Записки научных
семинаров ПОМИ
Том 258, 1999 г.

V. P. Gerdt

INVOLUTIVE DIVISION TECHNIQUE: SOME GENERALIZATIONS AND OPTIMIZATIONS

Abstract. In this paper, in addition to the earlier introduced involutive divisions, we consider a new class of divisions induced by admissible monomial orderings. We prove that these divisions are noetherian and constructive. Thereby each of them allows one to compute an involutive Gröbner basis of a polynomial ideal by sequentially examining multiplicative reductions of nonmultiplicative prolongations. We study dependence of involutive algorithms on the completion ordering. Based on properties of particular involutive divisions two computational optimizations are suggested. One of them consists in a special choice of the completion ordering. Another optimization is related to recomputing multiplicative and nonmultiplicative variables in the course of the algorithm.

1. Introduction

In paper [1] a concept of involutive monomial division was invented which forms the foundation of general involutive algorithms [1, 2] for construction of Gröbner bases [3] of a special form called involutive. This notion, by a well-known correspondence [4, 5] between polynomials and linear homogeneous partial differential equations (PDEs) with constant coefficients, follows the notion of involutivity for PDEs. An involutive form of a system of PDEs is its interreduced completion by the differential consequences called prolongations[1], incorporating all integrability conditions into the system [6, 8]. The integrability conditions play the same role in the completion procedure for PDEs as nontrivial S-polynomials in the Buchberger algorithm [10, 11] for construction of Gröbner bases.

Given a finite polynomial set and an admissible monomial ordering, an involutive division satisfying the axiomatic properties proposed in [1] leads to a self-consistent separation of variables for any polynomial in the

Preprint JINR E5-98-151, Dubna, 1998. Submitted to CASC'98, International Conference "Computer Algebra in Scientific Computing" (April 20-24, St-Petersburg, Russia).

[1]Prolongation for PDE means its differentiation whereas for a polynomial this means multiplication by the corresponding variable.

set into disjoined subsets of so-called multiplicative and nonmultiplicative variables.

The idea of the separation of variables into multiplicative and nonmultiplicative goes back to classical papers of Janet [6] and Thomas [7]. They used particular separations of independent variables for completing systems of partial differential equations to involution. More recently one of the possible separations already introduced by Janet [6] was intensively used by Pommaret [8] in the formal theory of partial differential equations. These classical separations allow one to generate the integrability conditions by means of multiplicative reductions of nonmultiplicative prolongations. Just this fact was first used in [9] as a platform for an involutive algorithm for construction of Pommaret bases of polynomial ideals.

If an involutive division satisfies some extra conditions: noetherity and constructivity [1], then an involutive basis may be constructed algorithmically by sequential examination of single nonmultiplicative prolongations only. Whereas Thomas and Janet divisions satisfy all the extra conditions, Pommaret division, being constructive, is non-noetherian. This implies that Pommaret bases of positive dimensional ideals may be infinite. The uniqueness properties of involutive bases are investigated in [2] where a special form of an algorithm proposed for construction of a minimal involutive basis which is unique much like to a reduced Gröbner basis. In addition to the above mentioned classical divisions, in paper [2] two more divisions were introduced which satisfy all the extra conditions.

Recently it was shown [12] that one can also construct different possible separations of variables for a fixed monomial set. These separations can not be considered, generally, as functions of a set and its element as defined in [1]. Nevertheless, the results of paper [12] demonstrate for a wide class of divisions how one can change the division dynamically in the course of the completion. This increases the flexibility of the involutive technique and may also increase the efficiency of computations.

An involutive basis is a special kind of Gröbner basis, though, generally, it may be redundant. However, extra elements in the former may facilitate many underlying computations. The structure of a Pommaret basis, for example, reveals a number of attractive features convenient for solving zero-dimensional polynomial systems [13]. An involutive basis for any division allows one to compute easily the Hilbert function and the Hilbert polynomial by explicit and compact formulae [12, 14].

Computation of Janet bases relying upon the original Janet algorithm was implemented in Reduce and used for finding the size of a Lie symmetry group for PDEs [15] and for classification of ordinary differential equations admitting nontrivial Lie symmetries [16]. The study of algorithmic aspects of the general completion procedure for Pommaret division and implementation in Axiom was done in [17]. The completion to involution of polynomial bases for Pommaret division was algorithmized and implemented in Reduce, first, in [9], and then with algorithmic improvements in [1]. The main improvement is incorporation of an involutive analogue of Buchberger's chain criterion. Recently different involutive divisions were implemented also in Mathematica [14].

In the present paper we introduce a class of involutive divisions induced by admissible orderings and prove their noetherity and constructivity. For the new class of divisions, along with the classical ones and two divisions of paper [2], we study the stability of the partial involutivity for monomial and polynomial sets under their completion by irreducible nonmultiplicative prolongations. We generalize the involutive algorithms to different main and completion orderings. The completion ordering serves for selection of a nonmultiplicative prolongation to be treated next. In so doing, a completion ordering defines the selection strategy in involutive algorithms similar to the selection strategy for critical pairs in Buchberger algorithm [10, 11]. For different divisions we find some completion orderings which preserve the property of partial involutivity and thereby save computing time. We indicate also a 'pairwise' property which is valid for all known divisions. This property can be used to efficiently recompute the separations when a new polynomial has to be added.

2. Background of involutive method

In this section, we recall basic definitions and facts of papers [1, 2] which are used in the next sections.

2.1. Preliminaries.

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

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. For the least common multiple of two monomials $u, v \in \mathbb{M}$ we shall use the conventional notation $lcm(u, v)$. If monomial u divides monomial v we shall write $u|v$. In this paper we shall distinguish two admissible monomial orderings: *main ordering* and *completion ordering* denoted by $\succ$ and $\sqsupset$, respectively. The main ordering serves, as usually, for isolation of the leading terms in polynomials whereas the completion ordering is used for taking the lowest nonmultiplicative prolongations by the normal strategy [1] and thereby controlling the property of partial involutivity. Besides, throughout the 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 the polynomial $f \in \mathbb{R}$ with respect to $\succ$ will be 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. The least common multiple of the set $\{lm(f) \mid f \in F\}$ will be denoted by $lcm(F)$.

