x_\sigma\, b_\nu(x) = x^{j'} \in B[\mathcal{N}]$; these monomials constitute the *border subset* $B_\sigma[\mathcal{N}] := (x_\sigma\mathcal{N}) \setminus \mathcal{N} \subset B[\mathcal{N}]$.

Definition 8.2. A normal set $\mathcal{N} \subset \mathcal{T}^s$, with $x_1, \ldots, x_s \in \mathcal{N}$, for which one or several border subsets B_σ have exactly s elements, is called a *quasi-univariate* normal set. (For a simpler notation, the distinguished variable x_σ to which the quasi-univariate situation refers will commonly be called x_s.) □

An element in B_s has the form $x^{k_\nu} x_s^{n_\nu}$, with a vanishing s-component in k_ν and $n_\nu \geq 1$. The requirement $1, x_1, \ldots, x_{s-1} \in \mathcal{N}$, together with $|B_s| = s$, restricts the k_ν to 0 and the unit vectors e_σ, $\sigma = 1(1)s - 1$. Thus, the nondistinguished variables $x_1, \ldots, x_{s-1}$ can occur only *disjointly and linearly* in the monomials of a quasi-univariate normal set with distinguished variable x_s. Closedness of $\mathcal{N}$ further requires that $n_\sigma \leq n_s$, $\sigma = 1(1)s - 1$, $n_s \geq 2$, where n_σ is the x_s-exponent of the multiple of x_σ in B_s. For $m \geq s$ (which we have generally assumed), quasi-univariate normal sets always exist.

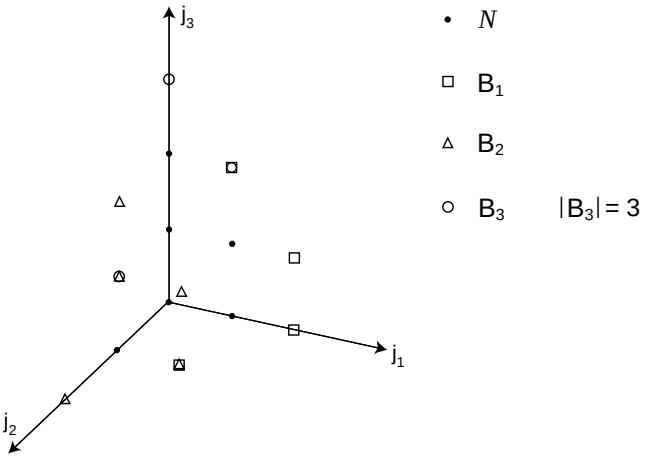

Figure 8.1.

Example 8.3: Definition 8.2 loosely says: A quasi-univariate normal set contains only products of one element from $\{1, x_1, \ldots, x_{s-1}\}$ with a power of x_s. Thus, a quasi-univariate normal set consists of s "columns" of length n_σ in the direction of x_s; cf. Figure 8.1. For $s = 1$, this reduces to $1, x, .., x^{n-1}$, which explains the name.

In $\mathcal{T}^3(7)$ (cf. Example 8.1), the following normal sets are quasi-univariate, with distinguished variable z : $(1, x, y, z, z^2, z^3, z^4)$, $(1, x, y, z, yz, z^2, z^3)$, $(1, x, y, z, yz, z^2, yz^2)$, $(1, x, y, z, xz, yz, z^2)$, and the two resulting from exchanging the roles of x and y in the 2nd and the 3rd set. The normal set $\{1, x, y, z\}$ of Example 8.2 is quasi-univariate with respect to each of the three variables. □

Theorem 8.5. Consider a quasi-univariate normal set $\mathcal{N}$ from $\mathcal{T}^s(m)$, $m \geq s + 1$, with distinguished variable x_s, and form a multiplication matrix $A_s \in \mathbb{C}^{s \times s}$ with respect to $\mathcal{N}$ by properly choosing the trivial rows and by completing the nontrivial rows with *arbitrary* complex numbers. If A_s is nonderogatory and has m linearly independent eigenvectors, it defines a commutative ring $\mathcal{R}$ with basis $\mathcal{N}$ which is the quotient ring of an ideal $\mathcal{I}[\mathcal{R}] \in \mathcal{P}^s(m)$. The m zeros of $\mathcal{I}[\mathcal{R}]$ are specified by the components of the normalized eigenvectors of A_s in the usual way.

Proof: The restriction on the eigenvectors of A_s excludes the delicate case of a multiple zero in $\mathcal{I}$; a multiple eigenvalue of A_s with an eigenspace of corresponding dimension is also excluded. Thus, after normalization, each eigenvector defines a zero $z_\mu \in \mathbb{C}^s$; also, by the structure of

the basis vector $\mathbf{b}$ and the trivial rows of A_s, each eigenvector must be internally consistent, i.e. satisfy (8.2). Therefore, we can define the remaining multiplication matrices A_σ via (8.1) and obtain a *commuting family* $\overline{A}$ which generates a border basis for the ideal $\mathcal{I}[\mathcal{R}]$ with the m zeros z_μ. □

Corollary 8.6. Under the assumptions of Theorem 8.5, a small perturbation of the nontrivial rows of A_s does *not* invalidate the conclusions of the Theorem. In particular, the eigenvectors remain internally consistent and the zeros are continuous functions of the perturbation.

Proof: The restrictions on A_s hold in an open domain in the data space of the elements of the nontrivial rows; therefore, they hold in a sufficiently small neighborhood of A_s. Under the assumptions of Theorem 8.5, the components of the normalized eigenvectors are continuous functions of the nontrivial elements of A_s. □

Example 8.4: We take the situation of Example 8.1, but choose the quasi-univariate normal set $\mathcal{N}_0 = \{1, x, y, z, xz, yz, z^2\}$, with the components in $\mathbf{b}_0$ in the same order. To find the transformation matrix M_{01} which yields the multiplication matrix $A_3^{(0)}$ with respect to $\mathbf{b}_0$ we have only to express the new normal set element z^2 in terms of the original basis $\mathbf{b}_1$ which is achieved by the 4th row of $A_3^{(1)}$. With

$$M_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \frac{-643}{61} & 7 & \frac{-455}{61} & \frac{400}{61} & 2 & \frac{-125}{61} & \frac{151}{61} \end{pmatrix},$$

we obtain $A_3^{(0)} = M_{01}\, A_3^{(1)}\, M_{01}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \frac{520}{183} & 0 & \frac{-520}{183} & \frac{-385}{61} & \frac{269}{61} & \frac{190}{183} & \frac{5}{3} \\ \frac{60}{61} & 0 & \frac{-60}{61} & \frac{99}{61} & \frac{-50}{61} & \frac{219}{61} & -1 \\ \frac{485}{61} & -9 & \frac{613}{61} & \frac{-191}{61} & \frac{-89}{61} & \frac{-197}{61} & 3 \end{pmatrix},$

which obviously has the right form. Since the z-component takes a different value in each of the 7 zeros, the assumptions of Theorem 8.5 are satisfied.

When we subject the elements in the lower 3 rows of $A_3^{(0)}$ to random perturbations say of maximal modulus .0003, the relevant components of the eigenvectors change only by quantities of that same order. Also, the internal consistency of the eigenvectors remains fully intact: The defects in the constraints (8.2) remain at the round-off level of the computation. □

Proposition 8.7. Consider a quasi-univariate normal set and the multiplication matrix A_s for the distinguished variable x_s. If A_s satisfies the assumptions of Theorem 8.5, the nontrivial rows of the other A_σ may be determined from A_s directly without a solution of the eigenproblem.

Proof: The elements x^j in a border subset B_σ, $\sigma \neq s$, fall in one of 3 categories:

(a) x^j is also in B_s;

(b) $x^j = x_s^{\lambda_j}\, x^{\bar{j}}$ is "above" an element $x^{\bar{j}} \in B_s$ (cf. Figure 8.1);

(c) neither (a) nor (b).

The rows $a_{x^j}^T$ for (a) and (b) can be found directly from A_s and $A_s^{\lambda_j+1}$, respectively. For the remaining nontrivial rows (case (c)), one can write down relations which relate them to an x_σ-neighbor of an element in B_s; these relations are *linear* in the rows of A_σ. They must have a unique solution since we know from Theorem 8.5 that A_σ is uniquely defined by A_s. A_s has been assumed as nonderogatory; therefore, by Proposition 8.4, the A_σ must also be *mutually* commuting. □

Example 8.4, continued: For $\mathcal{N}_0$, the set B_1 consists of $x^2,\ xy,\ x^2z, x\,y\,z,\ x\,z^2$. $x\,z^2$ is in (a); the 4 others are in (c). The 4 linear equations for these nontrivial rows of A_1 are:

$$a_{x^2}^T \cdot A_3 = a_{x^2z}^T = a_{xz}^T \cdot A_1 \quad \text{and} \quad a_{xy}^T \cdot A_3 = a_{xyz}^T = a_{yz}^T \cdot A_1\,. \quad \square$$

The quasi-univariate situation also sheds light on the potential shortcomings of a multiplication matrix A_s whose border subset $B_s[\mathcal{N}]$ is larger than s, say e.g. $s+1$. In this case, $\mathcal{N}$ must contain one monomial nonlinear in the x_σ, $\sigma < s$, and possibly products of it with powers of x_s. Let x_1x_2 be that monomial. Then the nontrivial row in A_s for the border element $x_1x_2x_s^{k_{12}} = x_s \cdot x_1x_2x_s^{k_{12}-1}$, with $x_1x_2x_s^{k_{12}-1} \in \mathcal{N}$, is the end of a chain of trivial rows; this causes the corresponding components in the eigenvectors of A_s to be internally consistent with respect to multiplication with the respective eigenvalue: In the μ-th eigenvector, the component for $x_1x_2x_s^\kappa$ will equal $\zeta_{\mu s}$ times the component for $x_1x_2x_s^{\kappa-1}$, a consistency which holds automatically for all components $x_\sigma x_s^\kappa$.

But there *cannot* be any consistency between the values of the components $x_1x_2x_s^\kappa$ and $x_1x_s^\kappa$ or $x_2x_s^\kappa$, resp.; actually, the monomial x_1x_2 simply takes the place of a further nondistinguished variable in the quasi-univariate case whose value at the zeros is independent of the values of the other x_σ. The necessary relations with respect to factors x_1 or x_2 (or generally x_σ, $\sigma < s$) are only introduced into the eigenvectors of A_s by the fact that A_s commutes with the other A_σ.

Example 8.5: We consider Example 8.1 and round $A_3^{(1)}$ to 6 relative decimal digits. The 2nd through 4th components of the normalized eigenvectors give approximations to the zeros in Z with deviations of $O(10^{-5})$ throughout. When we compare the 5th components (for xy) with the products of the 2nd and 3rd components, the differences vary between .3 and 12 units of 10^{-5}. If we do the same with the components no. 6 and the products of no. 2 and no. 4, or with no. 7 and the products of no. 3. and no. 4, the differences are at the round-off level. This shows that the internal inconsistency of the rounded multiplication matrix is restricted to the relations between the normal set monomials x, y and xy. □

The surprisingly strong result of Theorem 8.5 and Corollary 8.6 appears to suggest that the computational determination of a basis for the quotient ring associated with a 0-dimensional polynomial system should be led towards a quasi-univariate normal set. At present, it is not clear how this may generally be achieved and how a distinguished variable may be selected a priori. We will also find aspects of a normal set from a numerical point of view which do not favor quasi-univariate normal sets; for large m, the strong asymmetry in a quasi-univariate representation may result in a poor condition of the eigenproblem for $A_s^{(0)}$.

Exercises

1. In translating the representation of a quotient ring from one normal set basis $\mathcal{N}_1$ to another one $\mathcal{N}_2$, it may not always happen that all elements of $\mathcal{N}_2 \setminus \mathcal{N}_1 \cap \mathcal{N}_2$ are in the border set $B[\mathcal{N}_1]$ so that their normal forms with respect to $\mathbf{b}_1$ can be read from one of the multiplication matrices $A_\sigma^{(1)}$; cf. Example 8.1. In this case, we can form intermediate normal sets $\mathcal{N}_{1\kappa}$, with $\mathcal{N}_{10} = \mathcal{N}_1, \mathcal{N}_{1k} = \mathcal{N}_2$ such that $\mathcal{N}_{1,\kappa+1} \setminus \mathcal{N}_{1\kappa} \cap \mathcal{N}_{1,\kappa+1} \subset B[\mathcal{N}_{1\kappa}]$ and the transformation matrices for the transition from $\mathcal{N}_{1\kappa}$ to $\mathcal{N}_{1,\kappa+1}$ can be written down directly.

(a) Use this approach with the data of Example 8.1 to find the representation of $\mathcal{R}$ with reference to the ("univariate") normal set $\widehat{\mathcal{N}} = \{1, z, z^2, z^3, z^4, z^5, z^6\}$.

(b) From the information about the zeros, determine the only nontrivial row of $\widehat{A}_3$ directly. How can you also determine the first row of the multiplication matrices $\widehat{A}_1$ and $\widehat{A}_2$ (why are they nontrivial for $\widehat{\mathcal{N}}$)? How can you obtain the remaining rows of $\widehat{A}_1$ and $\widehat{A}_2$ from their first row and the last row of $\widehat{A}_3$?

(c) Assume that you have been given the last row of $\widehat{A}_3$ and the first row of $\widehat{A}_1$ and $\widehat{A}_2$. Convince yourself that they contain the complete information about the zeros of $\mathcal{I}[\mathcal{R}]$. How would you find the zeros from this information?

2. (a) Consider Example 8.2 and convince yourself that its normal set $\mathcal{N} = \{1, x, y, z\}$ is quasi-univariate for *each* of the three variables. How does this agree with the fact that each of the three *perturbed* multiplication matrices $\tilde{A}_\sigma$ yields a different zero set?

(b) For the quotient ring $\widetilde{\mathcal{R}}_2$ defined by $\mathcal{N}$ and $\tilde{A}_2$, find the associated multiplication matrices $\tilde{A}_1$ and $\tilde{A}_3$ by the procedure described in section 8.1.3 (above Example 8.4, continued). Verify that these yield the same zero set as $\tilde{A}_2$ within round-off.

8.2 Normal Set Representations of 0-Dimensional Ideals

In section 2.5.2, we had introduced our standard representation of a 0-dimensional ideal by a *normal set* and the related multiplication matrices mod $\mathcal{I}$ or—equivalently—the related border basis; cf. Definition 2.23. In this section, we consider various aspects of this representation which are important for its computational use.

For an ideal $\mathcal{I} \subset \mathcal{P}^s(m)$, we have a normal set $\mathcal{N} \in \mathcal{T}^s(m)$, with the associated monomial basis vector $\mathbf{b}(x) = (b_\mu(x),\ \mu = 1(1)m)$ of $\mathcal{R}[\mathcal{I}]$. The border set $B[\mathcal{N}]$ consists of N monomials $x^j,\ j \in \mathbb{N}_0^s$. By (8.6), the quantitative part of the normal set representation of $\mathcal{I}$ consists of the N row vectors $a_j^T \in \mathbb{C}^m$ which specify the normal forms of the border monomials x^j mod $\mathcal{I}$:

$$\mathrm{NF}_{\mathcal{I}}[x^j] \;=\; a_j^T\, \mathbf{b}(x) \qquad \forall\, x^j \in B[\mathcal{N}]\,. \tag{8.12}$$

These a_j^T furnish the nontrivial rows of the multiplication matrices A_σ mod $\mathcal{I}$ as well as the coefficients of the polynomials in the border basis $\mathcal{B}_{\mathcal{N}}[\mathcal{I}] = \{bb_j(x) := x^j - a_j^T\, \mathbf{b}(x)\}$.

8.2.1 Computation of Normal Forms and Border Basis Expansions

With the aid of the normal set representation of $\mathcal{I}$, we must be able to compute the normal form $\mathrm{NF}_{\mathcal{I}}[p]$ in span $\mathcal{N}$ for a specified $p \in \mathcal{P}^s$; cf. Definition 2.20.

Proposition 8.8. In the situation just described,

$$\mathrm{NF}_{\mathcal{I}}[p(x)] \;=\; \mathrm{NF}_{\mathcal{I}}[e_1^T\, p(x)\mathbf{b}(x)] \;=\; e_1^T\, p(A)\, \mathbf{b}(x) \tag{8.13}$$

so that the normal form functionals $\mathbf{c}^T$ which form the basis of the dual space $\mathcal{D}[\mathcal{R}]$ conjugate to $\mathbf{b}$ are defined by $\mathbf{c}^T[p] = e_1^T\, p(A)$.

Proof: Compare (2.20) in Corollary 2.6 and Proposition 2.13. □

For small values of m and a low total degree of p, the evaluation of (8.13) provides a quick and easy way for the computation of $\mathrm{NF}_{\mathcal{I}}[p]$. Note that, as long as $x^j \in \mathcal{N}$, with $x^j = b_\nu(x) = e_\nu^T \mathbf{b}(x)$, $\mathrm{NF}[x^j] = e_1^T A^j = e_\nu$ remains a unit vector; for $x^j \in B[\mathcal{N}]$, $\mathrm{NF}[x^j]$ equals a row in one of the A_σ. Thus the actual computation starts when the recursive evaluation of the normal forms of the monomials in $p(x) = \sum_{j\in J} \alpha_j x^j$ leaves the border set.

To deal with the "distance" of a monomial from $\mathcal{N}$, we remember the "hull sets" of a normal set $\mathcal{N}$ which are generated by an iteration of the border operation; cf. Definition 2.21, (2.59):

For a closed set $\mathcal{N} \subset \mathcal{T}^s$, the *hull sets* $H_\ell[\mathcal{N}]$, $\ell = 0, 1, 2, \ldots$, are defined by

$$H_0[\mathcal{N}] \;:=\; \mathcal{N}\,, \quad H_{\ell+1}[\mathcal{N}] \;:=\; H_\ell[\mathcal{N}] \,\cup\, B[H_\ell[\mathcal{N}]] \;\subset\; \mathcal{T}^s\,.$$

Obviously, we may reach any monomial x^j in $H_\ell[\mathcal{N}]$ from an appropriate monomial in $B[\mathcal{N}]$ by $\ell - 1$ successive multiplications by suitable variables so that $\mathrm{NF}[x^j]$ may be found from (8.13) by $\ell - 1$ vector-matrix multiplications.

Definition 8.3. With reference to a fixed normal set $\mathcal{N} \subset \mathcal{T}^s$, consider the map $\ell : \mathcal{T}^s \to \mathbb{N}_0$ defined by $\ell(x^j) := \min\{\lambda : x^j \in H_\lambda[\mathcal{N}]\}$. The $\mathcal{N}$-*index* of a polynomial $p(x) = \sum_{j\in J} \alpha_j x^j \in \mathcal{P}^s$ is $\ell(p) := \max_{j\in J} \ell(x^j)$. The terms in p whose monomials satisfy $\ell(x^j) = \ell(p)$ are the $\mathcal{N}$-*leading terms* of p. □

Example 8.6: By its definition (8.10), each border basis element $bb_j(x)$ has $\mathcal{N}$-index 1 and one $\mathcal{N}$-leading term x^j. A polynomial $x^k\, bb_j(x)$ has $\mathcal{N}$-index $|k| + 1$ and the leading term x^{k+j}. Generally, a polynomial has more than one $\mathcal{N}$-leading term; if all terms of p are in $B[H_{\ell-1}[\mathcal{N}]]$, p consists only of $\mathcal{N}$-leading terms. □

The number of vector-matrix multiplications necessary to find $\mathrm{NF}[p]$ from (8.13) is, of course, bounded by the sum of the $\mathcal{N}$-indices of its terms, but an intelligent evaluation will strive to use common intermediate monomials to arrive at the various monomials composing p. Thus the minimal number of necessary vector-matrix multiplications may be much smaller. Also, due to the special structure of the A_σ with many trivial and perhaps only a few nontrivial rows which may themselves be quite sparse, the cost of a vector-matrix multiplication is often much less than m^2 arithmetic operations ($m = |\mathcal{N}|$).

The more conventional way of computing normal forms is the reduction of p to a polynomial in $\mathcal{N}$ by the successive subtraction of polynomials in $\mathcal{I}$. With the border basis elements bb_j of (8.10), we have a means of reducing the $\mathcal{N}$-index of a monomial by one in one subtraction: Assume that $x^{\bar\jmath}$ with $\ell(x^{\bar\jmath}) = \ell > 1$ is a multiple $x^k\, x^j$ of the leading monomial x^j of one of the border basis elements bb_j; there must be one or several such bb_j. Then, by (8.10),

$$x^{\bar\jmath} - x^k\, bb_j(x) \;=\; a_j^T\, x^k\, \mathbf{b}(x)\,; \tag{8.14}$$

thus, this reduction step generates a polynomial of $\mathcal{N}$-index $\ell-1$. But this polynomial may have several $\mathcal{N}$-leading monomials so that the continuation of this reduction procedure will generally involve more and more monomials after a few steps. If it is applied to all monomials in a given polynmial p, (almost) all of the monomials in the sets $B[H_\lambda[\mathcal{N}]]$ will become involved as λ decreases; at the same time, the magnitude of these sets decreases with λ. An a priori control which minimizes the number of individual subtractions of a multiple of a border basis element is hard to conceive, taking into account the many possible shapes of a normal set in s dimensions. While the individual reduction steps are not unique, the final result $\mathrm{NF}_{\mathcal{I}}[p]$ must be unique; otherwise two different polynomials in span $\mathcal{N}$ would differ by a polynomial in $\mathcal{I}$.

For moderate values of ℓ, we must expect $\mathrm{O}(\ell\, m\, n)$ operations, where $n \sim |\, B[H_\lambda[\mathcal{N}]]\,|$ for low λ. This appears comparable to the count for an algorithm based on (8.13). Actual numbers will depend strongly on the implemented strategies for the multiple use of operations and on the specific situations at hand.

Normal form computation may also be based on

Proposition 8.9. For $\mathcal{I}$ with normal set $\mathcal{N}$, the normal form mod $\mathcal{I}$ of a polynomial $p \in \mathcal{P}^s$ is the interpolation polynomial in span $\mathcal{N}$ of the values $p(z_\mu)$ specified at the zeros $z_\mu \in Z(\mathcal{I})$.
Proof: $p - \mathrm{NF}_{\mathcal{I}}[p] \in \mathcal{I}$ implies $p(z_\mu) = \mathrm{NF}_{\mathcal{I}}[p](z_\mu)$. □

Thus, if a normal form computation mod $\mathcal{I}$ follows *after* the computation of the zeros of $\mathcal{I}$ so that the zeros z_μ and the matrix X of the joint eigenvectors of the A_σ are available, the coefficients $\mathbf{c}^T(p)$ of the normal form of a polynomial p may also be computed from the linear system

$$\mathbf{c}^T(p)\, X \;=\; (\, p(z_1) \ldots p(z_m)\,)\,. \tag{8.15}$$

Multiple zeros require the usual modification; cf. section 8.5. Note that the cost of this approach does not depend on the $\mathcal{N}$-index of p but on the cost of the evaluations of p. The cost of solving (8.15) is $\mathrm{O}(m^3)$; this cost may be reduced by the use of recursive interpolation algorithms (cf. section 9.6).

Example 8.7: We consider the ideal $\mathcal{I}$ of Example 8.2, specified by the normal set $\mathcal{N} = \{1, x, y, z\}$ and the multiplication matrices A_1, A_2, A_3. We wish to find the normal form of the polynomial $p(x, y, z) = x^4 - x^2yz + 3x^2y + 2x^2z - xyz$. The hull sets are $H_\ell[\mathcal{N}] = \{\text{monomials in } x, y, z \text{ of total degree} \le \ell + 1\}$. Thus, p has $\mathcal{N}$-index 3 and the two $\mathcal{N}$-leading terms x^4 and $-x^2yz$.

When we use (8.13) to compute the normal form, we may compose $\mathbf{c}^T(p)$ from the nontrivial rows $a^T_{x^j} := \mathbf{c}^T(x^j)$ in the A_σ as

$$a^T_{x^2}\, A_1^2 + a^T_{xy}\, A_1\, (-A_3 + 3\, I) + 2\, a^T_{xz}\, A_1 - a^T_{xz}\, A_2\;;$$

the only economization possible is in the computation for the second and third term of p. With the values from Example 8.2, we obtain

$$\mathrm{NF}_{\mathcal{I}}[p] \;=\; 1 + \tfrac{24}{7}\, x + \tfrac{9}{7}\, y - \tfrac{1}{7}\, z\;.$$

When we use (8.14), we may at first reduce the monomials x^4 and x^2yz by $x^2\, bb_{x^2}$ and $x^2\, bb_{yz}$, resp., where bb_{x^j} denotes the border basis element with $\mathcal{N}$-leading term x^j; this generates polynomials with monomials $x^3,\ x^2y,\ x^2z,\ x^2$. The first three terms, together with the remaining

terms of p, may be reduced by x-multiples of bb_{x^2}, bb_{xy}, bb_{xz}, bb_{yz}, respectively. Now we have arrived at polynomials which contain only terms with monomials from $B[\mathcal{N}]$ or $\mathcal{N}$ itself. The final expression is, of course, the same as above.

The values of p at the zeros in Z are, in the order of the zeros in Example 8.2, 7, -5, 8, 0. The linear system of (8.15) becomes

$$(c_1(p),\, c_2(p),\, c_3(p),\, c_4(p)) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 2 & 0 \\ 1 & -2 & 0 & -1 \\ 0 & 0 & -1 & -2 \end{pmatrix} = (7,\, -5,\, 8,\, 0)$$

which yields directly the normal form coefficients as above. □

For various purposes it is desirable to find not only the normal form $\mathrm{NF}_{\mathcal{I}}[p]$ but a full "expansion" of $p \in \mathcal{P}^s$ in terms of the border basis $\mathcal{B}_{\mathcal{N}}$:

$$p(x) \;=\; \mathrm{NF}[p] + \sum_{x^j \in B[\mathcal{N}]} q_j(x)\, bb_j(x)\,; \tag{8.16}$$

such representations exist since $p - \mathrm{NF}[p] \in \mathcal{I}$. Equation (8.16) is a generalization of the representation (5.16) in the univariate case. The sum in (8.16) cannot be unique in general because of the arbitrariness in the reduction of p to its (unique) normal form.

To determine one particular set of q_j, one has to follow a path of the reduction $p \xrightarrow{\mathcal{B}} \mathrm{NF}[p]$. If the reduction proceeds by subtraction of multiples of the bb_j's, then one simply has to accumulate these multiples over the reduction; cf. (8.14). When the normal form has been formed as $e_1^T\, p(A)\, \mathbf{b}$ (cf. (8.13)), we can extend this representation in the following way:

With $\mathbf{bb} := (bb_1, \ldots, bb_N)^T$, we have—as relations in $\mathcal{P}^s$—

$$x_\sigma \cdot \mathbf{b}(x) \;=\; A_\sigma\, \mathbf{b}(x) + B_\sigma\, \mathbf{bb}(x)\,, \quad \sigma = 1(1)s, \tag{8.17}$$

where $B_\sigma \in \{0,1\}^{m \times N}$ has μ-th rows of zeros for $x_\sigma b_\mu(x) \in \mathcal{N}$ and a 1 in the j-th position for $x_\sigma b_\mu(x) = x^j \in B[\mathcal{N}]$. Equation (8.17) may now be extended recursively: Let

$$x^k \cdot \mathbf{b}(x) \;=\; A^k\, \mathbf{b}(x) + B^k(x)\, \mathbf{bb}(x)\,;$$

then

$$x_\sigma x^k \cdot \mathbf{b}(x) \;=\; A_\sigma\, [A^k\, \mathbf{b}(x) + B^k(x)\, \mathbf{bb}(x)] + B_\sigma\, x^k\, \mathbf{bb}(x)\,.$$

Thus, the $B^k(x)$ matrices have to follow the recursion

$$B^{k+e_\sigma}(x) \;:=\; A_\sigma\, B^k(x) + x^k\, B_\sigma\,. \tag{8.18}$$

With this recursion, we may turn the equivalence

$$p(x) \cdot \mathbf{b}(x) \;=\; (\sum_k \alpha_k x^k) \cdot \mathbf{b}(x) \;\equiv\; (\sum_k \alpha_k A^k)\, \mathbf{b}(x) \mod \mathcal{I}$$

into the equation in $\mathcal{P}^s$

$$p(x) \cdot \mathbf{b}(x) \;=\; \sum_k \alpha_k\, (A^k\, \mathbf{b}(x) + B^k(x)\, \mathbf{bb}(x)) \qquad \text{or}$$

$$\begin{aligned} p(x) &= p(x)\, e_1^T \mathbf{b}(x) \\ &= \textstyle\sum_k \alpha_k \,(e_1^T A^k\, \mathbf{b}(x) + e_1^T B^k(x)\, \mathbf{bb}(x)) \;=\; \mathrm{NF}[p] + \sum_{x^j \in B[\mathcal{N}]} q_j(x)\, bb_j(x)\,. \end{aligned} \tag{8.19}$$

Example 8.7, continued: For the normal set, the multiplication matrices and the border basis of Example 8.2, we have the matrices

$$B_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

With an iterated application of (8.18), we obtain the first rows b_k of the B^k, $k \in \mathbb{N}_0^3$; e.g.,

$$\begin{aligned} b_{4,0,0} &= (x^2 + 2\,x + \tfrac{31}{7},\; -x - \tfrac{12}{7},\; x + \tfrac{6}{7},\; 0,\; 0,\; 0)\,, \\ b_{2,1,1} &= (-\tfrac{4}{7}\,x,\; \tfrac{2}{7}\,x,\; -\tfrac{8}{7}\,x,\; 0,\; x^2,\; 0) \\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{etc.} \end{aligned}$$

Then (8.19) yields, with the normal form found previously,

$$\begin{aligned} p(x) \;=\;& (1 + \tfrac{24}{7}\,x + \tfrac{9}{7}\,y - \tfrac{1}{7}\,z) \\ & + (1 + \tfrac{18}{7}\,x + x^2)\, bb_1(x) + \tfrac{12}{7}\,x\, bb_2(x) + (4 + \tfrac{29}{7}\,x)\, bb_3(x) + (-x^2 - x)\, bb_5(x)\,. \;\square \end{aligned}$$

8.2.2 The Syzygies of a Border Basis

The row vectors $a_j^T \in \mathbb{C}^m$, $x^j \in B[\mathcal{N}]$, which define a normal set representation of $\mathcal{I}$ determine the nontrivial rows of the $m \times m$ matrices A_σ as well as the border basis elements $bb_j(x)$. Therefore, the commutativity conditions (8.8) on the A_σ must also be representable in terms of the border basis elements bb_k. Let $\mathbf{b}(x) = (b_\mu(x))^T = (x^{j_1}, \ldots, x^{j_m})^T$ be the normal set vector for $\mathcal{N}$; for the present purpose, we denote the μth row of A_σ by $a_{\sigma\mu}^T$; iff $x^j = x_\sigma\, b_\mu(x) \in B[\mathcal{N}]$ then $a_{\sigma\mu}^T = a_j^T$ is nontrivial.

