Dynamical Aspects of Involutive Bases Computations

Ralf Hemmecke

Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria
ralf@hemmecke.de

Abstract. The article is a contribution to a more efficient computation of involutive bases. We present an algorithm which computes a 'sliced division'. A sliced division is an admissible partial division in the sense of Apel. Admissibility requires a certain order on the terms. Instead of ordering the terms in advance, our algorithm additionally returns such an order for which the computed sliced division is admissible. Our algorithm gives rise to a whole class of sliced divisions since there is some freedom to choose certain elements in the course of its run. We show that each sliced division refines the Thomas division and thus leads to terminating completion algorithms for the computation of involutive bases. A sliced division is such that its cones 'cover' a relatively 'big' part of the term monoid generated by the given terms. The number of prolongations that must be considered during the involutive basis algorithm is tightly connected to the dimensions and number of the cones. By some computer experiments, we show how this new division can be fruitful for the involutive basis algorithm.

We generalise the sliced division algorithm so that it can be seen as an algorithm which is parameterised by two choice functions and give particular choice functions for the computation of the classical divisions of Janet, Pommaret, and Thomas.

1 Introduction

Involutive bases have their origin in the Riquier-Janet Theory of partial differential equations at the beginning of the 20th century. In Riquier's Existence and Uniqueness Theorem, a separation of variables into multiplicative and non-multiplicative ones is essential. Janet was the first to give an algorithm to transform a system of partial differential equations (PDEs) into a canonical form (passive system) required for Riquier's Theorem. He also described a particular separation of variables. Zharkov and Blinkov [8] translated Janet's algorithm into a polynomial context where its form is strikingly similar to Buchberger's well known Gröbner basis algorithm [3]. In fact, the polynomial Janet algorithm computes a Gröbner basis, though not a reduced one, but it does this in a slightly different fashion. Basically, it is also a critical element/completion algorithm, however, instead of S-polynomials, it considers *prolongations* as critical elements, and the usual polynomial reduction is applied in a restricted sense.

Later Apel [1] and Gerdt/Blinkov [4] introduced the notion of involutive division in order to generalise the separation of variables that could be used in Janet's algorithm. Unfortunately, two slightly differing notions for involutive division are now available and it remains to be seen which one is more appropriate. Our paper follows the ideas of Apel.

The article is structured as follows. We first recall the basic definitions. In Section 5 we present an algorithm to compute a sliced division and prove termination and correctness of this algorithm. In Section 6 we show that each sliced division refines the Thomas division on the same set of terms. Section 7 deals with a generalisation of the sliced division algorithm. We show that every generalised sliced division is an admissible partial division. We present the classical partial divisions as generalised sliced divisions. In Section 8 we show by some computer experiments how the involutive basis algorithm can benefit from using the sliced division sub-algorithm.

Parts of the material presented in this article have already been given in a talk at the ACA 2001 conference, Albuquerque, New Mexico.

2 Preliminaries

For the whole paper let $X = \{x_1, \ldots, x_n\}$ be a set of indeterminates and $\mathbb{K}[X]$ be the set of polynomials in X over the field $\mathbb{K}$ of coefficients. By T we denote the set of power products of $\mathbb{K}[X]$. Since we are not interested in this paper in computations with respect to different term orders, we fix a certain admissible term order. We denote for $0 \neq f \in \mathbb{K}[X]$ by $\operatorname{supp} f \subset T$ the set of terms of f that appear with a non-zero coefficient and by $\operatorname{lt} f$ the biggest term of $\operatorname{supp} f$ with respect to the term order. Furthermore, if $F \subseteq \mathbb{K}[X]$, let $\operatorname{lt}(F) := \{\operatorname{lt} f \mid 0 \neq f \in F\}$.

By $\deg_x t$ we denote the degree of $t \in T$ in $x \in X$, whereas $\deg t$ is the total degree of t.

Definition 1. *For any set $U \subseteq T$ we define $\langle U \rangle$ as the monoid generated by U, i. e., $\langle U \rangle := \{t \in T \mid \exists u_1, \ldots, u_m \in U : t = u_1 u_2 \cdots u_m\}$. By definition, the product of $m = 0$ elements is 1, in particular, $\langle \emptyset \rangle = \{1\}$.*

Definition 2. *Let $Y \subseteq X$, $t \in T$, $U \subseteq T$. By tU we denote the set $\{tu \mid u \in U\}$. The set $t\langle Y \rangle$ is called a **cone**, t its **base point**, and the elements of Y its **multipliers**. The number of elements of Y is called the **dimension** of the cone.*

Definition 3. *The lexicographical order on T is defined by $u <_{\text{lex}} v$ iff there exists an $i \in \{1, \ldots, n\}$ such that $\deg_{x_j} u = \deg_{x_j} v$ for all $1 \leq j < i$ and $\deg_{x_i} u < \deg_{x_i} v$. The term u is inverse lexicographically smaller than v (denoted $u <_{\text{invlex}} v$) iff $v <_{\text{lex}} u$.*

3 Partial Divisions

After Zharkov and Blinkov [8] brought the Janet algorithm to a polynomial context (see chapter 8), Apel and Gerdt/Blinkov realised that the particular choice of multiplicative and non-multiplicative variables that was used by Janet in his algorithm could be generalised. They came up with the concept of involutive division [1], [4] which is called admissible partial division in [2].

In order to get an intuitive picture of a partial division, one should read the ordinary divisibility relation $u \mid v$ of two terms $u, v \in T$ as $v \in u\langle X\rangle$. That is to say: to each term $t \in T$ we assign the cone of all its multiples. If we restrict these cones to sub-cones and define divisibility in terms of these restricted cones, we arrive at the concept of partial division. The word 'partial' should suggest that two terms which are ordinarily divisible might not be divisible with respect to some partial division. The idea behind 'admissible partial division' is that cones should be disjoint whereas 'complete' suggests that a certain region is completely covered by disjoint cones.

Apel and Gerdt/Blinkov introduced slightly different notions of involutive division. Since this paper is based on Apel's version, the definitions below mainly follow the definitions in [2].

