ELSEVIER

Mathematics and Computers in Simulation 45 (1998) 543–560

MATHEMATICS AND COMPUTERS IN SIMULATION

Minimal involutive bases

Vladimir P. Gerdt[a,*], Yuri A. Blinkov[b]

[a] *Joint Institute for Nuclear Research, 141980 Dubna, Russian Federation*
[b] *Saratov University, 410071 Saratov, Russian Federation*

Abstract

In this paper, we present an algorithm for construction of minimal involutive polynomial bases which are Gröbner bases of the special form. The most general involutive algorithms are based on the concept of involutive monomial division which leads to partition of variables into multiplicative and non-multiplicative. This partition gives thereby the self-consistent computational procedure for constructing an involutive basis by performing non-multiplicative prolongations and multiplicative reductions. Every specific involutive division generates a particular form of involutive computational procedure. In addition to three involutive divisions used by Thomas, Janet and Pommaret for analysis of partial differential equations we define two new ones. These two divisions, as well as Thomas division, do not depend on the order of variables. We prove noetherity, continuity and constructivity of the new divisions that provides correctness and termination of involutive algorithms for any finite set of input polynomials and any admissible monomial ordering. We show that, given an admissible monomial ordering, a monic minimal involutive basis is uniquely defined and thereby can be considered as canonical much like the reduced Gröbner basis. © 1998 IMACS/Elsevier Science B.V.

Keywords: Computer algebra; Polynomial ideals; Gröbner bases; Involutive monomial division; Minimal involutive bases; Involutive algorithm

1. Introduction

Computational aspects of constructing Gröbner bases invented by Buchberger [1] are now under intensive investigation due to the great theoretical and practical importance of these bases in computational commutative algebra and algebraic geometry [2–4]. Gröbner bases are also becoming of greater importance in non-commutative [5–7] and differential algebra [8,9].

Since its invention about thirty years ago, feasibility of the Buchberger algorithm has been notably increased. First of all, it was resulted from discovering criteria for avoiding unnecessary reductions [10–12] which allow a partial extension to non-commutative case [7]. Next, the key role of the reduction and, especially, selection strategies was experimentally observed, and heuristically good

[*] Corresponding author.

PII S0378-4754(97)00128-6

strategies were found [13]. For construction of a lexicographical Gröbner basis, which is the most useful for solving polynomial equations, an efficient computation scheme was developed in [14] based on converting a basis from one ordering into another.

On the other hand, Zharkov and Blinkov [15] were pioneered in revealing another computational scheme for Gröbner bases construction in commutative algebra. They used the partition of variables into multiplicative and non-multiplicative invented in Pommaret [16] to bring partial differential equations into so-called involutive form [17] which has all the integrability conditions satisfied. Zharkov and Blinkov showed that sequential multiplication of the polynomials in the system by non-multiplicative variables, and reduction of these prolonged polynomials modulo others, by means of their multiplicative power products only, ends up, under certain conditions, with a Gröbner basis. Though the latter is generally not the reduced basis, it reveals some attractive features [18].

Already first computer experiments carried out in [15] showed rather high efficiency of the new computational scheme. However, that algorithm terminates, generally, only for zero-dimensional ideals and for degree compatible term orderings [19]. The algebraic origin of such an algorithmic behavior was analyzed in [20] where it was also shown that Pommaret involutive bases are just Gröbner ones of ideals in the commutative rings with respect to non-commutative gradings. Interconnection of Pommaret bases and Gröbner bases was recently investigated also in [21].

In our previous paper [22], general algorithmic foundations of involutive approach to commutative algebra were considered, and a number of new concepts was introduced allowing one to study the involutive algorithmic procedure in its general form. The central concept of our analysis is involutive monomial division. Every specific involutive division generates some particular computation procedure for constructing the corresponding involutive basis. Every involutive basis, if it is finite, was proved to be a Gröbner basis, generally, redundant. We formulated the axiomatic properties of an involutive division which provide a proper partition of variables into multiplicative and non-multiplicative, and, hence, to construct different divisions. It was also proved that those partitions used by Janet [17], Thomas [23] and Pommaret [16] are generated by particular involutive divisions.

Important properties of noetherity, continuity and constructivity for an involutive division were also characterized. Noetherity provides for the existence of a finite involutive monomial basis for any monomial ideal much like to the conventional monomial bases. Continuity assures involutivity of every locally involutive set. Constructivity is a strengthening of continuity. It allows one to compute an involutive monomial basis from the initial one by means of its enlargement with single non-multiplicative prolongations only, that is, to avoid enlargement with multiplicative prolongations. We showed that Janet and Thomas divisions are noetherian, continuous and constructive whereas Pommaret division, being continuous and constructive, is not noetherian. Just by this reason a positive-dimensional polynomial ideal, generally, does not have a finite Pommaret basis. We presented in [22] a general form of the involutive algorithm. Its correctness follows from continuity of a division while termination holds for any polynomial ideal and for any admissible monomial ordering only for noetherian divisions. The algorithm involves the Buchberger's chain criterion to avoid unnecessary reductions.

In the present paper, in addition to Janet, Thomas and Pommaret divisions analyzed in [22], we give examples of two more involutive divisions which are proved to be continuous, constructive and noetherian. We present also the special form of an involutive algorithm which, given a constructive noetherian division, provides computation of a minimal involutive basis. We show that the monic form of the latter is uniquely defined for any fixed admissible monomial ordering.

The rest of the paper is organized as follows. In Section 2, we give a brief review of involutive concepts and methods which are used in the following sections. In Section 3, we consider some examples of involutive monomial divisions including those introduced by Thomas, Janet and Pommaret along with two new ones. In Section 4, we study the minimal involutive monomial bases. The algorithm for construction of minimal polynomial bases is described in Section 5, and some concluding remarks are given in Section 6.

2. Background of involutive approach

In this section, we briefly describe the fundamentals of the general involutive approach proposed in [22] which are used in Sections 3–5.

Let $\mathbb{N}$ be a set of non-negative integers, and $\mathbb{M} = \left\{x_1^{d_1} \cdots x_n^{d_n} | d_i \in \mathbb{N}\right\}$ be a set of monomials in the polynomial ring $\mathbb{R} = K[x_1, \ldots, x_n]$ over zero characteristic field K.

By deg(u) and deg$_i$(u) we denote the total degree of $u \in \mathbb{M}$ and the degree of variable x_i in u, respectively. An admissible monomial ordering is denoted by $\succ$, and throughout this paper we shall assume that

$$x_1 \succ x_2 \succ \cdots \succ x_n \tag{1}$$

The leading monomial and the leading coefficient of polynomial $f \in \mathbb{R}$ with respect to ordering $\prec$ are denoted by lm(f) and lc(f), respectively. If $F \subset \mathbb{R}$ is a polynomial set, then by lm(F) we denote the leading monomial set for F, and Id(F) will denote the ideal in R generated by F. For the least common multiple and for the greatest common divisor of two monomials $u, v \in \mathbb{M}$ we shall use the conventional notations lcm(u,v) and gcd(u,v), respectively. If monomial u divides monomial v we shall write $u|v$.

Definition 2.1 An *involutive division* L on $\mathbb{M}$ is given, if for any finite monomial set $U \subset \mathbb{M}$ and for any $u \in U$ there is given a submonoid $L(u, U)$ of $\mathbb{M}$ satisfying the conditions:

(a) If $w \in L(u,U)$ and $v|w$, then $v{\in}L(u,U)$
(b) If $u,v \in U$ and $uL(u,U) \cap vL(v,U) \neq \emptyset$, then $u{\in}vL(v,U)$ or $v \in uL(u,U)$
(c) If $v{\in}U$ and $v{\in}\, uL(u,U)$, then $L(v,U)\ {\subseteq}L(u,U)$
(d) If $V \subseteq U$, then $L(u,U) \subseteq L(u,V)$ for all $u \in V$

Elements of $L(u,U)$ are called *multiplicative* for u. If $w \in uL(u,U)$ we shall write $u|_L w$ and call u ($L-$)*involutive divisor* of w. The monomial w in its turn is called ($L-$)*involutive multiple* of u. In such an event monomial $v = w/u$ is *multiplicative* for u and the equality $w = uv$ will be written as $w{=}\ u{\times}v$. If u is the conventional divisor of w but not involutive one we shall write, as usual, $w{=}\ u{\cdot}v$. Then v is said to be *non-multiplicative* for u.