2.2. Involutive monomial division.

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 $L(u, U)$, $u \in U$ 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 is called (L)-involutive multiple of u. In such an event the monomial $v = w/u$ is multiplicative for u and the equality $w = uv$ will be written as $w = u \times v$. If u is a conventional divisor of w but not an involutive one we shall write, as usual, $w = u \cdot v$. Then v is said to be nonmultiplicative for u.*

Definition 2.1. *We shall say that an 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 $u \in U$ provides the separation

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

of the set of variables into two subsets: *multiplicative* $M_L(u, U) \subset L(u, U)$ and *nonmultiplicative* $NM_L(u, U) \cap L(u, U) = \emptyset$. Conversely, if for any finite set $U \subset \mathbb{M}$ and any $u \in U$ the separation (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 an 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.

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 with respect to L or L-involutive if*

$$(\forall u \in U)\ (\forall w \in \mathbb{M})\ (\exists v \in U)\ \ [\ uw \in vL(v,U)\ ]\,.$$

Definition 2.5. *We shall call the set $\cup_{u \in U}\, u\mathbb{M}$ the cone generated by U and denote it by $C(U)$. The set $\cup_{u \in U}\, u\, L(u,U)$ will be called the involutive cone of U with respect to L and denoted by $C_L(U)$.*

Thus, the set U is L-involutive if its cone $C(U)$ coincides with its involutive cone $C_L(U)$.

Definition 2.6. *An L-involutive monomial set $\widetilde{U}$ is called L-completion of a set $U \subseteq \widetilde{U}$ if*

$$(\forall u \in U)\ (\forall w \in \mathbb{M})\ (\exists v \in \widetilde{U})\ \ [\ uw \in vL(v,\widetilde{U})\ ]\,.$$

If there exists a finite L-completion $\widetilde{U}$ 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 with respect to L.

Proposition 2.7 [1]**.** *If an involutive division L is noetherian, then every monomial ideal has a finite involutive basis $\overline{U}$.*

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 set $U \in \mathbb{M}$ and for any finite sequence $\{u_i\}_{(1 \le i \le k)}$ of elements in U such that*

$$(\forall\, i < k)\ (\exists x_j \in NM_L(u_i,U))\ \ [\ u_{i+1}|_L u_i \cdot x_j\ ] \tag{3}$$

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

Theorem 2.10 [1]. *If an involutive division L is continuous then local involutivity of a 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*

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

the following condition holds:

$$(\forall w \in \cup_{u \in U}\, u\, L(u,U))\ \ [\ u \cdot x_i \notin wL(w, U \cup \{w\})\ ]. \qquad (4)$$

Definition 2.12. *Let L be an involutive division, and $Id(U)$ be a monomial ideal. Then an L-involutive basis $\overline{U}$ of $Id(U)$ will be called minimal if for any other involutive basis $\overline{V}$ of the same ideal the inclusion $\overline{U} \subseteq \overline{V}$ holds.*

Proposition 2.13 [2]. *If $U \subset \mathbb{M}$ is a finitely generated set with respect to a constructive involutive division, then the monomial ideal $Id(U)$ has a unique minimal involutive basis.*

2.3. Involutive polynomial sets.

Definition 2.14. *Given a finite set of polynomials $F \subset \mathbb{R}$ and a main ordering $\succ$, multiplicative and nonmultiplicative 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 similarly to their conventional analogues [10, 11] with the use of involutive division instead of the conventional one.

Definition 2.17. *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 Lreducible modulo $f \in F$ if p has a term $t = a\,u$, $(a \in K \setminus \{0\})$, $u \in \mathbb{M}$ such that $u = lm(f) \times v$, $v \in L(lm(f), lm(F))$. It yields the L-reduction $p \to g = p - (a/lc(f))\, f\, v$.*

(ii) *p is L-reducible modulo F if there is $f \in F$ 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 $lm(f)$ $(f \in F)$ and $h = fu$ we shall write $h = f \times u$.

Definition 2.16. *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 monomials which are involutively multiple of any element in $lm(F)$.*

Remark 2.17. The further definitions and theorems of this section which involve the completion ordering $\sqsubset$ generalize those in [1] where $\sqsubset$ is the same as the main ordering $\succ$. The proofs of the generalized theorems are immediate extensions of the underlying proofs in [1].

Definition 2.18. *An L-autoreduced set F is called (L-involutive) if*

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

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

$$(\forall f \in F)\ (\forall u \in \mathbb{M})\ (lm(f) \cdot u \sqsubset v)\quad [\ NF_L(fu, F) = 0\ ]\,, \tag{5}$$

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

Theorem 2.19 [1]**.** *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*

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

Correspondingly, partial involutivity (5) holds iff

$$\begin{gathered}(\forall f \in F)\ (\forall x_i \in NM_L(lm(f), lm(F)))\ (lm(f) \cdot x_i \sqsubset v)\\ [\ NF_L(f \cdot x_i, F) = 0\ ]\,.\end{gathered}$$

Theorem 2.20 [1]**.** *If $F \subset \mathbb{R}$ is an L-involutive basis of $Id(F)$, 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 the set F is partially involutive up to the monomial v with respect to $\sqsubset$, then the equality of the normal forms $NF(p, F) = NF_L(p, F)$ holds for any p such that $lm(p) \sqsubset v$.*

Theorem 2.21. *Let L be a continuous involutive division, F be a finite L-autoreduced polynomial set and $NF_L(p, F)$ be an algorithm of L-involutive normal form. Then the following are equivalent:*

(i) *F is an L-involutive basis of $Id(F)$.*

(ii) *For all $g \in F$, $x \in NM_L(lm(g), lm(F))$ there is $f \in F$ satisfying $lm(g) \cdot x = lm(f) \times w$ and a chain of polynomials in F of the form*

$$f \equiv f_k, f_{k-1}, \dots, f_0, g_0, \dots, g_{m-1}, g_m \equiv g$$

such that

$$NF_L(S_L(f_{i-1}, f_i), F) = NF_L(S(f_0, g_0), F) =$$
$$= NF_L(S_L(g_{j-1}, g_j), F) = 0\,,$$

where $0 \le i \le k$, $0 \le j \le m$, $S(f_0, g_0)$ is the conventional S-polynomial [10,11] *and $S_L(f_i, f_j) = f_i \cdot x - f_j \times w$ is its special form which occurs in involutive algorithms* [1].