Definition 4. *Let $(Y_t)_{t\in T}$ be a family of subsets of X. The family $\mathcal{M} = (t\langle Y_t\rangle)_{t\in T}$ is called a **partial division**. If $v \in u\langle Y_u\rangle$, then v is called an $\mathcal{M}$**-multiple** of u, and u is an $\mathcal{M}$**-divisor** of v.*

*Let $U \subseteq T$. Each family $\mathcal{N} = (t\langle Y_t\rangle)_{t\in U}$ **induces** a partial division $\mathcal{M} = (t\langle Y_t\rangle)_{t\in T}$ by setting $Y_t := X$ for $t \notin U$. We will also call $\mathcal{N}$ a partial division and mean its induced partial division.*

*Let $\sqsubset$ be a total order on $U \subseteq T$. A partial division $\mathcal{M} = (t\langle Y_t\rangle)_{t\in T}$ is called **admissible on** $(U, \sqsubset)$ if for all $u, v \in U$ with $u \sqsubset v$, one of the conditions*

$$u\langle X\rangle \cap v\langle Y_v\rangle = \emptyset \text{ or} \tag{1}$$

$$u\langle Y_u\rangle \subset v\langle Y_v\rangle \tag{2}$$

*holds. $\mathcal{M}$ is **admissible on** U if there exists a total order $\sqsubset$ on U such that $\mathcal{M}$ is admissible on $(U, \sqsubset)$.*

*The set U will be called **complete** if there exists an admissible partial division $(t\langle Y_t\rangle)_{t\in T}$ on U and*

$$\bigcup_{t\in U} t\langle Y_t\rangle = \bigcup_{t\in U} t\langle X\rangle.$$

Remark 1. The first condition of admissibility involves the set X. So it would have been more precise to speak of X-admissibility. Because of the following observation, this additional qualification is not needed. Suppose a partial division $(u\langle Y_u\rangle)_{u\in U}$ is X-admissible on $(U, \sqsubset)$. Then it is also X'-admissible for all $X' \supseteq \bigcup_{u\in U} Y_u$.

Let $u, v \in U$ with $u \sqsubset v$ and suppose the relation

$$u\langle X\rangle \cap v\langle Y_v\rangle = \emptyset \tag{3}$$

holds. Then also

$$u\langle X'\rangle \cap v\langle Y_v\rangle = \emptyset \tag{4}$$

trivially holds for all $X' \subset X$. From (3) it follows that $\deg_x u > \deg_x v$ for some $x \in X \setminus Y_v$. Therefore, (4) holds for $X' \supset X$, as well.

The following definition introduces a partial order on the set of all partial divisions.

Definition 5. *Let $\mathcal{M} = (M_t)_{t\in T}$ and $\mathcal{N} = (N_t)_{t\in T}$ be two partial divisions. If $M_t \subseteq N_t$ for all $t \in T$ we say that $\mathcal{N}$ **refines** $\mathcal{M}$. Let $U \subseteq T$. $\mathcal{M}$ and $\mathcal{N}$ are U-**equivalent** if $M_u = N_u$ for all $u \in U$ (denoted $\mathcal{M} \equiv_U \mathcal{N}$).*

4 Classical Partial Divisions

The following three divisions are called 'classical' in the literature. We include them here as examples of admissible partial divisions. Whereas the Thomas division is important for the termination of the involutive basis algorithm, we will refer to Janet and Pommaret division in Section 7.

Janet [5] used a particular partial division which is defined as follows.

Example 1 (Janet Division). Let $U \subseteq T$ be a finite set of power products. Define $Y_t = X$ for all $t \notin U$ and

$$Y_t := \left\{ x_i \in X \;\middle|\; \nexists u \in U : \deg_{x_i} u > \deg_{x_i} t \wedge \forall\, 1 \le j < i : \deg_{x_j} u = \deg_{x_j} t \right\}$$

for all $t \in U$. The division $(t\langle Y_t\rangle)_{t\in T}$ is called **Janet division on** U.

The Thomas division [7] is mainly of theoretical interest. Apel showed in [1] that the involutive basis algorithm will terminate if one chooses a partial division which refines the Thomas division.

Example 2 (Thomas Division). Let $U \subseteq T$ be a set of power products. Define $Y_t = X$ for all $t \notin U$ and $Y_t := \{x \in X \mid \forall u \in U : \deg_x u \le \deg_x t\}$ for all $t \in U$. The division $(t\langle Y_t\rangle)_{t\in T}$ is called **Thomas division on** U.

Another division is due to Pommaret [6].

Example 3 (Pommaret Division). Let $Y_1 := X$. If $t \in \langle x_1, \ldots, x_k\rangle$ and $\deg_{x_k} t > 0$ for some $k \in \{1, \ldots, n\}$ then let $Y_t := \{x_k, \ldots, x_n\}$. The division $(t\langle Y_t\rangle)_{t\in T}$ is called **Pommaret division**.

All of the above divisions are admissible with respect to the inverse lexicographical order on T (cf. [1]).

As one easily recognises, Janet and Pommaret divisions can be defined for any permutation of the variables.

Gerdt/Blinkov [4] gave further divisions whereas Apel [1] considers the whole lattice of partial divisions and argues to prefer a maximal (with respect to the refinement relation, cf. Definition 5) admissible division in each step of the involutive basis algorithm.

5 Sliced Division Algorithm

In this section we present an algorithm which not only computes an admissible partial division for a given set U of terms but also a particular order on U so that the resulting division is admissible on U with respect to that order. This approach is different from Apel's sub-maximal refinement of a division with respect to some given order.

The basic objective for the sliced division algorithm was to find an admissible partial division on a set U of terms such that the cones attached to elements of U cover a relatively 'big' part of the monoid ideal generated by U. This is achieved by assigning all variables as multiplicative to a term of minimal total degree and then applying such an assignment recursively (with fewer variables) to the remaining terms.