Definition 2.2 We shall say that involutive division L is *globally defined* if for any $u \in \mathbb{M}$ its multiplicative monomials are defined irrespective of the monomial set $U \ni u$, that is, if $L(u,U) = L(u)$.

Definition 2.1 for every $u{\in}\ U \subset \mathbb{M}$ provides the partition

$$\{x_1, \ldots, x_n\} = M_L(u, U) \cup NM_L(u, U), \quad M_L(u, U) \cap NM_L(u, U) = \emptyset \tag{2}$$

of the set of variables into two subsets: *multiplicative* $M_L(u,U) \subset L(u,U)$ and *non-multiplicative* $NM_L(u,U) \notin L(u,U)$. Conversely, if for any finite set $U \in \mathbb{M}$ and any $u \in U$ the partition (2) is given such that the corresponding submonoid $L(u,U)$ of monomials in variables in $M_L(u,U)$ satisfies the conditions (b)–(d), then the partition generates the involutive division.

The conventional monomial division, obviously, satisfies condition (b) only in the univariate case.

In what follows monomial sets are assumed to be finite, unless involutive division L is globally defined. In this case, since L is defined irrespective to the monomial set, it admits extension to infinite sets.

Definition 2.3 A monomial set $U \in \mathbb{M}$ is *involutively autoreduced* or *L-autoreduced* if the condition $uL(u,U) \cap vL(v,U) = \emptyset$ holds for all distinct $u,v \in U$.

Definition 2.4 Given an involutive division L, a monomial set U is *involutive*[1] with respect to L or L-involutive if

$$\cup_{u \in U} u\mathbb{M} = \cup_{u \in U} uL(u,U) \tag{3}$$

Definition 2.5 An L-involute monomial set $\tilde{U}$ is called *L-completion* of a set $U \subseteq \tilde{U}$ if

$$\cup_{u \in U} u\mathbb{M} = \cup_{u \in \tilde{U}} uL(u,U)$$

If there exists a finite L-completion $\tilde{U}$ of a finite set U, then the latter is *finitely generated* with respect to L. The involutive division L is *noetherian* if every finite set U is finitely generated.

Proposition 2.6 [22] *If involutive division L is noetherian, then every monomial ideal has a finite involutive basis* $\tilde{U}$.

Proposition 2.7 *If U is a finitely generated monomial set, then so is set obtained by autoreduction of U in the sense of the conventional monomial division.*

Proof It follows immediately from observation that any involutive completion of U is also an involutive completion of its autoreduced subset.

Definition 2.8 A monomial set U is called *locally involutive* with respect to the involutive division L if

$$(\forall u \in U)(\forall x_i \in NM_L(u,U))(\exists v \in U)[v|_L(u \cdot x_i)].$$

Definition 2.9 A division L is called *continuous* if for any finite set $U \in \mathbb{M}$ and for any finite sequence $\{u_i\}_{(1 \le i \le k)}$ of element in U such that

$$(\forall i < k)(\exists x_j \in NM_L(u_i,U))[u_{i+1}|_L u_i \cdot x_j] \tag{4}$$

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

[1] Janet [17] and Thomas [23] call such sets *complete*.

Theorem 2.10 [22] *If involutive division L is continuous then local involutivity of any monomial set U implies its involutivity.*

Definition 2.11 A continuous involutive division L is *constructive* if for any $U \subset \mathbb{M}, u \in U$, $x_i \in NM_L(u, U)$ such that $u \cdot x_i$ has no involutive divisors in U and

$$(\forall v \in U)\big(\forall x_j \in NM_L(v, U)\big)\big(v \cdot x_j | u \cdot x_i,\ v \cdot x_j \neq u \cdot x_i\big)\big[v \cdot x_j \in \cup_{u \in U} uL(u, U)\big]$$

the following condition holds:

$$(\forall w \in \cup_{u \in U} uL(u, U)[u \cdot x_i \notin wL(w, U \cup \{w\})] \tag{5}$$

Given a finite set of polynomials $F \subset \mathbb{R}$ and an admissible ordering $\succ$, multiplicative and non-multiplicative variables for $f \in F$ are defined in terms of lm(f) and the leading monomial set lm(F).

The concepts of involutive polynomial reduction and involutive normal form are introduced similar to their conventional analogues [11] with the use of involutive division instead of the conventional one.

Definition 2.12 Let L be an involutive division L on $\mathbb{M}$, and let F be a finite set of polynomials. Then we shall say:

(i) p is *L-reducible modulo* $f \in F$ if p has a term $t = au \in \mathbb{T}(a \neq 0)$ such that $u = \mathrm{lm}(f) \times v$, $v \in L(\mathrm{lm}(f), \mathrm{lm}(F))$. It yields the *L-reduction* $p \rightarrow g = p - (a/lc(f))fv$.
(ii) p is *L-reducible modulo F* if there exists $f \in F$ such that p is L-reducible modulo f.
(iii) p is *in L-normal form modulo F* if p is not L-reducible modulo F.

We denote the L-normal form of p modulo F by $NF_L(p, F)$. In contrast, the conventional normal form will be denoted by $NF(p,F)$. If monomial u is multiplicative to $\mathrm{lm}(f)(f \in F)$, and $h{=}fu$ we shall write $h{=}f{\times}u$.

Definition 2.13 A finite polynomial set F is *L-autoreduced* if the leading monomial set lm(F) of F is L-autoreduced and every $f \in F$ does not contain involutively multiple of any element in lm(F).

Theorem 2.14 [22] If set $F \subset \mathbb{R}$ *is L-autoreduced, then* $NF_L(p, F) = 0$ *iff* $p \in \mathbb{R}$ *is presented in the form* $p = \sum_{ij} c_i f_i \times u_{ij}$, *where* $f_i \in F$, $c_i \in K$, and $u_{ij} \in L(\mathrm{lm}(F),\ \mathrm{lm}(F))$ *are such that* $u_{ij} \neq u_{ik}$ *for* $i \neq k$.

Corollary 2.15 [22] *If polynomial set F is L-autoreduced, then $NF_L(p, F)$ is uniquely defined for any $p \in \mathbb{R}$, and $NF_L(p_1 + p_2, F) = NF_L(p_1, F) + NF_L(p_2, F)$*

Definition 2.16 *An L*-autoreduced set F is called $(L-)$ *involutive if*

$$(\forall f \in F)\,(\forall u \in \mathbb{M})\,[NF_L(fu, F) = 0]$$

Given $v \in \mathbb{M}$ and an L-autoreduced set F, if there exist $f \in F$ such that $\mathrm{lm}(f) \prec v$ and

$$(\forall f \in F)\,(\forall u \in \mathbb{M})\,(\mathrm{lm}(f) \cdot u \prec v)\,[NF_L(fu, F) = 0] \tag{6}$$

then F is called *partially involutive up to the monomial v* with respect to the admissible ordering $\prec$. F is still said to be partially involutive up to v if $v \prec \mathrm{lm}(f)$ for all $f \in F$.

Theorem 2.17 [22] *An L-autoreduced set $F \subset \mathbb{R}$ is involutive with respect to a continuous involutive division L iff the following (local) involutivity conditions hold*

$$(\forall f \in F)\, (\forall x_i \in NM_L(\mathrm{lm}(f), \mathrm{lm}(F)))\, [NF_L(f \cdot x_i, F) = 0]$$

Correspondingly, partial involutivity (6) *holds iff*

$$(\forall f \in F)\, (\forall x_i \in NM_L(\mathrm{lm}(f),\, \mathrm{lm}(F)))(\mathrm{lm}(f) \cdot x_i \prec v)[NF_L(f \cdot x_i, F) = 0]$$

Theorem 2.18 [22] *If $F \subset \mathbb{R}$ is an L-involutive basis, then it is also a Gröbner basis, and the equality of the conventional and L-normal forms $NF(p, F) = NF_L(p, F)$ holds for any polynomial $p \in \mathbb{R}$. If set F is partially involutive up to the monomial v, then the equality of the normal forms $NF(p, F) = NF_L(p, F)$ holds for any $p \in \mathbb{R}$* such that $\mathrm{lm}(p) \prec v$.

