

Noether normalization guided by monomial cone decompositions

Daniel Robertz

*Lehrstuhl B für Mathematik, RWTH Aachen University, Templergraben 64, D-52062 Aachen,
Germany*

Abstract

This paper explains the relevance of partitioning the set of standard monomials into cones for constructing a Noether normalization for an ideal in a polynomial ring. Such a decomposition of the complement of the corresponding initial ideal in the set of all monomials – also known as a Stanley decomposition – is constructed in the context of Janet bases, in order to come up with sparse coordinate changes which achieve Noether normal position for the given ideal.

Key words: Noether normalization; involutive bases; Janet bases; Stanley decompositions; sparse coordinate change

1. Introduction

Noether normalization is a very important part of commutative algebra (cf. e.g. (Eisenbud, 1995)). The “normalization lemma” is usually proved in a constructive manner, but a computationally satisfactory solution does not seem to exist. For most of the computational approaches today it is common that the application of a random change of coordinates produces very large results, which are difficult to handle afterwards.

A general algorithm for the computation of a Noether normalization was outlined by Vasconcelos (Vasconcelos, 1998, Algorithm 2.3.1, p. 36). In order to turn this algorithm effective, important details need to be filled in. The method for Noether normalization given in Section 4 of the present paper can be understood as a specialization of this algorithm. In particular, the problem of deciding whether an ideal contains a monic polynomial in a given variable is addressed without computing the intersection of the ideal with a subring, and a way to choose a sparse coordinate change is explained.

Along these lines, a (probabilistic) algorithm was presented by A. Logar in (Logar, 1989), which comes up with a relatively sparse coordinate transformation that puts a

* This research was partly supported by a scholarship of the Deutsche Forschungsgemeinschaft.
Email address: daniel@momo.math.rwth-aachen.de (Daniel Robertz).

prime ideal into Noether normal position (and, after small modifications, a non-prime ideal as well). However, this algorithm is based on intersecting with a subring and makes use of very expensive Gröbner basis computations w.r.t. the lexicographical term ordering. In comparison to Logar’s suggestion, the approach described in Section 4 computes Janet bases only with respect to the degree-reverse lexicographical ordering and further narrows down the set of variables which should be altered by a coordinate change.

Similarly, in (Greuel and Pfister, 2008) an algorithm is described which applies a random triangular linear coordinate change and again uses the lexicographical term ordering (ibid., Algorithm 3.4.5). Examples show that the method of the present paper seems to be more efficient and gives sparser results than implementations in SINGULAR (Greuel et al., 2005) (cf. Example 15 and Section 6). The present paper gives guidance of how to replace the above mentioned random coordinate change by a more deterministic one. The proposed algorithm is still probabilistic, in the sense that the coefficients of the coordinate change need to be chosen outside an algebraic hypersurface, but the number of non-zero coefficients is drastically reduced, and the obstructions for the algorithm to achieve progress are clearly identified in Section 5.

Furthermore, an algorithm was presented in the same spirit in the appendix to (Bermejo and Gimenez, 2006), where again a random triangular linear coordinate transformation without further qualification is applied.

A different approach to sparse Noether normalization was discussed in (Eisenbud and Sturmfels, 1994) resulting in the problem of finding a non-root of the Chow form of the projective variety under consideration. As the authors remark, a complete expansion of the Chow form would be too big in practice.

A referee directed the author’s attention to the article (Hashemi, 2008), where coefficient growth is suggested to be counteracted by modular computations and an incremental strategy for random linear coordinate changes is proposed. However, no explicit method for determining non-zero entries in the transformation matrix is given.

The approach in the present paper uses Janet bases, and the Stanley decompositions (Sturmfels, 1990) they define, to detect sparse coordinate transformations. In principle, the method can be carried out with involutive bases defined with respect to other Noetherian involutive divisions as well, but we were able to build on an existing implementation for the Janet division, and that led to good results. In this context of involutive bases, a connection of Noether normalization to Pommaret bases was derived in (Seiler, 2007, part II, Section 4). However, for a given ideal no (finite) Pommaret basis may exist in the chosen coordinates (cf. also (Hausdorf and Seiler, 2002)). It is a problem similar to the one addressed below to find suitable coordinate transformations such that the ideal has a Pommaret basis in the new coordinates. The fact that for every ideal a Janet basis exists in any system of coordinates allows to treat a substantially larger class of examples with sparse transformations, cf. Example 15 below, where the proposed coordinate changes do not lead to Pommaret bases. As a referee pointed out, a Rees decomposition (Sturmfels and White, 1991) is a particular kind of Stanley decomposition to which the method of Section 4 applies. However, Example 15 again shows that a weaker notion of Stanley decomposition suffices.

After recalling a certain type of Stanley decomposition from old work by M. Janet (Janet, 1929) in Section 2, the definition of Janet basis is given in Section 3 using this concept. A lemma is proven that decides the existence of a monic polynomial in a given

variable in an ideal in the context of Janet bases. In Section 4 the main algorithm for Noether normalization which uses monomial cone decompositions is described. Section 5 completes the proof of the algorithm in Section 4 with an argument that was too technical to be presented in the previous section. The last section records data of comparisons of some already available implementations of Noether normalization algorithms with the one implemented by the author.

2. Monomial Cone Decompositions

The beginning of this section fixes the notation for the rest of the paper. Afterwards, we recall the notion of monomial cone decomposition for a multiple closed set of monomials and its complement (Plesken and Robertz, 2005), and we outline one way of constructing such decompositions.

Let $R := K[x_1, \dots, x_n]$ be a commutative polynomial algebra with standard grading, where K is a field of arbitrary characteristic. If $L \subseteq R$, then $\langle L \rangle$ is the ideal of R generated by L . For a finite subset $y = \{y_1, \dots, y_r\} \subseteq R$ we denote by

$$\text{Mon}(y) := \left\{ \prod_{i=1}^r y_i^{\alpha_i} \mid \alpha \in (\mathbb{Z}_{\geq 0})^r \right\}$$

the commutative monoid of monomials in y_1, \dots, y_r , and in particular we set $\text{Mon}(R) := \text{Mon}(\{x_1, \dots, x_n\})$.

A term ordering $>$ on $\text{Mon}(R)$ (or on R , for short, if the set of variables $\{x_1, \dots, x_n\}$ is understood) is a total ordering on $\text{Mon}(R)$ which is a well-ordering and compatible with the semigroup structure on $\text{Mon}(R)$.

If a term ordering $>$ on $\text{Mon}(R)$ is fixed, then for each non-zero $p \in R$, $\text{lm}(p)$ denotes the $>$ -greatest monomial occurring in p (i.e. with non-zero coefficient). For a subset $S \subseteq R$ we set $\text{lm}(S) := \{\text{lm}(p) \mid 0 \neq p \in S\}$.

The idea of partitioning certain sets of monomials into cones can at least be traced back to Ch. Méray (Méray, 1880), who dealt with the formal theory of partial differential equations (cf. also the works of his successors Ch. Riquier (Riquier, 1910) and M. Janet (Janet, 1929)). We use it in the context of what is now called Janet basis.

Definition 1. A set $S \subseteq \text{Mon}(R)$ is said to be *Mon}(R)-multiple closed*, if

$$ms \in S \quad \text{for all } m \in \text{Mon}(R), \quad s \in S.$$

Every set $G \subseteq \text{Mon}(R)$ satisfying

$$\text{Mon}(R)G = \{mg \mid m \in \text{Mon}(R), g \in G\} = S$$

is called a *generating set* for S .

The following lemma can be seen as a special case of Hilbert's basis theorem (cf. also (Janet, 1929)).

Lemma 2. *Every Mon}(R)-multiple closed set has a finite generating set; every ascending sequence of Mon}(R)-multiple closed sets becomes stationary.*

Moreover, every $\text{Mon}(R)$ -multiple closed set has a unique minimal generating set, which is obtained from any generating set G by removing all elements which have a proper divisor in G .

We are going to partition multiple closed sets (and, more importantly, their complements in $\text{Mon}(R)$) into cones of monomials, one instrumental fact being that the latter are again $\text{Mon}(R')$ -multiple closed sets with $R' = K[\mu]$ for some $\mu \subseteq \{x_1, \dots, x_n\}$.