Algorithm 1 SLICEDDIVISION

Call: $M := \text{slicedDivision}(Y, U)$

Input: $Y \subseteq X$ finite set of indeterminates
$U = \{u_1, \ldots, u_r\} \subseteq w\langle Y\rangle$ for some $w \in \langle X \setminus Y\rangle$ where $r = \operatorname{card} U$

Output: A list $[v_1\langle Y_{v_1}\rangle, \ldots, v_r\langle Y_{v_r}\rangle]$ of Y-cones such that $U = \{v_1, \ldots, v_r\}$ and $\forall i, j = 1, \ldots, r : i < j \implies (v_i\langle Y\rangle \cap v_j\langle Y_{v_j}\rangle = \emptyset \vee v_i\langle Y_{v_i}\rangle \subset v_j\langle Y_{v_j}\rangle)$

$L := []$ # *empty list*
<u>if</u> $U = \emptyset$ <u>then</u> <u>return</u> L
<u>if</u> $Y = \emptyset$ <u>then</u> <u>return</u> $[w\langle Y\rangle]$ # *Note that here* $U = w\langle Y\rangle = \{w\}$ *if* $Y = \emptyset$.
Choose $m \in U$ with $\deg m = \min\{\deg u \mid u \in U\}$
$C := (U \cap m\langle Y\rangle) \setminus \{m\}$; $L_C := \text{slicedDivision}(Y, C)$
$V := U \setminus m\langle Y\rangle$ # *same as* $V := U \setminus (C \cup \{m\})$
<u>while</u> $V \neq \emptyset$ <u>do</u>
  Choose $x \in Y$ such that $\deg_x(\gcd V) < \deg_x m$
  $d := \deg_x(\gcd V)$
  $S := \{v \in V \mid \deg_x v = d\}$
  $V := V \setminus S$
  $L_S := \text{slicedDivision}(Y \setminus \{x\}, S)$
  $L := \text{concat}(L_S, L)$
<u>return</u> $\text{concat}(L_C, [m\langle Y\rangle], L)$

5.1 Some Comments to the Algorithm

Informally speaking, one should associate the set U of terms with its monoid ideal represented in some $\mathbb{N}^n$. As the first step, some element m of minimal total degree is taken from U and gets the full-dimensional cone assigned to it (a shifted copy of $\mathbb{N}^n$). All elements which are divisible by m are treated recursively. Any of the other elements will get a cone which is at most of dimension $n-1$. By taking hyperplanes perpendicular to the direction of some variable x (chosen in each iteration step), slices are cut from the 'outermost' part of the ideal until the cone of m is reached. The elements inside such a slice correspond to elements of V (cf. Algorithm 1) having minimal degree in x. Such slices are of dimension $n-1$ and thus can be treated recursively.

Definition 6. *Let $U \subseteq T$ be a finite set of terms and $[u_1\langle Y_{u_1}\rangle, \ldots, u_r\langle Y_{u_r}\rangle]$ be an output of* SLICEDDIVISION(X, U). *$(u\langle Y_u\rangle)_{u\in U}$ is called a* ***sliced division on*** *U.*

The condition $U \subseteq w\langle Y\rangle$, $w \in \langle X \setminus Y\rangle$ in the specification of Algorithm 1 just states that elements of U agree in the 'non-multiplicative part'.

5.2 Termination and Correctness

Theorem 1. *The algorithm* SLICEDDIVISION *(page 173) terminates and meets its specification.*

Proof. One easily verifies that the parameters of recursive calls of the algorithm fulfil the input specification.

Termination. Because of lines 3, 6, and 7, the choice of x in line 8 is possible. There can be only finitely many while iterations (lines 7–13), since S contains at least one element and thus the cardinality of V decreases. In each recursive call the sum of the cardinality of the input parameters is strictly smaller than $\operatorname{card} Y + \operatorname{card} U$. Thus the recursion depth is bounded, and hence SLICEDDIVISION terminates.

Correctness. Let Y and U be as specified in the input of Algorithm 1. The proof will be an induction on the number of elements in the input sets. Obviously, the algorithm is correct if it is started with empty input parameters. Let us assume that the algorithm is correct if the sum of the cardinalities of the input parameters is smaller than $\operatorname{card} Y + \operatorname{card} U$. Let $[v_1\langle Y_{v_1}\rangle, \ldots, v_{r'}\langle Y_{v_{r'}}\rangle]$ be the output of the algorithm for Y and U. Consider the particular run where this output was produced. Let m, C, and V be as specified before the while loop, and let s be the number of actual iterations.

In the following let σ range over $1, \ldots, s$. The values of x, and S after the σ-th iteration will be denoted by x_σ and S_σ.

First, we must show that $r' = r$. By induction hypothesis, we have $\operatorname{card} C = \operatorname{card} L_C$ and $\operatorname{card} S_\sigma = \operatorname{card} L_{S_\sigma}$ for all σ. From lines 1, 13, and 14 and the fact that U is equal to the disjoint union $C \cup \{m\} \cup S_s \cup \cdots \cup S_1$, we can conclude $r = r'$.

Lines 5, 12, and 14 together with the induction hypothesis then imply $U = \{v_1, \ldots, v_r\}$.

Take $i, j \in \{1, \ldots, r\}$ with $i < j$. It remains to show that

$$v_i\langle Y\rangle \cap v_j\langle Y_{v_j}\rangle = \emptyset \text{ or} \tag{5}$$

$$v_i\langle Y_{v_i}\rangle \subset v_j\langle Y_{v_j}\rangle \tag{6}$$

holds. There are several cases to consider.

