Nœther Bases and Their Applications

Amir Hashemi and Hossein Parnian

Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran
Amir.Hashemi@cc.iut.ac.ir,Hossein.Parnian@math.iut.ac.ir

Werner M. Seiler

Institut für Mathematik, Universität Kassel, Heinrich-Plett-Straße 40, 34132 Kassel, Germany
Seiler@mathematik.uni-kassel.de

Abstract

In this paper, we introduce a new involutive division, called *D-Nœther division*, and the corresponding notion of a *Nœther basis*. It is shown that that an ideal is in Nœther position, if and only if it possesses a finite Nœther basis. We present a deterministic algorithm which, given a homogeneous ideal, finds a linear change of variables so that the ideal after performing this change possesses a finite Nœther basis (and equivalently is in Nœther position). Furthermore, we define the new concept of an ideal of *Nœther type* and study its connections with Rees decompositions. We have implemented all the algorithms described in this paper in MAPLE and assess their performance on a number of benchmark examples.

1 Introduction

Assume that $\mathcal{R}$ is the polynomial ring $\mathcal{K}[x_1,\ldots,x_n]$ where $\mathcal{K}$ is an arbitrary infinite field. Let $\mathcal{I}$ be a homogeneous ideal of $\mathcal{R}$ with the Krull dimension D. Then, we say that $\mathcal{I}$ is in *Nœther position*, if $\mathcal{K}[x_{n-D+1},\ldots,x_n] \hookrightarrow \mathcal{R}/\mathcal{I}$ is an integral ring extension, i.e. the image in $\mathcal{R}/\mathcal{I}$ of x_i for any $i = 1,\ldots,n-D$ is a root of a polynomial of the form $X^s + g_1X^{s-1} + \cdots + g_s = 0$ where s is an integer and $g_1,\ldots,g_s \in \mathcal{K}[x_{n-D+1},\ldots,x_n]$, see e.g. [6] for more details. This notion may be considered as an effective notion of genericity which has many applications in various domains of algebraic geometry such as affine ring theory, dimension theory, ring normalization and primary decomposition, we refer to [11, Chp. 3] for further information. In this direction, Giusti et al. [10] applied this notion to compute the dimension of a variety. Also, it was used by Krick and Logar [17] to compute the radical of an ideal and by Lecerf [18] to solve a system of polynomial equations and inequations. By introducing the new notion of an ideal in simultaneous Nœther position, Bardet et al. [1] analyzed the complexity of Gröbner bases computation by Faugère's F_5 algorithm.

It is worth noting that $\mathcal{I}$ being in Nœther position is equivalent to $\mathcal{R}/\mathcal{I}$ being a finitely generated $\mathcal{K}[x_{n-D+1},\ldots,x_n]$-module. In this case, $\mathcal{K}[x_{n-D+1},\ldots,x_n]$ is called a *Nœther normalization* of $\mathcal{R}/\mathcal{I}$. The Nœther normalization lemma states that after a generic linear change of variables, we may assume that $\mathcal{K}[x_{n-D+1},\ldots,x_n]$ is a Nœther normalization of $\mathcal{R}/\mathcal{I}$ and in consequence $\mathcal{I}$ is in Nœther position, see [11]. In this context two main questions may arise: How to check whether a given homogeneous ideal is in Nœther position? And in the case of a negative answer, how to find efficiently a linear change of variables Φ so that $\Phi(\mathcal{I})$ is in Nœther position? Logar [19] proposed the use of Gröbner bases with respect to the lexicographical monomial ordering (which is very expensive to compute) for a Nœther position test and if the ideal is not in such a position, he presented a random (and relatively sparse) linear change of variables to transform the ideal into Nœther position. Similarly, Greuel and Pfister [11] described an algorithm by applying random triangular linear changes of variables and again by computing lexicographic Gröbner basis. However, Bermejo and Gimenez [2, 3] presented an algorithm by using a random triangular linear changes of variables (depending on the dimension of the ideal) and by making use of Gröbner basis computations with respect to the degree reverse lexicographical monomial ordering. Finally, the first author in [12] gave a simple and efficient algorithm for Nœther position test without computing the dimension of the input (monomial) ideal.

In this paper, we are interested in exploring a deterministic and efficient algorithm to achieve a sparse linear change of variables transforming a given homogeneous ideal into Nœther position. In this direction, Robertz [22] described a (probabilistic) algorithm by applying *involutive bases* and *Stanley decompositions* to detect sparse linear transformations. Involutive bases are a particular kind of Gröbner bases with additional combinatorial properties. The origin of these bases lies with methods developed by Riquier [21] and Janet [16] for the analysis of partial differential equations. Zharkov and Blinkov [29] introduced the notion of *involutive polynomial bases*. Later on, Gerdt and Blinkov [9] introduced a more general concept of *involutive division* and *involutive bases* for polynomial ideals which may be considered as an effective alternative approach to the theory of Gröbner bases. Pommaret bases are a particular form of involutive bases introduced by Zharkov and Blinkov [29]. In general, a given ideal may not possess a finite Pommaret basis, however, if the ideal is in *quasi-stable position* (see Section 2 for the definition), then the ideal has a finite Pommaret basis. In particular, the third author [25] developed a deterministic approach (by performing repeatedly elementary linear changes and in each step computing the Janet basis of the ideal) to transform an ideal into quasi-stable position (see also [26]). It should be pointed out that Hashemi et al. [14] defined the notion of *weakly D-quasi-stable position* and showed that it is equivalent to Nœther position. In addition, they proposed a general framework to transform deterministically an ideal into a large number of combinatorially defined generic positions (including weakly D-quasi-stable position).

In this work, we first introduce a new involutive basis, called *Nœther basis*, and show that any homogeneous ideal in Nœther position has a finite Nœther basis and vice versa. Then, using this property and applying the approach presented in [25], we describe a deterministic algorithm to find a linear change of variables for a given homogeneous ideal so that the transformed ideal has a finite Nœther basis and equivalently is in Nœther position. In addition, we define the new concept of an ideal of *Nœther type* and study some of its properties in the context of this paper. All the algorithms described in this paper have been implemented in MAPLE and their performance is measured through several benchmark examples.

The article is organized as follows. In the next section, we review the basic definitions and notations which will be used throughout this paper. In Section 3, we define the D-Nœther division and discuss some of its basic properties. Section 4 is devoted to introducing the concept of Nœther bases and to showing that an ideal is in Nœther position, if and only if it possesses a finite Nœther basis. In Section 5, based on the results of the preceding sections, we describe a deterministic algorithm to transform a given homogeneous ideal into Nœther position and to compute the Nœther basis of the transformed ideal. Finally, we define the notion of an ideal of Nœther type and study some of its properties.

2 Preliminaries

In this section, we will fix the basic notations and recall some preliminaries needed in the subsequent sections. Throughout this paper, we let $\mathcal{R} = \mathcal{K}[x_1, \ldots, x_n]$ be the polynomial ring over an infinite field $\mathcal{K}$. We consider always *homogeneous* polynomials $f_1, \ldots, f_k \in \mathcal{R}$ and the ideal $\mathcal{I} = \langle f_1, \ldots, f_k \rangle$ generated by them. Furthermore, the dimension of $\mathcal{I}$ is the Krull dimension of the factor ring $\mathcal{R}/\mathcal{I}$ and is denoted by $D = \dim(\mathcal{I})$. We shall note that the Krull dimension corresponds to the dimension as *affine* and not as *projective* variety. We denote the degree with respect to a variable x_i of a polynomial $f \in \mathcal{R}$ by $\deg_i(f)$.

We will work mainly with the *degree reverse lexicographical monomial* ordering with $x_n \prec_{drl} \cdots \prec_{drl} x_1$. More precisely, for two monomials x^α and x^β we write $x^\alpha \prec_{drl} x^\beta$ if either $\deg(x^\alpha) < \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and the right-most non-zero entry of $\beta - \alpha$ is negative. The *leading monomial* of a polynomial $0 \neq f \in \mathcal{R}$, denoted by $\mathrm{LM}(f)$, is the greatest monomial appearing in f and its coefficient is called the *leading coefficient* of f, denoted by $\mathrm{LC}(f)$. The *leading term* of f is the product $\mathrm{LT}(f) = \mathrm{LC}(f)\mathrm{LM}(f)$. If $F \subset \mathcal{R}$ is a set of polynomials, $\mathrm{LM}(F)$ stands for the set $\{\mathrm{LM}(f) \mid f \in F\}$. The *leading ideal* of $\mathcal{I}$ is the monomial ideal $\mathrm{LM}(\mathcal{I}) = \langle \mathrm{LM}(f) \mid 0 \neq f \in \mathcal{I} \rangle$. A finite set $G \subset \mathcal{I}$ is called a *Gröbner basis* of $\mathcal{I}$ with respect to $\prec$, if $\mathrm{LM}(\mathcal{I}) = \langle \mathrm{LM}(G) \rangle$. We refer to [5] for more details on the theory of Gröbner bases. We continue by recalling some definitions and results from the theory of involutive bases, see [8, 26] for more information. Let $\mathcal{M}$ be the set of all monomials in $\mathcal{R}$.