Proof. $(i) \Longrightarrow (ii)$ immediately follows from Theorems 2.19 and 2.20 if one takes $f_0 = f$, $g_0 = g$. To prove $(ii) \Longrightarrow (i)$ one suffices to show that $NF_L(g \cdot x, F) = 0$. Assume for a contradiction that there are nonmultiplicative prolongations which are L-irreducible to zero modulo F. Let $g \cdot x$ be such a prolongation which is the lowest with respect to the main ordering $\succ$. This means the partial involutivity of F up to $lm(g) \cdot x$ with respect to $\succ$. Correspondingly, the condition (ii) implies the representation [11] (cf. the proof of Theorem 8.1. in [1]) $S_L(f, g) = g \cdot x - f \times w = \sum_{ij} f_i u_{ij}$ where $f_i \in F$ and $lm(f_i u_{ij}) \prec lm(g) \cdot x$ that contradicts $NF_L(g \cdot x, F) \neq 0$. $\square$

Corollary 2.22 [1]. *Let F be a finite L-autoreduced polynomial set, and let $g \cdot x$ be a nonmultiplicative prolongation of $g \in F$. If the following holds*

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

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

then the prolongation $g \cdot x$ may be discarded in the course of an involutive algorithm.

Remark 2.23. Theorem 2.19 is the algorithmic characterization of involutivity whereas Theorem 2.20 relates Gröbner bases and involutive bases. Theorem 2.21 and Corollary 2.22 yield an involutive analog of the Buchberger's chain criterion [10].

Definition 2.24. *Given a constructive division L, a finite involutive basis G of ideal $Id(G)$ is called minimal if $lt(G)$ is the minimal involutive basis of the monomial ideal generated by $\{lt(f) \mid f \in Id(G)\}$.*

Theorem 2.25 [2]**.** *A monic minimal involutive basis is unique.*

3. Examples of involutive divisions

3.1. Previously introduced divisions.

We give, first, examples of divisions corresponding to separations introduced by Janet, Thomas and Pommaret for the purpose of involutivity analysis of PDEs, and two more divisions proposed in [2]. For the proof of validity of properties (a)–(d) in Definition 2.1 for these divisions we refer to [1, 2].

Definition 3.1. Thomas division [7]**.** *Given a finite set $U \subset \mathbb{M}$, the variable x_i is considered as multiplicative for $u \in U$ if $\deg_i(u) = \max\{\deg_i(v) \mid v \in U\}$, and nonmultiplicative, otherwise.*

Definition 3.2. Janet division [6]**.** *Let the set $U \subset \mathbb{M}$ be finite. For each $1 \leq i \leq n$ divide U into groups labeled by non-negative integers $d_1, \ldots, d_i$:*

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

A variable x_i is multiplicative for $u \in U$ if $i = 1$ and

$$\deg_1(u) = \max\{\deg_1(v) \mid v \in U\},$$

or if $i > 1$, $u \in [d_1, \ldots, d_{i-1}]$ and

$$\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_1, \ldots, d_{i-1}]\}.$$

Definition 3.3 Pommaret division [8]**.** *] 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 nonmultiplicative. For $u = 1$ all the variables are multiplicative.*

Definition 3.4. Division I [2]**.** *Let U be a finite monomial set. The variable x_i is nonmultiplicative for $u \in U$ if there is $v \in U$ such that*

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

and $x_i \in \{x_{i_1}, \ldots, x_{i_m}\}$.

Definition 3.5. Division II [2]. *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* $d_{\max}(u) = \max\{d_1, \ldots, d_n\}$.

Remark 3.6. Thomas division, Divisions I and II do not depend on the ordering on the variables. Janet and Pommaret divisions, as defined, are based on the ordering given in (1). Pommaret division and Division II are globally defined in accordance with Definition 2.1.

All these divisions are constructive, and except Pommaret division they are noetherian [1, 2].

3.2. Induced division.

Now we consider a new class of involutive divisions induced by admissible monomial orderings (cf. [12]).

Definition 3.7 Induced division. *Given an admissible monomial ordering* $\succ$[1] *a variable* x_i *is nonmultiplicative for* $u \in U$ *if there is* $v \in U$ *such that* $v \prec u$ *and* $\deg_i(u) < \deg_i(v)$.

Proposition 3.8. *The separation given in Definition* 3.7 *is an involutive division.*

Proof. Let $L_\succ(u, U)$ be the submonoid generated by multiplicative variables. We must prove the properties (b–c) in Definition 3.7 because (a) and (d) hold obviously.

(b) Let there be a monomial w such that $w \in uL_\succ(u, U) \cap vL_\succ(v, U)$ with $u, v \in U$ and $u \neq v$. Assume $u \succ v$ and $\neg v|u$. Then, there is a variable $x|(lcm(u, v)/u)$ such that $x \notin L_\succ(u, U)$. Since $v|w$ we obtain $x|(w/u)$ that contradicts $w \in uL_\succ(u, U)$. Thus, $v|u$ and $w = v \times (w/v) = v \times [(w/u)(u/v)]$. This yields $u \in vL_\succ(v, U)$.

(c) Let $v \in uL_\succ(u, U)$ and $w \in vL_\succ(v, U)$ with $u, v \in U$, and, hence, $u|v$ and $u|w$. Suppose $w \notin uL_\succ(u, U)$. It follows the existence of a variable $x|(w/u)$, $\neg x|(v/u)$ and a monomial $t \prec u \prec v$, $t \in U$ such that $x|(lcm(u, t)/u)$. This suggests that $x|(lcm(v, t)/v)$ at $t \prec v$, contradicting our initial assumption. $\square$

Remark 3.9. Generally, an ordering $\succ$ defining Induced division implies some variable ordering which is not compatible with (1). However, below we assume that the ordering $\succ$ is compatible with (1).

[1] This ordering is generally different from the main ordering introduced in Sec. 2.1.

To distinguish the above divisions, the abbreviations T, J, P, I, II, $D_{\succ}$ will be sometimes used. For illustrative purposes we consider three particular orderings to induce involutive divisions: lexicographical, degree-lexicographical and degree-reverse-lexicographical. To distinguish these three orderings we shall use the subscripts L, DL, DRL, respectively.

There are certain relations between separations generated by those divisions.