1. $v_i, v_j \in C$: (5) or (6) follows by induction hypothesis.
2. $v_i \in C$, $v_j = m$: We have $Y_{v_j} = Y$ and (6) by construction of C.
3. $v_i \in C \cup \{m\}$, $v_j \in S_\sigma$ for some $\sigma \in \{1, \dots, s\}$: By construction of m, C, and S_σ, we have $m\langle Y\rangle \cap v_j\langle Y_{v_j}\rangle = \emptyset$, because $\deg_{x_\sigma} v_j < \deg_{x_\sigma} m$ and $x_\sigma \in X \setminus Y_{v_j}$. Since $c\langle Y_c\rangle \subset m\langle Y\rangle$ for all $c \in C$, relation (5) holds.
4. $v_i \in S_\sigma$, $v_j \in S_{\sigma'}$ for some $\sigma, \sigma' \in \{1, \dots, s\}$: If $\sigma = \sigma'$ then (5) or (6) follows from the induction hypothesis and Remark 1. Otherwise, $i < j$ implies $\sigma > \sigma'$ by line 14 and construction of L in line 13. The inequality $\deg_{x_{\sigma'}}(v_i t) > \deg_{x_{\sigma'}} v_j$ holds for $t = 1$ by construction of $S_{\sigma'}$ and remains true for any $t \in \langle Y\rangle$. Since $x_{\sigma'} \notin Y_{v_j}$, we can conclude (5).

By line 14 there cannot be other cases. Thus, the correctness of slicedDivision is proved. □

Corollary 1. *Let $W \subseteq T$ be a finite set of terms, and $[w_1\langle Y_{w_1}\rangle, \dots, w_r\langle Y_{w_r}\rangle]$ an output of* slicedDivision(X, W)*. Define $\sqsubset$ on W by $w_i \sqsubset w_j \iff i < j$, $i, j = 1, \dots, r$. Then $\mathcal{M} = (t\langle Y_t\rangle)_{t \in W}$ is admissible on $(W, \sqsubset)$.*

We want to emphasise the fact that instead of giving an order $\sqsubset$ in advance and then compute an admissible partial division with respect to that order, our algorithm only starts with a set of terms and returns a division and an order for which this division is admissible.

One easily verifies that slicedDivision never calls itself with an empty set of variables if it is started with a non-empty set Y. Line 3 is only important if the algorithm is initially called with an empty set of variables or for a generalisation of the algorithm. In fact, algorithm slicedDivision also meets its specification if an arbitrary element $m \in U$ in line 4 is chosen. For such a generalisation, however, it can happen that the algorithm calls itself with an empty set Y. One easily verifies that the proof of Theorem 1 does not depend on the particular choice of m. For an extensive treatment of the generalised algorithm see Section 7.

6 Sliced Division Refines Thomas Division

As Apel showed in [1], termination of the involutive basis algorithm (Algorithm 2) is guaranteed if the division used in its while loop refines the Thomas division.

The following property of the Thomas division is easy to prove.

Lemma 1. *Let $U, V \subseteq T$ be two sets with $U \supseteq V$ and $(t\langle Y_t\rangle)_{t \in T}$, $(t\langle Z_t\rangle)_{t \in T}$ be the Thomas divisions on U and V, respectively. Then $Y_t \subseteq Z_t$ for all $t \in T$.*

Proof. For all $t \in T \setminus U$ the equality $Y_t = Z_t = X$ holds. Trivially, $Y_t \subseteq Z_t = X$ is true for all $t \in U \setminus V$. For all $t \in V$ and all $x \in X \setminus Z_t$ there exists $t' \in V$ with $\deg_x t' > \deg_x t$ and, therefore $x \in X \setminus Y_t$. Hence, $Y_t \subseteq Z_t$. □

Theorem 2. *Let $Y \subseteq X$ be a set of variables, $U \subset T$ be a finite set of terms, and $[u_1\langle Y_{u_1}\rangle, \ldots, u_r\langle Y_{u_r}\rangle] = \text{SLICEDDIVISION}(Y, U)$. Then for the Thomas division $(t\langle Z_t\rangle)_{t\in T}$ on U the relation $Z_u \cap Y \subseteq Y_u$ holds for all $u \in U$.*

Proof. Since for $U = \emptyset$ there is nothing to prove, assume that $\operatorname{card} U = r > 0$ and that the theorem is correct if the number of terms is less than r. Consider the run of SLICEDDIVISION where $[u_1\langle Y_{u_1}\rangle, \ldots, u_r\langle Y_{u_r}\rangle]$ was computed. Let s be the number of iterations of the while loop, and let C and m be as defined in the algorithm. After the σ-th iteration ($\sigma = 1, \ldots, s$) of the while loop the values of x and S are denoted by x_σ and S_σ, respectively. Then U is the disjoint union $C \cup \{m\} \cup S_s \cup \cdots \cup S_1$.

Trivially, $Z_m \cap Y \subseteq Y_m = Y$. From the induction hypothesis it follows that $Z_u \cap Y \subseteq Y_u$ for all $u \in C$. Now consider S_σ for some $\sigma \in \{1, \ldots, s\}$. Take any $u \in S_\sigma$. From the induction hypothesis we get $Z_u \cap (Y \setminus \{x_\sigma\}) \subseteq Y_u$ (see line 12 of Algorithm 1). By definition of the Thomas division, we have $x_\sigma \notin Z_u$ since $\deg_{x_\sigma} u < \deg_{x_\sigma} m$. Hence, $Z_u \cap Y \subseteq Y_u$ as claimed. □

The following corollary is Theorem 2 for the special case $X = Y$.

Corollary 2. *Let $U \subseteq T$ be a finite set of terms. Then a sliced division on U refines the Thomas division on U.*

7 Generalised Sliced Division

The algorithm SLICEDDIVISION was designed to construct an admissible partial division on a set U of terms such that the cones attached to elements of U cover a relatively 'big' part of the monoid ideal generated by U. For theoretical considerations it is interesting to generalise the algorithm such that it can compute other known admissible divisions.

As we have already seen, the particular choice of m in line 4 of Algorithm 1 does not affect the correctness of Theorem 1. By a further generalised form of SLICEDDIVISION, not only one can compute the Janet division, but also Pommaret and Thomas division as we shall see in section 7.2.

Let us first generalise the sliced division algorithm.