Theorem 2.19 [22] *Let F be a finite L-autoreduced polynomal set, and let $g{\cdot}x$ be a non-multiplicative prolongation of $g \in F$. Then $NF_L(g \cdot x, F) = 0$ if the following holds*

$$(\forall h \in F)\, (\forall u \in \mathbb{M})\, (\mathrm{lm}(h) \cdot u \prec \mathrm{lm}(g \cdot x))\, [NF_L(h \cdot u, F) = 0]$$

$$(\exists f, f_0, g_0 \in F) \begin{bmatrix} \mathrm{lm}(f_0)|\mathrm{lm}(f),\ \mathrm{lm}(g_0)|\mathrm{lm}(g) \\ \mathrm{lm}(f)|_L \mathrm{lm}(g \cdot x),\ \mathrm{lcm}(f_0, g_0) \prec \mathrm{lm}(g \cdot x) \\ NF_L(f_0 \cdot \frac{\mathrm{lt}(f)}{\mathrm{lt}(f_0)}, F) = NF_L(g_0 \cdot \frac{\mathrm{lt}(g)}{\mathrm{lt}(g_0)}, F) = 0 \end{bmatrix}$$

3. Examples of involutive divisions

First of all, we give three examples of involutive division used in [16,17,23] for analysis of algebraic differential equations. For the proof of validity of properties (b)–(d) in Definition 2.1 for these divisions we refer to [22].

Example 3.1 Thomas division [23]. Given a finite set $U \subset \mathbb{M}$, the variable x_i is considered as multiplicative for $u \in U$ if $\deg_i(u) = \max\{\deg_i(v) | v \in U\}$, and non-multiplicative, otherwise.

Example 3.2 Janet division [17]. Let set $U \subset \mathbb{M}$ be finite. For each $1 \leq i \leq n$ divide U into groups labeled by non-negative integers $d_1, \ldots, d_i$:

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

A variable x_i is multiplicative for $u \in U$ if $i=1$ and $\deg_1(u) = \max\{\deg_1(v) | v \in U\}$, or if $i > 1$, $u \in [d_1, \ldots, d_{i-1}]$ and $\deg_i(u) = \max\{\deg_i(v) | v \in [d_1, \ldots, d_{i-1}]\}$.

Example 3.3 Pommaret division [16]. For a monomial $u = x_1^{d_1} \cdots x_k^{d_k}$ with $d_k > 0$ the variables x_j, $j \geq k$ are considered as multiplicative and the other variables as non-multiplicative. For $u=1$ all the variables are multiplicative.

Now we present two more examples of divisions which, as does Thomas division, do not rest on the variable ordering.

Example 3.4 Division I. Let U be a finite monomial set. The variable x_i is non-multiplicative for $u\in U$ if there is $v\in U$ such that

$$x_{i_1}^{d_1}\cdots x_{i_m}^{d_m}u = \mathrm{lcm}(u,v),\ 1\le m\le [n/2],\ d_j>0(1\le j\le m),$$

and $x_i\in\{x_{i_1},\dots,x_{i_m}\}$

Example 3.5 Division II. For monomial $u=x_1^{d_1}\cdots x_k^{d_n}$ the variable x_i is multiplicative if $d_i=d_{\max}(u)$ where $d_{\max}(u)=\max\{d_1,\dots,d_n\}$.

To distinguish the above divisions, the related subscripts T,J,P,I,II will be used. We note that

- Thomas division, Divisions I and II do not depend on the ordering on the variables x_i. Two other divisions, as defined, are based on the ordering (1).
- Pommaret division and Division I are globally defined in accordance with Definition 2.1, and, hence, admit extension to infinite monomial sets.

Proposition 3.6 *Divisions* I *and* II *are involutive*

Proof *Division* I. First of all, we prove that the condition (b) in Definition 2.1 is fulfilled. Let $u\neq v$ be elements in U such that $u|_I w$ and $v|_I w$ for some $w\in\mathbb{M}$. If $u|_I v$ or $v|_I u$, then we are done. Otherwise, lcm(u,v)/u or lcm(u,v)/v contains non-multiplicative variable for u or v, respectively. Because $\mathrm{lcm}(u,v)|w$, it follows that w cannot be involutively multiple of both u and v.

Consider now $u\in U$ such that $u|_I v$ for some $v\in U$, and $v\neq u$. Suppose $v|_I w$ for some $w\in\mathbb{M}$, and assume for a contradiction that w is not involutively multiple of u. Then there are variables $x_{i_1},\dots,x_{i_m}(1\le m\le[n/2])$ containing in w/v which are non-multiplicative for u and there is $t\in U$ such that $ux_{i_1}^{k_1}\cdots x_{i_m}^{k_m}=\mathrm{lcm}(u,t)$. Because v/u does not contain $x_{i_1},\dots,x_{i_m}$ it follows $vx_{i_1}^{k_1}\cdots x_{i_m}^{k_m}=\mathrm{lcm}(v,t)$ that contradicts our assumption that $w\in vL(v,U)$ and proves the fulfilment of condition (c).

The condition (d) holds too, since an enlargement of the set U may, obviously, only produce extra non-multiplicative variables for any $u\in U$.

Division II. Let u with $d_u=d_{\max}(u)$ be an involutive divisor of some monomial $w\in\mathbb{M}$. Then, by definition, $\deg_i(u)=\min(\deg_i(w),d_u)$ $(1\le i\le n)$. Thus, given monomial w and number d_u such that $d_u\le d_w$ where $d_w=d_{\max}(w)$, the corresponding involutive divisor u of w is uniquely defined. If there are two involutive divisors u,v of w with $d_u<d_v$, then it follows that

$$\begin{array}{ll} \deg_i(u)=\deg_i(v)=\deg_i(w) & \text{if } \deg_i(w)\le d_u \\ d_u<\deg_i(v)=\min(\deg_i(w),d_v) & \text{if } \deg_i(w)>d_u \end{array}$$

Hence, u is involutive divisor of v and the condition (b) is fulfilled.

The condition (c) is an easy consequence of the relation $\deg_i(u)=\min(\deg_i(v),d_u)$ and $\deg_i(v)=\min(\deg_i(w),d_v)$.

The condition (d) holds trivially, because the division as well as Pommaret one does not depend on monomial set U at all. □

Table 1

Monomial	Thomas		Janet		Pommaret		Division I		Division II	
	M_T	NM_T	M_J	NM_J	M_P	NM_P	M_{I}	NM_{I}	M_{II}	NM_{II}
x^2	x	y,z	x,y,z	–	x,y,z	–	x	y,z	x	y,z
xy	y	x,z	y,z	x	y,z	x	y	x,z	x,y	z
z	z	x,y	y,z	x	z	x,y	y,z	x	z	x,y

Proposition 3.7 *For any finite monomial set U and any monomial $u \in U$, the inclusion $M_T(u,U) \subseteq M_I(u,U)$ and, respectively, $NM_I \subseteq NM_T(u,U)$ holds.*

Proof If $x_i \in NM_I(u,U)$, then, obviously, $\deg_i(u) < h_i = \max\{\deg_i(u) | u \in U\}$, and, hence $x_i \in NM_T(u,U)$. □

Example 3.8 $U = \{x^2, xy, z\}$ $(x \succ y \succ z)$. Table 1

Proposition 3.9 *Divisions given by Examples* 3.1–3.5 *are continuous and constructive. All these divisions except that of Pommaret are also noetherian.*

Proof The proof for Thomas, Janet and Pommaret divisions is given in [22]. Consider Divisions I and II.

