NUMERICAL ALGEBRAIC GEOMETRY: THE CANONICAL DECOMPOSITION AND NUMERICAL GRÖBNER BASES *

KIM BATSELIER†, PHILIPPE DREESEN†, AND BART DE MOOR †

Abstract. This article introduces the canonical decomposition of the vector space of multivariate polynomials for a given monomial ordering. Its importance lies in solving multivariate polynomial systems and computing Gröbner bases. An SVD-based algorithm is presented which numerically computes the canonical decomposition. It is then shown how by introducing the notion of divisibility into this algorithm a numerical Gröbner basis can also be computed. In addition, a criterion for the zero-dimensionality of the solution set of a multivariate polynomial system is derived and the ideal membership problem is solved. Numerical experiments are presented and discussed.

Key words. singular value decomposition, principal angles, Macaulay matrix, multivariate polynomials, numerical Gröbner basis, inexact polynomials

AMS subject classifications. 15A03,15B05,15A18,15A23

1. Introduction. Multivariate polynomials appear in a myriad of applications [6, 8, 11, 30]. Often in these applications, the problem that needs to be solved is equivalent with finding the roots of a system of multivariate polynomials. With the advent of the Gröbner basis and Buchberger's Algorithm [7], symbolic methods became the standard tool for solving polynomial systems. These are studied in a branch of mathematics called computational algebraic geometry [10, 11]. It however lacks a strong focus towards numerical methods and symbolic methods have inherent difficulties to deal with noisy data. Hence there is a need for numerically stable methods. The domain of numerical linear algebra does have this focus and is already applied to some problems involving univariate polynomials. For example, computing approximate GCD's of two polynomials has been extensively studied with different approaches [2, 9, 14, 41]. An interesting observation is that the matrices involved are in most cases structured and some research therefore focuses on how methods can exploit this structure [1, 4, 27, 31]. Contrary to the univariate case, the use of numerical linear algebra methods for problems involving multivariate polynomials is not so widespread [5, 19, 39, 40]. It is the goal of this article to introduce concepts from algebraic geometry in the setting of numerical linear algebra. Central in this setting is the canonical decomposition of the vector space of multivariate polynomials. Through this concept, the interrelations between the ideal membership problem, finding a Gröbner basis, checking the zero-dimensionality of the solution set of a polynomial system and separating the affine roots from the roots at infinity are demonstrated. In addition, an

*Kim Batselier is a research assistant at the Katholieke Universiteit 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 Katholieke Universiteit 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/(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; The scientific responsibility is assumed by its authors.

†Department of Electrical Engineering ESAT-SCD, KU Leuven / IBBT Future Health Department, 3001 Leuven, Belgium

algorithm which primarily uses the singular value decomposition (SVD) is presented and illustrated with numerical examples. All algorithms were implemented in Octave [13] and are freely available on request. All numerical experiments were performed on a 2.66 GHz quad-core desktop computer with 8 GB RAM using Octave and took around 3 seconds or less to complete.

The outline of this article is as follows. First, some necessary notation is introduced in Section 2. In Section 3, the Macaulay matrix is defined. An interpretation of its row space is given which naturally leads to the ideal membership problem. The rank of the Macaulay matrix results in the canonical decomposition described in Section 4. An algorithm is described to compute this decomposition and numerical experiments are given. Both cases of exact and inexact coefficients are investigated. The notion of divisibility is introduced into the canonical decomposition in Section 5. This leads to some important applications: a condition is derived for the zero-dimensionality of the solution set of a monomial system and the total number of affine roots can be computed. Another important application is the computation of a numerical Gröbner basis, described in Section 6. This problem has already received some attention for the cases of both exact and inexact coefficients [28, 29, 32, 33, 34]. To our knowledge, no SVD-based method to compute a Gröbner basis has been proposed yet. The results for monomial systems are then extended to general polynomial systems. In Section 7 the ideal membership problem is solved by applying the insights of the previous sections. Finally, some conclusions are given together with suggestions for future research.

2. Vector Space of Multivariate Polynomials. The vector space of all multivariate polynomials over n variables up to degree d over $\mathbb{C}$ will be denoted by $\mathcal{C}_d^n$. Consequently the polynomial ring is denoted by $\mathcal{C}^n$. A canonical basis for this vector space consists of all monomials from degree 0 up to 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 $\dim(\mathcal{C}_d^n) = q(d)$. A monomial $x^a = x_1^{a_1} \ldots x_n^{a_n}$ has a multidegree $(a_1, \ldots, a_n) \in \mathbb{N}_0^n$ and (total) degree $|a| = \sum_{i=1}^n a_i$. The degree of a polynomial p, $\deg(p)$, then corresponds with the highest degree of all monomials of p. It is possible to order the terms of multivariate polynomials in different ways and results will 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 [10, 11]. In the next paragraph the monomial ordering which will be used throughout the whole of this article is defined.

2.1. Monomial Orderings. Note that we can reconstruct the monomial x^a from its multidegree $a = (a_1, \ldots, a_n)$. 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 nonzero 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. Once a monomial ordering $>$ is chosen we can uniquely identify the monomial with largest degree of a polynomial f according to $>$. This monomial is called the leading monomial of f and is denoted by $\mathrm{LM}(f)$. A monomial ordering also allows for a multivariate polynomial f to be represented by its coefficient vector. One simply orders the coefficients in a row vector, degree negative lex 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*

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

where the degree negative lex ordering of the monomials 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 the matrix or vector $(.)$.

3. Macaulay Matrix. In this section the main object of this article, the Macaulay matrix, is introduced. Its row space is linked with the concept of an ideal in algebraic geometry and this leads to the ideal membership problem.

DEFINITION 3.1. *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 $d \geq \max(d_1, \ldots, d_s)$ is the matrix containing the coefficients of*

$$M(d) = \begin{pmatrix} f_1 \\ x_1 f_1 \\ \vdots \\ x_n^{d-d_1} f_1 \\ f_2 \\ x_1 f_2 \\ \vdots \\ x_n^{d-d_s} f_s \end{pmatrix} \tag{3.1}$$

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

EXAMPLE 3.1. *For the following polynomial system in $\mathcal{C}_2^2$*

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

the Macaulay matrix of degree three is

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

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. The Macaulay matrix depends explicitly on the degree d for which it is defined, hence the notation $M(d)$. It was Macaulay who introduced this matrix, drawing from earlier work by Sylvester [37], in his work on elimination theory, resultants and solving multivariate polynomial systems [24, 25]. For a degree d the number of rows $p(d)$ of $M(d)$ is given by the polynomial

$$p(d) = \sum_{i=1}^{s} \binom{d - d_i + n}{n} = \frac{s}{n!}\, d^n + O(d^{n-1}) \tag{3.2}$$

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

$$q(d) = \binom{d+n}{n} = \frac{1}{n!}\, d^n + O(d^{n-1}). \tag{3.3}$$

From these two expressions it is clear that the number of rows will grow faster than the number of columns as soon as $s > 1$. We denote the rank of $M(d)$ by $r(d)$ and the dimension of its right null space by $c(d)$.

3.1. Row space of the Macaulay Matrix. A first interesting observation is the interpretation of the row space of $M(d)$. The row space $\mathcal{M}_d$ describes all n-variate polynomials

$$\mathcal{M}_d = \left\{ \sum_{i=1}^{s} h_i\, f_i \ : \ h_i \in C^n_{d-d_i}\ (i = 1, \ldots, s) \right\}. \tag{3.4}$$

This is closely related to the following concept of algebraic geometry.

Definition 3.2. *Let $f_1, \ldots, f_s \in \mathcal{C}^n_d$. Then we set*

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in \mathcal{C}^n_d \right\} \tag{3.5}$$

and call it the ideal generated by $f_1, \ldots, f_s$.

The ideal hence contains all polynomial combinations (3.4) without any constraints on the degrees of $h_1, \ldots, h_s$. In addition, an ideal is called zero-dimensional when the solution set of $f_1, \ldots, f_s$ is finite. We will denote all polynomials of the ideal $\langle f_1, \ldots, f_s \rangle$ with a degree from 0 up to d by $\langle f_1, \ldots, f_s \rangle_d$. It is now tempting

to interpret $\mathcal{M}_d$ as $\langle f_1, \ldots, f_s \rangle_d$ but this is not necessarily the case. $\mathcal{M}_d$ does not in general contain all polynomials of degree d which can be written as a polynomial combination (3.4).