Proposition 3.10. *For any U, $u \in U$ and $\succ$ the inclusions $M_T(u,U) \subseteq M_J(u,U)$, $M_T(u,U) \subseteq M_I(u,U)$, $M_T(u,U) \subseteq M_{D_{\succ}}(u,U)$ hold. If U is autoreduced with respect to Pommaret division, then also $M_P(u,U) \subseteq M_J(u,U)$.*

Proof. The inclusion $M_T(u,U) \subseteq M_{D_{\succ}}(u,U)$ follows from the observation that $x \in T(u,U)$ implies $x \in D_{\succ}(u,U)$. The other inclusions proved in [1, 2]. $\square$

The following example explicitly shows that all eight divisions we use in this paper are different. In the table we list the multiplicative variables for every division.

Example 3.11. [14] Multiplicative variables for elements in the monomial set $U = \{x^2y, xz, y^2, yz, z^3\}$ $(x \succ y \succ z)$ for different divisions:

Monomial	Multiplicative variables						
	T	J	P	I	II	D_L	D_{DL}	D_{DRL}
x^2y	x	x,y,z	y,z	x	x	x	x	x
xz	—	y,z	z	x	x,z	x	x,z	x,z
y^2	y	y,z	y,z	y	y	x,y	x,y	y
yz	—	z	z	—	y,z	x,y	x,y,z	x,y,z
z^3	z	z	z	z	z	x,y,z	z	z

Proposition 3.12. *Induced division is noetherian, continuous and constructive.*

Proof. *Noetherity.* follows immediately from noetherity of Thomas division and the underlying inclusion in Proposition 3.10.

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 (3). 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:

$$\text{(i)} \quad u_i = u_{i-1} \cdot x_j\,; \qquad \text{(ii)} \quad u_i \neq u_{i-1} \cdot x_j\,. \tag{6}$$

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 (6).

Show that $t_{k+1}|_D lcm(t_{k+1}, t_k)$ and $\neg t_k | t_{k+1}$. We have $t_{k+1} \times \widetilde{w}_{k+1} = u_{i_k-1} \cdot x_{j_k} = t_k \cdot \widetilde{v}_k$ where $\neg \widetilde{w}_{k+1} | \widetilde{v}_k$. Indeed, suppose $\widetilde{w}_{k+1} | \widetilde{v}_k$. Apparently, we obtain the relation $t_{k+1} = u_l \cdot z_l$ where $i_k \leq l < i_{k+1}$, and the variable $x_{j_l} \in NM_D(u_l, U)$, which figures in Definition 2.9 of the sequence $\{u_i\}$, satisfies $x_{j_l} | \widetilde{w}_{k+1}$ and $\neg x_{j_l} | z_l$. This suggests, by definition of the division, the existence of $p \in U$ such that $p \prec u_l$ and $\deg_{j_l}(u_l) < \deg_{j_l}(p)$. Since $p \prec t_{k+1}$ and $\deg_{j_l}(u_l) = \deg_{j_l}(t_{k+1})$, it contradicts multiplicativity of x_{j_l} for t_{k+1}.

Therefore, we obtain the relation

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

which, by Definition 3.7, implies $t_k \succ t_{k+1}$ since $w_k \neq 1$ for all k.

It remains to prove that elements in the sequence $\{u_i\}_{(1\leq i\leq M)}$ which occur in the left-hand side of relation (i) in (6) 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 (6). Let u_{i_m} $(j < i_m < k)$ be the nearest such element to u_j. Considering the same nonmultiplicative 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 (6) has two identical elements $u_{i_k} = u_{i_m}$ with $i_k > i_m$.

Constructivity. Let $u, u_1 \in U$, $v \in D_\succ(u_1, U)$ and $x_i \notin D_\succ(u, U)$ be such that $u \cdot x_i = u_1 v \times w$, $w \in D_\succ(u_1 v, U \cup \{u_1 v\})$. Show that $w \in D_\succ(u_1, U)$. Assume that there is $x_j \notin D_\succ(u_1, U)$ satisfying $x_j | w$. This implies the existence $t \in U$ satisfying $t \prec u$, $\deg_j(t) > \deg_j(u_1)$. Then, because $t \prec u_1 v$, the condition $\neg x_j | v$ leads to the contradictory condition $\deg_j(t) > \deg_j(u_1 v)$. Therefore, $x_j | v$. $\square$

4. Completion of monomial sets to involution

If U is a finitely generated monomial set with respect to the fixed involutive division L, then its finite completion gives an involutive basis of the monomial ideal generated by U. There may be different involutively autoreduced bases of the same monomial ideal. For instance, from Definitions 3.1 and 3.2 it is easy to see that any finite monomial set is Thomas and Janet autoreduced. Therefore, enlarging a Thomas or a Janet basis by a prolongation of any its element and then completing the enlarged set leads to another Thomas and Janet basis, respectively. Similarly, Division I and Induced division do not provide uniqueness of involutively autoreduced bases whereas Pommaret division and Division II do, as well as any globally defined division [2].

4.1. Completion algorithm.

Theorem 4.1. *If U is a finitely generated set with respect to a constructive involutive division, then the following algorithm computes the uniquely defined minimal completion $\overline{U}$ of U, that is, for any other completion $\widetilde{U}$ the inclusion $\overline{U} \subseteq \widetilde{U}$ holds.*

Algorithm **InvolutiveCompletion:**

Input: U, a finite monomial set

Output: $\widetilde{U}$, an involutive completion of U

1 **begin**

2 $\widetilde{U} := U$

3 **while** exist $u \in \widetilde{U}$ and $x \in NM_L(u, \widetilde{U})$ such that

4 $u \cdot x$ has no involutive divisors in $\widetilde{U}$ **do**

5 **choose** any $\sqsubset$ and such u and x with the lowest $u \cdot x$ w.r.t. $\sqsubset$

6 $\widetilde{U} := \widetilde{U} \cup \{u \cdot x\}$

7 **end**

8 **end**

Proof. This completion algorithm is a slightly generalized version of that in [1] where ordering $\sqsubset$ is assumed to be fixed in the course of the completion. As proved in [1] (see the proof of Theorem 4.14), the output $\overline{U}$ of the algorithm and the number of irreducible prolongations are invariant on the choice of ordering in line 5.