Continuity. Let u be a finite set, and $\{u_i\}_{(1\leq i\leq M)}$ be a sequence of elements in U satisfying the conditions (4). In accordance with Definition 2.9, we shall show that there are no coinciding elements in the sequence for each of the two divisions. There are the following two alternatives:

$$(i) \quad u_i = u_{i-1}\cdot x_j; \qquad (ii) \quad u_i \neq u_{i-1}\cdot x_j \tag{7}$$

Extract from the sequence $\{u_i\}$ the subsequence $\{t_k \equiv u_{i_k}\}_{(1\leq k\leq K\leq M)}$ of those elements which occur in the left-hand side of relation (ii) in (7).

Division I. Show that $t_k|_l \mathrm{lcm}(t_{k-1},t_k)$ and $t_k \neq \mathrm{lcm}(t_{k-1},t_k)$. We have $t_k \times \tilde{w}_k = u_{i_k-1}\cdot x_{j_k} = t_{k-1}\cdot \tilde{v}_{k-1}$ where $\neg\tilde{w}_k|\tilde{v}_{k-1}$. Indeed, suppose $\tilde{w}_k|\tilde{v}_{k-1}$. Apparently, this implies the relation $t_k = u_l\cdot z_l$ where $i_{k-1}\leq l < i_k$, and the variable $x_{j_l} \in NM_I(u_l,U)$, which figures in Definition 2.9 of the sequence $\{u_i\}$, satisfies $x_{j_l}|\tilde{w}_k$ and $\neg x_{j_l}|z_l$. It follows that $\mathrm{lcm}(t_k,u_{l+1}) = t_k x_{ji}$ what, in accordance with definition of the division in Example 3.4, contradicts multiplicativity of x_{j_l} for t_k. Therefore, we obtain the relation

$$\begin{cases} t_k\cdot v_k = t_{k+1}\times w_{k+1} \\ \gcd(v_k,w_{k+1}) = \gcd(v_k,w_k) = 1 \end{cases} \tag{8}$$

where w_{k+1} contains more then $[n/2]$ variables with positive exponents, and, hence, v_k contains only non-multiplicative variables for t_k.

We claim now that any v_j occurring in (8) with $j{>}k$ as well as v_k contain only non-multiplicative variables for t_k. For $j = k+1$, we multiply $t_k v_k$ by v_{k+1}

$$\begin{cases} t_k v_k u_{k+1} = (t_{k+1}\cdot v_{k+1})w_{k+1} = (t_{k+2}\times w_{k+2})w_{k+1}, \\ \gcd(v_k,w_{k+1}) = \gcd(v_{k+1},w_{k+1}) = \gcd(v_{k+1},w_{k+2}) = 1. \end{cases}$$

It yields

$$\begin{cases} t_k\hat{v}_k v_{k+1} = (t_{k+2} \times \hat{w}_{k+2})w_{k+1}, \\ \gcd(\hat{v}_k v_{k+1}, \hat{w}_{k+2}w_{k+1}) = 1 \end{cases} \tag{9}$$

Because w_{k+1} contains more than $[n/2]$ variables, the number of variables occurring in the product $\hat{v}_k v_{k+1}$ is less or equal $[n/2]$, and thus, variables which are multiplicative for t_k are not contained in v_{k+1}.

If we proceed, sequentially multiplying the upper equality in Eq. (9) by $v_{k+j}(j = 2, \ldots)$, rewriting the right-hand side of every product in terms of t_{k+j+1} and cancelling the common factors, then we obtain the equality

$$\begin{cases} t_k\hat{v}_k \cdots \hat{v}_{k+j-1}v_{k+j} = (t_{k+j+1} \times \hat{w}_{k+j+1})\hat{w}_{k+1} \cdots \hat{w}_{k+j-1}w_{k+j} \\ \gcd(\hat{v}_k \cdots \hat{v}_{k+j-1}v_{k+j}, \hat{w}_{k+j+1}\hat{w}_{k+1} \cdots \hat{w}_{k+j-1}w_{k+j}) = 1 \end{cases}$$

It proves the claim and implies $t_i \neq t_j$ for $i \neq j$.

It remains to prove that elements of the sequence $\{u_i\}_{(1\leq i\leq M)}$ which occur in the left-hand side of relation (i) in (7) are also distinct. Assume for a contradiction that there are two elements $u_j = u_k$ with $j<k$. In between these elements there is, obviously, an element from the left-hand side of relation (ii) in (7). Let $u_{i_m}(j < i_m < k)$ be the nearest such element to u_j. Considering the same non-multiplicative prolongations of u_k as those of u_j in the initial sequence, one can construct a sequence such that the subsequence of the left-hand sides of relation (ii) in (7) has two identical elements $u_{i_k} = u_{i_m}$ with $i_k > i_m$.

Division II. The above defined elements t_k which occur in the left-hand side of the relation (*ii*) in Eq. (7) are distinct because $d_{\max}(t_{k+1}) < d_{\max}(t_k)$. The other elements occurring in relation (*i*) in Eq. (7) are also distinct since $\deg(u_{i_k+j}) = \deg(u_{i_k+j-1}) + 1\ (j = 1, \ldots, i_{k+1} - i_k - 1)$ and

$$d_{\max}(t_k) = d_{\max}(u_{i_k+1}) = \cdots = d_{\max}(u_{i_{k+1}-1}).$$

Constructivity. *Division* I. Let $u \cdot x_i,\ u \in U,\ x_i \in NM_I(u, U)$ be a non-multiplicative prolongation such that

$$u \cdot x_i = u_1 v \times w,\ u_1 \in U,\ v \in I(u_1, U),\ w \in I(u_1 v, U \cup \{u_1 v\}),\ w \neq 1.$$

Show that if $x_j|w$, then $x_j \in M_I(u_1, U)$. Suppose $x_j \in NM_I(u_1, U)$. It means that there is $v_1 \in U$ satisfying $\deg_j(u_1) < \deg_j(v_1)$. Because $\neg x_j|v$, we have $\deg_j(u_1 v) < \deg_j(v_1)$, and, hence, $x_j \in NM_I(u_1 v, U \cup \{u_1 v\})$.

Division II. Since this division is globally defined, its constructivity is an immediate consequence of the property (c) in Definition 2.1.

Noetherity. *Division* I. Its noetherity follows from Proposition 3.7 and noetherity of Thomas division, since every Thomas completion of a set U, obviously, is also its completion with respect to Division I.

Division II. Given a finite set $U \subset \mathbb{M}$ and $u \in U$ with $d_u = d_{\max}(u)$, complete the set by the monomial $x_1^{d_u} \cdots x_n^{d_u}$ and all its divisors multiple of u. If we do such a completion for every $u \in U$ we obtain, apparently, an involutive completion of U.□

4. Minimal involutive monomial bases

Let U be a finitely generated monomial set with respect to involutive division L. In this case, a finite involutive completion $\tilde{U} \supseteq U$ forms the involutive basis of the monomial ideal generated by U. A monomial ideal may not have the unique involutively autoreduced basis. For instance, from the definition of Janet division given in Example 3.2 it is easy to see that any finite monomial set is Janet autoreduced. Therefore, enlargement of a Janet basis by a prolongation of any its element and Janet completion of the enlarged set leads to another Janet basis of the same monomial ideal. Similarly, Thomas division and Division I do not provide uniqueness of involutively autoreduced bases whereas Pommaret division and Division II do, as the following proposition shows.

Proposition 4.1 *Let L be a globally defined involutive division. Then any monomial ideal has the unique L-involutive basis.*

Proof Assume that there are two distinct L-bases $\bar{U}_1$ and $\bar{U}_2$ of the monomial ideal Id(U) where U is the finite monomial set generating the ideal and autoreduced in the sense of the conventional monomial division. Both $\bar{U}_1$ and $\bar{U}_2$ are apparently involutive completions of U. It follows $\bar{U}_1 \backslash \bar{U}_2 \neq \emptyset$ and $\bar{U}_2 \backslash \bar{U}_1 \neq \emptyset$. Otherwise one sets $\bar{U}_1$, $\bar{U}_2$ would contain another, and, hence, could not be L-autoreduced. Indeed, let $\bar{U}_2 \subset \bar{U}_1$. Then any element of $u \in \bar{U}_1 \backslash \bar{U}_2$ is multiple of some element in U, and, in accordance with Definition 2.5, u is involutively multiple of some element $v \in \bar{U}_2$.

