On the null spaces of the Macaulay matrix

Kim Batselier , Philippe Dreesen, Bart De Moor[1]

Department of Electrical Engineering ESAT-STADIUS Center for Dynamical Systems, Signal Processing and Data Analytics, KU Leuven / IBBT Future Health Department, 3001 Leuven, Belgium

---

Abstract

In this article both the left and right null space of the Macaulay matrix are described. The left null space is shown to be linked with the occurrence of syzygies in its row space. It is also demonstrated how the dimension of the left null space is described by a piecewise function of polynomials. We present two algorithms that determine these polynomials. Furthermore we show how the finiteness of the number of basis syzygies results in the notion of the degree of regularity. This concept plays a crucial role in describing a basis for the right null space of the Macaulay matrix in terms of differential functionals. We define a canonical null space for the Macaulay matrix in terms of the projective roots of a polynomial system and extend the multiplication property of this canonical basis to the projective case. This results in an algorithm to determine the upper triangular commuting multiplication matrices. Finally, we discuss how Stetter's eigenvalue problem to determine the roots of a multivariate polynomial system can be extended to the case where a multivariate polynomial system has both affine roots and roots at infinity.

Keywords: Macaulay matrix, multivariate polynomials, row space, null space, syzygies, roots
2010 MSC: 54B05,

Email address: `kim.batselier@esat.kuleuven.be` ()

[1] Kim Batselier is a research assistant at the KU Leuven, Belgium. Philippe Dreesen is supported by the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen). Bart De Moor is a full professor at the KU Leuven, Belgium. Research supported by Research Council KUL: GOA/10/09 MaNet , PFV/10/002 (OPTEC), several PhD/postdoc & fellow grants, Flemish Government:IOF: IOF/KP/SCORES4CHEM,FWO: PhD/postdoc grants, projects: G.0588.09 (Brain-machine), G.0377.09 (Mechatronics MPC), G.0377.12 (Structured systems),IWT: PhD Grants, projects: SBO LeCoPro, SBO Climaqs, SBO POM, EUROSTARS SMART, iMinds 2012, Belgian Federal Science Policy Office: IUAP P7/19 (DYSCO, Dynamical systems, control and optimization, 2012-2017),EU: ERNSI, FP7-EMBOCON (ICT-248940), FP7-SADCO (MC ITN-264735), ERC ST HIGHWIND (259 166), ERC AdG A-DATADRIVE-B,COST: Action ICO806: IntelliCIS.

2010 MSC: 12E05,
2010 MSC: 65F99

---

1. Introduction

Many problems in computer science, physics and engineering require a mathematical modelling step and multivariate polynomials are a natural modelling tool [1]. This results in problems in which one needs to compute the roots of a multivariate polynomial system, divide multivariate polynomials, eliminate variables, compute greatest common divisors, etc. The area of mathematics in which multivariate polynomials are studied is algebraic geometry and has a rich history spanning many centuries [2]. Most methods to solve these problems are symbolical and involve the computation of a Gröbner basis [3, 4, 5]. From the point of view of engineering however, one is mainly interested in approximate answers obtained from numerical methods. Hence, there is a need to have a framework of numerical methods that solve problems such as polynomial root-finding, elimination, etc. Although some numerical methods are available, there was no unifying framework. For example, the most important and known numerical method for solving multivariate polynomial systems is numerical polynomial homotopy continuation (NPHC) [6, 7, 8, 9], but it is not possible to eliminate variables, compute greatest common divisors or do polynomial divisions in this framework. It is possible to solve many of these problems with multivariate polynomials in a numerical linear algebra framework. An important milestone in this respect was the discovery of Stetter that finding the affine roots of a multivariate polynomial system is equivalent with solving an eigenvalue problem [10, 11]. In his approach however, it is still necessary to first compute a Gröbner basis before the eigenvalue problem can be written down. We have developed a numerical linear algebra framework where no symbolical computations are required. Problems such as elimination of variables [12], computing an approximate greatest common divisor [13], computing a Gröbner and border basis [14], finding the affine roots of a polynomial system are all solved numerically in this Polynomial Numerical Linear Algebra (PNLA) framework. The Macaulay matrix plays a central role in all these problems [15, 16].

The Macaulay matrix is defined for a certain degree d and it is important to understand how its size and dimensions of its fundamental subspaces change as a function of d. These are in fact described by different polynomials in d. We will explain how this comes about in this article through the analysis of the left null space of $M(d)$. This analysis will lead us to the definition of the degree of regularity of a multivariate polynomial system $f_1, \ldots, f_s$. In addition, two algorithms that determine the polynomial expression $l(d)$ for the dimension of the left null space of $M(d)$ are presented. Once the polynomials that describe the dimensions of the fundamental subspaces are understood, we move on to describe the right null space of the Macaulay matrix. The affine roots of a multivariate polynomial system $f_1, \ldots, f_s$ are usually described by the dual vector space of the quotient space $\mathcal{C}^n/\langle f_1, \ldots, f_s \rangle$. In this article we will describe the right null space of $M(d)$ as the annihilator of its row space and express this by means of a functional basis. An important observation here is that also roots at infinity are described by this functional basis and that multiplicities of roots result in a certain multiplicity structure. Stetter's method to find the affine roots of a multivariate polynomial system is by means of an eigenvalue problem that describes a monomial multiplication within the quotient space $\mathcal{C}^n/\langle f_1, \ldots, f_s \rangle$. We will extend this monomial multiplication property to the projective case and present an algorithm that derives the corresponding projective multiplication matrices.

Before defining the Macaulay matrix, we first discuss the numerical linear algebra framework in which we will describe multivariate polynomials and introduce the monomial ordering that will be used. Most of the algorithms described in this article are implemented in MATLAB [17]/Octave[18] and are freely available at `https://github.com/kbatseli/PNLA_MATLAB_OCTAVE`.

2. Vector space of multivariate polynomials

The ring of multivariate polynomials in n variables with complex coefficients is denoted by $\mathcal{C}^n$. It is easy to show that the subset of $\mathcal{C}^n$, containing all multivariate polynomials of total degrees from 0 up to d forms a vector space. We will denote this vector space by $\mathcal{C}^n_d$. We consider multivariate polynomials that occur in computer science and engineering applications and limit ourselves therefore, without loss of generality, to multivariate polynomials with only real coefficients. Throughout this article we will use a monomial basis as a basis for $\mathcal{C}^n_d$. Since the total number of monomials in n variables from degree 0 up to degree d is given by

$$q(d) = \binom{d+n}{n}$$

it follows that dim $\mathcal{C}_d^n = q(d)$. The total degree of a monomial $x^a = x_1^{a_1} \ldots x_n^{a_n}$ is defined as $|a| = \sum_{i=1}^n a_i$. The degree of a polynomial p, $\deg(p)$, then corresponds with the degree of the monomial of p with highest degree. It is possible to order the terms of multivariate polynomials in different ways and results typically depend on which ordering is chosen. It is therefore important to specify which ordering is used. For a formal definition of monomial orderings together with a detailed description of some relevant orderings in computational algebraic geometry see [5, 4].

2.1. Monomial orderings and homogeneous polynomials

It is possible to reconstruct the monomial $x^a = x_1^{a_1} \ldots x_n^{a_n}$ from the n-tuple of exponents $a = (a_1, \ldots, a_n) \in \mathbb{N}_0^n$. Furthermore, any ordering $>$ we establish on the space $\mathbb{N}_0^n$ will give us an ordering on monomials: if $a > b$ according to this ordering, we will also say that $x^a > x^b$.

Definition 2.1. *Degree negative lexicographic. Let a and $b \in \mathbb{N}_0^n$. We say $a >_{dnlex} b$ if*

$$|a| = \sum_{i=1}^n a_i > |b| = \sum_{i=1}^n b_i, \text{ or } |a| = |b| \text{ and } a >_{nlex} b$$

where $a >_{nlex} b$ if, in the vector difference $a - b \in \mathbb{Z}^n$, the leftmost non-zero entry is negative.

Example 2.1. $(2,0,0) >_{dnlex} (0,0,1)$ *because* $|(2,0,0)| > |(0,0,1)|$ *which implies* $x_1^2 >_{dnlex} x_3$. *Likewise,* $(0,1,1) >_{dnlex} (2,0,0)$ *because* $(0,1,1) >_{nlex} (2,0,0)$ *and this implies that* $x_2x_3 >_{dnlex} x_1^2$.

The ordering is graded because it first compares the degrees of the two monomials and applies the negative lexicographic ordering when there is a tie. The ordering is also multiplicative, which means that if $a <_{\text{dnlex}} b$ this implies that $ac <_{\text{dnlex}} bc$ for all $c \in \mathbb{N}_0^n$. Once a monomial ordering is fixed we can represent a multivariate polynomial f by its coefficient vector. One simply orders the coefficients in a row vector, degree negative lexicographically ordered, in ascending degree. The following example illustrates.

Example 2.2. *The polynomial* $f = 2 + 3x_1 - 4x_2 + x_1x_2 - 8x_1x_3 - 7x_2^2 + 3x_3^2$ *in* C_3^2 *is represented by the vector*

$$\begin{array}{cccccccccc} 1 & x_1 & x_2 & x_3 & x_1^2 & x_1x_2 & x_1x_3 & x_2^2 & x_2x_3 & x_3^2 \\ \end{array}$$
$$\begin{pmatrix} 2 & 3 & -4 & 0 & 0 & 1 & -8 & -7 & 0 & 3 \end{pmatrix}$$

where the degree negative lexicographic ordering is indicated above each coefficient.

By convention a coefficient vector will always be a row vector. Depending on the context we will use the label f for both a polynomial and its coefficient vector. $(.)^T$ will denote the transpose of a matrix or vector. Points at infinity will play an important role in this article and these are naturally connected to homogeneous polynomials. A polynomial of degree d is homogeneous when every term is of degree d. A non-homogeneous polynomial can easily be made homogeneous by introducing an extra variable x_0.