Definition 8.4. The *boundary set* $\partial\mathcal{N}$ of a closed monomial set $\mathcal{N} \subset \mathcal{T}^s$ is defined by (cf. Definition 2.17)

$$\partial\mathcal{N} \;:=\; \{\, x^j \in \mathcal{N} \;:\; \text{At least one positive neighbor of } x^j \text{ is in } B[\mathcal{N}]\,\}\,. \quad \square \tag{8.20}$$

Definition 8.5. For a closed monomial set $\mathcal{N} \subset \mathcal{T}^s$, $|\mathcal{N}| = m$, with boundary set $\partial\mathcal{N} = \{b_\mu\}$, $|\partial\mathcal{N}| =: \bar{m} \le m\}$, we consider the following *edges* $e_{\mu\sigma_1\sigma_2} = [x^{j_1}, x^{j_2}]$ between the N monomials of $B[\mathcal{N}]$: For each triple $(\mu, \sigma_1, \sigma_2)$, $b_\mu \in \partial\mathcal{N}$, $\sigma_1 \neq \sigma_2 \in \{1, .., s\}$,
(i) if $x_{\sigma_1} b_\mu \in B[\mathcal{N}]$, $x_{\sigma_2} b_\mu \notin B[\mathcal{N}]$,

$$e_{\mu\sigma_1\sigma_2} \;:=\; [x_{\sigma_1}\, b_\mu,\; x_{\sigma_1} x_{\sigma_2}\, b_\mu]\,, \tag{8.21}$$

(ii) if $x_{\sigma_1} b_\mu,\ x_{\sigma_2} b_\mu \in B[\mathcal{N}]$,

$$e_{\mu\sigma_1\sigma_2} \ := \ [x_{\sigma_1} b_\mu, x_{\sigma_2} b_\mu]\,, \tag{8.22}$$

(iii) if $x_{\sigma_1} b_\mu,\ x_{\sigma_2} b_\mu \notin B[\mathcal{N}]$: $\quad e_{\mu\sigma_1\sigma_2}$ not defined.

The *border web* $BW_{\mathcal{N}}$ of $\mathcal{N}$ is the set of all edges $e_{\mu\sigma_1\sigma_2}$ in $B[\mathcal{N}]$. Obviously, $\bar{N} := |BW_{\mathcal{N}}| \le \bar{m}\,\frac{s(s-1)}{2}$. $\square$

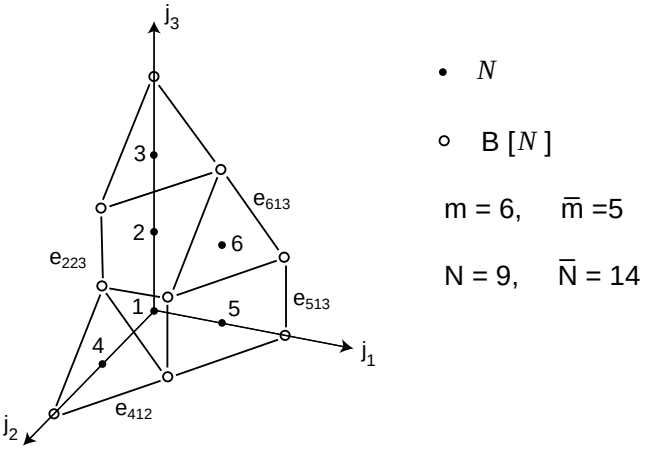

Figure 8.2.

Proposition 8.10. For a normal set $\mathcal{N} \subset \mathcal{T}^s$, consider the set of N nontrivial row vectors $a^T_{\sigma\mu} \in \mathbb{C}^m$ which define the potential multiplication matrices A_σ, $\sigma = 1(1)s$, for a ring $\mathcal{R} =$ span $\mathcal{N}$. The A_σ *commute* iff their trivial rows have been set properly and the following conditions hold (cf. Figure 8.2):

- for each $e_{\mu\sigma_1\sigma_2} \in BW_{\mathcal{N}}$ of type (i), where $a^T_{\sigma_2\mu} = e^T_{\bar{\mu}}$ is a trivial row in A_{σ_2} but $x_{\sigma_1} b_{\bar{\mu}}(x) = x_{\sigma_2} x_{\sigma_1} b_\mu(x)$ is in $B[\mathcal{N}]$:

$$a^T_{\sigma_1\bar{\mu}} \ = \ e^T_{\bar{\mu}} A_{\sigma_1} \ = \ e^T_\mu A_{\sigma_2} A_{\sigma_1} \ = \ e^T_\mu A_{\sigma_1} A_{\sigma_2} \ = \ a^T_{\sigma_1\mu} A_{\sigma_2}\,. \tag{8.23}$$

- for each $e_{\mu\sigma_1\sigma_2} \in BW_{\mathcal{N}}$ of type (ii), with both $a^T_{\sigma_i\mu}$ nontrivials rows of A_{σ_i}:

$$a^T_{\sigma_2\mu} A_{\sigma_1} \ = \ e^T_\mu A_{\sigma_2} A_{\sigma_1} \ = \ e^T_\mu A_{\sigma_1} A_{\sigma_2} \ = \ a^T_{\sigma_1\mu} A_{\sigma_2}\,. \tag{8.24}$$

Proof: For fixed σ_1, σ_2, the condition determined by $e_{\mu\sigma_1\sigma_2}$ implies that the μth row of $A_{\sigma_1} A_{\sigma_2} - A_{\sigma_2} A_{\sigma_1}$ vanishes. $\square$

Let $\mathcal{S}$ be the set of all equations (8.23) and (8.24). For each triple $(\mu, \sigma_1, \sigma_2)$ which occurs in an equation of $\mathcal{S}$, we consider the monomial $x_{\sigma_1} x_{\sigma_2} b_\mu$; cf. Figure 8.2. In case (i), with $x_{\sigma_2} b_\mu =: b_{\bar{\mu}}$, we consider the two border basis elements $bb_{\bar{k}}$, with leading term $x_{\sigma_1} b_{\bar{\mu}}$, and bb_k, with leading term $x_{\sigma_1} b_\mu$, and form

$$\begin{aligned} bb_{\bar{k}}(x) - x_{\sigma_2} bb_k(x) \ &= \ (x_{\sigma_1} b_{\bar{\mu}}(x) - a^T_{\sigma_1\bar{\mu}} \mathbf{b}(x)) - (x_{\sigma_2} x_{\sigma_1} b_\mu(x) - x_{\sigma_2} a^T_{\sigma_1\mu} \mathbf{b}(x)) \\ &= \ -\,(a^T_{\sigma_1\bar{\mu}} - a^T_{\sigma_1\mu} x_{\sigma_2})\, \mathbf{b}(x)\,. \end{aligned}$$

Some components of $x_{\sigma_2}\mathbf{b}(x)$ are in $B[\mathcal{N}]$; with the aid of border basis elements, they may be reduced to the components of $A_{\sigma_2}\mathbf{b}(x) \in \mathcal{N}$. Thus,

$$a^T_{\sigma_1\bar{\mu}} - a^T_{\sigma_1\mu} A_{\sigma_2} = 0 \qquad \Longleftrightarrow \qquad bb_{\bar{k}}(x) - x_{\sigma_2} bb_k(x) \xrightarrow{\mathcal{B}} 0\,. \tag{8.25}$$

In case (ii), we consider the two border basis elements bb_{k_1}, with leading term $x_{\sigma_1} b_\mu$, and bb_{k_2}, with leading term $x_{\sigma_2} b_\mu$, and form

$$\begin{aligned} x_{\sigma_1} bb_{k_2}(x) - x_{\sigma_2} bb_{k_1}(x) &= (x_{\sigma_1} x_{\sigma_2} b_\mu(x) - x_{\sigma_1} a^T_{\sigma_2\mu}\mathbf{b}(x)) - (x_{\sigma_2} x_{\sigma_1} b_\mu(x) - x_{\sigma_2} a^T_{\sigma_1\mu}\mathbf{b}(x)) \\ &= -(a^T_{\sigma_2\mu} x_{\sigma_1} - a^T_{\sigma_1\mu} x_{\sigma_2})\,\mathbf{b}(x)\,. \end{aligned}$$

Again, we can reduce the right-hand side with border basis elements to components in $\mathcal{N}$ and obtain

$$a^T_{\sigma_2\mu} A_{\sigma_1} - a^T_{\sigma_1\mu} A_{\sigma_2} = 0 \qquad \Longleftrightarrow \qquad x_{\sigma_1} bb_{k_2}(x) - x_{\sigma_2} bb_{k_1}(x) \xrightarrow{\mathcal{B}} 0\,. \tag{8.26}$$

Above (cf. (8.23) and (8.24)), we have found that the left-hand sides of (8.25) and (8.26) are equivalent to the commutativity of the A_σ matrices. Now, we have found that the same relations are equivalent to the fact that certain polynomial combinations of the border basis elements can be reduced, by subtraction of suitable elements from the border basis set $\mathcal{B}$, to the zero polynomial. Thus, the right-hand sides in (8.25) and (8.26), formed over all triples $(\mu, \sigma_1, \sigma_2)$ described above, are equivalent to the commutativity of the A_σ.

All these right-hand sides combine two "neighboring" border basis elements in a way which implies the cancellation of the $\mathcal{N}$-leading term of the combination.

Definition 8.6. Consider a set $\mathcal{B}$ of polynomials in $\mathcal{P}^s$ for which leading monomials are defined. Take two polynomials $p_1, p_2 \in \mathcal{B}$, with leading monomials x^{j_1}, x^{j_2}; their least common multiple is $x^k := \text{l.c.m.}(x^{j_1}, x^{j_2}) = x^{k-j_1} x^{j_1} = x^{k-j_2} x^{j_2}$. The S-*polynomial*[12] of p_1, p_2 is

$$S[p_1, p_2] := l.c.(p_2)\, x^{k-j_1} p_1(x) - l.c.(p_1)\, x^{k-j_2} p_2(x)\,, \tag{8.27}$$

where $l.c.$ denotes the $\mathcal{N}$-leading coefficient. □

Note that $S[p_2, p_1] = -S[p_1, p_2]$ so that, in most contexts, the order of the arguments does not matter.

Theorem 8.11. In the situation described at the beginning of this section, the following facts are equivalent:

- The multiplication matrices A_σ which represent the multiplicative structure of $\mathcal{R}$ with respect to the normal set basis $\mathbf{b}$ commute.

- All S-polynomials formed for neighboring elements $bb_k(x)$ of the border basis $\mathcal{B}$ may be reduced to 0 by polynomials from $\mathcal{B}$.

- The S-polynomials formed for *any* two elements of the border basis $\mathcal{B}$ may be reduced to 0 by polynomials from $\mathcal{B}$.

Proof: It remains only to show that the 2nd fact implies the 3rd one. Consider $bb_k, bb_\ell \in \mathcal{B}$ with leading terms x^k, x^ℓ, resp., and their least common multiple $x^K := \text{l.c.m.}(x^k, x^\ell) = x^{K-k} x^k =$

[12] This terminology has been introduced by B. Buchberger in his thesis; the S in S-polynomial refers to syzygy.

$x^{K-\ell}\,x^{\ell}$. The S-polynomial of bb_k, bb_ℓ is $S[bb_k, bb_\ell] = x^{K-k}\,bb_k(x) - x^{K-\ell}\,bb_\ell(x)$. Due to the closedness of a normal set, there must be a chain of monomials $x^{k_\nu} \in B[\mathcal{N}],\ \nu = 0, 1, \ldots, n$, such that $k_0 = k,\ k_n = \ell$, and $x^{k_{\nu+1}}$ and x^{k_ν} are "neighboring monomials" in $B[\mathcal{N}]$ which means that they satisfy one of the following two relations:

(i) $\exists\, x_\sigma:\qquad x^{\kappa} = x_\sigma\, x^{\kappa'}\quad$ or $\quad x^{\kappa'} = x_\sigma\, x^{\kappa}$,

(ii) $\exists\, x_{\sigma_1}, x_{\sigma_2}:\ x_{\sigma_2}\, x^{\kappa} = x_{\sigma_1}\, x^{\kappa'}$,

where the monomial in the equation is a divisor of x^K. Thus, by the chain, we may compose the relation $x^{K-k}\,x^k = x^{K-\ell}\,x^\ell$ by a sum of x^j-multiples of the relations for neighboring monomials. Accordingly, we may compose the S-polynomial of bb_k, bb_ℓ by a sum of multiples of S-polynomials of neighboring border basis elements. Since each of these may be reduced to 0 by $\mathcal{B}$, this is also true for the sum. □

Corollary 8.12. Consider a set $\mathcal{N} \in \mathcal{T}^s(m)$ and a polynomial set $\mathcal{B} = \{bb_j\} \subset \mathcal{P}^s,\ |\mathcal{B}| = |B[\mathcal{N}]|$, where each $bb_j \in \mathcal{B}$ has its support in $\mathcal{N} \cup B[\mathcal{N}]$, with only one monomial $x^j \in B[\mathcal{N}]$. Iff the S-polynomials of any two polynomials in $\mathcal{B}$ may be reduced to 0 by polynomials from $\mathcal{B}$, then $\mathcal{B}$ generates an ideal $\langle\mathcal{B}\rangle \subset \mathcal{P}^s(m)$, with normal set $\mathcal{N}$.

Proof: Compare Theorems 8.1, 8.3, and 8.11. □

Example 8.8: We take the situation in Example 8.2, with $\mathcal{N} = \{1, x, y, z\},\ \partial\mathcal{N} = \{x, y, z\}$, and $B[\mathcal{N}] = \{x^2, xy, xz, y^2, yz, z^2\}$ and 9 edges in $BW_{\mathcal{N}}$. All edges are of type (ii); the corresponding 9 commutativity relations (8.24) for the multiplication matrices are

$$a^T_{\sigma_2\mu}\,A_{\sigma_1} = a^T_{\sigma_1\mu}\,A_{\sigma_2}\,, \qquad \mu = 2(1)4\,, \quad \sigma_1 \neq \sigma_2 \in \{1, 2, 3\}\,.$$

For the triple $\mu = 2,\ \sigma_1 = 2,\ \sigma_2 = 1$, e.g., we have $a^T_{12}\,A_2 = a^T_{22}\,A_1$ or

$$(1,\ 2,\ -1,\ 1)\begin{pmatrix} 0 & 0 & 1 & 0 \\ 2 & \frac{-4}{7} & \frac{2}{7} & \frac{6}{7} \\ 4 & \frac{-10}{7} & \frac{5}{7} & \frac{8}{7} \\ 0 & \frac{-4}{7} & \frac{2}{7} & \frac{-8}{7} \end{pmatrix} = (2,\ \tfrac{-4}{7},\ \tfrac{2}{7},\ \tfrac{6}{7})\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 2 & -1 & 1 \\ 2 & \frac{-4}{7} & \frac{2}{7} & \frac{6}{7} \\ 0 & \frac{-8}{7} & \frac{4}{7} & \frac{-2}{7} \end{pmatrix}$$
$$= (0,\ \tfrac{-2}{7},\ \tfrac{8}{7},\ \tfrac{-4}{7})\,;$$

for $\mu = 4,\ \sigma_1 = 2,\ \sigma_2 = 1$, we have $a^T_{14}\,A_2 = a^T_{24}\,A_1$ or

$$(0,\ \tfrac{-8}{7},\ \tfrac{4}{7},\ \tfrac{-2}{7})\,A_2 \;=\; (0,\ 0,\ \tfrac{3}{7},\ \tfrac{8}{7}) \;=\; (0,\ \tfrac{-4}{7},\ \tfrac{2}{7},\ \tfrac{-8}{7})\,A_1\,.$$

Correspondingly, there are 9 reduction relations (8.26) for the 6 border basis elements bb_κ of Example 8.2. For the triple (1,2,1), we have

$$\begin{aligned} S[bb_1, bb_2] &= y\,bb_1(x, y, z) - x\,bb_2(x, y, z) \\ &= y\,(x^2 - (2x - y + z + 1)) - x\,(xy - (-4x + 2y + 6z + 14)/7) \\ &= (-4x^2 - 12xy + 6xz + 7y^2 - 7yz + 14x - 7y)/7 \end{aligned}$$

which is reduced to 0 by subtraction of $\frac{-4}{7}\,bb_1 - \frac{12}{7}\,bb_2 + \frac{6}{7}\,bb_3 + bb_4 - bb_5$. Similarly, $y\,bb_3(x, y, z) - x\,bb_5(x, y, z) = (-\frac{4}{7}x^2 + \frac{10}{7}xy - \frac{8}{7}xz - \frac{4}{7}y^2 + \frac{2}{7}yz)$ reduces to 0 by subtraction of the border basis polynomials with the respective leading terms.

For non-neighboring border basis elements, e.g., bb_1 and bb_6 with leading terms x^2 and z^2, resp., we may use the chain $(x^2, xz),\ (xz,\ z^2)$ to obtain

$$S[bb_1, bb_6] \ = \ z^2\, bb_1(x, y, z) - x^2\, bb_6(x, y, z) \ = \ z\,(z\, bb_1 - x\, bb_3) + x\,(z\, bb_3 - x\, bb_6) \ = \ 0$$

by (8.26).

If we had been presented with the 6 polynomials bb_κ of Example 8.2, without further information, we could have chosen the set $\mathcal{N}$ as $\{1, x, y, z\}$ to conform with Corollary 8.12. We could then have formed the 9 reduction relations (8.26) and verified the reduction to 0. This would have told us that the bb_κ generate an ideal $\mathcal{I}$ with 4 zeros. From the bb_κ, we could have formed the multiplication matrices A_σ of $\mathcal{R}[\mathcal{I}]$ and computed the zeros. □

Theorem 8.11 shows that the elements $bb_j(x)$ of a border basis $\mathcal{B}$ of a polynomial ideal $\mathcal{I} \subset \mathcal{P}^s$ satisfy a multitude of identities: Assume (for notational simplicity) that the elements $b_{\bar{\mu}}$ through b_m are in $\partial\mathcal{N}$ and have an x_1-neighbor in $B[\mathcal{N}]$. When we spell out the reduction $x_1\,\mathbf{b}(x) \ \xrightarrow{\mathcal{B}}\ A_1\,\mathbf{b}(x)$, we obtain—as a relation in $\mathcal{P}^s$—

$$x_1\,\mathbf{b}(x) \ = \ A_1\,\mathbf{b}(x) + (0, \ldots, 0, bb_{k_{\bar{\mu}}}(x), \ldots, bb_{k_m}(x))^T\,, \tag{8.28}$$

where bb_{k_μ} is the border basis element with leading term $x_1 b_\mu(x)$; such relations hold for all x_σ-multiples of $\mathbf{b}$. Thus, (8.26) implies, e.g.,

$$\begin{aligned} x_{\sigma_1} bb_{k_2}(x) - x_{\sigma_2} bb_{k_1}(x) \ &= \ (a^T_{\sigma_2\mu} x_{\sigma_1} - a_{\sigma_1\mu} x_{\sigma_2})\,\mathbf{b}(x) \\ &= \ (a^T_{\sigma_2\mu} A_{\sigma_1} - a_{\sigma_1\mu} A_{\sigma_2})\,\mathbf{b}(x) + a^T_{\sigma_2\mu}\mathbf{bb}_{\sigma_1}(x) - a^T_{\sigma_1\mu}\mathbf{bb}_{\sigma_2}(x)\,, \end{aligned}$$

where $\mathbf{bb}_\sigma(x)$ is the m-vector of zeros and bb_j's arising from the reduction of $x_\sigma\mathbf{b}(x)$; cf. (8.28). Since the first member of the right-hand side vanishes for commuting A_σ, we have the identity in $\mathcal{P}^s$

$$x_{\sigma_1} bb_{k_2}(x) - x_{\sigma_2} bb_{k_1}(x) - a^T_{\sigma_2\mu}\mathbf{bb}_{\sigma_1}(x) + a^T_{\sigma_1\mu}\mathbf{bb}_{\sigma_2}(x) \ = \ 0\,, \tag{8.29}$$

which must be satisfied by the border basis elements if they are to be consistent and define a nontrivial 0-dimensional ideal. Similar identities arise from the relations (8.25).

These nontrivial syzygies (cf. Definition 2.3) of the border basis $\mathcal{B}$ of a 0-dimensional ideal $\mathcal{I}$ represent nontrivial representations of the 0-polyomial by the bb_k; they show that the bb_k are not independent. This was, of course, to be expected since they possess N s coefficients while $\mathcal{I}$ is determined by m s data in $\mathbb{C}^s$. Because of these syzygies, we cannot expect uniqueness in the representation (8.16) of a polynomial $p \in \mathcal{P}^s$ as we may add arbitrary multiples of a syzygy (8.29) to it.

The set of all syzygies of a border basis is a linear space with an algebraic structure (a "module") and can be generated from a basis; but we will not make use of this structure in a formal way. *Trivial* syzygies $\sum_\nu q_\nu p_\nu = 0$, with $q_\nu \in \langle\{p_\nu\}\rangle$, exist in any polynomial system $\{p_\nu\}$, e.g., $p_{\nu_2}\, p_{\nu_1} - p_{\nu_1}\, p_{\nu_2} = 0$.

Example 8.8, continued: We may rewrite the reductions, e.g., the ones displayed above, into the syzygies $y\, bb_1 - x\, bb_2 = \frac{-4}{7}\, bb_1 - \frac{12}{7}\, bb_2 + \frac{6}{7}\, bb_3 + bb_4 - bb_5$ or

$$(y+\tfrac{4}{7})\, bb_1(x, y, z) + (-x+\tfrac{12}{7})\, bb_2(x, y, z) - \tfrac{6}{7}\, bb_3(x, y, z) - bb_4(x, y, z) + bb_5(x, y, z) \ = \ 0\,,$$

and $y\, bb_3 - x\, bb_5 \ = \ \frac{-4}{7}\, bb_1 + \frac{10}{7}\, bb_2 - \frac{8}{7}\, bb_3 - \frac{4}{7}\, bb_4 + \frac{2}{7}\, bb_5$ or

$$\tfrac{4}{7}\, bb_1(x, y, z) - \tfrac{10}{7}\, bb_2(x, y, z) + (y+\tfrac{8}{7})\, bb_3(x, y, z) + \tfrac{4}{7}\, bb_4(x, y, z) - (x+\tfrac{2}{7})\, bb_5(x, y, z) \ = \ 0\,.$$

8.2.3 Admissible Data for a Normal Set Representation

At the end of section 8.1.2, we observed that *computed* multiplication matrices will generally not commute exactly. Corollary 8.12 expresses the same dilemma in terms of border bases: In a *computed* border basis, the S-polynomials will generally not reduce to 0 exactly. Let us take another look at this situation:

When we fix a (feasible) normal set $\mathcal{N} \in \mathcal{T}^s(m)$ for the representation of an ideal $\mathcal{I} \in \mathcal{P}^s(m)$, the data of the normal set representation of $\mathcal{I}$ consist of the N row vectors $a_j^T \in \mathbb{C}^m$, $x^j \in B[\mathcal{N}]$; cf. the beginning of section 8.2. As we have seen in section 8.2.2, the a_j^T cannot take arbitrary values but must satisfy the relations (8.23) and (8.24) or (8.25) and (8.26), resp., which are quadratic polynomials in the components of the a_j^T. Thus they define an algebraic manifold in the data space $\mathcal{A} = \mathbb{C}^{Nm}$ of the a_j^T.

Definition 8.7. For a normal set representation with normal set $\mathcal{N} \in \mathcal{T}^s(m)$, the algebraic manifold

$$\mathcal{M}_\mathcal{N} := \{\, a_j^T \in \mathbb{C}^m \text{ satisfying the commutativity constraints in Proposition 8.10} \,\} \subset \mathcal{A} \tag{8.30}$$

is the *admissible-data manifold* of $\mathcal{N}$. A set of $N = |B[\mathcal{N}]|$ vectors $a_j^T \in \mathbb{C}^m$ specifies an ideal $\mathcal{I} \in \mathcal{P}^s(m)$ iff $\{a_j^T\} \in \mathcal{M}_\mathcal{N}$. □

Proposition 8.13. The admissible-data manifold $\mathcal{M}_\mathcal{N}$ has dimension $m\,s$.

Proof: Take a zero set $Z \subset (\mathbb{C}^s)^m$ of m disjoint zeros $z_\mu \in \mathbb{C}^s$ and consider the nontrivial row vectors a_j^T in the A_σ matrices generated (for $\mathcal{N}$) by (8.1) so that the $m \times m$ matrix $\mathbf{b}(\mathbf{z})$ is the normalized joint eigenvector matrix of the commuting matrix family $\overline{A}$ generated by the A_σ. Since $\mathbf{b}(\mathbf{z})$ is regular, (8.1) defines a *bijective* mapping between a full ms-dimensional neighborhood of Z and the associated neighborhood of the nontrivial rows of the A_σ on $\mathcal{M}_\mathcal{N}$. Thus $\mathcal{M}_\mathcal{N}$ is ms-dimensional at all of its points which correspond to a set of m disjoint zeros. The situation at a point which corresponds to a zero set with some multiple zero will be analyzed in section 9.3. □

The *codimension* of $\mathcal{M}_\mathcal{N}$ in $\mathcal{A} = \mathbb{C}^{Nm}$ is positive except when either s or m is 1: A univariate polynomial is its own border basis and all coefficient values are admissible. For $\mathcal{I} \in \mathcal{P}^s(1), \mathcal{N} = \{1\}$ is the only possible normal set and the s values $a_j^T \in \mathbb{C}^1$ are the components of the only zero z. In all other cases, we have $N > s$ and $\operatorname{codim} \mathcal{M}_\mathcal{N} = (N - s)\,m > 0$. However,[13] at least for $s > 2$, the set $\mathcal{S}$ of relations (8.23) and (8.24) in Proposition 8.10 which expresses the commutativity constraints defining the admissible-data manifold $\mathcal{M}_\mathcal{N}$, contains $\bar{N} := |B W_\mathcal{N}| > N - s$ equations. Thus $\mathcal{S}$ constitutes a consistent *overdetermined* representation of $\mathcal{M}_\mathcal{N}$. In Example 8.8, e.g., we have $N - s = 3$ but $\bar{N} = 9$.

This is an unfortunate situation for computational purposes: Assume that, from a representation $(\mathcal{N}, \{\tilde{a}_j\})$, we wish to reach a proper neighboring representation $(\mathcal{N}, \{a_j\})$, with $a_j^T = \tilde{a}_j^T + \Delta a_j^T$ and small modifications Δa_j^T; the Δa_j^T are to be found by a Newton step applied to the equations for some requested property and for the position on $\mathcal{M}_\mathcal{N}$. Thus we need the Jacobian of the system $\mathcal{S}$ at the $\tilde{a}_j$; because of the quadratic character of $\mathcal{S}$, the elements of this matrix contain the $\tilde{a}_j^T$. In a computational situation, their values carry round-off errors

[13] The nontypical situation for $s = 2$ variables is discussed in Exercise 8.2-5.

(or worse) which raise the rank of the Jacobian above its theoretical value $N - s$; this may lead to serious computational difficulties. Therefore, we must attempt to specify a subset $\mathcal{S}_0$ of $\mathcal{S}$, with $\bar{N}_0 = N - s$ relations, which defines the admissible-data manifold $\mathcal{M}_{\mathcal{N}}$ *without overdetermination*. Fortunately, there are some well-known rules which permit a reduction of the set $\mathcal{S}$:

Proposition 8.14. Consider a system $\mathcal{S}$ of edge conditions of type (8.25) and (8.26) on the border web $BW_{\mathcal{N}}$ of a normal set $\mathcal{N}$.

(a) Consider three monomials $x^{k_j} \in B[\mathcal{N}]$, $j = 1(1)3$, and let $x^{k_{j_1 j_2}}$ be the least common multiples (l.c.m.) of $x^{k_{j_1}}$ and $x^{k_{j_2}}$. Assume that $x^{k_{12}}$ and $x^{k_{23}}$ divide $x^{k_{13}}$. Then the condition on the edge $[x^{k_1}, x^{k_3}]$ follows from those on $[x^{k_1}, x^{k_2}]$ and $[x^{k_2}, x^{k_3}]$.

(b) Consider two monomials $x^{k_1}, x^{k_2} \in B[\mathcal{N}]$ which are *coprime*, i.e. l.c.m.$(x^{k_1}, x^{k_2}) = x^{k_1} x^{k_2}$. Then the S-polynomial $S[bb_{k_1}, bb_{k_2}]$ reduces to 0 with $\{bb_{k_1}, bb_{k_2}\}$.

Proof:

(a)
$$x^{k_{13}-k_1} bb_{k_1} - x^{k_{13}-k_3} bb_{k_3} = \\ (x^{k_{12}-k_1} bb_{k_1} - x^{k_{12}-k_2} bb_{k_2})\, x^{k_{13}-k_{12}} + (x^{k_{23}-k_2} bb_{k_2} - x^{k_{23}-k_3} bb_{k_3})\, x^{k_{13}-k_{23}}\,.$$

(b)
$$\begin{aligned} S[bb_{k_1}, bb_{k_2}] &= x^{k_2} \cdot (x^{k_1} - a_{k_1}^T \mathbf{b}(x)) - x^{k_1} \cdot (x^{k_2} - a_{k_2}^T \mathbf{b}(x)) \\ &= -(x^{k_2} - a_{k_2}^T \mathbf{b}(x))\, a_{k_1}^T \mathbf{b}(x) + (x^{k_1} - a_{k_1}^T \mathbf{b}(x))\, a_{k_2}^T \mathbf{b}(x). \end{aligned}$$

□

It is obvious that part (a) of Proposition 8.14 can be extended to the case where some edge $[x^{k_1}, x^{k_r}]$ closes a longer "chain" of edges $[x^{k_j}, x^{k_{j+1}}]$, $j = 1(1)r - 1$, if all l.c.m.$(x^{k_j}, x^{k_{j+1}})$ divide l.c.m.(x^{k_1}, x^{k_r}). This permits the elimination of various conditions on edges which "close a circle" in $BW_{\mathcal{N}}$. However, the assumption on the l.c.m. of the chained edges is rather restrictive. If this assumption is not met, the chain relation will only lead to a representation of some monomial multiple of the relation for the closing edge in terms of the relations on the edges of the chain; this happens because we must multiply the relation in the proof above by a monomial x^{ℓ} which makes $x^{k_{1r}} x^{\ell}$ a multiple of all the l.c.m.$(x^{k_j}, x^{k_{j+1}})$.

In terms of multiplication matrices, this implies only $(a_{k_1}^T A^{k_{1r}-k_1} - a_{k_r}^T A^{k_{1r}-k_r})\, A^{\ell} = 0$, which yields the relation (8.24) for the closing edge only if A^{ℓ} is regular. In terms of zeros of the underlying ideal, this means that none of the zeros must have a vanishing x_λ component for λ a nonvanishing component of ℓ. But the zero sets $Z^s(m)$ which do not meet this condition comprise a low-dimensional subset of the $\mathbb{C}^{sm}$ which parametrizes the admissible-data-manifold $\mathcal{M}_{\mathcal{N}}$. Therefore, the commutativity relation on the closing edge is a consequence of the relations along the chain *almost everywhere* on $\mathcal{M}_{\mathcal{N}}$; hence it must be an *algebraic* consequence of these relations. By continuity, this algebraic consequence must also hold on the low-dimensional parts of $\mathcal{M}_{\mathcal{N}}$ where it cannot be derived in the above straightforward manner. This implies:

Proposition 8.15. On the border web $WB_{\mathcal{N}}$, conditions of $\mathcal{S}$ on the closing edge of a loop are satisfied if they are satisfied on the remaining edges of the loop.

Thus, one may delete from the web *all* edges which close circles. The remaining web possesses exactly $N - 1$ edges which connect the N monomials in $B[\mathcal{N}]$; it may, e.g., have the form of one continuous thread which proceeds from one monomial to another without any branches. But we must still remove $s - 1$ further edges to arrive at $\bar{N}_0 = N - s$. This is made possible by part (b) of Proposition 8.14 which permits the introduction of "virtual" edges between certain monomials of $BW_{\mathcal{N}}$ along which the relation (8.26) is automatically satisfied.

