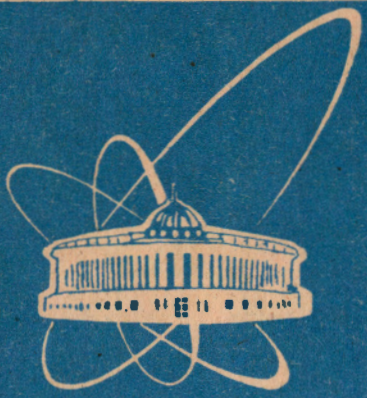

ОБЪЕДИНЕННЫЙ
ИНСТИТУТ
ЯДЕРНЫХ
ИССЛЕДОВАНИЙ

Дубна

E5-97-3

V.P.Gerdt, Yu.A.Blinkov[1]

INVOLUTIVE BASES OF POLYNOMIAL IDEALS

Submitted to «Journal of Symbolic Computation»

[1]Saratov State University, Russia

1997

1 Introduction

In modern times the Gröbner bases method invented in (Buchberger, 1965) has become one of the most universal algorithmic tools for analyzing and solving polynomial equations (Buchberger, 1985; Becker, Weispfenning and Kredel, 1993). Even in the general case, when the roots cannot be exactly computed, the method is still able to obtain valuable information about the solutions. In particular, it allows one to verify compatibility of the initial equations and compute the dimension of the solution space. For the last few years notable progress has been achieved in extension of the Gröbner bases method to non-commutative (Mora, 1988; Kandri-Rody and Weispfenning, 1990) and differential algebras (Carra'Ferro, 1987 and Ollivier, 1990).

On the other hand, already by the early 20s the foundation of a constructive approach to algebraic analysis of partial differential equations was laid by Riquier (1910) and Janet (1920) giving, among other things, answers to the same general questions of compatibility and dimension. Later on, this approach, in the context of partial differential equations, was developed by Thomas (1937) and more recently by Pommaret (1978). The main idea of the approach, as with the computation of a Gröbner basis, is rewriting the initial differential system into another, so-called, involutive form (Gerdt, 1995).

In the involutive approach, unlike the Gröbner basis method, independent variables for each equation are separated into two distinct groups called multiplicative and non-multiplicative. Such a separation is determined by the structure of the leading derivative terms. A differential system is called involutive if its non-multiplicative derivatives are algebraic consequences of multiplicative ones. In doing so, Janet (1920), Thomas (1937) and Pommaret (1978) used different separations of variables.

In Zharkov and Blinkov (1993, 1994) it was argued that the involutive technique along with the Gröbner basis one can be used in commutative algebra. Based on the definition of multiplicative and non-multiplicative variables as given in Pommaret (1978), Zharkov and Blinkov (1993, 1994) proved, among other things, that an involutive basis is a Gröbner one. Moreover, their computational experience demonstrated a reasonably high efficiency of the new algorithm when it terminates. The termination, however, does not hold, generally, for positive dimensional ideals, while for zero-dimensional ones it does for any degree-compatible monomial orderings (Zharkov and Blinkov, 1994). Apart from that, the Pommaret involutive form of Gröbner bases for zero-dimensional polynomial ideals reveals a number of rather attractive features (Zharkov, 1994*a*).

In the present paper we consider an algorithmic technique more general than that proposed by Zharkov and Blinkov (1993, 1994) for the involutive analysis of polynomial ideals. First of all, we introduce a new concept of involutive monomial division (Sect.3) which leads to the self-consistent separation of the whole set of variables into multiplicative and non-multiplicative subsets. Given an admissible ordering, the separation is applied to polynomials in terms of their leading monomials. That concept generalizes also the particular choice used in Janet (1920), Thomas (1937) and Pom-

maret (1978) for involutive analysis of partial differential equations. We characterize also important properties of noetherity and continuity for involutive division (Sect.4). Noetherity provides for the existence of a finite involutive basis for any polynomial ideal. Continuity allows one to construct that basis algorithmically. It is shown that Thomas and Janet divisions are both noetherian and continuous whereas Pommaret division being continuous is not noetherian.

Given an involutive division, we define an involutive reduction and an involutive normal form (Sect.5). As this takes place, we show that much like the Pommaret normal form, investigated in Zharkov and Blinkov (1993), the general involutive normal form is also unique and linear. Then we define involutive systems by analogy with differential equations (Sect.6). To be involutive, systems are required to satisfy the involutivity conditions, which form the basis for their algorithmic construction.

We prove (Sect.7) that any involutive basis, if it exists, is a special, generally extended, form of the reduced Gröbner basis. Though it is unique for Pommaret division (Zharkov and Blinkov, 1994), generally, it may not be the case, as is shown by an explicit example. We propose an algorithm for construction of involutive polynomial bases (Sect.8). Its correctness is proved for any continuous involutive division and for arbitrary admissible monomial ordering, while its termination holds, generally, for noetherian divisions. The algorithm is an improved and generalized version of one proposed in Zharkov and Blinkov (1994) and Zharkov (1994*a*), and has been implemented in Reduce for Pommaret division. The main improvement is the incorporation of Buchberger's chain criterion.

By the example of cyclic 6-th roots we illustrate the efficiency of the current implementation and its rather smooth behavior with respect to variation of ordering between variables.

2 Preliminaries

Let $\mathbb{R} = K[x_1, \ldots, x_n]$ be a polynomial ring over the field K of characteristic zero. In this paper we use the notations:

f, g, h, p, q are polynomials in $\mathbb{R}$.
a, b, c are elements in K.
F, G, H are finite subsets of $\mathbb{R}$.
$\mathbb{N}$ is the set of non-negative integers.
$\mathbb{M} = \{ x_1^{d_1} \cdots x_n^{d_n} \mid d_i \in \mathbb{N}, i = 1, \ldots, n \}$ is the set of monomials in $\mathbb{R}$.
$\mathbb{T} = \{ a\,u \mid u \in \mathbb{M}, a \in K \}$ is the set of terms in $\mathbb{R}$.
u, v, w, s, t are monomials or terms with nonzero coefficients.
U, V, W are finite subsets of $\mathbb{M}$.
$deg_i(u)$ is the degree of x_i in u.
$deg(u)$ is the total degree of u.
$cf(f, u) \in K$ is the coefficient of the term u of the polynomial f.
$Id(F)$ is the ideal in $\mathbb{R}$ generated by the polynomial set F.

$\succ$ is an admissible monomial ordering with $x_1 \succ x_2 \succ \cdots \succ x_n$.
$lt(f)$ is the leading term of f w.r.t. the ordering $\succ$.
$lc(f) = cf(f, lt(f))$ is the leading coefficient of f.
$lm(f) = lt(f)/lc(f)$ is the leading monomial of f.
$lm(F) = \{ lm(f) \mid f \in F \}$ is the set of the leading monomials of F.
$lcm(F)$ is the least common multiple of the set $\{ lm(f) \mid f \in F \}$.

If the monomial u divides the monomial v we shall write $u|v$.

3 Involutive Monomial Division

Definition 3.1 We shall say that an *involutive division* L or $L-$*division* is given on $\mathbb{M}$ if for any finite set $U \subset \mathbb{M}$ a relation $|_L$ is defined on $U \times \mathbb{M}$ such that for any $u \in U$, $w \in \mathbb{M}$ the following holds:

(i). $u|_L w$ implies $u|w$.

(ii). $u|_L u$ for any $u \in U$.

(iii). $u|_L(uv)$ and $u|_L(uw)$ if and only if $u|_L(uvw)$.

(iv). If $u|_L w$ and $v|_L w$ for $u, v \in U$ and $w \in \mathbb{M}$, then $u|_L v$ or $v|_L u$.

(v). If $u|_L v$ and $v|_L w$ for $u, v \in U$ and $w \in \mathbb{M}$, then $u|_L w$.

(vi). If $V \subseteq U$ and $u \in V$, then $u|_L w$ w.r.t. U implies $u|_L w$ w.r.t. V.

If $u|_L(w = uv)$, we say u is an *involutive divisor* of w, w is an *involutive multiple* of u, and v is *multiplicative* for u. In such an event we shall write $w = u \times v$. If u is the conventional divisor of w but not the involutive one we shall write, as usual, $w = u \cdot v$. Then v is said to be *non-multiplicative* for u.