Definition 2.2. *Let $f \in \mathcal{C}_d^n$ of degree d, then its homogenization $f^h \in \mathcal{C}_d^{n+1}$ is the polynomial obtained by multiplying each term of f with a power of x_0 such that its degree becomes d.*

Example 2.3. *Let*

$$f = x_1^2 + 9x_3 - 5,$$

then its homogenization is

$$f^h = x_1^2 + 9x_0x_3 - 5x_0^2.$$

The vector space of all homogeneous polynomials in $n+1$ variables and of degree d is denoted by $\mathcal{P}_d^n$. This vector space is spanned by all monomials in $n+1$ variables of degree d and hence

$$\dim\ \mathcal{P}_d^n = \binom{d+n}{n}. \tag{1}$$

In order to describe solution sets of systems of homogeneous polynomials, the projective space needs to be introduced. First, an equivalence relation $\sim$ on the non-zero points of $\mathbb{C}^{n+1}$ is defined by setting

$$(x_0', \ldots, x_n') \sim (x_0, \ldots, x_n)$$

if there is a non-zero $\lambda \in \mathbb{C}$ such that $(x_0', \ldots, x_n') = \lambda\,(x_0, \ldots, x_n)$.

Definition 2.3. *([4, p 368]) The n-dimensional projective space $\mathbb{P}^n$ is the set of equivalence classes of $\sim$ on $\mathbb{C}^{n+1} - \{0\}$. Each non-zero $(n+1)$-tuple $(x_0, \ldots, x_n)$ defines a point p in $\mathbb{P}^n$, and we say that $(x_0, \ldots, x_n)$ are homogeneous coordinates of p.*

The origin $(0,\ldots,0) \in \mathbb{C}^{n+1}$ is not a point in the projective space. Because of the equivalence relation $\sim$, an infinite number of projective points $(x_0,\ldots,x_n)$ can be associated with 1 affine point $(x_1,\ldots,x_n)$. The affine space $\mathbb{C}^n$ can be retrieved as a 'slice' of the projective space:

$$\mathbb{C}^n \; = \; \{(1, x_1, \ldots, x_n) \in \mathbb{P}^n\}.$$

This means that given a projective point $p = (x_0,\ldots,x_n)$ with $x_0 \neq 0$, its affine counterpart is $(1, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$. The projective points for which $x_0 = 0$ are called points at infinity.

2.2. Macaulay matrix

We now introduce the main object of this article, the Macaulay matrix, and give two interpretations to its row space. Both interpretations will be important later on when we discuss the null space of $M(d)$ and $M(d)^T$.

Definition 2.4. *Given a set of polynomials $f_1,\ldots,f_s \in \mathcal{C}^n$, each of degree $d_i\,(i = 1,\ldots,s)$, then the Macaulay matrix of degree d is the matrix containing the coefficients of*

$$M(d) \; = \; \begin{pmatrix} f_1 \\ x_1 f_1 \\ \vdots \\ x_n^{d-d_1} f_1 \\ f_2 \\ x_1 f_2 \\ \vdots \\ x_n^{d-d_s} f_s \end{pmatrix} \tag{2}$$

where each polynomial f_i is multiplied with all monomials from degree 0 up to $d - d_i$ for all $i = 1,\ldots,s$.

When constructing the Macaulay matrix, it is more practical to start with the coefficient vectors of the original polynomial system $f_1,\ldots,f_s$, after which all the rows corresponding to multiplied polynomials $x^a\, f_i$ up to a degree $\max(d_1,\ldots,d_s)$ are added. Then one can add the coefficient vectors of all polynomials $x^a\, f_i$ of one degree higher and so forth until the desired degree d is obtained. This is illustrated in the following example.

Example 2.4. *For the following polynomial system in* $\mathcal{C}_2^2$

$$\begin{cases} f_1: & x_1x_2 - 2x_2 & = & 0, \\ f_2: & x_2 - 3 & = & 0, \end{cases}$$

we have that $\max(d_1, d_2) = 2$ *and we want to construct* $M(3)$*. The first 2 rows then correspond with the coefficient vectors of* f_1, f_2*. Since* $\max(d_1, d_2) = 2$ *and* $d_2 = 1$*, the next 2 rows correspond to the coefficient vectors of* $x_1 f_2$ *and* $x_2 f_2$ *of degree 2. Notice that these first 4 rows make up* $M(2)$ *when the columns are limited to all monomials of degree 0 up to 2. The next rows that are added are the coefficient vectors of* $x_1 f_1, x_2 f_1$ *and* $x_1^2 f_2, x_1x_2 f_2, x_2^2 f_2$ *which are all polynomials of degree 3. This way of constructing the Macaulay matrix* $M(3)$ *then results in*

$$M(3) \;=\; \begin{array}{c} \\ f_1 \\ f_2 \\ x_1\,f_2 \\ x_2\,f_2 \\ x_1 f_1 \\ x_2 f_1 \\ x_1^2\,f_2 \\ x_1x_2\,f_2 \\ x_2^2\,f_2 \end{array} \begin{array}{c} \begin{array}{cccccccccc} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{array} \\ \left(\begin{array}{cccccccccc} 0 & 0 & -2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \end{array}\right) \end{array}.$$

Each row of the Macaulay matrix contains the coefficients of one of the f_i's. The multiplication of the f_i's with the monomials x^a results in the Macaulay matrix having a quasi-Toeplitz structure, in the sense of being almost or nearly Toeplitz. The Macaulay matrix depends explicitly on the degree d for which it is defined, hence the notation $M(d)$. The reason (2) is called the Macaulay matrix is because it was Macaulay who introduced this matrix, drawing from earlier work by Sylvester [19], in his work on elimination theory, resultants and solving multivariate polynomial systems [20, 21]. It is in fact a generalization of the Sylvester matrix to n variables and an arbitrary degree d. The MATLAB/Octave routine in the PNLA framework that returns $M(d)$ for a given polynomial system and degree d is getM.m.

For a given degree d, the number of rows $p(d)$ of $M(d)$ is given by the polynomial

$$p(d) \;=\; \sum_{i=1}^{s} \binom{d-d_i+n}{n} \;=\; \frac{s}{n!}\, d^n + O(d^{n-1}) \tag{3}$$

and the number of columns $q(d)$ by

$$q(d) \;=\; \binom{d+n}{n} \;=\; \frac{1}{n!}\, d^n + O(d^{n-1}). \tag{4}$$

From these two expressions it is clear that the number of rows will grow faster than the number of columns as soon as the total amount of multivariate polynomials $s > 1$. We denote the rank of $M(d)$ by $r(d)$ and the dimension of its left and right null space by $l(d)$ and $c(d)$ respectively. The rank-nullity theorems for $M(d)^T$ and $M(d)$ are then expressed as

$$\begin{aligned} q(d) &= r(d) + c(d), \\ p(d) &= r(d) + l(d). \end{aligned}$$

This shows that $r(d), l(d), c(d)$ are also polynomials over all positive integers $d > \max(d_1, \ldots, d_s)$. This polynomial increase of the dimensions of $M(d)$ is due to the combinatorial explosion of the number of monomials and is the main bottleneck when solving problems in practice. The following example illustrates this polynomial nature of $r(d), l(d), c(d)$, together with the interesting observation that the degree of $c(d)$ is linked to the dimension of the affine solution set of $f_1, \ldots, f_s$.

Example 2.5. *Consider the Macaulay matrix $M(d)$ of one multivariate polynomial $f \in C^n_{d_1}$. The structure of the matrix ensures that it is always of full row rank ($l(d) = 0$). Hence*

$$r(d) = p(d) = \binom{d-d_1+n}{n} = \frac{d^n}{n!} + \frac{n(n-2d_1+1)}{2n!} d^{n-1} + O(d^{n-2}),$$

and

$$\begin{aligned} c(d) &= q(d) - r(d) \\ &= \tfrac{d^n}{n!} + \tfrac{n(n+1)}{2n!} d^{n-1} + O(d^{n-2}) - \tfrac{d^n}{n!} - \tfrac{n(n-2d_1+1)}{2n!} d^{n-1} - O(d^{n-2}) \\ &= \tfrac{d_1}{(n-1)!} d^{n-1} + O(d^{n-2}). \end{aligned}$$

An interesting observation from Example 2.5 is that the dimension of the right null space is a polynomial of degree $n-1$. This corresponds intuitively with the dimension of the affine solution set. For example, the surface of a ball is 2-dimensional and is described by one polynomial in 3 variables ($n = 3$) of degree 2. The connection between the degree of $c(d)$ and the dimension of the solution set will be made more explicit in Section 4. We will now present two interpretations of the row space of the Macaulay matrix. The first is the affine interpretation of the row space of $M(d)$. The row space of $M(d)$, denoted by $\mathcal{M}_d$, contains all n-variate polynomials

$$\mathcal{M}_d = \left\{ \sum_{i=1}^{s} h_i\, f_i \ : \ h_i \in C^n_{d-d_i} \ (i = 1, \ldots, s) \right\}. \tag{5}$$

A polynomial ideal $\langle f_1, \ldots, f_s \rangle$ is defined as the set

$$\langle f_1, \ldots, f_s \rangle \ = \ \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in \mathcal{C}^n \right\}.$$

It is now tempting to have the following interpretation

$$\mathcal{M}_d \ = \ \langle f_1, \ldots, f_s \rangle \cap \mathcal{C}^n_d \triangleq \langle f_1, \ldots, f_s \rangle_d,$$

or in words: the row space of $M(d)$ contains all polynomials of the ideal $\langle f_1, \ldots, f_s \rangle$ from degree 0 up to d. This is not necessarily valid. $\mathcal{M}_d$ does not in general contain all polynomials of degree d that can be written as a polynomial combination (5).