7.1 Every Generalised Sliced Division is an Admissible Partial Division

Let $U \subseteq T$ be a finite set of terms. SLICEDDIVISION(X, U) always returns a partial division where at least one term of U has a full-dimensional cone. It cannot compute, for example, the Pommaret division for the terms $\{x_1x_2^2, x_1^2x_2\}$ since x_1 is not Pommaret-multiplicative for both terms. To produce admissible divisions on a set U where no element of U will get a cone corresponding to all possible variables, we introduce a distinct symbol $\infty \notin U$ and allow to choose in line 4 of SLICEDDIVSION either an element of U or this symbol depending on whether or not the final division should contain a full-dimensional cone.

In order to simplify notation, for $m = \infty$, $Y \subseteq X$, and $U \subseteq T$, we require that the set $U \cap m\langle Y\rangle$ is empty (no matter how $m\langle Y\rangle$ is actually defined), and we declare $\deg_x t < \deg_x m$ for all $x \in X$, $t \in T$.

By using the same specification as that of $\textsc{slicedDivision}$, the generalised version of Algorithm 1 is obtained by replacing lines 4, 8, and 14 by

4: $m := \textsc{chooseFirst}(Y, U)$
8: $x := \textsc{chooseNonMultiplier}(Y, V, m)$
14: <u>if</u> $m \in U$ <u>then</u> <u>return</u> $\textsc{concat}(L_C, [m\langle Y\rangle], L)$ <u>else</u> <u>return</u> L

with two sub-algorithms $\textsc{chooseFirst}$ and $\textsc{chooseNonMultiplier}$. These algorithms should have the following properties.

S1 If $\emptyset \neq U \subseteq T$ is a finite set of terms, $Y \subseteq X$, and $m = \textsc{chooseFirst}(Y, U)$ then $m \in U \cup \{\infty\}$.

S2 Let $\emptyset \neq V \subseteq T$ be a finite set of terms, $Y \subseteq X$, $m \in T \cup \{\infty\}$,

$$\forall v \in V\, \exists y \in Y : \deg_y v < \deg_y m$$

and $x = \textsc{chooseNonMultiplier}(Y, V, m)$. Then

$$x \in Y \wedge \exists v \in V : \deg_x v < \deg_x m.$$

One easily verifies that the input specifications are always satisfied when these functions are called in the generalised sliced division algorithm. By lines 6 and 7 of Algorithm 1 it follows $\forall v \in V\, \exists y \in Y : \deg_y v < \deg_y m$.

Theorem 3. *The generalised version of the algorithm* $\textsc{slicedDivision}$ *terminates and meets its specification.*

Proof. The proof of termination and correctness of the generalised version is similar to the proof of Theorem 1. In fact, our proof of Theorem 1 has been formulated in such a way that it can even be taken literally. One should note that the cases 2 and 3 at the end of the proof cannot occur if $m = \infty$, since in the proof $v_i, v_j \in U$, but $\infty \notin U$. $\square$

Remark 2. For given U and Y, one may think of ∞ as the term $m = \operatorname{lcm}(U) \prod_{y \in Y} y$ as it fulfils all conditions that we posed on ∞. Since the cone $m\langle Y\rangle$ is never returned and $\deg_y v < \deg_y m$ will be true for all $y \in Y$ and $v \in V$, such an assignment would not cause any problem.

We define a **generalised sliced division** to be a division which is induced by the output of a generalised sliced division algorithm.

7.2 Janet, Pommaret, and Thomas Divisions as Generalised Sliced Divisions

In this section, let $W \subseteq T$ be a finite set of terms and let $\sqsubset = <_{\text{invlex}}$ be the inverse lexicographical order on W. Let $\mathcal{J}$, $\mathcal{P}$, and $\mathcal{T}$ be the Janet, Pommaret, and Thomas division on W, respectively. They are admissible on $(W, \sqsubset)$.

We are going to present particular sub-algorithms such that the generalised form of Algorithm 1 computes one of the classical divisions if these sub-algorithms are used.

Definition 7. *Let $\emptyset \neq Y \subseteq X$ and $\emptyset \neq U, V \subseteq W$ finite sets of terms. Let $m \in T \cup \{\infty\}$ and assume $\forall v \in V\, \exists y \in Y : \deg_y v < \deg_y m$. We define the following functions.*

Janet case: *Let $\mathrm{CF}_{\mathcal{J}}(Y, U) := \max_{<_{\mathrm{lex}}} U$. Let $\mathrm{CNM}_{\mathcal{J}}(Y, V, m) := x_i$ where i is the smallest index such that $\deg_{x_i} v < \deg_{x_i} m$ for some $v \in V$.*

Pommaret case: *Let x_k be such that k is the smallest index of all variables of Y and let $U' := U \cap \langle (X \setminus Y) \cup \{x_k\}\rangle$ then $\mathrm{CF}_{\mathcal{P}}(Y, U)$ returns ∞ if $U' = \emptyset$, otherwise it returns the element of U' of smallest degree. Let $\mathrm{CNM}_{\mathcal{P}} := \mathrm{CNM}_{\mathcal{J}}$.*

Thomas case: *Let $\mathrm{CF}_{\mathcal{T}}(Y, U)$ return $l := \mathrm{lcm}(U)$ if $l \in U$ and $\deg_y t \leq \deg_y l$ for all $y \in Y$ and $t \in W$, otherwise let it return ∞. Let $\mathrm{CNM}_{\mathcal{T}}(Y, V, m) := x_i$ where i is the smallest index such that $\deg_{x_i} v < \deg_{x_i} m$ and $\deg_{x_i} v < \deg_{x_i}(\mathrm{lcm}\, W)$ for some $v \in V$.*

Definition 8. *Let $\mathcal{M}$ be a partial division and $\mathrm{CF}_{\mathcal{M}}$ and $\mathrm{CNM}_{\mathcal{M}}$ be functions satisfying **S1** and **S2** in place of the algorithms* CHOOSEFIRST *and* CHOOSENONMULTIPLIER, *respectively. The algorithm which is obtained from Algorithm 1 by replacing lines 4, 8, and 14 by*

4: $m := \mathrm{CF}_{\mathcal{M}}(Y, U)$
8: $x := \mathrm{CNM}_{\mathcal{M}}(Y, U, m)$
14: ***if*** $m \in U$ ***then return*** $\mathrm{CONCAT}(L_C, [m\langle Y\rangle], L)$ ***else return*** L

is called SLICEDDIVISION$_{\mathcal{M}}$.