The conventional monomial division, obviously, satisfies condition (iv) only in the univariate case. The simplest bivariate example: $x|(xy)$ and $y|(xy)$ but $\neg x|y$ and $\neg y|x$.

Definition 3.1 for each $u \in U$ provides separation of the set of variables

$$\{x_1, \ldots, x_n\} = M(u, U) \cup NM(u, U)$$

into two disjoined subsets ($M \cap NM = \emptyset$) of *multiplicative* $M(u, U)$ and *non-multiplicative* $NM(u, U)$ variables. It is convenient to define an involutive division for a monomial set just by specifying the subsets of multiplicative and non-multiplicative variables to satisfy the conditions (iv)-(vi). The other conditions will be fulfilled by the construction.

Given involutive division L and finite set U, for each $u \in U$ let $L(u, U) \subseteq \mathbb{M}$ be a set of multiplicative monomials for u, that is,

$$u|_L v \iff v \in uL(u, U). \tag{1}$$

Then it is easy to see that Definition 3.1 admits another form:

Definition 3.2 An *involutive division* L on $\mathbb{M}$ is given, if for any finite $U \subset \mathbb{M}$ and for any $u \in U$ there is given a submonoid $L(u,U)$ of $\mathbb{M}$ satisfying the conditions:

(a). If $u, v \in U$ and $uL(u,U) \cap vL(v,U) \neq \emptyset$, then $u \in vL(v,U)$ or $v \in uL(u,U)$.

(b). If $v \in U$ and $v \in uL(u,U)$, then $L(v,U) \subseteq L(u,U)$.

(c). If $V \subseteq U$, then $L(u,U) \subseteq L(u,V)$ for all $u \in V$.

Indeed, by the conditions (i)-(iii) in Definition 3.1, the set $L(u,U) \subseteq \mathbb{M}$, as defined in (1), is a submonoid under the natural multiplication. The conditions (a),(b) and (c) in Definition 3.2 are nothing else than those (iv),(v) and (vi) in Definition 3.1.

We consider three different examples of involutive division introduced in Janet (1920), Thomas (1937) and Pommaret (1978) for analysis of algebraic differential equations. In doing so, we give, firstly, the definition of multiplicative and non-multiplicative variables for each of the divisions, and, secondly, prove the fulfillment of the three extra conditions.

Definition 3.3 *Thomas division* (Thomas, 1937). Given finite set U, let

$$h_i = max\{\ deg_i(u) \mid u \in U\ \}.$$

A variable x_i is considered as multiplicative for $u \in U$ if $deg_i(u) = h_i$ and non-multiplicative, otherwise.

Definition 3.4 *Janet division* (Janet, 1920). Let U be a finite set. For each $1 \leq i \leq n$ divide U into groups labeled by non-negative integers $d_1, \ldots, d_i$:

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

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 3.5 *Pommaret division* (Pommaret, 1978). For a monomial $x_1^{d_1} \cdots x_k^{d_k}$ with $d_k > 0$ the variables x_j with $j \geq k$ are considered as multiplicative and x_j with $j < k$ as non-multiplicative. For $u = 1$ all the variables are multiplicative.

We note that

- Thomas division does not depend on the ordering on the variables x_i. Janet and Pommaret divisions, as defined, are based on the ordering of the variables assumed in Sect.2.

- The separation of variables into multiplicative and non-multiplicative ones for Thomas and Janet divisions are defined in terms of the whole set U. Contrastingly, Pommaret division is determined in terms of the monomial itself, regardless of the others, and, by this reason, admits extension to infinite monomial sets, unlike Thomas and Janet divisions.

To distinguish the above divisions the related subscripts T, J, P will be used.

Proposition 3.6 *Thomas, Janet and Pommaret monomial divisions are involutive.*

Proof According to the above remark we must prove that the conditions (iv)-(vi) in Definition 3.1 are satisfied.

Let u be a Thomas divisor of $w \in \mathbb{M}$, that is, $w = u \times v$. Then $deg_i(v) = deg_i(w) - h_i$ if $deg_i(w) \geq h_i$ and $deg_i(v) = 0$ if $deg_i(w) < h_i$. Thus, if w has an involutive divisor u, then w/u is uniquely defined, and, hence, u is unique in U. It implies also the property (v) for Thomas division, since $u|_T v$ for $u, v \in U$ if and only if $u = v$. The property (vi) also follows since any h_i for V is less than or equal to the corresponding h_i for U.

Let now $u, v \in U$ be two different Janet divisors of w, such that $deg_i(u) = deg_i(v) = d_i$ for $1 \leq i < k \leq n$ and assume, for definiteness, that $deg_k(u) > deg_k(v)$. Then, since both u, v are members of the same group $[d_1, \ldots, d_{k-1}]$, the variable x_k is non-multiplicative for v. Hence, if u is a Janet divisor of w such that $deg_k(w) \geq deg_k(u) > deg_k(v)$, then v is not Janet divisor. In other words, similar to Thomas division, any monomial $w \in \mathbb{M}$ cannot have different Janet divisors in any set U. A monomial group may only be decreased by diminishing the set U what implies the relation (vi).

Lastly, consider a Pommaret divisor u of the monomial $w = x_1^{d_1} \cdots x_m^{d_m}$ with $m \leq n$. By definition, u constitutes a left subset of the string representation for w as it is shown.

$$w = \overbrace{\underbrace{x_1 \cdots x_1}_{d_1} \cdots}^{u} \cdots \underbrace{x_m \cdots x_m}_{d_m}. \tag{2}$$

It makes evident the fulfillment of the conditions (iv) and (v) for Pommaret division while the condition (vi) trivially holds since the division does not depend on the set U at all. □

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

Proof If $x_i \in M_J(u,U)$, $u \in [d_1, \ldots, d_{i-1}]$, then, by definition,

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

Hence, $x_i \in M_T(u,U)$ implies $x_i \in M_J(u,U)$. □

Definition 3.8 A set U is called *involutively autoreduced* with respect to division L or *L−autoreduced* if it does not contain elements L−divisible by other elements in U.

Proposition 3.9 *If U is $L-$autoreduced, then any monomial $w \in \mathbb{M}$ has at most one $L-$involutive divisor in U.*

Proof This follows immediately from the property (iv) of involutive division. In terms of Definition 3.2 it means that $uL(u,U) \cap vL(v,u) = \emptyset$ for all distinct $u, v \in U$, if U is involutively autoreduced. □

Proposition 3.10 (Zharkov, 1994b). *If set U is autoreduced with respect to Pommaret division, then for any $u \in U$ $M_P(u,U) \subseteq M_J(u,U)$ and $NM_J(u,U) \subseteq NM_P(u,U)$, respectively.*

Proof Let $u = x_1^{d_1} \cdots x_k^{d_k} \in \mathbb{M}$ be a monomial with $d_k > 0$ and $v \in U$ be its Pommaret divisor. Then, as follows from the representation (2), $v = x_1^{d_1} \cdots x_{m-1}^{d_{m-1}} x_m^r$ with $1 \leq m \leq k$ and $1 \leq r \leq d_m$. It means that $v \in [d_1, \ldots, d_{m-1}]$. Since U is autoreduced by Pommaret division, there are no other members of the same group with degree in x_m higher than r. Therefore, v is also a Janet divisor of u, and u/v being Pommaret multiplicative for u is also Janet multiplicative. □

Example 3.11 $U = \{xy, y^2, z\}$ $(x \succ y \succ z)$.

	Thomas		Janet		Pommaret	
monomial	M_T	NM_T	M_J	NM_J	M_P	NM_P
xy	x	y, z	x, y, z	$-$	y, z	x
y^2	y	x, z	y, z	x	y, z	x
z	z	x, y	z	x, y	z	x, y

4 Involutive Monomial Sets

Definition 4.1 Given an involutive division L, a set U is called *involutive* with respect to L or $L-$*involutive*, if any multiple of some element $u \in U$, is also $(L-)$involutively multiple of element $v \in U$, generally, different from u. It means that

$$(\forall u \in U)\ (\forall w \in \mathbb{M})\ (\exists v \in U)\ \ [\ v|_L(uw)\ ] \tag{3}$$

or, in accordance with (1) and Definition 3.2,

$$\cup_{u \in U} u\,\mathbb{M} = \cup_{u \in U} u\,L(u,U).$$

Definition 4.2 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 and only if its cone $C(U)$ coincides with its involutive cone $C_L(U)$.