Example 2.6. *Consider the following polynomial system in* $\mathcal{C}^2_1$

$$\begin{cases} f_1 : x_1^2 + 2x_1 + 1 &= 0, \\ f_2 : x_1^2 + x_1 + 1 &= 0. \end{cases}$$

From

$$(-1 - x_1)\, f_1 + (2 + x_1)\, f_2 = 1 \tag{6}$$

it follows that $1 \in \langle f_1, f_2 \rangle$. *However,* $1 \notin \mathcal{M}_2$. *In fact,* (6) *tells us that* $1 \in \mathcal{M}_3$. *Deciding whether a given multivariate polynomial* p *lies in the polynomial ideal generated by* $f_1, \ldots, f_s$ *is called the ideal membership problem. A numerical algorithm that solves this problem is also presented in [14].*

As Example 2.6 shows, the reason that not all polynomials of degree d lie in $\mathcal{M}_d$ is that it is possible that a polynomial combination of a degree higher than d is required. There is a different interpretation of the row space of $M(d)$ such that all polynomials of degree d are contained in it. This requires the notion of homogeneous polynomials and will be crucial in Section 4 to understand the null space of the Macaulay matrix. It will turn out that the dimension of the null space of $M(d)$ is related to the total number of projective roots of the polynomial system. This includes roots at infinity and in this way homogeneous polynomials are relevant. Given a set of non-homogeneous polynomials $f_1, \ldots, f_s$ we can also interpret $\mathcal{M}_d$ as the vector space

$$\mathcal{M}_d \;=\; \left\{ \sum_{i=1}^{s} h_i\, f_i^h \;:\; h_i \in \mathcal{P}^n_{d-d_i}\; (i = 1, \ldots, s) \right\}, \tag{7}$$

where the f_i^h's are homogeneous versions of $f_1, \ldots, f_s$ and the h_i's are also homogeneous. The corresponding homogeneous ideal is denoted by $\langle f_1^h, \ldots, f_s^h \rangle$. The homogeneity guarantees that all homogeneous polynomials of degree d are contained in $\mathcal{M}_d$. Or in other words,

$$\mathcal{M}_d \;=\; \langle f_1^h, \ldots, f_s^h \rangle_d,$$

where $\langle f_1^h, \ldots, f_s^h \rangle_d$ are all homogeneous polynomials of degree d contained in the homogeneous ideal $\langle f_1^h, \ldots, f_s^h \rangle$. An important consequence is then that

$$\dim \langle f_1^h, \ldots, f_s^h \rangle_d = r(d).$$

The homogenization of $f_1, \ldots, f_s$ typically introduces extra roots that satisfy $x_0 = 0$ and at least one $x_i \neq 0\,(i = 1, \ldots, s)$. These points are roots at infinity. We revisit Example 2.4 to illustrate this point.

Example 2.7. *The homogenization of the polynomial system in Example 2.4 is*

$$\begin{cases} f_1^h : & x_1 x_2 - 2x_2 x_0 &=& 0, \\ f_2^h : & x_2 - 3x_0 &=& 0. \end{cases}$$

All homogeneous polynomials $\sum_{i=1}^{2} h_i\, f_i^h$ *of degree 3 belong to the row space* *of*

$$
\begin{array}{c}
 \\ x_0f_1 \\ x_0^2f_2 \\ x_0x_1f_2 \\ x_0x_2f_2 \\ x_1f_1 \\ x_2f_1 \\ x_1^2\,f_2 \\ x_1x_2\,f_2 \\ x_2^2\,f_2
\end{array}
\begin{array}{c}
\begin{array}{cccccccccc}
x_0^3 & x_1x_0^2 & x_2x_0^2 & x_1^2x_0 & x_1x_2x_0 & x_2^2x_0 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3
\end{array} \\
\begin{pmatrix}
0 & 0 & -2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
-3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1
\end{pmatrix}
\end{array},
$$

which equals $M(3)$ from Example 2.4. Note that the non-homogeneous polynomial system had only 1 root $= \{(2,3)\}$. After homogenization, the resulting polynomial system f_1^h, f_2^h has 2 nontrivial roots $= \{(1,2,3),(0,1,0)\}$.

The homogeneous interpretation is in effect nothing but a relabelling of the columns and rows of $M(d)$. Both of these interpretations are used in this article. When discussing the left null space of $M(d)$ we will employ the affine interpretation, while for the right null space the homogeneous interpretation is important.

3. Left null space

In this section we present a detailed analysis of the left null space of $M(d)$. The main focus will be to derive the polynomial expression $l(d)$ for a given polynomial system $f_1, \ldots, f_s$. This will naturally lead to the notion of the degree of regularity, which will be important for describing the right null space. The left null space of $M(d)$, $\text{null}(M(d)^T)$, is the vector space

$$\text{null}(M(d)^T) = \{h \in \mathbb{R}^{p(d)} \mid h\, M(d) = 0\}.$$

The vectors h are not to be interpreted as polynomials but rather as s-tuples of multivariate polynomials. Indeed, from the affine row space interpretation we see that the expression $hM(d) = 0$ is equivalent with

$$\sum_{i=1}^{s} h_i\, f_i = 0. \tag{8}$$

The vector h therefore contains the coefficients of all polynomials h_i. A polynomial combination such as (8) is called a syzygy [22], from the Greek word $\sigma\upsilon\zeta\upsilon\gamma\iota\alpha$, which refers to an alignment of three celestial bodies. In our case, the polynomials h_i are thought to be in syzygy with the polynomials f_i, hence their polynomial combination is zero. This brings us to the interpretation of the dimension of the left null space, $l(d)$. It simply counts the total number of syzygies that occur in $\mathcal{M}_d$. It is therefore possible to identify with each syzygy a linearly dependent row of $M(d)$. The linear dependence of this particular row is then with respect to the remaining rows of $M(d)$.

3.1. Expressing $l(d)$ in terms of basis syzygies

Each element of the left null space corresponds with a syzygy of multivariate polynomials and with a linearly dependent row of the Macaulay matrix $M(d)$. Algorithm 3.1 finds a maximal set of such linearly dependent rows l for a given Macaulay matrix $M(d)$, starting from the top row r_1 where r_i stands for the ith row of the Macaulay matrix.

Algorithm 3.1. *Find a maximal set of linearly dependent rows*
Input: *Macaulay matrix $M(d)$*
Output: *a maximal set of linearly dependent rows l*

```
l ← ∅
if r_1 = 0 then
   l ← [l , r_1]
end if
for i = 2 : 1 : p(d) do
   if r_i linearly dependent with respect to {r_1, ..., r_{i-1}} then
      l ← [l , r_i]
   end if
end for
```

Once the linearly dependent rows of $M(d)$ are identified with Algorithm 3.1, it then becomes possible to write down a polynomial expression for $l(d)$. Indeed, suppose the first element l_1 of l is found using Algorithm 3.1. This row is then linearly dependent with respect to all rows above it. In fact, this linear dependence expresses a certain syzygy $\sum_{i=1}^{s} h_i\, f_i = 0$. The row l_1 then also corresponds with a certain monomial multiple $x_i^{\alpha}\, f_k$ since it is a row of the Macaulay matrix. Observe now that

$$x_j^{\beta} \sum_{i=1}^{s} h_i \, f_i = 0,$$

which means that all rows corresponding with $x_j^{\beta} x_i^{\alpha} \, f_k$ will also be linearly dependent. We will call l_1 in this case a basis syzygy and its monomial multiples $x_j^{\beta} l_1$, derived syzygies. The degree of a basis syzygy is taken to be the maximal degree over its terms. The above observation can now be summarized in the following lemma.

Lemma 3.1. *If a basis syzygy l has a degree d_l, then it introduces a term*

$$\binom{d - d_l + n}{n} \tag{9}$$

to the polynomial $l(d)$.

Proof 3.1. *This follows from $x_j^{\beta} \sum_{i=1}^{s} h_i \, f_i = 0$ and the fact that the total number of monomials x_j^{β} at a degree $d \geq d_l$ is given by* (9).

It can be shown that the number of basis syzygies is finite. This is in fact linked with the finiteness of the Gröbner basis for a polynomial ideal [5, p. 223]. We will now assume that all basis syzygies were found, using for example Algorithm 3.1 for a sufficiently large degree d, and explain how all basis syzygies can be used to derive an expression for the polynomial $l(d)$. As mentioned above, each linearly dependent row can be labelled as a monomial multiple of one of the polynomials $f_1, \ldots, f_s$. The first step of the syzygy analysis is to divide the basis syzygies into groups according to the polynomial that is multiplied. The following example illustrates this grouping of basis syzygies.

Example 3.1. *Consider the following polynomial system in C^3*

$$\left\{ \begin{array}{lccc} f_1 : & x^2 \, y^2 + z & = & 0, \\ f_2 : & x \, y - 1 & = & 0, \\ f_3 : & x^2 + z & = & 0, \end{array} \right.$$

where $x_1 = x$, $x_2 = y$, $x_3 = z$. The first basis syzygy is found, using Algorithm 3.1, in $M(4)$ and corresponds with the row

$$xy \, f_3.$$

The remaining basis syzygies are all found in $M(6)$ and correspond with the rows

$$x^3y\, f_2,\; x^2y^2\, f_2,\; xy^2z\, f_2.$$

We can now divide these basis syzygies into the following two groups

$$\{xy\, f_3\} \quad \textit{and} \quad \{x^3y\, f_2, x^2y^2\, f_2, xy^2z\, f_2\},$$

which is one group for f_3 and one group for f_2.

The key observation here is that each of these groups can be analysed separately since no interference between rows of different groups is possible (indeed, they involve different polynomials). We will now continue Example 3.1 and show how all contributions of basis syzygies to $l(d)$ are described by binomial coefficients.

Example 3.2. *The first group $\{xy\, f_3\}$ has only one element and describes a syzygy of degree 4. Lemma 3.1 tells us then that this will introduce a term*

$$\binom{d-4+3}{3}$$

to $l(d)$. We can therefore write

$$l(d) \;=\; \binom{d-4+3}{3} \;=\; \frac{1}{6}d^3 - d^2 + \frac{11}{6}\,d - 1.\; (d \geq 4) \tag{10}$$

The second group has three basis syzygies, $\{x^3y\, f_2, x^2y^2\, f_2, xy^2z\, f_2\}$, of degree 6 and therefore introduces 3 terms

$$\binom{d-6+3}{3}.$$

We can therefore update $l(d)$ to

$$\begin{aligned} l(d) &= \tbinom{d-4+3}{3} + 3\,\tbinom{d-6+3}{3} \\ &= \tfrac{2}{3}d^3 - 7d^2 + \tfrac{76}{3}d - 31.\; (d \geq 4). \end{aligned} \tag{11}$$

Expression (11) for $l(d)$ is still valid for degrees $d \geq 4$, since the 3 extra binomial coefficient terms correspond with polynomials that have roots at $d \in \{3,4,5\}$. The difference between (10) and (11) is only visible therefore for

$d \geq 6$. We have not yet found the final expression for $l(d)$ however. The 3 binomial coefficient terms at degree 6 will count too many contributions. Take for example the basis syzygies corresponding with the rows x^3yf_2 and $x^2y^2f_2$. Their least common multiple is $x^3y^2f_2$, which means that the linearly dependent row $x^3y^2f_2$ will be counted twice by (11). *It should however be counted only once.*

Example 3.2 shows that the the analysis of all syzygies is reduced to a combinatorial problem: within a group of basis syzygies, one needs to count the total number of linearly dependent rows these basis syzygies 'generate'. This combinatorial problem is solved by the Inclusion-Exclusion principle.