Definition 3. A set $C \subseteq \text{Mon}(R)$ is called a (*monomial*) *cone* if there exist $m \in C$ and $\mu \subseteq \{x_1, \dots, x_n\}$ such that $\text{Mon}(\mu)m = C$. The uniquely determined monomial m is called the *vertex* of the cone C , and the elements of μ (of $\bar{\mu} := \{x_1, \dots, x_n\} \setminus \mu$) are called the *multiplicative* (resp. *non-multiplicative*) *variables* for C . We often also refer to such a cone C by giving the pair (m, μ) .

Definition 4. Let $S \subseteq \text{Mon}(R)$. A (*monomial*) *cone decomposition* of S is a finite set $\{(m_1, \mu_1), \dots, (m_r, \mu_r)\}$, where $m_i \in \text{Mon}(R)$, $\mu_i \subseteq \{x_1, \dots, x_n\}$, and such that the cones $C_i := \text{Mon}(\mu_i)m_i$ satisfy

$$\bigcup_{i=1}^r C_i = S \quad \text{and} \quad C_i \cap C_j = \emptyset \quad \text{for all} \quad i \neq j.$$

The next algorithm constructs a particular cone decomposition of a $\text{Mon}(R)$ -multiple closed set S , which goes back to Maurice Janet (Janet, 1929).

Algorithm 1 (Decompose).

Input: A $\text{Mon}(\eta)$ -multiple closed set $S \subseteq \text{Mon}(R)$, where $\emptyset \neq \eta \subseteq \{x_1, \dots, x_n\}$

Output: A cone decomposition of S

Algorithm:

- 1: determine the minimal generating set G for S
- 2: **if** $|G| \leq 1$ **or** $|\eta| = 1$ **then**
- 3: **return** $\{(m, \eta) \mid m \in G\}$
- 4: **else**
- 5: let y be the first variable in η in the chosen enumeration
- 6: $d := \max \{\deg_y(g) \mid g \in G\}$
- 7: for $i = 0, \dots, d$, recursively decompose the $\text{Mon}(\eta \setminus \{y\})$ -multiple closed set generated by $\bigcup_{j=0}^i \{y^{i-j}g \mid g \in G, \deg_y(g) = j\}$ and get $C^{(i)} = \{(m_1^{(i)}, \mu_1^{(i)}), \dots, (m_{r_i}^{(i)}, \mu_{r_i}^{(i)})\}$
- 8: for $j = 1, \dots, r_d$, replace $\mu_j^{(d)}$ by $\mu_j^{(d)} \cup \{y\}$
- 9: **return** $\bigcup_{i=0}^d C^{(i)}$
- 10: **fi**

For a proof of correctness of the previous algorithm we refer to (Robertz, 2006).

Example 5. Let $S \subset \text{Mon}(K[x_1, x_2, x_3])$ be generated by $\{x_1x_2, x_1^3x_3\}$ and define $\eta = \{x_1, x_2, x_3\}$. Then the previous algorithm sets $d = 3$ and is applied recursively to $(\emptyset, \{x_2, x_3\})$, $(\{x_1x_2\}, \{x_2, x_3\})$, $(\{x_1^2x_2\}, \{x_2, x_3\})$, and $(\{x_1^3x_2, x_1^3x_3\}, \{x_2, x_3\})$, where

the first component in each pair is a generating set for a $\text{Mon}(\{x_2, x_3\})$ -multiple closed set. Only the last recursive run starts new recursions; the arguments are $(\{x_1^3 x_3\}, \{x_3\})$, $(\{x_1^3 x_2\}, \{x_3\})$. The final result is $\{(x_1^3 x_2, \{x_1, x_2, x_3\}), (x_1^3 x_3, \{x_1, x_3\}), (x_1^2 x_2, \{x_2, x_3\}), (x_1 x_2, \{x_2, x_3\})\}$.

Next we give a similar algorithm which produces a cone decomposition for the complement of a $\text{Mon}(R)$ -multiple closed set S in $\text{Mon}(R)$. Decompositions produced by this algorithm will be used in the following sections in case $S = \text{lm}(I)$ for an ideal I of R , i.e. to get a partition of the set of “standard monomials”. In this case we also call such a partition a cone decomposition of R/I .

Algorithm 2 (DecomposeComplement).

Input: A $\text{Mon}(\eta)$ -multiple closed set $S \subseteq \text{Mon}(R)$, where $\eta \subseteq \{x_1, \dots, x_n\}$, and a monomial $v \in \text{Mon}(R)$ such that $S \subseteq \text{Mon}(\eta)v$

Output: A cone decomposition of $\text{Mon}(\eta)v \setminus S$

Algorithm:

- 1: determine the minimal generating set G for S
- 2: **if** $G = \emptyset$ **then** *// the complement equals $\text{Mon}(\eta)v$, which is a cone*
- 3: **return** $\{(v, \eta)\}$
- 4: **elif** $|\eta| = 1$ **then** *// the complement is a finite set of monomials*
- 5: **return** $\{(mv, \emptyset) \mid m \in \text{Mon}(\eta), mv \notin S\}$
- 6: **else**
- 7: let y be the first variable in η in the chosen enumeration
- 8: $d := \max \{\deg_y(g) \mid g \in G\}$
- 9: for $i = 0, \dots, d$, recursively decompose the complement of the $\text{Mon}(\eta \setminus \{y\})$ -multiple closed set generated by $\bigcup_{j=0}^i \{y^{i-j} g \mid g \in G, \deg_y(g) = j\}$ by using $y^i v$ instead of v and get $C^{(i)} = \{(m_1^{(i)}, \mu_1^{(i)}), \dots, (m_{r_i}^{(i)}, \mu_{r_i}^{(i)})\}$
- 10: for $j = 1, \dots, r_d$, replace $\mu_j^{(d)}$ by $\mu_j^{(d)} \cup \{y\}$
- 11: **return** $\bigcup_{i=0}^d C^{(i)}$
- 12: **fi**

As before, for a proof of correctness of the previous algorithm we refer to (Robertz, 2006).

Example 6. Applying Algorithm 2 to the same data as in Example 5 and $v = 1$ leads again to $d = 3$ and the same recursive calls with additional arguments $v = 1$, x_1 , x_1^2 , resp. x_1^3 . After additional recursive runs, these terminate with $\{(1, \{x_2, x_3\})\}$, $\{(x_1, \{x_3\})\}$, $\{(x_1^2, \{x_3\})\}$, resp. $\{(x_1^3, \emptyset)\}$. As final result we obtain: $\{(1, \{x_2, x_3\}), (x_1, \{x_3\}), (x_1^2, \{x_3\}), (x_1^3, \{x_1\})\}$.

Definition 7. We call the cone decomposition of S (of $\text{Mon}(R) \setminus S$) which is constructed by Algorithm 1 (resp. 2) the *Janet decomposition* of S (resp. of $\text{Mon}(R) \setminus S$, or of R/I if $S = \text{lm}(I)$ for an ideal I of R).

3. Janet Bases

In this section we give the basic definitions for Janet bases and their most important properties, and we derive a lemma which is used for Noether normalization in the next section.

Janet bases are named after Maurice Janet (Janet, 1929) who developed this technique for the structural analysis of systems of (linear) partial differential equations (cf. also (Pommaret, 1994), (Gerdt, 2005), (Plesken and Robertz, 2005)). For the role played by Janet bases in the solution of ordinary differential equations, cf. e.g. (Schwarz, 2008).

Definition 8. A finite set $J = \{(m_1, \mu_1), \dots, (m_r, \mu_r)\}$, where $m_i \in \text{Mon}(R)$ and $\mu_i \subseteq \{x_1, \dots, x_n\}$, is a *Janet basis* (for the monomial ideal $\langle m_1, \dots, m_r \rangle$ in R) if it is the Janet decomposition of $\langle m_1, \dots, m_r \rangle$ in the sense of Definition 7, for some ordering of the variables.

In what follows we fix a term ordering $>$ on $\text{Mon}(R)$.

Definition 9. A finite set $J = \{(p_1, \mu_1), \dots, (p_r, \mu_r)\}$, where $0 \neq p_i \in R$ and $\mu_i \subseteq \{x_1, \dots, x_n\}$, is a *Janet basis* w.r.t. $>$ (for the ideal $\langle p_1, \dots, p_r \rangle$ in R) if $\{(\text{lm}(p_1), \mu_1), \dots, (\text{lm}(p_r), \mu_r)\}$ is a Janet basis for $\text{lm}(\langle p_1, \dots, p_r \rangle)$. In this case, the set $\{p_1, \dots, p_r\}$ is often referred to as a Janet basis for $\langle p_1, \dots, p_r \rangle$ as well, and we also write $\langle J \rangle$ for $\langle p_1, \dots, p_r \rangle$ and $\text{lm}(J)$ for $\{\text{lm}(p_1), \dots, \text{lm}(p_r)\}$.