We obtain that for any $u \in \bar{U}_1 \backslash \bar{U}_2$ there is $v \in \bar{U}_2 \backslash \bar{U}_1$ such that $v|_L u$ and for any $v \in \bar{U}_2 \backslash \bar{U}_1$ there is $w \in \bar{U}_1 \backslash \bar{U}_2$ such that $w|_L v$. Thus, by property (c) in Definition 2.1, given $u \in \bar{U}_1 \backslash \bar{U}_2$ there exist $w \in \bar{U}_1 \backslash \bar{U}_2$ such that $w|_L u$. Since $\tilde{U}_1$ is L-autoreduced, it is possible only if $u = w$. But this implies $u = v$. The obtained contradiction proves the proposition.

Definition 4.2 Let L be an involutive division, and Id(U) be a monomial ideal. Then its L-involutive basis $\bar{U}$ will be called *minimal* if for any other involutive basis $\bar{V}$ of the same ideal the inclusion $\bar{U} \subseteq \bar{V}$ holds.

Proposition 4.3 *If* $U \subset \mathbb{M}$ *is a finitely generated set with respect to a constructive involutive division, then monomial ideal* Id(U) *has the minimal involutive basis.*

Proof The proof follows immediately from Proposition 2.7 and existence of the minimal involutive completion for a finitely generated set [22].

If L is constructive, then to compute the minimal involutive basis for an ideal generated by a given finite monomial set one can use the following algorithm which is a slightly modified version of algorithm **InvolutiveCompletion** in paper [22].

Algorithm **MinimalInvolutiveMonomialBasis:**
Input: U, a finite monomial set
Output: $\bar{U}$, minimal involutive basis of Id(U)

```
begin
  $\bar{U} := Autoreduce(U)$
  choose any admissible monomial ordering $\prec$
  while exist $u \in \bar{U}$ and $x \in NM_L(u, \bar{U})$ s.t.
    $u{\cdot}x$ has no involutive divisors in $\bar{U}$ do
    choose such $u$, $x$ with the lowest $u \cdot x$ w.r.t. $\prec$
    $\bar{U} := \bar{U} \cup \{u \cdot x\}$
  end
end
```

The proof of *correctness and termination*, for a finitely generated set, of this algorithm is the same as that of algorithm **InvolutiveCompletion** [22] if Proposition 2.7 is taken into account. In effect, the below algorithm constructs the minimal involutive completion of an autoreduced, in the sense of the conventional monomial division, initial monomial set. This autoreduction is just done in line 2 of the algorithm.

Example 4.4 (Continuation of Example 3.8). The minimal involutive bases of the ideal generated by the set $U = (x^2, xy, z)\ (x \succ y \succ z)$ are given by

$$\begin{aligned}
&\bar{U}_T = \{x^2, xy, z, xz, yz, x^2y, xyz, x^2z, x^2yz\}\\
&\bar{U}_J = \{x^2, xy, z, xz\}\\
&\bar{U}_P = \{x^2, xy, z, xz, yz, y^2z, \ldots, y^kz, \ldots\}\\
&\bar{U}_I = \{x^2, xy, z, xz, x^2y, xyz, x^2z, x^2yz\}\\
&\bar{U}_{II} = \{x^2, xy, z, xz, yz, xyz\}
\end{aligned}$$

where $k \in \mathbb{N}(k > 2)$, and subscripts in the left-hand sides stand for different involutive divisions considered in Section 3. This example explicitly shows that Pommaret division is not noetherian. However, for another ordering $z \succ x \succ y$ the set U is finitely generated, and then $\bar{U}_P = U$.

One should note that selection of a L-irreducible non-multiplicative prolongation which is lowest with respect to an admissible monomial ordering and which we call *normal* is of fundamental importance for the above algorithm. We demonstrate this fact by the following example.

Example 4.5 Let $U = \{x^2, xz, y\}$ and L be Pommaret division with $x \succ y \succ z$. By the normal selection strategy, the lowest irreducible non-multiplicative prolongation is $y \cdot x$ with respect to any admissible monomial ordering. Enlargement of U by xy gives the Pommaret basis $\bar{U} = \{x^2, xy, xz, y\}$ of ideal Id(U) which is obviously minimal. This shows that U is a finitely generated set. However, if we would take first the prolongation $xz{\cdot}y$ which is involutively irreducible modulo U, but not lowest, then we might obtain the infinite chain of irreducible prolongations:

$$xz \to xyz \to xy^2z \cdots \to xy^kz \to \cdots$$

Definition 4.6 Let L be a constructive involutive division, U be a finite monomial set and $V =$ *Autoreduce*(U). Then set U will be called (L—) *compact* if $U = V$ or U is obtained from V in the course of the above algorithm. As an immediate consequence of this definition we have the following corollary.

Corollary 4.7 *If $U \subset \mathbb{M}$ is finitely generated set with respect to a constructive involutive division L, then a compact involutive basis of ideal* Id(U) *is minimal.*

5. Minimal involutive bases of polynomial ideals

In paper [22], we proposed the next algorithm **InvolutiveBasis** for computation of involutive bases of polynomial ideals. In the algorithm the initial polynomial set F is subject, first of all, to the conventional autoreduction in line 2. Next are two main steps which are sequentially made:

(i) By the normal strategy, a non-multiplicative prolongation $g{\cdot}x$ of element g in the intermediate basis G with the lowest $\mathrm{lm}(g{\cdot}x)$ is selected in line 5. If there are several different non-multiplicative prolongations with the same leading term, then any of them may be selected.
(ii) If $h = NF_L(g \cdot x, G) \neq 0$, then G is enlarged by h, and the involutive autoreduction of the enlarged set is done in line 8.

In order to apply the criterion in line 7 for elimination of superfluous involutive reductions and also to avoid repeated prolongations, the auxiliary set T of triples (g, u, P) is used. Here $g \in G$, and u is either the lowest, with respect to the ordering $\prec$, leading monomial in $\mathrm{lm}(G)$ such that g was produced by non-multiplicative prolongations of $f \in G$ with $u = \mathrm{lm}(f)$, or $u = \mathrm{lm}(g)$ if there is no such f in G. Those variables in $NM_L(g,G)$ have been chosen in line 5 collected in set P.

Algorithm **Involutive Basis:**

Input: F, a finite polynomial set
Output: G, an involutive basis of the ideal $\mathrm{Id}(F)$

```
begin                                                                          1
    $G$ : Autoreduce ($F$); $T := \emptyset$                                   2
    for each $g \in G$ do $T := T \cup \{(g, \mathrm{lm}(g), \emptyset)\}$    3
    while exist $(g, u, P) \in T$ and $x \in NM_L(\mathrm{lm}(g), \mathrm{lm}(G))\backslash P$ do   4
      choose such $(g, u, P)$, $x$ with the lowest $\mathrm{lm}(g){\cdot}x$ w.r.t. $\prec$   5
      $T := T \backslash \{(g,u,P)\} \cup \{(g,u,P \cup \{x\})\}$             6
      if Criterion$(g{\cdot}x,u,T)$ is false then $h := NF_L(g{\cdot}x,G)$    7
        if $h \neq 0$ then $G := Autoreduce_L(G \cup \{h\})$                 8
          if $\mathrm{lm}(h) = \mathrm{lm}(g{\cdot}x)$ then $T := T \cup \{(h,u,\emptyset)\}$   9
          else $T := T \cup \{(h, \mathrm{lm}(h), \emptyset)\}$             10
      $Q := T$; $T := \emptyset$                                              11
      for each $g \in G$ do                                                   12
        if exist $(f, u, P) \in Q$ s.t. $\mathrm{lm}(f) = \mathrm{lm}(g)$ then  13
          choose $g_1 \in G$ s.t. $\mathrm{lm}(g_1)|_L u$                     14
          $T := T \cup \{(g, \mathrm{lm}(g_1), P)\}$                          15
        else $T := T \cup \{(g, \mathrm{lm}(g), \emptyset)\}$                 16
    end                                                                        17
end                                                                            18
```

Criterion (g,u,T) is true provided that if there is $(f,v,D) \in T$ such that $\mathrm{lm}(f)|_L \mathrm{lm}(g)$ and $\mathrm{lcm}(u, v) \prec \mathrm{lm}(g)$. Correctness of this criterion, which is just the involutive form [22] of the Buchberger's chain criterion, is provided by Theorem 2.19.