It is trivial to check that the functions $\mathrm{CF}_{\mathcal{J}}$, $\mathrm{CF}_{\mathcal{P}}$, and $\mathrm{CF}_{\mathcal{T}}$ fulfil the property **S1**. $\mathrm{CNM}_{\mathcal{J}}$ and $\mathrm{CNM}_{\mathcal{P}}$ fulfil **S2**. For $\mathrm{CNM}_{\mathcal{T}}$ we must show that there is some $y \in Y$ and some $v \in V$ in line 8 such that $\deg_y v < \deg_y m$ and $\deg_y v < \deg_y(\mathrm{lcm}\, W)$. If $m \in W$, this follows by the input specification given in Definition 8. If $m = \infty$, it follows from the definition of $\mathrm{CF}_{\mathcal{T}}$.

Since SLICEDDIVISION$_{\mathcal{J}}$, SLICEDDIVISION$_{\mathcal{P}}$, and SLICEDDIVISION$_{\mathcal{T}}$ are generalised sliced division algorithms, by Theorem 3, they return admissible partial divisions.

Theorem 4. *Let $Y \subseteq X$, $U = \{u_1, \ldots u_r\} \subseteq W$. Let $\mathcal{M} = (t\langle X_t\rangle)_{t \in T}$ where $\mathcal{M}$ stands for the Janet division $\mathcal{J}$, the Pommaret division $\mathcal{P}$, or the Thomas division $\mathcal{T}$ on W. Let $\forall u \in U : X_u \subseteq Y$ and $[v_1\langle Y_{v_1}\rangle, \ldots, v_r\langle Y_{v_r}\rangle] =$ SLICEDDIVISION$_{\mathcal{M}}(Y, U)$. If $\mathcal{M} = \mathcal{P}$ is the Pommaret division then additionally assume that there exists $k \in \{1, \ldots, n\}$ such that $Y = \{x_k, \ldots, x_n\}$. Then $X_u = Y_u$ for all $u \in U$.*

Proof. The proof goes by induction on the cardinality of the input parameters Y and U. All line numbers will refer to SLICEDDIVISION$_{\mathcal{M}}$. For empty input parameters there is nothing to show. Now consider $Y \subseteq X$ and $U \subseteq W$ and assume that the theorem is proved for all calls of SLICEDDIVISION$_{\mathcal{M}}$ where the sum of the cardinalities of the input parameters is strictly less than $\operatorname{card} Y + \operatorname{card} U$. Let m, C, and V be as defined in lines 4–6. Let s be the number of iterations of the while loop, and let y_σ, d_σ, S_σ, and V_σ be the values of x, d, S, and V after the σ-th iteration ($\sigma = 1, \ldots, s$). By the input specification of $\text{SLICEDDIVISION}_{\mathcal{M}}$, there exists an element $w \in \langle X \setminus Y \rangle$ such that $U \subseteq W \cap w\langle Y \rangle$. For line 12 we find that $S_\sigma \subseteq y_\sigma^{d_\sigma} w \langle Y \setminus \{y_\sigma\} \rangle$, thus the input specification of $\text{SLICEDDIVISION}_{\mathcal{M}}$ is satisfied. There are two cases to consider.

$m \in U$: By line 14, $Y_m = Y$ will be returned, it remains to show $X_m = Y$. Since $\operatorname{card} C, \operatorname{card} V < \operatorname{card} U$, the correct assignment of multiplicative variables for the elements of $U \setminus \{m\}$ follows from the induction hypothesis if we can show that the assumptions of the theorem are satisfied in lines 5 and 12. For line 5 this is trivial, since $C \subsetneq U$ and Y does not change. Note that $C = \emptyset$ if $\mathcal{M} = \mathcal{J}$.

For the remaining considerations, we treat the various cases separately.

$\mathcal{M} = \mathcal{J}$: From the assumption of the theorem, $X_m \subseteq Y$. By definition of $\mathcal{J}$ and $\text{CF}_{\mathcal{J}}$, we must have $X_m = Y$. By $m = \max_{<_{\text{lex}}} U$, line 6, the choice of y_σ through $\text{CNM}_{\mathcal{J}}$, and from line 10 we conclude $\deg_{y_\sigma} v < \deg_{y_\sigma} m$ for all $v \in S_\sigma$. By definition of the Janet division, y_σ is non-multiplicative for all elements of S_σ. Hence, the theorem is applicable for $(Y \setminus \{y_\sigma\}, S_\sigma)$ in line 12.

$\mathcal{M} = \mathcal{T}$: From the assumption of the theorem, $X_m \subseteq Y$. By definition of $\mathcal{T}$ and $\text{CF}_{\mathcal{T}}$, we must have $X_m = Y$. By $m = \operatorname{lcm}(U)$, line 6, the choice of y_σ through $\text{CNM}_{\mathcal{T}}$, and from line 10 we conclude $\deg_{y_\sigma} v < \deg_{y_\sigma} m$ for all $v \in S_\sigma$. By definition of the Thomas division, y_σ is non-multiplicative for all elements of S_σ. Hence, the theorem is applicable for $(Y \setminus \{y_\sigma\}, S_\sigma)$ in line 12.

$\mathcal{M} = \mathcal{P}$: Let $U' = U \cap \langle (X \setminus Y) \cup \{x_k\} \rangle$. By definition of the Pommaret division, $X_u = Y$ for all $u \in U'$. By definition of $\text{CF}_{\mathcal{P}}$, $m = w x_k^a \in U'$ with the smallest possible a. Note that $U' \subseteq m\langle Y \rangle$. By the choice of m and line 6, it follows that for all $v \in V$ $\deg_{x_k} v < a$ and $\exists j > k : \deg_{x_j} v > 0$. Therefore $y_\sigma = x_k$ and $x_k \notin X_v$. Hence, the theorem is applicable for $(Y \setminus \{x_k\}, S_\sigma) = (\{x_{k+1}, \ldots, x_n\}, S_\sigma)$ in line 12.