Definition 2.1. *An* involutive division $\mathcal{L}$ *is defined on* $\mathcal{M}$*, if, for any nonempty finite set* $U \subset \mathcal{M}$ *and for any monomial* $u \in U$*, we can partition the set of variables* $\{x_1, \ldots, x_n\}$ *into two disjoint subsets* $M_{\mathcal{L}}(u, U)$ *of* multiplicative *variables and* $NM_{\mathcal{L}}(u, U)$ *of* non-multiplicative *variables such that for any* $u, v \in U$ *the following conditions hold:*

1. *If* $u\mathcal{L}(u, U) \cap v\mathcal{L}(v, U) \neq \emptyset$ *then either* $u \in v\mathcal{L}(v, U)$ *or* $v \in u\mathcal{L}(u, U)$*,*
2. *If* $v \in U$ *and* $v \in u\mathcal{L}(u, U)$ *then* $\mathcal{L}(v, U) \subseteq \mathcal{L}(u, U)$*,*
3. *If* $u \in V$ *and* $V \subseteq U$ *then* $\mathcal{L}(u, U) \subseteq \mathcal{L}(u, V)$*,*

where $\mathcal{L}(u, U)$ *denotes the subset of* $\mathcal{M}$ *consisting of all monomials in the variables* $M_{\mathcal{L}}(u, U)$*. For* $u \in U$*, if* $w \in u\mathcal{L}(u, U)$*, then we write* $w = u \times t$ *for* $t \in \mathcal{L}(u, U)$ *(or equivalently this property is denoted by* $u \mid_{\mathcal{L}} w$*) and in this case we say that* u *is an* involutive divisor *of* w*. If* $w = ut$ *with* $t \notin \mathcal{L}(u, U)$*, then we write* $w = u \cdot t$*.*

Given an involutive division $\mathcal{L}$ and a monomial ordering $\prec$, we are able to describe an $\mathcal{L}$-division algorithm (similar to the well-known division algorithm for polynomials) to $\mathcal{L}$-divide a given polynomial by a set of polynomials. In the literature, many different examples of involutive divisions can be found, however, in this paper we are only concerned with the Janet and the Pommaret division which are recalled below.

Definition 2.2. *For a finite set* $U \subset \mathcal{M}$ *of monomials, a sequence of non-negative integers* $d_1, \ldots, d_n$ *and an index* $0 \leq i \leq n$ *define*

$$[d_1, \ldots, d_i] = \{u \in U \mid d_j = \deg_j(u), 1 \leq j \leq i\}.$$

x_1 *is Janet multiplicative (or shortly* $\mathcal{J}$*-multiplicative) for* $u \in U$*, if* $\deg_1(u) = \max\{\deg_1(v) \mid v \in U\}$*. For* $i > 1$*,* x_i *is* $\mathcal{J}$*-multiplicative for* $u \in U$*, if* $\deg_i(u) = \max\{\deg_i(v) \mid v \in [\deg_1(u), \ldots, \deg_{i-1}(u)]\}$*.*

Definition 2.3. *For* $u = x_1^{d_1} \cdots x_k^{d_k}$ *with* $d_k > 0$*, the integer* k *is called the* class *of* u *and is denoted by* $\operatorname{cls}(u)$*. The variables* $x_{\operatorname{cls}(u)}, \ldots, x_n$ *are Pommaret multiplicative (or shortly* $\mathcal{P}$*-multiplicative) for* u*. For* $u = 1$*, all variables are Pommaret multiplicative.*

Example 2.4. *For* $U = \{x_1^2, x_1x_2x_3\} \subset \mathcal{K}[x_1, x_2, x_3]$*, we have*

Monomial	$M_{\mathcal{J}}$	$NM_{\mathcal{J}}$	$M_{\mathcal{P}}$	$NM_{\mathcal{P}}$
x_1^2	x_1, x_2, x_3		x_1, x_2, x_3	
$x_1x_2x_3$	x_2, x_3	x_1	x_3	x_1, x_2

Definition 2.5. *For a finite set* $U \subset \mathcal{M}$ *of monomials, the sets* $\mathcal{C}(U) = \bigcup_{u \in U} u\mathcal{M}$ *and* $\mathcal{C}_{\mathcal{L}}(U) = \bigcup_{u \in U} u\mathcal{L}(u, U)$ *are called the* cone *and the* $\mathcal{L}$-involutive cone*, respectively, generated by* U*.*

Definition 2.6. *For a finite set* $U \subset \mathcal{M}$ *of monomials, a superset* $U \subseteq \tilde{U} \subseteq \mathcal{M}$ *is called an* $\mathcal{L}$-completion*, if* $\mathcal{C}(U) = \mathcal{C}_{\mathcal{L}}(\tilde{U})$*. Furthermore,* U *is* $\mathcal{L}$-complete *or* $\mathcal{L}$-involutive*, if we have* $\mathcal{C}_{\mathcal{L}}(U) = \mathcal{C}(U)$*. An involutive division* $\mathcal{L}$ *is said to be* Nœtherian*, if every finite set* U *possesses a finite* $\mathcal{L}$*-completion.*

We are now ready to introduce the concept of an involutive basis. A finite set $F \subset \mathcal{R}$ is $\mathcal{L}$-autoreduced, if for any $f \in F$ no monomial occurring in f is $\mathcal{L}$-divisible by an element in $\operatorname{LM}(F) \setminus \{\operatorname{LM}(f)\}$.

Definition 2.7. *Let* $\mathcal{I} \subset \mathcal{R}$ *be an ideal,* $\mathcal{L}$ *an involutive division and* $\prec$ *a monomial ordering. Then a finite* $\mathcal{L}$*-autoreduced subset* $G \subset \mathcal{I}$ *is called* $\mathcal{L}$-involutive basis *(or shortly involutive basis) for* $\mathcal{I}$*, if for each* $f \in \mathcal{I}$ *there exists* $g \in G$ *so that* $\operatorname{LM}(g)|_{\mathcal{L}}\operatorname{LM}(f)$*.*

It follows immediately from this definition that every involutive basis forms a Gröbner basis for the ideal it generates. In addition to Nœtherianity, an algorithmically suitable involutive division must be *continuous* and *constructive.*

Definition 2.8. *An involutive division* $\mathcal{L}$ *is* continuous*, if for any finite set* $U \subset \mathcal{M}$ *and for any finite sequence* $\{u_i\}_{1 \leq i \leq k}$ *of elements in* U *with*

$$(\forall i < k)\,(\exists x_j \in NM_{\mathcal{L}}(u_i, U))\;[u_{i+1} \mid_{\mathcal{L}} u_i.x_j] \tag{1}$$

the inequality $u_i \neq u_j$ *for* $i \neq j$ *holds.*

Definition 2.9. *A continuous involutive division $\mathcal{L}$ is* constructive*, if for any $U \subset \mathcal{M}$, $u \in U$, $x_i \in NM_{\mathcal{L}}(u,U)$ with $u.x_i \notin C_{\mathcal{L}}(U)$ and*

$$(\forall v \in U)(\forall x_j \in NM_{\mathcal{L}}(v,U))\ (v \cdot x_j \mid u \cdot x_i,\ v \cdot x_j \neq u \cdot x_i)\ [v \cdot x_j \in C_{\mathcal{L}}(U)] \tag{2}$$

the following condition holds:

$$(\forall w \in C_{\mathcal{L}}(U))\ [u \cdot x_i \notin w\mathcal{L}(w, U \cup \{w\})]. \tag{3}$$

It is worth noting that, if an involutive division $\mathcal{L}$ is continuous, then for constructing an involutive basis, one may consider an involutive variant of Buchberger's criterion by constructing non-multiplicative prolongations (instead of S-polynomials) and performing $\mathcal{L}$-division. In consequence, Def. 2.7 becomes then equivalent to the statement that for each $f \in G$ and each $x_i \in NM_{\mathcal{L}}(\mathrm{LM}(f), \mathrm{LM}(G))$, the remainder of the $\mathcal{L}$-division of $x_i f$ by G is zero. Moreover, if $\mathcal{L}$ is constructive, then in the course of involutive basis computations one does not need to enlarge the intermediate basis by adding multiplicative prolongations.

Gerdt and Blinkov [9, Prop. 3.6, Cor. 4.11, Prop. 4.13] proved that both the Janet and the Pommaret division are involutive, continuous and constructive. Furthermore, in loc. cit. Prop. 4.5, they showed that the Janet division is Nœtherian, however the following simple example illustrates that Pommaret division is not Nœtherian.

Example 2.10. *Let $\mathcal{I} = \langle x_1x_2 \rangle \subset \mathcal{K}[x_1, x_2]$. Its Pommaret basis is the infinite set $\{x_1^i x_2 \mid i \geq 1\}$.*

It should be pointed out that if a given ideal is in *quasi-stable position* (see below for definition), then it has a finite Pommaret basis. In addition, if $\mathcal{K}$ is infinite, then, any ideal can be put by a generic linear change of variables into quasi-stable position and possesses then a finite Pommaret basis, see [25] for more details.