Definition 5.1 Given a constructive division L, a finite involutive basis G of ideal $\mathrm{Id}(G)$ is called *minimal* if $\mathrm{lt}(G)$ is the minimal involutive basis of the monomial ideal generated by $\{\mathrm{lt}(f) | f \in \mathrm{Id}(G)\}$.

Theorem 5.2 *A monic minimal involutive basis is unique.*

Proof Assume for a contradiction that a polynomial ideal $\mathrm{Id}(F)$ has two distinct monic minimal involutive bases G_1 and G_2. Their minimality means that $\mathrm{lm}(G_1) = \mathrm{lm}(G_2)$. Since G_1 and G_2 are distinct there are $g_1 \in G_1$ and $g_2 \in G_2$ such that lt(g_1)=lt(g_2) but $g_1 \neq g_2$. Since $g_1 - g_2 \in$Id(F), by Theorem 2.18, we have $NF_L(g_1 - g_2, G_1) = NF_L\ (g_1 - g_2, G_2) = 0$. Therefore, at least one of the sets G_1, G_2 is not involutively autoreduced, and, hence, in accordance with Definition 2.16, it cannot be involutive basis. □

For a globally defined involutive division, by Proposition 4.1, this proof, obviously, is also valid for polynomial ideals with infinite involutive bases. Therefore, we have the following corollary.

Corollary 5.3 *Given a globally defined involutive division, every polynomial ideal has the unique involutive basis.*

Thus, given a globally defined involutive division L, the output of algorithm **InvolutiveBasis**, in the case of its termination, is unique for a given polynomial ideal irrespective of an ideal generating set F in the input.

However, even though the algorithm may not terminate it is still able to compute a Gröbner basis as the following proposition shows.

Proposition 5.4 *Let L be a continuous involutive division and G be an intermediate polynomial basis generated by algorithm* **InvolutiveBasis**. *If the ordering $\prec$ is degree compatible, then i a finite number of steps G becomes a Gröbner basis.*

Proof Let the current prolongation $g{\cdot}x$ is such that $h = NF_L(g \cdot G) \neq 0$. Then at the second main step of the algorithm (step (ii) as described above), the intermediate polynomial set is enlarged by h. In so doing there are two alternatives:

$$(a)\ \mathrm{lm}(h) = \mathrm{lm}(g \cdot x); \quad (b)\ \mathrm{lm}(h) \prec \mathrm{lm}(g \cdot x).$$

In the latter case, lm($g{\cdot}x$) is involutively reducible by some $\mathrm{lt}(f) \in \mathrm{lt}(G)$, that is, $\mathrm{lm}(g) \cdot x = \mathrm{lm}(f) \times w$. Then, by Theorem 2.14 and Corollary 2.15 we have the equality $NF_L(g \cdot x, G) = NF_L(S(f,g), G)$ where $S(f,g) = g \cdot x - f \times w$ is an S-polynomial.

In this case, unlike the case (a), the monomial ideal Id(lm(G)) is changed. Indeed, let there is a polynomial $h_1 \in G$ such that lm(h) is multiple of lm(h_1) but not involutively multiple, that is, lm(h)=lm (h_1) ·(lm(h)/lm(h_1)). By the normal selection strategy, set G satisfies the condition (6) of partial involutivity up to the monomial lm(h) with respect to the ordering $\prec$ what implies $NF_L(h,F)=0$.

Furthermore, by Theorem 2.18, $NF_L(S(g_1,\ g_2),\ G) = NF(S(g_1,\ g_2),\ G) = 0$ for any S-polynomial $S(g_1, g_2)$, (g_1, $g_2 \in G$) with lcm(lm(g_1),(lm (g_2))$\prec$lm($g{\cdot}x$).

It remains to prove that every $S(g_1, g_2)$ such that $NF(S(g_1, g_2), G) \neq 0$ is computed at some step of the algorithm. Since set G is L-autoreduced, monomial u=lcm(lm(g_1), lm(g_2)) cannot be involutively multiple of both lm(g_1), lm(g_2). Hence, by degree compatibility of the ordering $\prec$, in a finite number of steps at least one of g_1, g_2 will be non-multiplicatively prolonged to a polynomial g with lm(g)=u. Let g be obtained by non-multiplicatively prolongations of g_1, and the current prolongation be g with u=lm(g_1)·(u/lm(g_1)). If u is involutively multiple of lm(g_2) or lm(g_3), where g_3 is a polynomial obtained in the course of the algorithm by non-multiplicative prolongations of g_2, then we are done.

Otherwise, there is to be $\tilde{g} \in G$ such that $u = \mathrm{lm}(\tilde{g}) = \mathrm{lm}(g_2) \cdot (u/\mathrm{lm}(g_2))$, and one of the two polynomials $g, \tilde{g}$ will be constructed before the another. Since their leading monomials coincide, the leading monomial of the latter will be involutively reducible by the leading monomial of the former. □

Though, by Corollary 5.3, algorithm **InvolutiveBasis**, if it terminates, computes the minimal involutive basis for a globally defined involutive division it may not be the case for arbitrary involutive division. If we use, for instance, any of divisions in Example 3.1–3.2 and 3.4, then, given a polynomial ideal Id(F), the algorithm output depends on the structure of input generating set F.

Example 5.5 Let $F = \{x^2y-1, xy^2-1, y^4-1\}$. The lexicorgraphical Janet basis for $x \succ y \succ z$ computed by algorithm **InvolutiveBasis** is

$$\{x^2y-1, x^2-1, xy^2-1, xy-1, x-1, y^4-1, y^3-1, y^2-1, y-1\}$$

The reduced Gröbner basis $\{x-1, y-1\}$ of Id(F) is also the minimal Janet basis.

Proposition 5.6 *If algorithm* **InvolutiveBasis** *takes a reduced Gröbner basis as input it produces a minimal involutive basis for a constructive involutive division.*

Proof Let $g\cdot x$ be a non-multiplicative prolongation of element g in intermediate polynomial set G, and $h = NF_L(g\cdot x, G)$. We note that either h=0 or $\mathrm{lm}(h) = \mathrm{lm}(g\cdot x)$. Otherwise, as shown in the proof of Proposition 5.4, lm(h) would not belong to monomial ideal Id(lm(G)) = Id(lm(F)). Thus, the output monomial set lm(G) is constructed just as it would be done by applying algorithm **MinimalInvolutiveMonomialBasis** to lm(F). It follows that lm(G) is the minimal basis of Id(lm(F)). □

The next algorithm constructs a minimal involutive basis, and generally deals with less number of intermediate polynomials than algorithm **InvolutiveBasis** causing the computational efficiency to increase.

Theorem 5.7 *Let F be a finite subset of* $\mathbb{R}$ *and L be a constructive involutive division. Suppose ordering* $\succ$ *is degree compatible. Then algorithm* **MinimalInvolutiveBasis** *computes a minimal involutive basis of* Id(F) *if this basis is finite. If L is noetherian, then the basis is computed for any ordering.*

Proof *Correctness.* First of all, we recall that correctness of the involutive criterion which is verified in lines 14, 23 follows from Theorem 2.19. As distinct from the algorithm **InvolutiveBasis** here are two disjoint subsets T and Q of the triples. They are built in such a way that $\mathrm{lm}(g) \prec \mathrm{lm}(f)$ for any g in $(g,u,P) \in T$ and f in $(f,v,D) \in Q$. Let $\tilde{G}$ be a polynomial set $\{g | (g,u,P) \in Q\}$. First of all, we claim the ideal $\mathrm{Id}(G \cup \tilde{G})$ is an invariant of the **repeat**-loop. Indeed, it is trivially true upon initialization. Inside the loop, if a polynomial is removed from G in lines 18 and 28, then it is added to $\tilde{G}$. On the other hand, removal of a triple from Q, that is, the corresponding polynomial from $\tilde{G}$ in line 11, does not change G iff $NF_L(g,G) = 0$.