Definition 4.3 A finite set $\tilde{U} \subset \mathbb{M}$ will be called *involutive closure* of a set $U \subseteq \tilde{U}$ with respect to the involutive division L if $C_L(\tilde{U}) = C(U)$. If there exists an involutive closure $\tilde{U}$ of the set U, then the latter is said to be *finitely generated* with respect to L. The involutive division L is called *noetherian* if every finite set U is finitely generated.

Proposition 4.4 *Given a noetherian involutive division L, every monomial ideal U has a finite involutive basis.*

Proof It is an immediately consequence of Definition 4.3 and Dickson's lemma (Becker, Weispfenning and Kredel, 1993). □

Proposition 4.5 *Thomas and Janet divisions are noetherian.*

Proof Given finite set U, consider the monomial $h = x_1^{h_1} \cdots x_n^{h_n}$ where, as given in the definition of Thomas division, $h_i = max\{\ deg_i(u) \mid u \in U\ \}$, and form the finite set $V \subset \mathbb{M}$ of all the different monomials v such that $v|h$ and $u|v$ for some $u \in U$. The set V, which contains, in particular, the monomial h and the initial set U, is involutive for Thomas division. Indeed, let $w = x_1^{d_1} \cdots x_n^{d_n}$ be multiple of some $u \in V$. If $w \in V$, then, obviously, $w \in C_T(V)$. Otherwise, let $\{d_{i_1}, \ldots, d_{i_k}\}$ $(k \leq n)$ be the nonempty set which contains all the exponents d_i $(1 \leq i \leq n)$ in w such that $d_{i_1} > h_{i_1}, \ldots, d_{i_k} > h_{i_k}$. Then there exists $v \in V$ satisfying

$$w = v\, x_{i_1}^{d_{i_1} - h_{i_1}} \cdots x_{i_k}^{d_{i_k} - h_{i_k}}.$$

Since $deg_{i_1}(v) = h_{i_1}, \ldots, deg_{i_k}(v) = h_{i_k}$, v is a Thomas involutive divisor of w, and, hence, $w \in C_T(V)$.

Furthermore, from Proposition 3.7 it follows that there is a subset of V which is an involutive set for U with respect to Janet division. □

Definition 4.6 Multiplication of a monomial $u \in U$ by a variable x is called the *prolongation* of u. Given involutive division specified by the set U, the prolongation is called *multiplicative* if x is multiplicative for u and *non-multiplicative*, otherwise.

In construction of involutive sets the following concept of local involutivity plays the crucial role and admits the direct extension to polynomial sets (see Sect.6).

Definition 4.7 A set U is called *locally involutive* with respect to the involutive division L if any non-multiplicative prolongation of any element in U has an involutive divisor in U, that is,

$$(\forall u \in U)\ (\forall x_i \in NM(u,U))\ (\exists v \in U)\ \ [\ v|_L(u \cdot x_i)\ ] \tag{4}$$

In accordance with Definition 4.1, the conditions (4), apparently, are necessary for involutivity of U. Generally, however, they not sufficient, as the next simple example shows.

Example 4.8 Let L be an involutive division on $\mathbb{M} \subset K[x,y,z]$ defined by the table

monomial	M	NM
1	x,y,z	–
x	x,z	y
y	x,y	z
z	y,z	x
$u \in \mathbb{M} \mid deg(u) \geq 2$	–	x,y,z

It is easy to see that all properties listed in Definition 3.1 (3.2) are satisfied, and the set $U = \{x,y,z\}$ is locally involutive. For instance, $x \cdot y = y \times x$. However, U is not involutive since none $u \in \mathbb{M}$ with $deg_x(u) > 0, deg_y(u) > 0, deg_z u > 0$, e.g. xyz, has involutive divisors in U.

The following definition and theorem enable one to reveal involutive divisions providing involutivity of every locally involutive set, and thereby allowing to use the involutive algorithms described below.

Definition 4.9 An involutive division L will be called *continuous* if for any finite set U and for any finite sequence $\{u_i\}_{(1 \leq i \leq k)}$ of elements in U such that

$$(\forall i < k)\ (\exists x_j \in NM(u_i, U))\ \ [\ u_{i+1}|_L u_i \cdot x_j\ ] \qquad (5)$$

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

Theorem 4.10 *If an involutive division L is continuous then local involutivity of any set U implies its involutivity.*

Proof Let set U be locally involutive, and such that any sequence in U satisfying (5) has no coinciding elements. We must prove that U satisfies (3). Take any $u \in U$ and any $w \in \mathbb{M}$ and show that there is $v \in U$ such that $v|_L(uw)$. If $u|_L(uw)$ we are done. Otherwise, there is $x_{k_1} \in NM(u,U)$ such that w contains x_{k_1}. Then $u \cdot x_{k_1}$ has an involutive divisor $v_1 \in U$. If $v_1|_L(uw)$ we are done. Otherwise, there are $x_{k_2} \in NM(v_1,U)$ and $v_2 \in U$ such that uw/v_1 contains x_{k_2} and $v_2|_L(v_1 \cdot x_{k_2})$. Going on, we obtain the sequence $u, v_1, v_2, \ldots$ of elements in U satisfying (5). By construction, each element of the sequence divides uw. Since all the elements are distinct and uw has a finite number of distinct divisors, it follows that the above sequence in U is finite, and, hence, it ends up with an involutive divisor of uw. □

Corollary 4.11 *Thomas, Janet and Pommaret divisions are continuous.*

Proof Let U be a finite set, and $\{u_i\}_{(1 \leq i \leq k)}$ be a sequence of elements in U satisfying the conditions (5). We shall show that there cannot be coinciding elements in the sequence for three divisions.

It is ease to see that $u_{i+1}|_T(u_i \cdot x_{k_i})$ implies $u_{i+1} = u_i \cdot x_{k_i}$. Indeed, suppose that $u_i \cdot x_{k_i} = u_{i+1} \times v_{i+1}$. Since $x_{k_i} \in NM_T(u_i, U)$, v_{i+1} does not contain x_{k_i}. If v_{i+1} would contain any other variable x_{j_i}, then it would mean that $deg_{x_{j_i}}(u_i) > deg_{x_{j_i}}(u_{i+1})$, and, hence, x_{j_i} could not be multiplicative for u_{i+1}. Therefore, any Thomas sequence satisfying (5) consists of distinct elements.

If $u_{i+1}|_J(u_i \cdot x_{k_i})$, then from definition of Janet division it follows that $u_{i+1} \succ_{Lex} u_i$, where $\succ_{Lex}$ is the lexicographical ordering corresponding to the choice of variable order $x_1 \succ x_2 \succ \cdots \succ x_n$ as assumed in Sect.2. It is now obvious that $u_i \neq u_j$ for $i \neq j$ for Janet division.

Let now $u_{i+1}|_P(u_i \cdot x_{k_i})$. Then the representation (2) shows clearly that $u_{i+1} \succ_{RevLex} u_i$ where $\succ_{RevLex}$ is the reverse lexicographical ordering on $\mathbb{M}$ induced by the assumed variable order. □

Theorem 4.12 *Let U be a non-involutive finitely generated set with respect to a continuous division L. Then there is a procedure of constructing an involutive closure of U based on completion of U by non-multiplicative prolongations of its elements.*

Proof Given U, by Definition 4.3, there exists a finite involutive closure $\tilde{U}$ of U. Show that $\tilde{U}$ contains some non-multiplicative prolongations of elements in U. Assume for a contradiction that there are no such elements in $\tilde{U}$. Since set U is not involutive there exists a non-multiplicative prolongation of elements in U which has no involutive divisors in U.