Definition 2.11. *A monomial ideal $\mathcal{I} \subset \mathcal{R}$ is* quasi-stable*, if for any monomial $m \in \mathcal{I}$ and all positive integers i, j, s with $1 \leq j < i \leq n$, if $x_i^s \mid m$, there exists an integer $t \geq 0$ such that $x_j^t(m/x_i^s) \in \mathcal{I}$. An ideal $\mathcal{I} \subset \mathcal{R}$ is in* quasi-stable position*, if $\mathrm{LM}(\mathcal{I})$ is quasi stable.*

Proposition 2.12 ([25, Prop. 4.4])**.** *A homogeneous ideal $\mathcal{I}$ has a finite Pommaret basis, if and only if it is in quasi stable position.*

The third author [25] developed a deterministic approach which, given a homogeneous ideal, constructs by performing repeatedly an elementary linear change of variables and performing a test on the Janet basis of the transformed ideal a new coordinate system such that the final transformed ideal is in quasi-stable position.

We conclude this section by recalling the notion of an ideal in Nœther position. We say that a homogeneous ideal $\mathcal{I}$ with $\dim(\mathcal{I}) = D$ is in *Nœther position*, if $\mathcal{K}[x_{n-D+1}, \ldots, x_n] \hookrightarrow \mathcal{R}/\mathcal{I}$ is an integral ring extension, i.e. the image in $\mathcal{R}/\mathcal{I}$ of x_i for any $i = 1, \ldots, n-D$ is a root of a polynomial of the form $X^s + g_1X^{s-1} + \cdots + g_s = 0$ where s is an integer and $g_1, \ldots, g_s \in \mathcal{K}[x_{n-D+1}, \ldots, x_n]$. Geometrically, the Nœther position guarantees that, for any values of $x_{n-D+1}, \ldots, x_n$ in an algebraic closure of $\mathcal{K}$, the system obtaining by replacing these values in the f_i's has exactly the same number of solutions (counting with multiplicity). Bermejo and Gimenez [2, Lem. 4.1] provided the following effective test (using Gröbner bases) for being in Nœther position.

Lemma 2.13. *For any ideal $\mathcal{I} \subset \mathcal{R}$, the following conditions are equivalent:*

1. *$\mathcal{I}$ is in Nœther position,*
2. *For any $i = 1, \ldots, n-D$, there exists $r_i \in \mathbb{N}$ such that $x_i^{r_i} \in \mathrm{LM}(\mathcal{I})$,*
3. *$\dim(\mathcal{I} + \langle x_{n-D+1}, \ldots, x_n \rangle) = 0$.*

Using this lemma, one can easily check that an ideal in quasi-stable position is also in Nœther position (note that the converse is not always true). Based on this simple observation and the definition of quasi stable ideals, Hashemi et al. [14] introduced the notion of *weakly D-quasi-stable ideals* and showed that it is equivalent to Nœther position.

Definition 2.14. *A monomial ideal $\mathcal{I}$ of dimension D is called* weakly D-quasi-stable*, if for any monomial $m \in \mathcal{I}$, any $j = n-D+1, \ldots, n$ and any integer s with $x_j^s \mid m$, there exists an integer t such that $x_i^t(m/x_j^s) \in \mathcal{I}$ for $i = 1, \ldots, n-D$. An ideal $\mathcal{I}$ is in* weakly D-quasi-stable position*, if $\mathrm{LM}(\mathcal{I})$ is weakly D-quasi-stable.*

Theorem 2.15 ([14, Thm. 4.4])**.** *A homogeneous ideal is in weakly D-quasi-stable position, if and only if it is in Nœther position.*

3 Nœther bases

In this section, we first introduce the new *D-Nœther division* and then discuss some of its properties which are useful in the context of involutive bases theory. Based on this division, we will also define the concept of Nœther bases. Furthermore, we provide equivalent conditions for the existence of a finite Nœther basis for a given ideal. In particular, we show that for any ideal having a finite Nœther basis is equivalent to being in Nœther position.

Definition 3.1. *For any finite set $U \subset \mathcal{M}$, any integer $0 \leq D \leq n$ and any $u \in U$, the variable x_i is called* D-Nœther multiplicative *(denoted by $\mathcal{N}$-multiplicative) for u, if one of the following conditions hold:*

1. $\operatorname{cls}(u) \leq n - D$ *and x_i is Janet multiplicative for $u \in U$,*

2. $\operatorname{cls}(u) > n - D$ *and $i > n - D$ and x_i is Janet multiplicative for $u \in U$.*

To show that this division is an involutive division, we shall need the following lemma which may be considered as a rephrasing of the well-known fact that for the Janet division any monomial set is $\mathcal{J}$-autoreduced.

Lemma 3.2. *Let $U \subset \mathcal{M}$ be a finite set and $u, v \in U$. If there is $w \in \mathcal{M}$ such that $u \mid_{\mathcal{J}} w$ and $v \mid_{\mathcal{J}} w$ then $u = v$.*

Proof. Assume to the contrary that $u \neq v$. Therefore, without loss of generality, we may assume that there exists an index j such that for $1 \leq i < j$ we have $\deg_i(u) = \deg_i(v)$ and $\deg_j(u) > \deg_j(v)$. According to the definition of the Janet division, x_j thus cannot be $\mathcal{J}$-multiplicative for v. Since $u \mid_{\mathcal{J}} w$ and $v \mid_{\mathcal{J}} w$, we must have $u \times u_1 = v \times v_1 = w$ which entails that x_j must be a $\mathcal{J}$-multiplicative variable for v which leads to a contradiction. □

Proposition 3.3. *The D-Nœther division is an involutive division.*

Proof. Let $U \subset \mathcal{M}$ be a finite set and D an integer. We must prove that the conditions stated in Def. 2.1 hold. Let $u, v \in U$ be two D-Nœther divisors of $w \in \mathcal{M}$. According to Def. 3.1, $u, v \in U$ are Janet divisors of w and by Lem. 3.2 we have $u = v$, implying the first condition in Def. 2.1. To prove the second condition, let $u, v \in U$, $v \in u\mathcal{N}(u, U)$ and x_i be a D-Nœther multiplicative variable for v. Three cases must be distinguished. If either $\operatorname{cls}(u) \leq n - D$ or $i > n - D$, then, by definition and the properties of the Janet division, x_i is $\mathcal{J}$-multiplicative for v and thus also $\mathcal{N}$-multiplicative for u. It is impossible that $\operatorname{cls}(u) > n - D$, $i \leq n - D$ and $\operatorname{cls}(v) \leq n - D$, because $v \in u\mathcal{N}(u, U)$ by assumption. It is also impossible that $\operatorname{cls}(u) > n - D$, $i \leq n - D$ and $\operatorname{cls}(v) > n - D$ due to the assumption that x_i is an $\mathcal{N}$-multiplicative variable for v. Finally, to check the last condition in Def. 2.1, let $u \in V$ with $V \subseteq U$. By the properties of the Janet division, we have $\mathcal{J}(u, U) \subseteq \mathcal{J}(u, V)$ which implies that $\mathcal{N}(u, U) \subseteq \mathcal{N}(u, V)$, proving the claim. □

Corollary 3.4. *For any finite set $U \subset \mathcal{M}$, any integer $0 \leq D \leq n$ and any $u \in U$ the following inclusions hold:*

$$M_{\mathcal{N}}(u, U) \subseteq M_{\mathcal{J}}(u, U), \quad NM_{\mathcal{J}}(u, U) \subseteq NM_{\mathcal{N}}(u, U)\,.$$

Proof. The assertion follows immediately from the definition of the D-Nœther division. □

Example 3.5. *For $U = \{x_1x_2, x_2x_3, x_3x_4\} \subset \mathcal{K}[x_1, x_2, x_3, x_4]$ and $D = \dim(\langle U \rangle) = 2$, we have:*

Monomial	$M_{\mathcal{N}}$	$NM_{\mathcal{N}}$	$M_{\mathcal{J}}$	$NM_{\mathcal{J}}$	$M_{\mathcal{P}}$	$NM_{\mathcal{P}}$
x_1x_2	x_1, x_2, x_3, x_4		x_1, x_2, x_3, x_4		x_2, x_3, x_4	x_1
x_2x_3	x_3, x_4	x_1, x_2	x_2, x_3, x_4	x_1	x_3, x_4	x_1, x_2
x_3x_4	x_3, x_4	x_1, x_2	x_3, x_4	x_1, x_2	x_4	x_1, x_2, x_3

Next, we show that the D-Nœther division is continuous, but not constructive. Given its close connection to the Janet division, it is not surprising that the following proof is very similar to the proof of the continuity of the Janet division.