Theorem 3.1. *(Inclusion-Exclusion Principle [4, p. 454]) Let $A_1, \ldots, A_n$ be a collection of finite sets with $|A_i|$ the cardinality of A_i. Then*

$$|\cup_{i=1}^{n} A_i| \;=\; \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \leq i_1 < \ldots < i_k \leq n} |A_{i_1} \cap \ldots \cap A_{i_k}| \right). \tag{12}$$

The Inclusion-Exclusion Principle is the final component that allows us to conclude the analysis of all syzygies of Example 3.2.

Example 3.3. *If we denote the set of all monomial multiples of $x^3y\, f_2$ by A_1 and likewise A_2, A_3 for $x^2y^2\, f_2, xy^2z\, f_2$ respectively, then applying Theorem 3.1 on these sets results in the final expression for $l(d)$. Note that all terms of* (12) *for $k = 1$ are the binomial coefficients of Lemma 3.1, which already have been added to $l(d)$ in* (11). *The remaining analysis is hence on all terms of* (12) *for $k \geq 2$. The cardinality of the intersections $A_1 \cap A_2, A_1 \cap A_3, A_2 \cap A_3$ are described by the binomial coefficients*

$$\binom{d-7+3}{3}, \binom{d-7+3}{3}, \binom{d-8+3}{3},$$

which will each contribute to $l(d)$ with a minus sign since $k = 2$. The degrees for which these terms are introduced are the degrees of the least common multiples between $x^3y\, f_2$ and $x^2y^2\, f_2$, between $x^3y\, f_2$ and $xy^2z\, f_2$ and between $x^2y^2\, f_2$ and $xy^2z\, f_2$. These degrees are 7, 8 and 7 respectively. The next intersection, $A_1 \cap A_2 \cap A_3$, corresponds with a binomial term introduced at the degree of the least common multiple of all 3 basis syzygies in f_2. This least *common multiple is $x^3y^2z\, f_2$ with a degree of 8. This concludes the analysis of all linearly dependent rows of $M(d)$ and we can therefore write*

$$\begin{aligned} l(d) &= \tbinom{d-4+3}{3} + 3\tbinom{d-6+3}{3} - 2\tbinom{d-7+3}{3} - \tbinom{d-8+3}{3} + \tbinom{d-8+3}{3} \\ &= \tbinom{d-4+3}{3} + 3\tbinom{d-6+3}{3} - 2\tbinom{d-7+3}{3} \\ &= \tfrac{1}{3}d^3 - 2d^2 + \tfrac{2}{3}d + 9.\ (d \geq 4) \end{aligned}$$

Note that the terms at degree 8 have cancelled one another. Since the term $\binom{d-7+3}{3}$ has roots at $d \in \{4, 5, 6\}$, this expression for $l(d)$ is valid for all $d \geq 4$.

An important observation is that once the polynomial expression $l(d)$ is known, then the rank of $M(d)$ and the dimension of its null space are also fully determined for all $d \geq 4$ by:

$$\begin{aligned} r(d) &= p(d) - l(d) = \frac{1}{6}d^3 + d^2 + \frac{5}{6}d - 10, \\ c(d) &= q(d) - r(d) = d + 11. \end{aligned}$$

Algorithm 3.2 summarizes the iterative syzygy analysis outlined above to determine the polynomial expression for $l(d)$.

Algorithm 3.2. *Find $l(d)$*
Input: *polynomial system $f_1, \ldots, f_n \in \mathcal{C}^n$*
Output: *$l(d)$*

$d \leftarrow max(deg(f_1), deg(f_2), \ldots, deg(f_s))$
$l \leftarrow \varnothing$
$l(d) \leftarrow \varnothing$
while *not all basis syzygies found* ***do***
  find new basis syzygies l using Algorithm 3.1 on $M(d)$
  update $l(d)$ using Lemma 3.1 and the Inclusion-Exclusion principle
  $d \leftarrow d + 1$
end while

A stop criterion is needed to be able to decide whether all basis syzygies have been found. This is intimately linked with the occurrence of a Gröbner basis in $\mathcal{M}_d$. Indeed, it is a well-known result that all basis syzygies of

$\langle f_1, \ldots, f_s \rangle$ can be determined from a Gröbner basis [5, p. 223]. The reduction to zero of every S-polynomial of a pair of polynomials in a Gröbner basis provides a basis syzygy. This implies that it is required to construct $M(d)$ for a degree which contains all these S-polynomials. The link between a Gröbner basis and $\mathcal{M}_d$ is described in detail in [14]. The finiteness of the amount of basis syzygies has a very important consequence. It ensures that Algorithm 3.2 stops and that the polynomial expressions for $l(d), r(d)$ and $c(d)$ do not change anymore after a finite amount of steps. As a consequence, the domain of the final polynomial expressions for $l(d), r(d)$ and $c(d)$ has a particular lower bound $d^\star$. In Example 3.3, the domain of these polynomials was lower bounded by 4. We will call this lower bound on the domain of the final polynomial expressions for $l(d), r(d)$ and $c(d)$ the degree of regularity.

Definition 3.1. *The minimal degree $d^\star \in \mathbb{N}$ for which the output of Algorithm 3.2 describes the dimension of the left null space of $M(d)$ is called the degree of regularity.*

This degree of regularity is of vital importance in the next section where we discuss the right null space of $M(d)$. From the analysis above we see that in order to find the degree of regularity $d^\star$, it is required to construct the Macaulay matrix for a degree larger than $d^\star$. For example, the degree of regularity $d^\star = 4$ of the polynomial system in Example 3.1 was found from $M(6)$. The following example illustrates that the degree for which all basis syzygies are found can be quite high and consequently that the total number of binomial terms of $l(d)$ can be very large.

Example 3.4. *Consider the following polynomial system in C^4*

$$\begin{cases} f_1: & x_2^2\,x_3 + 2\,x_1\,x_2\,x_4 - 2\,x_1 - x_3 = 0, \\ f_2: & -x_1^3\,x_3 + 4\,x_1\,x_2^2\,x_3 + 4\,x_1^2\,x_2\,x_4 + 2\,x_2^3\,x_4 + 4\,x_1^2 - 10\,x_2^2 \\ & +4\,x_1\,x_3 - 10\,x_2\,x_4 + 2 = 0, \\ f_3: & 2\,x_2\,x_3\,x_4 + x_1\,x_4^2 - x_1 - 2\,x_3 = 0, \\ f_4: & -x_1\,x_3^3 + 4\,x_2\,x_3^2\,x_4 + 4\,x_1\,x_3\,x_4^2 + 2\,x_2\,x_4^3 + 4\,x_1\,x_3 \\ & +4\,x_3^2 - 10\,x_2\,x_4 - 10\,x_4^2 + 2 = 0, \end{cases}$$

with degrees $d_1 = d_3 = 3$, $d_2 = d_4 = 4$. The first basis syzygy group is found in $M(7)$ and corresponds with the row $x_2^2\,x_3\,f_2$. The next basis syzygies group *are the rows*

$$\{x_2^2\,x_3\,f_3,\ x_2^3\,x_4\,f_3,\ x_1\,x_2^2\,x_4^2\,f_3,\ x_1^3\,x_2\,x_3^2\,f_3,\ x_1^2\,x_2\,x_4^3\,f_3,\ x_1^4\,x_3\,x_4^4\,f_3,\ x_1^2\,x_2\,x_3^4\,x_4^2\,f_3,$$
$$x_2^2\,x_4^7\,f_3,\ x_1^2\,x_2\,x_3^6\,x_4\,f_3,\ x_1\,x_2\,x_4^8\,f_3,\ x_1^2\,x_2\,x_3^8\,f_3,\ x_1^3\,x_3\,x_4^8\,f_3\}$$

and are found for the degrees

$$\{6,\ 7,\ 8,\ 9,\ 9,\ 12,\ 12,\ 12,\ 13,\ 13,\ 14,\ 15\}.$$

The last basis syzygy group are the rows

$$\{x_2^2\,x_3\,f_4,\ x_2\,x_3\,x_4\,f_4,\ x_1\,x_2\,x_4^2\,f_4,\ x_2^3\,x_4\,f_4,\ x_1^3\,x_4^2\,f_4,\ x_1^2\,x_4^3\,f_4,\ x_1^4\,x_3\,x_4\,f_4,$$
$$x_1^3\,x_2\,x_3^2\,f_4,\ x_1^3\,x_3^2\,x_4\,f_4,\ x_1^2\,x_3^3\,x_4\,f_4,\ x_1\,x_2^5\,f_4,\ x_1^5\,x_3^2\,f_4,\ x_1^4\,x_3^3\,f_4,\ x_1^3\,x_3^4\,f_4\}$$

and are found for the degrees

$$\{7,\ 7,\ 8,\ 8,\ 9,\ 9,\ 10,\ 10,\ 10,\ 10,\ 10,\ 11,\ 11,\ 11\}.$$

Application of the Inclusion-Exclusion Principle for each of these groups results in the final expression

$$\begin{aligned} l(d) &= \tbinom{d-6+4}{4} + 4\tbinom{d-7+4}{4} + \tbinom{d-8+4}{4} - 6\tbinom{d-11+4}{4} + 4\tbinom{d-13+4}{4} - \tbinom{d-14+4}{4} \\ &= \tfrac{1}{8}\,d^4 - \tfrac{13}{12}\,d^3 - \tfrac{5}{8}\,d^2 + \tfrac{19}{12}\,d + 105.\ (d \geq 10) \end{aligned}$$

Observe that $l(d)$ consists in fact of 10241 binomial terms, of which 10225 cancel out until only 16 terms are left.