EXAMPLE 3.2. *Consider the following polynomial system in* $\mathcal{C}_4^3$

$$\begin{cases} -9 - x_2^2 - x_3^2 - 3\,x_2^2x_3^2 + 8\,x_2x_3 = 0 \\ -9 - x_3^2 - x_1^2 - 3\,x_1^2x_3^2 + 8\,x_1x_3 = 0 \\ -9 - x_1^2 - x_2^2 - 3\,x_1^2x_2^2 + 8\,x_1x_2 = 0 \end{cases}$$

The polynomial $p = 867\,x_1^5 - 1560\,x_3\,x_2\,x_1 - 2312\,x_2^2\,x_1 + 1560\,x_3\,x_1^2 + 2104\,x_2\,x_1^2 - 1526\,x_1^3 + 4896\,x_2 - 2295\,x_1$ *of degree five is not an element of* $\mathcal{M}_5$. *This can easily be verified by a rank test: append the coefficient vector of* p *to* $M(5)$ *and the rank increases which means that* p *does not lie in* $\mathcal{M}_5$. *Remarkably,* $p \in \mathcal{M}_{11}$ *which implies that a polynomial combination of degree eleven is necessary in order to construct* p. *All terms of degrees six up to eleven cancel one another.*

As the example shows, the reason for not all polynomials written as (3.4) of degree d lying in $\mathcal{M}_d$ is that it is possible that a polynomial combination of a degree higher than d is required. The problem of determining whether a given multivariate polynomial p lies in the ideal $\langle f_1, \ldots, f_s \rangle$ generated by given polynomials $f_1, \ldots, f_s$ is called the ideal membership problem in algebraic geometry.

PROBLEM 3.1. *Let* $p, f_1, \ldots, f_s \in \mathcal{C}_d^n$, *then decide whether* $p \in \langle f_1, \ldots, f_s \rangle$.

Example 3.2 indicates that Problem 3.1 could be solved using numerical linear algebra: one could append the coefficient vector of p to the Macaulay matrix $M(d)$ and do a rank test. The two most common numerical methods for rank revealing are the SVD and a rank-revealing QR decomposition. The SVD is the most robust way of determining the numerical rank of a matrix and is therefore the method of choice in this article. As Example 3.2 also showed, it is not sufficient to do the rank test only for the degree of the given polynomial p. The algorithm requires a stop condition on the degree d for which $M(d)$ should be constructed. This results in the following proposition.

PROPOSITION 3.3. *There exists a degree* d_I *such that the ideal membership problem can be decided by a rank-test of* $M(d_I)$.

Upper bounds are available on this degree d_I. They are sharp and doubly exponential [22, 38] which renders them useless for practical purposes. In section 7 it will be shown how Problem 3.1 can be solved numerically without the need of constructing $M(d)$ for the large upper bound on d_I.

Remarkably, 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 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 3.4. *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 from multiplying each term of* f *with a power of* x_0 *such that its degree becomes* d.

EXAMPLE 3.3. *Let* $f = x_1^2 + 9x_3 - 5 \in \mathcal{C}_2^3$. *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 will be denoted by $\mathcal{P}_d^{n+1}$. This vector space is spanned by all monomials in $n+1$

variables of degree d and hence

$$\dim\left(\mathcal{P}_d^n\right) = \binom{d+n}{n}$$

which equals the number of columns of $M(d)$. This is no coincidence, given a set of non-homogeneous polynomials $f_1, \ldots, f_s$ we can also interpret $\mathcal{M}_d$ as the vector space

$$\mathcal{M}_d \;=\; \left\{ \sum_{i=1}^{s} h_i\, f_i^h \;:\; \deg(h_i) = d - d_i \;(i = 1, \ldots, s) \right\} \tag{3.6}$$

where the f_i^h's are $f_1, \ldots, f_s$ homogenized 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 ensures that the effect of higher order terms cancelling one another does not occur and therefore 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 $\langle f_1^h, \ldots, f_s^h \rangle$. We revisit Example 3.1 to illustrate this point.

EXAMPLE 3.4. *The homogenization of the polynomial system in Example 3.1 is*

$$\left\{ \begin{array}{lrcl} f_1^h: & x_1x_2 - 2x_2x_0 & = & 0 \\ f_2^h: & x_2 - 3x_0 & = & 0. \end{array} \right.$$

All homogeneous polynomials $\sum_{i=1}^{2} h_i\, f_i^h$ *of degree three are described by the row space of*

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

which equals $M(3)$ *from Example 3.1.*

Note that the homogeneous interpretation is in effect nothing but a relabelling of the columns and rows of $M(d)$. The fact that all homogeneous polynomials of degree d are contained in $\mathcal{M}_d$ simplifies the ideal membership problem for a homogeneous polynomial to a single rank test.

PROPOSITION 3.5. *Let* $f_1, \ldots, f_s \in \mathcal{C}_d^n$ *and* $p \in \mathcal{P}_d^{n+1}$. *Then* $p \in \langle f_1^h, \ldots, f_s^h \rangle$ *if and only if*

$$\operatorname{rank}\left(\begin{pmatrix} M(d) \\ p \end{pmatrix} \right) \;=\; \operatorname{rank}\left(M(d) \right). \tag{3.7}$$

4. The Canonical Decomposition of $\mathcal{C}_d^n$. First, the canonical decomposition is defined and illustrated with an example. Then, the SVD-based algorithm to compute the canonical decomposition numerically is presented. This is followed by a detailed discussion on numerical aspects which are illustrated by worked-out examples.

4.1. Definition. The interpretation of the row space immediately results in a similar interpretation for the rank of $M(d)$. Evidently, the rank $r(d)$ counts the number of linear independent polynomials lying in $\mathcal{M}_d$. More interestingly, the rank also counts the number of linear independent leading monomials of $\mathcal{M}_d$. This can be easily seen from bringing the Macaulay matrix $M(d)$ into a reduced row echelon form $R(d)$. In order for the linear independent monomials to be leading monomials a column permutation Q is required which flips all columns from left to right. The reduced row echelon form then ensures that each pivot element corresponds with a linear independent leading monomial. The $r(d)$ polynomials which can be read off from $R(d)$ span $\mathcal{M}_d$ and will have an important interpretation. Interpreting the rank $r(d)$ in terms of linear independent leading monomials naturally leads to a canonical decomposition of $\mathcal{C}_d^n$. The vector space spanned by the $r(d)$ leading monomials of $R(d)$ will be denoted $\mathcal{A}_d$. Its complement spanned by the remaining monomials will be denoted $\mathcal{B}_d$. These mononials that span $\mathcal{B}_d$ will be called the normal set or standard monomials. This leads to the following definition.

DEFINITION 4.1. *Let $f_1, \ldots, f_s$ be a multivariate polynomial system with a given monomial ordering. Then the decomposition of the monomial basis of $\mathcal{C}_d^n$ into a set of linear independent leading monomials $A(d)$ and standard monomials $B(d)$ is called its canonical decomposition.*

Naturally,

$$\mathcal{C}_d^n \;=\; \mathcal{A}_d \oplus \mathcal{B}_d$$

and $\dim \mathcal{A}_d = r(d), \dim \mathcal{B}_d = c(d)$. Again, note that the monomial bases for $\mathcal{A}_d$ and $\mathcal{B}_d$ can also be interpreted for the homogeneous case.

EXAMPLE 4.1. *We revisit the following polynomial system*

$$\left\{ \begin{array}{lrcl} f_1: & x_1\,x_2 - 2x_2 & = & 0 \\ f_2: & x_2 - 3 & = & 0 \end{array} \right.$$

and fix the degree to three. First, the left-to-right column permutation Q is applied to $M(3)$,

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

Now bringing $M(3)\,Q$ into reduced row echelon form results in

$$R(3) = \begin{array}{c} \begin{matrix} x_2^3 & x_1x_2^2 & x_1^2x_2 & x_1^3 & x_2^2 & x_1x_2 & x_1^2 & x_2 & x_1 & 1 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -27 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -18 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -12 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -9 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

from which the monomial basis of $\mathcal{A}_3$ can be read off: $\{x_1, x_2, x_1^2, x_1x_2, x_2^2, x_1^2x_2, x_1x_2^2, x_2^3\}$. In matrix form this monomial basis is

$$A(3) = \begin{array}{c} \begin{matrix} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{matrix} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Its complement $\mathcal{B}_3$ is spanned in this case by

$$B(3) = \begin{array}{c} \begin{matrix} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

with the corresponding normal set $\{1, x_1^3\}$.