Proposition 3.6. *The D-Nœther division is continuous.*

Proof. Let U be a finite set, $0 \leq D \leq n$ and $\{u_i\}_{1\leq i\leq k}$ a finite sequence of elements in U satisfying (1). We shall show that there are no coinciding elements in this sequence. Assume that $u_{i+1} \mid_{\mathcal{N}} u_i \cdot x_{i_1}$. We claim that then $u_i \prec_{lex} u_{i+1}$ where $\prec_{lex}$ is the lexicographical monomial ordering with $x_n \prec \cdots \prec x_1$. To prove this claim, we first note that $u_{i+1} \neq u_i$, otherwise if $u_i = u_{i+1}$ then $x_{i_1} \in M_{\mathcal{N}}(u_i, U)$ which contradicts our assumptions. It follows that there is an index t such that $\deg_l(u_i) = \deg_l(u_{i+1})$ for each $l < t$ and $\deg_t(u_i) \neq \deg_t(u_{i+1})$. If $\deg_t(u_i) > \deg_t(u_{i+1})$, then the assumption $u_{i+1} \mid_{\mathcal{N}} (u_i \cdot x_{i_1})$ entails $x_t \in M_{\mathcal{N}}(u_{i+1}, U)$ which leads to a contradiction (note that $u_i, u_{i+1} \in [d_1, \ldots, d_{t-1}]$). This proves the claim and consequently $u_i \neq u_j$ for $i \neq j$. □

Example 3.7. *Let $U = \{x_1x_2, x_1x_2x_3, x_3x_4\} \subset \mathcal{K}[x_1, x_2, x_3, x_4]$. For the choice $D = \dim(\langle U\rangle) = 2$, we find $M_{\mathcal{N}}(x_1x_2) = \{x_1, x_2, x_4\}$, $M_{\mathcal{N}}(x_1x_2x_3) = \{x_3, x_4\}$ and $M_{\mathcal{N}}(x_3x_4) = \{x_3, x_4\}$. In particular, we have $(x_1x_2x_3) \cdot x_1 \notin C_{\mathcal{N}}(U)$ and $(x_1x_2x_3) \cdot x_1$ satisfies condition (2) in the definition of constructivity, but $(x_1x_2x_3) \cdot x_1 \in C_{\mathcal{N}}(U \cup \{w = x_1x_2 \times x_1\})$ since $(x_1x_2x_3) \cdot x_1 = w \times x_3$ and $x_3 \in M_{\mathcal{N}}(w, U \cup \{w\})$.*

Definition 3.8. *Let $\mathcal{I} \subset \mathcal{R}$ be a homogeneous ideal and $\prec$ a monomial ordering. Then a finite $\mathcal{N}$-autoreduced subset $G \subset \mathcal{I}$ for the choice $D = \dim(\mathcal{I})$ is called a* D-Nœther basis *for $\mathcal{I}$, if for each $f \in \mathcal{I}$ there exists $g \in G$ so that $\mathrm{LM}(g) \mid_{\mathcal{N}} \mathrm{LM}(f)$.*

Example 3.9. *The D-Nœther division is not Nœtherian, as one can see with the help of the same ideal already used in Example 2.10. Consider again $\mathcal{I} = \langle x_1x_2\rangle \subset \mathcal{K}[x_1, x_2]$. Obviously, $D = \dim(\mathcal{I}) = 1$ and the Nœther basis of $\mathcal{I}$ is the infinite set $\{x_1^i x_2 \mid i \geq 1\}$. It is easy to see that Nœtherianity of D-Nœther division holds for the special cases $D = 0, n$.*

We shall now investigate when a finite Nœther basis exists using the following lemma.

Lemma 3.10. *Let $U \subset \mathcal{M}$ be the minimal Janet basis of $\langle U\rangle$. Then, there do not exist monomials $u_1, u_2 \in U$ such that $u_1 \neq u_2$ and $\deg_i(u_1) = \deg_i(u_2)$ for each $1 \leq i \leq \mathrm{cls}(u_1)$.*

Proof. Assume in the contrary that there are monomials u_1, u_2 satisfying the mentioned conditions. We claim that then there exists a proper subset $U' \subsetneq U$ forming a Janet basis for $\langle U\rangle$. Let $U' = U \setminus A$ where

$$A = \{u \in U \mid \deg_i(u_1) = \deg_i(u), 1 \leq i \leq \mathrm{cls}(u_1), u \neq u_1\}.$$

Then A is not empty, as $u_2 \in A$. It is easy to see that for all $t > \mathrm{cls}(u_1)$, x_t is Janet multiplicative for $u_1 \in U'$ which entails that the elements of A belong to the $\mathcal{J}$-cone of U'. This completes the proof of the claim which contradicts the minimality of U. □

In analogy to the situation for Pommaret bases (see in particular Prop. 2.12), we now show that a finite Nœther basis exists in generic position and that it then coincides with the Janet basis.

Theorem 3.11. *Let $\mathcal{I} \subset \mathcal{R}$ be a monomial ideal with $D = \dim(\mathcal{I})$. The following conditions are equivalent:*

1. *$\mathcal{I}$ is weakly D-quasi-stable.*
2. *If U is the minimal Janet basis for $\mathcal{I}$, then $M_{\mathcal{J}}(u, U) = M_{\mathcal{N}}(u, U)$ for all $u \in U$,*
3. *There exists a finite Janet basis U for $\mathcal{I}$ with $M_{\mathcal{J}}(u, U) = M_{\mathcal{N}}(u, U)$ for all $u \in U$,*
4. *$\mathcal{I}$ possesses a finite Nœther basis.*

Proof. (1 ⇒ 2). Suppose that $\mathcal{I}$ is weakly D-quasi-stable and U is the minimal Janet basis for $\mathcal{I}$. We show that for all $u \in U$, $M_{\mathcal{J}}(u, U) = M_{\mathcal{N}}(u, U)$. We know that $M_{\mathcal{N}}(u, U) \subseteq M_{\mathcal{J}}(u, U)$. Now assume in the contrary that there exists $u \in U$ such that $M_{\mathcal{N}}(u, U) \subsetneq M_{\mathcal{J}}(u, U)$. According to Def. 3.1, we have $\mathrm{cls}(u) > n - D$ and there exists $i \leq n - D$ such that x_i is Janet multiplicative for u. Suppose that $u = x_1^{d_1} \cdots x_i^{d_i} \cdots x_j^{d_j}$ where $j = \mathrm{cls}(u)$. Since $\mathcal{I}$ is weakly D-quasi-stable, there exists an integer t such that $u_1 = x_i^t(u/x_j^{d_j}) \in \mathcal{I}$. On the other hand, U is a Janet basis for $\mathcal{I}$ and thus there exists $m \in U$ such that $m = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid_{\mathcal{J}} u_1$. By the definition of Janet division, it follows from $m, u \in U$ that we have $\alpha_\ell = d_\ell$ for each $\ell < i$. In addition, since x_i is Janet multiplicative for u and $t \geq 0$, we find $\alpha_i = d_i$. By similar arguments, we obtain $\deg_\ell(u) = \deg_\ell(m)$ for $1 \leq \ell \leq j-1$, Thus u and m belong to $[d_1, \ldots, d_{j-1}]$ and $\mathrm{cls}(m) = j - 1$, which leads to a contradiction by applying Lem. 3.10.

(2 ⇒ 3). This implication is obvious.

$(3 \Rightarrow 1)$. Suppose that U is a finite Janet basis for $\mathcal{I}$ and $M_{\mathcal{J}}(u,U) = M_{\mathcal{N}}(u,U)$ for all $u \in U$. We show that $\mathcal{I}$ is weakly D-quasi-stable. Let $m = x_1^{\alpha_1} \cdots x_j^{\alpha_j} \cdots x_n^{\alpha_n} \in U$, $0 \neq j > n-D, 1 \leq i \leq n-D$. We shall prove that $x_i^t(m/x_j^{\alpha_j})$ for some t belongs to $\mathcal{I}$. Let $\ell = \max\{\deg_i(u) \mid u \in U\}$. We consider $h = x_i^{\ell-\alpha_i+1}m \in \mathcal{I}$. Since U is a Janet basis for $\mathcal{I}$, there exists $u_1 = x_1^{\beta_1} \cdots x_n^{\beta_n} \in U$ such that $u_1 \mid_{\mathcal{J}} h$. Note that ℓ is of maximal degree in x_i in U which implies that x_i is Janet multiplicative for u_1. It then follows that $\deg_t(u_1) = \deg_t(m)$ for each $1 \leq t \leq i-1$ and $\deg_t(u_1) \leq \deg_t(m)$ for each $i \leq t \leq n-D$. On the other hand, due to the definition of h, x_i must be Janet multiplicative for u_1 and from $x_i \in M_{\mathcal{J}}(u_1,U) = M_{\mathcal{N}}(u_1,U)$ we conclude that $\text{cls}(u_1) \leq n-D$ and $\deg_t(u_1) = 0$ for each $t > n-D$ (see Def. 3.1). Thus, there exists an integer t so that $u_1 \mid x_i^t(m/x_j^{\alpha_j})$ proving the desired result.

$(3 \Rightarrow 4)$. The proof is obvious.