Take any degree compatible monomial ordering $\prec$ and select $u_1 \in U$ with a non-multiplicative prolongation $u_1 \cdot x_{i_1} \notin U$ which is not involutive multiple of any element in U, and which is the lowest with respect to $\prec$. Since $\tilde{U}$ is involutive there is $v_1 \in \tilde{U} \setminus U$ and $1 \prec w_1 \in \mathbb{M}$ such that $u_1 \cdot x_{i_1} = v_1 \times w_1$. From the condition $C(U) = C_L(\tilde{U})$ it follows that v_1 is multiple of some $u_2 \in U$ with $deg(u_2) < deg(v_1)$. This implies $u_1 \cdot x_1 = u_2 \cdot v_2$ where $v_2 = v_1 w_1 / u_2$. Since $u_1 \cdot x_1$ has no involutive divisors in U, the monomial v_2 contains a variable $x_2 \in NM_L(u_2, U)$. Then we find $u_2 \cdot v_2 = (u_2 \cdot x_2)(v_2/x_2) = (u_3 \times w_3)(v_2/x_2)$. Now monomial (v_2/x_2) contains $x_3 \in MN_L(u_3, U)$, and we can continue this rewriting procedure. As a result we construct the sequence of elements in U satisfying condition (5). But then, by continuity of division L, this sequence ends up with an element $u \in U$ such that $u_1 \cdot x_{i_1} = u \times (v_1 w_1 / u)$ what contradicts our assumption.

Now instead of U take $U_1 = U \cup \{u_1 \cdot x_{i_1}\}$ where $u_1 \in U$ and $u_1 \cdot x_{i_1} \in \tilde{U}$ is the above considered lowest non-multiplicative prolongation. If set U_1 is not involutive, then it can be further completed by the lowest non-multiplicative prolongation. Since the set $\tilde{U}$ is finite, by repeating this completion procedure, in a finite number of steps we construct the set $\bar{U} \subseteq \tilde{U}$ which is an involutive closure of U. □

As an immediate consequence of the above described constructive procedure of completing a set U by non-multiplicative prolongations of its elements we have the following corollary.

Corollary 4.13 *If U is a finitely generated set with respect to a continuous involutive division, then there is the unique minimal involutive closure $\tilde{U}$ of U such that for any other involutive closure $\bar{U}$ the inclusion $\tilde{U} \subseteq \bar{U}$ holds.*

The following algorithm, given a continuous division L, computes the minimal involutive closure $\tilde{U}$ for any finitely generated set U at any fixed admissible ordering $\prec$.

Correctness. By Definitions 4.3, 4.7 and 4.9, if the algorithm terminates it computes an involutive closure of U. Its minimality follows from the below proved fact that, by the selection strategy, the involutive divisor of any non-multiplicative prolongation is always treated before the prolongation.

Algorithm **InvolutiveClosure:**

Input: U, a finite monomial set
Output: $\tilde{U}$, an involutive closure of U
begin
  $\tilde{U} := U$
  while exist $u \in \tilde{U}$ and $x \in NM(u, \tilde{U})$ such that
    $u \cdot x$ has no involutive divisors in $\tilde{U}$ **do**
    choose such u and x with the lowest $u \cdot x$ w.r.t. $\prec$
    $\tilde{U} := \tilde{U} \cup \{u \cdot x\}$
  end
end

Termination holds if U is finitely generated and $\prec$ is degree compatible, as shown in the proof of Theorem 4.12. To prove termination for any finitely generated set and for any admissible ordering we note that termination does not hold only if there exists a monomial $u \in U$ with infinite chain of its irreducible non-multiplicative prolongations

$$u \to u \cdot x_{i_1} \to \ldots \to u \cdot (x_{i_1}^{d_1} \cdots x_{i_k}^{d_k}) \to \ldots, \tag{6}$$

generated by the **while**-loop. All these prolongations are sequentially included in the set U. Suppose that we have such a case. Note, first of all, that, by property (vi) in Definition 3.1, an enlargement of the set U never leads to transition of a non-multiplicative variable of u into multiplicative.

On the other hand, by Theorem 4.12, since set U is finitely generated, there is a procedure of completion of U by non-multiplicative prolongations of its elements resulting in construction of a finite involutive closure $\tilde{U}$ of U. Let us fix such a finite set $\tilde{U}$ corresponding to the input set U. Any element $u \cdot t$ of chain (6) has an involutive divisor in $\tilde{U}$ of the form $v \cdot w$ where $v \in U$, and w contains non-multiplicative variables for v. Moving further along the chain, we eventually reach a prolongation $u \cdot t$ which

does not belong to the set $\tilde{U}$. Let $u \cdot t$ be the first such prolongation among all those generating infinite chains of the form (6). The resulting equality $u \cdot t = (v \cdot w) \times (ut/vw)$ shows that $v \cdot w \prec u \cdot t$. But then, by the selection strategy used in the algorithm, the prolongation $v \cdot w$ had to be treated before $u \cdot t$ was considered. Furthermore, since the current set V constructed by means of prolongations considered before $u \cdot t$ is a subset of $\tilde{U}$, the monomial vw, being an involutive divisor of ut with respect to the division L specified by $\tilde{U}$, is also a divisor for L specified by V. Any non-multiplicative prolongation chain (6) is thereby cut off what contradicts our assumption.

Example 4.14 (Continuation of Example 3.11). The minimal involutive bases of the set $U = (xy, y^2, z)$ $(x \succ y \succ z)$ for Thomas, Janet and Pommaret divisions are

$$\begin{aligned} \tilde{U}_T &= \{xy, y^2, z, xz, yz, xy^2, xyz, y^2z, xy^2z\}, \\ \tilde{U}_J &= \{xy, y^2, z, xz, yz\}, \\ \tilde{U}_P &= \{xy, y^2, z, xz, yz, x^2y, x^2z, \ldots, x^ky, \ldots, x^mz, \ldots\}, \end{aligned}$$

where $k, m \in \mathbb{N}$. These bases can be easily derived from U using algorithm **InvolutiveClosure**. Note that $\tilde{U}_J \subset \tilde{U}_T$ and $\tilde{U}_J \subset \tilde{U}_P$ in agreement with Propositions 3.7 and 3.10. This example explicitly shows that Pommaret division is not noetherian. However, for another ordering $z \succ y \succ x$ the set U is finitely generated, and then $\tilde{U}_P = U$.

5 Polynomial Reduction

In this section we generalize the results obtained by Zharkov and Blinkov (1993, 1994) for Pommaret division to arbitrary involutive division as it introduced in Definition 3.1 or 3.2.

Definition 5.1 Given a finite polynomial set $F \subset \mathbb{R}$ and an admissible ordering $\succ$, the concept of multiplicative and non-multiplicative variables for $f \in F$ is to be defined in terms of $lm(f)$ and the leading monomial set $lm(F)$.

Therefore, as soon as we have polynomials rather than monomials, any involutive division is to be determined on the basis of some admissible ordering, even when it does not depend on the latter for the pure monomial case, as with Thomas division.

The concepts of involutive polynomial reduction and involutive normal form are introduced similar to their conventional analogues (Buchberger, 1985) with the use of involutive division instead of the conventional one.

Definition 5.2 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 $u = lm(f) \times v$, $v \in L(lm(f), lm(F))$. It yields the *$L-$reduction* $p \rightarrow g = p - (a/lc(f))\, f \times v$.

(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 an $L-$ normal form of p modulo F by $NF_L(p, F)$. In contrast, a conventional normal form will be denoted by $NF(p, F)$. As an involutive normal form algorithm one can use, for example, the following:

Algorithm **InvolutiveNormalForm:**

Input: p, F
Output: $h = NF_L(p, F)$
begin
  $h := p$
  while exist $f \in F$ and a term u of h such that
    $lm(f)|_L(u/cf(h, u))$ **do**
    choose the first such f
    $h := h - (u/lt(f))f$
  end
  if $h \neq 0$ **and** $lc(h) \neq 1$ **then** $h := h/lc(h)$
end

Correctness and *termination* of this algorithm can be proved, apparently, as they do for the conventional normal form algorithm (Buchberger, 1985; Becker, Weispfenning and Kredel, 1993). Since involutive reductions form a fixed subset of the conventional ones, generally, $NF_L(p, F) \neq NF(p, F)$.

Definition 5.3 A set F is called *involutively autoreduced* with respect to the given involutive division L, or *$L-$autoreduced*, if the set $lm(F)$ is $L-$autoreduced and every $f \in F$ has no terms $t = cf(f, t)\, u \neq lt(f)$ with $cf(f, t) \neq 0$ and $u \in C_L(lm(F))$.

Given an involutive division L and a finite set F, the following algorithm returns an $L-$autoreduced set H, denoted by $H = Autoreduce_L(F)$, and such that $Id(F) = Id(H)$.

Correctness of the algorithm is obvious from the **while**-loop structure. Since the underlying set of involutive interreductions is a subset of the conventional interreductions, its *termination* follows from that for the conventional autoreduction (Buchberger, 1985; Becker, Weispfenning and Kredel, 1993).