For the sake of readability the notation for $A(d)$ and $B(d)$ is used for both the set of monomials and the matrices as in Example 4.1. The dependence of the canonical decomposition on the monomial ordering is easily understood from Example 4.1. A different admissible monomial ordering would correspond with a different column permutation Q prior to bringing $M(3)$ into the reduced row echelon form and this would result in different monomials bases $A(3)$ and $B(3)$.

The importance of this canonical decomposition is twofold. As will be shown in Section 6, the linear independent monomials $A(d)$ play an important role in the computation of a Gröbner basis of $f_1, \ldots, f_s$. The normal set $B(d)$ is intimately linked with the problem of finding the roots of the polynomial system $f_1, \ldots, f_s$. Indeed, it is well-known that for a polynomial system $f_1, \ldots, f_s$ with a finite amount of projective roots, the quotient ring $\mathcal{C}^n/\langle f_1^h, \ldots, f_s^h \rangle$ is a finite-dimensional vector space [10, 11]. The dimension of this vector space equals the total amount of projective roots of $f_1^h, \ldots, f_s^h$, counting multiplicities. From the rank-nullity theorem it then follows

that

$$\begin{aligned} c(d) &= q(d) - \text{rank}\,(\,M(d)\,) \\ &= \dim\,\mathcal{C}_d^n - \dim\,\langle f_1^h, \ldots, f_s^h\rangle_d \\ &= \dim\,\mathcal{C}_d^n / \langle f_1^h, \ldots, f_s^h\rangle_d \\ &= \dim\,\mathcal{B}_d. \end{aligned}$$

This function $c(d)$ which counts the number of homogeneous standard monomials of degree d is called the Hilbert function. This leads to the following proposition.

PROPOSITION 4.2. *For a zero-dimensional ideal $\langle f_1^h, \ldots, f_s^h\rangle$ with m projective roots (counting multiplicities) there exists a degree d_c such that $\forall\, d \geq d_c$*

$$c(d) \;=\; m.$$

Furthermore, $m = d_1 \cdots d_s$ according to Bézout's Theorem [10, p.97] when $s = n$. This effectively links the degrees of the polynomials $f_1, \ldots, f_s$ with the nullity of the Macaulay matrix. The roots can be retrieved from a generalized eigenvalue problem as discussed in [35, 36]. In practice, one is only interested in the affine roots. How these can be separated from the roots at infinity without computing a Gröbner basis is discussed in [12]. Another interesting result is that if the nullity $c(d)$ never converges to a fixed number m then it will grow polynomially. The degree of this polynomial $c(d)$ then equals the dimension of the projective solution set [11, p.463].

It is commonly known that bringing a matrix into a reduced row echelon form is numerically not the most reliable way of determining the rank of a matrix. In the next section a more robust SVD-based method for computing the canonical decomposition of $\mathcal{C}_d^n$ and finding the polynomial basis $R(d)$ is presented.

4.2. Numerical Computation of the Canonical Decomposition. As mentioned in the previous section, the rank determination of $M(d)$ is the first essential step in computing the canonical decomposition of $\mathcal{C}_d^n$. Bringing the matrix into reduced row echelon form by means of a Gauss-Jordan elimination is not a robust method for determining the rank. In addition, since the monomial ordering is fixed no column pivoting is allowed which results in potential numerical instabilities. We therefore propose to use the SVD for which numerical stable algorithms exist [17]. In addition, an orthogonal basis U for $\mathcal{M}_d$ can also be retrieved from the right singular vectors. The next step is to find $A(d), B(d)$ and the $r(d)$ polynomials of $R(d)$. The key idea here is that each of these $r(d)$ polynomials is spanned by the standard monomials and one leading monomial of $A(d)$. Suppose a subset $A \subseteq A(d)$ and $B \subseteq B(d)$, both ordered in ascending order, are available. It is then possible to test whether the next monomial larger than the largest monomial of $A(d)$ is a linear independent leading monomial. We will illustrate the principle by the following example.

EXAMPLE 4.2. *Suppose that the following subsets*

$$A \;=\; \{x_1, x_2\}, \qquad B \;=\; \{1\}$$

of

$$A(3) = \{x_1, x_2, x_1^2, x_1x_2, x_2^2, x_1^2x_2, x_1x_2^2, x_2^3\},\; B(3) = \{1, x_1^3\}$$

from Example 4.1 are available. The next monomial according to the monomial ordering is x_1^2. The next possible polynomial from $R(3)$ is then spanned by $\{1, x_1^2\}$. If such

a polynomial lies in $\mathcal{M}_3$ then x_1^2 is a linear independent leading monomial and can be added to A. If not, x_1^2 should be added to B. This procedure can be repeated until all monomials up to degree three have been tested. For the case of x_1^2 there is indeed such a polynomial present in $R(3)$ as can be seen from Example 4.1: $x_1^2 - 4$. This polynomial therefore lies in both the vector spaces $\mathcal{M}_3$ and span$(1, x_1^2)$. Computing a basis for the intersection between $\mathcal{M}_3$ and span$(1, x_1^2)$ will therefore reveal whether $x_1^2 \in A(3)$.

Given the subsets A and B, testing whether a monomial $x^a \in A(d)$ corresponds with computing the intersection between $\mathcal{M}_d$ and span(B, x^a). If we denote the matrix containing the monomials (B, x^a) by E and an orthogonal basis for $\mathcal{M}_d$ by U, then one way of computing the intersection would be to solve the following overdetermined linear system

$$\begin{pmatrix} U^T & E^T \end{pmatrix} x = 0. \tag{4.1}$$

If there is a non-empty intersection then (4.1) has a non-trivial solution x. The size of the matrix $\begin{pmatrix} U^T & E^T \end{pmatrix}$ can grow rather large ($q(d) \times (r(d) + m)$, where m is the cardinality of E). Using principal angles to determine the intersection involves a smaller matrix ($q(d) \times m$) and is therefore preferred. An intersection implies a principal angle of zero between the two vector spaces. The cosine of the principal angles can be retrieved from the following theorem.

THEOREM 4.3. *Assume that the columns of U^T and E^T form orthogonal bases for two subspaces of $\mathcal{C}_d^n$. Let*

$$U\,E^T, = Y\,C\,Z^T, \quad C = \operatorname{diag}(\sigma_1, \ldots, \sigma_m), \tag{4.2}$$

be the SVD of $U\,E^T$ where $Y^TY = I_r, Z^TZ = I_m$. If we assume that $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_m$, then the cosines of the principal angles associated with this pair of subspaces are given by

$$\cos(\theta_k) = \sigma_k(U\,E^T).$$

Proof. See [3, p. 582]. □

Computing principal angles smaller than 10^{-8} in double precision is impossible using Theorem 4.3. This is easily seen from the second order approximation of the cosine of its Maclaurin series: $\cos(x) \approx 1 - x^2/2$. If $x < 10^{-8}$ then the $x^2/2$ term will be smaller than the machine precision $\epsilon \approx 2 \times 10^{-16}$ and hence $\cos(x)$ will be exactly 1. For small principal angles it is numerically better to compute the sines using the following Theorem.

THEOREM 4.4. *The singular values $\mu_1, \ldots, \mu_q$ of the matrix $E^T - U^T\,U\,E^T$ are given by $\mu_k = \sqrt{1 - \sigma_k^2}$ where the σ_k are defined in (4.2). Moreover, the principal angles satisfy the equalities $\theta_k = \arcsin(\mu_k)$. The right principal vectors can be computed as*

$$v_k = E^T\,z_k, \quad k = 1, \ldots, m,$$

where z_k are the corresponding right singular vectors of $E^T - U^T\,U\,E^T$.

Proof. Proofs can be found in both [3, p. 582-583] and [20, p. 6]. □

Testing for a non-empty intersection between the row spaces of U and E is hence equivalent with inspecting the the smallest singular value μ_m of $E^T - U^T\,U\,E^T$. The

columns of this $q(d) \times m$ matrix span the orthogonal projection of $\text{span}(B, x^a)$ onto the orthogonal complement of $\mathcal{M}_d$. If there is a non-empty intersection, then the reduced polynomial r can be retrieved as the right singular vector v_m corresponding with μ_m. The whole algorithm is summarized in pseudo-code in Algorithm 4.1. The algorithm iterates over all n-variate monomials from degree 0 up do d, in ascending order. The set containing all these monomials is denoted by $\mathcal{T}_d^n$. The computational complexity is dominated by the SVD of $M(d)$ for determining the rank and computing the orthogonal basis for $\mathcal{M}_d$. A full SVD is not required, only the diagonal matrix containing the singular vales and right singular vectors need to be computed. This takes approximately $4p(d)q(d)^2+8q(d)^3$ flops. All subsequent SVD's of $E^T - U^T\,U\,E^T$ in Algorithm 4.1 have a total computational complexity of $O(q(d)^2)$.