Furthermore, set T is handled by the lower **while**-loop in lines 19–29 just as it done in algorithm **InvolutiveBasis** except for restriction in line 20 and the set contraction in lines 27–28. In the latter cases, all the elements in G with $\mathrm{lm}(g) \succ \mathrm{lm}(h)$, where h is the normal form of the current prolongation, are moved to G. Thus, this **while**-loop preserves the property of partial involutivity up to monomial $v \prec \mathrm{lm}(h)$ for the intermediate set G, in accordance with Theorems 2.17 and 2.18, if there is a partially involutive set in the input of the loop. Besides, two elements with coinciding leading terms obviously never occur in set $\tilde{G}$.

In what follows polynomials in $\tilde{G}$, if $\tilde{G} \neq \emptyset$, are successively selected in accordance with the normal strategy; taken out of the set and L-reduced modulo G. The upper **while**-loop in lines 9–13 proceeds until the normal form h of the selected polynomial does not vanish. Then set G is enlarged by h in line 14. The **repeat**-loop terminates when set $\tilde{G}$ becomes empty in line 11 and the lower **while**-loop does not lead to appearance of new elements in this set. It means that the output set G is an involutive basis of ideal Id(G)=Id(F).

Algorithm **MinimalInvolutiveBasis:**

```
Input: $F$, a finite polynomial set
Output: $G$, the minimal involutive basis of the ideal Id($F$)
begin
  $F$:= 60> $Autoreduce(F)$
  choose $g \in F$ with the lowest lm($g$) w.r.t. $\prec$
  $T := \{(g, \mathrm{lm}(g), \emptyset)\}; Q := \emptyset; G := \{g\}$
  for each $f \in F\backslash\{g\}$ do
  $Q := Q \cup \{(f, \mathrm{lm}(f), \emptyset)\}$
  repeat
    $h$:=0
    while $Q \neq \emptyset$ and $h$=0 do
      choose $g$ in $(g, u, P) \in Q$ with the lowest lm($g$) w.r.t. $\prec$
      $Q := Q\backslash\{(g, u, P)\}$
      if $Criterion(g,u,T)$ is false then $h := NF_L(g, G)$
    end
    if $h \neq 0$ then $G := G \cup \{h\}$
      if $\mathrm{lm}(h) = \mathrm{lm}(g)$ then $T := T \cup \{(h, u, P)\}$
      else $T := T \cup \{(h, \mathrm{lm}(h), \emptyset)\}$
        for each $f$ in $(f, v, D) \in T$ s.t. $\mathrm{lm}(f) \succ \mathrm{lm}(h)$ do
        $T := T\backslash\{(f, v, D)\}; Q := Q \cup \{(f, v, D)\}; G := G\backslash\{f\}$
      while exist $(g, u, P) \in T$ and $x \in NM_L(g, G)\backslash P$ and, if $Q \neq \emptyset$,
        s.t. $\mathrm{lm}(g \cdot x) \prec \mathrm{lm}(f)$ for all $f$ in $(f, v, D) \in Q$ do
        choose such $(g, u, P), x$ with the lowest $\mathrm{lm}(g) \cdot x$ w.r.t. $\prec$
        $T := T\backslash\{(g, u, P)\} \cup \{(g, u, P \cup \{x\})\}$
        if $Criterion(g{\cdot}x,u,T)$ is false then $h := NF_L(g \cdot x, G)$
          if $h \neq 0$ then $G := G \cup \{h\}$
            if $\mathrm{lm}(h) = \mathrm{lm}(g \cdot x)$ then $T := T \cup \{(h, u, \emptyset)\}$
            else $T := T \cup \{(h, \mathrm{lm}(h), \emptyset)\}$
              for each $f$ in $(f, v, D) \in T$ with $\mathrm{lm}(f) \succ \mathrm{lm}(h)$ do
              $T := T\backslash\{(f, v, D)\}; Q := Q \cup \{(f, v, D)\}; G := G\backslash\{f\}$
      end
    until $Q \neq \emptyset$
end
```

Now, by Corollary 4.7, to prove minimality of the output basis it is sufficient to show that the lower **while**-loop always ends up with L-autoreduced polynomial set G such that lt(G) is compact. As we have already seen, this loop preserves partial involutivity. Initially there is a single polynomial which has the minimal leading monomial, and, therefore, its handling in the loop produces a compact leading monomial set.

Suppose a partially involutive polynomial set G with compact lm(G) was produced by the lower **while**-loop, and then it is enlarged by $h = NF_L(g, G)$ in line 14 when G is partially involutive up to some monomial $v \prec \mathrm{lm}(g)$.

If lm(h) $=$ lm(g), then, by restriction in line 20, lm(h)$\succ$lm(f) for all $f{\in}G$. By property (d) in Definition 2.1, we obtain that $NM_L(\mathrm{lm}(f), \mathrm{lm}(G_1 = G \cup \{h\})) \subseteq NM_L(\mathrm{lm}(f), \mathrm{lm}(G))$ for any $f{\in}G$.

Let lm(h) has no conventional divisors in lm(G). Then, starting with the set $G_0 = Autoreduce\ (G_1)$, completing G_0 with irreducible non-multiplicative prolongations of its elements by the normal strategy, we construct set $G_2 \supseteq G_1$ partially involutive up to the monomial v and with compact lm(G_2). If we start now with set lm(G_1) and complete it, if necessary, with irreducible non-multiplicative prolongations of its elements in order to obtain a partially involutive set up to v, then we arrive at the same set G_2. Indeed, even in the presence of extra intermediate elements, if $G_2 \backslash G_1 \neq \emptyset$, there cannot occur reduction of an element $p{\in}G$ either by an element in G or by an extra element. The former reduction is impossible by property (d) of involutive division. The latter reduction, if it would hold, by properties (c)–(d) and by Theorem 2.18, would lead to reducibility of p in the earlier set G when h has not been added yet.

If lm(h) is multiple of some element in lm(G), then continuation of processing with G_1 in the lower **while**-loop yields a partially involutive polynomial set up to lm(h). In doing so, h is involutively reduced either to zero, or to a polynomial which changes the monomial ideal Id(lm(G)), as we have shown in the proof of Proposition 5.4. Correspondingly, G, after contraction in lines 27–28, is reset to the partially involutive form with the compact leading monomial set.

In the case when lm(h)$\prec$lm(g), the elimination which is done in line 18 converts, apparently, the situation into one of two alternatives we have just considered.

Thus, the **repeat**-loop, if it terminates, ends up with an involutive set G with compact lm(G), that is, with the minimal involutive basis.

Termination. As it shown in the proof of Proposition 5.4, there may be a finite number of cases when polynomial g chosen in lines 10 or prolongation $g{\cdot}x$ chosen in line 21 have reducible leading monomials. It implies finitely many redistribution of triples between $T$and Q done in lines 18 and 28. If Id(F) has the finite minimal involutive basis, and ordering $\prec$ is degree compatible, then the lower **while**-loop terminates irrespective of Q is empty set or not. This follows immediately from Propositions 5.4, 5.6 and compactness of lm(G). Since the upper **while**-loop is obviously terminates, and set Q is refreshed finitely many times, in a finite number of steps the algorithm arrives at $Q{=}\emptyset$ in line 30.

If involutive division L is noetherian then the algorithm terminates for any ordering $\prec$ because the lower **while**-loop terminates for the same reason as the **while**-loop does in algorithm **InvolutiveBasis** [22].