More generally, an *involutive basis* is defined if the reference to Janet decomposition in the previous definitions is replaced by a possibly different way of partitioning multiple closed sets of monomials into cones, as constituted by an *involutive division*, studied e.g. by Gerdt, Blinkov (Gerdt and Blinkov, 1998), Apel (Apel, 1998), Seiler (Seiler, 2007) and others; cf. (Gerdt, 2005) for a survey. As another particular case of involutive bases, *Pommaret bases* are investigated e.g. in (Seiler, 2007).

For the existence of Janet bases, their algorithmic construction, and further applications which are not mentioned in what follows, we refer to (Gerdt and Blinkov, 1998), (Gerdt, 2005), (Plesken and Robertz, 2005), (Seiler, 2007), (Robertz, 2007), and the references therein.

Remark 10. If $J = \{(p_1, \mu_1), \dots, (p_s, \mu_s)\}$ is a Janet basis for the ideal $\langle J \rangle$ in R , then every $f \in R$ can be written *uniquely* in the form

$$f = r + \sum_{i=1}^s c_i \cdot p_i \tag{1}$$

with $c_i \in K[\mu_i]$ for each i , and $r \in R$ such that no monomial occurring with non-zero coefficient in r lies in any cone with vertex $\text{lm}(p)$ for some polynomial p in the Janet basis J , i.e., exactly the polynomials in $\langle J \rangle$ are reduced to zero by subtracting suitable multiples of the polynomials p_i with coefficients that are polynomials in the multiplicative variables for $\text{lm}(p_i)$, and the representation (1) of f is unique.

In particular, we have the equality $\langle \text{lm}(J) \rangle = \text{lm}(\langle J \rangle)$, which is used as a criterion for the termination of algorithms constructing Janet bases, or, more generally, involutive

bases, and which is also well known from Buchberger's algorithm computing Gröbner bases (Buchberger, 2006). In fact, every involutive basis is also a Gröbner basis, but the former comes with a lot more combinatorial information about the ideal.

Before presenting a small example we summarize the most important features of monomial cone decompositions in this context.

Remark 11. (1) By definition, every Janet basis for an ideal I comes with a cone decomposition of $\text{lm}(I)$ as well as with one of I . Moreover, since the procedures that construct the Janet decompositions of $\text{lm}(I)$ and of $\text{Mon}(R) \setminus \text{lm}(I)$ deal with the same minimal generating set G for $\text{lm}(I)$, cf. Section 2, we can think of a Janet basis as providing a cone decomposition of $\text{Mon}(R) \setminus \text{lm}(I)$ (and R/I) at the same time.

- (2) (Plesken and Robertz, 2005) A cone decomposition $\{ (m_1, \mu_1), \dots, (m_r, \mu_r) \}$ of R/I allows to enumerate a K -vector space basis of R/I , which is conveniently encoded in the *generalized Hilbert series*

$$\sum_{i=1}^r m_i \prod_{x \in \mu_i} \frac{1}{1-x} \quad (2)$$

and yields the Hilbert series $\sum_{k \geq 0} \dim_K(R/I)_k \cdot t^k$ for a standard graded ideal I via the substitution $x_i = t$, $i = 1, \dots, n$, into (2).

- (3) The maximum of the dimensions $|\mu_i|$ of cones in a decomposition of R/I equals the Krull dimension of R/I (cf. e.g. (Stanley, 1996, I.5) in combination with the previous remark (2), or (Sturmfels and White, 1991)).

Example 12. Let $R = K[x, y]$ with the degree-reverse lexicographical ordering satisfying $x > y$ (cf. also the beginning of Section 4). Let the ideal I of R be generated by $g_1 = x^2 - y$ and $g_2 = xy - y$. Then we have $\text{lm}(g_1) = x^2$, $\text{lm}(g_2) = xy$ and the method of Section 2 gives the following cone decomposition of the $\text{Mon}(R)$ -multiple closed set generated by x^2 and xy :

$$\{ (x^2, \{x, y\}), (xy, \{y\}) \}.$$

This result indicates that we need to check whether $f := x \cdot g_2 \in I$ has a representation of the form (1) with $p_i = g_i$. The monomials appearing in $f = x^2y - xy$ lie in the cones $(x^2, \{x, y\})$ resp. $(xy, \{y\})$. Reduction gives $g_3 := y^2 - y \in I$, which does not have such a representation yet. So, we include g_3 in our list of generators, and for this example, we already arrive at the (minimal) Janet basis $\{ (g_1, \{x, y\}), (g_2, \{y\}), (g_3, \{y\}) \}$ for I .

The following lemma will be used in the next section to detect effective coordinate changes which transform a given ideal into Noether normal position.

Lemma 13. *Let I be an ideal of $R = K[x_1, \dots, x_n]$. Let J be a Janet basis for I and $\{ (m_i, \mu_i) \mid i = 1, \dots, r \}$ a cone decomposition of R/I , where $m_i \in \text{Mon}(R)$, $i = 1, \dots, r$. Set $\nu := \bigcup_{i=1}^r \mu_i$. Then for every $x \in \{x_1, \dots, x_n\}$ we have:*

$$x \notin \nu \iff \exists p \in J : \text{lm}(p) = x^e \text{ for some } e \in \mathbb{Z}_{\geq 0}.$$

(In case $I = R$, the statement holds for $\nu = \emptyset$.)

Proof. “ \Leftarrow ”: If $p \in J$ exists with $\text{lm}(p) = x^e$ for some $e \geq 0$, then $x^e \cdot m \in \text{lm}(I)$ for all $m \in \text{Mon}(R)$. In particular, $x^e \cdot m_i \in \text{lm}(I)$ for all $i = 1, \dots, r$. Therefore, $x \notin \mu_i$ for all $i = 1, \dots, r$.

“ \Rightarrow ”: If $x \notin \nu$, then $x \notin \mu_i$ for all $i = 1, \dots, r$. By definition, a cone decomposition consists of finitely many cones. Hence, there exists $j \in \mathbb{Z}_{\geq 0}$ such that $x^j \notin \text{Mon}(R) \setminus \text{lm}(I)$, i.e. $x^j \in \text{lm}(I)$. Since $\text{lm}(J)$ is a Janet basis for $\text{lm}(I)$, there exists $p \in J$ such that $\text{lm}(p)$ divides x^j , i.e. $\text{lm}(p) = x^e$ for some $0 \leq e \leq j$. \square

4. Noether Normalization with Janet Bases

Let $R = K[x_1, \dots, x_n]$, where K is an infinite¹ field. In what follows, every automorphism of R maps 1 to 1. We fix once and for all the degree-reverse lexicographical ordering² on $\text{Mon}(R)$ with $x_1 > \dots > x_n$:

$$x^a > x^b \quad : \iff \begin{cases} \sum_{i=1}^n a_i > \sum_{i=1}^n b_i \text{ or} \\ \sum_{i=1}^n a_i = \sum_{i=1}^n b_i \text{ and } b_j > a_j \\ \text{for } j = \max\{1 \leq i \leq n \mid a_i \neq b_i\}. \end{cases}$$

In the following recursive algorithm the given polynomial ring R is not changed, but the given ideal I of R is possibly transformed under automorphisms of R in order to arrive at a Noether normalization of R/I .

Algorithm 3 (NoetherNormalization).

Input: A finite set $L \subset R = K[x_1, \dots, x_n]$ generating a non-trivial ideal $I = \langle L \rangle$ of R

Output: A ring automorphism $\phi : R \rightarrow R$ and a subset $P \subseteq \{1, \dots, n\}$ such that $y := \{\phi(x_i) + \phi(I) \mid i \in P\} \subset R/\phi(I)$ is algebraically independent over K and $R/\phi(I)$ is integral over $K[y]$

Algorithm:

- 1: compute Janet basis J for $I = \langle L \rangle$, and monomial cone decomposition $C = \{(m_i, \mu_i) \mid i = 1, \dots, r\}$ of R/I ; set $\nu := \bigcup_{i=1}^r \mu_i$; $d := \max_{i=1, \dots, r} |\mu_i|$
- 2: **if** $|\nu| = d$ **then** // total number of mult. variables equals Krull dimension
- 3: **return** $(\text{id}_R, \{i \mid x_i \in \nu\})$
- 4: **else**
- 5: denote by z the $>$ -greatest variable in ν

¹ See the proof of Algorithm 3 for a comment about necessary changes for finite fields.