ALGORITHM 4.1. *Computation of the Canonical Decomposition of* $\mathcal{C}_d^n$
***Input**: orthogonal basis* U *of* $\mathcal{M}_d$*, tolerance* τ
***Output**:* $A(d), B(d)$ *and polynomials* $R(d)$

```
A(d), B(d), R(d) ← ∅
for all x^a ∈ T_d^n do
   construct E from B(d) and x^a
   construct E^T − U^T U E^T
   [W S Z] ← SVD(E^T − U^T U E^T)
   if arcsin(μ_m) < τ then
      append x^a to A(d)
      append v_m^T to R(d)
   else
      append x^a to B(d)
   end if
end for
```

4.3. Numerical Experiments - Exact Coefficients. We first consider the case of polynomials with exact coefficients. Determining the rank of $M(d)$ is the first crucial step in the algorithm. If a wrong rank is estimated from the SVD the subsequent canonical decomposition will also be wrong. The default tolerance used in the SVD-based rank determination is $\tau = k \times \text{eps}(\sigma_1)$ where $k = \max(p(d), q(d))$ and $\text{eps}(\sigma_1)$ returns the positive distance from the largest singular value of $M(d)$ to the next larger in magnitude double precision floating point number. The numerical rank $r(d)$ is chosen such that $\sigma_{r(d)} > \tau > \sigma_{r(d)+1}$. The approxi-rank gap $\sigma_{r(d)}/\sigma_{r(d)+1}$ [23, p. 920] then determines the difficulty of revealing the numerical rank. In practice, a rather well-conditioning of determining the numerical rank of the Macaulay matrix for nonzero-dimensional ideals is observed. Approxi-rank gaps are typically around 10^{10}. Small approxi-rank gaps of around unity indicate inherent 'difficult' polynomial systems. Scaling the polynomials such that their coefficient vector is a unit vector before constructing the Macaulay matrix can also improve the approxi-rank gap somewhat. The same tolerance τ can be used to test whether a principal angle is numerically zero. We illustrate the algorithm with the following numerical example.

EXAMPLE 4.3. *Consider the following polynomial system in* $\mathcal{C}_4^3$

$$\left\{\begin{array}{rcl} x_1^2 + x_1\,x_3 - 2\,x_2 + 5 & = & 0 \\ 2\,x_1^3\,x_2 + 7\,x_2\,x_3^2 - 4\,x_1\,x_2\,x_3 + 3\,x_1 - 2 & = & 0 \\ x_2^4 + 2\,x_2\,x_3 + 5\,x_1^2 - 5 & = & 0 \end{array}\right.$$

with degrees $d_1 = 2, d_2 = 4, d_3 = 4$. *The canonical decomposition is computed for* $d = 10$ *with Algorithm 4.1. Each polynomial is normalized and the* 333×286 *Macaulay matrix* $M(10)$ *is constructed. From its SVD the tolerance is set to* $\tau = 1.47 \times 10^{-13}$ *and the numerical rank is determined as 254 with an approxi-rank gap of* $\approx 4 \times 10^{13}$. *This implies that* $A(10)$ *and* $B(10)$ *will have 254 and 32 monomials respectively. Algorithm 4.1 indeed returns this number of monomials and corresponding polynomials* $R(10)$. *We will discuss in Section 6 why this canonical decomposition is correct. The principal angles corresponding with the leading monomials* $A(10)$ *are all around* 10^{-15} *and hence the tolerance* τ *for the rank-test also works for the principal angles. The smallest principal angle for a monomial of the normal set* $B(10)$ *is* 2.17×10^{-9}. *Note that the rank estimated from the reduced row echelon form of* $M(10)$ *is 259 which is a strong indication that the reduced row echelon form is not well-suited to compute* $A(10), B(10)$ *and* $R(10)$.

4.4. Numerical Experiments - Inexact Coefficients. When the polynomials have inexact coefficients two cases need to be considered. First, suppose that the measured noisy polynomials $\tilde{f}_1, \ldots, \tilde{f}_s$ are perturbations of the nonzero coefficients of $f_1, \ldots, f_s$. This means that in the Macaulay matrix no new nonzero entries are introduced. It is therefore very likely that the rank and the computed canonical decomposition for $\tilde{f}_1, \ldots, \tilde{f}_s$ will remain the same and $\tilde{R}(d)$ lies 'close' to $R(d)$.

EXAMPLE 4.4. *We revisit the polynomial system of Example 4.3 and perturb its nonzero coefficients with random noise, uniformly drawn from the interval* $[0, 0.01]$. *The SVD of* $\tilde{M}(10)$ *of the perturbed polynomial system also reveals a numerical rank of 254 with an approxi-rank gap of* 5.05×10^{13}. *The exact same canonical decomposition* $\tilde{A}(10), \tilde{B}(10)$ *as for* $f_1, \ldots, f_s$ *is returned by Algorithm 4.1. The largest absolute error in the coefficients of* $\tilde{R}(10)$, $max|R(10) - \tilde{R}(10)|$, *is* 0.2496. *The average absolute error is* 3.744×10^{-4} *which means that* $R(10)$ *is not perturbed much on average.*

The case where new nonzero coefficients are introduced by noise is quite problematic. Suppose, for example, that a new nonzero term is added to f_1 such that $\deg(\tilde{f}_1) = d_1 + 1$. Then we know from Bézout's Theorem ($n = s$) that for some degree $c(d)$ will be $(d_1 + 1) \cdots d_s$ instead of $d_1 \cdots d_s$. Hence, the rank of $M(d)$ and the canonical decomposition is expected to change dramatically.

EXAMPLE 4.5. *The term* $0.0046\, x_1\, x_2^2$ *is added to* f_1 *of Example 4.3.* $\tilde{M}(10)$ *now has a numerical rank of 236 with an approxi-rank gap of* 1.67×10^{13}. *The numerical rank is therefore well-defined. If we would like to recover the numerical rank of the original polynomial system* $f_1, \ldots, f_s$ *for* $\tilde{f}_1, \ldots, f_s$ *a numerical tolerance* τ *between* 2.027×10^{-16} *and* 1.682×10^{-16} *needs to be chosen. This is for all practical purposes impossible.*

The last case is when new nonzero coefficients are introduced but the degrees of the perturbed system equal the degrees of the unperturbed system. We can now infer, again using Bézout's Theorem, that the numerical rank of $\tilde{M}(d)$ will be the same as of $M(d)$. If we think in terms of the reduced row echelon form then it is clear that new pivots will be introduced by the noisy coefficients and hence $\tilde{A}(d)$ and $\tilde{B}(d)$ will be different from $A(d)$ and $B(d)$. There is even a possibility that Algorithm 4.1 fails to compute a correct decomposition. The reason is made clear from the following example.