If such a virtual edge closes a circle on $BW_{\mathcal{N}}$, it permits the elimination of another real edge of the web. For example, we may select one "extremal" monomial (power of one variable) $x_{\sigma'}^{j_{\sigma'}}$; it is connected to the other $s-1$ extremal monomials by virtual edges. This permits the elimination of the $s-1$ edges which previously met these monomials and reduces the number of real edges in $\mathcal{S}$, with active conditions, to $N-s$. Thus we may reach a subset $\mathcal{S}_0$ of $\mathcal{S}$ with the correct number of relations and with each $x^j \in B[\mathcal{N}]$ appearing in at least one relation.

From these arguments and from the evidence in nontrivial—but admittedly not very large—examples, it appears that the relations of such a subset $\mathcal{S}_0$ characterize the admissible-data-manifold $\mathcal{M}_{\mathcal{N}}$ completely and without overdetermination. A rigorous proof of this fact would naturally be highly desirable.

From the practical point of view, an easy way to eliminate many unnecessary relations from $\mathcal{S}$ is given by Proposition 8.4: In a generic situation, it suffices to consider the relations which originate from the commutativity of a fixed multiplication matrix, say A_s, with the remaining matrices A_σ. This eliminates those relations (8.23) and (8.24) where neither σ_1 nor σ_2 equals s. In the remaining web, circles are easier to spot and the elimination of the connections to the extremal points k_σ, $\sigma = 1(1)s-1$, is straightforward.

Example 8.9: Consider $\mathcal{N} = \{1, x_3, x_3^2, x_2, x_1, x_1x_3\}$, with $B[J_{\mathcal{N}}] = \{(0,0,3), (0,1,2), (1,0,2), (1,1,1), (2,0,1), (0,1,1), (0,2,0).(1,1,0), (2,0,0)\}$, $N = 9$, $\overline{N} = 14$; cf. Figure 8.2. The consideration of Proposition 8.4, with $\sigma_3 = 1$, removes the 5 edges $e_{\mu\sigma_1\sigma_2}$ with $\sigma_1\sigma_2 = 23$ and leaves only one closed loop; cf. Figure 8.3. By Proposition 8.15, we can remove (say) e_{413} and replace the edges to the extremal points $(0,2,0)$ and $(0,0,3)$ by virtual edges. This leaves us with a subset $\mathcal{S}_0$ with $\bar{N}_0 = 9-3 = 6$ edges.

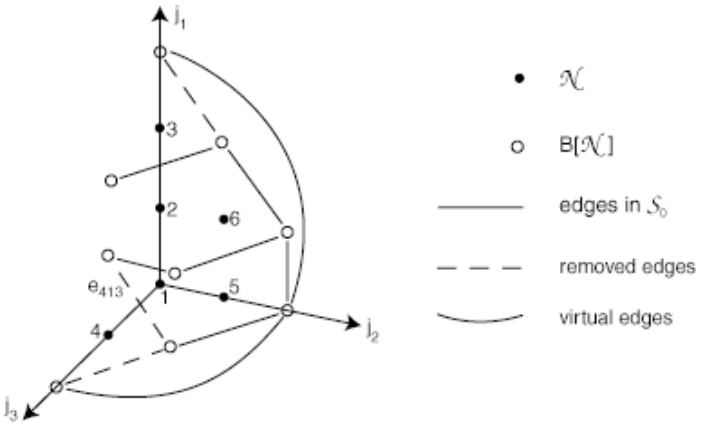

Figure 8.3.

When we form the 36×24 Jacobian matrix $J(\mathcal{S})$ of the full system $\mathcal{S}$ and assume that the $\tilde{a}_j^T$ *satisfy the consistency conditions*, we find rank $J(\mathcal{S}) = 12$. The same rank is found for the 12×24 Jacobian matrix of a minimal set $\mathcal{S}_0$ of conditions exhibited above. If the consistency conditions are violated, the rank of $J(\mathcal{S})$ increases; for generic elements in the $\widetilde{A}_\sigma$ or *for generic perturbations of the* $\tilde{a}_j^T$, it becomes 24.

Of course, with a small violation of the consistency conditions, the singular values of $J(\mathcal{S})$ may still reflect the generic rank to some extent; but this reflection may be so vague that it cannot be utilized numerically: In an experimental computation for the above normal set $\mathcal{N}$, we formed exact rational matrices $\widetilde{A}_\sigma$, $\sigma = x, y, z$, for a set of 4 "random" zeros with integer components of O(1). Then we formed the 36×24 Jacobian $J(\mathcal{S})$ for the exact $\tilde{a}_j^T$ and for approximations obtained by rounding them to 5 decimal digits. There were precisely 12 nonvanishing singular values (between 223 and 36) for the exact data, as predicted by our considerations. For the perturbed values, there were 24 nonvanishing singular values decreasing smoothly from 242 to .187. In the critical places from the 11th to the 14th singular value (ordered in decreasing size), we found the values $\approx 19.87, 14.92, 12.29, 11.61$ without any indication of a jump in size! Thus the only chance for obtaining a Newton step with 12 further conditions for the 24 increments would have been the immediate use of a subsystem $\mathcal{S}_0$ of only 12 equations.

The quasi-univariate feature of $\mathcal{N}$ gives rise to a further special situation: Take z as the distinguished variable and eliminate the relations generated by $A_x A_y = A_y A_x$. According to the considerations in section 8.1.3, the remaining 6 relations must be *linear* and of full rank in the rows $a_{x^2}^T, a_{xy}^T, a_{y^2}^T$; thus, the 24×12 Jacobian matrix of these relations with respect to $a_{x^2}^T, a_{xy}^T, a_{y^2}^T$ *only* must not contain any components of these rows and have rank 12 for generic $a_{xz}^T, a_{yz}^T, a_{z^2}^T$. This is also confirmed by the respective computations. This also reconfirms Proposition 8.7 which asserts that the rows $a_{xz}^T, a_{yz}^T, a_{z^2}^T$ of A_z can be chosen arbitrarily and that the other rows of A_x, A_y are then determined by $\mathcal{S}_0$. □

In the general case, the selection of the free parameters is not so simple. For example, the conjecture that there may always exist a subset of s vectors a_j^T whose data may be chosen arbitrarily and thus determine the generated ideal can be disproved by a simple counter-example: In $\mathcal{P}^2$, consider the normal set $\{1, y, x, y^2, xy, x^2\}$, with $B[\mathcal{N}] = \{y^3, xy^2, x^2y, x^3\}$. When we choose any two of the monomials in $B[\mathcal{N}]$ as leading monomials of two border basis polynomials, with generic coefficients, and analyze the ideals generated by them, we find that each of these ideals has *more than* 6 zeros. Thus it cannot be possible to generate an ideal in $\mathcal{P}^2(6)$ by two border basis elements for the above normal set.

Exercises

1. Consider the set $\mathcal{B}$ of the following 10 polynomials:

$$\begin{pmatrix} bb_1 \\ bb_2 \\ bb_3 \\ bb_4 \\ bb_5 \\ bb_6 \\ bb_7 \\ bb_8 \\ bb_9 \\ bb_{10} \end{pmatrix} = \begin{pmatrix} 56z^2 \\ 56y^2 \\ 14x^2 \\ 16yz^2 \\ 112xz^2 \\ 112y^2z \\ 16xyz \\ 14x^2z \\ 16xy^2 \\ 4x^2y \end{pmatrix} - \begin{pmatrix} 28 & -62 & 14 & -2 & 28 & -13 & -1 \\ 252 & 162 & 14 & 54 & -84 & 15 & 27 \\ 28 & -34 & 14 & -16 & 28 & -26 & -2 \\ 16 & 8 & 8 & 2 & -4 & 1 & 1 \\ -28 & -338 & -14 & 74 & 140 & -79 & 37 \\ 0 & -144 & 0 & -6 & 364 & 45 & -3 \\ 4 & -34 & 2 & 2 & 28 & 13 & 1 \\ 14 & 121 & 7 & -4 & -28 & 2 & -2 \\ 60 & 66 & 30 & 54 & -12 & 15 & -5 \\ 16 & 8 & 8 & 2 & 4 & 1 & -3 \end{pmatrix} \begin{pmatrix} 1 \\ z \\ y \\ x \\ yz \\ xz \\ xy \end{pmatrix}.$$

(a) If $\mathcal{B}$ is the border basis of a nontrivial ideal $\mathcal{I}$, what is the associated normal set basis

b of the quotient ring $\mathcal{R}[\mathcal{I}]$? What are the multiplication matrices A_σ of $\mathcal{R}[\mathcal{I}]$ with respect to **b** ?

(b) Prove that $\mathcal{R} = \text{span } \mathbf{b}$ with a multiplicative structure defined by the A_σ is indeed the quotient ring of an ideal $\mathcal{I} \subset \mathcal{P}^s(7)$. (Compare Theorem 8.1.)

(c) Compute and reduce at least a few of the S-polynomials $S[bb_j, bb_{j'}]$ for a (partial) *direct* verification that $\mathcal{B}$ is a border basis. (Compare Corollary 8.12.)

(d) Compute the 7 zeros of $\mathcal{I}$ from the nonderogatory one of the three multiplication matrices. From the zeros, explain why the other two A_σ are derogatory. Find a simple linear combination of these two matrices which is nonderogatory and determine the zeros from it.

2. Consider the normal set $\mathcal{N}_1$ of Example 8.1.

(a) Identify the border set $B[\mathcal{N}_1]$ and its subsets $B_\sigma[\mathcal{N}_1]$, $\sigma = 1, 2, 3$; cf. Definition 8.2. Verify that $\mathcal{N}_1$ is not quasi-univariate with respect to either variable.

(b) Identify the boundary set $\partial\mathcal{N}_1$ (cf. Definition 8.4) and the monomials $b_\mu \in \mathcal{N}_1$ for which $x \cdot b_\mu \in B[\mathcal{N}_1]$ (there must be as many as there are nontrivial rows in $A_1^{(1)}$). For each of these b_μ, consider $y \cdot b_\mu$ and $z \cdot b_\mu$ and write down the respective relations (8.23) or (8.24). Check their validity for the $A_\sigma^{(1)}$ of Example 8.1.

(c) Write down all elements of the border basis $\mathcal{B}$ for the ideal of Example 8.1. Translate the relations (8.23) and (8.24) found in (b) into syzygies of $\mathcal{B}$ and verify their validity.

3. Consider the "rectangular" normal set $\mathcal{N} = \{1, x, y, xy, z, xz, yz, xyz, z^2, xz^2, yz^2, xyz^2\} \subset \mathcal{T}^3(12)$. In answering the following questions, sketch the situation in $\mathbb{N}_0^3$.

(a) How many elements (N) has the border set $B[J_\mathcal{N}]$? How many edges ($\overline{N}$) are there in the web representing the consistency relations in $\mathcal{S}$?

(b) Compile the $\overline{N}$ consistency relations for the nontrivial rows of the multiplication matrices A_σ of a quotient ring with basis $\mathcal{N}$. Determine the Jacobian of these relations with respect to the nontrivial elements of the A_σ.

(c) How many edges are left after the deletion of all edges representing relations occurring only in $A_x A_y = A_y A_x$? Which further edges can you delete (and why) to bring the number of the remaining ones to $\overline{N}_0 = N - 3$?

(d) Write down the remaining set $\mathcal{S}_0$ of relations in terms of the row vectors a_j^T of the A_σ and in terms of syzygies for the border basis elements bb_j.

4. (a) Consider the ideal $\mathcal{I}$ with the *zero set* $J_\mathcal{N} \subset \mathbb{N}_0^3$ from the previous exercise. Verify that the normal set $\mathcal{N}$ is feasible for $\mathcal{I}$. Determine the multiplication matrices A_x, A_y, A_z of $\mathcal{R}[\mathcal{I}]$ with respect to the normal set basis $\mathcal{N}$.

(b) Evaluate the Jacobian from (b) in the previous exercise at the elements of the current A_σ. Verify that the rank of the Jacobian is $\overline{N}_0$.

(c) Select the rows from the Jacobian which correspond to the relations in $\mathcal{S}_0$ and verify that this submatrix has full rank.

5. Consider the determination of the admissible-data manifold $\mathcal{M}_\mathcal{N}$ for $s = 2$ variables.

(a) Convince yourself that, for a normal set with $|B[\mathcal{N}]| = N$, $\overline{N} = N - 1$ and that $\overline{N}_0 = N - 2$ is obtained by taking into account the virtual edge between the two extremal points of $B[J_\mathcal{N}]$.

(b) Compute the rank and the singular values of the Jacobian of the relations in $\mathcal{S}$ and $\mathcal{S}_0$, resp., for numerical examples with exact and perturbed multiplication matrices.

8.3 Regular Systems of Polynomials

8.3.1 Complete Intersections

It would be nice if the situation at each simple zero of a polynomial system resembled that at a zero of a regular system of s *linear* equations p_ν in s variables. This situation is very clear cut: Each of the equations $p_\nu(x) = 0$ represents a hyperplane in $\mathbb{C}^s$ or $\mathbb{R}^s$ and there is the well-known *alternative*:

- if the normal vectors of the s hyperplanes span the s-space there is a unique intersection point z ("regular case");

- else there exists a d-dimensional subspace ($d > 0$) which is parallel to each hyperplane, in which case the hyperplanes either have a common linear manifold of dimension d or they have no point in common ("singular case").

Algebraically, in the regular case the ideal $\langle p_\nu, \nu = 1(1)s\rangle$ consists of all polynomials in $\mathcal{P}^s$ which vanish at z and is a maximal ideal; in the singular case, the ideal is either d-dimensional, with a linear zero manifold, or trivial. The corresponding *criterion* is well known:

Proposition 8.16. Let $p_\nu(x) = \alpha_{\nu 0} + \sum_{\sigma=1}^{s} \alpha_{\nu\sigma} x_\sigma,\ \nu = 1(1)s$, and let $A := (\ \alpha_{\nu\sigma},\ \sigma > 0\ ) \in \mathbb{C}^{s\times s},\ a := (\ \alpha_{\nu 0}\ ) \in \mathbb{C}^s,\ \overline{A} := (\ A \mid a\ ) \in \mathbb{C}^{s\times(s+1)}$. For *nonsingular* A, the situation is regular and $z = -A^{-1}a$ is the unique solution. For *singular* A, with $\mathrm{rk}(A) = s - d =: r$ and $A\,z = 0$ for $z \in Z$, $\dim(Z) = d$, if $\mathrm{rk}(\overline{A}) = r$ then the zero set $Z[\langle p_\nu\rangle] = -A^{+}a + Z$ where A^{+} is the Moore–Penrose pseudo-inverse of A; else $Z[\langle p_\nu\rangle] = \emptyset$ and $\langle p_\nu\rangle = \langle 1\rangle$.

From *numerical* linear algebra we know that this strict, discontinuous separation between the regular and the singular case makes sense only for *exact* coefficients $\alpha_{\nu\sigma}$ and can only be verified with *exact computation*. From a computational point of view, there is a *transition regime* where A becomes increasingly *ill-conditioned*; with *empirical* coefficients, this means that the pseudozero sets containing the valid approximations for z become larger and larger and that the naive use of approximate computation can lead to large deviations in the result. We will return to this aspect in section 9.4; at present we consider the intrinsic case.

We observe that there is a natural one-to-one correspondence between points z in $\mathbb{C}^s$ and 0-dimensional ideals $\mathcal{I}_z$ in $\mathcal{P}^s$ with z as their only (simple) zero. Moreover, for each $z = (\zeta_\sigma) \in \mathbb{C}^s$, there exist systems P of s polynomials $p_\sigma \in \mathcal{P}^s$ such that $\langle P\rangle = \mathcal{I}_z$, e.g., $p_\sigma(x) = x_\sigma - \zeta_\sigma,\ \sigma = 1(1)s$. Thus, each 0-dimensional ideal in $\mathcal{P}^s(1)$ may be *generated* by s polynomials. Does this observation generalize to $m > 1$?

Definition 8.8. A 0-dimensional ideal $\mathcal{I} \subset \mathcal{P}^s,\ s > 1$, which can be generated by s polynomials, is called a *complete intersection ideal* and its generating system a *complete intersection system*. The variety (=zero set) of such an ideal is also called a *complete intersection*. □

More generally, an $(s - n)$-dimensional ideal in $\mathcal{P}^s$ which can be generated by n polynomials and the associated variety may also be called a complete intersection (ideal) and the generating system a complete intersection system. The essential characteristic of a complete intersection

system $\{p_\nu, \nu = 1(1)n\}$ is the following: When we consider the sequence of ideals $\mathcal{I}_\nu := \langle p_1, \ldots, p_\nu \rangle$, $\nu = 1(1)n$, we must have $\dim \mathcal{I}_\nu = s - \nu$ for any numbering of the polynomials in the system; with other words, each further generating polynomial must reduce the dimension exactly by one. In this text, we will restrict the use of the term to the case $n = s$ as in Definition 8.8. Naturally, a complete intersection ideal may also have bases of a structure which requires more than s basis elements; cf. Example 8.2.

In the introduction to Chapter 8, we have required a *regular polynomial system* in s variables to consist of s polynomials and to have a 0-dimensional zero set; thus, each regular polynomial system in $\mathcal{P}^s$ is a complete intersection system and generates a complete intersection ideal. However, with a regular system we have also associated that it is sufficiently removed from a singular situation.

Any set Z of m points in $\mathbb{C}^s$ represents a complete intersection when it is interpreted as the set of *simple* zeros of a polynomial ideal in $\mathcal{P}^s$. This can be seen as follows:

Definition 8.9. A linear form $a : x \to a^T x$ on $\mathbb{C}^s$ is *separating* for a finite set $Z \subset \mathbb{C}^s$ if it takes different values for each $z \in Z$. □

Example 8.9: If the points $z_\mu \in Z$ have different $\bar{\sigma}$-th components, the linear form $a^T x = x_{\bar{\sigma}}$ is separating on Z. Only in a set Z where no such $\bar{\sigma}$ exists do we have to take recourse to a less simple form. Take, e.g., $Z = \{(0, 0), (1, 0), (0, 1)\} \subset \mathbb{R}^2$; now, no individual component is separating, but a natural separating linear form is $a^T x = x_1 - x_2$. □

Proposition 8.17. For any m-element set $Z \subset \mathbb{C}^s$, there exist infinitely many separating linear forms.

Proof: For each pair μ_1, μ_2, the relation $a^T z_{\mu_1} = a^T z_{\mu_2}$ represents an $(s-1)$-dimensional linear subspace in the s-dimensional vector space $\mathcal{A}$ of the a^T. The $m(m-1)/2$ (finitely many) subspaces defined by the disjoint pairs of z_μ, $\mu = 1(1)m$, which have to be *avoided*, cannot fill $\mathcal{A}$. □

Theorem 8.18. For any finite set $Z = \{z_\mu, \mu = 1(1)m\} \subset \mathbb{C}^s$, there exist sets P of s polynomials $p_\sigma \in \mathcal{P}^s$, $\sigma = 1(1)s$, such that the ideal $\mathcal{I} = \langle P \rangle \subset \mathcal{P}^s$ has a simple zero at each $z_\mu \in Z$ but no other zeros.

Proof: Choose a separating linear form $a_s^T x$ for Z which exists by Proposition 8.17, with distinct values $\omega_{s\mu} := a_s^T z_\mu \in \mathbb{C}^s$, $\mu = 1(1)m$. Let $q_s(w) := \prod_{\mu=1}^m (w - \omega_{s\mu}) \in \mathcal{P}_m^1$.

Now choose $s-1$ row vectors $a_\sigma^T \in \mathbb{C}^s$, $\sigma = 1(1)s-1$, such that they span the $\mathbb{C}^s$ together with a_s^T. For each $\sigma = 1(1)s-1$, let $\omega_{\sigma\mu} := a_\sigma^T z_\mu$, $\mu = 1(1)m$, and form the interpolation polynomial $q_\sigma(w) \in \mathcal{P}_{m-1}^1$ with $q_\sigma(\omega_{s\mu}) = \omega_{\sigma\mu}$, $\mu = 1(1)m$. By their construction, the s polynomials

$$p_\sigma(x) := a_\sigma^T x - q_\sigma(a_s^T x), \quad \sigma = 1(1)s-1, \qquad p_s(x) := q_s(a_s^T x), \tag{8.31}$$

vanish at each $z_\mu \in Z$; these can only be simple common zeros by construction of q_s. Assume that there exists $\bar{z} \notin Z$ with $p_\sigma(\bar{z}) = 0$, $\sigma = 1(1)s$. For $\sigma = s$, this implies $a_s^T \bar{z} = a_s^T z_\mu$ for some $\bar{\mu} \in \{1, .., m\}$; hence $a_\sigma^T \bar{z} = q_\sigma(a_s^T z_{\bar{\mu}}) = a_\sigma^T z_{\bar{\mu}}$ for $\sigma = 1(1)s-1$. But this implies $\bar{z} = z_{\bar{\mu}}$ since the a_σ^T span the $\mathbb{C}^s$. □

Example 8.10: If we have an ideal $\mathcal{I}$ with m simple zeros whose last components differ, a

complete intersection basis for $\mathcal{I}$ may have the structure

$$x_\sigma - q_\sigma(x_s)\,,\ \sigma = 1(1)s-1, \quad q_s(x_s)\,.$$

Note that all q_σ in this basis are *univariate* polynomials of degrees $m-1$ and m resp. This is the Groebner basis of the ideal for a lexicographic ordering, with x_s the lowest variable; cf. section 8.4.2.

For the ideal with $Z = \{(0,0),(1,0),(0,1)\} \subset \mathbb{R}^2$ in Example 8.9, with a separating linear form $a_2^T x = x_1 - x_2$, we have $q_2(w) = w^3 - w$; with $a_1^T x = x_1 + x_2$, we obtain $q_1(w) = w^2$ so that a complete intersection representation of this ideal is

$$p_1(x_1,x_2) \;=\; x_1 + x_2 - (x_1-x_2)^2\,, \quad p_2(x_1,x_2) \;=\; (x_1-x_2)^3 - (x_1-x_2)\,.$$

This representation appears unnaturally complicated for the simple location of the zeros. There is the more "natural" basis $\{x_1^2 - x_1,\ x_1x_2,\ x_2^2 - x_2\}$; but no two of its elements suffice to describe the ideal correctly. □

Example 8.11: For a nondegenerate set $Z = \{z_\mu,\ \mu = 1(1)4\} \subset \mathbb{C}^2$ (no three points on a straight line), there exists a one-parametric family of conic sections which pass through the 4 points since a conic section is defined by 5 of its points. Any two of the quadratic polynomials which describe the conic sections generate the ideal with Z as zero set. □

Since we have seen that a finite set of simple zeros always represents a complete intersection, zero constellations which are not complete intersections must contain multiple zeros. Even then, a complete intersection often prevails:

Theorem 8.19. All 0-dimensional polynomial ideals in $\mathcal{P}^s$ with no zeros of a multiplicity greater than 2 are complete intersection ideals.

Proof: Without loss of generality, assume that z_1 is a double zero, with the associated dual basis element (cf. Definition 2.14) $\sum_{\sigma=1}^s \gamma_{1\sigma}\partial_{x_\sigma}[z_1]$. In the choice of the separating linear form a_s^T of the proof of Theorem 8.18, we introduce the additional subspace restriction $a_s^T c_1 \neq 0$, with $c_1 := (\gamma_{1\sigma}) \in \mathbb{C}^s$; this leaves the choice of a_s^T feasible and we choose the a_σ^T as in the proof of Theorem 8.1. To the univariate polynomial $q_s(w)$ which vanishes at the $\omega_\mu = a_s^T z_\mu$ we attach a second factor $(w-\omega_1)$. For the univariate interpolation polynomials $q_\sigma(w)$ we add the requirement that $q'_\sigma(\omega_1) = a_\sigma^T c_1 \,/\, a_s^T c_1$. Now, the polynomials (8.31) satisfy $\sum_{\sigma=1}^s \gamma_{1\sigma}\partial_{x_\sigma} p_\sigma(z_1) = 0,\ \sigma = 1(1)s$, in addition to $p_\sigma(z_\mu) = 0$. For each further double zero, the same procedure can be employed. □

Example 8.10, continued: We choose the same zero set $Z = \{(0,0),(1,0),(0,1)\}$ and assume that the polynomials in the ideal have a vanishing x_2-derivative at (1,0). With a_σ^T as previously, we have $a_1^T c = 1,\ a_2^T c = -1$, and

$$\begin{aligned} p_1(x_1,x_2) \;&=\; x_1 + x_2 - (3(x_1-x_2) + 2(x_1-x_2)^2 - 3(x_1-x_2)^3)/2\,, \\ p_2(x_1,x_2) \;&=\; (x_1 - x_2 + 1)(x_1-x_2)(x_1-x_2-1)^2\,; \end{aligned}$$

surprisingly, this set permits a reduction to a much simpler basis of only 2 polynomials, viz. $\{\,x_1^2 - x_1,\ x_2^2 + (x_1-1)x_2\,\}$. In any case, the ideal with the above zero set is a complete intersection ideal. □

Example 8.11, continued: When we specify three points in $\mathbb{C}^2$ and a tangential direction in one of them, there is again a one-parametric family of conic sections satisfying these data. Thus,

the respective ideal can be generated by two quadratic equations as previously. Note that the previous example is a special case of this situation so that the reduced representation was to be expected. □

From the proof of Theorem 8.19, we expect that difficulties may arise when the dual space of an ideal in $\mathcal{P}^2$ contains more than one first-order derivative at the same zero z_μ, which is a perfectly reasonable case; cf. section 8.5. Following the construction above, we should now satisfy more than one condition for the derivatives q'_σ at the respective ω_μ. Also, in $\mathcal{P}^s$, if s first-order derivative conditions are associated with the same z_μ, this implies that *all* first-order derivatives must vanish at z_μ. The following classical counterexample shows that, in $\mathcal{P}^2$, there are simple (but very degenerate) polynomial ideals with a triple zero of this type which cannot be generated by only 2 polynomials; the analogous construction works for an $s+1$-fold zero and s variables:

Example 8.12: In $\mathcal{P}^2$, consider $\mathcal{I} := \{p \in \mathcal{P}^2 : p(0,0) = \partial_{x_1} p(0,0) = \partial_{x_2} p(0,0) = 0\}$, with no further zero or multiplicity, and assume $\mathcal{I} = \langle p_1, p_2 \rangle$. Each $p \in \mathcal{I}$ must have a Taylor expansion

$$p(x_1, x_2) = x_1^2\, q_1(x_1, x_2) + x_1\, x_2\, q_2(x_1, x_2) + x_2^2\, q_3(x_1, x_2)\,,$$

which implies

$$\partial_{x_1^2} p_\nu(0,0) = q_{\nu 1}(0,0), \quad \partial_{x_1 x_2} p_\nu(0,0) = q_{\nu 2}(0,0), \quad \partial_{x_2^2} p_\nu(0,0) = q_{\nu 3}(0,0), \quad \nu = 1, 2.$$

Since there exists a vector $(\gamma_1, \gamma_2, \gamma_3)$ such that $\sum_{j=1}^3 \gamma_j\, q_{\nu j}(0,0) = 0$ for $\nu = 1$ and 2, there exists a 2nd order derivative at (0,0) which vanishes for all $p \in \mathcal{I}$. Thus the assumption of a complete intersection is incompatible with a triple zero of the above kind. Note that this implies that a zero of this type cannot occur with a regular polynomial system.

When we keep the 3-fold zero at (0,0) but change the derivative conditions, we may well have a complete intersection ideal: For $\mathcal{I} := \{p \in \mathcal{P}^2 : p(0,0) = \partial_{x_1} p(0,0) = \partial_{x_1}^2 p(0,0) = 0\}$, with no further zero or multiplicity, there is the trivial basis $\{x_1^3, x_2\}$. □

Obviously, the dual spaces $\mathcal{D}$ whose associated ideal $\mathcal{I}[\mathcal{D}]$ is not a complete intersection ideal constitute a very "thin" subset of all dual spaces of dimension m in s variables; furthermore, they cannot appear with regular polynomial systems.

In the normal set representation of an ideal $\mathcal{I}$ with respect to a *quasi-univariate* normal set $\mathcal{N}$, with distinguished variable x_s, consider the border basis subset $\mathcal{B}_s = \{bb_1, \ldots, bb_s\}$ of the border basis $\mathcal{B}_\mathcal{N}$ of $\mathcal{I}$ whose members bb_σ, $\sigma = 1(1)s$, have their $\mathcal{N}$-leading monomials x^{j_σ} in the border subset $B_s[\mathcal{N}]$.

Proposition 8.20. $\mathcal{B}_s$ is a complete intersection system, with $\langle \mathcal{B}_s \rangle = \langle \mathcal{B}_\mathcal{N} \rangle = \mathcal{I}$.

Proof: Compare Theorem 8.5 and Proposition 8.7. □

Thus, the border basis of a quasi-univariate normal set representation contains at least one complete intersection system as a subset.

Example 8.13: In Example 8.2, the normal set $\mathcal{N} = \{1, x, y, z\}$ is quasi-univariate with respect to each variable; the assumptions of Theorem 8.5 are satisfied for x and y as distinguished variables. Hence (with the notation of Example 8.2), the following border basis subsets are complete intersection systems for $\mathcal{I}[\mathcal{R}]$: $\{bb_1, bb_2, bb_3\}$ and $\{bb_2, bb_4, bb_5\}$. □

8.3.2 Continuity of Polynomial Zeros

In section 5.1.1, we have convinced ourselves that the zeros of a univariate polynomial p are continuous functions of the coefficients of p, and analytic functions in the case of simple zeros. Of course, the quantitative meaning of that assertion depends on the particular *representation* of p which we have in mind (cf. section 5.1.2), but a change between representations by different bases amounts essentially to a regular linear transformation between the coefficients. The simplicity of the situation rests strongly on the fact that there is a unique relation between a univariate polynomial p and the ideal $\langle p \rangle$; cf. section 5.1.3.

With 0-dimensional systems P of *multivariate* polynomials and the associated ideals $\langle P \rangle$, this situation is quite different because of the many potential basis representations of ideals in $\mathcal{P}^s$ which cannot be related in a simple linear way. Also many basis representations consist of more than s polynomials and are thus overdetermined; cf. section 8.2.2. Even when we restrict ourselves to complete intersection ideals and bases with s polynomials represented in terms of monomials, the supports of the basis polynomials may be quite distinct in two different bases for the same ideal. Thus, when we consider the maps from the coefficients of one basis to the individual zeros of $\mathcal{I} = \langle P \rangle$ and the analogous maps from the coefficients of another basis, it may not be obvious at all how these maps are related.

Therefore, in our analysis of the relations between an ideal $\mathcal{I} = \langle P \rangle \subset \mathcal{P}^s$ and the zero set $Z[\mathcal{I}]$, we assume throughout that a particular complete intersection system P has been specified as generating system for $\mathcal{I}$. This defines a data space $\mathcal{A}$ for the coefficients in $P = P(x; a)$, with $a \in \mathcal{A}$. With our regularity concept, each neighboring system $P(x;\ a + \Delta a)$, with $\|\Delta a\|$ sufficiently small, defines an ideal $\widetilde{\mathcal{I}}$, with a zero set $Z[\widetilde{\mathcal{I}}]$ of the same magnitude (counting multiplicities), and we can introduce the data→result maps

$$F_\mu \ : \quad \mathcal{A} \ \to \ \mathbb{C}^s \,, \qquad \text{with } \ F_\mu(a) = z_\mu \,, \ \mu = 1(1)m \,,$$

whose domains are neighborhoods of $a \in \mathcal{A}$, and use them as reference for our analysis of the continuity of the zeros.