Corollary 4.2. *If set U is conventionally autoreduced, then the algorithm computes the minimal involutive basis of monomial ideal $Id(U)$.*

In practice, in the course of the completion one has to choose the lowest nonmultiplicative prolongation and to check whether it has an involutive divisor in the set. The timing of computation is thereby determined by the total number of prolongations checked.

Theorem 4.3. *The number of nonmultiplicative prolongations checked in the course of algorithm* **InvolutiveCompletion** *with a constructive division L is invariant on the choice of completion ordering in line* 5.

Proof. As it has been noticed in the proof of Theorem 4.1, the number of irreducible prolongations, as well as the completed set itself, is invariant. Therefore, we must prove invariance of the number of reducible prolongations.

Let there be two different completion procedures of U to $\overline{U}$ based on different choice of completion orderings. Assume that the first procedure needs more reducible prolongations to check than the second one. Let $u \cdot x = v \times w$ $(u, v \in \widetilde{U}_1)$ be the first prolongation checked in the course of the first procedure and such that in the course of the second one the prolongation is not checked. This suggests $x \in M_L(u, \widetilde{U}_2)$ where $\widetilde{U}_2$ is the current set for the second procedure. If $w \neq 1$, by admissibility of a completion ordering, we obtain $u \times x = v \times w$ $(u, v \in \widetilde{U}_2)$. From property (b) in Definition 2.1 we deduce $u \in vL(v, \widetilde{U}_2)$, and, hence, x cannot be nonmultiplicative for u as we assumed for the first procedure.

If $w = 1$ we find that $x \in NM_L(u, \widetilde{U}_1) \cap M_L(u, \widetilde{U}_2)$ where u and $v = ux$ are elements in both $\widetilde{U}_1, \widetilde{U}_2$. From the property (d) in Definition2.1 and invariance of the final completed set $\overline{U}$ is follows that in some step of the second procedure x becomes nonmultiplicative for u. Then the prolongation $u \cdot x$ will be also checked that contradicts our assumption. $\square$

This theorem generalizes Remark 3.13 in [14] which is concerned with L-autoreduced sets and fixed completion orderings.

Example 4.4. (Continuation of Example 3.11). The minimal involutive bases of the ideal generated by the set $U = \{x^2y, xz, y^2, yz, z^3\}$ $(x \succ y \succ z)$ are given by

$$\overline{U}_T = \{x^2y^2z^3, x^2y^2z^2, x^2y^2z, x^2y^2, x^2yz^3, x^2yz^2, x^2yz, x^2y, x^2z^3,$$
$$x^2z^2, x^2z, xy^2z^3, xy^2z^2, xy^2z, xy^2, xyz^3, xyz^2, xyz, xz^3, xz^2,$$
$$xz, y^2z^3, y^2z^2, y^2z, y^2, yz^3, yz^2, yz, z^3\},$$
$$\overline{U}_J = \{x^2y, x^2z, xy^2, xyz, xz, y^2, yz, z^3\},$$
$$\overline{U}_P = \{x^2y, x^2z, xy^2, xyz, xz, y^2, yz, z^3, \ldots, x^ky, \ldots, x^lz, \ldots\},$$

$$\overline{U}_I = \{x^2y^2z^3, x^2y^2z^2, x^2y^2z, x^2y^2, x^2yz^3, x^2yz^2, x^2yz, x^2y, xy^2z^3,$$
$$xy^2z^2, xy^2z, xy^2, xyz^3, xyz^2, xyz, xz^3, xz^2, xz, y^2z^3, y^2z^2,$$
$$y^2z, y^2, yz^3, yz^2, yz, z^3\},$$
$$\overline{U}_{II} = \{x^2y^2, x^2y, xy^2, xyz, xz, y^2, yz, z^3\},$$
$$\overline{U}_L = \{x^2y, xz^2, xz, y^2, yz^2, yz, z^3\},$$
$$\overline{U}_{DL} = \{x^2y, xz, y^2, yz, z^3\},$$
$$\overline{U}_{DRL} = \{x^2y, xy^2, xz, y^2, yz, z^3\},$$

where $k,\, l \in \mathbb{N}$ $(k, l > 2)$, and subscripts in the left-hand sides stand for different involutive divisions considered in Sec. 3. This example explicitly shows that Pommaret division is not noetherian, since it leads to an infinite monomial basis.

4.2. Pair property.

In the course of algorithm **InvolutiveCompletion** the current monomial set $\widetilde{U}$ is enlarged by irreducible nonmultiplicative prolongations in line 6. As this takes place, for a nonglobally defined division one has to recompute the separation into multiplicative and nonmultiplicative variables for *all* monomials. The next definition and proposition give a prescription for efficient recomputing.

Definition 4.5. *We shall say that an involutive division L is pairwise if for any finite set U and any $u \in U$ $(U \setminus \{u\} \neq \emptyset)$, the following holds:*

$$L(u, U) = \cap_{v \in U \setminus \{u\}} L(u, \{v\})$$

or, equivalently,

$$M_L(u, U) = \cap_{v \in U \setminus \{u\}} M_L(u, \{v\}),$$
$$NM_L(u, U) = \cup_{v \in U \setminus \{u\}} NM_L(u, \{v\}). \tag{7}$$

Therefore, for a pairwise division L and a monomial set U the correction of the separation due to enlargement of U by an element v is performed by formula

$$NM_L(u, U \cup \{v\}) = NM_L(u, U) \cup NM_L(u, \{u, v\}). \tag{8}$$

Proposition 4.6. *All the above defined divisions are pairwise.*

Proof. Pommaret division and Division II, as globally defined divisions, are trivially pairwise.

Thomas division. Since

$$\max\{\deg_i(w) \mid w \in U\} = \max_{v\in U\setminus\{u\}}\{\max\{\deg_i(u), \deg_i(v)\}\},$$

Definition 3.1 implies apparently (7).

Janet division. For $i = 1$, by our convention (1) and Definition 3.2, Janet case is reduced to Thomas one, and we are done. Let now $i > 1$ and $\deg_1(u) = d_1, \ldots, \deg_{i-1}(u) = d_{i-1}$. If the group $[d_1, \ldots, d_{i-1}]$ of elements in U contains, in addition to u, some extra elements, then

$$\max\{\deg_i(w) \mid w \in [d_1, \ldots, d_{i-1}]\} =$$
$$= \max_{v\in[d_1,\ldots,d_{i-1}]\setminus\{u\}}\{\max\{\deg_i(u), \deg_i(v)\}\},$$

and $x_i \in M_J(u, U)$, otherwise. This suggests the pairwise property.