² We have chosen this term ordering because it is used most often for the computation of Gröbner and Janet bases. However, Algorithm 3 also works for the degree lexicographical ordering, and the corresponding arguments are even simpler in that case.

- 6: choose $p \in J$ with $\text{lm}(p) \in \text{Mon}(\nu)$
- 7: define automorphism

$$\psi : R \rightarrow R : x_i \mapsto \begin{cases} x_i, & \text{if } x_i = z \text{ or } x_i \notin \text{lm}(p), \\ x_i - \alpha_i \cdot z, & \text{otherwise,} \end{cases} \quad i = 1, \dots, n, \quad (3)$$

where $\alpha_i \in K$ are chosen s.t. $\psi(p)$ contains the monomial z^e , $e = \deg(\psi(p))$

- 8: $(\phi, P) := \text{NoetherNormalization}(\psi(J))$
- 9: **return** $(\phi \circ \psi, P)$
- 10: **fi**

Proof. We need to show that, if $|\nu| = d$, then a Noether normalization of R/I is determined by the cone decomposition C , and otherwise the algorithm arrives at this situation in finitely many steps using the coordinate transformations defined in (3).

- (1) Let us assume that $|\nu| = d$. Without loss of generality, let (m_1, μ_1) be a cone in C with $|\mu_1| = d$, i.e. $\mu_1 = \nu$. We have $m \cdot m_1 \notin \text{lm}(I)$ for all $m \in \text{Mon}(\nu)$. Let $t \in \text{Mon}(R)$ be a divisor of m_1 . Then we have $m \cdot t \notin \text{lm}(I)$ for all $m \in \text{Mon}(\nu)$, because otherwise $m \cdot t \in \text{lm}(I)$ implies $m \cdot m_1 = \frac{m_1}{t} \cdot m \cdot t \in \text{lm}(I)$, a contradiction. In particular, $m \cdot 1 \notin \text{lm}(I)$ for all $m \in \text{Mon}(\nu)$. Hence, $y := \{x + I \mid x \in \nu\} \subset R/I$ is algebraically independent over K , since a non-trivial polynomial relation among the elements of y would yield a non-zero polynomial $p \in I \cap K[\nu]$, which would necessarily give $\text{lm}(p) \in \text{lm}(I) \cap K[\nu]$.

Now it is clear that $K[y] \subseteq R/I$. Let $\bar{\nu} := \{x_1, \dots, x_n\} \setminus \nu$, which has cardinality $n - d$. For each $x \in \bar{\nu}$ there exists $p \in J$ with $\text{lm}(p) = x^e$ for some $e \geq 0$ by Lemma 13. Since the term ordering $>$ respects multiplication of monomials and is a well-ordering, no monomial in p which is different from x^e is divisible by x^e . Hence, p is a monic polynomial in x whose coefficients are polynomials in the variables $\{x_1, \dots, x_n\} \setminus \{x\}$. As y is algebraically independent over K , we can consider the ideal \bar{I} generated by I in $K(\nu)[\bar{\nu}]$. By the previous arguments, this ideal is zero-dimensional. A Janet basis for this ideal with respect to a lexicographic term ordering therefore yields integral relations for $x_{i_j} + I$ over $K[y][x_{i_1} + I] \dots [x_{i_{j-1}} + I]$, $j = 1, \dots, n - d$, in some order $\{x_{i_1}, \dots, x_{i_{n-d}}\} = \bar{\nu}$. This shows that $K[y] \subseteq R/I$ is an integral extension.

Note that it is not necessary to perform the last construction if the tower of extensions $K[y] \subseteq \dots \subseteq K[y][x_{i_1} + I] \dots [x_{i_{n-d}} + I]$ is not needed.

- (2) Let us assume now that $|\nu| > d$. Since C consists of finitely many cones with at most d multiplicative variables, we have $\text{Mon}(\nu) \not\subseteq \text{Mon}(R) \setminus \text{lm}(I)$. Hence, there exists $q \in I$ with $\text{lm}(q) \in \text{lm}(I) \cap \text{Mon}(\nu)$. Now $\text{lm}(q)$ has a (unique) Janet divisor $p \in J$ with $\text{lm}(p) \in \text{Mon}(\nu)$, which shows that p in step 6 exists. By Lemma 13, $\text{lm}(p)$ is not a power of z .

The parameters $\alpha_i \in K$ in the definition of the coordinate transformation (3) can be chosen as point in a Zariski open set in affine space (defined as the complement of the set of values for which the coefficient of z^e in $\psi(p)$ cancels), which can be seen to be non-empty and therefore dense by inspection of (3) and because K is assumed

to be infinite. For a suggestion of how to attain a sparse coordinate transformation, cf. Remark 14 (3).

If K is not large enough, then we might need to replace $x_i \mapsto x_i + \alpha_i \cdot z$ by $x_i \mapsto x_i + \alpha_i \cdot z^\beta$ for some $\beta > 1$ for at least one i . It is well known that it is always possible to find such parameters so that the resulting transformation meets the requirement, see (Nagata, 1962, p. 44) or (Vasconcelos, 1998, A.5). However, we do not analyze this case in detail, but assume again in what follows that ψ respects the standard grading of R .

In order to ensure progress of the algorithm (i.e. termination in finitely many steps), another “open condition” needs to be imposed on the α_i . Let J' be the Janet basis computed in step 1 by the recursive call of the algorithm in step 8. The intention of defining ψ as in (3) is that the number of polynomials in J' whose leading monomial is a power of a variable, is greater than the corresponding number in J . Lemma 13 then implies that $|\nu'| < |\nu|$, where ν' is defined in step 1 of the recursive run, and since $|\nu|$ is bounded below by the Krull dimension d (cf. Remark 11 (3)), termination of the algorithm then follows.

Not every admissible coordinate transformation chosen in (3) defined by parameters α_i which are allowed up to this point of the proof, leads to the intended increase in the number of leading monomials of J which are univariate powers. This can only fail³ if $\text{lm}(\psi(p)) \neq z^e$ or if the leading monomial of another polynomial in J that is a power of another variable changes to a proper multivariate monomial⁴. Only these two cases can possibly prevent the intended progress, because, in general, every power of a variable which already occurs as leading monomial in a generating set G for an ideal will be multiple of a leading monomial of a Janet basis element, as $\text{lm}(G) \subseteq \text{lm}(\langle G \rangle)$, so a (possibly smaller) power of the same variable occurs as leading monomial in the Janet basis.

The case $\text{lm}(\psi(p)) \neq z^e$ is harmless: There nevertheless exists a non-zero element q in $\langle \psi(J) \rangle$ whose leading monomial is a power of z for all choices of the α_i that satisfy the condition above and lie outside a hypersurface defined in Proposition 17 in the more detailed discussion in Section 5. In fact, the dense set of admissible parameters α_i can be taken to be the complement of that hypersurface. As q is reduced to zero w.r.t. the Janet basis for $\langle \psi(J) \rangle$, there exists a polynomial in that Janet basis whose leading monomial is a power of z .

As for the second possible obstruction to progress, a change of a leading monomial y^m to a proper multivariate monomial, where $y \in \{x_1, \dots, x_n\}$, cannot happen if $y > z$, because ψ fixes y and respects the grading. Since z is chosen to be the $>$ -greatest variable in ν , after the application of j coordinate transformations like ψ , there exist at least polynomials p_1, \dots, p_j in the most recent Janet basis with $\text{lm}(p_i) \in K[x_i]$, $i = 1, \dots, j$. \square

³ Let $>$ be the degree-reverse lexicographical ordering on $R = K[w, x, y, z]$ with $w > x > y > z$. A homogeneous example is $p = y^2z + xz^2$, which is transformed under $\psi_1 : R \rightarrow R$, mapping z to $z + y$ and fixing the other variables, to a polynomial containing y^3 , but with leading monomial xy^2 . An example with non-linear change of coordinates is $p = x^2yz + wy^2$, which is transformed under $\psi_2 : R \rightarrow R$, mapping y to $y + x^2$, z to $z + x$, and fixing the other variables, to a polynomial containing x^5 , but with leading monomial wx^4 .