Due to the linearity of polynomials in their coefficients, we have

$$P(x;\ a + \Delta a) \ = \ P(x; a) + P(x; \Delta a) \ = \ \{\, p_\nu(x; a) + p_\nu(x; \Delta a) \,\} \,,$$

and due to the differentiability with respect to the variables x, we have the Taylor expansions

$$P(x + \Delta x; a) \ = \ P(x; a) + P'(x; a)\, \Delta x + \ldots \ = \ \{\, p_\nu(x; a) + p'_\nu(x; a)\, \Delta x + \ldots \} \,;$$

cf. (1.9). Thus, the zeros $z_\mu + \Delta z_\mu$ of the ideal generated by a neighboring system with coefficients $a + \Delta a$, satisfy

$$\begin{aligned} &P(z_\mu + \Delta z_\mu; a + \Delta a) \ = \\ &\qquad P(z_\mu; a) + P'(z_\mu; a)\, \Delta z_\mu + P(z_\mu; \Delta a) + \mathrm{O}(\|\Delta z_\mu\|^2) + \mathrm{O}(\|\Delta a\| \|\Delta z_\mu\|) \ = \ 0 \,. \end{aligned} \tag{8.32}$$

At a simple zero z_μ of $P(x; a)$, with a regular Jacobian $P'(z_\mu; a)$, this implies

$$\begin{aligned} \Delta z_\mu \ &= \ F_\mu(a + \Delta a) - F_\mu(a) = \tfrac{d}{da}\, F_\mu(a)\, \Delta a + \mathrm{O}(\|\Delta a\|^2) \\ &= \ -\left(P'(z_\mu; a)\right)^{-1} P(z_\mu, \Delta a) + \mathrm{O}(\|\Delta a\|^2) \\ &= \ \left(P'(z_\mu; a)\right)^{-1} \left(-\textstyle\sum_{j \in J_\nu} \Delta\alpha_{\nu j} z_\mu^j\right) + \mathrm{O}(\|\Delta a\|^2) \,. \end{aligned} \tag{8.33}$$

Proposition 8.21. In a sufficiently small neighborhood of the specified coefficients, a simple zero z_μ of the regular polynomial system $P(x;a)$ is a differentiable (and hence continuous) function of the coefficients in the system P.

From (8.33), we observe that the increments of a simple zero are really determined by the *residuals* $\Delta p_\nu(z_\mu) = \sum_{j\in J_\nu} \Delta\alpha_{\nu j} z_\mu^j$ of the original zeros in the modified polynomials. When we consider P as a map from the $\mathbb{C}^s$ of the x-arguments to the $\mathbb{C}^s$ of the $p_\nu(x)$, the implicit function theorem tells us that – for regular $P'(x)$ – there is an analytic function $\Delta P(x) \to \Delta x$ such that $P(x+\Delta x) = P(x) + \Delta P(x)$; cf., e.g., [8.4], section 10.2.

Theorem 8.22. In the neighborhood of a simple zero $z_\mu \in \mathbb{C}^s$ of a regular polynomial system $P \in (\mathcal{P}^s)^s$, there exists a bijective analytic map between approximate zeros $z_\mu + \Delta z_\mu$ and residuals $\Delta P := P(z_\mu + \Delta z_\mu)$.

Quantitatively, we have, with appropriately matching norms,

$$\|\Delta P\| \;\le\; \|P'(z_\mu)\|\,\|\Delta z_\mu\| + \mathrm{O}(\|\Delta z_\mu\|^2) \qquad \text{and}$$

$$\|\Delta z_\mu\| \;\le\; \|(P'(z_\mu))^{-1}\|\,\|\Delta P\| + \mathrm{O}(\|\Delta P\|^2)\,. \tag{8.34}$$

Proposition 8.23. The absolute condition of a simple zero $z_\mu \in \mathbb{C}^s$ of the regular polynomial system $P \in (\mathcal{P}^s)^s$ is quantified by $\|(P'(z_\mu))^{-1}\|$, where $\|..\|$ is the operator norm for the norms in the solution and the residual spaces.

Example 8.14: In $\mathcal{P}^2$, consider the zero set of the ideal generated by two nondegenerate quadratic polynomials (**x**:=(x,y))

$$p_\nu(x,y) = \mathbf{x}^T A_\nu \mathbf{x} + a_\nu^T \mathbf{x} + \alpha_{\nu 0}\,, \quad \nu = 1,2\,,$$

with regular symmetric $A_\nu \in \mathbb{C}^{2\times 2}$, $a_\nu^T \in \mathbb{C}^2$, $\alpha_{\nu 0} \in \mathbb{C}$, i.e. the 4 real or complex intersection points of two conic sections. If the intersection angles are not very acute, small shifts in the conic sections lead to small changes in the zeros. At a zero $z_\mu = (\xi_\mu, \eta_\mu)$, we have from (8.33)

$$\Delta z_\mu \;=\; -\begin{pmatrix} 2\,(\xi_\mu,\eta_\mu)\,A_1 + a_1^T \\ 2\,(\xi_\mu,\eta_\mu)\,A_2 + a_2^T \end{pmatrix}^{-1} \begin{pmatrix} (z_\mu^T \Delta A_1 + \Delta a_1^T)\,z_\mu + \Delta\alpha_{10} \\ (z_\mu^T \Delta A_2 + \Delta a_2^T)\,z_\mu + \Delta\alpha_{20} \end{pmatrix},$$

which displays the effect of a change in individual coefficients on the components of the zeros. □

For *near-singular* $P'(z_\mu)$, the condition of the zero z_μ may become arbitrarily bad; cf. (8.34). This reflects a situation where the gradient vectors $p_\nu'(z_\mu)$ are nearly linearly dependent or—equivalently—two or more of the manifolds $p_\nu(x) = 0$ are nearly tangential at z_μ so that the zero must react extremely sensitively to certain small perturbations in the p_ν.

Singularity of $P'(z_\mu)$ characterizes z_μ as a *multiple zero* of P. In the univariate case, at a multiple zero, differentiability of the coefficient→zero map disappears but continuity is retained as Hölder-continuity; cf. Proposition 5.1. For a multivariate complete intersection system, this remains true, but the analysis must consider the particular derivative structure of the multiple zero. We will regard this in detail in sections 8.5 and 9.3; at this point we only demonstrate the situation with a simple example:

Example 8.15: In $\mathcal{P}^2$, consider $p_1(x, y) = x^2 + y^2 - 1,\ p_2(x, y) = x^2 + y^2 + 2x - 3$, with a real double zero of $\langle p_1, p_2\rangle$ at (1,0). For perturbations of the two constant terms,

$$p_\nu(1 + \Delta x, \Delta y) \;=\; 2\nu\,\Delta x + (\Delta x)^2 + (\Delta y)^2 + \Delta\alpha_{\nu 0} = 0\,, \quad \nu = 1, 2\,.$$

This implies

$$\Delta x = (\Delta\alpha_{10} - \Delta\alpha_{20})/2\,, \quad \Delta y = \pm\sqrt{\Delta\alpha_{20} - 2\,\Delta\alpha_{10}}\,(1 + \mathrm{O}(\|\Delta a\|))\,,$$

which displays the Hölder-continuity of the y-component while the x-component remains differentiable. □

8.3.3 Expansion by a Complete Intersection System

In section 8.2.1 (cf. (8.16)), we had observed that, in the expansion

$$p(x) \;=\; \mathrm{NF}_{\mathcal{I}}[p] + \sum_{x^j \in B[\mathcal{N}]} q_j(x)\, bb_j(x)$$

of a polynomial $p \in \mathcal{P}^s$ with respect to an arbitrary border basis $\mathcal{B}_\mathcal{N}$ of a 0-dimensional ideal $\mathcal{I}$, the q_j are generally not unique because there exist nontrivial syzygies between the bb_j. If we consider the same type of an expansion with respect to a complete intersection system, the non-uniqueness can be removed in as much as one pleases. This is due to a fundamental property of complete intersection systems:

Proposition 8.24. A complete intersection system $P = \{p_1, \ldots, p_s\} \subset \mathcal{P}^s$ has no nontrivial syzygies, i.e.

$$\sum_{\nu=1}^{s} q_\nu(x)\, p_\nu(x) \;=\; 0 \quad \text{(zero polynomial)} \quad \text{implies} \quad q_\nu \in \langle P\rangle\,, \quad \nu = 1(1)s\,. \tag{8.35}$$

Proof: An algebraic proof has been pointed out to me by D. Cox, but it requires too many technicalities to be reproduced here. Geometrically, the plausibility of (8.35) is seen thus: Let $\widehat{V}_\sigma := \cap_{\nu\neq\sigma} V[p_\nu],\ \sigma = 1(1)s$. For a complete intersection, $\dim \widehat{V}_\sigma = 1$ and $\dim V[p_\sigma] \cap \hat{V}_\sigma = 0$. For some $\sigma \in \{1, .., s\}$, take $x \in \widehat{V}_\sigma,\ x \notin V[p_\sigma]$. Substitution into the sum in (8.35) shows that q_σ vanishes on $\widehat{V}_\sigma$ with the possible exception of its intersection with $V[p_\sigma]$; by continuity, it must vanish on all of $\widehat{V}_\sigma$ which implies $q_\sigma \in \langle p_\nu,\ \nu \neq \sigma\rangle \subset \langle P\rangle$. □

When we write (8.35) in the equivalent form

$$\text{With}\ \ q_\nu \in \mathcal{R}[\langle P\rangle]\,, \quad \sum_{\nu=1}^{s} q_\nu(x)\, p_\nu(x) \;\equiv\; 0 \qquad \text{implies} \quad q_\nu \;=\; 0\,, \quad \nu = 1(1)s\,, \tag{8.36}$$

then it is a natural extension of the fundamental concept of (scalar) linear independence of a system of s linear polynomials in s variables in linear algebra:

$$\text{With}\ \ \gamma_\nu \in \mathbb{C}\,, \quad \sum_{\nu=1}^{s} \gamma_\nu\, p_\nu(x) \;\equiv\; 0 \qquad \text{implies} \quad \gamma_\nu = 0\,,\ \nu = 1(1)s\,.$$

Thus it would be meaningful to call a system $P \subset \mathcal{P}^s$ which satisfies (8.36) *polynomially linearly independent*. But, surprisingly, a term for this property appears not to exist in polynomial algebra.

Theorem 8.25. Consider a complete intersection ideal $\mathcal{I} = \langle p_1, \ldots, p_s \rangle \subset \mathcal{P}^s$ and its quotient ring $\mathcal{R}[\mathcal{I}]$, with an arbitrary but fixed basis $\mathbf{b}$. In the expansion of $p \in \mathcal{P}^s$

$$p(x) \;=\; \mathrm{NF}_{\mathcal{I}}[p] + \sum_{\nu=1}^{s} q_\nu(x)\, p_\nu(x)\,, \tag{8.37}$$

the normal forms $\mathrm{NF}_{\mathcal{I}}[q_\nu] =: d_{1,\nu}(x) \in \mathcal{R}[\mathcal{I}]$ are unique.

Proof: Let $q_\nu(x) = d_{1,\nu}(x) + \sum_{\nu_1} q_{\nu\nu_1} p_{\nu_1}(x)$; consider another expansion (8.37) of p with coefficients $\hat{q}_\nu$ and $\hat{d}_{1,\nu}(x) := \mathrm{NF}_{\mathcal{I}}[\hat{q}_\nu]$ so that

$$\sum_{\nu=1}^{s} \left[(\hat{d}_{1,\nu}(x) - d_{1,\nu}(x)) + \sum_{\nu_1=1}^{s} (\hat{q}_{\nu\nu_1}(x) - q_{\nu\nu_1}(x))\, p_{\nu_1}(x) \right] p_\nu(x) \;=\; 0\,.$$

By Proposition 8.24, this requires $[\ldots] \in \mathcal{I}$ and hence $\hat{d}_{1,\nu} = d_{1,\nu},\ \nu = 1(1)s$. □

The idea of the proof of Theorem 8.25 may directly be extended to representations of the zero polynomial by an expression homogeneous in the p_ν of a degree greater than 1. Therefore, one can extend the uniqueness assertion to the normal forms of the $q_{\nu\nu_1}$ above and further. Thus we arrive at

Corollary 8.26. In the situation of Theorem 8.25, there exists a unique (finite) expansion of an arbitrary polynomial $p \in \mathcal{P}^s$ of the form

$$\begin{aligned} p(x) \;=\;& d_0(x) + \textstyle\sum_\nu d_{1,\nu}(x)\, p_\nu(x) + \sum_{\nu \le \nu_1} d_{2,\nu\nu_1}\, p_\nu(x)\, p_{\nu_1}(x) + \ldots \\ & + \textstyle\sum_{\nu \le \nu_1 \le \ldots \le \nu_{k-1}} d_{k,\nu\nu_1\ldots\nu_{k-1}}\, p_\nu(x)\, p_{\nu_1}(x) \ldots p_{\nu_{k-1}}(x)\,, \end{aligned} \tag{8.38}$$

with all coefficients $d_{\ldots}(x) = \sum_\mu \delta_{\ldots,\mu}\, b_\mu(x) \in \mathcal{R}[\mathcal{I}]$.

The importance of the expansions (8.37) and (8.38) will appear when we consider empirical systems of polyomials: Since the specified indetermination in such systems refers to the particular form in which the system is given, it is important to refer other data also to this given system. Naturally, for a p of high degree, there are also intermediate forms between an expansion (8.37) to linear terms in the p_ν and the full expansion (8.38). Note that for an ideal with only *one* zero $z = (\zeta_1, ..\zeta_s)$ and the generating complete intersection system $\{x_1 - \zeta_1, \ldots, x_s - \zeta_s\}$, (8.38) becomes the Taylor expansion of p about z.

Example 8.16: The ideal considered in Examples 8.2 and 8.7 is a complete intersection ideal by Theorem 8.19; by Proposition 8.20, generating complete intersection systems are easily obtained since the normal set $\{1, x, y, z\}$ in Example 8.2 is quasi-univariate w.r.t each variable. Therefore, each of the three subsets $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ of the border basis $\mathcal{B}$ in Example 8.7 is a generating complete intersection system. In the following, we use $\mathcal{B}_1 = \{bb_1, bb_2, bb_3\}$.

With $\mathcal{B}_1$, two different expansions (8.37) of the polynomial $p = x^4 - x^2yz + 3x^2y +$

$2\,x^2z - xyz$ in Example 8.7 are, e.g., with $\mathrm{NF}_{\mathcal{I}}[p] = 1 + \frac{24}{7}\,x + \frac{9}{7}\,y - \frac{1}{7}\,z$, $p(x,y,z) =$

$$\begin{aligned}\mathrm{NF}_{\mathcal{I}}[p] \quad &+(-\tfrac{11}{21} - \tfrac{18}{7}\,x + \tfrac{8}{7}\,y - \tfrac{11}{3}\,z + x^2 - 2\,xy - 3\,xz + \tfrac{2}{3}\,y^2 - \tfrac{2}{3}\,yz - z^2)\; bb_1(x,y,z)\\ &+(\tfrac{16}{21} + \tfrac{14}{3}\,x - \tfrac{16}{21}\,y + \tfrac{27}{14}\,z + 2\,x^2 - \tfrac{2}{3}\,xy + \tfrac{25}{6}\,xz - \tfrac{7}{6}\,yz + \tfrac{7}{6}\,z^2)\; bb_2(x,y,z)\\ &+(\tfrac{34}{21} - 2\,x + \tfrac{17}{14}\,y - \tfrac{50}{21}\,z + 3\,x^2 - \tfrac{9}{2}\,xy + xz + \tfrac{7}{6}\,y^2 - \tfrac{7}{6}\,yz)\; bb_3(x,y,z)\end{aligned}$$

and

$$\begin{aligned}\mathrm{NF}_{\mathcal{I}}[p] \quad &+(1 + \tfrac{22}{21}\,x - \tfrac{11}{21}\,x^2 - \tfrac{2}{3}\,xy - xz - \tfrac{2}{3}\,x^2y - x^2z)\; bb_1(x,y,z)\\ &+(\tfrac{52}{21}\,x + \tfrac{10}{7}\,x^2 + \tfrac{7}{6}\,xz + \tfrac{2}{3}\,x^3 + \tfrac{7}{6}\,x^2z)\; bb_2(x,y,z)\\ &+(4 + \tfrac{37}{21}\,x - \tfrac{29}{21}\,x^2 - \tfrac{7}{6}\,xy + x^3 - \tfrac{7}{6}\,x^2y)\; bb_3(x,y,z)\,.\end{aligned}$$

For the coefficients q_ν of the bb_ν in *both* expressions, we find

$$\mathrm{NF}_{\mathcal{I}}[q_1] = \tfrac{6}{7} + 4\,x - \tfrac{15}{7}\,y + \tfrac{1}{7}\,z\,,\ \mathrm{NF}_{\mathcal{I}}[q_2] = \tfrac{10}{7} + \tfrac{30}{7}\,x - \tfrac{4}{7}\,y + z\,,\ \mathrm{NF}_{\mathcal{I}}[q_3] = \tfrac{2}{7} + \tfrac{31}{7}\,x - 2\,y - \tfrac{6}{7}\,z\,.$$

With a full expansion of the q_ν in terms of the bb_ν and a collection of terms, we obtain the *unique* representation (8.38) of p in terms of the ideal basis $\{bb_1, bb_2, bb_3\}$

$$\begin{aligned}p(x,y,z) \;=\;& (1 + \tfrac{24}{7}\,x + \tfrac{9}{7}\,y - \tfrac{1}{7}\,z) + (-\tfrac{6}{7} + 4\,x - \tfrac{15}{7}\,y + \tfrac{1}{7}\,z)\; bb_1(x,y,z)\\ &+(\tfrac{10}{7} + \tfrac{30}{7}\,x - \tfrac{4}{7}\,y + z)\; bb_2(x,y,z) + (\tfrac{2}{7} + \tfrac{31}{7}\,x - 2\,y - \tfrac{6}{7}\,z)\; bb_3(x,y,z)\\ &+(bb_1(x,y,z))^2 - bb_2(x,y,z)\; bb_3(x,y,z)\,. \quad \square\end{aligned}$$

An expansion (8.37) or (8.38) can rarely be determined directly, except in trivial cases. Normally, one must first have a normal set for the quotient ring $\mathcal{R}[\langle p_1, \ldots, p_s\rangle]$ and an associated border basis of the complete intersection ideal; then, one may proceed as explained in section 8.2.1. In order to proceed further from (8.16) to (8.37), we must have a representation of the border basis elements bb_j in terms of the complete intersection system $P = \{p_\nu\}$:

$$bb_j(x) \;=\; \sum_{\nu=1}^{s} v_{j\nu}(x)\,p_\nu(x) \quad \forall\, bb_j \in \mathcal{B}\,. \tag{8.39}$$

If the bb_j are determined by iterated linear combination from the original system P, the determination of the coefficients $v_{j\nu}$ in (8.39) requires simply a bookkeeping in the procedure by which the border basis $\mathcal{B}$ is determined. Unfortunately, current computer algebra systems will not furnish that bookkeeping, not even for a Groebner basis computation, but it is clear that it can easily be implemented. If the complete intersection basis is a *subset* of the border basis, as in Example 8.13 above, (8.39) requires that the border basis elements not used are represented by the complete intersection basis.

From (8.16) and (8.39), the expansion (8.37) is then immediately obtained:

$$\begin{aligned}p(x) \;&=\; \mathrm{NF}[p] + \textstyle\sum_j q_j(x)\,bb_j(x) \;=\; d_0(x) + \sum_j q_j(x) \sum_\nu v_{j\nu}(x)\; p_\nu(x)\\ &=\; d_0(x) + \textstyle\sum_\nu \;(\sum_j q_j(x)\,v_{j\nu}(x))\; p_\nu(x)\,.\end{aligned} \tag{8.40}$$

Thus, an implementation of (8.37) and the more detailed expansions which may be further derived from it meets no principal difficulties if a normal set and border basis algorithm with

sufficient bookkeeping is available. Normal set and border basis algorithms will be further discussed in later sections; cf. also section 8.4.4 for the special case of Groebner bases.

In section 5.1.3, we have "expanded" a polynomial $p \in \mathcal{P}^1$ in powers of a specified polynomial s; cf. Proposition 5.3 and (5.18). This expansion is a generalization of the Taylor expansion of p; truncated copies of the expansion furnish higher order approximations simultaneously in the vicinity of *all* zeros of s (or $\langle s \rangle$). Equation (8.38) is the multivariate counterpart of (5.18):

Proposition 8.27. In the situation of Theorem 8.25, let the zero set $Z[\mathcal{I}] \subset \mathbb{C}^s$ consist of m simple zeros. Let $r_k \in \mathcal{P}^s$ be the remainder of the expansion (8.38) truncated after the k-th order terms. Then all derivatives of r_k of an order $\leq k$ vanish at each point $z_\mu \in Z[\mathcal{I}]$.

Proof: The proof follows immediately from the fact that each p_ν vanishes at each z_μ. □

Example 8.16, continued: $r_1 = bb_1^2 - bb_2\, bb_3$; the Taylor expansion of r_1 at the zero (1,2,0) of $\mathcal{I}$ is, for example,

$$r_1(x, y, z) \;=\; -\tfrac{144}{49}\,(x-1)^2 + \tfrac{32}{49}\,(x-1)(y-2) - \tfrac{114}{49}\,(x-1)z + \tfrac{69}{49}\,(y-2)^2 - \tfrac{167}{49}\,(y-2)z + \tfrac{103}{49}\,z^2\,.$$

Thus the linear part of the expansion of p at the end of Example 8.16 is a good approximation of p simultaneously at each of the 4 zeros of the ideal. □

8.3.4 Number of Zeros of a Complete Intersection System

A strict upper bound for the number of zeros (counting multiplicities) of a regular multivariate polynomial system has been known for a long time:

Proposition 8.28 (Bézout). For a regular system $P = \{p_\nu \in \mathcal{P}^s,\ \nu = 1(1)s\},\ d_\nu := \deg\, p_\nu$, the potential number of zeros is bounded by

$$m_{\text{Bézout}} \;=\; \prod_{\nu=1}^{s} d_\nu\,. \tag{8.41}$$

It is well known (cf., e.g., [2.11]) that the bound (8.41) is assumed if all p_ν are generic and *dense*, i.e. if they contain all terms of total degree $\leq d_\nu$. But most polynomial systems are extremely *sparse*; for such systems, the actual number of zeros may be considerably smaller than $m_{\text{Bézout}}$, perhaps by an order of magnitude. That it is the presence of the high degree monomials which determines the true number of zeros is obvious from the simplest examples: Two generic quadratic equations in two variables have 4 zeros, but the two quadratic equations

$$\alpha_{11}^{(\nu)}\, x\, y + \alpha_{10}^{(\nu)}\, x + \alpha_{01}^{(\nu)}\, y + \alpha_{00}^{(\nu)} \;=\; 0\,, \qquad \nu = 1, 2\,,$$

can only have two zeros because we may readily elminate the xy-term from one of the equations which leaves us with a quadratic and a linear equation.

Fortunately, there exists a bound on the number m of zeros which takes into account the sparsity structure of the p_ν. It is associated with the names of Bernstein, Khovanski, and Kushnirenko, and with terms like "Newton polytopes" and "mixed volumes"; in this text, it will be denoted as BKK-bound. Although its formal specification is rather straightforward, its

concise derivation and its computation for $s > 2$ are rather complicated. Therefore, we will not formulate an explicit expression for the BKK-bound but rather explain its meaning and use. A more thorough introduction (which still avoids unnecessary mathematical technicalities) may be found in Chapter 7 of [2.11] which also contains references to the original literature about the subject.

In 2002, a procedure for the evaluation of the BKK-bound was not yet available in either Maple 7 or in Mathematica 4. However, there are some special packages which serve that purpose, e.g., PHC pack by J.Verschelde ([8.5]). In any case, in this introductory report, we assume that it is possible to retrieve the value BKK(P) of the BKK-bound for a specified regular system P of polynomial equations. Naturally, the computational effort increases with the number s of variables and the degrees d_ν of the polynomials.

What is the meaning of the integer number BKK(P) which is generated by a BKK-bound algorithm? Consider the system

$$P \;=\; \{p_\nu,\ \nu = 1(1)s\} \subset (\mathcal{P}^s)^s\ ,\ \text{with } p_\nu(x) = \sum_{j \in J_\nu} \alpha_j^{(\nu)} x^j,\ \alpha_j^{(\nu)} \in \mathbb{C},\ \nu = 1(1)s\ .$$

For *fixed supports* J_ν, almost all instantiations of the coefficients lead to the same number m of isolated zeros z_μ (counting multiplicities) of P; thus m is invariant and independent of the particular coefficient values for large regions of the data space $\mathcal{A}$ of P which is determined by the support J_ν, $\nu = 1(1)s$. The BKK-bound BKK(P) is *equal* to this number m of zeros which prevails for almost all coefficient values in $\mathcal{A}$ or—as it is often expressed—for "generic coefficients." Moreover, it is the *maximal* number of isolated zeros which can occur for a system with the supports J_ν.

Only for coefficient values from some lower-dimensional manifold in $\mathcal{A}$, the actual number of zeros may be smaller than BKK(P), or there may exist a zero manifold. That a zero which exists for generic coefficients may *disappear* for a particular instantiation of the coefficients is well known: A generic linear system $A\,x = b$ has 1 zero; this zero disappears when the coefficient matrix A is singular and the right-hand side b not in the image space of A. Actually, the zero moves towards ∞ as the coefficients move towards values for which the system is inconsistent. A trivial nonlinear example is $p_1(x, y) = (x - \alpha_1)(y - \beta_1) - 1,\ \ p_2(x, y) = (x-\alpha_2)(y-\beta_2)+1$. For generic α_ν, β_ν, there are 2 zeros, in agreement with BKK($\{p_1, p_2\}$) = 2. For $\alpha_2 \to \alpha_1$, one of the zeros disappears to ∞; the other one follows as $\beta_2 \to \beta_1$ and the system has become inconsistent. Polynomial systems with "diverging zeros" will be considered in section 9.5.

All this applies with the important reservation that the BKK-bound does not always count a simple or multiple zero with one or several components 0 ! This may happen when one or several of the p_ν possess *no constant term*. That such a reservation is necessary is explained by the observation that the BKK-bound is invariant against multiplication of the p_ν by monomials: It is obvious that such multiplications will generally introduce further zeros, at 0 or with some zero components.

Fortunately, there is a simple trick to get rid of this deficiency; it was proposed by T. Y. Li: As we have seen in section 8.3.2, the zeros of a regular polynomial system are continuous functions of the coefficients of the p_ν and hence of their constant terms. This remains valid when a constant term happens to vanish as long as there is a *generic* constant term in each equation.

Thus, the BKK-bound gives the correct number of zeros, independently of their location in the finite $\mathbb{C}^s$, when we append a generic constant term to the p_ν with $\alpha_0^{(\nu)} = 0$. When this is done after multiplication of the p_ν by monomials, the BKK-bound is no longer invariant against such multiplications.

Example 8.17 (from [2.11]): In $\mathcal{P}^2$, consider the very sparse system with generic coefficients

$$P(x,y) = \left\{ \begin{array}{rcl} p_1(x,y) & = & \alpha_{32}^{(1)} x^3y^2 + \alpha_{02}^{(1)} y^2 + \alpha_{10}^{(1)} x + \alpha_{00}^{(1)} \\ p_2(x,y) & = & \alpha_{14}^{(2)} x\, y^4 + \alpha_{30}^{(2)} x^3 + \alpha_{01}^{(2)} y \end{array} \right\} = 0. \tag{8.42}$$

Upon input of the supports of p_1 and p_2, a BKK-package delivers $\mathrm{BKK}(\{p_1, p_2\}) = 18$. Since p_2 does not contain a constant term, this value may not include some zero with a vanishing component. However, it is easily seen that, for p_2, the vanishing of one zero component would imply that of the other one, which is incompatible with p_1. Accordingly, $\mathrm{BKK}(\{p_1, p_2 + \alpha_{00}^{(2)}\})$ has the same value 18.

This value is also generated for $\mathrm{BKK}(\{p_1, x\, p_2\})$ and for $\mathrm{BKK}(\{y\, p_1, x\, p_2\})$, although the actual number of zeros for these systems is 20 and 24, respectively. The correct values are now obtained from $\mathrm{BKK}(\{p_1, x\, p_2 + \alpha_{00}^{(2)}\})$ and $\mathrm{BKK}(\{y\, p_1 + \beta_{00}^{(1)}, x\, p_2 + \alpha_{00}^{(2)}\})$. The additional zeros with zero components are easily spotted: $\{p_1, x\, p_2\}$ inherits all zeros from P and it has the additional zeros $(0, \pm\sqrt{-\alpha_{00}^{(1)}/\alpha_{02}^{(1)}})$. $\{y\, p_1, x\, p_2\}$ has a further zero at $(0,0)$; this is a 4-fold zero because the first three partial x-derivatives also vanish at $(0,0)$. With a nonzero constant term, this zero splits into 4 isolated zeros .

Note that the Bézout numbers (8.41) for the above systems are 25, 30, and 36, resp., which are rather misleading values. □

For a superficial explanation of how $\mathrm{BKK}(P)$ is *defined*, we must introduce the following notion:

Definition 8.10. In $\mathbb{N}_0^s$, the grid of nonnegative integer s-tuples, consider the set of the $j \in J$, the support of $p \in \mathcal{P}^s$. The *convex hull* of this set is the *Newton polytope* of p :

$$\mathrm{NP}(p) := \mathcal{C}\{j \in J\} \subset \mathbb{R}^s . \tag{8.43}$$

Due to its convexity, the Newton polytope of a multivariate polynomial $p \in \mathcal{P}^s$ reflects the sparsity of p in a very special way: Only those monomials x^j whose exponent j generates a *corner* of $\mathrm{NP}(p)$ are essential for the shape of the polytope. Exponents $k \in \mathbb{N}_0^s$ which lie on a *face* or in the *interior* of $\mathrm{NP}(p)$ are irrelevant; the presence or absence of these exponents does not influence the position and shape of $\mathrm{NP}(p)$. Since we will see below that $\mathrm{BKK}(P)$ is exclusively determined by the Newton polytopes $\mathrm{NP}(p_\nu)$, $\nu = 1(1)s$, this implies that the number of zeros of an s-variate polynomial system $\{p_\nu, \nu = 1(1)s\}$ depends only on the presence of certain distinguished monomials in each p_ν while the presence or absence of the remaining terms is irrelevant for the number of zeros (with the exception of some special instantiations of the coefficients).