Algorithm **InvolutiveAutoreduction:**

Input: F
Output: $H = Autoreduce_L(F)$
begin
  $H := F$
  while exist $h \in H$ and $g \in H \setminus \{h\}$
    such that h is reducible modulo g **do**
    choose the first such h
    $H' := H \setminus \{h\}$
    $h' := NF_L(h, H)$
    if $h' = 0$ **then** $H := H'$
    else $H := H' \cup \{h'\}$
  end
end

Theorem 5.4 *If set F is $L-$autoreduced, then $NF_L(p, F) = 0$ if and only if p is presented in terms of a finite sum of the form*

$$p \in \mathbb{S}_F \subset \mathbb{R}, \quad \mathbb{S}_F = \{ \sum_{ij} f_i \times u_{ij} \mid f_i \in F, u_{ij} \in \mathbb{T} \} \tag{7}$$

with $lm(u_{ij}) \neq lm(u_{ik})$ for $j \neq k$.

Proof $\Longrightarrow$: If $NF_L(p, F) = 0$, then, by Definition 5.2 of involutive reductions, at each intermediate reduction step the current value p' of p is rewritten as $p' \rightarrow p'' = p' - f_i \times u_{ij}$. Since the reduction chain is finite by admissibility of an ordering $\succ$, the representation (7) holds.

$\Longleftarrow$: Let p is given by expression (7). Firstly, we show that $lm(p)$ has an involutive divisor in the set $lm(F)$. For this purpose select the leading term in the right hand side of (7). It has the form $s = lt(f_i \times u_{ij}) = lt(f_i) \times u_{ij}$ with some i, j and cannot appear in any other term $lt(f_k) \times u_{kl}$. Otherwise, the underlying monomial $s/lc(s)$ would have two involutive divisors $lm(f_i)$ and $lm(f_k)$ what by Proposition 3.9 would contradict the involutive autoreduction of F. Secondly, since p is involutively reducible, after each reduction step the representation (7), obviously, still holds providing the further reductions until the chain stops when we obtain zero at a certain step. It just means that $NF_L(p, F) = 0$. □

Corollary 5.5 *If set F is $L-$autoreduced, then the $L-$normal form, for an arbitrary algorithm of its computation and for any polynomials p_1, p_2 and p, has the properties:*

(i). *Uniqueness: if $h_1 = NF_L(p, F)$ and $h_2 = NF_L(p, F)$ then $h_1 = h_2$.*

(ii). *Linearity: $NF_L(p_1 + p_2, F) = NF_L(p_1, F) + NF_L(p_2, F)$.*

Proof (i) By an involutive normal form algorithm, $h_1 = p - \sum_{ij} f_i \times u_{ij}$ and $h_2 = p - \sum_{ij} f_i \times v_{ij}$. Therefore, $h_1 - h_2$ has the representation (7), and $NF_L(h_1 - h_2, F) = 0$ by Theorem 5.4. On the other hand, since h_1 and h_2 are normal forms, they have no involutive divisors and so does $h_1 - h_2$. Hence, we have $h_1 = h_2$.

(ii) Denote $p_1 + p_2$ by p_3 and let

$$h_1 = NF_L(p_1, F), \quad h_2 = NF_L(p_2, F), \quad h_3 = NF_L(p_3, F).$$

Then $NF_L(h_3 - h_1 - h_2, F) = h_3 - h_1 - h_2$, since none of h_1, h_2, h_3 has involutive divisors in $lm(F)$. In addition, because $h_k = p_k - \sum_{ij} f_i \times v_{k;ij}$ $(k = 1, 2, 3)$, we have $h_3 - h_1 - h_2 \in \mathbb{S}_F$. Thus, by Theorem 5.4, $NF_L(h_3 - h_1 - h_2, F) = 0$, and, hence, $h_3 = h_1 + h_2$. □

6 Involutivity Conditions

Definition 6.1 Multiplication of a polynomial $f \in F$ by a variable x is called the *prolongation* of f. Given involutive division specified by the set $lm(F)$, the prolongation is called *multiplicative* if x is multiplicative for $lm(f)$ and *non-multiplicative*, otherwise.

Definition 6.2 An L–autoreduced set F is called *(L–)involutive* if

$$(\forall f \in F)\ (\forall u \in \mathbb{M})\ \ [\, NF_L(fu, F) = 0\,]. \tag{8}$$

Definition 6.3 An L–involutive set F will be called *(L–)involutive basis* of the ideal $Id(F)$ if it is *normalized*, that is, $lc(f) = 1$ holds for all $f \in F$.

Proposition 6.4 *Let F be an involutive polynomial basis. Then the monomial set $lm(F)$ is also involutive.*

Proof It follows immediately from Definitions 4.1, 6.2 and 6.3 □

It is clear from Definition 6.3 and the linearity of the involutive normal form by Corollary 5.5 that an *involutive basis* provides decision of the ideal membership problem. Hence, we have the following corollary.

Corollary 6.5 *If set F is L–involutive, then $p \in Id(F)$ if and only if $NF_L(p, F) = 0$. In this case, obviously, the equality $\mathbb{S}_F = Id(F)$ holds.*

The definition of involutive polynomial sets is the direct extension of that for involutive monomial sets in Sect.4. The theorem below imparts the constructive characterization of involutivity, which is the heart of the involutive algorithms.

Theorem 6.6 *An L–autoreduced set F is involutive with respect to a continuous involutive division L if and only if the following conditions of local involutivity hold*

$$(\forall f \in F)\ (\forall x_i \in NM(f, F))\ \ [\, NF_L(f \cdot x_i, F) = 0\,]. \tag{9}$$

Proof $\Longrightarrow$: Since $x_i \in \mathbb{M}$ we are done.

$\Longleftarrow$: An immediate consequence of (9) is local involutivity of the set $lm(F)$ in accordance with Definition 4.7. Then, by continuity of division L, this set is involutive. Thus, for any $f \in F$ and any $u \in \mathbb{M}$ the monomial $lm(f) \cdot u$ has the involutive divisor $lm(g)$, $g \in F$.

We claim that the polynomial $f \cdot u$ can be presented as follows

$$f \cdot u = g \times v + \sum_{ij} f_i v_{ij}, \tag{10}$$

where $v, v_{ij} \in \mathbb{T}$, $f_i \in F$ and relation $lm(f \cdot u) = lm(g \times v) \succ lm(f_i v_{ij})$ holds for any term of the sum. Indeed, if u is multiplicative for f we are trivially done. Otherwise u contains $x_k \in NM(f, lm(F))$. Then, the local involutivity of F, by Theorem 5.4, yields the representation

$$f \cdot x_k = g_1 \times u_1 + \sum_{ij} f_i \times u_{ij} \tag{11}$$

with $g_1 \in F$ and $lm(f \cdot x_k) = lm(f_1 u_1) \succ f_i u_{ij}$ for any term under the summation sign. If monomial u/x_k is multiplicative for g_1, then (10) immediately follows from (11) with $g = g_1$ and $v = u_1 u/x_k$. Otherwise, multiply both sides of (11) by u/x_k, take a variable $x_m \in NM(g_1, lm(F))$, which is contained in u/x_k, and apply the local involutivity conditions for $g_1 \cdot x_m$. It gives the relation

$$f \cdot u = (g_2 \times u_2) u_1 u/(x_k x_m) + \sum_{ij} f_i \tilde{u}_{ij} \tag{12}$$

where inequality $lm(g_2) u u_1 u_2/(x_k x_m) \succ lm(f_i \tilde{u}_{ij})$ holds for all i, j. If $u u_1/(x_k x_m)$ is still non-multiplicative for g_2 the relation (12) can be further rewritten by using the local involutivity conditions until we obtain relation (10). This is guaranteed by continuity of involutive division L, because all the polynomials $g_1, g_2, \ldots \in F$ are distinct, since their leading monomials, by construction, form the sequence satisfying (5).

Next, similar rewriting the every term $f_i v_{ij}$ in (10) gives $f_i v_{ij} = f_k \times w_k + \sum_{lm} f_l w_{lm}$ with $lm(f_i v_{ij}) = lm(f_k \times w_k) \succ lm(f_l w_{lm})$. Proceeding with this way, by admissibility of ordering $\prec$, we find, in a finite number of steps, that $f \cdot u \in \mathbb{S}_F$. □

The next definition of partial involutivity is useful for the algorithmic construction of involutive bases as we show below.