$(4 \Rightarrow 3)$. Suppose that U is a finite Nœther basis for $\mathcal{I}$. It is enough to show $M_{\mathcal{J}}(u,U) = M_{\mathcal{N}}(u,U)$ for each $u \in U$. Now suppose that there exists $u \in U$ such that $M_{\mathcal{N}}(u,U) \subsetneq M_{\mathcal{J}}(u,U)$. According to Def. 3.1, $\text{cls}(u) > n-D$ and for some $i \leq n-D$, x_i is Janet multiplicative for u. Since U is a Nœther basis for $\mathcal{I}$, there exists $u_1 \neq u$ such that $u_1 \in U, u_1 \mid_{\mathcal{N}} u \cdot x_i$. This implies that $u_1 \mid_{\mathcal{J}} u \cdot x_i$ which entails $u = u_1$ (using the fact that x_i is Janet multiplicative for u) and this gives rise to a contradiction. □

This theorem together with Thm. 2.15 has the following obvious consequence.

Corollary 3.12. *A homogeneous ideal $\mathcal{I} \subset \mathcal{R}$ is in Nœther position, if and only if it possesses a finite Nœther basis.*

Remark 3.13. *It should be noted that the condition of minimality in the second part of Thm. 3.11 is essential. To see this, let $\mathcal{I} = \langle x_1, x_1x_2 \rangle \subset \mathcal{K}[x_1,x_2]$. Then, $D = \dim(\mathcal{I}) = 1$ and $\mathcal{I}$ is in Nœther position and $U = \{x_1, x_1x_2\}$ is a Janet basis for $\mathcal{I}$ that is not minimal. Also, we have $M_{\mathcal{N}}(x_1x_2,U) = \{x_2\} \neq M_{\mathcal{J}}(x_1x_2,U) = \{x_1,x_2\}$.*

Proposition 3.14. *Every homogeneous ideal $\mathcal{I} \subset \mathcal{R}$ having a finite Pommaret basis possesses a finite Nœther basis, too.*

Proof. By Prop. 2.12, the existence of a finite Pommaret basis for $\mathcal{I}$ is equivalent to $\mathcal{I}$ being in quasi-stable position. Comparing Defs. 2.11 and 2.14, this implies that $\mathcal{I}$ is in weakly D-quasi-stable position and hence has a finite Nœther basis by Thm. 3.11. □

Since in general weak D-quasi-stability is strictly weaker than quasi-stability, the converse of Prop. 3.14 is of course not true.

Example 3.15. *Let $\mathcal{I} = \langle x_1^2, x_1x_2x_3 \rangle \subset \mathcal{K}[x_1,x_2,x_3]$. The minimal Janet basis of $\mathcal{I}$ is $\{x_1^2, x_1x_2x_3\}$ and simultaneously a Nœther basis of $\mathcal{I}$. However, the minimal Pommaret basis of $\mathcal{I}$ is the infinite set $\{x_1x_2^ix_3, x_1^2 \mid i \geq 1\}$.*

According to [25, Thm. 2.16], quasi-stability is a generic condition. Hence, obviously the same is true for weak D-quasi-stability which proves the following result.

Corollary 3.16. *Every homogeneous ideal $\mathcal{I} \subset \mathcal{R}$ has a finite Nœther basis in generic position.*

4 Computation of Nœther bases

In this section, we describe an algorithm, which, given a homogeneous ideal, finds an explicit linear change of variables such that the transformed ideal possesses a finite Nœther basis. Since the D-Nœther division is not constructive, [9, Thm. 4.14] cannot be directly applied to construct a Nœther basis for an ideal (even if the ideal is in Nœther position). Below, we show how we can adapt a construction described by the third author in [25].

Our next goal is to describe a deterministic algorithm for the construction of a sparse linear change of variables to transform the input ideal into Nœther position. For this purpose, we apply the iterative method presented in [25] using at each step an elementary linear change of variables, computing the minimal Janet basis of the transformed ideal and performing a test to check whether or not the desired position has been achieved. The following subalgorithm determines whether or not a given monomial Janet basis is a Nœther basis. If A is an ordered set, then $A[i]$ stands for the i-th element of A.

Algorithm 1 Test

```
1: Input: A finite set $U \subset R$ of monomials
2: Output: True if any element of $U$ has the same number of $D$-Nœther and Janet multiplicative
   variables, and otherwise a triple $(false, x_i, x_j)$ with $x_i, x_j$ two variables
3: if $\exists u \in U$ s.t. $M_{\mathcal{N}}(u,U) \neq M_{\mathcal{J}}(u,U)$ then
4:     $V := M_{\mathcal{J}}(u,U) \setminus M_{\mathcal{N}}(u,U)$
5:     return$(false, V[1], x_{\mathrm{cls}(u)})$
6: end if
7: return $(true)$
```

In the following algorithm for the construction of a Nœther basis, the call JanetBasis calculates the minimal Janet basis for a given ideal.

Algorithm 2 NoetherBasis

```
1: Input: A finite set $F \subset \mathcal{R}$ of homogeneous polynomials
2: Output: A linear change $\Phi$ so that $\langle \Phi(F) \rangle$ has a finite Nœther basis
3: $\Phi$ :=the identity linear change
4: $J$ :=JanetBasis$(F, \prec)$
5: $A$ :=Test(LM$(J)$)
6: while $A \neq true$ do
7:     $\phi := A[3] \mapsto A[3] + cA[2]$ where $c \in \mathcal{K}$ is a random number
8:     $Temp$ :=JanetBasis$(\Phi \circ \phi(J), \prec)$
9:     $B$ :=Test(LM$(Temp)$)
10:    if $B \neq A$ then
11:        $\Phi := \Phi \circ \phi$
12:        $A := B$
13:    end if
14: end while
15: return $(\Phi)$
```

To prove the termination and correctness of this algorithm, we shall need the following lemma.

Lemma 4.1. *If U is a minimal monomial Janet basis and $D = \dim(\langle U \rangle)$, then for all $u \in U$ we have*

$$M_{\mathcal{J}}(u,U) \backslash M_{\mathcal{N}}(u,U) \subseteq M_{\mathcal{J}}(u,U) \backslash M_{\mathcal{P}}(u)$$

Proof. To prove the desired inclusion we must show that $M_{\mathcal{P}}(u) \subseteq M_{\mathcal{N}}(u,U)$ for all $u \in U$. For each $u \in U$, two cases must be distinguished. If $\mathrm{cls}(u) \leq n - D$, then $M_{\mathcal{N}}(u,U) = M_{\mathcal{J}}(u,U)$ and therefore $M_{\mathcal{P}}(u) \subseteq M_{\mathcal{N}}(u,U)$. By Prop. 13 and Cor. 15 in [7], we conclude that $M_{\mathcal{P}}(u) \subseteq M_{\mathcal{J}}(u,U)$ for all $u \in U$ and this proves the assertion in the first case. Otherwise, if $\mathrm{cls}(u) > n - D$, then, from the inclusion $M_{\mathcal{P}}(u) \subseteq M_{\mathcal{J}}(u,U)$ and the definition of the D-Nœther division, we obtain $M_{\mathcal{P}}(u) \subseteq M_{\mathcal{N}}(u,U)$ which completes the proof. □

Theorem 4.2. *For a given homogeneous ideal $\mathcal{I} \subset \mathcal{R}$, the algorithm* NoetherBasis *terminates in finitely many steps and returns a linear change of variables Φ such that the transformed $\Phi(\mathcal{I})$ possesses a finite Nœther basis.*

Proof. Note that if we replace in the algorithm Test the line 4 by "$V := M_{\mathcal{J}}(u,U) \setminus M_{\mathcal{P}}(u,U)$", then we obtain the algorithm described in [25, Rem. 2.18] to find a linear change of variables such that the transformed ideal has a finite Pommaret basis. This, together with Lem. 4.1, implies the finite termination and correctness of the algorithm NoetherBasis. □

Remark 4.3. *Strictly speaking, the above algorithm* NoetherBasis *is not deterministic, as in line* 7 *a random number c is chosen. If we always take* $c = 1$ *and remove the lines* 10−13 *in* NoetherBasis*, then one obtains a completely deterministic algorithm. It follows by the same arguments as in [25, Rem. 9.11] that over an infinite field $\mathcal{K}$ this modified algorithm still terminates after finitely many steps.*

We illustrate the steps of the algorithm NoetherBasis through a simple example.