EXAMPLE 4.6. *Again, we revisit the polynomial system of Example 4.3 but now perturb each polynomial with noise uniformly drawn from the interval* $[0, 0.01]$ *such that each possible monomial has a nonzero coefficient. As a consequence, the coefficient vectors become very dense. The numerical rank of* $\tilde{M}(10)$ *is, as predicted,*

again 254 with an approxi-rank gap of $\approx 5 \times 10^{13}$. *Even though the rank was estimated correctly, Algorithm 4.1 fails to compute the correct decomposition* $\tilde{A}(d), \tilde{B}(d)$. $\tilde{A}(d)$ *contains 256 monomials instead of 254. The reason lies in the fact that the original numerical tolerance* τ *used for the rank-test is not appropriate anymore to test perturbed principal angles. To make matters worse, it becomes impossible to set a tolerance such that the 'original' decomposition* $A(d), B(d)$ *is recovered. The first wrong monomial of* $\tilde{B}(10)$ *is* $x_1\, x_3$. *This monomial should normally lie in* $\tilde{A}(10)$. *The principal angle to test whether* $x_1\, x_3$ *lies in* $\tilde{A}(10)$ *is* 9.8×10^{-6}. *In order to recover the right decomposition one should choose a tolerance such that this principal angle is considered to be numerically zero. If Algorithm 4.1 is rerun with* $\tau = 1.1 \times 10^{-5}$ *then indeed* $x_1\, x_3$ *lies in* $\tilde{A}(10)$ *but now* x_1^4 *lies wrongfully in* $\tilde{A}(10)$. *The principal angle for this monomial is* $8.6 \times 10^{-6} < \tau$ *which means that no tolerance can recover the original canonical decomposition.*

The previous example shows that computing the canonical decomposition for a polynomial system with noisy coefficients is an ill-posed problem. A small perturbation leads to a non-continuous change of the solution. This will also have some implications for the numerical computation of a Gröbner basis for a noisy polynomial system. When an upper bound on the magnitude of the noise is known it is possible to derive an upper bound on the perturbation of the principal angles. But the example above already shows that it is impossible to try to recover the right canonical decomposition of a polynomial system where the perturbations introduce new nonzero monomials. However, it is possible to use this upper bound on the noise to preprocess the perturbed polynomial system such that the result of Algorithm 4.1 improves significantly. The problem of determining the canonical decomposition is well-behaved when only the nonzero coefficients of the original system are perturbed. One could therefore set all coefficients smaller in magnitude than the upper bound on the noise to zero before running Algorithm 4.1. This acts as a sort of regularization of the problem.

EXAMPLE 4.7. *All coefficients of Example 4.6 which are smaller in magnitude than* 0.01 *are set to zero. Algorithm 4.1 again recovers the correct canonical decomposition* $\tilde{A}(10), \tilde{B}(10), \tilde{R}(10)$. *The largest absolute error in the coefficients of* $\tilde{R}(10)$, $max|R(10) - \tilde{R}(10)|$, *is* 0.21901 *and the average absolute error is* 2.18×10^{-4} *which is similar to the case of Example 4.4.*

5. The Reduced Canonical Decomposition of $\mathcal{C}_d^n$. Introducing the notion of divisibility naturally leads to the concept of a reduced canonical decomposition. First, some new notation and concepts are introduced after which Algorithm 4.1 is adjusted such that it produces the reduced decomposition. A numerical example is then worked out and discussed.

5.1. The Reduced Monomials $A^\star(d), B^\star(d)$ and Reduced Polynomials $G(d)$. The polynomial basis $R(d)$ will grow unbounded with the rank $r(d)$. It is possible however to reduce this basis to a finite subset which generates the whole ideal $\langle f_1, \ldots, f_s \rangle$. It will be shown in Section 6 that for a sufficiently large degree, this reduced polynomial basis is a Gröbner basis. First the reduced leading monomials $A^\star(d)$ are defined.

DEFINITION 5.1. *Given a set of linear independent leading monomials* $A(d)$, *then the set of reduced leading monomials* $A^\star(d)$ *is defined as the smallest subset of* $A(d)$ *for which each element of* $A(d)$ *is divisible by an element of* $A^\star(d)$.

Since there is a one-to-one mapping between leading monomials in $A(d)$ and polynomials of $R(d)$, each element of $A^\star(d)$ will also correspond with a polynomial.

DEFINITION 5.2. *For a given canonical decomposition $A(d), B(d), R(d)$ the reduced polynomials $G(d)$ are defined as the polynomials of $R(d)$ corresponding with the reduced monomial system $A^\star(d)$:*

$$G(d) \;=\; \{r \in R(d) : \forall a \in A^\star(d),\; LM(r) = a\}.$$

The reduced leading monomials $A^\star(d)$ can be interpreted as a polynomial system for which the Macaulay matrix can also be constructed. We will denote this matrix by $M_{A^\star}(d)$ and it is essential for defining the reduced normal set $B^\star(d)$.

DEFINITION 5.3. *Let $A(d), B(d)$ be a canonical decomposition implied by $f_1, \ldots, f_s$ and a given monomial ordering. Then the reduced normal set $B^\star(d)$ is the normal set obtained from the canonical decomposition implied by $A^\star(d)$ and the same monomial ordering.*

Typically $B^\star(d) \subseteq B(d)$. The following example illustrates why this is the case.

EXAMPLE 5.1. *The reduced monomial system $A^\star(3)$ of the canonical decomposition in Example 4.3 is*

$$A^\star(3) \;=\; \{x_1, x_2\}.$$

Its Macaulay matrix of degree 3 is

$$M_{A^\star}(3) \;=\; \begin{array}{c} \begin{array}{cccccccccc} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

which is almost the same as $A(3)$ except for the monomial x_1^3. Note that this means that the reduced normal set is

$$B^\star(3) \;=\; \{1\}.$$

The property that the reduced normal set $B^\star(d) \subseteq B(d)$ holds in general. When constructing the Macaulay matrix of $A^\star(d)$ it is possible that columns corresponding with standard monomials $B(d)$ are filled. Hence these monomials will not be in $B^\star(d)$ anymore. Using the following lemma it is easy to determine the standard monomials from $M_{A^\star}(d)$.

LEMMA 5.4. *Each standard monomial of $B^\star(d)$ derived from the Macaulay matrix $M_{A^\star}(d)$ always corresponds with a zero column of $M_{A^\star}(d)$.*

Proof. This follows trivially from the structure of the Macaulay matrix. ∎

Now a useful property on the zero-dimensionality of monomial ideals will be derived. First, the concept of a pure component is introduced.

DEFINITION 5.5. *We call a monomial* x_k^d $(1 \leq k \leq n)$ *a pure component and denote the set of these* n *monomials by* X_n^d.

For example, $X_3^5 = \{x_1^5, x_2^5, x_3^5\}$. It is clear from the definition of the reduced leading monomials that if pure components are present in $A(d)$ that they will also be present in $A^\star(d)$. The following lemma determines the growth of $B^\star(d)$.

LEMMA 5.6. *All monomials in* n *variables of degree*

$$d \geq d_{max} = n\,(d_0 - 1) + 1$$

can be written as a product of an element of $X_n^{d_0}$ *with another monomial.*

Proof. The proof can be completely done in $\mathbb{N}_0^n$ since there is a bijection between the exponents of monomials and $\mathbb{N}_0^n$. We first show that for any degree $d < d_{\max}$, monomials can be found which cannot be written as a product of a pure component and another monomial. For degree $d_{\max} - 1 = n\,(d_0 - 1)$ we can write the following monomial

$$(d_0 - 1, d_0 - 1, \ldots, d_0 - 1) \tag{5.1}$$

which clearly cannot be written as a product of a pure component and another monomial. It's possible to come up with similar examples for all degrees between d_0 and $d_{\max} - 1$ by just subtracting the necessary amount of a component of (5.1). For degree $d_{\max} = n\,(d_0 - 1) + 1$ we can write the following monomial

$$(d_0, d_0 - 1, \ldots, d_0 - 1) \tag{5.2}$$

which is clearly the product of $x_1^{d_0}$ and $x_2^{d_0-1} \ldots\ x_n^{d_0-1}$. Any other monomial of degree $d_{\max}$ can now be formed by rearranging (5.2) (subtracting from one component and adding to another). If, however, one component is subtracted with a certain amount then the other components should be increased such that the sum of all components remains constant. From this it is easy to see that there will always be at least 1 component $\geq d_0$. □

Furthermore, the presence of a pure component for each variable is a necessary condition for the finiteness of $B^\star(d)$. This is easily seen by an example. If there is no pure component for the variable x_1, then all subsequent powers of x_1 will be zero columns in $M_{A^\star}(d)$ and $B^\star(d)$ will grow linearly.

A monomial system $A^\star(d)$ has a projective solution set because it is already homogeneous. It is shown in [11, p.452] that the dimension of this projective solution set is always one less than its affine solution set. Hence, if the monomial ideal has a finite number of affine roots it will have no projective roots whatsoever. We can now state the following theorem relating the zero-dimensionality of a monomial system to the presence of all pure components.

THEOREM 5.7. *A monomial system* $A^\star(d)$ *has* m *affine roots, counting multiplicities, if and only if it contains for each indeterminate* x_i $(1 \leq i \leq n)$ *a pure component. It then also holds that from a certain degree:* $\dim \mathcal{B}_d^\star = m$.

Proof. This follows from Lemma 5.4 and 5.6. □

In the same vein as $M_{A^\star}(d)$, the Macaulay matrix of the reduced polynomials $G(d)$ will be denoted $M_G(d)$.