$m = \infty$: This case does not occur if $\mathcal{M}$ is the Janet division. From lines 5 and 6 follows $C = \emptyset$ and $V = U$. Let $\sigma \in \{1, \ldots, s\}$. Correct assignment of the multipliers follows from the induction hypothesis applied to $(Y \setminus \{y_\sigma\}, S_\sigma)$ in line 12. We must show that the assumptions of the theorem are applicable.

If $\mathcal{M} = \mathcal{T}$ then $X_v \subseteq Y \setminus \{y_\sigma\}$ for all $v \in V$ follows from the definition of $\text{CNM}_{\mathcal{T}}$ and the definition of the Thomas division on W.

If $\mathcal{M}$ is the Pommaret division, we observe that $y_\sigma = x_k$ by $\text{CNM}_{\mathcal{P}}$ and that for all $v \in V$ there exists $j > k$ such that $\deg_{x_j} v > 0$, i.e., $X_v \subseteq \{x_{k+1}, \ldots, x_n\}$.

Hence, all assumptions of the theorem are satisfied in line 12 and we get $X_u = Y_u$ for all $u \in S_\sigma$ and consequently for all $u \in U$.

The theorem is proved. □

The following corollary states that Janet, Pommaret, and Thomas divisions are generalised sliced divisions.

Corollary 3. *Let $\mathcal{M}$ be the Janet, the Pommaret, or the Thomas division on W. Let $[v_1\langle Y_{v_1}\rangle, \ldots, v_r\langle Y_{v_r}\rangle] = \textsc{slicedDivision}_{\mathcal{M}}(X, W)$. $\mathcal{M}$ and the induced division of $(v\langle Y_v\rangle)_{v\in W}$ are W-equivalent.*

8 Computer Experiments

The involutive basis algorithm appears in various flavours in the literature, for example, [8], [1], [4]. Let us give here only a basic treatment which is necessary to understand our computer experiments. For more details we refer to the papers above.

In order to make the paper as self-contained as possible, we repeat here several definitions.

Definition 9. *Let $G \subseteq \mathbb{K}[X]$ be a set of polynomials. G is called an* ***involutive basis*** *if G is a Gröbner basis and $\operatorname{lt}(G)$ is complete (cf. Def. 4).*

A list of equivalent conditions can be found in [1].

Definition 10. *Let $G \subseteq \mathbb{K}[X]$ be a set of polynomials and let $\mathcal{M} = (M_t)_{t\in T}$ be a partial division. We say that $f \in \mathbb{K}[X]$ is in* ***$\mathcal{M}$-normal form*** *with respect to G if $\operatorname{supp} f \cap M_{\operatorname{lt} g} = \emptyset$ for every $g \in G \setminus \{0\}$.*

Obviously, this leads to a concept of restricted reduction; elements in G can only be multiplied by their respective multiplicative variables in order to reduce some term of f. The sub-algorithm $\mathrm{NF}_{\mathcal{M}}$ that computes an $\mathcal{M}$-normal form is similar to a normal form algorithm in a Gröbner basis computation where divisor and multiple is replaced by $\mathcal{M}$-divisor and $\mathcal{M}$-multiple. For example, if $G = \{x^2, y^2\}$ and $\mathcal{M}$ denotes the Janet division on $\operatorname{lt} G$. Then $\mathrm{NF}_{\mathcal{M}}(xy^2, G) = xy^2$ since there is no $\mathcal{M}$-divisor of xy^2 in $\operatorname{lt} G$.

The basic form of the involutive basis algorithm is given in Algorithm 2. The different approaches for a definition of an admissible partial division [2] and an involutive division [4] are reflected in the sub-algorithm $\textsc{partialDivision}$. Termination of $\textsc{involutiveBasis}$ is ensured by Apel through the requirement that $\mathcal{M}$ be an admissible partial division on $\operatorname{lt}(G)$ that refines the Thomas division on $\operatorname{lt}(G)$. Gerdt and Blinkov require that $\textsc{partialDivision}$ returns a constructive involutive division (cf. definition in [4]). Our Algorithm 2 incorporates already some statements (reflected by the set P in lines 1, 6, and 11) to avoid multiple reductions of the same prolongation. We refer to [1] for conditions on $\textsc{partialDivision}$ such that Algorithm 2 will be correct. While the Janet division fulfils these conditions, the algorithm $\textsc{slicedDivision}$ does not. In order to yield an involutive basis, Algorithm 2 is iterated until all elements of C from line 3 immediately reduce to zero. Termination follows from the fact that $\textsc{slicedDivision}$ refines the Thomas division (cf. [1]). We denote this iterated algorithm by $\textsc{ibsd}$.

Algorithm 2 INVOLUTIVEBASIS

Call: $G = \textsc{involutiveBasis}(F)$

Input: $F \subset K[X] \setminus \{0\}$ is a finite set of polynomials.

Output: G is an involutive basis of the ideal of F in $\mathbb{K}[X]$.

$G := F; \quad P := \emptyset$
$\mathcal{M} := (t\langle Y_t \rangle)_{t \in \mathrm{lt}(G)} := \textsc{partialDivision}(\mathrm{lt}\, G)$
$C := \{xg \mid g \in G \wedge x \in X \setminus Y_{\mathrm{lt}\, g}\}$
<u>while</u> $C \neq \emptyset$ <u>do</u>
  Choose smallest (w.r.t. the term order) p from C
  $C := C \setminus \{p\}; \quad P := P \cup \{p\}$
  $h := \mathrm{NF}_{\mathcal{M}}(p, G)$
  <u>if</u> $h \neq 0$ <u>then</u>
    $G := G \cup \{h\}$
    $\mathcal{M} := (t\langle Y_t \rangle)_{t \in \mathrm{lt}(G)} := \textsc{partialDivision}(\mathrm{lt}\, G)$
    $C := \{xg \mid g \in G \wedge x \in X \setminus Y_{\mathrm{lt}\, g}\} \setminus P$
<u>return</u> G

If in Algorithm 2 PARTIALDIVISION returns the Janet division, it is denoted by JB. If PARTIALDIVISION returns a sub-maximally refined (cf. [1]) Janet division, we denote Algorithm 2 by JBR.