Example 8.17, continued: Figure 8.4 shows the Newton polytopes of the two polynomials P_1, p_2 in (8.42) and of the polynomials $y\, p_1$ and $x\, p_2$. With p_1, p_2 of (8.42), all terms contribute to the definition of $\mathrm{NP}(p_1)$ and $\mathrm{NP}(p_2)$, resp.; cf. Figure 8.4. Additional terms with the monomials y, xy, x^2y in p_1 would not affect $\mathrm{NP}(p_1)$. The addition of a constant term to p_2 does affect

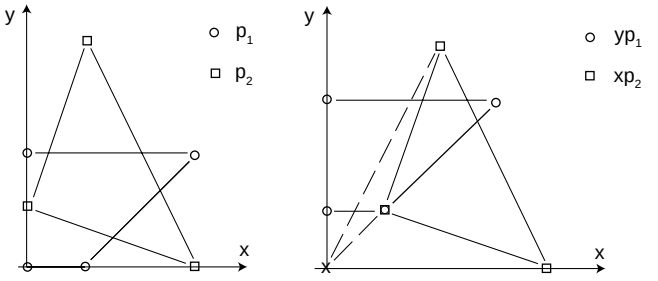

Figure 8.4.

NP(p_2), but it turns out that the BKK-bound is not affected. The addition of constant terms to $x\ p_2$ and to $y\ p_1$ affects the Newton polytopes of these polynomials, and this change is reflected by the BKK-bound as it should be; cf. above. □

For a set of s polytopes $P_\sigma,\ \sigma = 1(1)s$, with corners in $\mathbb{N}_0^s$ (so-called lattice polytopes), a mapping

$$\text{MV}: \quad P_1, \ldots, P_s \ \rightarrow \ \mathbb{Z}_0$$

to the nonnegative integers has been defined which is called the *mixed volume* of $P_1, \ldots, P_s$; it is a symmetric function of its arguments. This function defines the BKK-bound :

$$\text{BKK}(\{p_1, \ldots, p_s\}) \ := \ \text{MV}\ (\text{NP}(p_1), \ldots, \text{NP}(p_s))\ . \tag{8.44}$$

We refrain from giving a formal definition of the function MV and point the reader once more to the explanations in [2.11]. Since a mixed volume is only defined for s lattice polytopes in N_0^s, the BKK-bound is only defined for a system of s polynomials in $\mathcal{P}^s$, i.e. for a regular system. When a 0-dimensional ideal in $\mathcal{P}^s$ is defined by more than s polynomials, the number of its zeros cannot be determined by (8.44). This is natural because BKK(P) depends only on the *support* of P and an overdetermined system is inconsistent for almost all instantiations of its coefficients.

The number $m\ =$ BKK(P) of zeros of P equals the dimension of the quotient ring $\mathcal{R}[\langle P\rangle]$; thus, the knowledge of m puts the elements of the set $\mathcal{T}^s(m)$ (cf. Definition 2.18) at our disposal for a basis of $\mathcal{R}[\langle P\rangle]$. There are two potential reasons why some particular normal set $\mathcal{N} \in \mathcal{T}^s(m)$ may not be feasible for the specified system P :

(i) $\mathcal{N}$ contains the complete support of one or more of the p_ν; this would imply $p_\nu \in \mathcal{R}[\langle P\rangle]$ which is a contradiction.

(ii) For a basis $\mathbf{c}^T$ of the dual space $\mathcal{D}[\langle P\rangle]$, the matrix $\mathbf{c}^T(\mathbf{b})$ is singular; cf. Proposition 2.12.

Condition (i) may easily be checked; it may exclude various sets $\mathcal{N} \in \mathcal{T}^s(m)$ for *all* systems with a particular support structure. Condition (ii), on the other hand, cannot be checked a priori when we do not know the zeros of P. Also, $\mathbf{c}^T(\mathbf{b})$ will generally not be singular for all P of a given support structure but only when their coefficients lie on some manifold in the data space. Therefore, an algorithm for the determination of a normal set basis vector $\mathbf{b}(x)$ for $\mathcal{R}[\langle P\rangle]$ can comply with (i) but must rely on intermediate numerical results for compliance

with (ii). This is also true for the exceptional case that BKK(P) is not the correct dimension of $\mathcal{R}[\langle P\rangle]$; cf. the remarks above.

Example 8.18: Consider the three systems $\{p_1,\ p_2\}$, $\{p_1,\ x\ p_2\}$, $\{y\ p_1,\ x\ p_2\}$ of Example 8.17, with $m = 18,\ 20,\ 24$, respectively. When we consider "nice" normal sets for (8.42), we may try the 16 monomials $x^{j_1}y^{j_2}$, $0 \le j_1, j_2 \le 3$, and two further ones, say $x^5,\ y^5$. But this $\mathcal{N}$ would contain the full support of p_1 and is therefore not admissible.

In another attempt, we could choose the 15 monomials $x^{j_1}y^{j_2}$, $0 \le j_1 + j_2 \le 4$, and look for 3 further ones: Among the monomials of total degree 5, we have to avoid x^3y^2 and $x\ y^4$, but we could take $y^5,\ x^2y^3,\ x^4y$ and obtain a satisfactory normal set.

Composing a normal set for $\{p_1,\ x\ p_2\}$ in the same fashion, we can now include all degree 5 monomials except x^3y^2 which provides the requested 20 basis elements. For $\{y\ p_1,\ x\ p_2\}$, we can begin with the 21 monomials of total degree ≤ 5 and avoid $x^3y^3,\ x^2y^4$ in choosing 3 further monomials. □

Example 8.19: Consider a generic dense system in $(\mathcal{P}^s)^s$, with all polynomials of total degree d. Here the BKK-bound agrees with the Bézout bound d^s. The "hypercube" normal set $\mathcal{N} = \{x^j,\ \|j\|_{\max} \le d-1\}$ is in $\mathcal{T}^s(d^s)$ and not excluded by (i). □

The compliance with (i) generally excludes only a small part of the wide variety of sets in $\mathcal{T}^s(m)$ as potential normal sets for some specified P.

Exercises

1. Consider the ideal $\mathcal{I} \in \mathcal{P}^3(8)$ whose zero set Z consists of the 8 corners of the unit cube in $\mathbb{R}^3$.

(a) Find a simple separating functional for Z. By the construction in the proof of Theorem 8.18, design a 3-element basis P for $\mathcal{I}$. What are the degrees of the 3 polynomials in P and hence the Bézout number of P.

(b) Obviously, there are several pairs of planes in $\mathbb{R}^3$ which contain all points of Z. By an appropriate selection of three such pairs, compose a basis for $\mathcal{I}$ consisting of 3 quadratic equations.

(c) Choose some polynomial in $\mathcal{P}_4^3$ and form its expansion (8.38) in terms of the quadratic complete intersection system found in (b).

2. Design pairs (p_1, p_2) of quadratic polynomials in $\mathcal{P}^2$ such that their common zeros have various condition properties with respect to changes in the coefficients.

(a) Use the manifolds $p_\nu = 0$ in the x, y-plane to find pairs whose 4 zeros are well-conditioned. Check by forming the singular values of P' at the zeros. Find a pair with 4 well-conditioned complex zeros.

(b) In the same fashion, find pairs with ill-conditioned zeros and verify via P'. Can you make all 4 zeros very ill conditioned? Find changes of the coefficients which display the ill-conditioning fully.

3. With a software package for the computation of the BKK-bound, find experimentally how the generic presence of certain terms in a specified polynomial system in $(\mathcal{P}^s)^s$, $s = 2$ and 3, influences the number of zeros of that system. Compare with the Bézout number for the same system.

8.4 Groebner Bases

In virtually all texts on constructive polynomial algebra, Groebner bases play a central role, both as the standard representation of polynomial ideals and as a tool for performing various tasks with polynomial ideals; cf., e.g., [2.10] and many others. In section 2.5.3, we have indicated why we have not followed that path in this book; the reader should refer to these explanations now.

On the other hand, powerful software for the determination of Groebner bases for polynomial systems with *rational* coefficients is available in Maple and Mathematica, and in practically all more specialized computer algebra systems. Software for general border bases is—at this time—still restricted to local developments. Therefore, Groebner bases often present the only available access to some computational task and it is important to have a clear view of their characterization, their potential, and their shortcomings. This section is devoted to this objective.

8.4.1 Term Order and Order-Based Reduction

A term order specifies a strict sequential order in the infinite set $\mathcal{T}^s$ of all monomials or terms x^j in s variables.

Definition 8.11. A linear order $\prec$ in the set $\mathcal{T}^s$, $s \geq 1$, which is compatible with multiplication so that

$$x^{j_1} \prec x^{j_2} \quad \Longrightarrow \quad x^j\, x^{j_1} \prec x^j\, x^{j_2}\,, \quad \forall\, j \in \mathbb{N}^s\,, \tag{8.45}$$

and for which $1 = x^0$ is the first ("lowest") element, is called a *term order*. Naturally, $x^{j_2} \succ x^{j_1}$ is synonymous with $x^{j_1} \prec x^{j_2}$. □

In $\mathcal{T}^1$, $1 \prec x \prec x^2 \prec x^3 \prec \ldots$ is the only possible term order. For $s > 1$, there are a few widely used choices:

Definition 8.12. Assume that we have specified a linear order between the components x_σ of $x = (x_1, \ldots, x_s)$ and numbered them such that $1 \prec x_s \prec x_{s-1} \prec \ldots \prec x_2 \prec x_1$; further assume that we write the elements in $\mathcal{T}^s$ as $x_1^{j_1} \ldots x_s^{j_s}$:

(1) the *lexicographic* order $\prec_{lex}$ is defined by

$x^j \prec_{lex} x^k$ if either $j_1 < k_1$ or $j_\sigma = k_\sigma$ for $\sigma = 1(1)\bar{s} - 1$ and $j_{\bar{s}} < k_{\bar{s}}$;

(2) the *graded lexicographic* orders $\prec_{glex}$ and $\prec_{grevlex}$ are defined by

$x^j \prec_{g(rev)lex} x^k$ if either (total) $\deg(x^j) < \deg(x^k)$ or the total degrees are equal and $x^j \prec_{(rev)lex} x^k$; here, $x^j \prec_{revlex} x^k$ if either $j_s > k_s$ or $j_\sigma = k_\sigma$ for $\sigma = s(-1)\bar{s} + 1$ and $j_{\bar{s}} > k_{\bar{s}}$. □

For equal total degrees, the graded lexicographic orders can also be characterized by

$$x^j \quad \begin{matrix} \prec_{glex} \\ \prec_{grevlex} \end{matrix} \quad x^k \quad \text{if the} \quad \begin{matrix} \text{"leftmost"} \\ \text{"rightmost"} \end{matrix} \quad \text{nonvanishing component of } k - j \text{ is} \quad \begin{matrix} \text{positive} \\ \text{negative} \end{matrix}\,.$$

Maple implements the *lex* order, with the notation `plex` ("pure lexicographic"), and the *grevlex* order, with `tdeg` ("total degree") and as a *default*. This is also the order which will most

often be used in this book. Note that the reverse lexicographic order without a superimposed degree ordering would not satisfy $1 \prec x_\sigma$. There exist abstract definitions of a term order which admit further possibilities, but they will be of no concern in our context.

Example 8.20: For the lexicographic order, we have, e.g., $x_1^3 x_2 x_3^3 \succ_{lex} x_1^2 x_2^4 x_3^2$, or $x_1^3 x_2 x_3^2 \succ_{lex} x_1^3 x_3^3$, etc.

For the *grevlex* order, we have, e.g., $x_1^3 x_2 x_3^3 \prec_{grevlex} x_1^2 x_2^4 x_3^2$ but $x_1^3 x_2 x_3^2 \succ_{grevlex} x_1^3 x_3^3$ though for a different reason than in the *lex* order. □

A term order defines a linear order in the terms of a multivariate polynomial by the order of their monomials. In particular, there is now a well-defined *leading term* in each polynomial in $\mathcal{P}^s$:

Definition 8.13. Consider $p(x) = \sum_{j \in J} \alpha_{j_1 .. j_s} x_1^{j_1} \dots x_s^{j_s} \in \mathcal{P}^s$. With respect to some specified term order $\prec$, the term $\alpha_k x^k$ with $x^j \prec x^k$ for all $j \in J,\ j \neq k$, is the *$\prec$-leading term* (l.t.) of p, with the *$\prec$-leading coefficient* (l.c.) α_k and the *$\prec$-leading monomial* (l.m.) x^k. If it is evident or irrelevant which order is referred to, we will also say *order-leading term, etc.* or simply leading term, etc. □

Example 8.20, continued: For a univariate polynomial, the leading term is always the one with the highest power of the variable. In $p(x) = 2\, x_1^3 x_2 x_3^3 - 3\, x_1^2 x_2^4 x_3^2 \in \mathcal{P}^3$, for *grevlex* order, the leading term is the second one, with a leading coefficient -3; for *lex* order, the leading term is the first one, with leading coefficient 2. □

The definition of leading monomials permits the introduction of an order-based *reduction procedure* for multivariate polynomials: In $\mathcal{P}^1$, when we divide $p(x)$ of degree n by $s(x)$ of degree $m \leq n$, we form (cf. (5.41) in section 5.3)

$$r_1(x) := p(x) - \frac{l.t.(p)}{l.t.(s)} \cdot s(x) \tag{8.46}$$

and know that $\deg r_1 < \deg p$. We continue this procedure with the successive remainders r_λ until $\deg r_\ell < \deg s$; then r_ℓ is the unique *remainder* of the division and the accumulated factors of s in (8.46) compose the *quotient* q. The procedure must terminate because the degree of the remainder decreases in each step. In terms of the ideal $\langle s \rangle$ and its quotient ring spanned by $\{1, x, \dots, x^{m-1}\}$, this procedure can also be interpreted as the reduction of p to $\mathrm{NF}_{\langle s \rangle}[p] = r_\ell$.

In $\mathcal{P}^n,\ n > 1$, with a specified term order, assume that the order-l.m. of the divisor polynomial s divides the order-l.m. of the dividend polynomial p. Then we can perform the same reduction step (8.46); again we can be sure that $\mathrm{l.m.}(r_1) \prec \mathrm{l.m.}(p)$, which is now not simply a consequence of a diminished degree. Naturally, our initial assumption may cease to hold after one or few steps.

But when l.m.(s) not or no longer divides l.m.(r_ℓ), it may still divide other terms in r_ℓ. If we reduce such terms in the same fashion, in the sequence of their term order, we will arrive at a polynomial r none of whose terms are divisible by l.m.(s). This r is the result of the *reduction of p by s* with respect to the term order $\prec$, which is often denoted by

$$p \xrightarrow{s} r\ ;$$

if the term order is important, it should be denoted explicitly.

Proposition 8.29. For a specified term order, the result r of the reduction $p \xrightarrow{s} r$ in $\mathcal{P}^n$ is uniquely defined. A polynomial p is irreducible by s, with l.m.$(s) = x^k$, iff none of the monomials x^j in p satisfy $j \geq k$, where $\geq$ is the componentwise partial order in $\mathbb{N}_0^s$.

Proof: Assume that p could also be reduced to r'; then r and r' must differ by a multiple of s : $r' = r + q \cdot s$. Clearly, $q\,s$ contains terms which are divisible by l.m.(s), e.g., the term l.t.$(q)\cdot$ l.t.(s) which cannot cancel in $q\,s$. Thus, r' cannot be the result of the reduction of p by s. The observation about the irreducibility is obvious. □

If $x^k =$ l.m.(s), all other monomials x^j in s must satisfy $x^j \prec x^k$. For the `tdeg` order $\prec_{grevlex}$, this means that either their total degree is smaller than $|k|$, or—if it is equal—$x^j \prec_{revlex} x^k$. Note that each exponent $k \in \mathbb{N}^s$ separates the grid hyperplane $|j| := \sum_{\sigma=1}^{s} j_\sigma = |k|$ into three disjoint sets: $\{x^j \prec_{revlex} x^k\}$, $\{x^j \succ_{revlex} x^k\}$, $\{x^k\}$; cf. Figure 8.5.

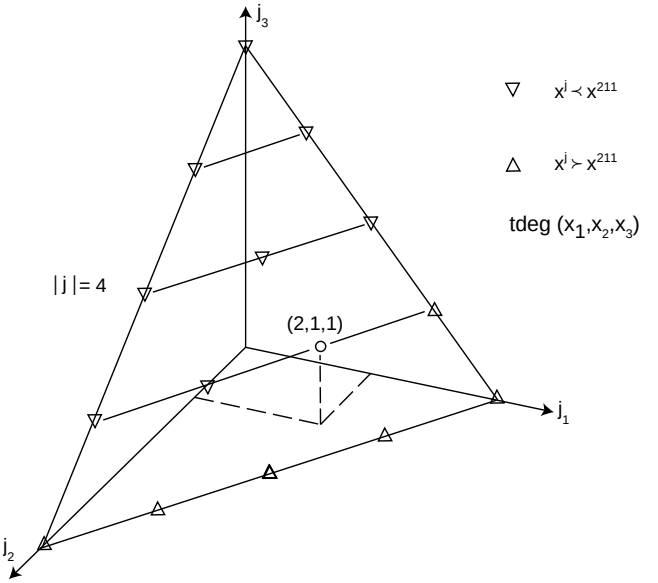

Figure 8.5.

Now consider a set $S = \{s_1, \ldots, s_n\} \subset (\mathcal{P}^s)^n$, $n > 1$, of divisor polynomials and define order-reduction by S as successive order-reduction by any one of the s_ν. The potential for reduction is now strongly increased, but it turns out that the result of the reduction need no longer be unique: It may happen that there exist polynomials $\bar{s}(x) = \sum_{\nu=1}^{n} q_\nu\, s_\nu \neq 0$ which are irreducible by any one of the s_ν. Then $r(x)$ and $r'(x) = r(x) + \bar{s}(x)$ may both be S-reduced forms of p. A simple example (from [2.10]) is the following:

Example 8.21: In $\mathcal{P}^2$, let $p(x, y) = x^2y + xy^2 + y^2$, $S = \{s_1, s_2\}$ with $s_1(x, y) = xy - 1$, $s_2(x, y) = y^2 - 1$. With `tdeg` order,

$$p \;=\; x^2y + xy^2 + y^2 \quad \begin{cases} \xrightarrow{s_1} \quad x + y + y^2 \quad \xrightarrow{s_2} \quad x + y + 1 \quad =: r\,, \\ \xrightarrow{s_2} \quad x^2y + x + 1 \quad \xrightarrow{s_1} \quad 2\,x + 1 \quad =: r'\,. \end{cases}$$

Obviously, both r and r' are irreducible by S, and so is $\bar{s} = r' - r = x - y$. □

On the other hand, the normal form computation discussed in section 8.2.1 is a reduction very much like our present reduction procedure for the divisor set $\mathcal{B} = \{ bb_j \}$, with their $\mathcal{N}$-leading monomials x^j not defined by a term order but by $x^j \in B[\mathcal{N}]$. There, the result of the reduction, viz. $\mathrm{NF}_{\langle \mathcal{B} \rangle}[p]$, has been unique. We had also observed that the elements bb_j of a border basis $\mathcal{B}$ must satisfy a large number of constraints; cf. section 8.2.2. This suggests that—in the present setting with a term order—the polynomials $s_\nu \in S$ also have to satisfy *constraints* if the reduction by S is to be unique.

8.4.2 Groebner Bases

Can we have a normal set $\mathcal{N}$ and associated border basis elements whose $\mathcal{N}$-leading monomials x^k are also their order-leading monomials with respect to some specified term order $\prec$? At first sight, this appears to require that $x^j \prec x^k$ for each $x^j \in \mathcal{N}$ and $x^k \in B[\mathcal{N}]$.

Definition 8.14. The *generic normal set* $\mathcal{N}_\prec$ of m elements in s variables for a specified term order $\prec$ is the set of the m $\prec$-lowest elements in $\mathcal{T}^s$. □

Example 8.22: Consider $s = 3$ and $m = 7$. For $\prec_{grevlex}$, we have $\mathcal{N}_\prec = \{1, x_3, x_2, x_1, x_3^2, x_2x_3, x_1x_3\}$ while $glex$ generates the slightly different generic normal set $\{1, x_3, x_2, x_1, x_3^2, x_2x_3, x_2^2\}$. For $\prec_{lex}$, we obtain the univariate generic normal set $\{1, x_3, x_3^2, x_3^3, x_3^4, x_3^5, x_3^6\}$. Generic lexicographic normal sets are always univariate which exhibits why the lexicographic order is inferior to a graded order in many respects.

The *symmetric* normal set $\mathcal{N}_{symm} = \{1, x_3, x_2, x_1, x_2x_3, x_1x_3, x_1x_2\}$ (cf. Example 8.1) cannot be generic for *any* term order since this would require $x_2x_3 \prec x_3^2$ and $x_2x_3 \prec x_2^2$, but neither $x_2 \prec x_3$ nor $x_3 \prec x_2$ can support both relations if $\prec$ is compatible with multiplication. □

Definition 8.15. The border basis $\mathcal{B}_\mathcal{N} = \{bb_k(x)\}$ for the normal set $\mathcal{N}$ is *order-compatible* for a specified term order $\prec$ iff

$$\mathcal{N}\text{-leading monomial of } bb_k \;=\; \prec\text{-leading monomial of } bb_k \quad \forall\, bb_k \in \mathcal{B}_\mathcal{N}\,. \quad \square \qquad (8.47)$$

For the generic normal set $\mathcal{N}_\prec \in \mathcal{T}^s(m)$ of some term order, a border basis is automatically order compatible; cf. Definition 8.14. For a nongeneric normal set $\mathcal{N} \in \mathcal{T}^s(m)$, compatibility with a specified term order can be obtained iff those monomials from $\mathcal{N}$ which succeed the $\mathcal{N}$-leading monomial of some bb_k *do not occur* in bb_k.

Example 8.22, continued: Consider the symmetric normal set $\mathcal{N}_{symm}$ and *grevlex* order. Of the monomials in $B[\mathcal{N}_{symm}]$, x_3^2 precedes x_2x_3, x_1x_3, x_1x_2 and x_2^2 precedes x_1x_2. Thus, in order to satisfy (8.47), bb_{002} must have no further quadratic terms at all and bb_{020} must not contain a term with x_1x_2. (We will see later that this corresponds to certain degeneracies in the zero set $Z[P]$ of the system P.) □

In principle, *each* normal set in $\mathcal{T}^s(m)$ can support an order-compatible border basis for a specified term order, if the corresponding restrictions on the occurrence of coefficients in the bb_k are met. These restrictions imposed by order compatibility are independent of the intrinsic restrictions which we have derived in section 8.2.3 and supplementary to them. Thus, the

specification and use of a term order *restricts* the liberty in representing a polynomial ideal for computational purposes. Actually, for a specified term order, the restriction imposed by (8.47) admits only *one uniquely defined*[14] border basis for the ideal of a regular polynomial system:

Theorem 8.30. For a 0-dimensional polynomial system $P \subset (\mathcal{P}^s)^s$ and a specified term order $\prec$, there exists a unique $\prec$-compatible border basis $\mathcal{B}[\langle P\rangle]$.

Proof: Since the unique existence of a Groebner basis (cf. Definition 8.16 below) has been proved in different ways and is a well-known fact, we give only an intuitive survey of a proof.

Assume at first that the generic normal set C for the specified term order is a feasible monomial basis for $\mathcal{R}[\langle P\rangle]$. As we have just observed, the border basis $\mathcal{B}_{\mathcal{N}_\prec}[\langle P\rangle]$ is automatically order-compatible. There cannot exist an order-compatible border basis for a different normal set: This normal set would have to include (at least) one of the leading monomials of $\mathcal{B}_{\mathcal{N}_\prec}[\langle P\rangle]$, say x^k, and a monomial x^j of $\mathcal{N}_\prec$ would now function as leading monomial. But this requires that x^j was present in the border basis element bb_k which implies that x^k is present in the new border basis element bb_j, which contradicts the term order.

Now assume that $\mathcal{N}_\prec$ is not a feasible normal set for $\mathcal{R}[\langle P\rangle]$. We form new normal sets by successively replacing a monomial of highest term order in the edge of $\mathcal{N}_\prec$ by a lowest order monomial in the previous border set (respecting the closedness of the result, of course). Since almost all sets in $\mathcal{T}^s(m)$ are feasible normal sets for a specified system P, we must reach a feasible normal set after finitely many steps. Assume that the replacement of *one* element from $\partial\mathcal{N}_\prec$ (the highest one in term order) by the lowest order monomial in $B[\mathcal{N}_\prec]$ is sufficient. This means that the violation of the feasibility of $\mathcal{N}_\prec$ has been caused only by the removed monomial $x^{k_m} = b_m(x) \in \mathcal{N}_\prec$ which implies

$$b_m(z_\mu) \;\in\; \text{span}\,\{b_1(z_\mu), \ldots, b_{m-1}(z_\mu)\}\,, \qquad \text{for all } z_\mu \in Z[P]\,,$$

and the existence of coefficients $\beta_{m\mu}$ such that

$$\text{NF}_{\langle P\rangle}[b_m(x)] \;=\; \sum_{\mu=1}^{m-1} \beta_{m\mu}\, b_\mu(x)\,.$$

Thus, in the border basis for the modified normal set $\mathcal{N}$, the border basis element with the $\mathcal{N}$-leading monomial b_m (which is now in $B[\mathcal{N}]$) contains only monomials $b_\mu \prec b_m$ but *not* the monomial $b_{m+1} \succ b_m$ incorporated into $\mathcal{N}$ in place of b_m. Thus the $\mathcal{N}$-border basis is order compatible. Reversely, this argument shows how the vanishing of the coefficient of b_{m+1} in the border basis element with the $\mathcal{N}$-leading monomial b_m implies that the previous normal set cannot have been feasible; this establishes uniqueness. □

Definition 8.16. For a specified term order $\prec$, the unique $\prec$-compatible border basis $\mathcal{B}[\langle P\rangle]$ is called the *border Groebner basis* $\mathcal{G}_\prec[\langle P\rangle]$ of $\langle P\rangle$. (The subscript on $\mathcal{G}$ will be omitted if the order is evident.) □

Example 8.23: Consider the two quadratic polynomials in 2 variables which describe two

[14] Here and in the following, *uniqueness* always refers to some *normalized* form of the polynomials, e.g., with the coefficient 1 in the $\mathcal{N}$-leading term.

axiparallel ellipses:

$$P := \begin{cases} p_1(x,y) &= x^2 + 4\,y^2 - 4\,; \\ p_2(x,y) &= 9\,x^2 + y^2 - 2\,y - 8\,. \end{cases}$$

Obviously, $m = 4$, and the generic normal set for `tdeg` (with $x \succ y$) is $\mathcal{N}_\prec = \{1, y, x, y^2\}$. But the 4 zeros of P form two pairs with equal y-components (and two pairs with equal x-components), which makes $\mathcal{N}_\prec$ infeasible as may easily be verified. When we replace y^2 by the lowest monomial xy in $B[\mathcal{N}_\prec]$, we obtain the normal set $\mathcal{N} = \{1, y, x, xy\}$, with $B[\mathcal{N}] = \{y^2, x^2, xy^2, x^2y\}$. It is easily checked that the feasibility of this normal set is not impaired by the symmetries of the zeros. By the argument in the proof of Theorem 8.30, the border basis $\mathcal{B}_\mathcal{N}[P]$ should be order compatible.

Solving for $x^2,\ y^2$ in P yields

$$bb_{20}(x,y) \;=\; x^2 - \tfrac{8}{35}\,y - \tfrac{5}{4}\,, \qquad bb_{02}(x,y) \;=\; y^2 + \tfrac{2}{35}\,y - \tfrac{5}{4}\,;$$

substitution of bb_{02} into $y\,bb_{20}$ and $x\,bb_{02}$ yield

$$bb_{21}(x,y) \;=\; x^2y - \tfrac{6061}{4900}\,y - \tfrac{2}{7}\,, \qquad bb_{12}(x,y) \;=\; xy^2 + \tfrac{2}{35}\,xy - \tfrac{5}{4}\,x\,.$$

The critical border basis element is b_{02} with the $\mathcal{N}$-leading monomial y^2; it must not contain the monomial $xy \succ y^2$. Since this is the case, the above $\mathcal{B}_\mathcal{N}[\langle P\rangle]$ is indeed order compatible and thus the border Groebner basis $\mathcal{G}_\prec[\langle P\rangle]$. □

The order-compatibility of a border Groebner basis has the following important consequence:

Theorem 8.31. Let $\mathcal{N}$ be the normal set associated with the border Groebner basis $\mathcal{G}[\langle P\rangle]$ for some specified term order. Consider the corner set $C[\mathcal{N}] \subset B[\mathcal{N}]$; cf. Definition 2.21, (2.57). The elements of $\mathcal{G}[\langle P\rangle]$ with leading monomials in $C[\mathcal{N}]$ constitute a complete basis of $\langle P\rangle$.

Proof: Denote the corner subset of $\mathcal{G}[\langle P\rangle]$ by $\mathcal{C}[\langle P\rangle]$. We show that the remaining elements of $\mathcal{G}[\langle P\rangle]$ are uniquely determined by the elements in $\mathcal{C}[\langle P\rangle]$. By the definition of $C[\mathcal{N}]$, each element in $B[\mathcal{N}] \setminus C[\mathcal{N}]$ is a monomial multiple of some element in $C[\mathcal{N}]$. Since the corner basis elements cb_k are order compatible, this is also true, by (8.45) for all polynomials which are monomial multiples of them.

Now we consider the monomials in $B[\mathcal{N}] \setminus C[\mathcal{N}]$ in increasing term order and determine their associated border basis elements by taking appropriate multiples of elements in $\mathcal{C}[\langle P\rangle]$. Due to the order-compatibility of the elements in $\mathcal{C}[\langle P\rangle]$ and the consideration of the border basis elements in increasing term order of their leading monomials, the multiples will only contain monomials from $\mathcal{N}$ or leading monomials of basis elements in $\mathcal{C}[\langle P\rangle]$ or leading monomials of border basis elements already processed and represented. Thus, all border basis elements not in $\mathcal{C}[\langle P\rangle]$ can be recursively determined. □

The fact that the "corner basis" $\mathcal{C}[\langle P\rangle]$ may be extended into a full border basis implies that the multiplication matrices of $\mathcal{R}[\langle P\rangle]$ may also be determined from the polynomials in $\mathcal{C}[\langle P\rangle]$. Thus, the corner basis contains the full information necessary for the computation of the zero set of the underlying ideal.

Definition 8.17. The corner basis subset $\mathcal{C}_\prec[\langle P\rangle]$ of the border Groebner basis $\mathcal{G}_\prec[\langle P\rangle]$ is called the *reduced Groebner basis* of P. □

In section 8.4.1, we had observed that order-based reduction by a polynomial set S is, generally, not unique. According to section 8.2.1, uniqueness prevails for a set which is an order-compatible border basis. By reversing the argument in the proof of Theorem 8.31, we see that the non-corner elements of a Groebner basis may be reduced to 0 by the corner elements. Thus, order-based reduction by a reduced Groebner basis is unique.