Example 4.4. *Let $\mathcal{I}_1 = \langle x_1^2x_2, x_1x_2x_3\rangle \subset \mathcal{K}[x_1, x_2, x_3]$ and $x_3 \prec_{drl} x_2 \prec_{drl} x_1$. Then, one sees readily that $G_1 = \{x_1^2x_2, x_1x_2x_3\}$ is the minimal Janet basis for $\mathcal{I}_1$. Note that $D = \dim(\mathcal{I}) = 2$ and thus $M_{\mathcal{J}}(x_1^2x_2, J_1) = \{x_1, x_2, x_3\}$, $M_{\mathcal{N}}(x_1^2x_2, J_1) = \{x_2, x_3\}$ and, $M_{\mathcal{P}}(x_1^2x_2) = \{x_2, x_3\}$. Thus, $\mathcal{I}_1$ is not in Nœther position by Thm. 3.11 and, invoking the algorithm* Test, *we perform the linear change $[x_2 = x_2+x_1]$. Applying this change on $\mathcal{I}_1$, we get the ideal $\mathcal{I}_2 = \langle x_1^2(x_2+x_1), x_1(x_2+x_1)x_3\rangle$. Computing the minimal Janet basis $G_2 = \{x_1^2(x_2+x_1), x_1(x_2+x_1)x_3\}$ for $\mathcal{I}_2$, we can see that $\mathrm{LM}(G_2) = \{x_1^3, x_1^2x_3\}$. Since $M_{\mathcal{J}}(x_1^3, \mathrm{LM}(G_2)) = M_{\mathcal{N}}(x_1^3, \mathrm{LM}(G_2))$, $M_{\mathcal{J}}(x_1^2x_3, \mathrm{LM}(G_2)) = M_{\mathcal{N}}(x_1^2x_3, \mathrm{LM}(G_2))$, G_2 is a finite Nœther basis for $\mathcal{I}_2$. It is worth noting that it follows from $M_{\mathcal{J}}(x_1^2x_3, \mathrm{LM}(G_2)) = \{x_2, x_3\}$ and $M_{\mathcal{P}}(x_1^2x_3, \mathrm{LM}(G_2)) = \{x_3\}$ that G_2 is not a finite Pommaret basis for $\mathcal{I}_2$. Applying the algorithm described in [25] to compute finite Pommaret bases, we shall continue by performing the additional linear change $[x_3 = x_3 + x_2]$. We get in turn the ideal $\mathcal{I}_3 = \langle x_1^2(x_2 + x_1), x_1(x_2 + x_1)(x_3 + x_2)\rangle$. Computing the minimal Janet basis $G_3 = \{x_1(x_2 + x_1)(x_3 + x_2), x_1^3 - x_1^2x_3 - x_1x_2^2 - x_1x_2x_3\}$ for $\mathcal{I}_3$, we can observe that $\mathrm{LM}(G_3) = \{x_1^2x_2, x_1^3\}$. If we turn our attention to this set, then one can see that $M_{\mathcal{J}}(x_1^3, \mathrm{LM}(G_3)) = M_{\mathcal{P}}(x_1^3, \mathrm{LM}(G_3))$, $M_{\mathcal{J}}(x_1^2x_2, \mathrm{LM}(G_3)) = M_{\mathcal{P}}(x_1^2x_2, \mathrm{LM}(G_3))$, and thus that G_3 is a finite Pommaret basis for $\mathcal{I}_3$.*

We end this section by comparing the performance of our proposed algorithm to transform a given ideal into Nœther position with other existing algorithms. For this purpose, we chose two known algorithms, namely NoetherNormalization due to Robertz [22] [1] and WDQSPosition proposed by the first author in [13] based on the notion of weakly D-quasi-stable position. We have implemented NoetherBasis and WDQSPosition in Maple 18[2]. In the following tables, we compare only the number of performed elementary linear changes (to transform the input ideal into Nœther position) for some well-known examples[3] from computer algebra literature. In the paper at hand, we only want to compare the structure and the behavior of the algorithms and not the running times of their implementations which are also influenced by many other factors. All computations were done over the field of the rational number using the degree reverse lexicographical ordering.

Weispfenning94	changes
NoetherBasis	1
WDQSPosition	1
NoetherNormalization	1

Sturmfels and Eisenbud	changes
NoetherBasis	11
WDQSPosition	17
NoetherNormalization	11

Liu	changes
NoetherBasis	4
WDQSPosition	4
NoetherNormalization	4

Eco7	changes
NoetherBasis	2
WDQSPosition	2
NoetherNormalization	2

Vermeer	changes
NoetherBasis	1
WDQSPosition	2
NoetherNormalization	1

Gerdt2	changes
NoetherBasis	1
WDQSPosition	1
NoetherNormalization	1

Remark 4.5. *One can see that the sparsity of the linear changes constructed by our algorithm is the same as for Robertz' algorithm. It should be mentioned that* NoetherBasis *is a deterministic algorithm, while the one by Robertz is probabilistic. The latter algorithm proceeds as follows. It computes a Janet basis G for its input ideal $\mathcal{I}$ and then uses it to compute a monomial cone decomposition $\oplus_{i=1}^s \mathcal{K}[X_i].m_i$ with $X_i \subset \{x_1, \ldots, x_n\}$ for $\mathcal{R}/\mathcal{I}$. If there exists a polynomial $g \in G$ such that $\mathrm{LM}(g)$ is in terms of $X = \cup_{i=1}^s X_i$, then the algorithm applies the linear change $x_i = x_i + \alpha_i z$ for each i where α_i is a random number, z the greatest variable in X and $x_i \neq z$ a variable appearing in $\mathrm{LM}(g)$. Robertz proved that if $|X| = \dim(\mathcal{I})$ then the algorithm terminates. Note that in each iteration of Robertz' algorithm, several elementary linear changes may be applied, however, in our approach only one elementary linear change is performed. In certain situation, Robertz' algorithm also permutes some variables. Finally, the advantage of our algorithm is that (in contrast to Robertz' algorithm) we do not need to compute a monomial cone decomposition for $\mathcal{R}/\mathcal{I}$.*

Remark 4.6. *Let us briefly explain how the algorithm* WDQSPosition *works. Given a homogeneous ideal $\mathcal{I}$, if the algorithms finds a monomial $m \in \mathrm{LM}(\mathcal{I})$, integers $i = 1, \ldots, n - D$, $j = n - D + 1, \ldots, n$ and s such that $x_j^s \mid m$ and for any integer t we have $x_i^t(m/x_j^s) \in \mathrm{LM}(\mathcal{I})$, then it makes the elementary linear change $x_j = x_j + x_i$ and it repeats this process until no obstructions remain. As one can see, the way of finding linear changes in this algorithm is quite different from the one presented in the algorithm*

[1] We refer to `http://math.rwth-aachen.de/Janet/involutive` for the Maple implementation of this algorithm.

[2] The Maple code of our implementations and examples are available at `http://amirhashemi.iut.ac.ir/softwares`

[3] For further details see the SymbolicData Project (`http://www.SymbolicData.org`)

NOETHERBASIS *and for this reason we find for some examples a different number of changes of variables. One can think of many natural strategies to choose the next elementary linear change, but as examples in [24] show no strategy is always the best. It remains an interesting open question for further research to compare experimentally the average performance of different strategies. As our results here indicate, the differences can be significant.*

5 Ideals of Nœther type

In this section, we present some properties of the D-Nœther division related to syzygy modules. For this purpose, we recall first some related concepts and facts from [25]. It is well-known by Schreyer's theorem [23] that, keeping track of Gröbner basis computations, we are able to compute a Gröbner basis for the syzygy module of the computed Gröbner basis, see also [4]. An involutive version of this theorem was stated in [25] by replacing S-polynomials by non-multiplicative prolongations and keeping the trace of performed involutive divisions. Now, let us first briefly explain the main strategy used in [25] to compute involutive bases for submodules. For this, one needs the concept of Schreyer's module ordering which is a module monomial ordering on a free module. Given a finite set $\{g_1, \ldots, g_t\}$ and free module $\mathcal{R}^t$, let $\{\mathbf{e}_1, \ldots, \mathbf{e}_t\}$ be the standard basis of $\mathcal{R}^t$. Furthermore, let $\prec$ be a monomial ordering on $\mathcal{R}$. A module monomial in $\mathcal{R}^t$ is an element of the form $x^\alpha \mathbf{e}_i$ for some i, where x^α is a monomial in $\mathcal{R}$. *Schreyer's module ordering* is defined as follows: $x^\beta \mathbf{e}_j \prec_s x^\alpha \mathbf{e}_i$ if $\mathrm{LM}(x^\beta g_j) \prec \mathrm{LM}(x^\alpha g_i)$ and breaks ties by $i < j$.