As Example 3.4 shows, using Algorithm 3.2 to find the expression for $l(d)$ results in a large number of binomial terms. A large number of computations are actually wasted since most of these binomial terms cancel out and therefore do not contribute to $l(d)$. This approach has the disadvantage that the total number of binomial terms that needed to be computed grows combinatorially, while in fact the majority of them cancel one another. Algorithm 3.3 remedies this disadvantage. This iterative algorithm does not need to check each row of the Macaulay matrix, nor has to use the Inclusion-Exclusion Principle to find the final expression of $l(d)$ and corresponding degree of regularity $d^\star$. Instead of finding basis syzygies and calculating how these will propagate to higher degrees, we will simply update $l(d)$ iteratively. The algorithm is presented in pseudo-code in Algorithm 3.3. The main idea is to compute the numerical value $p(d) - r(d)$ and compare it with the evaluation of $l(d)$ for each degree d. Here $p(d)$ does not represent the polynomial expression in d but rather the evaluation of this polynomial for the value of d in the algorithm. The polynomial expression for $r(d)$ is not known and hence cannot be evaluated but this evaluation is found by the determination of the numerical rank of $M(d)$. If $p(d) - r(d) > l(d)$, then the polynomial $l(d)$ needs to count $p(d) - r(d) - l(d)$ additional linearly dependent rows. Furthermore, each of these additional rows will propagate to higher degrees and give rise to extra binomial terms. Similarly, if $p(d)-r(d) < l(d)$, then too many linearly dependent rows were counted and $l(d)$ needs to be adjusted with $l(d) - p(d) + r(d)$ negative binomial contributions. The $p(d) - r(d) < l(d)$ degrees for which positive contributions to $l(d)$ are made are stored in the vector d_+ and likewise for the $l(d)-p(d)+r(d)$ negative contributions in d_-. All information on how to express $l(d)$ in terms of binomial coefficients is hence stored in d_+ and d_-. Iterations need to start from a degree $d = \min(\deg(f_1), \deg(f_2), \ldots, \deg(f_s))$ to make sure that the updating of $l(d)$ reflects the correct occurrence of new basis and derived syzygies. Obviously, when there are polynomials f_i of $f_1, \ldots, f_s$ with a degree higher than $\min(\deg(f_1), \deg(f_2), \ldots, \deg(f_s))$, then they are not included in $M(d)$ for that particular degree. Since the algorithm iterates over the degrees, a Singular Value Decomposition (SVD)-based recursive orthogonalization algorithm [23] can be used to determine the numerical value $r(d)$ for each iteration. The binomial term in $l(d)$ that appears at the highest degree $d_{\max} = \max(d_+, d_-)$ determines the degree of regularity $d^\star$. Indeed, the polynomial

$$\binom{d - d_{\max} + n}{n}$$

has zeros for $d = \{d_{\max} - n, d_{\max} - n + 1, \ldots, d_{\max} - 1\}$ and therefore the final expression for $l(d)$ is valid for all $d \geq d^\star = d_{\max} - n$. An upper bound for $d_{\max}$ comes from the theory of resultants. Macaulay showed in [20] that it is possible to determine whether a homogeneous polynomial system $f_1^h, \ldots, f_n^h$ of degrees $d_1, \ldots, d_n$ has a nontrivial common root by computing the determinant of a submatrix of $M(d)$ for $d = \sum_{i=1}^n d_i - n + 1$. This essentially means that $d^\star \leq \sum_{i=1}^n d_i - n + 1$, which results in a maximal degree of $1 + \sum_{i=1}^n d_i$ in Algorithm 3.3.

Algorithm 3.3. *Find $l(d)$ and degree of regularity $d^\star$*
Input: *polynomial system $f_1, \ldots, f_n \in \mathcal{C}^n$*
Output: *$l(d)$ and degree of regularity $d^\star$*

$d \leftarrow min(deg(f_1), deg(f_2), \ldots, deg(f_s))$
$d_+ \leftarrow \varnothing$
$d_- \leftarrow \varnothing$
$l(d) \leftarrow 0$
$r(d) \leftarrow rank\ M(d)$
while $d \leq 1 + \sum_i^s deg(f_i)$ ***do***
  if $p(d) - r(d) > l(d)$ ***then***
    add d $p(d) - r(d) - l(d)$ times to d_+
  else if $p(d) - r(d) < l(d)$ ***then***
    add d $l(d) - p(d) + r(d)$ times to d_-
  end if
  $l(d) \leftarrow \sum_{i=1}^{|d_+|} \binom{d-d_+(i)+n}{n} - \sum_{i=1}^{|d_-|} \binom{d-d_-(i)+n}{n}$
  $d \leftarrow d + 1$
  $r(d) \leftarrow rank\ M(d)$
end while
$d^\star \leftarrow max(d_+, d_-) - n$

Symbolical methods compute a Gröbner basis G of $f_1, \ldots, f_s$ in order to describe all basis syzygies and find the degree of regularity. Algorithm 3.3 does not require the computation of a Gröbner basis. Instead, one needs to determine the numerical rank of $M(d)$ for increasing degrees d. Algorithm 3.3 is implemented in the MATLAB/Octave routine aln.m.

Example 3.5. *We illustrate Algorithm 3.3 with the polynomial system from Example 3.4:*

$$\begin{cases} f_1: & x_2^2\,x_3 + 2\,x_1\,x_2\,x_4 - 2\,x_1 - x_3 = 0, \\ f_2: & -x_1^3\,x_3 + 4\,x_1\,x_2^2\,x_3 + 4\,x_1^2\,x_2\,x_4 + 2\,x_2^3\,x_4 + 4\,x_1^2 - 10\,x_2^2 \\ & +4\,x_1\,x_3 - 10\,x_2\,x_4 + 2 = 0, \\ f_3: & 2\,x_2\,x_3\,x_4 + x_1\,x_4^2 - x_1 - 2\,x_3 = 0, \\ f_4: & -x_1\,x_3^3 + 4\,x_2\,x_3^2\,x_4 + 4\,x_1\,x_3\,x_4^2 + 2\,x_2\,x_4^3 + 4\,x_1\,x_3 \\ & +4\,x_3^2 - 10\,x_2\,x_4 - 10\,x_4^2 + 2 = 0. \end{cases}$$

The expression for $l(d)$ is initialized to 0. The Macaulay matrix is of full row rank for degrees 3, 4 and 5. For $d = 6$, we have that $p(6) - r(6) = 100 - 99 =$

$1 > l(6) = 0$. *We therefore set* $d_+ = 6$ *and*

$$l(d) = \binom{d-6+4}{4}.$$

After incrementing the degree we find that $p(7) - r(7) = 210 - 201 = 9 > l(7) = 5$ *and we therefore update* d_+ *and* $l(d)$ *to* $d_+ = \{6, 7, 7, 7, 7\}$ *and*

$$l(d) = \binom{d-6+4}{4} + 4\binom{d-7+4}{4}$$

respectively. The algorithm finishes at $d = 14$ *with*

$$d_+ = \{6, 7, 7, 7, 7, 8, 13, 13, 13, 13\},$$

and

$$d_- = \{11, 11, 11, 11, 11, 11, 14\},$$

which indeed corresponds with the final expression for $l(d)$

$$\begin{aligned} l(d) &= \tbinom{d-6+4}{4} + 4\tbinom{d-7+4}{4} + \tbinom{d-8+4}{4} + 4\tbinom{d-13+4}{4} - 6\tbinom{d-11+4}{4} - \tbinom{d-14+4}{4} \\ &= \tfrac{1}{8}\,d^4 - \tfrac{13}{12}\,d^3 - \tfrac{5}{8}\,d^2 + \tfrac{19}{12}\,d + 105.\ (d \geq 10) \end{aligned}$$

Observe that Algorithm 3.3 finds the desired expression for $l(d)$ *at* $d = 14$. *In contrast, the basis syzygies analysis using Algorithm 3.2 required the construction of* $M(15)$ *and the computation of 10241 binomial terms. From Algorithm 3.3 we can derive that the dimension of the left null space of* $M(d)$ *is described by the following piecewise-defined function*

$$l(d) = \begin{cases} 0, & \text{if} \quad 3 \leq d \leq 5 \\ \frac{d^4}{24} - \frac{7d^3}{12} + \frac{71d^2}{24} - \frac{77d}{12} + 5, & \text{if} \quad d = 6 \\ \frac{d^4}{4} - \frac{9d^3}{2} + \frac{121d^2}{4} - 90d + 100, & \text{if} \quad 7 \leq d \leq 10 \\ \frac{1}{8}\,d^4 - \frac{13}{12}\,d^3 - \frac{5}{8}\,d^2 + \frac{19}{12}\,d + 105, & \text{if} \quad d \geq 10. \end{cases}$$

The minimal degree for which the final polynomial expression for $l(d)$ *is valid is 10. Hence the degree of regularity is* $d^\star = 10$.

4. Right Null Space

The knowledge that $c(d)$ is a polynomial in d together with the homogeneous interpretation of $\mathcal{M}_d$ allows us to link the null space of the Macaulay matrix with the number of projective roots of $f_1, \ldots, f_s$. The notion of the dual of the row space will play an important role in describing these roots. After having described this dual vector space we will extend the monomial multiplication property of Stetter's eigenvalue problem [10, 11] to the projective case.

4.1. Link with projective roots

It is a classic result that for a polynomial system $f_1^h, \ldots, f_s^h$ with a finite number of projective roots, the quotient ring $\mathcal{P}^n / \langle f_1^h, \ldots, f_s^h \rangle$ is a finite-dimensional vector space [5, 4]. The dimension of this vector space equals the total number of projective roots of $f_1^h, \ldots, f_s^h$, counting multiplicities. From the rank-nullity theorem of $M(d)$ it then follows that

$$\begin{aligned} c(d) &= q(d) - r(d) \\ &= \dim\, \mathcal{P}_d^n - \dim\, \langle f_1^h, \ldots, f_s^h \rangle_d \\ &= \dim\, \mathcal{P}_d^n / \langle f_1^h, \ldots, f_s^h \rangle_d \end{aligned} \tag{13}$$

This leads to the following theorem.

Theorem 4.1. *For a zero-dimensional homogeneous ideal $\langle f_1^h, \ldots, f_s^h \rangle$ with m projective roots (counting multiplicities) and degree of regularity $d^\star$ we have that*

$$c(d) \;=\; m \quad \forall\, d \geq d^\star.$$

Proof 4.1. *This follows from* (13) *and Definition 3.1.*

Furthermore, when $s = n$, then $c(d) = m = d_1 \cdots d_s$ according to Bézout's Theorem [5, p.97]. This effectively links the degrees of the polynomials $f_1, \ldots, f_s$ to the nullity of the Macaulay matrix. The affine roots can be retrieved from a generalized eigenvalue problem as discussed in [24, 11]. In this article we will extend this generalized eigenvalue approach to the projective case. Another interesting result is that the degree of the polynomial $c(d)$ is the dimension of projective variety of $f_1^h, \ldots, f_s^h$.