5.2. Numerical Computation of $A^\star(d), B^\star(d)$ and $G(d)$. The definition of $A^\star(d)$ uses the complete set of linear independent leading monomials $A(d)$. A straightforward way to find $A^\star(d)$ would hence be to compute $A(d)$ using Algorithm 4.1, find $A^\star(d)$ from $A(d)$ and select the corresponding polynomials of $R(d)$ to obtain $G(d)$.

This is however not efficient since the whole canonical decomposition is computed while only subsets are required. By using the defining property of $A^\star(d)$ it is possible to adjust Algorithm 4.1 such that it directly computes $A^\star(d), B^\star(d)$ and $G(d)$. The algorithm iterates over a set of monomials $\mathcal{X}$ which is initially all monomials of degree 0 up to d. The key idea is that each monomial of $A(d)$ is a monomial multiple of a monomial of $A^\star(d)$. So as soon as a linear independent leading monomial x^a is found, all its monomial multiples do not need to be checked anymore and can be removed from $\mathcal{X}$. When the monomial x^a is not linear independent it is also removed from $\mathcal{X}$ and added to $B^\star(d)$. When $\mathcal{X}$ is empty the algorithm terminates. Removing monomial multiples of x^a from $\mathcal{X}$ reduces the number of iterations significantly and also guarantees that the computed $B^\star$ is correct. The whole procedure is summarized in pseudo-code in Algorithm 5.1. Again, the first SVD of $M(d)$ is computationally the most expensive step in the algorithm. The same arguments on the computational complexity apply as for Algorithm 4.1.

ALGORITHM 5.1. *Computation of $A^\star(d), B^\star(d)$ and $G(d)$*
***Input**: orthogonal basis U of $\mathcal{M}_d$, tolerance τ*
***Output**: $A^\star(d), B^\star(d)$ and polynomials $G(d)$*

```
A*(d), B*(d), G(d) ← ∅
X ← T_d^n
while X ≠ ∅ do
    x^a ← smallest monomial in X according to monomial ordering
    construct E from B*(d) and x^a
    construct E^T − U^T U E^T
    [W S Z] ← SVD(E^T − U^T U E^T)
    if arcsin(μ_m) < τ then
        append x^a to A*(d)
        remove x^a and all its monomial multiples from X
        append v_m^T to G(d)
    else
        append x^a to B*(d)
        remove x^a from X
    end if
end while
```

5.3. Numerical Experiments. Since Algorithm 5.1 is an adjustment of Algorithm 4.1 the same comments on numerical issues apply. We revisit the polynomial system of Example 4.3 and illustrate Algorithm 5.1 when the coefficients are exact and perturbed.

EXAMPLE 5.2. *$A(10)$ of Example 4.3 consists of 254 monomials. Running Algorithm 5.1 on the polynomial system results in the following reduced canonical decomposition:*

$$A^\star(10) = \{x_1\,x_3, x_1^3\,x_2, x_2^4, x_3\,x_2^3, x_3^3\,x_2, x_1^5, x_3^5\}$$
$$B^\star(10) = \{1, x_1, x_2, x_3, x_1^2, x_2\,x_1, x_2^2, x_2\,x_3, x_3^2, x_1^3, x_2\,x_1^2, x_2^2\,x_1, x_2^3, x_3\,x_2^2, x_2\,x_3^2, x_3^3,$$
$$x_1^4, x_2^2\,x_1^2, x_2^3\,x_1, x_3^2\,x_2^2, x_3^4, x_2^3\,x_1^2\}.$$

$A^\star(10)$ consists of 7 monomials and the normal set $B(10)$ is reduced from 32 to 22 monomials. $G(10)$ consists of the following 7 polynomials

$$\begin{cases}
0.89803 - 0.35921\,x_2 + 0.17961\,x_1^2 + 0.17961\,x_1x_3 = 0 \\
\\
-0.085592 + 0.12839\,x_1 + 0.85592\,x_2 - 0.34237\,x_2^2 + 0.17118\,x_1^2x_2 + 0.29957\,x_2x_3^2 \\
+ 0.085592\,x_1^3x_2 = 0 \\
\\
-0.6742 + 0.6742\,x_1^2 + 0.26968\,x_2x_3 + 0.13484\,x_2^4 = 0 \\
\\
-0.025205 - 0.77127\,x_1 + 0.0040328\,x_2 + 0.49401\,x_3 + 0.023188\,x_1^2 + 0.31254\,x_1x_2 \\
-0.19156\,x_2x_3 + 0.0020164\,x_3^2 - 0.15627\,x_1^3 - 0.010082\,x_1^2x_2 + 0.0075614\,x_2^3 \\
-0.017643\,x_3^3 - 0.025205\,x_1^4 + 0.0010082\,x_1x_2^3 + 0.0010082\,x_2^3x_3 = 0 \\
\\
-0.089289 - 0.13951\,x_1 - 0.71432\,x_2 - 0.022322\,x_3 + 0.39064\,x_1x_2 + 0.31251\,x_2^2 \\
-0.16742\,x_2x_3 - 0.26787\,x_1^2x_2 - 0.15626\,x_1x_2^2 + 0.066967\,x_2^2x_3 - 0.27345\,x_2x_3^2 \\
+ 0.044645\,x_1^2x_2^2 + 0.078128\,x_2x_3^3 = 0 \\
\\
0.69381 - 0.57918\,x_2 + 0.0034475\,x_3 + 0.37578\,x_1^2 + 0.12066\,x_2^2 - 0.030166\,x_3^2 \\
-0.0086188\,x_1^3 - 0.15514\,x_1^2x_2 + 0.0017238\,x_2^3 + 0.047404\,x_1^4 - 0.0025856\,x_1x_2^3 \\
+ 0.0086188\,x_1^5 = 0 \\
\\
0.19201 + 0.74673\,x_1 - 0.062728\,x_2 - 0.4885\,x_3 + 0.025128\,x_1^2 - 0.30287\,x_1x_2 \\
-0.0059821\,x_2^2 + 0.19451\,x_2x_3 + 0.062794\,x_3^2 + 0.16707\,x_1^3 + 0.0079195\,x_1^2x_2 \\
+ 0.0018612\,x_1x_2^2 - 0.0070246\,x_2^3 - 0.0022368\,x_2^2x_3 + 0.0033854\,x_2x_3^2 \\
+ 0.0081701\,x_3^3 + 0.025733\,x_1^4 - 0.00070942\,x_1^2x_2^2 - 3.8079 \times 10^{-5}\,x_1x_2^3 \\
-0.0019462\,x_3^4 - 2.0865 \times 10^{-5}\,x_1^2x_2^3 + 0.0002556\,x_3^5 = 0.
\end{cases}$$

When Algorithm 5.1 is run on the perturbed version of the polynomial system where no new nonzero coefficients are introduced, the same reduced monomial bases $\tilde{A}^\star(10), \tilde{B}^\star(10)$ are found. The largest absolute error in the coefficients between $G(10)$ and $\tilde{G}(10)$ is 0.012. The average error on the coefficients is 6.19×10^{-4}. As expected, if noisy coefficients which introduce new monomials are not removed prior to running Algorithm 5.1, the results are not correct. This preprocessing step also ensures that Algorithm 5.1 recovers the original reduced monomial bases and polynomials.

6. Gröbner basis. In this section the link is made between the reduced polynomials $G(d)$ and a Gröbner basis of the ideal $\langle f_1, \ldots, f_s \rangle$. This will lead to some insights on the separation of the roots of a polynomial system into an affine part and roots at infinity for the zero-dimensional case. A condition will be derived for this case to determine the affine part of the normal set. We first give the definition of a Gröbner basis.

DEFINITION 6.1. *Given a set of multivariate polynomials $f_1, \ldots, f_s$ and a monomial ordering, then a finite set of polynomials $G = \{g_1, \ldots, g_k\} \in \langle f_1, \ldots, f_s \rangle$ is a Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ if*

$$\forall\, p \in \langle f_1, \ldots, f_s \rangle, \exists\, g \in G \text{ such that } LM(g) \mid LM(p).$$

Note from the definition that a Gröbner basis depends on the monomial ordering. One can think of a Gröbner basis as another set of generators of the ideal $\langle f_1, \ldots, f_s \rangle$, hence the name 'basis'. It is a classic result that for each ideal $\langle f_1, \ldots, f_s \rangle$ there exists such a finite set of polynomials G [10, 11]. The finiteness of G relies on Hilbert's Basis Theorem [18]. This implies that there exists a particular degree d for which $G \in \mathcal{M}_d$ which leads to the following proposition.