Definition 6.7 Given $v \in \mathbb{M}$ and an $L-$autoreduced set F, if there exist $f \in F$ such that $lm(f) \prec v$ and

$$(\forall f \in F)\ (\forall u \in \mathbb{M})\ (lm(f) \cdot u \prec v)\ \ [\ NF_L(fu, F) = 0\ ], \tag{13}$$

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 $v \prec lm(f)$ for all $f \in F$.

Looking at the proofs of Theorems 4.10 and 6.6 it is easy to see that they prove also the following *conditions of partial involutivity.*

Corollary 6.8 *Given a continuous involutive division L, an $L-$autoreduced set F is partially involutive up to the monomial v if and only if*

$$(\forall f \in F)\ (\forall x_i \in NM(f, F))\ (lm(f) \cdot x_i \prec v)\ \ [\ NF_L(f \cdot x_i, F) = 0\ ]. \tag{14}$$

7 Gröbner Bases and Involutive Bases

In Zharkov and Blinkov (1993) it was shown that a *Pommaret basis*, that is, involutive basis for Pommaret division, is also a Gröbner basis, though, generally, not the reduced one. A similar property of a Janet basis was noticed in Zharkov (1994*b*). The following theorem shows that such a relation holds for any involutive division.

Theorem 7.1 *If set F is $L-$involutive, then the equality of the conventional and $L-$normal forms*

$$(\forall p \in \mathbb{R})\ \ [\ NF(p, F) = NF_L(p, F)\ ] \tag{15}$$

holds for any normal form algorithm.

Proof To prove the theorem it is sufficient to show that any polynomial p is reducible modulo F if and only if it is involutively reducible. But the latter statement is an easy consequence of Definitions 3.1 or 3.2 and 6.2. Indeed, if p is involutively reducible, then it is conventionally reducible. Conversely, let the term u have a divisor among the leading monomials of F, that is, $u = lc(u)\, lm(f) \cdot v$ for some $f \in F$ and $v \in \mathbb{M}$. By the condition (8) and Theorem 5.4, it implies $f \cdot v = \sum_{ij} f_i \times u_{ij}$. Hence, u has also the involutive divisor in $lm(F)$. It is just that f_i which satisfies the condition $lm(f_i) \times u_{ij} = lm(f) \cdot v$ and is unique. □

Corollary 7.2 *An involutive basis is a Gröbner basis.*

Proof According to the algorithmic characterization of Gröbner bases (Buchberger, 1965 and 1985; Becker, Weispfenning and Kredel, 1993) consider the S-polynomial of $f_i, f_j \in F$

$$S(f_i, f_j) = \frac{lcm(f_i, f_j)}{lt(f_i)} f_i - \frac{lcm(f_i, f_j)}{lt(f_j)} f_j\,. \tag{16}$$

Since $S(f_i, f_j) \in Id(F)$, by Corollary 6.5 and Theorem 7.1, we have $NF(S(f_i, f_j), F) = 0$. □

Corollary 7.3 *If set F is partially involutive up to the monomial v, then*

$$(\forall p \in \mathbb{R})\ (lm(p) \prec v)\ \ [\ NF(p, F) = NF_L(p, F)\ ]. \tag{17}$$

Proof It follows by perfect analogy to the proof of Theorem 7.1. □

Note that while a Pommaret basis, if it exists for the given ideal, is unique (Zharkov and Blinkov, 1994), this may not hold for other involutive divisions. We demonstrate it by the following explicit example.

Example 7.4 Two lexicographical ($x \succ y$) Janet bases F_1 and F_2

$$F_1 = \{xy^3 - y, \overbrace{xy^2 - 1, xy - y^2, x - y}^{y}, \overbrace{y^3 - 1}^{x}\},$$

$$F_2 = \{x^2y^3 - y^2, \overbrace{x^2y^2 - y, x^2y - 1, x^2 - y^2}^{y}, \overbrace{xy^3 - y}^{x}, \overbrace{xy^2 - 1, xy - y^2, x - y}^{x,y}, \overbrace{y^3 - 1}^{x}\},$$

with indicated non-multiplicative variables, are involutive. It can easily be verified. Both of them generate, obviously, the same ideal with the Gröbner basis $(x - y, y^3 - 1)$, which is also a Janet basis and, in this particular case, coincides with the Pommaret basis.

As was shown in Sect.4, given a polynomial set F and an arbitrary involutive division, the ideal $Id(F)$ may not have a finite involutive basis. For example, while a finite Pommaret basis exists for any zero-dimensional ideal (Pommaret, 1978; Zharkov and Blinkov, 1994 and Apel, 1995), it may not exist for a positive dimensional one. Generally, for positive dimensional ideals, the existence of finite Pommaret basis can be achieved by means of an appropriate linear transformation of variables (Pommaret, 1978 and Apel, 1995).

On the other hand, a noetherian involutive division, for example a Thomas or Janet one, implies the existence of finite involutive bases for any polynomial ideals as the following proposition shows.

Proposition 7.5 *If involutive division L is noetherian, then any polynomial ideal $Id(F)$ has a finite $L-$involutive basis.*

Proof Let G be the reduced monic Gröbner basis of $Id(F)$ which is finite for any polynomial ideal (Buchberger, 1985; Becker, Weispfenning and Kredel, 1993). If set G is not involutive, then complete it by non-multiplicative prolongations of its elements just as it done in algorithm **InvolutiveClosure**. This means that at every step of the completion we select a non-multiplicative prolongation with the lowest leading term which is $L-$irreducible modulo the current leading monomial set. By noetherity of L, in a finite number of steps, a polynomial set $\tilde{G}$ will be produced such that $lm(\tilde{G})$ be an $L-$autoreduced involutive closure of $lm(G)$. Finally, $L-$autoreduction of the tales in $\tilde{G}$ will give an L-involutive basis of $Id(F)$. □

8 Basic Algorithm

In this section we describe an algorithm for the construction of an involutive basis. The algorithm is an improved version of one presented in Zharkov and Blinkov (1994) for Pommaret division and generalized to any continuous involutive division L and any admissible ordering $\succ$. The main optimization is based on the use of Buchberger's chain criterion for avoiding unnecessary reductions introduced in Buchberger (1979) (see also Buchberger, 1985; Becker, Weispfenning and Kredel, 1993) which excludes also the repeated prolongations (Zharkov, 1994a) as we show below.

Corollary 7.3 shows that for any S-polynomial $S(f_i, f_j)$, given by formula (16), both its conventional and $L-$normal forms are vanishing as soon as the conditions (14) are satisfied up to the monomial $lcm(f_i, f_j)$. According to Theorem 5.4 and Corollary 5.5 the conditions (14) can be presented as $NF_L(S_L(f_i, f_j), F) = 0$, where $S_L(f_i, f_j)$ are just ($L-$involutive) S-polynomials of the special form

$$S_L(f_i, f_j) = f_i \cdot x - f_j \times u_{jk}\,. \tag{18}$$

The following theorem gives the involutive form of Buchberger's chain criterion.

Theorem 8.1 *Let F be a finite $L-$autoreduced polynomial 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*

$$(\forall h \in F)\ (\forall u \in \mathbb{M})\ (\ lm(h) \cdot u \prec lm(g \cdot x)\ )\ \ [\ NF_L(h \cdot u, F) = 0\ ]\,, \tag{19}$$

$$(\exists f, f_0, g_0 \in F) \left[\begin{array}{l} lm(f_0) | lm(f)\,,\ lm(g_0) | lm(g) \\ lm(f) |_L lm(g \cdot x)\,,\ lcm(f_0, g_0) \prec lm(g \cdot x) \\ NF_L(f_0 \cdot \frac{lt(f)}{lt(f_0)}, F) = NF_L(g_0 \cdot \frac{lt(g)}{lt(g_0)}, F) = 0 \end{array} \right]. \tag{20}$$

Proof Condition (20) yields that at least one of polynomials f, g can be considered as derived from f_0, g_0 by prolongations with at least one non-multiplicative among them. If, for example, $lm(f_0) \neq lm(f)$, it leads to the equality $f = lm(f_0) \cdot (lm(f)/lm(f_0))$ modulo F.