Division I and Induced division. For these division the pairwise property follows immediately from Definitions 3.4 and 3.7. □

4.3. Monotonicity.

Consider now another optimization related to the choice of a nonmultiplicative prolongation in line 5 of algorithm **InvolutiveCompletion**. The choice of the lowest prolongation with respect to some fixed ordering $\sqsubset$ is called *normal selection strategy* [1].

Definition 4.7. *Given a division L and an admissible ordering $\sqsubset$, a monomial set U will be called complete up to monomial w with respect to $\sqsubset$ if*

$$(\forall u \in U)\ (\forall x \in NM_L(u, U))\ (u \cdot x \sqsubseteq w)\ [\ u \cdot x \in C_L(U)\ ], \qquad (9)$$

where $C_L(U)$ is involutive cone of U by Definition 2.5. We call monomial w bound of completeness for U. If $u \cdot x \sqsupset w$ for all $u \in U$, $x \in NM_L(u, U)$, then we shall still say that U is completed up to w.

Definition 4.8. *We shall call division L monotone for $\sqsubset$ if for any set U and any monomial $w \in \mathbb{M}$ satisfying (9) the following holds:*

$$(\forall v \in U)\ (\forall x \in NM_L(v, U))\ (v \cdot x \notin C_L(U))$$
$$[\ U \cup \{v \cdot x\}\ \text{ is complete up to }\ w\ ].$$

We shall say that L is monotone if its monotonicity holds for any ordering $\sqsubset$.

Thus, monotonicity means that enlargement of U by an irreducible nonmultiplicative prolongation does not decrease its completeness bound.

Remark 4.9. If a division L is monotone for an ordering $\sqsubset$, then the choice of the latter as a completion ordering is beneficial for the algorithm **InvolutiveCompletion**. By Theorem 4.3, the total number of prolongations checked is invariant on the ordering. Monotonicity of the latter allows one to omit recomputing separations and checking prolongations which are lower than the current completeness bound.

Now we consider the monotonicity properties of different divisions defined in Sec. 2. Pommaret division and Division II, as globally defined, are trivially monotone.

Proposition 4.10. *Thomas division is monotone.*

Proof. From Definition 3.1 it follows immediately that $T(u,U) = T(u, U \cup \{v \cdot x\})$ for any $v \in U$, $x \in NM_T(v,U)$. $\square$

Proposition 4.11. *Janet division is monotone for lexicographical ordering.*

Proof. Denote the lexicographical completion ordering compatible with (1) by $\sqsubset_{\mathrm{Lex}}$. Consider a nonmultiplicative prolongation $v \cdot x_j \notin C_J(U)$ $(v \in U)$ such that $v \cdot x_j \sqsupset_{\mathrm{Lex}} w$ where w is the completeness bound of U in accordance with (9).

Suppose there is a pair $\{u \in U, x_k\}$, satisfying

$$\begin{gathered} ux_k \in C_J(U), \quad u \cdot x_k \notin C_J(U \cup \{vx_j\}), \\ u \cdot x_k \sqsubseteq_{\mathrm{Lex}} w \sqsubset_{\mathrm{Lex}} v \cdot x_j, \end{gathered} \tag{10}$$

and consider the lowest such pair with respect to $\sqsubset_{\mathrm{Lex}}$.

If $x_k \in J(u,U)$ we obtain

$$\begin{cases} \deg_1(u) = \deg_1(v) + 1, & \\ \deg_k(u) < \deg_k(v) & if \;\; j = 1, \\ \deg_i(u) = \deg_i(v) \ (i < j), & \\ \deg_j(u) = \deg_j(v) + 1, & \\ \deg_k(u) < \deg_k(v) & if \;\; j > 1. \end{cases}$$

Here $k > j$ and, if $k - j > 1$, then $\deg_m(u) = \deg_m(v)$ for all $l < m < k$. Consider now two alternatives:

(i) $w \in U$. In this case conditions (relat) are contradictory since from the rightmost condition it follows $\deg_i(u) = \deg_i(w)$ $(i < k)$ and $\deg_k(w) > \deg_k(u)$, that is, $x_k \in NM_J(u, U)$.

(ii) $w \notin U$. Then there is $t \in U$ such that $w \in tJ(t, U)$. Because $x_k \in J(u, U)$, for some $1 \leq p < k$ we have $\deg_i(t) = \deg_i(u) = \deg_i(vx_j)$ where $i \leq p$ and $\deg_{p+1}(t) < \deg_{p+1}(u) \leq \deg_{p+1}(w)$. Thus we obtain contradiction with $x_{p+1} \in J(t, U)$ which follows from $w \in tJ(t, U)$.

It is remains to prove that if $x_k \in NM_J(u, U)$, then $u \cdot x_k \in C_J(U \cup \{v \cdot x_j\})$. If $u \cdot x_k \in U$ we are done. Otherwise, we have $u \cdot x_k = q_1\, r_1$ for some $q_1 \in U$, $r_1 \in J(q, U)$ and $r_1 \notin J(U \cup \{v \cdot x_j\})$. Hence, there is $x_{i_1} | r_1$, $x_{i_1} \in NM_J(q_1, U \cup \{v \cdot x_j\})$, and $\deg(q_1 \cdot x_{i_1}) \sqsubset_{\mathrm{Lex}} \deg(u \cdot x_k)$. Then, by our assumption that prolongation $u \cdot x_k$ is the lowest satisfying (10), we have $q_1 \cdot x_{i_1} = q_2 \times r_2$, $q_2 \in U$, $r_2 \in J(q_2, U \cup v \cdot x_j)$. By property (d) in Definition 2.1, it yields $r_2 \in J(q_2, U)$, and, hence, $q_1 \times x_{i_1} = q_2 \times r_2$ in U. This is impossible, because any monomial set is Janet autoreduced. □

Remark 4.12. Janet division is not monotone for degree-lexicographical and degree-reverse-lexicographical orderings as the following example shows.