⁴ For an example for this phenomenon, cf. Example 16.

- Remark 14.** (1) If L generates a homogeneous ideal of R , defined over an infinite field, then the ideal in Noether position $\phi(\langle L \rangle)$ is homogeneous as well.
- (2) Using $\psi(J)$ as argument for the recursive call of Algorithm 3 rather than $\psi(L)$ results in a more efficient procedure because the Janet basis in the recursive run need not be constructed from scratch.
- (3) There are still degrees of freedom in the choice of p in step 6. An implementation of the above algorithm by the author chooses $p \in J$ such that $\text{lm}(p)$ involves the minimal number of variables and is maximal w.r.t. $>$ among these candidates. Preferably one should choose $p \in J$ such that $\text{lm}(p)$ is already divisible by a high power of z .
- (4) Step 7 could be modified to define the automorphism ψ as well as a new term ordering $\tilde{>}$ on R ensuring that $\text{lm}_{\tilde{>}}(\psi(p))$ is a power of z . Another improvement could be a permutation of the variables such that the variables in ν are smaller w.r.t. $>$ than those in $\{x_1, \dots, x_n\} \setminus \nu$, i.e. those for which a power already occurs as leading monomial of a Janet basis element (cf. also the end of the previous proof).
- (5) Experiments show that often $\alpha_i = \pm 1$ already lead to good results, which allows to keep coefficients small in the resulting Janet basis (cf. also Section 6).
- (6) The knowledge of the Hilbert function of R/I from step 1 of the algorithm should be of help in recursive runs.

Next we discuss an example of moderate size.

Example 15. Let $R = \mathbb{Q}[w, x, y, z]$ and choose the degree-reverse lexicographical ordering on R with $w > x > y > z$. Let the ideal I of R be generated by $L := \{y^2z - wxy^2, xyz - wz^2, y^2z - wx^2yz\}$. It is not radical and has five minimal associated primes of dimensions 1, 2, 2, 2, 2 respectively, and one embedded associated prime of dimension 1. All the following computations were done in MAPLE in a couple of seconds using the package INVOLUTIVE (Blinkov et al., 2003).

The cone decomposition for R/I , determined as in Section 2, consists of cones whose sets of multiplicative variables μ_i are among the following ones⁵:

$$\emptyset, \{w\}, \{x\}, \{y\}, \{z\}, \{w, x\}, \{w, y\}, \{x, y\}, \{x, z\}.$$

The Krull dimension d of R/I equals 2. We have $\nu_1 := \bigcup \mu_i = \{w, x, y, z\}$, and so $|\nu_1| = 4 > d$. In order to keep the coordinate transformation sparse, it is advisable to choose $p_1 = w^2z^4 - wy^2z^2 \in J$, whose leading monomial $\text{lm}(p_1) = w^2z^4$ involves only two variables. We choose the automorphism $\psi_1 : R \rightarrow R$ which maps z to $z - w$ and fixes all other variables.

The cone decomposition for $R/\psi_1(I)$ has sets of multiplicative variables among the following ones:

$$\emptyset, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}.$$

⁵ Using the package INVOLUTIVE, the generalized Hilbert series, cf. Remark 11 (2), can be obtained with the command FACTORMODULEBASIS, after applying INVOLUTIVEBASIS to L .

We have $\nu_2 := \{x, y, z\}$, so still $|\nu_2| = 3 > d$. Now we choose $p_2 = xy^2z^2 - w^2y^2 + wy^3 + 3wy^2z - y^3z - 2y^2z^2 \in J_2$ with $\text{lm}(p_2) = xy^2z^2$, and the automorphism $\psi_2 : R \rightarrow R$ mapping y to $y - x$, z to $z - x$, and fixing w and x .

Now the cone decomposition for $R/(\psi_2 \circ \psi_1)(I)$ consists of cones having sets of multiplicative variables either \emptyset , or $\{y\}$, or $\{z\}$, or $\{y, z\}$. So we have $\nu_3 := \{y, z\}$ and $|\nu_3| = d$, and we are done. Finally, $\psi_2 \circ \psi_1$ is defined by

$$w \mapsto w, \quad x \mapsto x, \quad y \mapsto y - x, \quad z \mapsto z - x - w.$$

Note that neither of the Janet bases J_1, J_2, J_3 is a Pommaret basis, i.e. the associated primes of the initial ideals $\text{lm}(\langle J_i \rangle) = \langle \text{lm}(J_i) \rangle$ are not nested in the sense of Bermejo and Gimenez (cf. (Bermejo and Gimenez, 2006), (Seiler, 2007, part II, Section 4), and (Caviglia and Sbarra, 2005)). The corresponding Stanley decompositions of the sets of standard monomials do not form Rees decompositions either.

The maximum number of summands of a polynomial in J_3 is 102. The coefficient in J_3 of largest absolute value equals 40.

A typical coordinate transformation given by SINGULAR's (Greuel et al., 2005) (randomized) command `noetherNormal` is defined by

$$w \mapsto w, \quad x \mapsto 10w + x, \quad y \mapsto 6w + 10x + y, \quad z \mapsto 8w + 4x + 3y + z,$$

which in this case results in a Gröbner basis of the transformed ideal with coefficient of largest absolute value of more than 30 decimal digits and maximum number of summands 123.

For a more systematic comparison of some existing implementations of Noether normalization algorithms, see Section 6.

The following example of a homogeneous ideal shows that a clever choice of the parameters α_i in Algorithm 3 can increase its efficiency.

Example 16. Let $R = \mathbb{Q}[x, y, z]$ and choose the degree-reverse lexicographical ordering on R with $x > y > z$. Let the ideal I of R be generated by $L := \{x^2yz - y^4, xy^2z - z^4\}$. It is not radical and has three associated primes of dimension 1.

The cone decomposition for R/I , determined as in Section 2, consists of cones having sets of multiplicative variables either \emptyset , or $\{x\}$, or $\{z\}$. The Krull dimension d of R/I equals 1, and we have $\nu = \{x, z\}$.

The Janet basis J contains an element $y^4 - x^2yz$ whose leading monomial is a power of y . The only element $p \in J$ whose leading monomial does not involve y is $p = x^3z^5 - yz^7$ with $\text{lm}(p) = x^3z^5$. After applying the automorphism $\psi_1 : R \rightarrow R$ which maps z to $z + x$ and fixes x and y , we get a Janet basis containing an element with leading monomial x^4 , but no element whose leading monomial is a power of y . Accordingly, in the recursive run of the algorithm we have $\nu' = \{y, z\}$, and a further coordinate change which maps z to $z + y$ achieves Noether normal position. However, if we had chosen $\psi'_1 : R \rightarrow R$ mapping z to $z - x$ instead of $z + x$, the new Janet basis would have contained elements with leading monomials x^4 and y^7 . In both cases, p is transformed to a polynomial in which x^8 occurs with non-zero coefficient, but the algorithm finishes earlier with the second choice. A deterministic way of finding the better choice needs to examine more than one element $p \in J$.

5. A condition on the coordinate transformation

In this section we complete the proof of Algorithm 3. This proof depends on the following technical argument which ensures progress of the algorithm whenever the coordinate transformation ψ is defined using values $\alpha_i \in K$ chosen in a Zariski open set defined in the following proposition.

In what follows, we denote by $\text{res}(p, q, x)$ the resultant of two polynomials p and q w.r.t. a variable x .

In the context of Algorithm 3, set $S := K(c_1, \dots, c_n)[x_1, \dots, x_n]$ with n new indeterminates c_i , extend the degree-reverse lexicographical ordering $>$ to S by neglecting the c_i , and define the ring automorphism

$$\psi_c : S \rightarrow S : \begin{cases} x_i, & \text{if } x_i = z \text{ or } x_i \notin \text{lm}(p), \\ x_i - c_i \cdot z, & \text{otherwise,} \end{cases} \quad (4)$$

$$c_j \mapsto c_j, \quad 1 \leq i, j \leq n.$$

Of course, ψ in (3) is obtained from ψ_c as restriction to R after substituting $\alpha_i \in K$ for c_i for $i = 1, \dots, n$. We write $\psi = (\psi_c)|_{c=\alpha}$ for this relationship, and we also write $K[c]$ for $K[c_1, \dots, c_n]$.