PROPOSITION 6.2. *For each set of multivariate polynomials $f_1, \ldots, f_s$ there exists a particular degree d_G such that for all $d \geq d_G : \ G \in \mathcal{M}_d$.*

d_G is related to d_I and hence also has doubly exponential upper bounds [26]. In order to determine whether a set of polynomials is a Gröbner basis one needs the notion of an S-polynomial.

DEFINITION 6.3. *Let f_1, f_2 be nonzero multivariate polynomials and x^γ the least common multiple of their leading monomials. The S-polynomial of f_1, f_2 is the combination*

$$S(f_1, f_2) \ = \ \frac{x^\gamma}{LT(f_1)} \, f_1 - \frac{x^\gamma}{LT(f_2)} \, f_2$$

where $LT(f_1), LT(f_2)$ are the leading terms of f_1, f_2 with respect to a monomial ordering.

It is clear from this definition that an S-polynomial is designed to produce cancellation of the leading terms and that it has a degree of at most $\deg(x^\gamma)$. A key component of Buchberger's Algorithm is constructing S-polynomials and computing their remainder on division by a set of polynomials. It was Lazard [21] who had the insight that computing this remainder is equivalent with bringing a matrix into triangular form. This led to Faugere's F4 and F5 algorithms [15, 16] which have become the golden standard to compute an exact Gröbner basis.

The reduced polynomials $G(d)$ computed from Algorithm 5.1 ensure by definition that

$$\forall \, p \in \mathcal{M}_d \, \exists \, g \in G(d) \text{ such that } \mathrm{LM}(g) \mid \mathrm{LM}(p).$$

This suggests that $G(d)$ is a Gröbner basis when $d \geq d_G$. A criterion is needed to be able to decide whether $G(d)$ is a Gröbner basis. This is given by Buchberger's criterion which we formulate in terms of the Macaulay matrix $M(d)$ and the reduced monomial system $A^\star(d)$.

THEOREM 6.4 (Buchberger's Criterion). *Let $f_1, \ldots, f_s$ be a multivariate polynomial system with reduced monomial system $A^\star(d)$ and reduced polynomials $G(d)$ for a given degree d. Then $G(d)$ is a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$ if $M(d^\star)$ has the same reduced leading monomials $A^\star(d)$ for a degree $d^\star$ such that all S-polynomials of $G(d)$ lie in $\mathcal{M}_{d^\star}$.*

Proof. Saying that $M(d^\star)$ has the same reduced leading monomials $A^\star(d)$ is equivalent with saying that all S-polynomials have a zero remainder on division by $G(d)$. This is exactly the stop-criterion for Buchberger's Algorithm [11, p.85]. ∎

Note that Buchberger's Criterion implies that for all degrees $d \geq d_G$, the Macaulay matrix $M_G(d)$ has the same reduced canonical decomposition as $M_{A^\star}(d)$. This implies the following useful corollary.

COROLLARY 6.5. *Let $f_1, \ldots, f_s$ be a multivariate polynomial system with a finite number of affine roots. Then $\forall d \geq d_G$ its reduced monomial set $A^\star(d)$ will contain for each indeterminate $x_i \, (1 \leq i \leq n)$ a pure component. Furthermore, $B^\star(d)$ is then the affine normal set.*

Proof. This follows from Theorem 5.7 and Buchberger's Criterion that $\forall\, d \geq d_G$ both $M_G(d)$ and $M_{A^\star}(d)$ have the same reduced monomial decomposition. □

If it is known that the solution set of a polynomial ideal is zero-dimensional, then detecting pure components in $A^\star(d)$ allows to determine the degree d_G. It then becomes possible to numerically compute all affine roots without the computation of a Gröbner basis. This is described in further detail in [12].

EXAMPLE 6.1. *Again, we revisit the polynomial system in $\mathcal{C}_4^3$ from Example 4.3. We assume the polynomial system has a zero-dimensional solution set and start to compute the reduced canonical decomposition from $d = 4$. Algorithm 5.1 returns*

$$A^\star(4) = \{x_1\, x_3, x_1^3\, x_2, x_2^4\}$$

which already contains 1 pure component: x_2^4. The next pure component, x_1^5, is retrieved for $d = 7$ in

$$A^\star(7) = \{x_1\, x_3, x_1^3\, x_2, x_2^4, x_2\, x_3^3, x_1^5\}.$$

The last pure component, x_3^5, is found for $d = d_G = 10$. The Gröbner basis is therefore $G(10)$ as given in Example 5.2. Indeed, computing an exact Gröbner basis in Maple and normalizing each polynomial results in $G(10)$.

The ill-posedness of the canonical decomposition under the influence of noise directly affects the computation of a Gröbner basis. As shown by Nagasaka in [29], it is impossible to define an approximate Gröbner basis in the same sense as an approximate GCD or approximate factorization of multivariate polynomials. Our numerical experiments indicate that it is probably best to apply the preprocessing step of removing 'small' nonzero coefficients and then to treat the remaining noisy polynomial system as 'exact'. In addition, Gröbner basis polynomials typically have large integer coefficients. It is even possible that these coefficients fall out of the range of the double precision standard. In this case it would be necessary to perform the computations in higher precision.

7. Solving the Ideal Membership problem. Solving the ideal membership problem for a non-homogeneous polynomial p is a rank test of the Macaulay matrix as in (3.7) for a sufficiently large degree. We can now give a more practical upper bound for this degree.

THEOREM 7.1. *Consider the ideal membership problem as described in Problem 3.1. Let $G = \{g_1, \ldots, g_k\}$ be a Gröbner basis of $\langle f_1, \ldots, f_s\rangle$ and*

$$G_p \;=\; \{g \in G \;:\; LM(g) \mid LM(p)\} \text{ and } d_0 = \max_{g \in G_p} deg(g).$$

Then

$$d_I \;\leq\; d_G + deg(p) - d_0. \tag{7.1}$$

Proof. Since G is a Gröbner basis $\exists\; g \in G : \mathrm{LM}(g) \mid \mathrm{LM}(p)$ and G_p is therefore never empty. Determining whether $p \in \langle f_1, \ldots, f_s\rangle$ is equivalent with checking whether the remainder of p on division by G is zero. Due to Lazard we know that determining this remainder is equivalent with the reduction of the matrix

$$Q \begin{pmatrix} M(d) \\ p \end{pmatrix}$$

to triangular form for a sufficiently large d with Q the column permutation as described in Section 4. Suppose that $g \in G_p$ and $\deg(g) = d_0$. The degree d_I is then such that it guarantees that $\frac{\mathrm{LT}(p)}{\mathrm{LT(g)}}\, g \in \mathcal{M}_{d_I}$. In the first division step of the multivariate division algorithm to compute the remainder, p will be updated to

$$p \leftarrow p - \frac{\mathrm{LT}(p)}{\mathrm{LT(g)}}\, g.$$

The multivariate division algorithm guarantees that the new p will have a smaller multidegree (according to the monomial ordering) [11, p.65]. In the next division step, another $g \in G$ such that $\mathrm{LT}(g)|\mathrm{LT}(p)$ is required. Since p has a smaller multidegree, the new g is also guaranteed to lie in $\mathcal{M}_{d_I}$. Therefore, all remaining steps of the division algorithm can be performed within $\mathcal{M}_{d_I}$ and the ideal membership problem can be solved. □

This means that in practice one can iteratively compute the reduced canonical decomposition of $M(d)$ using Algorithm 5.1, do the rank test for the ideal membership problem and increase the degree as long as the rank test fails. At some point d_G can be determined and the iterations can stop as soon as $d = d_G + \deg(p) - d_0$.