Thus, if the condition (20) holds, there is a chain of polynomials in F of the form

$$f \equiv f_k, f_{k-1}, \ldots, f_0, g_0, \ldots, g_{m-1}, g_m \equiv g\,, \tag{21}$$

where $k+m > 0$. Here f or g or both of them are produced by prolongations, including non-multiplicative ones, of the polynomials f_i or g_j in the chain whose indices are less than k or m, respectively.

The chain (21) has the property

$$NF(S_L(f, f_{k-1}), F) = \cdots = NF(S(f_0, g_0), F) = \cdots = NF(S_L(g_{m-1}, g), F) = 0\,.$$

This property is resulted from the observations as follow. Consider relation

$$lm(g) \cdot x = lm(f) \times w, \tag{22}$$

which means that w does not contain x. Otherwise, g would be reducible by f, and, hence, F could not be $L-$autoreduced. Thus, $lcm(f, g) = lm(g) \cdot x$. By admissibility of the monomial ordering $\prec$, the least common multiple of the leading monomials for pair of the neighboring polynomials in the chain (21) is less than or equal to $g \cdot x$. Then the above property of the chain follows immediately from partial involutivity (19) of F and Corollary 7.3. Furthermore, conditions (19-20) imply $NF_L(S(f_0, g_0), F) = NF(S(f_0, g_0), F) = 0$, and $NF_L(S_L(f_i, f_{i-1}), F) = NF(S(f_i, f_{i-1}), F) = 0$ as well as $NF_L(S_L(g_{i-1}, g_i), F) = NF(S(g_{i-1}, g_i), F) = 0$.

By construction, $lcm(f, \ldots, f_1, f_0, g_0, g_1, \ldots, g) = lcm(f, g)$ what leads (Becker, Weispfenning and Kredel, 1993) to the representation $S(f, g) = \sum_{ij} f_i u_{ij}$ where $f_i \in F$ and $lm(f_i u_{ij}) \prec lcm(f, g) = lm(g) \cdot x$. Then, condition 19, taking into account Corollaries 5.5 and 7.3, yields $NF_L(S_L(f, g), F) = NF(S(f, g), F) = 0$ in accordance with Buchberger (1979,1985). □

Algorithm **InvolutiveBasis:**

Input: F, a finite polynomial set
Output: G, an involutive basis of the ideal $Id(F)$
begin
  $G := Autoreduce(F)$
  $T := \emptyset$
  for each $g \in G$ **do** $T := T \cup \{(g, lm(g), \emptyset)\}$
  while exist $(g, u, P) \in T$ such that $NM(g, G) \setminus P \neq \emptyset$ **do**
    choose $(g, u, P) \in T$ and $x \in NM(g, G) \setminus P$ with the lowest $lm(g) \cdot x$
    $T := T \setminus \{(g, u, P)\} \cup \{(g, u, P \cup \{x\})\}$
    if exist $f \in (f, v, D) \in T$ such that $lm(f) |_L lm(g \cdot x)$ **then**
      if $lcm(u, v) = lm(g) \cdot x$ **then** $h := NF_L(g \cdot x, G)$
        if $h \neq 0$ **then** $T := T \cup \{(h, lm(h), \emptyset)\}$
    else $h := NF_L(g \cdot x, G)$
    $T := T \cup \{(h, u, \emptyset)\}$
    $G := Autoreduce_L(G \cup \{h\})$
    $Q := T$
    $T := \emptyset$
    for each $g \in G$ **do**
      if exist $(f, u, P) \in Q$ such that $lm(f) = lm(g)$ **then**
        choose $g_1 \in G$ such that $lm(g_1) |_L u$
        $T := T \cup \{(g, lm(g_1), P)\}$
      else $T := T \cup \{(g, lm(g), \emptyset)\}$
  end
end

Before analysis of correctness and termination of this algorithm, we give some necessary clarifications.

First of all, the conventional autoreduction of the initial polynomial set is done. It removes, in particular, all the predecessors of every polynomial from the initial set.

Set T collects all the triples (g, u, P); g is an element in the current basis G; $u = lm(f)$ where $f \in G$ is the predecessor of g, by a non-multiplicative prolongation of which g was derived, or $u = lm(g)$ if g has no such predecessor in G; P is a set containing the non-multiplicative variables of g have been used for its prolongations.

The current non-multiplicative prolongation $g \cdot x$ is selected to be the lowest with respect to the ordering $\succ$. If there are several different non-multiplicative prolongations with the same leading term, then any of them may be selected. This selection strategy will be called *normal*.

If the leading monomial of the current prolongation $g \cdot x$ is involutively reducible by the basis element $f \in G$, then the other conditions in (20) are verified. The verification is done in the form of comparison of $lcm(u, v)$ with $lcm(f, g)$, where u and v are the second elements of the triples containing g and f, respectively. By Theorem 8.1, the criterion (20) is false if and only if $lcm(u, v) = lcm(f, g) = g \cdot x$. One should be also noted that Buchberger's second criterion (Buchberger, 1985) can be applied in the involutive approach only in exceptional cases. Relation (22) shows that $lcm(f, g) = lm(f)lm(g)$ if and only if $lm(f) = x$ and $lm(g) = w$.

If the current prolongation is not reducible to zero, that is, $h = NF_L(g \cdot x, G) \neq 0$, then h is added to G.

After involutive autoreduction of the enlarged set G an adjustment of the set T is done. For an element $g \in G$ whose leading monomials was not mutually reduced, the second element u in the triple is kept, if the leading term of the corresponding predecessor of g was also not reduced. Otherwise, u is replaced by its involutive divisor in $lm(G)$. Essentially new leading monomials, that is, those not multiple of any others occurring in T before the autoreduction, are included in the refreshed T with their actual leading monomials as the second elements of the triples.

To provide the output polynomials being monic, in accordance with Definition 6.3, their normalization is assumed to be done at the step of computing involutive normal form.

Correctness. As we have shown, criterion (20) is used in algorithm **InvolutiveBasis** in accordance with Theorem 8.1. It is easy to show that there is the unique polynomial $g_1 \in G$ which is chosen in the inner **for each**-loop such that $lm(g_1)$ involutively divides u. Indeed, if the leading term of the predecessor h of g with $u = lm(h)$ has not been reduced, then $g_1 = h$. Otherwise, there is $g_1 \in G$ such that $g_1 \neq h$ and $lm(g_1)|_L u$. Its uniqueness of g_1 for the autoreduced set G is an immediate consequence of the property (v) in Definition 3.1. Besides, the replacement of u by g_1 does not violate, obviously, the conditions for applicability of the criterion. Furthermore, from Corollary 7.3 it follows that a leading monomial, being involutively reducible at some step of the algorithm, will never appear again among the leading monomials. This enables one to assign the set P of the used non-multiplicative variables for polynomial f to the corresponding polynomial g with $lm(g) = lm(f)$ as it is done in the inner **for each**-loop. Such an optimization allows one to avoid the repeated prolongations.

Therefore, if the algorithm terminates it produces, by Theorem 6.6, the involutive basis. The termination holds if and only if the set P in each triple $(g, u, P) \in T$ contains all non-multiplicative variables for basis element g. It just means that any non-multiplicative prolongation of every element in G is reduced to zero, and, hence, G is involutive.

Termination. Note that the initial value of the leading monomial set

$$U_0 = lm(Autoreduce(F))$$

is determined by the input set F subjected to the conventional autoreduction. Since only those monomials occur in the leading monomial set which have not been reducible at some step of the algorithm, the change in set $U = lm(G)$ after running the **while**-loop may take place only in two cases:

(i). $lm(g) \cdot x$ has no involutive divisors in U. In this case U is enlarged to include $lm(g) \cdot x$.

(ii). $g \cdot x$ is reducible by elements of U. Then U is enlarged to include $lm(h)$, where $h = NF_L(g \cdot x, G) \neq 0$ and $lm(h)$ is not multiple, in the conventional sense, of any elements in U_0.

The number of different $lm(h)$ occurring in case (ii) is finite by Dickson's lemma (Becker, Weispfenning and Kredel, 1993). Recall also that algorithms **InvolutiveAutoreduction** and **InvolutiveNormalForm** always terminate (Sect.5). Thus, the algorithm termination is determined by that of algorithm **InvolutiveClosure** considered in Sect.4. It follows that algorithm **InvolutiveBasis** terminates for any noetherian division and arbitrary input polynomial set F. If division L is not noetherian, then termination may not hold if an intermediate set $U = lm(G)$ is not finitely generated with respect to L as the below Example 8.2 shows. In the case of Pommaret division the algorithm terminates, however, for any degree compatible ordering and any zero-dimensional ideal (Zharkov and Blinkov, 1994).