Example 8.23, continued: The corner set $C[\mathcal{N}]$ is $\{y^2, x^2\}$ and the corner basis $\mathcal{C}_{grevlex}[\langle P\rangle]$ is $\{bb_{02}, bb_{20}\}$. The remaining two border basis elements were formed as $bb_{12} := x\, bb_{02}$ and $bb_{21} := y\, bb_{20} + \frac{8}{35}\, bb_{02}$, which displays their reduction to 0 by $\{bb_{02}, bb_{20}\}$. □

Example 8.24: Consider the polynomial system

$$P := \left\{ \begin{array}{lcl} p_1(x,y) & = & x^2 + \alpha_{02}^{(1)}\, y^2 + \alpha_{11}^{(1)}\, x\, y + \alpha_{10}^{(1)}\, x + \alpha_{01}^{(1)}\, y + \alpha_{00}^{(1)}, \\ p_2(x,y) & = & y^3 + \alpha_{02}^{(2)}\, y^2 + \alpha_{11}^{(2)}\, x\, y + \alpha_{10}^{(2)}\, x + \alpha_{01}^{(2)}\, y + \alpha_{00}^{(2)}. \end{array} \right.$$

Because of the absence of xy^2 terms, we may conjecture that P is the corner subset of a `tdeg`-compatible border basis of $\langle P\rangle$ for the normal set $\{1, y, x, y^2, xy, xy^2\}$. To confirm that conjecture for generic coefficients, our present knowledge requires that we extend P to a full border basis and check the commutativity of the multiplication matrices. This is an awkward job, but it leads to a positive result. Thus, P is the reduced Groebner basis $\mathcal{C}[\langle P\rangle]$. □

In the algebraic literature, the term Groebner basis denotes any basis of $\langle P\rangle$ which is a superset of the *reduced* Groebner basis $\mathcal{C}_\prec[\langle P\rangle]$; at the same time, the general term is often directly associated with the reduced Groebner basis. Also, most computer algebra software generates the reduced Groebner basis $\mathcal{C}_\prec[\langle P\rangle]$, e.g., the procedure `gbasis` in Maple. While we will follow this convention, the border Groebner basis $\mathcal{G}_\prec[\langle P\rangle]$ is also of central importance for us.

The property of border Groebner bases formulated in Theorem 8.31 does not *characterize* Groebner bases; there are polynomial systems P and normal sets $\mathcal{N}$ where the associated border basis $\mathcal{B}_\mathcal{N}[\langle P\rangle]$ is not order-compatible for any term order but where the subset $\mathcal{C}_\mathcal{N}[\langle P\rangle] \subset \mathcal{B}_\mathcal{N}[\langle P\rangle]$ of the basis elements with leading monomials in $C[\mathcal{N}]$ constitutes a basis for $\langle P\rangle$. But this is not true in general: It is easy to construct examples where the corner subset of a border basis does not generate the same ideal. In this sense, Groebner bases are distinguished border bases.

This "shortcoming" of arbitrary border bases is irrelevant in most computational contexts: In the algorithmic determination of normal sets and the associated border bases from some polynomial system P, the corner basis elements do not occur separately from the remaining border basis elements and the full border basis is generally determined anyway; cf. section 10.1.2. In the multiplication matrices which dominate computational tasks for the ideal $\langle P\rangle$, there is no distinction between corner and other border monomials of a normal set; generally, they require the full border basis for their determination.

The uniqueness (modulo normalization) of the reduced Groebner basis $\mathcal{C}_\prec[\mathcal{I}]$ for a specified term order $\prec$ (cf. Theorems 8.30 and 8.31) permits an easy decision about the identity of the ideals generated by two polynomial systems $P_1,\ P_2 \subset \mathcal{P}^s$: Iff $\mathcal{C}_\prec[\langle P_1\rangle] \equiv \mathcal{C}_\prec[\langle P_2\rangle]$, for an arbitrary fixed term order, the two polynomial systems generate the same polynomial ideal. Naturally, this is also a decision procedure for the identity of their zero sets.

8.4.3 Direct Characterization of Reduced Groebner Bases

According to Definition 8.17, the considerations of the previous section and Corollary 8.12, a reduced Groebner basis $\mathcal{C} = \{g_1, \ldots, g_k\} \subset \mathcal{P}^s$, $k \geq s$, must satisfy the following requirements:

(1) There exists a term order $\prec$ such the set L of the $\prec$-leading monomials of the g_κ constitutes the corner set $C[\mathcal{N}]$ of a closed finite set $\mathcal{N} \subset \mathcal{T}^s$;

(2) All S-polynomials $S[g_{\kappa_1}, g_{\kappa_2}]$, $g_{\kappa_1} \neq g_{\kappa_2} \in \mathcal{C}$, can be reduced to 0 by $\mathcal{C}$;

(3) Extend $\mathcal{C}$ to a border basis $\mathcal{G}_\mathcal{N}$: All S-polynomials $S(\bar{g}_{\kappa_1}, \bar{g}_{\kappa_2})$, $\bar{g}_{\kappa_1} \neq \bar{g}_{\kappa_2} \in \mathcal{G}_\mathcal{N}$, can be reduced to 0 by $\mathcal{C}$.

Proposition 8.32. $L = \{x^{j_\kappa},\ \kappa = 1(1)k\} \subset \mathcal{T}^s$ is the corner set of a finite closed subset of $\mathcal{T}^s$ iff

(i) L contains a "pure power" $x_\sigma^{m_\sigma}$, $m_\sigma \in \mathbb{N}$, of each variable x_σ, $\sigma = 1(1)s$;

(ii) none of the $x^{j_\kappa} \in L$ divides another monomial in L.

Proof: Let $\mathcal{I}_L := \langle L \rangle$ be the *monomial ideal* generated by L, i.e. the set of all polynomial multiples of the x^{j_κ}. The set $\mathcal{N}_L := \mathcal{T}^s \setminus \mathcal{I}_L$ is the only candidate for an $\mathcal{N}$ such that $C[\mathcal{N}] = L$; cf. section 2.5.1.

If there is no element $x_\sigma^{m_\sigma}$ in L for some σ, then $\mathcal{I}_L$ cannot contain any power x_σ^ℓ, $\ell \in \mathbb{N}$, and $\mathcal{T}^s \setminus \mathcal{I}_L$ is an infinite set. With (i), on the other hand, all elements x^j, $j \geq (m_1, \ldots, m_s)$ are in $\mathcal{I}_L$ and $\mathcal{T}^s \setminus \mathcal{I}_L$ is finite.

Let $x^{j_{\kappa'}} | x^{j_\kappa}$ so that $x^{j_\kappa} = x^j\, x^{j'_\kappa}$. Since all $x^j\, x^{j'_\kappa} \in \mathcal{I}_L$, x^{j_κ} has a negative neighbor $\notin \mathcal{N}$ so that $x^{j_\kappa} \notin C[\mathcal{N}]$; cf. Definitions 2.17 and 2.21. With (ii), on the other hand, none of the x^{j_κ} can have a negative neighbor in $\mathcal{I}_L$. $\square$

The insistence on a *finite* normal set stems from our current restriction to 0-dimensional ideals. Groebner bases may also be defined for positive-dimensional ideals; then condition (i) is irrelevant.

When we have a set L satisfying condition (ii), the monomial ideal $\mathcal{I}_L$ contains all monomials in the union of the closed positive orthants with vertices at the $x^{j_\kappa} \in L$; cf. Figure 8.6. Condition (ii) is often expressed by the intuitive phrase "the x^{j_κ} must form a *staircase*" and $\mathcal{N}_L$ is called "the set under the staircase."

A verification of requirement 2 appears to be demanding since there are $(k-1)k/2$ combinations of k corner basis elements g_κ. However, the rules of Proposition 8.14 apply immediately to the web of the monomials of the corner set $C[\mathcal{N}]$ where only edges of type (ii) occur so that the number of necessary reductions is diminished. Clearly, when the Groebner basis computation does not assume *a priori knowledge* about the existence of a *finite* normal set and its dimension, the extension in Proposition 8.15 *cannot* be applied.

Proposition 8.33. The above requirement (3) is automatically satisfied if requirements (1) and (2) are satisfied.

Proof: The additional basis elements $\bar{g}_{\bar{\kappa}}$ are formed by multiplying the appropriate g_κ by the appropriate monomial and reducing the nonleading monomials $\notin \mathcal{N}$ of the product with $\mathcal{C}$. Let (w.l.o.g.)

$$\bar{g}_i(x) = x^{\bar{j}_i} g_i(x) + \sum_\kappa \beta_{i\kappa} g_\kappa(x)\,, \quad i = 1, 2\,,$$

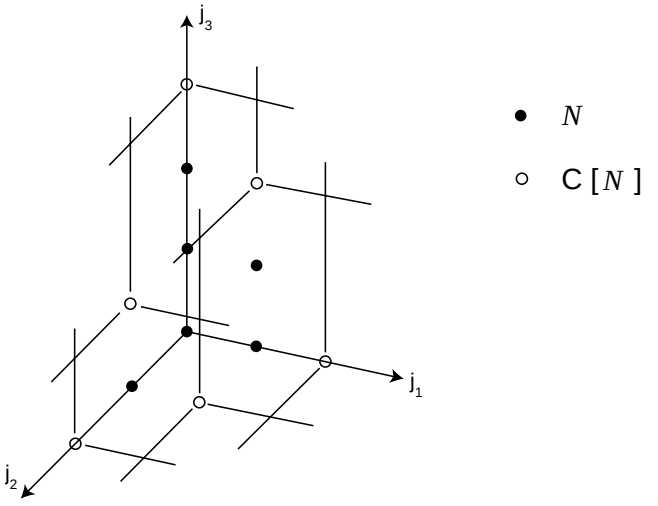

Figure 8.6.

so that the $\bar{g}_i$ have the leading monomials $x^{(j_i+\bar{j}_i)}$, and let j_{12} be the l.c.m. of these leading monomials. Then

$$S[\bar{g}_1, \bar{g}_2] = x^{j_{12}-j_1-\bar{j}_1}\bar{g}_1(x) - x^{j_{12}-j_2-\bar{j}_2}\bar{g}_2(x) = x^{j_{12}-j_1}g_1(x) - x^{j_{12}-j_2}g_2(x) + \text{multiples of } g_\kappa .$$

Since l.c.m.(x^{j_1}, x^{j_2}) divides j_{12}, the first two terms are a multiple of $S[g_1, g_2]$ whose reduction to 0 has been assumed. □

Thus we have proved

Theorem 8.34. A set of $k \geq s$ polynomials $g_\kappa \in \mathcal{P}^s$ is the reduced Groebner basis $\mathcal{C}_\prec[\mathcal{I}]$ of a 0-dimensional ideal $\mathcal{I} \subset \mathcal{P}^s$ with respect to the term order $\prec$ iff

(1) the $\prec$-leading monomials x^{j_κ} of the g_κ form a set L which satisfies the assumptions of Proposition 8.32;

(2) all S-polynomials of the g_κ reduce to 0 with $\mathcal{C}_\prec$.

Example 8.24, continued: With our newly gained insights, we can immediately recognize that the polynomial system P is the reduced Groebner basis of the ideal $\langle P\rangle$, with respect to the term order `tdeg`, $x \succ y$: For this term order, the set L of leading monomials of P is $\{x^2, y^3\}$; L satisfies the conditions of Proposition 8.32 for the 6-element normal set $\mathcal{N} = \{1, y, x, y^2, xy, xy^2\}$. Note that $\mathcal{N}$ is not identical with the support of P; it is precisely the fact that xy^2 is in $\mathcal{N}$ but not in the support of P which permits the interpretation. The only S-polynomial of P reduces to zero with P for arbitrary choices of the coefficients according to rule (a) of Proposition 8.14. This also establishes that $\langle P\rangle$ has 6 zeros. □

In virtually all texts on computational polynomial algebra, the contents of Theorem 8.34 (or some equivalent formulations) serve as the *Definition* of a reduced Groebner basis. Moreover, any set of polynomials which satisfies (2), with leading monomials defined by a *term order* (cf.

Definition 8.13), is usually called a Groebner basis. Thus, our definitions of a Groebner basis and of a reduced Groebner basis describe the same concepts but from a different end:

According to our observations in Chapter 2 and in section 8.1, computational polynomial algebra happens essentially in the quotient ring of a polynomial ideal rather than in the ideal itself. Therefore, our central focus is on monomial bases for quotient rings and the associated multiplication matrices; this makes it natural to consider bases for the ideal which carry the same symbolic and numeric information, viz. *border bases* (cf. section 2.5). All this proceeds without any consideration of a term order which is not a central concept from the algebraic point of view. When a term order is introduced, one particular border basis is singled out for each specific order, which is the Groebner (border) basis. For this particular border basis, a reduction to a corner basis is always possible, which is the reduced Groebner basis.

When one follows the usual approach which focuses on reduced Groebner bases, it is not so obvious that the concept of an ideal basis which admits the full set of potential monomial bases of the quotient ring, is not that of a corner basis but a border basis. As is easily established by counter examples, corner bases do not generally exist for an ideal $\mathcal{I} \subset \mathcal{P}^s$ with all normal sets which are feasible as bases for the quotient ring $\mathcal{R}[\mathcal{I}]$.

Example 8.25: Consider an ideal $\mathcal{I} \in \mathcal{P}^2(6)$, with $\mathcal{N} = \{1, y, x, y^2, xy, xy^2\}$ as a feasible normal set, and the associated border basis $\mathcal{B}_\mathcal{N}[\mathcal{I}]$. Because $\mathcal{N}$ is quasi-univariate with respect to y, we know that the two polynomials from $\mathcal{B}_\mathcal{N}[\mathcal{I}]$ with $\mathcal{N}$-leading monomials y^3, xy^3 constitute a complete intersection basis of $\mathcal{I}$; cf. Proposition 8.20. Assume that the corner subset $\mathcal{C}_\mathcal{N}$ of $\mathcal{B}_\mathcal{N}$, i.e. the two polynomials with $\mathcal{N}$-leading monomials x^2 and y^3, would constitute a basis for $\mathcal{I}$. We may assume that the support of both of these polynomials contains all 6 monomials in $\mathcal{N}$, because we can choose the coefficients of the quasi-univariate basis arbitrarily; cf. Theorem 8.5. When we now form the BKK-number of $\mathcal{C}$ (cf. section 8.3.4), we obtain $\mathrm{BKK}(\mathcal{C}_\mathcal{N}) = 7$. Thus, there are polynomial systems in $\mathcal{P}^2(6)$ for which $\mathcal{N}$ is a feasible normal set but for which there does not exist an $\mathcal{N}$-corner basis. □

8.4.4 Discontinuous Dependence of Groebner Bases on P

While the uniqueness of the reduced Groebner basis $\mathcal{C}_\prec[\langle P\rangle]$ for $P \in \mathcal{P}^s$ is a desirable property, it carries a fundamental drawback with it: Groebner bases cannot be *continuous functions* of P uniformly. We explain this vague statement at first with an intuitive example:

Example 8.26: Consider the family of polynomial systems

$$P_\varepsilon \;=\; \left\{ \begin{array}{rcl} p_1(x, y; \varepsilon) & = & x^2 + \varepsilon\, x\, y + y^2 - 1\,, \\ p_2(x, y) & = & y^3 - 3\, x^2\, y\,. \end{array} \right.$$

For small $|\varepsilon|$, $p_1 = 0$ describes a slightly distorted unit circle while $p_2 = 0$ consists of three straight lines through the origin under 0^0, 60^0, 120^0; cf. Figure 8.7. It is obvious that the 6 zeros of P_ε depend smoothly on ε as ε varies in a neighborhood of 0. In this sense (cf. also section 8.3.2), the ideal $\langle P\rangle$ varies smoothly for small $|\varepsilon|$.

For `tdeg` order with $x \succ y$, the reduced Groebner basis $\mathcal{C}[\langle P_\varepsilon\rangle]$, with indeterminate ε, consists of the 3 polynomials

$$g_1 = p_1(x, y; \varepsilon)\,, \quad g_2 = xy^2 + \frac{4}{3\,\varepsilon} y^3 - \frac{1}{\varepsilon} y\,, \quad g_3 = y^4 + \frac{9\,\varepsilon}{16 - 3\varepsilon^2}\, xy - \frac{12}{16 - 3\varepsilon^2}\, y^2\,;$$

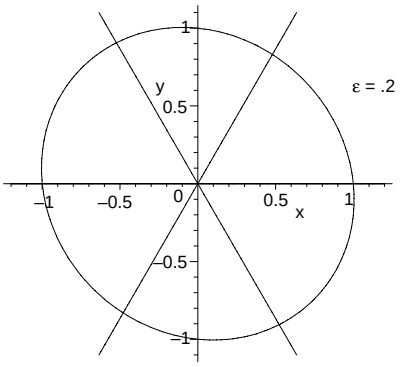

Figure 8.7.

the associated normal set is $\mathcal{N}_\varepsilon = \{1, y, x, y^2, xy, y^3\}$ with $C[\mathcal{N}_\varepsilon] = \{x^2, xy^2, y^4\}$. The multiplication matrices of $\mathcal{R}[\langle P_\varepsilon\rangle]$ with respect to the basis vector $\mathbf{b} = (1, y, x, y^2, xy, y^3)^T$ are

$$A_x = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & -\varepsilon & 0 \\ 0 & \frac{1}{\varepsilon} & 0 & 0 & 0 & \frac{-4}{3\varepsilon} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 0 & \frac{-3\varepsilon}{16-3\varepsilon^2} & \frac{12}{16-3\varepsilon^2} & 0 \end{pmatrix}, \quad A_y = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \frac{1}{\varepsilon} & 0 & 0 & 0 & \frac{-4}{3\varepsilon} \\ 0 & 0 & 0 & \frac{12}{16-3\varepsilon^2} & \frac{-9\varepsilon}{16-3\varepsilon^2} & 0 \end{pmatrix}.$$

It is immediately obvious that this representation of the ideal $\langle P_\varepsilon\rangle$ can only be valid for $\varepsilon \neq 0$. As $|\varepsilon|$ becomes small, the basis polynomial g_2 diverges if we leave its leading coefficient normalized; otherwise, its leading coefficient tends to 0. *Independently of this normalization*, the matrices A_x and A_y diverge and the condition number of their eigenproblems grows like $O(1/\varepsilon)$! Thus, while the representation remains mathematically correct for $\varepsilon \neq 0$, its computational use for numerically specified, tiny ε is not advisable.

For $\varepsilon = 0$ and the same term order `tdeg`, the reduced Groebner basis $\mathcal{C}[\langle P_0\rangle]$ becomes

$$g_1 = p_1(x, y; 0) = x^2 + y^2 - 1\,, \quad g_2 = y^3 - \frac{3}{4}\,y\,,$$

with $\mathcal{N}_0 = \{1, y, x, y^2, xy, xy^2\}$ and $C[\mathcal{N}_0] = \{x^2, y^3\}$. The multiplication matrices of $\mathcal{R}[\langle P_0\rangle]$

with respect to the monomial basis $\mathcal{N}_0$ are

$$A_x^{(0)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \frac{1}{4} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{4} & 0 & 0 \end{pmatrix}, \quad A_y^{(0)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & \frac{3}{4} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & \frac{3}{4} & 0 \end{pmatrix}.$$

There is no immediate way to understand the transition of $\mathcal{C}[\langle P_\varepsilon \rangle]$, $\mathcal{N}_\varepsilon$, A_x, A_y to $\mathcal{C}[\langle P_0 \rangle]$, $\mathcal{N}_0$, $A_x^{(0)}$, $A_y^{(0)}$ in the smooth fashion in which it occurs in the system P_ε and in its zeros. □

In Exercise 2.5-3 b, we have observed that, for $s \geq 2$, $m \geq 2$, there does not exist a normal set which is uniformly feasible for all ideals in $\mathcal{P}^s(m)$. Thus, when we "parametrize" the ideals in $\mathcal{P}^s(m)$ by the components of their zeros, the map from a point in this parameter space to the *unique* normal set $\mathcal{N}_\mathcal{C} \in \mathcal{T}^s(m)$ which supports the Groebner basis for that particular zero set must be *discontinuous* because the image space $\mathcal{T}^s(m)$ is a discrete set.

For fixed s, m and a specified term order $\prec$, consider the generic normal set $\mathcal{N}_g \in \mathcal{T}^s(m)$; cf. Definition 8.14. In the parameter space $\mathbb{C}^{s\times m}$, the relation (2.53) defines the singularity manifold $S_{\mathcal{N}_g}$ of codimension 1 which contains the zero locations for which $\mathcal{N}_g$ is not feasible. When the zero set moves onto $S_{\mathcal{N}_g}$, the image $\mathcal{N}_\mathcal{C}$ *jumps* from $\mathcal{N}_g$ to another normal set $\mathcal{N}_1$ which is distinguished by having one element in its corner set $C[\mathcal{N}_1]$ which precedes one element in $\mathcal{N}_1$. But $\mathcal{N}_1$ has its own singularity manifold $S_{\mathcal{N}_1}$ which (excepting some trivial situations) intersects with $S_{\mathcal{N}_g}$ in a manifold of codimension 2. When the zero set moves onto this manifold—either from within $S_{\mathcal{N}_g}$ or from outside—the Groebner normal set $\mathcal{N}_\mathcal{C}$ jumps to a different element $\mathcal{N}_2$ of $\mathcal{T}^s(m)$, with two order violations in its corner set, etc.

This mechanism generates a tree of manifolds in $\mathbb{C}^{s\times m}$ of higher and higher codimensions dg; each of these singularity manifolds is embedded in those which preceed it in the tree. The value of dg denotes, in an informal sense, the "degree of degeneracy" of the associated zero sets. In spite of this recursive embedding, a zero set of a high degree of degeneracy can be approached by a path consisting of generic zero sets; thus $\mathcal{N}_\mathcal{C}$ can jump over arbitrarily many intermediate values of dg.

Definition 8.18. A singularity of a normal set representation of a polynomial ideal of the kind described above is called a *representation singularity*.

Example 8.26, continued: Due to the symmetry of pairs of zeros of P_ε with respect to the origin, the `tdeg` Groebner normal set $\mathcal{N}_\varepsilon$ is not generic for that term order but has $dg = 1$: The corner element x^2 precedes the normal set element y^3. At $\varepsilon = 0$, the zero set becomes also symmetric to the x- and y-axes; this zero location lies on the singularity manifold $S_{\mathcal{N}_\varepsilon}$ of $\mathcal{N}_\varepsilon$ and induces the jump of the Groebner normal set to $\mathcal{N}_0$, with $dg = 2$: In $C[\mathcal{N}_0]$, the two corner monomials x^2, y^3 precede the normal set monomial xy^2. The zero positions at the corners of the unit hexagon could also have been reached in a continuous way from an unsymmetric generic position of the zeros, inducing an immediate jump from $\mathcal{N}_g$ to $\mathcal{N}_0$.

When we choose the term order `tdeg(y,x)`, it turns out that the transition from P_ε to P_0 does not affect the normal set $\mathcal{N}'_\varepsilon = \{1, x, y, x^2, xy, x^3\}$ of the associated Groebner bases; here, the zero location of P_0 does not lie on the singularity manifold of $\mathcal{N}'_\varepsilon$. For both lexicographic

term orders `plex(x,y)` and `plex(y,x)`, on the other hand, the degeneration degree of the normal set jumps in the transition from P_ε to P_0 and we have analogous discontinuity phenomena as described above. □

This discontinuity dilemma becomes a source of serious difficulties when we use coefficients of limited accuracy and approximate computation; it *cannot be avoided* for Groebner bases. Its origin is the insistence on order-compatibility in the selection of a basis for $\langle P\rangle$ which is implicit in the Groebner basis concept. (It is similar to the fact that we must have a singularity in the representation of a closed 2-manifold in 3-space when we insist on $z = \varphi(x, y)$.) Without this restriction, we can always choose a normal set $\mathcal{N} \in \mathcal{T}^s(m)$ whose singularity manifold $S_\mathcal{N}$ in $\mathbb{C}^{s\times m}$ is sufficiently removed from the location of the zero set $Z[\langle P\rangle]$ so that it can be safely used not only for P but also for all systems $\tilde{P}$ in a suitable neighborhood of P, due to the continuous behavior of the zeros.

The fact that a zero set $Z[\mathcal{I}]$ is close to the singularity manifold $S_{\mathcal{N}_\prec}$ of the unique normal set $\mathcal{N}_\prec$ associated with the Groebner basis $\mathcal{G}_\prec[\mathcal{I}]$ is displayed by the coefficients of $\mathcal{G}_\prec[\mathcal{I}]$ or—equivalently—by the elements of the multiplication matrices A_σ for $\mathcal{R}[\mathcal{I}]$ for the monomial basis $\mathcal{N}_\prec$: The closeness of $S_{\mathcal{N}_\prec}$ lets some elements in the A_σ *diverge* towards ∞. Depending on the normalization employed for $\mathcal{G}_\prec[\mathcal{I}]$, this means that either some coefficients in the Groebner basis have extremely large moduli (for l.c.=1) or that the modulus of some leading coefficients is excessively small; cf. the polynomial g_2 in $\mathcal{C}[\langle P_\varepsilon\rangle]$ in Example 8.26 above.

More generally, consider a regular system $P_0 \in (\mathcal{P}^s)^s$ which is *degenerate* in the following sense: For a specified term order, the Groebner basis $\mathcal{G}_\prec[\langle P_0\rangle]$ employs a normal set $\mathcal{N}_0$ different from the generic normal set $\mathcal{N}_g$ for $\prec$; this implies that the zero set $Z[P_0]$ lies on the singularity manifold $S_{\mathcal{N}_g}$. When we modify the coefficients of P_0 (keeping the convex hull of the supports J_ν of the polynomials in P_0 invariant; cf. section 8.4.3) so that the zero set $Z[\tilde{P}]$ moves away from $S_{\mathcal{N}_g}$, the border basis $\mathcal{B}_{\mathcal{N}_0}[\langle\tilde{P}\rangle]$ with the *original* normal set $\mathcal{N}_0$ cannot remain a Groebner basis: Order-incompatible monomials from $\mathcal{N}_0$ will appear, with small coefficients, in one or several of the elements of $\mathcal{B}_{\mathcal{N}_0}$ some of whose $\mathcal{N}_0$-leading monomials are $\prec$-lower than some elements in $\mathcal{N}_0$, due to the assumed degeneracy.

Definition 8.19. In the situation just described, the border basis $\mathcal{B}_{\mathcal{N}_0}[\langle\tilde{P}\rangle]$ which is the continuous extensions of $\mathcal{G}_\prec[\langle P_0\rangle]$ to neighboring polynomial systems $\tilde{P}$ of P_0, is called an *extended Groebner basis*. □

A fuller discussion of this concept appears in section 10.1.2. The term "extended Groebner basis" has been introduced by the author in his paper [8.6] where it was used for the extension of the *reduced* Groebner basis, i.e. for the *corner subset* of $\mathcal{B}_{\mathcal{N}_0}[\langle\tilde{P}\rangle]$ in the above context. There it has been proved that—for systems $\tilde{P}$ sufficiently close to the degenerate system P_0—this extended reduced Groebner basis is indeed a *basis* of $\langle\tilde{P}\rangle$; it determines the remaining elements of $\mathcal{B}_{\mathcal{N}_0}[\langle\tilde{P}\rangle]$ and thus the multiplication matrices of $\mathcal{R}[\langle\tilde{P}\rangle]$ with respect to the monomial basis $\mathcal{N}_0$.

Example 8.26, continued: The *extended* reduced Groebner basis $\mathcal{C}_{\mathcal{N}_0}[\langle P_\varepsilon\rangle]$ is easily found as

$$cb_1(x, y) \;=\; x^2 + \varepsilon\, x\, y + y^2 - 1\,, \quad cb_2(x, y) \;=\; y^3 - \frac{3}{4}\, y + \frac{3}{4}\,\varepsilon\, x\, y^2\,;$$

it is well-defined for $|\varepsilon| < 4/\sqrt{3} \approx 2.3$; the multiplication matrices of $\mathcal{R}[\langle P_\varepsilon\rangle]$ with respect to the normal set vector $\mathbf{b}_0 = (1, y, x, y^2, xy, xy^2)^T$ which also display the remaining elements

of the extended Groebner basis $\mathcal{B}_{\mathcal{N}_0}[\langle P_\varepsilon\rangle]$ are

$$A_x = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & -\varepsilon & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \frac{1}{4} & 0 & 0 & 0 & -\frac{\varepsilon}{4} \\ 0 & 0 & 0 & \frac{4}{16-3\varepsilon^2} & \frac{-3\varepsilon}{16-3\varepsilon^2} & 0 \end{pmatrix}, \; A_y = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & \frac{3}{4} & 0 & 0 & 0 & -\frac{3\varepsilon}{4} \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \frac{-3\varepsilon}{16-3\varepsilon^2} & \frac{12}{16-3\varepsilon^2} & 0 \end{pmatrix}.$$

These matrices and $\mathcal{B}_{\mathcal{N}_0}[\langle P_\varepsilon\rangle]$ turn smoothly into the $A_x^{(0)}$, $A_y^{(0)}$ matrices and $\mathcal{G}[\langle P_0\rangle]$ for $|\varepsilon| \to 0$. This shows that $\mathcal{B}_{\mathcal{N}_0}[\langle P_\varepsilon\rangle]$ rather than $\mathcal{G}[\langle P_\varepsilon\rangle]$ or its subset $\mathcal{C}[\langle P_\varepsilon\rangle]$ is the appropriate representation of the ideal $\langle P_\varepsilon\rangle$ for small values of $|\varepsilon|$. □

Extended Groebner bases present a possibility to overcome the discontinuous behavior of classical Groebner bases at the singularity manifolds of their normal sets. Since these discontinuities stem from the specification of a term order and the insistence on order-compatibility, the better approach appears to be a *term-order-free* determination of a monomial basis for $\mathcal{R}[\langle P\rangle]$ and of the associated multiplication matrices, with a careful observation of *numerical stability*. This will be one of our objectives in Chapter 10.

In the consideration of perturbations of the degenerate polynomial system P_0, we had restricted the *support* of the perturbations to the convex hull of the supports J_ν of the respective polynomials p_ν in P_0. Otherwise, we must consider the larger supports $\tilde{J}_\nu$ of $\tilde{P}$ as implicitly holding also for P_0; then the degeneracy in P_0 occurs explicitly as the coefficients of some monomials which define the Newton polygon of some $\tilde{p}_\nu$ tend to 0. If this makes $\mathrm{BKK}(P_0)$ smaller than $\mathrm{BKK}(\tilde{P})$, the corresponding number of zeros of $\tilde{P}$ must "disappear" to ∞ as the coefficients tend to 0; for $\tilde{P}$ close to P_0, these zeros will have very large moduli. In this case, which violates our regularity assumptions, a continuous extension from a border basis of $\langle P_0\rangle$ to one of $\langle\tilde{P}\rangle$ cannot exist because of the distinct dimensions of the normal sets. Such situations will be considered in section 9.5.

Example 8.27: In Example 8.26, when we replace the polynomial p_1 in P_ε by $\tilde{p}_1(x, y; \varepsilon) = p_1(x, y; 0) - \varepsilon\, xy^2$, this does not affect P_0; but now $\mathrm{BKK}(\tilde{P}_\varepsilon) = 8 > \mathrm{BKK}(P_0) = 6$. When we numerically compute the zeros of $\tilde{P}_\varepsilon$ for $\varepsilon = 10^{-3}$, we obtain the two zeros at $(\pm 1, 0)$ and 4 further zeros which lie within $\mathrm{O}(10^{-3})$ of the zeros of P_0, but there are two further zeros at approx. $(1333, -2308)$ and $(1334, 2310)$. □

Exercises

1. (a) For $s = 2$, there is no difference between $\prec_{glex}$ and $\prec_{grevlex}$; but this is no longer true for $s \geq 3$. Find the difference in the orderings of the quadratic and cubic monomials for $s = 3$ and 4.

(b) For `tdeg`, visualize the generic normal sets in $\mathcal{T}^3(m)$, for $m = 5(1)20$ (cf. Definition 8.14). Form some of the adjacent normal sets with low degrees of degeneracy.

2. (a) Consider the `tdeg`-based reduction of a monomial $x^j \in \mathcal{T}^2$ by two dense polynomials $s_i \in \mathcal{P}^2$, $i = 1, 2$, with coprime leading monomials x^{j_i} both of which divide x^j. Find the potential support of the remainders r_i of the reductions $x^j \xrightarrow{s_i} r_i$, $i = 1, 2$.