Definition 4.1. *The polynomial*

$$c(d) \ = \ dim \ \mathcal{P}_d^n / \langle f_1^h, \ldots, f_s^h \rangle_d \ (\forall \, d \geq d^\star)$$

is called the projective Hilbert Polynomial [4, p. 462]. The degree of this polynomial $c(d)$ equals the dimension of the projective variety [4, p.463].

Example 4.1. *For the polynomial system from Example 3.1 we had that $c(d) = d + 11$. Since this is a polynomial of degree 1, it follows that the projective solution set of $f_1^h, \ldots, f_s^h$ is one-dimensional. The number of affine solutions of $f_1^h, \ldots, f_s^h$ is finite: $\{(1,1,1,-1),(1,-1,-1,-1)\}$, which implies that the non-zero-dimensional part of the solution set lies 'at infinity'.*

4.2. Dual vector space

As soon as $d \geq d^\star$ and the number of projective roots is finite, then a basis of the null space can be explicitly written down in terms of the roots. This requires the notion of the dual vector space. We denote the dual vector space of $\mathcal{C}_d^n$ by $\mathcal{C}_d^{n'}$, the dual of $\mathcal{M}_d$ by $\mathcal{M}_d'$ and the annihilator of $\mathcal{M}_d$ by $\mathcal{M}_d^o$. By definition, the elements of $\mathcal{M}_d^o$ map each element of $\mathcal{M}_d$ to zero. Therefore, dim $\mathcal{M}_d^o = c(d)$, which implies $\mathcal{M}_d^o \cong \text{null}(M(d))$. A basis for $\mathcal{M}_d^o$ is described by differential functionals.

Definition 4.2. *([11, p 8]) Let $j \in \mathbb{N}_0^n$ and $z \in \mathbb{C}^n$, then the differential functional $\partial_j|_z \in \mathcal{C}_d^{n'}$ is defined by*

$$\partial_j|_z \equiv \frac{1}{j_1! \ldots j_n!} \, \frac{\partial^{j_1+\ldots+j_n}}{\partial x_1^{j_1} \ldots \partial x_n^{j_n}}|_z$$

where $|_z$ stands for evaluation in $z = (x_1, \ldots, x_n)$.

Being elements of the dual vector space, these differential functionals $\partial_j|_z$ can be represented as vectors. This is illustrated in the following simple example.

Example 4.2. *In $\mathcal{C}_3^{2'}$ the functionals $\partial_{00}|_z, \partial_{10}|_z, \partial_{01}|_z, \partial_{20}|_z, \partial_{11}|_z$ and $\partial_{02}|_z$*

have the following coefficient vectors

$$
(14) \qquad \begin{array}{cccccc}
\partial_{00}|_z & \partial_{10}|_z & \partial_{01}|_z & \partial_{20}|_z & \partial_{11}|_z & \partial_{02}|_z
\end{array}
$$
$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
x_1 & 1 & 0 & 0 & 0 & 0 \\
x_2 & 0 & 1 & 0 & 0 & 0 \\
x_1^2 & 2x_1 & 0 & 1 & 0 & 0 \\
x_1x_2 & x_2 & x_1 & 0 & 1 & 0 \\
x_2^2 & 0 & 2x_2 & 0 & 0 & 1 \\
x_1^3 & 3x_1^2 & 0 & 3x_1 & 0 & 0 \\
x_1^2x_2 & 2x_1x_2 & x_1^2 & x_2 & 2x_1 & 0 \\
x_1x_2^2 & x_2^2 & 2x_1x_2 & 0 & 0 & x_1 \\
x_2^3 & 0 & 3x_2^2 & 0 & 0 & 3x_2
\end{pmatrix},
$$

with $z = (x_1, x_2) \in \mathbb{C}^2$. *The homogeneous interpretation of* $\mathcal{M}_d$ *implies that the differential functionals also have a homogeneous interpretation. For the example above, the coefficient vectors of the corresponding differential functionals in* $\mathcal{P}_3^{2'}$ *are*

$$
(15) \qquad \begin{array}{cccccc}
\partial_{000}|_z & \partial_{010}|_z & \partial_{001}|_z & \partial_{020}|_z & \partial_{011}|_z & \partial_{002}|_z
\end{array}
$$
$$
\begin{pmatrix}
x_0^3 & 0 & 0 & 0 & 0 & 0 \\
x_0^2x_1 & x_0^2 & 0 & 0 & 0 & 0 \\
x_0^2x_2 & 0 & x_0^2 & 0 & 0 & 0 \\
x_0x_1^2 & 2x_0x_1 & 0 & x_0 & 0 & 0 \\
x_0x_1x_2 & x_0x_2 & x_0x_1 & 0 & x_0 & 0 \\
x_0x_2^2 & 0 & 2x_0x_2 & 0 & 0 & x_0 \\
x_1^3 & 3x_1^2 & 0 & 3x_1 & 0 & 0 \\
x_1^2x_2 & 2x_1x_2 & x_1^2 & x_2 & 2x_1 & 0 \\
x_1x_2^2 & x_2^2 & 2x_1x_2 & 0 & 0 & x_1 \\
x_2^3 & 0 & 3x_2^2 & 0 & 0 & 3x_2
\end{pmatrix},
$$

with $z = (x_0, x_1, x_2) \in \mathbb{P}^2$. *The matrix in* (14) *can be retrieved from* (15) *by setting* $x_0 = 1$.

We will make no further distinction between the linear functionals $\partial_j|_z$ and their coefficient vectors. Notice that these coefficient vectors are column vectors, since they are the dual elements of the row space of $M(d)$. The vectors $\partial_0|_z$ in the affine case can be seen as a generalization of the Vandermonde structure to the multivariate case. Applying the differential functional

$\partial_j|_z$ to the elements of $\mathcal{M}_d$ is then simply the matrix vector multiplication $M(d)\,\partial_j|_z$.

We know that when a polynomial system $f_1^h, \ldots, f_s^h$ has a finite number of m projective roots, then $\dim \mathcal{M}_d^o = c(d) = m$ for all $d \geq d^\star$. Hence, a basis for $\mathcal{M}_d^o$ will consist of differential functionals, evaluated in each projective root and taking multiplicities into account. This brings us to the definition of the canonical null space of $M(d)$.

Definition 4.3. *Let $f_1, \ldots, f_s \in \mathcal{C}^n$ with a zero-dimensional projective solution set and let $m_1, \ldots, m_t$ be the multiplicities of the t projective roots $z_i\,(1 \leq i \leq t)$ such that $\sum_{i=1}^t m_i = m$. Then for all $d \geq d^\star$ there exists a matrix K of m linearly independent columns such that*

$$M(d)\;K \;=\; 0.$$

Furthermore, K can be partitioned into

$$K = \begin{pmatrix} K_1 & K_2 & \ldots & K_t \end{pmatrix},$$

such that each K_i consists of m_i linear combinations of differential functionals $\partial_j|_{z_i} \in \mathcal{P}_d^{n'}\,(1 \leq i \leq t)$. We will call this matrix K the canonical null space of $M(d)$.

Definition 4.3 explicitly depends on the homogeneous interpretation of $\mathcal{M}_d$. Indeed, it is only for the homogeneous case that the projective roots come into the picture. The following example illustrates the structure of the canonical null space K for a small example.

Example 4.3. *Let us reconsider the small polynomial system from Example 2.4*

$$\left\{ \begin{array}{lrcl} f_1: & x_1x_2 - 2x_2 & = & 0, \\ f_2: & x_2 - 3 & = & 0, \end{array} \right.$$

with 1 affine root $(2,3)$. From Example 2.7 we know that its corresponding projective variety consists of 2 points: the affine solution $(1,2,3)$ and the root at infinity $(0,1,0)$. Indeed, $c(d) = 2\ \ (d \geq 2)$ and therefore the canonical null *space is*

$$
\begin{aligned}
K &= \begin{pmatrix} \partial_{000}|_{(1,2,3)} & \partial_{000}|_{(0,1,0)} \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 2 & 0 \\ 3 & 0 \\ 4 & 1 \\ 6 & 0 \\ 9 & 0 \end{pmatrix}.
\end{aligned}
$$

Defining the multiplicity of a zero using the dual space goes back to Macaulay [21]. It is also reminiscent of the univariate case. Remember that for a univariate polynomial $f(x) \in \mathcal{C}^1_d$, a zero z with multiplicity m means that

$$
\begin{pmatrix} f \\ f\,D_1 \\ \vdots \\ f\,D_{m-1} \end{pmatrix} \partial_0|_z \;=\; 0, \tag{16}
$$

where D_i is the i^{th} order differential operator. Or in other words, $f(z) = f'(z) = f^{''} = \ldots = f^{(m-1)}(z) = 0$. Alternatively, (16) can be written as

$$
f \;\begin{pmatrix} \partial_0|_z & \partial_1|_z & \partial_2|_z & \ldots & \partial_{m-1}|_z \end{pmatrix} \;=\; 0. \tag{17}
$$

As already mentioned in Definition 4.3, the multivariate case generalizes this principle by requiring linear combinations of differential functionals.

Example 4.4. *Consider the following polynomial system in $\mathcal{C}^2_2$ with the affine root $z = (1,2,3) \in \mathbb{P}^2$ of multiplicity 4 and no roots at infinity*

$$
\left\{ \begin{array}{rcl} (x_2-3)^2 &=& 0, \\ (x_1+1-x_2)^2 &=& 0. \end{array} \right.
$$

The degree of regularity $d^\star$ is 2 and the canonical null space is

$$
K \;=\; \begin{pmatrix} \partial_{000}|_{(1,2,3)} & \partial_{100}|_{(1,2,3)} & \partial_{010}|_{(1,2,3)} & \partial_{110}|_{(1,2,3)} - 2\partial_{020}|_{(1,2,3)} \end{pmatrix}. \tag{18}
$$

The different linear combinations of functionals needed to construct K_i are called the multiplicity structure of the root z_i. Observe that the multiplicity structure of a root is not unique. Indeed, for any nonsingular $m_i \times m_i$ matrix T we have that the column space of K_i equals the column space of $K_i T$. Finding the multiplicity structure for a given root of a polynomial system is an active area of research [25, 26]. Iterative algorithms to compute the multiplicity structure of a root z such as in [26] exploit the closedness property of the differential functionals $\partial_j|_z$ [11, p. 330] to reduce the size of the matrices in every iteration. We will not further discuss these algorithms here.