Example 4.13. Consider the conventionally autoreduced set $U = \{xz^2, x^2z, yzt^2\}$. Let completion ordering $\sqsubset$ be degree-lexicographical or degree-reverse-lexicographical ordering with $x \sqsupset y \sqsupset z \sqsupset t$. U is complete up to $w = x^2yz$. The lowest irreducible prolongation is $xyzt^2 \sqsupset w$. The next one in the set $\{xz^2, x^2z, yzt^2, xyzt^2\}$ is $xyz^2 \sqsubset w$.

Example 4.14. Consider the set $U = \{xy^2w^2, xzt, yzt\}$ and Division I generating the separation:

Monomial	Division I	
	M_I	NM_I
$p = xy^2w^2$	x, y, w	z, t
$v = xzt$	x, z, t	y, w
$u = yzt$	y, z, t, w	x

Let $x \sqsupset y \sqsupset z \sqsupset t \sqsupset w$ and $\sqsupset$ be any of the orderings: lexicographical, degree-lexicographical or degree-reverse-lexicographical. The bound of completeness for U is xyw^2. We find that $v \cdot w = u \cdot x = xztw$ is the lowest irreducible prolongation in U, and the next one for $U \cup \{xztw\}$ is $u \cdot w \sqsubset xyw^2$. Therefore, Division I is not monotone for three orderings considered.

Proposition 4.15. *Induced division is monotone for the ordering which induces this division.*

Proof. By Definition 3.7 of $D_{\sqsubset}$, enlargement of U by irreducible non-multiplicative prolongation $v \cdot x_j \sqsupset w$ $(v \in U)$ does not change the reducibility properties of those prolongations ux_k $(u \in U)$ which satisfy $ux_k \sqsubset v \cdot x_j$. $\square$

5. Construction of involutive bases for polynomial ideals

In this section we present the following algorithm for computation of minimal involutive bases of polynomial ideals which generalizes the algorithm of paper [2] to different completion and main orderings.

Algorithm **MinimalInvolutiveBasis:**

Input: F, a finite polynomial set; L, an involutive division;
$\succ$, a main ordering; $\sqsubset$, a completion ordering

Output: G, the minimal involutive basis of $Id(F)$ if algorithm terminates

begin
$F := Autoreduce(F)$
choose $g \in F$ with the lowest $lm(g)$ w.r.t. $\prec$
$T := \{(g, lm(g), \emptyset)\}$; $Q := \emptyset$; $G := \{g\}$
for each $f \in F \setminus \{g\}$ **do**
$Q := Q \cup \{(f, lm(f), \emptyset)\}$
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. $\prec$
$Q := Q \setminus \{(g, u, P)\}$
if $Criterion(g, u, T)$ is false **then** $h := NF_L(g, G)$
end

14 **if** $h \neq 0$ **then** $G := G \cup \{h\}$
15 **if** $lm(h) = lm(g)$ **then** $T := T \cup \{(h, u, P)\}$
16 **else** $T := T \cup \{(h, lm(h), \emptyset)\}$
17 **for each** f in $(f, v, D) \in T$ s.t. $lm(f) \succ lm(h)$**do**
18 $T := T \setminus \{(f, v, D)\}$; $Q := Q \cup \{(f, v, D)\}$; $G := G \setminus \{f\}$
19 **while** exist $(g, u, P) \in T$ and $x \in NM_L(g, G) \setminus P$ and, if $Q \neq \emptyset$,
20 s.t. $lm(g \cdot x) \prec lm(f)$ for all f in $(f, v, D) \in Q$ **do**
21 **choose** such $(g, u, P), x$ with the lowest $lm(g) \cdot x$ w.r.t. $\sqsubset$
22 $T := T \setminus \{(g, u, P)\} \cup \{(g, u, P \cup \{x\})\}$
23 **if** $Criterion(g \cdot x, u, T)$ is false **then** $h := NF_L(g \cdot x, G)$
24 **if** $h \neq 0$ **then** $G := G \cup \{h\}$
25 **if** $lm(h) = lm(g \cdot x)$ **then** $T := T \cup \{(h, u, \emptyset)\}$
26 **else** $T := T \cup \{(h, lm(h), \emptyset)\}$
27 **for each** f in $(f, v, D) \in T$ with $lm(f) \succ lm(h)$ **do**
28 $T := T \setminus \{(f, v, D)\}$; $Q := Q \cup \{(f, v, D\})$; $G := G \setminus \{f\}$
29 **end**
30 **until** $Q \neq \emptyset$
31 **end**

$Criterion(g, u, T)$ is true provided that if there is $(f, v, D) \in T$ such that $lm(f)|_L\, lm(g)$ and $lcm(u, v) \sqsubset lm(g)$. Correctness of this criterion, which is just the involutive form [1] of Buchberger's chain criterion [10], is provided by Corollary 2.22.

Theorem 5.1. *Let F be a finite subset of $\mathbb{R}$ and L be a constructive involutive division. Suppose the completion ordering $\sqsubset$ is degree compatible. Then the 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 completion ordering.*

Proof. The proof is the same as in [2] and based on Theorems 2.19, 2.20, and 4.1, Corollaries 2.22 and 4.2. □

Proposition 5.2. *The conventional autoreduction of the input polynomial set in line 2 is optional and may be omitted.*

Proof. Let F be a non-autoreduced set and the algorithm start with line 3. Subsequent to the initializion in lines 4 and 5 the upper **while**-loop selects, first of all, those polynomials in the triple set Q which have the same leading term as the element in $G = \{g\}$. If there is such a polynomial in the triple set Q with nonzero involutive normal form h computed in line 12, then $lm(h) \sqsubset lm(g)$. It follows from lines 14 and 18 that G becomes the one-element set $\{h\}$ as an input for the lower **while**-loop.

Thus, by restriction in line 20 for nonmultiplicative prolongations checked and redistribution of polynomials in line 28, in every step of the algorithm we have $lm(g) \sqsubset lm(f)$ for any g in $(g, u, P) \in T$ and f in $(f, v, D) \in Q$ whenever the set Q is nonempty.

Furthermore, as proved in [1, 2], in some step of the algorithm a polynomial h is added to the current polynomial set G in line 14 or in line 24, such that h is an element in the reduced Gröbner basis of $Id(F)$ with the lowest leading monomial with respect to the completion ordering $\sqsubset$. It implies the reduction of G to the one-element set $G = \{h\}$, and transfer of the rest to Q. Then G is sequentially completed by other polynomials from the reduced Gröbner basis and their nonmultiplicative prolongations. In so doing, the completion of $lm(G)$ due to the redistribution of polynomials between sets T and Q in lines 18 and 28 is monotone with respect to $\sqsubset$.