(b) Determine the potential supports of the remainders r_{12} and r_{21} defined by $r_1 \xrightarrow{s_2} r_{12}$ and $r_2 \xrightarrow{s_1} r_{21}$. Construct an example where the two supports differ.

(c) Assume that s_1, s_2 are two elements of a Groebner basis for `tdeg`. Verify that now the two supports in (b) coincide.

3. Use a suitable computer algebra system to determine the reduced Groebner bases $\mathcal{C}_\prec[\langle P\rangle]$ for various freely chosen polynomial systems P in 2, 3, and more variables.

(a) Verify the satisfaction of the criteria in Theorem 8.34.

(b) Try to design systems near the singularity manifold of the normal set associated with $\mathcal{C}_\prec[\langle P\rangle]$ by observing the magnitudes of the coefficients for l.c. $= 1$. Try to identify the causes of the degeneration.

4. By the procedure introduced in section 2.5.2, transform some of the Groebner bases found in Exercise 3 into border bases for other normal sets $\mathcal{N}$ which you choose.

(a) Check whether the corner subset of $\mathcal{B}_\mathcal{N}$ defines the same ideal (hint: determine its Groebner basis).

(b) For the near-singular Groebner bases found in Exercise 3 b , find normal sets $\mathcal{N}$ such that the $\mathcal{N}$-border basis does not contain large coefficients for l.c. $= 1$.

8.5 Multiple Zeros of Intrinsic Polynomial Systems

For univariate polynomials, we have seen in section 6.3 that a cluster of zeros is best understood and analyzed by considering it as the effect of appropriate perturbations on a multiple zero. To follow that same approach in the multivariate case, we must at first understand the structure and the properties of multiple zeros of polynomial ideals $\mathcal{I} \subset \mathcal{P}^s$ in $s > 1$ dimensions, a task which we have repeatedly delayed in Chapter 8. The key to that understanding is the structure of the subspace $\mathcal{D}_0$ of the dual space $\mathcal{D}[\mathcal{I}]$ which corresponds to the multiple zero $z_0 \in \mathbb{C}^s$ and of the associated ideals $\mathcal{I}_0 := \mathcal{I}[\mathcal{D}_0]$ and quotient rings $\mathcal{R}_0 := \mathcal{R}[\mathcal{D}_0]$.

8.5.1 Dual Space of a Multiple Zero

By our considerations in section 2.3.2, an m-fold zero z_0 of $\mathcal{I}$ must contribute m functionals $c_{01}, \ldots, c_{0m}$ to a basis of $\mathcal{D}[\mathcal{I}]$. These functionals define a dual space $\mathcal{D}_0$ which characterizes the ideal $\mathcal{I}_0 \supset \mathcal{I}$ of all polynomials with an m-fold zero of that particular structure at z_0. In the univariate case, the $c_{0\mu}$ are simply $\partial_{\mu-1}[z_0]$; cf. section 6.3.

With s variables, we have a much larger variety of potential differential functionals at our hand: Not only are these the $\binom{s+d-1}{d}$ functionals $\partial_j[z_0]$ of order $d = |j|,\ j \in \mathbb{N}_0^s$, of (2.37) in Definition 2.13, we have also to consider linear combinations of such functionals of equal or different orders. On the other hand, it is to be expected that there must be some restraints for combining such functionals into a basis of $\mathcal{D}_0$. The formal answer to that problem is provided by Definition 2.15 and Theorem 2.21 in section 2.3.2:

Definition 8.20. A zero z_0 of an 0-dimensional ideal $\mathcal{I} \subset \mathcal{P}^s$ is an *m-fold zero* of $\mathcal{I}$ if there exists a *closed* set of *m linearly independent* differentiation functionals $c_{0\mu} = \sum_j \beta_{\mu j}\partial_j[z_0]$ in the dual space $\mathcal{D}[\mathcal{I}]$. The m-dimensional dual space $\mathcal{D}_0 := \text{span}\ (c_{0\mu},\ \mu = 1(1)m)$ defines the

multiplicity structure of z_0; $\mathcal{I}_0 := \mathcal{I}[\mathcal{D}_0] \supset \mathcal{I}$ is the principal ideal of all polynomials which have an m-fold zero of the structure $\mathcal{D}_0$ at z_0. □

Definition 8.19 implies that—for $s \geq 2$—an s-variate m-fold zero z_0 is not fully characterized by its multipicity m but that there are as many qualitatively different versions of an m-fold zero as there are different m-dimensional dual spaces $\mathcal{D}_0$. To visualize the extent of this variability, we consider the case $s = 3$ with $m = 2$ and 3; the location $z_0 \in \mathbb{C}^3$ of the multiple zero is fixed and will not be denoted. Note that the fact that z_0 is a *zero* implies that $c_1 = \partial_0[z_0]$ must be a basis functional in any $\mathcal{D}_0$.

For $m = 2$, the other basis functional c_2 must be a differentiation functional at z_0 which forms a closed space jointly with c_1, i.e. $c_1(p) = c_2(p) = 0$ must imply $c_2(q\,p) = 0$ for each $q \in \mathcal{P}^3$; cf. Definition 2.15. It is easily seen that any functional

$$c_2 \;:=\; \beta_{100}\,\partial_{100} + \beta_{010}\,\partial_{010} + \beta_{001}\,\partial_{001}\,, \quad \text{with } b^T = (\beta_{100}, \beta_{010}, \beta_{001}) \neq 0\,, \tag{8.48}$$

satisfies this requirement: With e_σ the σ-th unit vector,

$$\begin{aligned} c_2(qp) \;&=\; \textstyle\sum_{\sigma=1}^{3} \beta_{e_\sigma}\,\partial_{e_\sigma}[z_0](qp) \;=\; q(z_0)\,\sum_\sigma \beta_{e_\sigma}\,\partial_{e_\sigma}[z_0](p) + p(z_0)\sum_\sigma \beta_{e_\sigma}\,\partial_{e_\sigma}[z_0](q) \\ &=\; c_1(q)\,c_2(p) + c_2(q)\,c_1(p) \;=\; 0\,. \end{aligned}$$

It is also clear that there are no other candidates because a second derivative would violate the closedness condition. Thus c_2 is a *directional first derivative* which appears as a natural generalization of the univariate situation. But even a double zero needs the specification of a (normalized) vector $b \in \mathbb{C}^3$ to characterize its multiplicity structure.

Equation (8.48) has an immediate intuitive interpretation: At a 2-fold zero $z_0 \in \mathbb{C}^3$ of $P = \{p_1, p_2, p_3\} \subset \mathcal{P}^3$, the tangential hyperplanes of the 3 manifolds $p_\nu = 0$ at z_0 intersect in the common *line* $x(t) = (\zeta_{01} + \beta_{100}t, \zeta_{02} + \beta_{010}t, \zeta_{03} + \beta_{001}t)$ so that this line is simultaneously tangential to all 3 manifolds in z_0.

Now take $m = 3$ and assume that a particular c_2 as in (8.48) has already been found as a basis element of $\mathcal{D}_0$. What are candidates for a functional c_3 such that $\mathcal{D}_0 = \text{span}\,(c_1, c_2, c_3)$ is the dual space of a primary ideal $\mathcal{I}_0$ with a zero at z_0? Two possible choices come to mind:

(i) Take another directional derivative $c_3^{(1)} := \sum_\sigma \gamma_{e_\sigma}\,\partial_{e_\sigma}$, with coefficients c^T linearly independent from b^T.

(ii) Take a second derivative in the direction specified by b:

$$c_3^{(2)} \;:=\; (\sum_\sigma \beta_{e_\sigma}\,\partial_{e_\sigma})\,(\sum_\sigma \beta_{e_\sigma}\,\partial_{e_\sigma})[z_0] \;=\; 2\,(\sum_{\sigma_1 \geq \sigma_2} \beta_{e_{\sigma_1}}\,\beta_{e_{\sigma_2}}\,\partial_{e_{\sigma_1}+e_{\sigma_2}})[z_0]\,.$$

Naturally, we may then also take a linear combination $c_3 := \lambda_1\,c_3^{(1)} + \lambda_2\,c_3^{(2)}$ which constitutes the general case. This yields a wide range of possibilities for the multiplicity structure of a triple zero; they may be parametrized by $\beta_{100} : \beta_{010} : \beta_{001}$ for c_2, $\gamma_{100} : \gamma_{010} : \gamma_{001}$ for $c_3^{(1)}$, and $\lambda_1 : \lambda_2$ for c_3. To go beyond $m = 3$, we clearly need a systematic formalization, particularly for $s > 3$.

Example 8.28: Consider the system $P \subset \mathcal{P}^3$ consisting of

$$\begin{aligned} p_1(x, y, z) \;&=\; 3x^2 - y^2 + 2\,yz - z^2 - 8\,x - 8\,y + 5\,z - 5\,, \\ p_2(x, y, z) \;&=\; x^3 - 6\,x^2 - 6\,xy - 4\,y^2 + z^2 + 3\,x + 7\,y - 7\,z + 15\,, \\ p_3(x, y, z) \;&=\; z^3 + 4\,x^2 + 2\,xy - 3\,z^2 - 13\,x - 5\,y + 6\,z + 5\,. \end{aligned}$$

An analysis along the lines of section 8.1 exhibits a triple zero $z_0 = (2, -1, 1)$ (plus 15 further simple zeros). Since a shift of the origin does not change the differential functionals, we move the origin to z_0. The Taylor-expansion of P about (2,-1,1) yields, with $\xi := x - 2$, $\eta := y + 1$, $\zeta := z - 1$,

$$\begin{aligned} p_1(\xi, \eta, \zeta) &:= 4\xi - 4\eta + \zeta + 3\xi^2 - \eta^2 + 2\eta\zeta - \zeta^2 , \\ p_2(\xi, \eta, \zeta) &:= -3\xi + 3\eta - 5\zeta - 6\xi\eta - 4\eta^2 + \zeta 2 + \xi^3 , \\ p_3(\xi, \eta, \zeta) &:= \xi - \eta + 3\zeta + 4\xi^2 + 2\xi\eta + \zeta^3 . \end{aligned}$$

The vanishing at 0 of the first order directional derivative $c_2 = \partial_\xi + \partial_\eta$ for all 3 polynomials is obvious. With some trial and error, one finds that $c_3 = ((\partial_\xi + \partial_\eta)^2 - 2\,\partial_\zeta)[(0, 0, 0)]$ also vanishes for all 3 polynomials (remember that $\partial_{\xi^2} = \frac{1}{2}\frac{\partial^2}{\partial \xi^2}$). Thus, the multiplicity structure of the triple zero z_0 of the original system is specified by the dual space $\mathcal{D}_0 = \text{span}\,(\partial_0, \partial_{x+y}, \partial^2_{x+y} - 2\,\partial_z)[z_0]$. □

For a formal treatment, we must at first understand the restrictions imposed by the required closedness of a basis of $\mathcal{D}_0$. The following formula is well known in multivariate analysis and often quoted as Leibniz' rule; cf. (1.8):

Proposition 8.35. Consider a differentiation functional ∂_j (2.37) with $j \in \mathbb{N}_0^s$. For $p, q \in \mathcal{P}^s$,

$$\partial_j(q\ p) \ = \ \sum_{0 \le k \le j} \partial_k(q)\, \partial_{j-k}(p) , \tag{8.49}$$

where the sum runs over all $k \in \mathbb{N}_0^s$, with $k \le j$ componentwise. Note that the factors in (2.37) imply that no numerical factors appear in (8.49).

Definition 8.21. The *anti-differentiation operators* s_σ, $\sigma = 1(1)s$, are defined by

$$s_\sigma\, \partial_j[z] := \begin{cases} \partial_{j-e_\sigma}[z] & \text{if } j_\sigma > 0 , \\ \text{0-functional} & \text{if } j_\sigma = 0 , \end{cases} \quad \text{and} \quad s_\sigma(\sum_j \gamma_j\, \partial_j[z_0]) := \sum_j \gamma_j\, s_\sigma\, \partial_j[z_0] . \ \square \tag{8.50}$$

Example 8.29: In $\mathcal{P}^3$, $s_1\, \partial_{210} = \partial_{110}$, $s_2\, \partial_{210} = \partial_{200}$, $s_3\, \partial_{210} = 0$; $s_2\,(2\,\partial_{210} - \partial_{021} + 3\,\partial_{102}) = 2\,\partial_{200} - \partial_{011}$. □

Theorem 8.36. In $\mathcal{P}^s$, consider a linear space $\mathcal{D}(z_0)$ of differentiation functionals c, with evaluation at z_0. $\mathcal{D}(z_0)$ is closed iff

$$c \ \in \ \mathcal{D}(z_0) \quad \Longrightarrow \quad s_\sigma\, c \ \in \ \mathcal{D}(z_0) , \quad \sigma = 1(1)s . \tag{8.51}$$

Proof: Closedness of $\mathcal{D}$ requires that $l \in \mathcal{D} \Rightarrow (l \cdot q) \in \mathcal{D}\ \forall\, q \in \mathcal{P}^s$; cf. Definition 2.15. By (8.49), all derivative evaluations of p which occur in an evaluation of $\partial_j(q\ p)$ are of the form $\partial_{j-k}(p) = s^k\, \partial_j(p) := s_{\sigma_1}^{k_1} \ldots s_{\sigma_s}^{k_s}\, \partial_j(p)$, $k \le j$. If $\partial_j(q\ p)$ is to vanish for *arbitrary* $q \in \mathcal{P}^s$ and $\partial_j(p) = 0$ then *all* $s^k\, \partial_j(p)$, $k \le j$, must vanish and vice versa. Linearity of the s_σ extends this to linear combinations of ∂_j's. □

Let us now derive an *algorithmic approach* for the determination of the dual space of a multiple zero $z_0 \in \mathbb{C}^s$ of a polynomial system $P \in \mathcal{P}^s$, assuming that we know the position

of z_0. It appears natural to proceed incrementally from ∂_0 and to look for further candidate functionals c_μ, with free parameters. Then we can attempt to determine the parameters such that span $(\mathcal{D}_0 \cup c_\mu)$ remains closed and $c_\mu(p_\nu)$ vanishes for the polynomials in the given system P. If this is possible, a new basis functional for $\mathcal{D}_0$ has been found. If it is not possible, we *save* the candidate c_μ, with its parameters partially chosen such that closedness is attained, for use in linear combinations with other candidates. If, at some point, none of the candidate functionals annihilates the polynomials in P, we are finished and $\mathcal{D}_0$ is complete. Naturally, this happens after finitely many steps.

For an intuitive development of such an algorithm, we assume at first that there exists a "monomial basis" $\mathbf{c}^T = \{\partial_{j_1}, \partial_{j_2}, \ldots, \partial_{j_m}\}$ of plain derivatives for $\mathcal{D}_0$. Then $\mathcal{D}_0$ may be viewed as a vector space $V \subset \mathbb{C}^s$ with basis $\{j_1, j_2, \ldots, j_m\}$. The operator s_σ moves $j \in V$ to its negative σ-neighbor (cf. Definition 2.17) or annihilates it if the σ-component of j is 0. Closedness appears as the direct analog of the closedness of a set of monomials $\mathcal{N} = \{x^{j_1}, \ldots, x^{j_m}\}$: Each negative neighbor of an $x^{j_\mu} \in \mathcal{N}$ must be in $\mathcal{N}$ or outside the first orthant. We define the degree $|j_\mu| = |(j_{\mu 1}, \ldots, j_{\mu s})| := \sum_\sigma |j_{\mu\sigma}|$ and the "total degree" $|d|$ of $d = \sum_\mu \gamma_\mu \partial_{j_\mu}$ by $\max_\mu |j_\mu|$.

Now we construct a monomial basis $\mathbf{c}^T$ incrementally by total degree, assuming that $\mathcal{D}_0$ admits such a basis. $\mathbf{c}^T$ must contain $\partial_{0,..,0}$, the only element of degree 0; this permits the ∂_{e_σ}, $\sigma = 1(1)s$, to be considered as candidates for further basis elements because they are consistent with closedness. A candidate is accepted if it actually annihilates the polynomials $p_\nu \in P$. Assume that—after a potential renumbering of components—the ∂_{e_σ} for $\sigma = 1(1)s_0$, $1 \le s_0 \le s$, pass this acceptance test. If $s_0 < s$, further candidates ∂_{j_μ} with a higher degree must have vanishing components $j_{\mu,s_0+1}, \ldots, j_{\mu,s}$ to comply with closedness.

Now we form "quadratic" candidates $\partial_{e_{\sigma_1}+e_{\sigma_2}}, \sigma_1, \sigma_2 \in \{1, .., s_0\}$, all of which satisfy closedness. If they are all inconsistent with P so that none of them is accepted, we are finished. But we are also finished if the accepted ∂_{j_μ} with $|j_\mu| = 2$ do not permit a further closed extension of the current basis $\mathbf{c}^T$ which requires the existence of ∂_j with $|\partial_j| = 3$ with all negative neighbors in $\mathbf{c}^T$. Otherwise, we continue with the existing "cubic" candidate(s) in the same fashion.

It is obvious that our assumption about $\mathcal{D}_0$ is restrictive and will not be satisfied in general. There are two principal ways in which we must extend the approach: Assume, at first, as previously that there are $s_0 < s$ plain derivatives ∂_{e_σ} which vanish for the $p_\nu \in P$ and no other first degree basis elements. Then, trivially, not only the $\partial_{e_{\sigma_1}+e_{\sigma_2}}$, $\sigma_1, \sigma_2 \in \{1, .., s_0\}$, retain closedness but also any linear combination of them. And we can add a linear combination of the *discarded* ∂_{e_σ}, $\sigma \in \{s_0 + 1, .., s\}$ to such a quadratic term and retain closedness. This gives us *one* candidate with a sizeable number of *free parameters* as a candidate which retains closedness. We can now require that this parametrized differentiation functional annihilates the p_ν and solve for the parameters which achieve that. Each linearly independent solution yields a basis element for $\mathcal{D}_0$. If there exists no solution for the parameters there are no basis elements beyond the linear ones.

How do we continue from existing quadratic basis functionals $d_1^{(2)}, \ldots, d_k^{(2)}$, each of which contains 2nd derivatives only with respect to $\sigma \in \{1, .., s_0\}$. A potential "cubic" functional $d^{(3)}$ must have a 3rd derivative part which is reduced to the 2nd derivative part of one of the $d_\kappa^{(2)}$ (or to a linear combination of them) by s_σ, $\sigma = 1(1)s_0$. Generally, this requires $k = s_0$ different $d_\kappa^{(2)}$. If $k < s_0$, $d^{(3)} = \sum_{|j|=3} \gamma_j^{(3)} \partial_j$ must be reduced to the *same* linear combination $\sum_\kappa \beta_\kappa d_\kappa^{(2)}$

by two *different* $s_{\sigma_1}, s_{\sigma_2}$, which requires that, for all $|j| = 2$, the ratio $\gamma^{(3)}_{j+e_{\sigma_1}} : \gamma^{(3)}_{j+e_{\sigma_2}}$ has the same fixed value; this reduces the number of free parameters considerably, and even more so if the results of more than two s_σ are to coincide. With this understanding, one can set up the equations necessary for closedness and annihilation of the p_ν and try to solve them. A potential further continuation beyond degree 3 has to follow the same principles.

Example 8.30: Consider the following system $P = \{p_1, p_2, p_3\} \subset \mathcal{P}^3$ with a multiple zero of unknown multiplicity at $z_0 = 0$:

$$\begin{aligned} p_1(x_1, x_2, x_3) &= x_1^2 - 4\,x_1x_2 + 4\,x_2^2 + x_3\,, \\ p_2(x_1, x_2, x_3) &= x_1^2 + x_2^2 + x_3^2 - 2\,x_3\,, \\ p_3(x_1, x_2, x_3) &= x_1^2x_2 + x_1x_2^2 + x_1x_2x_3\,. \end{aligned}$$

It can immediately be seen that ∂_{100} and ∂_{010} are the basis functionals c_2 and c_3 so that $s_0 = 2$; furthermore, ∂_{001} is naturally consistent with closedness but not with P. Above, we have seen that such functionals can be added to higher degree candidates; thus, the general quadratic functional which retains closedness is

$$d^{(2)} = \gamma^{(2)}_{200}\,\partial_{200} + \gamma^{(2)}_{110}\,\partial_{110} + \gamma^{(2)}_{020}\,\partial_{020} + \gamma^{(2)}_{001}\,\partial_{001}\,.$$

Consistency with P requires $d^{(2)}p_\nu = 0,\ \nu = 1(1)3$, or

$$\gamma^{(2)}_{200} - 4\,\gamma^{(2)}_{110} + 4\,\gamma^{(2)}_{020} + \gamma^{(2)}_{001} = 0\,, \qquad \gamma^{(2)}_{200} + \gamma^{(2)}_{020} - 2\,\gamma^{(2)}_{001} = 0\,,$$

while the annihilation of p_3 is trivial. This system has a 2-dimensional solution space so that there are two linearly independent $d^{(2)}$ functionals. As basis functionals c_4, c_5 we take

$$c_4 = d^{(2)}_1 = 4\,\partial_{200} - 3\,\partial_{110} - 4\,\partial_{020}\,, \quad c_5 = d^{(2)}_2 = 2\,\partial_{200} + 3\,\partial_{110} + 2\,\partial_{020} + 2\,\partial_{001}\,.$$

Since there are $2 = s_0$ $d^{(2)}$-functionals, we can set up the cubic candidate without restrictions: We "shift" (differentiate) $d^{(2)}$ in the x_1 and x_2 directions and obtain

$$d^{(3)} = \gamma^{(3)}_{300}\,\partial_{300} + \gamma^{(3)}_{210}\,\partial_{210} + \gamma^{(3)}_{120}\,\partial_{120} + \gamma^{(3)}_{030}\,\partial_{030} + \gamma^{(3)}_{101}\,\partial_{101} + \gamma^{(3)}_{011}\,\partial_{011}\,.$$

In this particular case, the introduction of functionals which have satisfied closedness but not consistency is futile: $d^{(2)}$, with free parameters, trivially annihilates p_3, and consistency with p_1, p_2 turns it into a linear combination of c_4, c_5 as we have seen. Closedness requires

$$s_1\,d^{(3)} = \beta_{11}\,c_4 + \beta_{12}\,c_5\,, \quad s_2\,d^{(3)} = \beta_{21}\,c_4 + \beta_{22}\,c_5\,, \quad s_3\,d^{(3)} = \beta_{31}\,c_2 + \beta_{32}\,c_3\,. \tag{8.52}$$

These are $4+4+2 = 10$ homogeneous equations for the 12 parameters $\gamma^{(3)}_{300}, \ldots, \gamma^{(3)}_{011}, \beta_{11}, \ldots, \beta_{32}$. $d^{(3)}$ annihilates p_1 and p_2 trivially, and $d^{(3)}p_3 = 0$ gives only one further homogeneous equation. The 11×12 homogeneous system has full rank so that there is exactly one nontrivial solution for a c_6: With smallest integer coefficients, we obtain

$$c_6 = 51\,\partial_{300} + 9\,\partial_{210} - 9\,\partial_{120} - 11\,\partial_{030} + 21\,\partial_{101} - \partial_{011}\,.$$

With $1 < s_0$ cubic functionals, a continuation would require a constant proportionality of the consecutive $\gamma^{(3)}_j$ which clearly is not there. Thus we are finished: The multiplicity of $z_0 = 0$ for

the system P is 6 and its multiplicity structure is given by $\mathcal{D}_0 = \text{span}\,\mathbf{c}^T$, with $\mathbf{c}^T = (c_1, \ldots, c_6)$ as computed above.

In a review of the result, we observe: c_4 and c_5 are "natural," their coefficients complete the $(x_1^2, x_1x_2, x_2^2, x_3)$-coefficient vectors $(1, -4, 4, 1)$ and $(1, 0, 1, -2)$ of p_1 and p_2 to a basis of the $\mathbb{C}^4$. c_6, on the other hand, is essentially determined by closedness conditions; consistency with p_3 is only incorporated through $\gamma^{(3)}_{210} = -\gamma^{(3)}_{120}$. c_6 could hardly have been found without explicit use of the system (8.52). Yet this particular form of c_6, together with $c_1, \ldots, c_5$, determines the details of the splitting of the 6-fold zero upon a perturbation of P, as we shall see in section 9.3. Also, P has a total of 12 zeros so that not even the multiplicity $m = 6$ could have easily been found without an algorithmic analysis of the above kind. □

There remains one last shortcoming of our algorithmic procedure: Generally, the s_0 first order differentials $c_2, \ldots, c_{s_0+1}$ in a basis of $\mathcal{D}_0$ will not be plain ∂_{e_σ} but s_0 linearly independent combinations of such derivatives. This may easily be repaired: A linear transformation of the variables which takes the vectors of the linear combinations into different unit vectors reduces the situation to the one which we have discussed. The appropriate transformation is found thus:

If there are s_0 linearly independent combinations of first derivatives at z_0 which vanish, the Jacobian $P'(z_0)$ has deficiency s_0 and there are s_0 column vectors $r_\tau = (\rho_{\tau 1}, \ldots, \rho_{\tau s})^T \in \mathbb{C}^s$ such that $P'(z_0)\, r_\sigma = 0$. When we complete these columns into a regular $s \times s$-matrix R and substitute $x = z_0 + R(y - z_0)$ in P to form $\widehat{P}(y)$, then the Jacobian of $\widehat{P}$ at z_0 will have s_0 leading vanishing columns which implies that the $\hat{p}_\nu(y)$ have vanishing first derivatives with respect to $y_1, \ldots, y_{s_0}$ at z_0. The columns r_τ may be found by Gaussian elimination in $P'(z_0)$.

Example 8.31: We return to our initial Example 8.28 and take the system in its shifted form; for notational clarity, we rename the variables ξ, η, ζ as x_1, x_2, x_3. The Jacobian

$$P'(0) = \begin{pmatrix} 4 & -4 & 1 \\ -3 & 3 & -5 \\ 1 & -1 & 3 \end{pmatrix} \quad \text{is annihilated by } r_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

We complete this column by $r_2 = (1, -1, 0)^T$, $r_3 = (0, 0, 1)^T$ and form $P(Ry) =: \widehat{P}(y)$:

$$\begin{aligned}
\hat{p}_1(y_1, y_2, y_3) &= 8\,y_2 + y_3 + 2\,y_1^2 + 8\,y_1y_2 + 2\,y_2^2 + 2\,y_1y_3 - 2\,y_2y_3 - y_3^2\,, \\
\hat{p}_2(y_1, y_2, y_3) &= -6\,y_2 - 5\,y_3 - 10\,y_1^2 + 8\,y_1y_2 + 2\,y_2^2 + y_3^2 + y_1^3 + 3\,y_1^2y_2 + 3\,y_1y_2^2 + y_2^3\,, \\
\hat{p}_3(y_1, y_2, y_3) &= 2\,y_2 + 3\,y_3 + 6\,y_1^2 + 8\,y_1y_2 + 2\,y_2^2 + y_3^3\,.
\end{aligned}$$

Now we have the plain derivative ∂_{100} for c_2 and $s_0 = 1$. Thus, a quadratic functional consistent with closedness can only have the form $\partial_{200} + \gamma_{010}\,\partial_{010} + \gamma_{001}\,\partial_{001}$. Consistency with $\widehat{P}$ yields 3 inhomogeneous equations for $\gamma_{010}, \gamma_{001}$, with a solution $\gamma_{010} = 0$, $\gamma_{001} = -2$, so that $c_3 = \partial_{200} - 2\,\partial_{001}$.

A cubic functional consistent with closedness is $\partial_{300} - 2\,\partial_{101} + \gamma^{(3)}_{010}\,\partial_{010} + \gamma^{(3)}_{001}\,\partial_{001}$. But now the 3 inhomogeneous equations for the two parameters are inconsistent so that we are finished. A return to the variables before the transformation turns c_2 into $\partial_{100} + \partial_{010}$ and c_3 into $\partial_{200} + \partial_{110} + \partial_{020} - 2\,\partial_{001}$. □

The practical difficulty in the application of the described procedure to a nontrivial polynomial system P lies in the fact that, generally, the multiple zero z_0 will only be known approximately; thus, $P'(z_0)$ will only be *close* to a matrix of deficiency s_0. This means that even

for intrinsic systems, the determination of the differentiability structure of a multiple zero may have to follow the same lines as for an empirical system which will be discussed in section 9.3.

The algorithmic determination of a basis for the dual space $\mathcal{D}_0(z_0)$ associated with a multiple zero of a complete intersection polynomial system has been described in [2.6]; its first (and supposedly only) implementation has been achieved by my student G.Thallinger; cf. [8.3]. There, a term order has been used as incremental guideline; the above presentation shows that a term order is really not necessary.

8.5.2 Normal Set Representation for a Multiple Zero

From the m-dimensional dual space $\mathcal{D}_0 = \text{span}\ \mathbf{c}^T = \text{span}\ (c_1, \ldots, c_n)$ describing the multiplicity structure of an m-fold zero $z_0 \in \mathbb{C}^s$ of $P \subset \mathcal{P}^s$, we want to determine the associated quotient ring $\mathcal{R}_0 = \mathcal{R}[\mathcal{D}_0]$ and primary ideal $\mathcal{I}_0 = \mathcal{I}[\mathcal{D}_0]$. We proceed in a standard way; cf. sections 2.3.2 and 8.1.1.

We select a suitable normal set $\mathcal{N}_0 = \{b_1, \ldots, b_m\}$ from $\mathcal{T}^s(m)$ which yields a regular matrix $\mathbf{c}^T(\mathbf{b})$. From section 2.3.2, we note that $x_\sigma\, \mathbf{b}(x) \equiv A_\sigma\, \mathbf{b}(x) \mod \mathcal{I}_0$ implies $\mathbf{c}^T(x_\sigma \mathbf{b}(x)) = A_\sigma\, \mathbf{c}^T(\mathbf{b}(x))$ so that

$$A_\sigma \;=\; \mathbf{c}^T(x_\sigma \mathbf{b}(x)) \cdot (\mathbf{c}^T(\mathbf{b}(x)))^{-1}\,, \qquad \sigma = 1(1)s\,. \tag{8.53}$$

Thus, we gain a normal set representation of $\mathcal{R}_0$ and $\mathcal{I}_0$. Generally, all matrices involved will be extremely sparse; cf. the examples below.

For the analysis of the zero cluster originating from a perturbation of the multiple zero, it will turn out to be advantageous to have a representation of $\mathcal{I}_0$ by a complete intersection system, i.e. by a basis of only s elements. If we select the normal set $\mathcal{N}_0$ considerately, we may be able to obtain such a basis as a subset of the full border basis $\mathcal{B}[\mathcal{I}_0]$:

Assume, e.g., that $\mathbf{c}^T$ does not contain differentiations with respect to $x_{s_0+1}, \ldots, x_s$; then we need not introduce these variables into the normal set $\mathcal{N}_0$. If we then choose $\mathcal{N}_0$ as quasi-univariate in the "active" variables $x_1, \ldots, x_{s_0}$ (cf. section 8.1.3), we can try to take the s_0 elements from a B_σ subset of the border basis (where x_σ is a distinguished variable) and complete the basis of $\mathcal{I}_0$ by $x_{s_0+1}, \ldots, x_s$.