The algorithm INVOLUTIVEBASIS presented in [4] where the Janet division is used, is denoted by JBC. This algorithm incorporates some improvements to Algorithm 2, in particular a variant of Buchberger's chain criterion is applied. Since the other, above mentioned, algorithms do not use criteria, we denote by JBW the algorithm JBC without application of criteria.

We have programmed a package CALIX[1] in the programming language ALDOR[2] to investigate all the above algorithms.

We have selected the well-known Cyclic4 and Cyclic6 examples as they appear in many collections of polynomial data[3]. They can also be found in [4].

We computed here involutive bases with respect to the degree inverse lexicographical order where first degrees are compared and ties are broken by $<_{\mathrm{invlex}}$. With respect to that term order, the (minimal) Janet bases of the above examples have much more elements than the reduced Gröbner bases which are 7 and 45, respectively.

Let us start with Cyclic4.

[1] `http://www.hemmecke.de/calix`
[2] `http://www.aldor.org`
[3] for example: `http://www.symbolicdata.org`

Cyclic4	Length	Prolong.	Reductions	Zeros
JBW	37	91	253	51
JB	37	82	254	49
JBR	29	61	198	35
JBC	37	47	**63**	**7**
IBSD	**7**	**34** (27)	194 (146)	28 (21)

The first column denotes the algorithm, the second contains the length of the involutive basis, the third contains the number of prolongations that have actually been reduced. The fourth column presents the number of elementary reductions, i. e., head reductions of the form $f \longrightarrow f - ctg$ for some coefficient c, some term t and a simplifier polynomial g. The last column counts the number of reductions to zero.

As can be seen from the JBR line, a submaximal refinement of the Janet division can result in a smaller involutive basis. The involutive basis is even smaller for IBSD. The numbers for IBSD include the fact that 2 iterations of Algorithm 2 have been performed. The values in parentheses incorporate the fact that one need not redo zero reductions in the next iteration after the last polynomial has been added to the basis.

For Cyclic6 the number of involutive basis elements differs even more between IBSD and the other algorithms.

Cyclic6	Length	Prolong.	Reductions	Zeros
JBW	385	20572	280696	11964
JB	840	3769	200522	2935
JBR	385	2912	106568	2160
JBC	385	9947	66910	1339
IBSD	**46**	**1104** (1044)	**48959** (45985)	**923** (863)

Surprisingly, the fact that by means of SLICEDDIVISION fewer polynomials are necessary to complete the basis than by using the Janet division, IBSD behaves better even against the Janet basis algorithm JBC which incorporates a variant of the chain criterion.

9 Conclusion

Apel suggested in [1] to use a maximally or sub-maximally refined division in an involutive basis algorithm. Our experiments seem to support this. However, instead of requiring a $\sqsubset$ ordering from the beginning and computing a sub-maximally refined partial division admissible with respect to that order, we compute with SLICEDDIVISION a partial division and an order $\sqsubset$ for which this division is admissible.

In our approach we use a sliced division in order to try to minimise the number of (non-multiplicative) prolongations that must be considered in the course of the involutive basis algorithm. Take, for example, x^7, xy, y^7. This is already an involutive basis with respect to a sliced division. No matter which order of the variables we use, in a Janet basis xy will not get the full cone and thus the basis will contain 8 elements.

One drawback of using SLICEDDIVISION is that Algorithm 2 must be iterated. Since sliced division is actually a whole class of admissible partial divisions, we will try to impose further conditions such that it is enough to consider each prolongation only once during an involutive basis computation or to find a connection between the division and the prolongations that must be reconsidered.

Acknowledgement. This work was supported by the Austrian Science Foundation (FWF), SFB F013, project 1304. I am grateful to Joachim Apel for valuable discussions on the subject of involutive bases. I also thank Raymond Hemmecke for his helpful feedback on earlier versions of this article.

References

1. Joachim Apel. The theory of involutive divisions and an application to Hilbert function computations. *Journal of Symbolic Computation*, 25(6):683–704, June 1998.
2. Joachim Apel. *Zu Berechenbarkeitsfragen der Idealtheorie.* Habilitationsschrift, Universität Leipzig, Fakultät für Mathematik und Informatik, Augustusplatz 10–11, 04109 Leipzig, 1998.
3. Bruno Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N. K. Bose, editor, *Recent Trends in Multidimensional Systems Theory*, chapter 6, pages 184–232. D. Reidel Publishing Company, Dordrecht, The Netherlands, 1985.
4. Vladimir P. Gerdt and Yuri A. Blinkov. Involutive bases of polynomial ideals. *Mathematics and Computers in Simulation*, 45:519–541, 1998.
5. Maurice Janet. Les systèmes d'équations aux dérivées partielles. *Journal de Mathematique. 8e série*, 3:65–151, 1920.
6. Jean-François Pommaret. *Systems of Partial Differential Equations and Lie Pseudogroups*, volume 14 of *Mathematics and Its Applications.* Gordon and Breach Science Publishers, Inc., One Park Avenue, New York, NY 10016, 1978.
7. Joseph Miller Thomas. *Differential Systems.* American Mathematical Society, New York, 1937.
8. A. Yu. Zharkov and Yuri A. Blinkov. Involution approach to solving systems of algebraic equations. In G. Jacob, N. E. Oussous, and S. Steinberg, editors, *Proceedings of the 1993 International IMACS Symposium on Symbolic Computation*, pages 11–16. IMACS, Laboratoire d'Informatique Fondamentale de Lille, France, 1993.