EXAMPLE 7.1. *As already mentioned in Example 3.2 the given polynomial* $p = 867\,x_1^5 - 1560\,x_3\,x_2\,x_1 - 2312\,x_2^2\,x_1 + 1560\,x_3\,x_1^2 + 2104\,x_2\,x_1^2 - 1526\,x_1^3 + 4896\,x_2 - 2295\,x_1$ *lies in* $\mathcal{M}_{11}$. *At* $d = 11$ *all pure components are found in* $A^\star(11)$ *which implies that the polynomial system has a finite affine solution set and* $d_G = 11$. *The rank test also succeeds, the numerical rank for both matrices in* (3.7) *is 300.*

8. Conclusions. This article introduced the canonical decomposition of the vector space $\mathcal{C}_d^n$. An SVD-based algorithm was presented which computes both the canonical and reduced decomposition reliably. It was also shown how under the presence of noise the problem of finding the canonical decomposition is ill-posed. A preprocessing of the coefficients was proposed to deal with this ill-posedness. Furthermore, the link between the polynomials $G(d)$ and a Gröbner basis was made. This resulted in a new condition to determine the affine normal set for zero-dimensional ideals. Finally, it was shown how the ideal membership problem can be solved by means of a rank test.

The polynomial growth of the dimensions of the Macaulay matrix can quickly restrict the computation of the SVD. Further research is needed whether it is possible to devise algorithms which have the robustness of the SVD for rank revealing and exploit both the sparsity and the structure of the Macaulay matrix.

REFERENCES

[1] DARIO BINI AND VICTOR Y. PAN, *Polynomial and matrix computations (vol. 1): fundamental algorithms*, Birkhauser Verlag, Basel, Switzerland, Switzerland, 1994.

[2] DARIO A. BINI AND PAOLA BOITO, *Structured matrix-based methods for polynomial ϵ-gcd: analysis and comparisons*, in Proceedings of the 2007 international symposium on Symbolic and algebraic computation, ISSAC '07, New York, NY, USA, 2007, ACM, pp. 9–16.

[3] ÅKE BJÖRCK AND GENE H. GOLUB, *Numerical methods for computing angles between linear subspaces*, Mathematics of Computation, 27 (1973), pp. pp. 579–594.

[4] PAOLA BOITO, *Structured Matrix Based Methods for Approximate Polynomial GCD*, Edizioni della Normale, 2011.

[5] D BONDYFALAT, B MOURRAIN, AND VY PAN, *Computation of a specified root of a polynomial system of equations using eigenvectors*, Linear Algebra and its Applications, 319 (2000), pp. 193–209. Annual International Symposium on Symbolic and Algebraic Computation (ISSAC 98), Rostock, Germany.

[6] N. K. BOSE, *Applied Multidimensional Systems Theory*, Van Nostrand Reinhold, 1982.

[7] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965.
[8] B. Buchberger, *Gröbner Bases and Systems Theory*, Multidimensional Systems and Signal Processing, 12 (2001), pp. 223–251.
[9] Robert M. Corless, Patrizia M. Gianni, Barry M. Trager, and Stephen M. Watt, *The singular value decomposition for polynomial systems*, in ACM International Symposium on Symbolic and Algebraic Computation, 1995, pp. 195–207.
[10] D. A. Cox, J. B. Little, and D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, March 2005.
[11] ———, *Ideals, Varieties and Algorithms*, Springer-Verlag, third ed., 2007.
[12] B. De Moor, P. Dreesen, and K. Batselier, *Back to the roots: Solving sets of multivariate polynomials with numerical linear algebra tools*, Tech. Report 12-169, KU Leuven Department of Electrical Engineering ESAT/SCD, 2012.
[13] John W Eaton, David Bateman, and Soren Hauberg, *GNU Octave Manual Version 3*, Network Theory Ltd., 2008.
[14] Ioannis Z. Emiris, André Galligo, and Henri Lombardi, *Certified approximate univariate GCDs*, Journal of Pure and Applied Algebra, 117 118 (1997), pp. 229 – 251.
[15] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*., Journal of Pure and Applied Algebra, 139 (1999), pp. 61–88.
[16] ———, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, in Proceedings of the 2002 international symposium on Symbolic and algebraic computation, ISSAC '02, New York, NY, USA, 2002, ACM, pp. 75–83.
[17] G. H. Golub and C. F. van Van Loan, *Matrix Computations*, The Johns Hopkins University Press, 3rd ed., Oct. 1996.
[18] D. Hilbert, *Ueber die Theorie der algebraischen Formen*, Springer, 1890.
[19] G. F. Jónsson and S. A. Vavasis, *Accurate solution of polynomial equations using Macaulay resultant matrices*, Math. Comput., 74 (2004), pp. 221–262.
[20] AV Knyazev and ME Argentati, *Principal angles between subspaces in an A-based scalar product: Algorithms and perturbation estimates*, SIAM Journal on Scientific Computing, 23 (2002), pp. 2008–2040.
[21] D. Lazard, *Gröbner-bases, gaussian elimination and resolution of systems of algebraic equations*, in EUROCAL, 1983, pp. 146–156.
[22] ———, *A note on upper bounds for ideal-theoretic problems*, Journal of Symbolic Computation, 13 (1992), pp. 231 – 233.
[23] TY Li and ZG Zeng, *A rank-revealing method with updating, downdating, and applications*, SIAM Journal on Matrix Analysis and Applications, 26 (2005), pp. 918–946.
[24] F. S. Macaulay, *On some formulae in elimination*, Proc. London Math. Soc., 35 (1902), pp. 3–27.
[25] ———, *The algebraic theory of modular systems*, Cambridge University Press, 1916.
[26] E. W. Mayr and A. R. Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals*, Advances in Mathematics, 46 (1982), pp. 305 – 329.
[27] B. Mourrain and V. Y. Pan, *Multivariate polynomials, duality, and structured matrices*, Journal of Complexity, 16 (2000), pp. 110 – 180.
[28] Kosaku Nagasaka, *A Study on Grobner Basis with Inexact Input*, in Computer Algebra in Scientific Computing, Proceedings, Gerdt, VP and Mayr, EW and Vorozhtsov, EV, ed., vol. 5743 of Lecture Notes in Computer Science, Tech Univ Munchen, Dept Informat; Grad Sch Human Dev & Environm; Kobe Univ, 2009, pp. 247–258. 11th International Workshop on Computer Algebra in Scientific Computing, Kobe, JAPAN, SEP 13-17, 2009.
[29] ———, *Backward error analysis of approximate Gröbner basis*. Preprint, 2012.
[30] L. Pachter and B. Sturmfels, eds., *Algebraic Statistics for Computational Biology*, Cambridge University Press, August 2005.
[31] Victor Y. Pan, *Structured matrices and polynomials: unified superfast algorithms*, Springer-Verlag New York, Inc., New York, NY, USA, 2001.
[32] T. Sasaki, *A Theory and an Algorithm of Approximate Gröbner Bases*, in 2011 13th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), Dongming Wang, V. Negru, T. Ida, T. Jebelean, D. Petcu, S. Watt, and D. Zaharie, eds., IEEE Comput. Soc., 2011 2011, pp. 23–30. 2011 13th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 26-29 Sept. 2011, Timisoara, Romania.
[33] Tateaki Sasaki and Fuji Kako, *Term Cancellations in Computing Floating-Point Gröbner Bases*, in Computer Algebra in Scientific Computing, Gerdt, VP and Koepf, W and Mayr,

EW and Vorozhtsov, EV, ed., vol. 6244 of Lecture Notes in Computer Science, Tech Univ Munchen, Dept Informat; Inst Informat & Automat Problems, 2010, pp. 220–231. 12th CASC International Workshop, Tsakhkadzor, ARMENIA, SEP 06-12, 2010.

[34] K Shirayanagi, *An Algorithm to compute Floating-Point Gröbner Bases*, in MathematicaL Computation with MAPLE V: Ideas and Applications, Lee, T, ed., 1993, pp. 95–106. Maple Summer Workshop and Symposium on Mathematical Computation with Maple V: Ideas and Applications, univ Michigan, Ann Arbor, MI, JUN 28-30, 1993.

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

[36] ———, *Numerical Polynomial Algebra*, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2004.

[37] J. J. Sylvester, *On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturms function and that of the greatest algebraical common measure*, Trans. Roy. Soc. Lond., (1853).

[38] C. K. Yap, *A New Lower Bound Construction for Commutative Thue Systems with Applications*, Journal Of Symbolic Computation, 12 (1991), pp. 1–27.

[39] Zhonggang Zeng, *A numerical elimination method for polynomial computations*, Theor. Comput. Sci., 409 (2008), pp. 318–331.

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

[41] Zhonggang Zeng and Barry H. Dayton, *The approximate gcd of inexact polynomials*, in Proceedings of the 2004 international symposium on Symbolic and algebraic computation, ISSAC '04, New York, NY, USA, 2004, ACM, pp. 320–327.