Proposition 17. *For the fixed choice of $p \in J$ in Algorithm 3, there exists a non-zero polynomial $\chi \in K[c]$ such that the ideal $\langle (\psi_c)|_{c=\alpha}(J) \rangle$ contains a non-zero polynomial whose leading monomial is a power of z whenever $\chi(\alpha) \neq 0$.*

For the proof we need the following two lemmas.

Lemma 18. *Using the previous notation, assume furthermore that*

- (i) $\nu \subseteq \{x_b, \dots, x_n\}$, $b \geq 1$, such that $\text{lm}(p) \in K[\nu]$ and $z = x_b \in \nu$;
- (ii) the top-degree part of $\psi_c(p)$ is in $K[c][x_a, \dots, x_n]$, $1 \leq a < b$;
- (iii) there exists $q \in \langle J \rangle$ such that $\text{lm}(q)$ is a power of x_a .

Let e and s be the total degree of p and q respectively. Then we have:

- (1) $\text{res}(\psi_c(p), \psi_c(q), x_a)$ has total degree $e \cdot s$.
- (2) $\text{res}(\psi_c(p), \psi_c(q), x_a)$ contains the monomial z^{es} with non-zero coefficient. More precisely, if $\text{lm}(p) = x_b^{\gamma_b} \dots x_n^{\gamma_n}$, then the monomial Γ^s occurs in this coefficient, where $\Gamma := c_{b+1}^{\gamma_{b+1}} \dots c_n^{\gamma_n}$. Among the monomials of degree $e \cdot s$ in $K[x_{a+1}, \dots, x_b]$ occurring in this resultant, z^{es} is the only one whose coefficient contains the monomial Γ^s .
- (3) If $c_{b+1}^{\epsilon_{b+1}} \dots c_n^{\epsilon_n} \neq \Gamma^s$ occurs in the coefficient of a monomial in $K[x_{a+1}, \dots, x_b]$ of degree $e \cdot s$ that appears in this resultant, then there exists $b+1 \leq k \leq n$ such that $\epsilon_k > s \cdot \gamma_k$ and $\epsilon_j = s \cdot \gamma_j$ for all $k < j \leq n$.

In particular, if $a+1 = b$, then the leading monomial of $\text{res}(\psi_c(p), \psi_c(q), x_a)$ is z^{es} , i.e. the coefficient of z^{es} is a non-zero polynomial in $K[c_{b+1}, \dots, c_n]$.

Proof. We may assume that p is not a constant. Let P be the degree e part of p and Q the degree s part of q . Write

$$\psi_c(P) = \sum_{i=0}^r u_i x_a^{r-i}, \quad \psi_c(Q) = \sum_{j=0}^s v_j x_a^{s-j},$$

with $u_i, v_j \in K[c_{b+1}, \dots, c_n][x_{a+1}, \dots, x_n]$ and $u_0 \neq 0, v_0 \neq 0$.

By construction of ψ_c , the coefficient of z^e in $\psi_c(P)$ is a polynomial w in $K[c_{b+1}, \dots, c_n]$ of positive degree; in fact, the monomials which occur in the expansion of w as a sum of terms are in one-to-one correspondence with the monomials occurring in the expansion of P that involve only variables that divide $\text{lm}(p)$ and possibly z . In particular, Γ occurs in w and corresponds to $\text{lm}(p)$. Thus, of course, we have $u_r \neq 0$. Moreover, by assumption (iii), and since the variable x_a is fixed by ψ_c , we have $v_0 \in K \setminus \{0\}$.

Recall that the Sylvester matrix, whose determinant is $\text{res}(\psi_c(P), \psi_c(Q), x_a)$, is given by

$$\begin{pmatrix} u_0 & 0 & 0 & v_0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \ddots & u_0 & \vdots & \ddots & v_0 \\ u_r & \ddots & \vdots & v_s & \ddots & \vdots \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & u_r & 0 & 0 & v_s \end{pmatrix} \in K[c][x_{a+1}, \dots, x_n]^{(r+s) \times (r+s)}.$$

$\underbrace{\hspace{10em}}_s \quad \underbrace{\hspace{10em}}_r$

We expand the resultant as a sum of terms each of which is obtained (up to sign) as product of entries of the previous matrix taken from $r+s$ distinct rows and $r+s$ distinct columns. Statement (1) obviously follows from (2). In the previous paragraph we have already shown that the summand $u_r^s v_0^r$ contributes a term $\Gamma^s z^{es}$ with non-zero coefficient to the resultant. In order to prove (2), we are going to show that this term is not canceled.

In order to ultimately arrive at statement (3) about coefficients in $K[c]$ of the summands of the resultant, we first look at the coefficients in one u_l .

Consider a term with monomial $x_{a+1}^{\xi_{a+1}} \dots x_b^{\xi_b}$ in the expansion of some u_l , and assume that $\Delta := c_{b+1}^{\delta_{b+1}} \dots c_n^{\delta_n}$ occurs as a monomial in the coefficient of this term. Then Δ occurs as monomial in the coefficient of $m := x_a^{r-l} x_{a+1}^{\xi_{a+1}} \dots x_b^{\xi_b}$ in $\psi_c(m')$, where

$$m' := x_a^{r-l} x_{a+1}^{\xi_{a+1}} \dots x_{b-1}^{\xi_{b-1}} x_b^{\xi_b - \delta_{b+1} - \dots - \delta_n} x_{b+1}^{\delta_{b+1}} \dots x_n^{\delta_n}$$

is a monomial in P and is uniquely determined by the property that $\Delta \cdot m$ occurs with a coefficient in $K \setminus \{0\}$ in $\psi_c(m')$.

Let $l < r$. Then we have $x_a \mid m'$, but $x_a \nmid \text{lm}(p)$ because $a < b$. Thus, $\text{lm}(p) \neq m'$, and necessarily $\text{lm}(p) > m'$ w.r.t. the degree-reverse lexicographical ordering (degrevlex).

Assume for a moment that $\Delta = \Gamma$. Recall that $\text{lm}(p) = x_b^{\gamma_b} \dots x_n^{\gamma_n}$. By homogeneity we get

$$\sum_{i=b}^n \gamma_i = e = (r-l) + \xi_{a+1} + \dots + \xi_{b-1} + \xi_b; \quad (5)$$

however, the definition of degrevlex and the assumption $\Delta = \Gamma$ imply

$$\gamma_b < \xi_b - \delta_{b+1} - \dots - \delta_n = \xi_b - \gamma_{b+1} - \dots - \gamma_n,$$

which together with (5) contradicts the non-negativity of $r-l + \xi_{a+1} + \dots + \xi_{b-1}$ as sum of entries of the exponent vector of m . Therefore, $\Delta \neq \Gamma$, whenever $l < r$; i.e., Γ only occurs as monomial in some coefficient of u_r .

On the other hand, if $l = r$ and $x_{a+1}^{\xi_{a+1}} \dots x_b^{\xi_b}$ occurs in u_r and is different from z^e , then the total degree of $x_{a+1}^{\xi_{a+1}} \dots x_b^{\xi_b}$ is e by homogeneity. So $\xi_b < e$, and for some $a < i < b$, x_i divides the corresponding m' , but $x_i \nmid \text{lm}(p)$. Hence, again $\text{lm}(p) > m'$, and if we assume $\Delta = \Gamma$, then by the definition of degrevlex

$$\deg_{x_b}(m') = \xi_b - \gamma_{b+1} - \dots - \gamma_n > \deg_{x_b}(\text{lm}(p)) = \gamma_b,$$

which contradicts $\xi_b < e = \gamma_b + \dots + \gamma_n$. Therefore, Γ only occurs as monomial in the coefficient of z^e in u_r .

In any case, if $\Delta \neq \Gamma$ then $\text{lm}(p) > m'$.

Now we investigate how monomials $c_{b+1}^{\epsilon_{b+1}} \dots c_n^{\epsilon_n}$ arise in a coefficient of some monomial in $K[x_{a+1}, \dots, x_b]$ appearing in the resultant. Every summand in the expansion of the resultant is produced by multiplying $\prod_{i=1}^s u_{\rho(i)}$, where $1 \leq \rho(i) \leq r$, by a product of certain $v_{\sigma(j)}$ (up to sign). In each $u_{\rho(i)}$ we consider a monomial Δ appearing in the coefficient of some monomial $x_{a+1}^{\xi_{a+1}} \dots x_b^{\xi_b}$ as above. We assume that at least one Δ of these is different from Γ ; fix such a Δ and the corresponding m' .