Let $G \subset \mathcal{R}^t$ be a finite set and $\mathcal{L}$ an involutive division. We divide G into t disjoint subsets $G_i = \{\mathbf{g} \in G \mid \mathrm{LM}(\mathbf{g}) = x^\alpha \mathbf{e}_i, x^\alpha \in \mathcal{M}\}$ where $\{\mathbf{e}_1, \ldots, \mathbf{e}_t\}$ is the standard basis of $\mathcal{R}^t$. In addition, for each i, let $B_i = \{x^\alpha \in \mathcal{M} \mid x^\alpha \mathbf{e}_i \in \mathrm{LM}(G_i)\}$. We assign to each $\mathbf{g} \in G_i$ the multiplicative variables $M_\mathcal{L}(\mathbf{g}, G) = \{x_i \mid x_i \in M_\mathcal{L}(x^\alpha, B_i)$ with $\mathrm{LM}(\mathbf{g}) = x^\alpha \mathbf{e}_i\}$. Then, the definition of involutive bases for submodules proceeds in the same way as for the ideals. Now, to recall the involutive version of Schreyer's theorem, let $G = \{g_1, \ldots, g_t\} \subset \mathcal{R}$ be an involutive basis. Suppose that $g_i \in G$ is an arbitrary element and x_k is a non-multiplicative variable for g_i. By the definition of involutive bases, there exists j so that $\mathrm{LM}(g_j)|_\mathcal{L} x_k \mathrm{LM}(g_i)$. In the definition of Schreyer's ordering, we shall order the elements of G in such a way that $i < j$. Therefore, we can write $x_k g_i = \sum_{j=1}^t p_j^{(i,k)} g_j$ where $p_j^{(i,k)} \in \mathcal{K}[M_\mathcal{L}(g_j, G)]$. This equation corresponds to the syzygy $\mathbf{S}_{i,k} = x_k \mathbf{e}_i - \sum_{j=1}^t p_j^{(i,k)} \mathbf{e}_j \in \mathcal{R}^t$. We denote the set of all thus constructed syzygies by $G_{\mathrm{Syz}} = \{\mathbf{S}_{i,k} \mid 1 \le i \le t; x_k \in NM_\mathcal{L}(g_i, G)\}$. By Schreyer's theorem, one expects that G_{Syz} forms an involutive basis for $\mathrm{Syz}(G)$. However, the involutive version of Schreyer's theorem does not hold for all involutive divisions. An involutive division $\mathcal{L}$ is said to be of *Schreyer type*, if $NM_\mathcal{L}(g, G)$ for each $g \in G$ remains an involutive basis. Both the Janet and the Pommaret divisions are of Schreyer type, see [25] for more information. Now, by an example, we show that D-Nœther division is not of Schreyer type.

Example 5.1. *Let $\mathcal{I} = \langle x_1^2, x_1x_2x_3x_4^2, x_1x_2x_3^2x_4 \rangle \subset \mathcal{K}[x_1, x_2, x_3, x_4]$ and $D = \dim(\mathcal{I}) = 3$. Then, $\mathcal{I}$ is in Nœther position and the Nœther basis of $\mathcal{I}$ is $G = \{x_1^2, x_1x_2x_3x_4^2, x_1x_2x_3^2x_4\}$. However, the set $NM_\mathcal{N}(x_1x_2x_3x_4^2, G) = \{x_1, x_3\}$ is not a Nœther basis, because it is not in Nœther position.*

The following simple lemma provides a necessary and sufficient condition for a set of variables to form a Nœther basis.

Lemma 5.2. *$U \subset \{x_1, \ldots, x_n\}$ is a Nœther basis for the ideal it generates, if and only if there exists $1 \le t \le n$ such that $U = \{x_1, \ldots, x_t\}$.*

Motivated by this observation, we introduce a new class of monomial ideals restricted to which the D-Nœther division is of Schreyer type.

Definition 5.3. *A monomial ideal $\mathcal{I} \subset \mathcal{R}$ is called of* Nœther type*, if it has a finite Nœther basis U and if for every $u \in U$ the set $NM_\mathcal{N}(u, U)$ is a Nœther basis. An ideal $\mathcal{I} \subset \mathcal{R}$ is of* Nœther type*, if* $\mathrm{LM}(\mathcal{I})$ *is of Nœther type.*

According to [25, Thm. 5.10], G_{Syz} forms for any continuous division of Schreyer type an involutive basis for $\mathrm{Syz}(G)$. Now, we can state a similar result for D-Nœther division. The proof is exactly the same as the one of [25, Thm. 5.10].

Theorem 5.4. *Let $\mathcal{I} = \langle G \rangle$ be an ideal of Nœther type and G a finite Nœther basis for $\mathcal{I}$. Then the set G_{Syz} is a Nœther basis for the syzygy module $Syz(G)$ with respect to the Schreyer ordering $\prec_s$.*

Unfortunately, we have not been able to provide an algebraic characterization of ideals of Nœther type and leave this question as an open problem for future research. In the sequel, we study the connection between the notions of genericity defined in this paper and the concepts of *Stanley* and *Rees decomposition*. For this purpose, we first recall these concepts from [25]. When we speak of a basis of a monomial ideal $\mathcal{I}$, we always assume that it is monomial, too.

Definition 5.5. *Let $\mathcal{I} \subset \mathcal{R}$ be a homogeneous ideal. A* Stanley decomposition *of the graded $\mathcal{K}$-algebra $A = \mathcal{R}/\mathcal{I}$ is an isomorphism of graded $\mathcal{K}$-linear spaces of the form $A \cong \bigoplus_{t\in T} \mathcal{K}[X_t] \cdot t$ where $T \subset \mathcal{M}$ is a finite set and $X_t \subseteq \{x_1, \dots, x_n\}$.*

In an algebraic context, such combinatorial decompositions were introduced by Stanley [27] for computing Hilbert functions. However, they appeared already much earlier in the works of Riquier [21] and Janet [16] as central tools of their approach to the integrability of general systems of partial differential equations. Even within algebra, a special class of Stanley decompositions was studied considerably earlier by Rees [20].

Definition 5.6. *With the same notations as above, the Stanley decomposition $A \cong \bigoplus_{t\in T} K[X_t] \cdot t$ is called* Rees decomposition*, if for each generator $t \in T$ there exists an index i, called the* level *of t, such that $X_t = \{x_i, \dots, x_n\}$.*

We should mention that if a homogeneous ideal $\mathcal{I} \subset \mathcal{R}$ is of Nœther type, then its Nœther basis immediately induces a Stanley decomposition for the ideal itself as a graded $\mathcal{K}$-algebra with the set T given by the basis and each set X_t consisting of the multiplicative variables of t (any involutive basis does this). Less trivial is determining a *complementary* Stanley decomposition, i. e. one of the factor ring $A = \mathcal{R}/\mathcal{I}$. For Janet bases, already Janet [16] provided the algorithm ComplementaryDecomposition recalled below (see also [26, Alg. 5.2]). Another possibility is the recursive algorithm DecomposeComplement given in [22]. If $\mathcal{I}$ is in quasi-stable position, then its Pommaret basis induces a Rees decomposition of $\mathcal{I}$. Furthermore, also its factor ring A possesses a Rees decomposition (below we shall show that the converse is true, too). A usually rather redundant one can be easily obtained using the Pommaret basis of $\mathcal{I}$, see [25, Cor. 3.8]. A less redundant one can be computed with an algorithm given by Hironaka [15] which actually boils down to applying ComplementaryDecomposition to the Pommaret basis of $\mathcal{I}$.

Theorem 5.7. *For any homogeneous ideal $\mathcal{I} \subset \mathcal{R}$, the factor ring $A = \mathcal{R}/\mathcal{I}$ possesses a Rees decomposition, if and only if $\mathcal{I}$ is in quasi-stable position.*

Proof. By Macaulay's theorem (see e. g. [5, Prop. 4, page 250]), $\mathcal{R}/\mathcal{I}$ and $\mathcal{R}/\mathrm{LM}(\mathcal{I})$ are isomorphic as $\mathcal{K}$-vector spaces. Without loss of generality, we may thus assume that $\mathcal{I}$ is a monomial ideal. Assume that A has a Rees decomposition, but that $\mathcal{I}$ were not quasi-stable. This implies the existence of a monomial $m = x_1^{\alpha_1} \cdots x_k^{\alpha_k} \in \mathcal{I}$ and an index $j < k$ such that $m_\ell = x_1^{\alpha_1} \cdots x_{k-1}^{\alpha_{k-1}} x_j^\ell \notin \mathcal{I}$ for any $\ell > 0$. The Rees decomposition yields for each ℓ a unique generator $t_\ell \in T$ such that $m_\ell \in \mathcal{K}[X_{t_\ell}] \cdot t_\ell$. Since T is a finite set, there exists a $t \in T$ and a bound $\ell_0 > 0$ such that $t_\ell = t$ for all $\ell \geq \ell_0$. But this is only possible, if $x_j \in X_t$ and hence if $X_t = \{x_c, \dots, x_n\}$ for some $c \leq j$. As $j < k$, we also have $x_k \in X_t$. By construction, we find thus $m_\ell x_k^{\alpha_k} = m x_j^\ell \in \mathcal{K}[X_t] \cdot t$ for any $\ell \geq \ell_0$. But now we have the contradiction $m x_j^\ell \in \mathcal{I}$ and $\mathcal{I} \cap \mathcal{K}[X_t] \cdot t = \emptyset$. The converse holds by [25, Cor. 3.8]. □

In the appendix of [25], an algorithm for the construction of Rees decompositions due to Sturmfels and White [28] is compared with the theory of Pommaret bases. In particular, it was shown in [25, Prop. A.3] that the level of each generator of a Rees decomposition constructed with this algorithm is bounded by the class of the generator. Thm. 5.7 implies now that actually much stronger statements are true: the algorithm of Sturmfels and White always constructs a transformation to quasi-stable position and in any Rees decomposition the level of each generator is exactly its class. We conclude the paper by recalling the algorithm ComplementaryDecomposition in the form given in [26, Alg. 5.2] and use it to state a result related to Thm. 5.7.