Therefore, the output of algorithm **MinimalInvolutiveBasis** irrespective of autoreduction in line 2 is the same as it would be for the reduced Gröbner basis in the input. $\square$

Remark 5.3. The choice of a completion ordering which is monotone for L preserves, obviously, the partial involutivity of the intermediate polynomial set G in the cause of its enlargement in line 23, if $lm(h) = lm(g \cdot x)$. Therefore, similar to the monomial case (c.f. Remark 4.9), this saves computing time for recomputing separations and checking irreducibility of nonmultiplicative prolongations unless L is globally defined anyway.

6. Conclusion.

The above described optimizations concern only that part of computing involutive bases which is related to completion by nonmultiplicative prolongations with irreducible leading terms. Another important step is to search for an involutive divisor among the leading monomials of an intermediate basis. This is important for efficient computation of the involutive normal form in lines 11 and 22 of algorithm **MinimalInvolutive-Basis**. Some related optimizations are considered in [14] for the purpose of implementating the algorithm **InvolutiveCompletion** in Mathematica for divisions of Sec .3.

A promising way to the further optimization of computation is related to the ideas of paper [12]. By appropriate dynamical refinement of an involutive division in the course of computation, one can decrease the total number of nonmultiplicative prolongations to be checked. This may lead to a notable reduction of computing time.

Algorithm **MinimalInvolutiveBasis** has been implemented in Reduce for Pommaret division. Computer experiments showed that thi algorithm is somewhat faster than our previous version of involutive algorithm also implemented in Reduce for Pommaret bases [1]. For a non-globally defined division the difference in speed is to be much greater as algorithm **MinimalInvolutiveBasis** deals with fewer intermediate polynomials and avoids intermediate autoreductions [2].

With the new implementation one needs, for example, 57 seconds to compute a degree-reverse-lexicographical Pommaret basis for 6th cyclic roots on an Pentium 100 Mhz computer, and 30 seconds for the 6th Katsura system. By comparison, the PoSSo software for computing Gröbner bases[2] needs for these examples 24 and 36 seconds, respectively.

7. Acknowledgements. The author thanks Joachim Apel, Matthias Berth and Yuri Blinkov for helpful discussions and comments. This work was partially supported by grant INTAS-96-184 and grants from the Russian Foundation for Basic Research Nos. 96-15-96030 and 98-01-00101.

References

1. V. P. Gerdt, Yu. A. Blinkov , *Involutive bases of polynomial ideals.* Preprint No. 1 (1996), Naturwissenschaftlich-Theoretisches Zentrum, University of Leipzig (1996); *Math. Comp. Sim.*, **45**, (1998), 519–542 .
2. V. P. Gerdt, Yu. A. Blinkov , *Minimal involutive bases.* Preprint JINR E5-4-1997, Dubna (1997); *Math. Comp. Simul.* **45**, (1998), 543–560 .
3. 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) .
4. J.-F. Pommaret , *Partial differential equations and group theory New perspectives for applications.* Kluwer, Dordrecht (1994) .
5. V. P. Gerdt , *Gröbner Bases and involutive methods for algebraic and differential equations.* Computer Algebra in Science and Engineering. J. Fleischer, J. Grabmeier, F. W. Hehl, W. Küchlin (eds.), World Scientific, Singapore (1995), pp. 117-137; *Math. Comput. Modelling* **25**, Nos. 8/9, (1997) 75-90 .
6. M. Janet , *Sur les Systèmes d'Equations aux Dérivées Partielles.* — J. Math. Pure et Appl. **3** (1920), 65–151 .

[2]URL: http://janet.dm.unipi.it/posso_demo.html

7. J. Thomas , *Differential Systems.* American Mathematical Society, New York (1937) .
8. J. E. Pommaret , *Systems of partial differential equations and Lie pseudogroups.* Gordon & Breach, New York (1978) .
9. A. Yu. Zharkov, Yu. A. Blinkov , *Involutive approach to investigating polynomial systems.* Proceedings of "SC 93" International IMACS Symposium on Symbolic Computation: New Trends and Developments (Lille, June 14–17, 1993). *Math. Comp. Simul.*, **42** (1996), pp. 323-332 .
10. B. Buchberger , *Gröbner bases: an algorithmic method in polynomial ideal theory.* Recent Trends in Multidimensional System Theory,. N. K. Bose (ed.), Reidel, Dordrecht (1985), pp. 184–232 .
11. T. Becker, V. Weispfenning, and H. Kredel , *Gröbner bases. A computational approach to commutative algebra.* Graduate Texts in Mathematics, **141**, Springer-Verlag, New York (1993) .
12. J. Apel , *Theory of involutive divisions and an pplication to Hilbert function.* To appear in *J. Symb. Comp.* (1997) .
13. A. Yu. Zharkov , *Solving zero-dimensional involutive systems.* Algorithms in Algebraic Geometry and Applications. L. Gonzales-Vega, T. Recio (eds.) Progress in Mathematics, Vol. 143, Birkhäuser, Basel (1996), pp.389–399. .
14. V. P. Gerdt, M. Berth, and G. Czichowski , *Involutive divisions in mathematica: Implementation and some applications.* Proceedings of the 6th Rhein Workshop on Computer Algebra. (Sankt-Augustin, Germany, March 31–April 3, 1998), J. Calmet (Ed.), Institute for Algorithms and Scientific Computing. GMD-SCAI, Sankt-Augustin (1998) pp. 74–91 .
15. F. Schwarz , *An algorithm for determining the size of symmetry groups.* — Computing **49** (1992), 95–115 .
16. F. Schwarz , *Janet bases of* 2^{nd} *order ordinary differential equations.* Proceedings of the ISSAC'96. Y. N. Lakshman (ed.), ACM Press (1996), pp. 179–188 .
17. W. M. Seiler , *Analysis and application of the formal theory of partial differential equations.* PhD Thesis, Lancaster University (1994) .

Laboratory of Computing
Techniques and Automation
Joint Institute for
Nuclear Research
141980 Dubna, Russia
gerdt@jinr.ru

Поступило 15 мая 1999 г.