Now $\text{lm}(p) > m'$, $\Delta \neq \Gamma$, and the definition of degrevlex imply that there exists $b+1 \leq k \leq n$ such that $\epsilon_j = s \cdot \gamma_j$ for all $k < j \leq n$ and $\epsilon_k > s \cdot \gamma_k$. This proves the homogeneous version of (3).

In particular, (3) implies that no monomial in $K[c]$ that occurs in the coefficient of z^{es} and is a multiple of a product of s monomial coefficients chosen from $u_{\rho(1)}, \dots, u_{\rho(s)}$ with at least one different from Γ , divides Γ^s . Hence, only the summand $u_r^s v_0^r$ contributes a term of the form $\Gamma^s z^{es}$ (with some coefficient in $K \setminus \{0\}$) to $\text{res}(\psi_c(P), \psi_c(Q), x_a)$. Since considering the polynomials p and q instead of their top-degree parts P, Q only adds terms of lower degree to $\text{res}(\psi_c(P), \psi_c(Q), x_a)$, this finishes the proof. \square

Lemma 19. *Under the assumptions of Lemma 18, assume furthermore that*

$$a = a_1 < a_2 < \dots < a_t < b$$

is a strictly increasing sequence such that there exist $q_{a_1} = q, q_{a_2}, \dots, q_{a_t} \in \langle J \rangle$ whose leading monomials $\text{lm}(q_{a_i})$ are respectively powers of x_{a_i} , $i = 1, \dots, t$, and such that for $j = 1, \dots, t-1$, the top-degree part of res_{a_j} is in $K[c][x_{a_{j+1}}, \dots, x_n]$, where

$$\text{res}_{a_1} := \text{res}(\psi_c(p), \psi_c(q), x_{a_1}),$$

$$\text{res}_{a_i} := \text{res}(\text{res}_{a_{i-1}}, \psi_c(q_{a_i}), x_{a_i}) \quad \text{for } i = 2, \dots, t.$$

Let $s_{a_1} = s, s_{a_2}, \dots, s_{a_t}$ denote the total degrees of $q_{a_1}, q_{a_2}, \dots, q_{a_t}$ respectively. Then we have:

- (1) res_{a_t} has total degree $e \cdot d$, where $d := s_{a_1} \cdot \dots \cdot s_{a_t}$.
- (2) res_{a_t} contains the monomial z^{ed} with non-zero coefficient. More precisely, the monomial Γ^d occurs in this coefficient, where Γ is defined in Lemma 18. Among the monomials of degree $e \cdot d$ in $K[x_{a_t+1}, \dots, x_b]$ occurring in res_{a_t} , z^{ed} is the only one whose coefficient contains the monomial Γ^d .
- (3) If $c_{b+1}^{\epsilon_{b+1}} \dots c_n^{\epsilon_n} \neq \Gamma^d$ occurs in the coefficient of a monomial in $K[x_{a_t+1}, \dots, x_b]$ of degree $e \cdot d$ that appears in this resultant, then there exists $b+1 \leq k \leq n$ such that $\epsilon_k > d \cdot \gamma_k$ and $\epsilon_j = d \cdot \gamma_j$ for all $k < j \leq n$.

In particular, if $a_t + 1 = b$, then the leading monomial of res_{a_t} is z^{ed} , i.e. the coefficient of z^{ed} is a non-zero polynomial in $K[c_{b+1}, \dots, c_n]$.

Proof by induction on t . If $t = 1$ then the assertions follow from Lemma 18.

Let $t > 1$. Similarly as in the proof of Lemma 18, we consider the top-degree parts P and Q of $\text{res}_{a_{t-1}}$ resp. q_{a_t} , which have degrees $e \cdot s_{a_1} \cdot \dots \cdot s_{a_{t-1}}$ resp. s_{a_t} . Write

$$P = \sum_{i=0}^r u_i x_{a_t}^{r-i}, \quad \psi_c(Q) = \sum_{j=0}^{s_{a_t}} v_j x_{a_t}^{s_{a_t}-j},$$

with $u_i, v_j \in K[c_{b+1}, \dots, c_n][x_{a_t+1}, \dots, x_n]$ and $u_0 \neq 0, v_0 \neq 0$.

The summand $u_r^{s_{a_t}} v_0^r$ of $\text{res}(P, \psi_c(Q), x_{a_t})$ contains $(z^{e \cdot s_{a_1} \cdot \dots \cdot s_{a_{t-1}}})^{s_{a_t}}$ with a coefficient in which $(\Gamma^{s_{a_1} \cdot \dots \cdot s_{a_{t-1}}})^{s_{a_t}}$ occurs with a coefficient in $K \setminus \{0\}$. This term $\Gamma^d z^{ed}$ is not canceled in the expansion of the resultant: A monomial $c_{b+1}^{\epsilon_{b+1}} \dots c_n^{\epsilon_n}$ occurring in the coefficient of some monomial in $K[x_{a_t+1}, \dots, x_b]$ in the resultant is a multiple of some product of s monomials $\Delta \in K[c]$ in $u_{\rho(i)}$, $i = 1, \dots, s$. By the induction hypothesis, if at least one Δ of these is different from $\Gamma^{s_{a_1} \cdot \dots \cdot s_{a_{t-1}}}$, then there exists $b+1 \leq k \leq n$ such that $\epsilon_k > d \cdot \gamma_k$ and $\epsilon_j = d \cdot \gamma_j$ for all $k < j \leq n$. In particular, the term $\Gamma^d z^{ed}$ arises in exactly one way as product of terms chosen from entries u_i and v_j when expanding the determinant of the Sylvester matrix.

The rest is analogous to the proof of the previous lemma. \square

Proof of Proposition 17. Let $1 \leq b \leq n$ be such that $z = x_b$.

If $\text{lm}((\psi_c)|_{c=\alpha}(p))$ is a power of z for all $(\alpha_1, \dots, \alpha_n) \in K^n$, then we can choose $\chi = 1$. So it is enough to find a polynomial $\chi \in K[c]$ with the desired property for each p for which $\text{lm}((\psi_c)|_{c=\alpha}(p))$ is *not* a power of z for some values α_i . This means that for such a polynomial p , we have $\text{lm}(\psi_c(p)) \notin K[x_b, \dots, x_n]$, as $z^{\deg(p)}$ is the greatest monomial of that degree in $K[x_b, \dots, x_n]$ w.r.t. $>$.

Choose $1 \leq a < b$ maximal such that the top-degree part of $\psi_c(p)$ is in $K[x_a, \dots, x_n]$.

Since z was chosen to be the $>$ -greatest variable in ν in Algorithm 3, Lemma 13 implies that for every $1 \leq i \leq b-1$, there exists $q_i \in J$ such that $\text{lm}(q_i)$ is a power of x_i . Now the coefficient of $z^{e \cdot s_{a_1} \cdot \dots \cdot s_{a_t}}$ in res_{a_t} referred to in Lemma 19 for a suitable sequence $a_1 = a < a_2 < \dots < a_t < b$, qualifies for the polynomial χ because it is the leading coefficient of res_{a_t} . \square

6. Comparison of implementations

Motivated by the experiments recorded in (Hashemi, 2008) we decided to include here a comparison of the implementations of Noether normalization algorithms accessible to the author at the time of writing. We tried three implementations in SINGULAR (Greuel et al., 2005) (*m*: `NoetherPosition` in `mregular.lib`; *n*: `NPos` in `noether.lib`; *a*: `noetherNormal` in `algebra.lib`), the implementation of Logar’s algorithm (Logar, 1989) in MACAULAY 2, version 1.2, (Grayson and Stillman, 2009) (`noetherNormalization` in `NoetherNormalization.m2`), an algorithm following (Greuel and Pfister, 2008) in MAGMA V2.15–4 (Bosma et al., 1997) (command `NoetherNormalization`), and the author’s implementation of Algorithm 3 included in the MAPLE package INVOLUTIVE (Blinkov et al., 2003). The author’s implementation realizes the coordinate change given in (3) as follows: start with the coefficient vector α whose entries are all 1; check whether the monomial z^e appears in the transformed top-degree part of p ; if this check fails, add 1 to one entry of α (in a rotary way) and try again.