4.3. Projective multiplication matrices and Stetter's eigenvalue problem

Stetter's approach to find the affine roots of multivariate polynomial systems is to phrase it as an eigenvalue problem [10, 11]. This eigenvalue problem expresses the multiplication of monomials within the quotient space $\mathcal{C}^n/\langle f_1, \ldots, f_s \rangle$. The standard procedure to find the affine roots is

1. to compute a Gröbner basis G for $\langle f_1, \ldots, f_s \rangle$,
2. derive a monomial basis for $\mathcal{C}^n/\langle f_1, \ldots, f_s \rangle$ from G,
3. solve the eigenvalue problem that expresses the multiplication of monomials within the quotient space $\mathcal{C}^n/\langle f_1, \ldots, f_s \rangle$,
4. read off the affine solutions from the eigenvectors.

It is possible to write down Stetter's eigenvalue problem without the computation of a Gröbner basis. Instead, one needs to write down the multiplication of the differential functional $\partial_j|_z$ with a monomial. Suppose that the polynomial system has only affine roots with no multiplicities. No homogeneous interpretation of the canonical null space K is required then. For a functional $\partial_0|_z$ the following relationship holds:

$$\begin{pmatrix} 1 \\ x_1 \\ x_2 \\ \vdots \\ x_n^{d-1} \end{pmatrix} x_1 \;=\; \begin{pmatrix} x_1 \\ x_1^2 \\ x_1 x_2 \\ \vdots \\ x_1 x_n^{d-1} \end{pmatrix}. \tag{19}$$

Or in other words, the operation of multiplying $\partial_0|_z$ with x_1 corresponds with a particular row selection of the same functional. In this case, the first row becomes the second, the second is mapped to row $n+2$, and so forth. If we want to express the multiplication of functionals in $\mathcal{C}_d^{n'}$ with monomials of degree 1, then only the rows corresponding with monomials up to degree $d-1$ are allowed to be multiplied. Indeed, monomials of degree d would be 'shifted' out of the coefficient vector. Hence (19) can be rewritten as

$$S_{10}\;\partial_0|_z\; x_1 \;=\; S_{01}\;\partial_0|_z, \tag{20}$$

where S_{10} selects at most all $\binom{d-1+n}{n}$ rows corresponding with monomials from degree 0 up to $d-1$ and S_{01} selects the corresponding rows after multiplication with x_1.

Example 4.5. *Writing down* (20) *for functionals in* $\mathcal{C}_2^{2'}$ *results in*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ x_1 \\ x_2 \\ x_1^2 \\ x_1x_2 \\ x_2^2 \end{pmatrix} x_1 \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ x_1 \\ x_2 \\ x_1^2 \\ x_1x_2 \\ x_2^2 \end{pmatrix}.$$

The selection matrix S_{10} *selects in this case all rows corresponding with all monomials of degree 0 up to 1.*

If S_{10} in Example 4.5 would have selected any of the rows corresponding with monomials of degree 2, then no corresponding S_{01} could have been constructed since the functionals do not contain any monomials of degree 3. Observe that relations similar to (20) can be written down for multiplication with any variable x_i. Indeed, for every variable x_i a corresponding row selection matrix can be derived. Under the assumption that none of the m affine roots has multiplicities, (19) can be extended to all functionals of affine roots $K = (\partial_0|_{z_1} \quad \ldots \quad \partial_0|_{z_m})$ and any multiplication variable x_i so that we can write

$$S_{i0}\; K\; D_i = \; S_{0i}\; K, \tag{21}$$

where D_i is a square diagonal matrix containing x_i's. The meaning of the 0 index in the row selection matrices will become clear when we discuss the homogeneous case. Now, it will be shown how (21) can be written as a standard or generalized eigenvalue problem. The $q(d) \times m$ matrix K cannot be directly computed from $M(d)$. It is possible however, to compute a numerical basis N for the null space of $M(d)$, using for example the SVD. Since both N and K are bases for the null space, they are related by a nonsingular matrix V, or in other words, $K = N\,V$. We can therefore replace K by $N\,V$ in (21) and obtain

$$
\begin{aligned}
S_{i0}\,N\;V\;D_i &= S_{0i}\;N\;V, \\
B\;V\;D_i &= A\;V,
\end{aligned}
\tag{22}
$$

where we have set $B = S_{i0}\,N$ and $A = S_{0i}\,N$. Since A and B are overdetermined matrices, (22) is not an eigenvalue problem yet. One way to transform it into a generalized eigenvalue problem would be to choose S_{i0} and S_{0i} such that A and B become square. In addition, B has to be regular since we know that the diagonal of D_i contains the x_i components of the affine roots. The second way is to transform (22) into an ordinary eigenvalue problem by writing it as

$$V\;D_i \;=\; B^{\dagger} A\;V,$$

where $B^{\dagger}$ is the Moore-Penrose pseudoinverse of B. Once the eigenvectors V are computed, the canonical null space K can be reconstructed as $N\,V$. The affine roots are then simply read off from K. The procedure to numerically compute the affine roots of $f_1, \ldots, f_s$ without a Gröbner basis is hence:

1. compute a numerical basis for the null space of $M(d)$ for $d \geq d^{\star}$,
2. choose S_{ij}, S_{ji} and form B, A,
3. solve the eigenvalue problem $B\;V\;D_i = A\;V$,
4. reconstruct K and read off the affine solutions.

More details on numerical affine root-finding using these two approaches, even when there are roots at infinity, can be found in [16].

In order to extend the monomial multiplication property (19) to the homogeneous case, one adjustment needs to be made: a monomial multiplication needs to be inserted on the right-hand side. Indeed, since each component of the differential functional $\partial_j|_z$ has the same total degree, $\partial_j|_z\; x_i$ will not correspond with a particular row selection of $\partial_j|_z$. The following example illustrates the extension of (19) to the homogeneous case.

Example 4.6. *The homogeneous extension of the monomial multiplication* *property in Example 4.5 is*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0^2 \\ x_0x_1 \\ x_0x_2 \\ x_1^2 \\ x_1x_2 \\ x_2^2 \end{pmatrix} x_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_0^2 \\ x_0x_1 \\ x_0x_2 \\ x_1^2 \\ x_1x_2 \\ x_2^2 \end{pmatrix} x_0.$$

The selection matrix on the left-hand side is again denoted S_{10}. Here the leftmost index means that in this side of the equation we multiply with x_1 and with x_0 on the other side. Likewise for the row selection matrix S_{01} on the right-hand side, here we multiply with x_0 and with x_1 on the other side. Observe that these selection matrices are identical to those of Example 4.5.

Consequently, the homogeneous monomial multiplication property can be be written as

$$S_{ij}\ K\ D_i \ = \ S_{ji}\ K\ D_j. \tag{23}$$

Choosing the two monomials x_i, x_j with which both sides of the equation will be multiplied respectively completely determines the selection matrices S_{ij}, S_{ji}. Since (23) is valid for the homogeneous case, this relation also holds for roots at infinity.

Stetter's Central Theorem of multivariate polynomial root finding says that the D_i matrices in the eigenvalue problems derived from (22) will in general not be a Jordan normal form when the affine roots have multiplicities[11, p. 52]. They are however still upper triangular. The same is true for the homogeneous case. We will now derive our algorithm to compute these upper triangular multiplication matrices D_i in the homogeneous case by means of an example.

Example 4.7. *Suppose we have the following polynomial system in $\mathcal{C}_4^2$*

$$\begin{cases} (x_1 - 2)\, x_2^2 &= 0, \\ (x_2 - 3)^2 &= 0. \end{cases}$$

It can be easily shown that there is an affine root $z_1 = (1, 2, 3)$ with multiplicity 2 and a root at infinity $z_2 = (0, 1, 0)$ with multiplicity 4. The degree of regularity is 4 and the canonical null space K is

$$(K_1 \quad K_2) = (\partial_{000}|_{z_1} \quad \partial_{100}|_{z_1} + 2\partial_{010}|_{z_1} \quad \partial_{000}|_{z_2} \quad \partial_{100}|_{z_2} \quad \partial_{010}|_{z_2} \quad 2\partial_{200}|_{z_2} + 3\partial_{101}|_1 01).$$

We start with the affine root z_1 and determine its entries of the multiplication matrices D_0, D_1. The first step is to write down the homogeneous multiplication property for $\partial_{000}|_{z_1}$

$$S_{01}\ \partial_{000}|_{z_1}\ x_0 \ = \ S_{10}\ \partial_{000}|_{z_1}\ x_1. \tag{24}$$

Both $\partial_{100}|_{z_1}$ and $\partial_{010}|_{z_1}$ are needed to describe the second column of the canonical null space. By taking the partial derivative of (24) *with respect to x_0 we obtain*

$$S_{01}\ (\partial_{000}|_{z_1} + \partial_{100}|_{z_1}\ x_0) \ = \ S_{10}\ \partial_{100}|_{z_1}\ x_1. \tag{25}$$

Likewise, taking the partial derivative of (24) *with respect to x_1 and multiplying both sides with 2 results in*

$$S_{01}\ 2\partial_{010}|_{z_1}\ x_0 \ = \ S_{10}\ (2\partial_{000}|_{z_1} + 2\partial_{010}|_{z_1}\ x_1). \tag{26}$$

Combining (24), (25) *and* (26) *and evaluating x_0, x_1 results in*

$$S_{01}\left(\partial_{000}|_{z_1} \quad \partial_{100}|_{z_1} + 2\partial_{010}|_{z_1}\right)\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \ = \ S_{10}\left(\partial_{000}|_{z_1} \quad \partial_{100}|_{z_1} + 2\partial_{010}|_{z_1}\right)\begin{pmatrix}2 & 2\\ 0 & 2\end{pmatrix}. \tag{27}$$

Observer how there is a 2 on the superdiagonal on the right-hand side. This already indicates that the multiplication matrix will not be in Jordan normal form. The procedure to determine the part of the multiplication matrices for the root at infinity is completely analogous to the analysis above. Starting off with writing down the multiplication property for $\partial_{000}|_{z_2}$

$$S_{01}\ \partial_{000}|_{z_2} x_0 \ = \ S_{10}\ \partial_{000}|_{z_2} x_1,$$

and taking partial derivatives with respect to x_0,

$$S_{01}\ (\partial_{000}|_{z_2} + \partial_{100}|_{z_2}\ x_0) \ = \ S_{10}\ \partial_{100}|_{z_2}\ x_1, \tag{28}$$

and with respect to x_1

$$S_{01}\ \partial_{010}|_{z_2}\ x_0 \ = \ S_{10}\ (\partial_{000}|_{z_2} + \partial_{010}|_{z_2}\ x_1).$$