6. Conclusion

As we noted above, algorithm **MinimalInvolutiveBasis** deals, generally, with less number of intermediate polynomials then algorithm **InvolutiveBasis**. Besides, if involutive division L is not globally defined, then we may not obtain the minimal involutive basis in the output of the latter algorithm. But even for globally defined divisions the former algorithm avoids the involutive autoreduction done in the latter algorithm at every step of the intermediate set enlargement. That is why we expect higher efficiency of algorithm **MinimalInvolutiveBasis** with respect to algorithm **IvolutiveBasis** for arbitrary involutive division.

One could also construct the minimal involutive basis by computing the reduced Gröbner basis and then enlarging it by non-multiplicative prolongations of its elements until the leading monomial set becomes involutive. To construct the reduced Gröbner basis one can use the Buchberger algorithm or perform the conventional autoreduction of an involutive basis computed by algorithm **InvolutiveBasis**. However, unlike Buchberger algorithm, algorithm **MinimalInvolutiveBasis** benefits from the involutive technique, and as we have argued is favored over the use of algorithm **InvolutiveBasis** for intermediate computation.

In paper [24] for constructing Janet bases for linear partial differential equations one more algorithm is described. Its analog in commutative algebra contains two basic subalgorithms which are successively performed: completion of a polynomial set by non-multiplicative prolongations of its elements until the set of leading monomials becomes involutive or complete (see footnote at page 4); the conventional autoreduction of the obtained set. In this case due to the second subalgorithm the output Janet bases are minimal. However, such an algorithmic procedure is far short of optimum from the computational point of view. In so doing one has to perform the repeated prolongations and deal with all the possible S-polynomials. In our algorithm **MinimalInvolutiveBasis** the repeated prolongations are eliminated by storing in the triple sets T and Q those non-multiplicative variables which have been used for a given polynomial. Furthermore, the use of the involutive analogue of the Buchberger's chain criterion allows one to cut considerably the number of computed S-polynomials.

The algorithms described in this paper just as Zharkov and Blinkov algorithm [25] can be extended to systems of linear systems of partial differential equations [26], and also to some classes of nonlinear systems. Being uniquely defined, minimal involutive bases much like reduced Gröbner bases can be considered as canonical ones for polynomial and differential ideals. The corresponding form of partial differential equation systems is just the standard [28] one. By transforming a given system into this form one can determine the dimension of the solution space and a set of initial conditions providing the existence of a uniquely defined and locally holomorphic solution [17,27–29]. Involutive algorithmic ideas may be also rather fruitful in constructing the canonical bases for finitely generated ideals in free Lie algebras and superalgebras [30].

Acknowledgements

The authors are grateful to Joris van der Hoeven for useful comments and suggestions on Division II, and to Joachim apel for important remarks. This work was supported in part by the RFBR grant No. 96-15-96030.

References

[1] B. Buchberger, An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-dimensional Polynomial Ideal (in German), PhD Thesis, University of Innsbruck, Austria, 1965.

[2] D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra, 2nd ed., Springer, New-York, 1995.

[3] T. Becker, V. Weispfenning, H. Kredel, Gröbner Bases, A Computational Approach to Commutative Algebra, Graduate Texts in Mathematics 141, Springer, New York, 1993.

[4] B. Mishra, Algorithmic Algebra, Springer, New York, 1993.

[5] T. Mora, An introduction to commutative and non-commutative Gröbner bases, Theor. Comp. Sci. 134 (1994) 131–173.

[6] A. Kandri-Rody, V. Weispfenning, Non-cummutative Gröbner bases in algebras of solvable type, J. Symb. Comp. 9 (1990) 1–26.

[7] A.A. Mikhalev, A.A. Zolotykh, Combinatiorial Aspects of Lie Superalgebras, CRC Press, Boca Raton, New York, 1995.

[8] G. Carra'Ferro, Gröbner bases of differential algebra, Lec. Not. Comp. Sci. 356 (1987) 129–140.

[9] F. Ollivier, Standard bases of differential ideals, Lec. Not. Comp. Sci. 508 (1990) 304–321.

[10] B. Buchberger, A Criterion for Deteching Unnecessary Reductions in the Construction of Gröbner Bases, in: E.W. Ng, (Ed.), Proceedings of EUROSAM 79, Springer, Berlin, 1979, pp. 3–21.

[11] B. Buchberger, Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, in: N.K. Bose (ed.), In Recent Trends in Multidimensional System Theory, Reidel, Dordrecht, 1985, pp. 184–232.

[12] R. Gebauer, H.M. Möller, On an installation of Buchberger's algorithm, J. Symb. Comp. 6 (1988) 275–286.

[13] A. Giovini, T. Mora, G. Niesi, L. Robbiano, C. Traverso, One sugar cube, please' or selection strategies in the Buchberger algorithm, in: S.M. Watt (Ed.), Proceedings of the ISSAC'91, ACM Press, 1991, pp. 49–54.

[14] J.C. Faugère, P. Gianni, D. Lazard, T. Mora, Efficient computation of zero-dimensional Gröbner bases by change of ordering, J. Symb. Comp. 16 (1993) 329–344.

[15] A.Yu. Zharkov, Yu.A. Blinkov, Involutive Approach to Investigating Polynomial Systems, In: Proceedings of SC 93, International IMACS Symposium on Symbolic Computation: New Trends and Developments (Lille, June 14–17, 1993), Math. Comp. Simul. 42 (1996), 323-332.

[16] J.F. Pommaret, Systems of Partial Differential Equations and Lie Pseudogroups, Gordon & Breach, New York, 1978.

[17] M. Janet, Sur les systèmes d'equations aux dérivées partielles, J. Math. Pure et Appl. 3 (1920) 65–151.

[18] A.Yu. Zharkov, Solving Zero-Dimensional Involutive Systems, L. Gonzales-Vega, T. Recio (eds.), in: Algorithms in Algebric Geometry and Applications, Progress in Mathematics, Vol. 143, Birkhäuser, Basel, 1996, pp. 389–399.

[19] A.Yu. Zharkov, Yu.A. Blinkov, Involutive Bases of Zero-Dimensional Ideals. Preprint No. E5-94-318, Joint Institute for Nuclear Research, Dubna, 1993.

[20] J. Apel, A Gröbner approach to involutive bases, J. Symb. Comp. 19 (1995) 441–457.

[21] P.A. García-Sánchez, Gröbner and involutive bases for zero-dimensional ideals, SIGSAM Bulletin 29(2) (1995) 12–15.

[22] V.P. Gerdt, Yu.A. Blinkov, Involutive Bases of Polynomial Ideals, Preprint-Nr. 1/1996, Naturwissenschaftlich-Theoretisches Zentrum, University of Leipzig, 1996, This issue.

[23] J. Thomas, Differential Systems, American Mathematical Society, New York, 1937.

[24] F. Schwarz, An algorithm for determining the size of symmetry groups, Computing 49 (1992) 95–115.

[25] V.P. Gerdt, Gröbner Bases and Involutive Methods for Algebraic and Differential Equations, in: J. Fleischer, J. Grabmeier, F.W. Hehl, W. Küchlin (Eds.), Computer Algebra in Science and Engineering, World Scientific, Singapore, 1995, pp. 117–137.

[26] V.P. Gerdt, Involutive Division Methods Applied to Algebraic and Differential Equations, In preparation.

[27] C. Riquier, Les Systèmes d'Equations aux Dérivées Partielles, Gauthier-Villars, Paris, 1910.

[28] G.J. Reid, Algorithms for reducing a system of PDEs to standard form, determining the dimension of its solution space and calculating its Taylor series solution, Euro. J. Appl. Maths. 2 (1992) 293–318.

[29] W.M. Seiler, Analysis and Application of the Formal Theory of Partial Differential Equations, PhD Thesis, Lancaster University, 1994.

[30] V.P. Gerdt, V.V. Kornyak, Construction of Finitely Presented Lie Algebras and Superalgebras, J. Symb. Comp., 21, pp. 337–349.