These programs were applied to some of the examples listed in (Decker et al., 1999) and to the “Haas example” treated in (Hashemi, 2008). The chosen examples define ideals over the rational numbers of Krull dimension at least 1.

For each example we record the logarithm with base 10 of the absolutely largest coefficient in the minimal Janet basis of the ideal $\phi(I)$ in Noether position (using the notation of Algorithm 3), where every polynomial was made primitive with integer coefficients. As the previously existing implementations have probabilistic behavior, we have run each example ten times and computed the arithmetic mean. The table below shows the data which measure how difficult we expect further computations with $\phi(I)$ to be. In case no number is given, the Noether normalization procedure did not finish within one hour on an AMD Opteron processor, 2.6 GHz, or allocated more than 10 GB memory on the same machine.

Acknowledgements

The author would like to thank the referees for their helpful reports, in particular for providing the author with the reference (Hashemi, 2008).

References

- Apel, J., 1998. The theory of involutive divisions and an application to Hilbert function computations. *J. Symb. Comp.* 25 (6), 683–704.
- Bermejo, I., Gimenez, P., 2006. Saturation and Castelnuovo-Mumford regularity. *J. Algebra* 303, 592–617.
- Blinkov, Y. A., Cid, C. F., Gerdt, V. P., Plesken, W., Robertz, D., 2003. The MAPLE Package “Janet”: I. Polynomial Systems. In: Ganzha, V. G., Mayr, E. W., Vorozhtsov, E. V. (Eds.), *Proc. of Computer Algebra in Scientific Computing CASC 2003*. Institut für Informatik, TU München, Garching, Germany, pp. 31–40, see also <http://wwwb.math.rwth-aachen.de/Janet>.
- Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24 (3-4), 235–265, *Computational algebra and number theory* (London, 1993).

	SING. ^m	SING. ⁿ	SING. ^a	M2	MAGMA	Algorithm 3
Gerdt	105.6	57.5	–	26.6	11.7	16.8
Gonnet	342.5	353.6	–	106.8	–	15.8
Haas	317.3	321.9	–	–	–	22.8
Horrocks	207.8	194.3	125.5	–	–	8.8
Lanconelli	83.8	91.5	40.8	–	–	0.7
Macaulay	78.8	0	51.0	76.7	0	0
mat3 ²	152.7	36.9	98.8	–	–	1.0
Mikro	699.6	696.1	–	454.5	–	316.7
Möller	334.9	95.6	–	–	–	8.7
Riemenschneider	105.1	66.5	–	6.8	3.3	0.3
Schwarz	196.0	183.8	334.2	122.6	3.1	64.3
Shimoyama- Yokoyama (2-dim)	18.6	8.5	6.5	4.5	1.9	1.1
Siebert	240.3	252.7	198.6	89.6	25.5	18.0
Sturmfels- Eisenbud	72.9	71.5	119.5	–	–	1.0

- Buchberger, B., 2006. An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal. *J. Symb. Comp.* 41 (3–4), 475–511, PhD Thesis, Univ. Innsbruck, English translation.
- Caviglia, G., Sbarra, E., 2005. Characteristic-free bounds for the Castelnuovo-Mumford regularity. *Compositio Mathematica* 141, 1365–1373.
- Decker, W., Greuel, G.-M., Pfister, G., 1999. Primary decomposition: algorithms and comparisons. In: Matzat, B. H., Greuel, G.-M., Hiss, G. (Eds.), *Algorithmic algebra and number theory (Heidelberg, 1997)*. Springer, Berlin, pp. 187–220.
- Eisenbud, D., 1995. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150 of Graduate Texts in Mathematics. Springer.
- Eisenbud, D., Sturmfels, B., 1994. Finding sparse systems of parameters. *Journal of Pure and Applied Algebra* 94, 143–157.
- Gerdt, V. P., 2005. Involutive Algorithms for Computing Gröbner Bases. In: Cojocaru, S., Pfister, G., Ufnarovski, V. (Eds.), *Computational Commutative and Non-Commutative Algebraic Geometry*. Vol. 196 of NATO Science Series III: Computer and Systems Sciences. IOS Press, Amsterdam, pp. 199–225.
- Gerdt, V. P., Blinkov, Y. A., 1998. Involutive bases of polynomial ideals. *Mathematics and Computers in Simulation* 45, 519–541.
- Grayson, D. R., Stillman, M. E., 2009. Macaulay 2, a software system for research in algebraic geometry. Available at <http://www.math.uiuc.edu/Macaulay2/>.

- Greuel, G.-M., Pfister, G., 2008. *A Singular Introduction to Commutative Algebra*, 2nd Edition. Springer.
- Greuel, G.-M., Pfister, G., Schönemann, H., 2005. *SINGULAR 3.0. A Computer Algebra System for Polynomial Computations*. Centre for Computer Algebra, University of Kaiserslautern. <http://www.singular.uni-kl.de>.
- Hashemi, A., 2008. Efficient Algorithms for Computing Noether Normalization. In: Kapur, D. (Ed.), *Computer Mathematics. 8th Asian Symposium, ASCM 2007, Singapore, December 15-17, 2007*. Vol. 5081 of *Lecture Notes in Artificial Intelligence*. Springer, pp. 97–107.
- Hausdorf, M., Seiler, W. M., 2002. An efficient algebraic algorithm for the geometric completion to involution. *Appl. Algebra Engrg. Comm. Comput.* 13 (3), 163–207.
- Janet, M., 1929. *Leçons sur les systèmes d'équations aux dérivées partielles*. Cahiers Scientifiques IV. Gauthiers-Villars, Paris.
- Logar, A., 1989. A computational proof of the Noether normalization lemma. In: *Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988)*. Vol. 357 of *Lecture Notes in Comput. Sci.* Springer, pp. 259–273.
- Méray, C., 1880. Démonstration générale de l'existence des intégrales des équations aux dérivées partielles. *Journal de mathématiques pures et appliquées*, 3e série, tome VI, 235–265.
- Nagata, M., 1962. *Local Rings*. Vol. 13 of *Interscience Tracts in Pure and Applied Mathematics*. John Wiley & Sons.
- Plesken, W., Robertz, D., 2005. Janet's approach to presentations and resolutions for polynomials and linear pdes. *Archiv der Math.* 84 (1), 22–37.
- Pommaret, J.-F., 1994. *Partial Differential Equations and Group Theory*. Vol. 293 of *Mathematics and its Applications*. Kluwer, Dordrecht.
- Riquier, C., 1910. *Les systèmes d'équations aux dérivées partielles*. Gauthiers-Villars, Paris.
- Robertz, D., 2006. *Formal Computational Methods for Control Theory*. Ph.D. thesis, RWTH Aachen University, Germany, available online at <http://darwin.bth.rwth-aachen.de/opus/volltexte/2006/1586>.
- Robertz, D., 2007. Janet bases and applications. In: Rosenkranz, M., Wang, D. (Eds.), *Gröbner Bases in Symbolic Analysis*. Vol. 2 of *Radon Series on Computational and Applied Mathematics*. Walter de Gruyter, pp. 139–168.
- Schwarz, F., 2008. Algorithmic Lie theory for solving ordinary differential equations. Vol. 291 of *Pure and Applied Mathematics*. Chapman & Hall.
- Seiler, W. M., 2007. A Combinatorial Approach to Involution and δ -Regularity: I. Involutive Bases in Polynomial Algebras of Solvable Type. II. Structure Analysis of Polynomial Modules with Pommaret Bases, preprints, [arXiv:math/0208247](https://arxiv.org/abs/math/0208247) and [arXiv:math/0208250](https://arxiv.org/abs/math/0208250).
- Stanley, R. P., 1996. *Combinatorics and Commutative Algebra*, 2nd Edition. Vol. 41 of *Progress in Mathematics*. Birkhäuser.
- Sturmfels, B., 1990. Gröbner bases and Stanley decompositions of determinantal rings. *Mathematische Zeitschrift* 205, 137–144.
- Sturmfels, B., White, N., 1991. Computing combinatorial decompositions of rings. *Combinatorica* 11 (3), 275–293.
- Vasconcelos, W. V., 1998. *Computational Methods in Commutative Algebra and Algebraic Geometry*. Vol. 2 of *Algorithms and Computation in Mathematics*. Springer.