Differential functionals of second degree are also needed. Taking the partial derivative of $\partial_{100}|_{z_2}$ with respect to x_0 to compute $\partial_{200}|_{z_2}$ results in

$$\frac{\partial}{\partial x_0}(\partial_{100}|_{z_2}) = 2\,\partial_{200}|_{z_2}$$

due to Definition 4.2. An additional partial derivative of (28) *with respect to x_0 results in the desired equation*

$$
\begin{aligned}
S_{01}\,(\partial_{100}|_{z_2} + \partial_{100}|_{z_2} + 2\partial_{200}|_{z_2}\,x_0) &= S_{10}\,2\partial_{200}|_{z_2}\,x_1, \\
S_{01}\,(2\,\partial_{100}|_{z_2} + 2\,\partial_{200}|_{z_2}\,x_0) &= S_{10}\,2\partial_{200}|_{z_2}\,x_1,
\end{aligned}
$$

and likewise for the $\partial_{101}|_{z_2}$ functional

$$S_{01}\,(3\partial_{001}|_{z_2} + 3\partial_{101}|_{z_2}\,x_0) = S_{10}\,3\partial_{101}|_{z_2}\,x_1,$$

Combining the results and evaluating the components, we can write

$$
\begin{aligned}
&S_{01}\left(\partial_{000}|_{z_2} \quad \partial_{100}|_{z_2} \quad \partial_{010}|_{z_2}\right)\begin{pmatrix}0&1&0&0\\0&0&0&2\\0&0&0&3\\0&0&0&0\end{pmatrix} \\
&= S_{10}\left(\partial_{000}|_{z_2} \quad \partial_{100}|_{z_2} \quad \partial_{010}|_{z_2}\right)\begin{pmatrix}1&0&1&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.
\end{aligned}
\tag{29}
$$

Finally, combining (27) *and* (29) *results in the homogeneous multiplication property for the whole canonical null space K*

$$S_{01}\,K\begin{pmatrix}1&1&0&0&0&0\\0&1&0&0&0&0\\0&0&0&1&0&0\\0&0&0&0&0&2\\0&0&0&0&0&3\\0&0&0&0&0&0\end{pmatrix} = S_{10}\,K\begin{pmatrix}2&2&0&0&0&0\\0&2&0&0&0&0\\0&0&1&0&1&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{pmatrix}.$$

By abuse of notation, we will also denote the upper triangular multiplication matrices by D_i, D_j. Doing so, (23) also holds for the case of roots with multiplicities. Algorithm 4.1 summarizes the whole procedure to derive the multiplication matrices for the projective case.

Algorithm 4.1. *:*
Input: *canonical null space K, multiplication monomials x_i, x_j*
Output: *projective multiplication matrices D_i, D_j*

determine row selection matrices from x_i, x_j
for *each projective root z_i* ***do***
write homogeneous multiplication property for z_i
apply partial derivatives to obtain higher order functionals
make linear combinations to reconstruct the multiplicity structure
write out the obtained multiplication relation in matrix form
end for
combine multiplication matrices for each root into D_i, D_j

Since the multiplication of monomials is commutative, this implies that the multiplication matrices D_i, D_j will also commute. The occurrence of multiple roots, whether they are affine or at infinity, poses a problem to determine them via an eigenvalue computation. Indeed, in order to be able to write

$$S_{ij}\; K\; D_i \;=\; S_{ji}\; K\; D_j$$

as an eigenvalue problem, either D_i or D_j has to be invertible. For affine roots this will always be the case for D_0. Roots at infinity will need a more careful choice of x_i, x_j. Let us suppose that D_j is invertible, we can then write

$$S_{ij}\; K\; D_i\, D_j^{-1} \;=\; S_{ji}\; K.$$

Again, substituting K by $N\,V$ and setting $S_{ij}N = B, S_{ji}N = A$ we get

$$B\,V\,D_i\,D_j^{-1} \;=\; AV. \tag{30}$$

Let

$$J_{ij} \;=\; T^{-1}\,D_i\,D_j^{-1}\,T$$

be the Jordan normal form of $D_i\,D_j^{-1}$. This allows us to rewrite (30) as

$$B\,V\,T\,J_{ij} \;=\; A\,V\,T. \tag{31}$$

This can again be converted into a generalized eigenvalue problem by making A, B square and B regular or into an ordinary eigenvalue problem by computing the pseudoinverse of B. The retrieved eigenvectors are in this case $V\,T$, from which we cannot reconstruct the canonical null space $K = N\,V$

since T is unknown. An additional difficulty lies in the numerically stable computation of the Jordan normal form J. Alternatively, one can compute the numerically stable Schur decomposition

$$B^{\dagger} A \;=\; Q\, U\, Q^{-1},$$

where Q is unitary and U upper triangular. The eigenvalues x_i/x_j can then be read off from the diagonal of U. In the projective case there is always at least one D_j invertible. This means that the n different x_i/x_j components of the projective roots can be computed from n Schur factorizations. Afterwards these components need to be matched to form the projective roots

$$(\frac{x_0}{x_j}, \frac{x_1}{x_j}, \ldots, 1, \ldots, \frac{x_n}{x_j}),$$

where the 1 appears in the j^{th} position.

5. Conclusions

In this article we provided a detailed analysis of the left and right null spaces of the Macaulay matrix. The left null space was shown to be linked with the occurrence of syzygies in the row space. It was also demonstrated how the dimension of the left null space is described by a piecewise function of polynomials. Two algorithms were presented that determine these polynomial expressions for $l(d)$. The finiteness of the number of basis syzygies resulted in the notion of the degree of regularity, which played a crucial role in describing a basis for the right null space of $M(d)$ in terms of differential functionals. The canonical null space K of $M(d)$ was defined and the multiplication property of this canonical basis was extended to the projective case. This resulted in upper triangular commuting multiplication matrices. Finally, we discussed how Stetter's eigenvalue problem can be extended to the case where both affine roots and roots at infinity are present.

References

[1] J. Grabmeier, E. Kaltofen, V. Weispfenning, Computer Algebra Handbook: Foundations, Applications, Systems, With Cd-Rom, Demo Versions, Springer-Verlag GmbH, 2003.

[2] J. A. Dieudonné, History of Algebraic Geometry, The Wadsworth mathematics series, Chapman & Hall, 1985.

[3] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. thesis, Mathematical Institute, University of Innsbruck, Austria (1965).

[4] D. A. Cox, J. B. Little, D. O'Shea, Ideals, Varieties and Algorithms, 3rd Edition, Springer-Verlag, 2007.

[5] D. A. Cox, J. B. Little, D. O'Shea, Using Algebraic Geometry, Graduate Texts in Mathematics, Springer-Verlag, 2005.

[6] A. Morgan, Solving polynomial systems using continuation for engineering and scientific problems, Prentice-Hall, Englewood Cliffs, N.J., 1987.

[7] A. J. Sommese, C. W. Wampler, Numerical Algebraic Geometry. In The Mathematics of Numerical Analysis., in: M. S. J.Renegar, S. Smale (Eds.), Lectures in Applied Mathematics. Proceedings of the AMS-SIAM Summer Seminar in Applied Mathematics, AMS, 1996, pp. 749–763.

[8] A. J. Sommese, J. Verschelde, C. W. Wampler, Numerical decomposition of the solution sets of polynomial systems into irreducible components, SIAM Journal on Numerical Analysis 38 (6) (2001) 2022–2046. doi:10.1137/S0036142900372549.

[9] J. Verschelde, Algorithm 795: PHCpack: a general-purpose solver for polynomial systems by homotopy continuation, ACM Trans. Math. Softw. 25 (2) (1999) 251–276.

[10] W. Auzinger, H. J. Stetter, An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations, in: Int. Conf. on Numerical Mathematics, Singapore 1988, Birkhäuser ISNM 86, 1988, pp. 11–30.

[11] H. J. Stetter, Numerical Polynomial Algebra, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2004.

[12] K. Batselier, P. Dreesen, B. De Moor, The Geometry of Multivariate Polynomial Division and Elimination, SIAM Journal on Matrix Analysis and Applications 34 (1) (2013) 102–125.

[13] K. Batselier, P. Dreesen, B. De Moor, A geometrical approach to finding multivariate approximate LCMs and GCDs, Linear Algebra and its Applications 438 (9) (2013) 3618–3628.

[14] K. Batselier, P. Dreesen, B. De Moor, Numerical Polynomial Algebra: The Canonical Decomposition and Numerical Gröbner Bases, submitted (2013).

[15] K. Batselier, A Numerical Linear Algebra Framework for Solving Problems with Multivariate Polynomials, Ph.D. thesis, Faculty of Engineering, KU Leuven (Leuven, Belgium) (2013).

[16] P. Dreesen, Back to the Roots: Polynomial System Solving Using Linear Algebra, Ph.D. thesis, Faculty of Engineering, KU Leuven (Leuven, Belgium) (2013).

[17] M. R2012a, The Mathworks Inc., natick, Massachusetts (2012).

[18] J. W. Eaton, D. Bateman, S. Hauberg, GNU Octave Manual Version 3, Network Theory Ltd., 2008.

[19] J. J. Sylvester, On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function and that of the greatest algebraical common measure, Trans. Roy. Soc. Lond.

[20] F. S. Macaulay, On some formulae in elimination, Proc. London Math. Soc. 35 (1902) 3–27.

[21] F. S. Macaulay, The algebraic theory of modular systems, Cambridge University Press, 1916.

[22] J. J. Sylvester, On the Intersections, Contacts, and Other Correlations of Two Conics Expressed by Indeterminate Coordinates, Cambridge and Dublin Mathematical Journal (1850) 262–282.

[23] K. Batselier, P. Dreesen, B. De Moor, A fast iterative orthogonalization scheme for the Macaulay matrix, Submitted (2013).

[24] H. J. Stetter, Matrix eigenproblems are at the heart of polynomial system solving, SIGSAM Bulletin 30 (4) (1996) 22–5.

[25] B. H. Dayton, Z. Zeng, Computing the multiplicity structure in solving polynomial systems, in: Proc. of ISSAC '05, ACM Press, 2005, pp. 116–123.

[26] Z. Zeng, The closedness subspace method for computing the multiplicity structure of a polynomial system, in: Interactions of Classical and Numerical Algebraic, 2009.