Even when we take a valid quasi-univariate normal set in all variables, it is not clear that we can select a complete intersection from the border basis because $\mathcal{I}_0$ may not be a complete intersection! Remember that the classic example of a 0-dimensional ideal which is *not* a complete intersection is the principal ideal of a triple zero in two variables, with $\mathcal{D}_0 = \text{span}\ (\partial_{20}, \partial_{11}, \partial_{02})$; cf. Example 8.12 in section 8.3.1. But there we had also found that such zeros cannot occur in regular systems.

Example 8.32: We take the system $\widehat{P}(y)$ of Example 8.31, with $\mathcal{D}_0 = \text{span}\ (\partial_{000}, \partial_{100}, \partial_{200} - 2\partial_{001})$. No differentiation with respect to y_2 appears in the multiplicity structure of the triple zero at 0; therefore, we take $\mathcal{N}_0 = \text{span}\ (1, y_1, y_3)$. This yields $\mathbf{c}^T(\mathbf{b}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$ and $\mathbf{c}^T(y_1\mathbf{b}) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, $\mathbf{c}^T(y_2\mathbf{b}) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $\mathbf{c}^T(y_3\mathbf{b}) = \begin{pmatrix} 0 & 0 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

A_1, A_2, A_3 are the same matrices with their last columns multiplied by $-\frac{1}{2}$; cf. (8.53). The border basis $\mathcal{B}_{\mathcal{N}_0}[\mathcal{I}_0]$ which can be read from the A_σ, is $\{2\,y_1^2+y_3,\ y_1y_3,\ y_3^2,\ y_2,\ y_1y_2,\ y_2y_3\}$. Because A_1 is nonderogatory, the subset $\{2\,y_1^2 + y_3,\ y_1y_3,\ y_2\}$ generates the full basis; it is a complete intersection basis for $\mathcal{I}_0$. □

Example 8.33: When we consider the 6-fold zero $z_0 = 0$ of the system $P(x)$ of Example 8.30, with its rather nontrivial multiplicity structure $\mathcal{D}_0$, we have to be more considerate in the choice of the normal set $\mathcal{N}_0$ to reach a regular matrix $\mathbf{c}^T(\mathbf{b})$: For each component c_μ of $\mathbf{c}^T$, the normal set vector $\mathbf{b}(x) = (b_1(x), \ldots, b_m(x))^T$ must contain at least one component which is not annihilated by c_μ. Thus, on account of $c_1,\ c_2$, and c_3, we must have $1,\ x_1,\ x_2$ in $\mathcal{N}_0$. When we further attempt to bypass the variable x_3, the functionals $c_4,\ c_5$ suggest the inclusion of x_1^2 and x_1x_2. Finally, to keep the normal set quasi-univariate in x_1, x_2, we take x_1^3 as $b_6(x)$. Now we have $\mathbf{b} = (1, x_1, x_2, x_1^2, x_1x_2, x_1^3)^T$ which yields

$$\mathbf{c}^T(\mathbf{b}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & -3 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 51 \end{pmatrix} \quad \text{and} \quad (\mathbf{c}^T(\mathbf{b}))^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{6} & \frac{1}{9} & 0 \\ 0 & 0 & 0 & \frac{1}{6} & \frac{-2}{9} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{51} \end{pmatrix}.$$

We must now form the matrices $\mathbf{c}^T(x_\sigma\mathbf{b}),\ \sigma = 1(1)3$, and multiply them by $(\mathbf{c}^T(\mathbf{b}))^{-1}$ to obtain the multiplication matrices A_σ for $\mathcal{R}_0 = \text{span}\,\mathbf{b}(x)$. This yields

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \frac{3}{17} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{-1}{3} & \frac{8}{9} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{3}{17} \\ 0 & 0 & 0 & 0 & 0 & \frac{-3}{17} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

for the multiplication matrices in the x_1, x_2-subspace, with a total of 5 different nontrivial rows from the normal forms of $x_2^2,\ x_1x_2^2,\ x_1^2x_2,\ x_1^3x_2,\ x_1^4$; this defines the 5 border basis elements in this subspace. The multiplication matrix A_1 for the distinguished variable x_1 of $\mathcal{N}_0$ is derogatory, but it turns out that the border basis elements with $\mathcal{N}_0$-leading monomials x_2^2 and $x_1^2x_2$ define the other 3 ones.

From p_1 and the normal form of x_2^2, we obtain the normal form of $x_3 \notin \mathcal{N}_0$ as $\frac{1}{3}\,x_1^2+\frac{4}{9}\,x_1x_2$. With $A_1,\ A_2$, this defines all other rows in A_3. Thus we have a complete intersection basis for $\mathcal{I}_0$ of the form

$$b_1 = x_2^2 + \tfrac{1}{3}\,x_1^2 - \tfrac{8}{9}\,x_1x_2\,, \quad b_2 = x_1^2x_2 - \tfrac{3}{17}\,x_1^3\,, \quad b_3 = x_3 - \tfrac{1}{3}\,x_1^2 - \tfrac{4}{9}\,x_1x_2\,.$$

For each polynomial combination p of these 3 polynomials, $\mathbf{c}^T[p]$ vanishes. □

8.5.3 From Multiplication Matrices to Dual Space

For a fixed normal set basis $\mathcal{N}_0$ of the quotient ring $\mathcal{R}_0$ of a multiple zero $z_0 \in \mathbb{C}^s$, the dual space $\mathcal{D}_0$ determines the multiplication matrices $A_{0\sigma}$. Thus we should also be able to determine

a basis $\mathbf{c}^T$ of $\mathcal{D}_0$ from $\mathcal{N}_0$ and the $A_{0\sigma}$, $\sigma = 1(1)s$. This task appears when we have found a normal set representation $(\mathcal{N}, \mathcal{B}_\mathcal{N})$ for the ideal $\langle P\rangle$ of the polynomial system $P \subset \mathcal{P}^s$ and the eigenanalysis of the A_σ exhibits a *joint invariant subspace* of a dimension $m_0 > 1$; cf. section 2.4.3. Note that $\mathcal{N} \in \mathcal{T}^s(m)$ is a normal set of $\langle P\rangle$ and not of the ideal $\mathcal{I}_0$ associated with z_0. In this case, we have (cf. (2.50)), for $\sigma = 1(1)s$,

$$A_\sigma\, X_0 = A_\sigma \begin{pmatrix} | & & | \\ x_{01} & .. & x_{0m_0} \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ x_{01} & .. & x_{0m_0} \\ | & & | \end{pmatrix} \begin{pmatrix} \zeta_{0\sigma} & \cdots & \\ & \ddots & \vdots \\ 0 & & \zeta_{0\sigma} \end{pmatrix} = X_0\, T_{0\sigma}, \tag{8.54}$$

where $x_{01} = \mathbf{b}(z_0) \in \mathbb{C}^m$ is the only joint eigenvector in the joint invariant subspace span X_0 of the commuting family $\overline{A}$ of the A_σ, and the $T_{0\sigma} = (\,t^{(\sigma)}_{\nu\mu}\,) \in \mathbb{C}^{m_0\times m_0}$ are upper triangular, with a diagonal of $\zeta_{0\sigma}$, the σ-component of z_0.

Equation (8.54) characterizes z_0 as an m_0-fold zero of $\langle P\rangle$ whose *multiplicity structure* we want to find from the $x_{0\mu} \in \mathbb{C}^m$, $\mu = 2(1)m_0$, and the matrices $T_{0\sigma}$, $\sigma = 1(1)s$. This means that we want to find a basis $\mathbf{c}_0^T = (c_1, \ldots, c_{m_0})$, with $c_\mu = \sum_j \gamma_{\mu j}\partial_j[z_0]$, of a dual space $\mathcal{D}_0$ such that

$$x_{0\mu} \;=\; c_\mu(\mathbf{b}(x))\,, \qquad \mu = 1(1)m_0\,, \tag{8.55}$$

after the first component of x_{01} has been normalized to 1 as usual.

At first, we note that the upper triangularity of the $T_{0\sigma}$ requires that the vectors $x_{0\mu}$ have been arranged in a particular order; from linear algebra, we know that this is always possible. When we interpret the $x_{0\mu}$ as $c_\mu(\mathbf{b})$, this is equivalent to the fact that each leading subset $(c_1, \ldots, c_{\tilde{\mu}})$ of $\mathbf{c}_0^T$ is *closed*:

Proposition 8.37. In $(\mathcal{P}^s)^*$, let $c_\mu = \sum \gamma_{\mu j}\partial_j[z_0]$, $\mu = 1(1)m_0$, and let $\mathbf{b}(x)$ be the normal set vector of $\mathcal{N} \in \mathcal{T}^s(m)$. Each leading subset of $\mathbf{c}_0^T = (c_1, \ldots, c_{m_0})$, $m_0 \le m$, is closed iff there exist upper triangular matrices $T_\sigma \in \mathbb{C}^{m_0\times m_0}$, with diag $T_\sigma = (\zeta_{0\sigma} \ldots \zeta_{0\sigma})$, such that

$$\mathbf{c}_0^T(x_\sigma \mathbf{b}(x)) \;=\; \mathbf{c}_0^T(\mathbf{b}(x))\; T_\sigma\,, \quad \sigma = 1(1)s\,. \tag{8.56}$$

Proof: By Proposition 8.35 and (8.54),

$$c_\mu(x_\sigma \mathbf{b}) \;=\; \partial_0[z_0]x_\sigma\; c_\mu(\mathbf{b}) + s_\sigma c_\mu(\mathbf{b}) \;=\; \zeta_{0\sigma}\, c_\mu(\mathbf{b}) + \sum_\nu t^{(\sigma)}_{\nu\mu}\, c_\nu(\mathbf{b})\,.$$

If each leading subset of $\mathbf{c}^T$ is closed, then $s_\sigma c_\mu$ is in the subspace span $(c_1, \ldots, c_{\mu-1})$ for all σ (cf. Theorem 8.36) and $t^{(\sigma)}_{\nu\mu} = 0$ for $\nu \ge \mu$. Vice versa, the triangularity of the T_σ implies $s_\sigma c_\mu \in$ span $(c_1, \ldots, c_{\mu-1})$ for all σ, since $\mathbf{b}$ is a basis of $\mathcal{R}$. $\square$

Thus, when we interpret the elements $t^{(\sigma)}_{\nu\mu}$ of the $T_{0\sigma}$ in (8.54) in terms of the coefficients $\gamma_{\mu j}$ of the dual space basis elements $c_\mu = \sum_j \gamma_{\mu j}\partial_j[z_0]$, we can assume that the c_μ are ordered in a closedness-consistent way, with $c_1 = \partial_0[z_0]$. Next, there must be at least one pure first-order differential $c_2 = \sum_\sigma \gamma_{2\sigma}\partial_{e_\sigma}[z_0]$; with $c_2(x_\sigma\mathbf{b}) = \zeta_{0\sigma}c_2(\mathbf{b}) + \gamma_{2\sigma}c_1(\mathbf{b})$, this yields immediately $\gamma_{2\sigma} = t^{(\sigma)}_{12}$ for $\sigma = 1(1)s$. If there are further pure first-order differentials $c_\mu = \sum_\sigma \gamma_{\mu\sigma}\partial_{e_\sigma}[z_0]$, $\mu = 3, \ldots$, we have correspondingly $c_\mu(x_\sigma\mathbf{b}) = \zeta_{0\sigma}c_\mu(\mathbf{b}) + \gamma_{\mu\sigma}\mathbf{b}(z_0)$, which implies $t^{(\sigma)}_{1\mu} = \gamma_{\mu\sigma}$, $t^{(\sigma)}_{\nu\mu} = 0$, $\nu = 2(1)\mu - 1$. Thus, the vanishing of all $t^{(\sigma)}_{\nu\mu}$, $\nu = 2(1)\mu - 1$,

for some μ-th column of T_σ signals the presence of a pure first-order basis element c_μ in $\mathbf{c}_0^T$, with coefficients given by the $t_{1\mu}^{(\sigma)}$. Note that an ordering of the c_μ like $\partial_0, \partial_{100}, \partial_{200}, \partial_{010}, \ldots$ does not violate the closedness assumption.

Let $M_1 = \{2, \ldots\}$ be the set of subscripts μ which refer to a pure first-order c_μ. Then the first appearance of nonvanishing elements $t_{\nu\mu}^{(\sigma)}$ in rows $\nu \in M_1$ signals that the respective c_μ is a second-order differential $c_\mu = \sum_\sigma \gamma_{\mu e_\sigma} \partial_{e_\sigma}[z_0] + \sum_{|j|=2} \gamma_{\mu j} \partial_j[z_0]$. From $c_\mu(x_\sigma \mathbf{b}) = \zeta_{0\sigma} c_\mu(\mathbf{b}) + s_\sigma c_\mu(\mathbf{b})$, with

$$s_\sigma c_\mu(\mathbf{b}) \;=\; \gamma_{\mu e_\sigma} \mathbf{b}(z_0) + \sum_{|j|=2} \gamma_{\mu j}\, \partial_{j-e_\sigma}[z_0] \;=\; \sum_{\nu<\mu} t_{\nu\mu}^{(\sigma)}\, c_\nu(\mathbf{b})\,,$$

we find that the $t_{1\mu}^{(\sigma)}$ again display the $\gamma_{\mu e_\sigma}$ while, by (8.50),

$$\text{2nd order part of } c_\mu \;=\; \sum_{\nu \in M_1} t_{\nu\mu}^{(\sigma)}\, \partial_{e_\sigma} c_\nu(\mathbf{b}) + \text{ differentials } \partial_j \text{ with } s_\sigma\, \partial_j = 0\,, \quad \sigma = 1(1)s\,. \tag{8.57}$$

The relations (8.57) must have a unique solution since $s_\sigma c_\mu \in \text{span}\,(c_1, \ldots, c_{\mu-1})$. Similarly, all further columns with vanishing elements except in row 1 and rows $\nu \in M_1$ refer to second-order differentials whose coefficients may be found from the nonvanishing $t_{\nu\mu}^{(\sigma)}$ via (8.57).

When we put all these μ into a set M_2, the first appearance of a column μ with a nonvanishing element in a row $\nu \in M_2$ of one of the T_σ signals that c_μ is a third-order differential whose coefficients may be determined in an analogous fashion. The continuation of the procedure is now obvious.

Example 8.34: We take the system $P(x, y, z)$ of Example 8.28 in its original form, before the shifting of the triple zero to the origin. A feasible normal set $\mathcal{N} \in \mathcal{T}^3(18)$ for $\langle P \rangle$ is (in the sequence of the components in the normal set vector) $\{1,\ x,\ y,\ z,\ x^2,\ xy,\ y^2,\ xz,\ yz, \ldots\}$, the associated multiplication matrix A_x has an invariant subspace X_0 of dimension 3, with eigenvalue 2:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \ldots \\ -10 & 5 & 1 & 2 & 3 & 6 & 5 & 0 & -2 & \ldots \\ & & & & & \ldots & & & & \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -1 & 1 & 0 \\ 1 & 0 & -2 \\ 4 & 4 & 1 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \\ 2 & 1 & -4 \\ -1 & 1 & 2 \\ \vdots & \vdots & \vdots \end{pmatrix}$$

$$= \begin{pmatrix} | & | & | \\ x_{01} & x_{02} & x_{03} \\ | & | & | \end{pmatrix} \begin{pmatrix} 2 & 1 & 0 \\ & 2 & 1 \\ & & 2 \end{pmatrix},$$

where the dots in the first 5 rows of A_x are short for 9 further 0 elements. It turns out that this

subspace X_0 is a joint invariant subspace of $A_x,\ A_y,\ A_z$, with

$$T_{01} = \begin{pmatrix} 2 & 1 & 0 \\ & 2 & 1 \\ & & 2 \end{pmatrix}, \quad T_{02} = \begin{pmatrix} -1 & 1 & 0 \\ & -1 & 1 \\ & & -1 \end{pmatrix}, \quad T_{03} = \begin{pmatrix} 1 & 0 & -2 \\ & 1 & 0 \\ & & 1 \end{pmatrix}.$$

From the eigenvector $x_{01} = (1, 2, -1, 1, \ldots)^T$ or from the diagonal elements of the $T_{0\sigma}$, we have the position of the triple zero at $z_0 =$ (2,-1,1). The 2nd column of the $T_{0\sigma}$ displays $c_2 = \partial_{100} + \partial_{010}$. Since $2 \in M_1$ and the 3rd columns of T_{01} and T_{02} have a nonvanishing element in row 2, c_3 must be a 2nd order differential. From (8.57), we have

$$c_3 \ = \ \partial_{100}\, c_2 + \ldots \ = \ \partial_{010}\, c_2 + \ldots \ = \ -\,2\,\partial_{001}\, c_1 + \ldots$$

which implies $c_3 = \partial_{200} + \partial_{110} + \partial_{020} - 2\,\partial_{001}$, as we had obtained it analytically. All evaluations of the above partials are at z_0, of course. □

Example 8.35: We take the system $P(x_1, x_2, x_3)$ of Example 8.30. A Groebner basis algorithm for the term order `tdeg(x3,x2,x1)` produces the normal set $\{1,\ x_1,\ x_2,\ x_3,\ x_1^2,\ x_1x_2,\ x_1x_3,\ x_2x_3,\ x_1^3,\ x_1^2x_2,\ x_1^2x_3,\ x_1^4\} \in \mathcal{T}^3(12)$ and associated multiplication matrices $A_1, A_2, A_3 \in \mathbb{C}^{12\times 12}$. These matrices have a joint invariant subspace of dimension 6 which is spanned by the vectors $x_{01} = (1, 0, .., 0)^T$, $x_{02} = (0, 1, 0, .., 0)^T$, $x_{03} = (0, 0, 1, 0, .., 0)^T$, $x_{04} = (0, 0, 0, 0, 4, -3, 0, .., 0)^T$, $x_{05} = (0, 0, 0, 2, 2, 3, 0, .., 0)^T$, $c_{06} = (0, .., 0, 21, -1, 51, 9, 0, 0)^T$, with a decomposition (8.54) with the matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 4 & 2 & 0 \\ & & 0 & -3 & 3 & 0 \\ & & & 0 & 0 & \frac{15}{2} \\ & & & & 0 & \frac{21}{2} \\ & & & & & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ & 0 & 0 & -3 & 3 & 0 \\ & & 0 & -4 & 2 & 0 \\ & & & 0 & 0 & \frac{5}{2} \\ & & & & 0 & \frac{-1}{2} \\ & & & & & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 2 & 0 \\ & 0 & 0 & 0 & 0 & 21 \\ & & 0 & 0 & 0 & -1 \\ & & & 0 & 0 & 0 \\ & & & & 0 & 0 \\ & & & & & 0 \end{pmatrix},$$

as $T_{01},\ T_{02},\ T_{03}$. The 0 diagonals appear because the multiple zero is at (0,0,0). Furthermore, we see that none of the A_σ is nonderogatory: Besides the only joint eigenvector x_{01}, there are the additional eigenvectors x_{03} for A_1, x_{02} for A_2, and x_{02}, x_{03}, x_{04} for A_3; but none of these is a joint eigenvector.

The functionals $c_2 = \partial_{100}$ and $c_3 = \partial_{010}$ are immediately read from T_{01} and T_{02}; thus $M_1 = \{2, 3\}$. The 5th column of T_{03} might indicate another first-order differential, but the 5th columns of the other $T_{0\sigma}$ have nonvanishing elements in rows $2,\ 3 \in M_1$. Thus we have, for $\mu = 4$ and 5, and for $\sigma = 1, 2, 3$,

$$c_\mu \ = \ t_{1\mu}^{(\sigma)}\, \partial_{e_\sigma} + t_{2\mu}^{(\sigma)}\, \partial_{e_\sigma}\, c_2 + t_{3\mu}^{(\sigma)}\, \partial_{e_\sigma}\, c_3 + \ldots\,,$$

which yields

$$\begin{aligned} c_4 \ &= \ \partial_{100}\,(4\,c_2 - 3\,c_3) + \ldots \ = \ \partial_{010}\,(-3\,c_2 - 4\,c_3) + \ldots \ = \ 4\,\partial_{200} - 3\,\partial_{110} - 4\,\partial_{020}\,, \\ c_5 &= \partial_{100}\,(2\,c_2 + 3\,c_3) + .. = \partial_{010}\,(3\,c_2 + 2\,c_3) + .. = 2\,\partial_{001} + .. \\ &= 2\,\partial_{200} + 3\,\partial_{110} + 2\,\partial_{020} + 2\,\partial_{001}\,. \end{aligned}$$

There are no further 2nd order differentials and the nonvanishing elements in rows 4, $5 \in M_2$ signal a third order functional c_6. From the generalization of (8.57), we have

$$c_6 \;=\; \partial_{100}\,(\tfrac{15}{2}\,c_4 + \tfrac{21}{2}\,c_5) + \ldots \;=\; \partial_{010}\,(\tfrac{5}{2}\,c_4 + \tfrac{-1}{2}\,c_5) + \ldots \;=\; \partial_{001}\,(21\,c_2 - c_3) + \ldots\,.$$

This yields a consistent representation of c_6 as

$$c_6 \;=\; 51\,\partial_{300} + 9\,\partial_{210} - 9\,\partial_{120} - 11\,\partial_{030} + 21\,\partial_{101} - \partial_{011}\,.$$

Thus we have found the same expressions as previously for the basis functionals of the dual space $\mathcal{D}_0$ which defines the multiplicity structure of the 6-fold zero at (0,0,0). □

Exercises

1. For $s = 2$ and 3, interpret the vanishing of various differential functionals geometrically in terms of the manifolds $p_\nu = 0,\ \nu = 1(1)s$; cf. our interpretation of (8.48).

2. Consider the polynomial system P specified by

$$\begin{aligned} p_1 &= 2\,x_1^2 + 3\,x_1x_2 + 3\,x_2^2 + 15\,x_1 + 21\,x_2 + 5\,x_3 + 35\,,\\ p_2 &= x_1^2 - 6\,x_1x_3 - 4\,x_3^2 + 5\,x_1 + 7\,x_2 - 6\,x_3 + 25\,,\\ p_3 &= x_2^2 - 3\,x_2x_3 - 3\,x_3^2 - 3\,x_1 + 13\,x_2 - 4\,x_3 + 22\,. \end{aligned}$$

(a) Form the Jacobian P' of P and check the overdetermined system $\{p_1,\ p_2,\ p_3,\ \det(P')\}$ $=:\ \bar{P}$ for a potential common zero, i.e. a multiple zero z_0 of P. (Compute a Groebner basis of $\bar{P}$.) Shift the origin of the $\mathbb{C}^3$ to z_0 so that the transformed system has no constant terms.

(b) Find the multiplicity and the multiplicity structure of the multiple zero 0 of the transformed system. (Use the approach of section 8.5.1.)

(c) Find a normal set and a border basis for the primary ideal of the multiple zero, in the transformed and the original coordinates.

3. For some polynomial ideal $\mathcal{I} \subset \mathcal{P}^3$, let the family $\overline{A}$ of multiplication matrices with respect to the normal set $\{1, x, y, z, \ldots\}$ have a joint invariant subspace X_0 of dimension 4. When its basis vectors x_1, x_2, x_3, x_4, in suitable order, are chosen as the first 4 vectors in the matrix $X = \mathbf{c}^T(\mathbf{b})$, the following upper triangular matrices are obtained from (cf. Example 8.34)

$$A_\sigma \begin{pmatrix} | & | & | & | \\ x_1 & x_2 & x_3 & x_4 \\ | & | & | & | \end{pmatrix} = \begin{pmatrix} | & | & | & | \\ x_1 & x_2 & x_3 & x_4 \\ | & | & | & | \end{pmatrix} T_{0\sigma}\,, \quad \sigma = x, y, z\,:$$

$$T_{0x} = \begin{pmatrix} 5 & 1 & 0 & -1 \\ & 5 & 0 & 2 \\ & & 5 & -3 \\ & & & 5 \end{pmatrix},\ T_{0y} = \begin{pmatrix} 2 & 3 & 1 & 2 \\ & 2 & 0 & 3 \\ & & 2 & -9 \\ & & & 2 \end{pmatrix},\ T_{0z} = \begin{pmatrix} -3 & 0 & -1 & 1 \\ & -3 & 0 & 3 \\ & & -3 & 0 \\ & & & -3 \end{pmatrix}.$$

(a) What is the location and the multiplicity structure of the associated 4-fold zero z_0 of $\mathcal{I}$?

(b) Determine the multiplication matrices A_{0x}, A_{0y}, A_{0z} and the border basis $\mathcal{B}_0$ of the ideal $\mathcal{I}_0$ of z_0 with respect to the normal set $\mathcal{N}_0 = \{1, x, y, z\}$.

(c) Convince yourself that none of the multiplication matrices of $\mathcal{I}_0$ is nonderogatory and that none of the 3-element border basis subsets derived from the quasi-univariate structure of $\mathcal{N}_0$ generates $\mathcal{I}_0$ (but a positive-dimensional ideal). To establish $\mathcal{I}_0$ as a complete intersection, find another 3-element subset of $\mathcal{B}_0$ which generates $\mathcal{I}_0$.

4. In $\mathcal{P}^3$, consider the differentiation functionals (with evaluation at a fixed $z_0 \in \mathbb{C}^3$)

$$c_1 = \partial_0\,, \quad c_2 = \partial_{100} + \partial_{010}\,, \quad c_3 = \partial_{100} + \partial_{001}\,, \quad c_4 = \partial_{200} + \partial_{110} + \partial_{020} + 3\,\partial_{100}\,,$$
$$c_5 = \partial_{300} + \partial_{210} + \partial_{120} + \partial_{030} + 6\,\partial_{200} + 3\,\partial_{110} - \partial_{020} + \partial_{011} + \partial_{002} - 2\,\partial_{010} + \partial_{001}\,.$$

Let $\mathcal{D}_0 = \text{span}\,(c_1, \ldots, c_5)$, with $z_0 = (1, -2, 3)$.

(a) Verify that each subset $(c_1, \ldots, c_\mu)$, $\mu = 2, 3, 4, 5$, is closed.

(b) Find a feasible normal set basis $\mathcal{N}_0 \in \mathcal{T}^3(5)$ for $\mathcal{R}_0 = \mathcal{R}[\mathcal{D}_0]$ (i.e. that $\mathbf{c}^T(\mathbf{b})$ is regular). Verify that all normal sets with $1, x_1, x_2, x_3$, and some quadratic monomial are feasible. Verify that all these normal sets are quasi-univariate.

(c) For a chosen $\mathcal{N}_0$ and associated normal set vector $\mathbf{b}$, determine the multiplication matrices A_{01}, A_{02}, A_{03} of $\mathcal{R}_0$ via (8.53) and the associated border basis $\mathcal{B}_0$ of $\mathcal{I}_0 = \mathcal{I}[\mathcal{D}_0]$. Check whether there exist 3-element subsets $\mathcal{B}_c$ of $\mathcal{B}_0$ (complete intersection bases) such that $\langle \mathcal{B}_c \rangle = \langle \mathcal{B}_0 \rangle = \mathcal{I}_0$.

(d) Form polynomial combinations of the polynomials in $\mathcal{B}_0$ and check that they are annihilated by the functionals of $\mathcal{D}_0$.

(e) Compute the associated upper-triangular matrices $T_{0\sigma}$, $\sigma = 1(1)3$, of (8.54)

(i) by representing the columns of $\mathbf{c}^T(x_\sigma \mathbf{b})$ in terms of the basis $\mathbf{c}^T(\mathbf{b})$,

(ii) from the interpretation of the elements of the $T_{0\sigma}$ in terms of the c_μ as in section 8.5.3.

Historical and Bibliographical Notes 8

The central role of the S-polynomial criterion in the work of Buchberger has dominated the attitude of computer algebraists towards basis representations of polynomial ideals for decades. There appear to have been no serious attempts to develop alternate approaches and criteria, at least for the important special case of 0-dimensional polynomial ideals where the finite dimension of the quotient ring and the dual space designates those as natural representations. Not even the gradual recognition of the Central Theorem (cf. section 2.4) as the proper tool for the determination of the zeros of a 0-dimensional polynomial system P during the 1990s changed that situation, at first: Normal sets and multiplication matrices for $\mathcal{R}[\langle P \rangle]$ had to be found via Groebner bases for $\langle P \rangle$.

Eventually, the related but largely independent efforts of B. Mourrain and the author of this book have initiated a change: In numerous conference presentations, I have emphasized the desirability of a direct determination of a basis for $\mathcal{R}[\langle P \rangle]$ and of its multiplicative structure. The formal basis for the novel approach was laid by Mourrain's paper [8.1] and further work. Simultaneously, there began first attempts towards an algorithmic realization, e.g., in [8.2].

Various open questions remained: For the (generally) overdetermined representation of $\langle P \rangle$ by a reduced Groebner basis, the S-polynomial criterion (Theorem 8.34) guarantees completeness and consistency in a minimal way. For a highly overdetermined normal set representation $(\mathcal{N}, \mathcal{B}_\mathcal{N})$ of $\langle P \rangle$, the commutativity of the multiplication matrices A_σ constitutes a

sufficient but highly *redundant* set of conditions. Are there minimal sets of conditions which *guarantee* commutativity and hence consistency? Preliminary answers to this and other natural questions have been given in sections 8.1 and 8.2.

While the regularity of a *linear* multivariate system is considered as its most important property, the analogous regularity property of polynomial systems—often denoted by the term "complete intersection"—has received far less attention. From the numerical point of view, it is crucial in almost every aspect, as will be seen in Chapter 9. Also, the remarkable fact that the number of zeros of a 0-dimensional regular system can be precisely determined from its sparsity pattern by *symbolic* computation has not been widely utilized in polynomial algebra so far. Actually, the knowledge of the BKK-number of a regular polynomial system makes the use of term order obsolete in many respects (cf., e.g., Chapter 10).

One of the reasons for the introduction of dual spaces in [2.6] was the analysis of the structure of multiple zeros of polynomial systems. The content of section 8.5 is largely from [8.3]. In spite of their many facets, multiple zeros have attracted little attention in polynomial algebra so far.

In view of the immense literature on the subject of Groebner bases (cf., e.g., [2.10]–[2.13]), further notes on this subject appear unnecessary.

References

[8.1] B. Mourrain: A New Criterion for Normal Form Algorithms, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Science Vol. 1719, Springer, Berlin, 1999, 430–443.

[8.2] B. Mourrain, Ph. Trébuchet: Solving Projective Complete Intersections Faster, in: Proceed. ISSAC 2000 (Ed. C. Traverso), ACM, New York, 231–238, 2000.

B. Mourrain, Ph. Trébuchet: Normal Form Computation for Zero-Dimensional Ideals, in: Proceed. ISSAC 2002 (Ed. T. Mora), ACM, New York, 2002.

[8.3] H.J. Stetter: Analysis of Zero Clusters in Multivariate Polynomial Systems, in: Proceed. ISSAC 1996 (Ed. Y.N. Lakshman), ACM, New York, 127–135, 1996.

G. Thallinger: Analysis of Zero Clusters in Multivariate Polynomial Systems, Diploma Thesis, Tech. Univ. Vienna, 1996.

[8.4] J. Dieudonné: Foundations of Modern Analysis, Academic Press, New York, 1968 (7th Ed.).

[8.5] J. Verschelde: Algorithm 795: PHC-pack: A General-Purpose Solver for Polynomial Systems by Homotopy Continuation, Trans. Math. Software **25** (1999), 251–276.

[8.6] H.J. Stetter: Stabilization of Polynomial Systems Solving with Groebner Bases, in: Proceed. ISSAC 1997 (Ed. W. Kuechlin), ACM, New York, 117–124, 1997.