Algorithm 3 ComplementaryDecomposition

```
1: Input: A minimal (monomial) Janet basis $U$ for monomial ideal $\mathcal{I}$
2: Output: A finite complementary decomposition for $\mathcal{R}/\mathcal{I}$
3: $\bar{U} := \emptyset$
4: for $k$ from $1$ to $n$ do
5:     for all $\emptyset \neq [d_1, \ldots, d_{k-1}] \subseteq U$ do
6:     choose arbitrary $u \in [d_1, \ldots, d_{k-1}]$
7:     $N := \{x_{k+1}, \ldots, x_n\} \cup \{x_i \in M_{\mathcal{J}}(u, U) \mid i < k\}$
8:         for $i$ from $0$ to $\max\{\deg_k(m) \mid m \in [d_1, \ldots, d_{k-1}]\}$ do
9:             if $\nexists m \in [d_1, \ldots, d_{k-1}]$ such that $\deg_k(m) = i$ then
10:                $\bar{U} := \bar{U} \cup \{(x_1^{d_1} \cdots x_{k-1}^{d_{k-1}} x_k^i, N)\}$
11:            end if
12:        end for
13:    end for
14: end for
15: return($\bar{U}$)
```

Theorem 5.8. *Let $U \subset \mathcal{M}$ be the minimal Janet basis for $\mathcal{I} = \langle U \rangle$. Then U is also a Pommaret basis, if and only if the above algorithm yields a Rees decomposition for $\mathcal{R}/\mathcal{I}$.*

Proof. Assume that U is simultaneously a finite Pommaret and Janet basis. By [26, Prop. 5.1.4], the output of the above algorithm, say $A \cong \bigoplus_{(t,N_t)\in\bar{U}} \mathcal{K}[N_t] \cdot t$ where $\bar{U}$ is a finite set and $N_t \subseteq \{x_1, \ldots, x_n\}$, is a Stanley decomposition of $\mathcal{R}/\mathcal{I}$. We claim that it is even a Rees decomposition. By the structure of the algorithm, we set in each step $N = \{x_{k+1}, \ldots, x_n\} \cup \{x_i \in M_{\mathcal{J}}(u, U) \mid i < k\}$. Now, two cases may arise. If $k \leq \operatorname{cls}(u)$, then $\{x_i \in M_{\mathcal{J}}(u, U) \mid i < k\}$ is the empty set and in turn $N = \{x_{k+1}, \ldots, x_n\}$ which proves our claim in this case.

Otherwise, we have $k > \operatorname{cls}(u)$. Since U is a Pommaret basis, $M_{\mathcal{J}}(u, U) = M_{\mathcal{P}}(u)$ and thus $N = \{x_{k+1}, \ldots, x_n\} \cup \{x_{\operatorname{cls}(u)}, \ldots, x_{k-1}\}$. We show that in this case the conditions in the **if**-loop in the line 9 are not satisfied and hence we do not add any element to $\bar{U}$. By Lem. 3.10, there does not exist a monomial $m \in U$ with $u \neq m$ and $\deg_i(u) = \deg_i(m)$ for all $1 \leq i \leq \operatorname{cls}(u)$. It follows that $\max\{\deg_k(m) \mid m \in [d_1, \ldots, d_{k-1}]\} = 0$. Since, for $i = 0$, we have $u \in [d_1, \ldots, d_{k-1}]$, the conditions in the **if**-loop are not satisfied and we are done.

Conversely, according to Thm. 5.7, $\langle U \rangle$ is quasi-stable and thus has a finite Pommaret basis (see Prop. 2.12). On the other hand, U is the minimal Janet basis for $\langle U \rangle$ which is a finite Pommaret basis by [7, Thm. 17], and this ends the proof. □

Acknowledgements

The work of the second author was partially performed as part of the H2020-FETOPEN-2016-2017-CSA project SC^2 (712689). The authors would like to thank the anonymous reviewers for their helpful comments.

References

[1] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the F_5 Gröbner basis algorithm. *J. Symb. Comput.*, 70:49–70, 2015.

[2] Isabel Bermejo and Philippe Gimenez. Computing the Castelnuovo-Mumford regularity of some subschemes of $\mathbb{P}^n_K$ using quotients of monomial ideals. *J. Pure Appl. Algebra*, 164(1-2):23–33, 2001.

[3] Isabel Bermejo and Philippe Gimenez. Saturation and Castelnuovo-Mumford regularity. *J. Algebra*, 303(2):592–617, 2006.

[4] David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry. 2nd ed.*, volume 185. New York, NY: Springer, 2005.

[5] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. 4th revised ed.* Cham: Springer, 2015.

[6] David Eisenbud. *Commutative algebra. With a view toward algebraic geometry.*, volume 150 of *Graduate Texts in Mathematics.* Berlin:Springer-Verlag, 1995.

[7] Vladimir P. Gerdt. On the relation between Pommaret and Janet bases. In *Computer algebra in scientific computing*, (Samarkand, 2000), pages 167–181. Berlin:Springer, 2000.

[8] Vladimir P. Gerdt. Involutive algorithms for computing Gröbner bases. In *Computational commutative and non-commutative algebraic geometry. Proceedings of the NATO Advanced Research Workshop, 2004*, pages 199–225. Amsterdam: IOS Press, 2005.

[9] Vladimir P. Gerdt and Yuri A. Blinkov. Involutive bases of polynomial ideals. *Math. Comput. Simul.*, 45(5-6):519–541, 1998.

[10] Marc Giusti, Klemens Hägele, Grégoire Lecerf, Joël Marchand, and Bruno Salvy. The projective Noether Maple package: Computing the dimension of a projective variety. *J. Symb. Comput.*, 30(3):291–307, 2000.

[11] Gert-Martin Greuel and Gerhard Pfister. *A Singular introduction to commutative algebra. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann. 2nd extended ed.* Berlin: Springer, 2007.

[12] Amir Hashemi. Efficient algorithms for computing Noether normalization. In *Asian Symposium on Computer Mathematics*, volume 5081 of *Lect. Notes Comput. Sci.*, pages 97–107. Berlin:Springer, 2008.

[13] Amir Hashemi. Effective computation of radical of ideals and its application to invariant theory. In *International Congress on Mathematical Software*, volume 8592 of *Lect. Notes Comput. Sci.*, pages 382–389. Springer, Berlin, Heidelberg, 2014.

[14] Amir Hashemi, Michael Schweinfurter, and Werner M. Seiler. Deterministic genericity for polynomial ideals. *J. Symb. Comput.*, 86:20–50, 2018.

[15] Heisuke Hironaka. Idealistic exponents of singularity. In *Algebraic Geometry – The Johns Hopkins Centennial Lectures*, pages 52–125. Johns Hopkins University Press, Baltimore, 1977.

[16] Maurice Janet. *Leçons sur les systèmes d'équations aux dérivées partielles.* Cahiers Scientifiques, Fascicule IV. Gauthier-Villars, Paris, 1929.

[17] Teresa Krick and Alessandro Logar. An algorithm for the computation of the radical of an ideal in the ring of polynomials. In *Applied algebra, algebraic algorithms and error-correcting codes.*, volume 539 of *Lect. Notes Comput. Sci.*, pages 195–205. Berlin:Springer-Verlag, 1991.

[18] Grégoire Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003.

[19] Alessandro Logar. A computational proof of the Noether normalization lemma. Applied algebra, algebraic algorithms and error-correcting codes. volume 357 of *Lect. Notes Comput. Sci.*, pages 259–273., 1989.

[20] David Rees. A basis theorem for polynomial modules. *Proc. Cambridge Phil. Soc.*, 52:12–16, 1956.

[21] Charles Riquier. *Les systèmes d'équations aux derivées partielles.* Gauthier-Villars, Paris, 1910.

[22] Daniel Robertz. Noether normalization guided by monomial cone decompositions. *J. Symb. Comput.*, 44(10):1359–1373, 2009.

[23] Frank-Olaf Schreyer. Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionssatz. Master's thesis, University of Hamburg, Germany, 1980.

[24] Michael Schweinfurter. *Deterministic Genericity and the Computation of Homological Invariants.* PhD thesis, Fachbereich Mathematik und Naturwissenschaften, Universität Kassel, 2016.

[25] Werner M. Seiler. A combinatorial approach to involution and δ-regularity. II: Structure analysis of polynomial modules with Pommaret bases. *Appl. Algebra Eng. Commun. Comput.*, 20(3-4):261–338, 2009.

[26] Werner M. Seiler. *Involution: The formal theory of differential equations and its applications in computer algebra*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2009.

[27] Richard P. Stanley. Hilbert functions of graded algebras. *Adv. Math.*, 28:57–83, 1978.

[28] Bernd Sturmfels and Neil White. Computing combinatorial decompositions of rings. *Combinatorica*, 11:275–293, 1991.

[29] Alexey Yu. Zharkov and Yuri A. Blinkov. Involution approach to investigating polynomial systems. *Math. Comput. Simulation*, 42(4-6):pp. 323–332, 1996.