Thus, because the involutive division L is continuous, once algorithm **InvolutiveClosure** terminates, an involutively closed set $\tilde{U}$ will be constructed such that autoreduction of the corresponding set G does not produce new leading monomials. G is, obviously, the output involutive basis.

By Proposition 4.5, it implies, in particular, the algorithm termination for Thomas and Janet divisions. However, for Pommaret division, which is not noetherian, the algorithm may not terminate even in the case when there is a finite Pommaret basis but the ordering is not degree compatible as the following simple example shows.

Example 8.2 The set $F = \{x^2 - 1, xy - 1, z\}$ generates a zero-dimensional ideal with the lexicographical Pommaret basis $(x \succ y \succ z)$ given by $G = \{x - y, y^2 - 1, yz, z\}$. However, following the above algorithm we have to choose $z \cdot y$ as the first prolongation which is lexicographically lowest. Since polynomial $h = yz$ has no Pommaret divisors among $lm(F)$, we find $F \cup \{yz\}$ as an intermediate basis. The next lowest prolongation is $yz \cdot y$ again has no Pommaret divisors among the leading monomials of the enlarged set. Exploring this procedure further produces the infinite involutively irreducible set

$$\{x^2 - 1, xy - 1, z, yz, y^2z, \ldots, y^kz, \ldots\} \quad k \in \mathbb{N}.$$

It is well-known (Pommaret, 1978; Zharkov and Blinkov, 1993 and 1994; Apel, 1995) that positive dimensional ideals may not have finite Pommaret bases. Example 4.14 illustrates this fact at the monomial level. The following more non-trivial example shows the output of algorithm **InvolutiveBasis** for Pommaret and Janet divisions in the case of polynomial ideal.

Example 8.3 Cyclic 4-th roots.

NM_J	NM_P	Initial Polynomial Set
x_2	–	$x_1 + x_2 + x_3 + x_4$
x_3	x_1	$x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$
x_4	x_1, x_2	$x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2$
–	x_1, x_2, x_3	$x_1x_2x_3x_4 - 1$

Here we choose the degree-reverse-lexicographical-ordering with the order of variables as in Sect.2 and show non-multiplicative variables for each polynomial. Note that, since the initial set is not autoreduced, the inclusion $NM_J \subseteq NM_P$ (see Proposition 3.10) does not hold.

Application of algorithm **InvolutiveBasis** gives the following form of Janet and Pommaret bases

NM_J	NM_P	Janet and Pommaret Bases
–	–	$x_1 + x_2 + x_3 + x_4$
x_1	x_1	$x_2^2 + 2x_2x_4 + x_4^2$
x_1, x_2	x_1, x_2	$x_2x_3^2 + x_3^2x_4 - x_2x_4^2 - x_4^3$
x_1, x_2, x_3	x_1, x_2, x_3	$x_2x_3x_4^2 + x_3^2x_4^2 - x_2x_3^3 + x_3x_4^3 - x_4^4 - 1$
x_1, x_2, x_3	x_1, x_2, x_3	$x_2x_4^4 + x_4^5 - x_2 - x_4$
x_1, x_2, x_3	x_1, x_2, x_3	$x_3^2x_4^4 + x_2x_3 - x_2x_4 + x_3x_4 - 2x_4^2$
x_1, x_2	x_1, x_2, x_3	$x_3^3x_4^2 + x_3^2x_4^3 - x_3 - x_4$
	x_1, x_2, x_3	$x_3^4x_4^2 + x_2x_3 - x_3^2 - x_2x_4 + x_3x_4 - x_4^2$
		.....

The Janet basis consists of the upper seven polynomials and coincides with the Gröbner basis, while the Pommaret basis is infinite and contains also prolongations of the seventh polynomial with respect to its non-multiplicative variable x_3. Note that the ideal is one-dimensional, which is why it does not have a finite Pommaret basis.

The algorithm **InvolutiveBasis** has been implemented in Reduce 3.5 for the degree-reverse-lexicographical-ordering and Pommaret division refined in a certain way to provide the algorithm termination for any polynomial ideal. This refinement is equivalent to the dynamical incorporation of some noetherian involutive division in the computational process. Its detailed description will be given elsewhere. In addition, the current package called INVBASE is considerably faster than previous version (Zharkov and Blinkov, 1994), in particular, since it uses the criterion (20).

Experimentally, we observed much smoother behavior of the algorithm **Involutive Basis** with respect to Buchberger algorithm[1] as the ordering changes. Consider, for instance, the following example.

Example 8.4 Cyclic 6-th roots.

$x_1 + x_2 + x_3 + x_4 + x_5 + x_6$,
$x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_1$,
$x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_6 + x_5x_6x_1 + x_6x_1x_2$,
$x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_6 + x_4x_5x_6x_1 + x_5x_6x_1x_2 + x_6x_1x_2x_3$,
$x_1x_2x_3x_4x_5 + x_2x_3x_4x_5x_6 + x_3x_4x_5x_6x_1 + x_4x_5x_6x_1x_2 + x_5x_6x_1x_2x_3 + x_6x_1x_2x_3x_4$,
$x_1x_2x_3x_4x_5x_6 - 1$.

The next table gives the timings of INVBASE on an 66 Mhz MS-DOS based AT/486 computer for different degree-reverse-lexicographical-orderings.

Ordering	Timing (sec.)
$x_1 \succ x_2 \succ x_3 \succ x_4 \succ x_5 \succ x_6$	1040
$x_1 \succ x_2 \succ x_4 \succ x_6 \succ x_3 \succ x_5$	514
$x_1 \succ x_2 \succ x_4 \succ x_6 \succ x_5 \succ x_3$	437
$x_1 \succ x_2 \succ x_6 \succ x_3 \succ x_4 \succ x_5$	1066
$x_1 \succ x_3 \succ x_4 \succ x_5 \succ x_2 \succ x_6$	604
$x_1 \succ x_3 \succ x_4 \succ x_6 \succ x_5 \succ x_2$	136
$x_1 \succ x_4 \succ x_2 \succ x_3 \succ x_5 \succ x_6$	993
$x_1 \succ x_4 \succ x_5 \succ x_6 \succ x_2 \succ x_3$	1001
$x_1 \succ x_5 \succ x_3 \succ x_4 \succ x_6 \succ x_2$	364
$x_1 \succ x_5 \succ x_6 \succ x_2 \succ x_3 \succ x_4$	1045
$x_1 \succ x_6 \succ x_3 \succ x_2 \succ x_4 \succ x_5$	1012
$x_1 \succ x_6 \succ x_5 \succ x_2 \succ x_4 \succ x_3$	590

Comparison with the package GROEBNER implementing Buchberger algorithm on the same Reduce 3.5 platform shows that its corresponding timings are not only much

[1]More precisely, with respect to its implementation in Reduce 3.5.

larger than those presented in the table, but also vary dramatically with the order of the variables. This fact was already observed by Zharkov and Blinkov (1994) where some comparative data for GROEBNER and the previous version of the INVBASE package are presented.

9 Conclusion

Buchberger algorithm and the involutive one are based on different rewriting techniques, namely, on the use of S-polynomials and prolongations, respectively, as well as on distinct reduction processes. Nevertheless, as we demonstrate in this paper, they are in fact very interconnected. If, as we propose in the algorithm **InvolutiveBasis**, we choose the current prolongation in increasing order with respect to given monomial ordering, then the conventional and involutive normal form will coincide. What is more, the involutive reduction of the prolongation is equivalent to the consideration of a certain S-polynomial. Just this fact makes it possible to use Buchberger's criteria.

Very recently another interesting facet of interrelation of both methods was discovered by Apel (1995), namely, that Pommaret bases can be associated with Gröbner ones in appropriate graded structures. Earlier such Gröbner bases were intensively investigated in more general context in Mora (1988). That observation gives us an opportunity to algorithmically construct Pommaret bases whenever they exist (Apel, 1995). Though such an analogy also enables one to take advantage of Buchberger's criteria, it is restricted to Pommaret division.

Thus, all the above, as well as computer experiments with both techniques, offers a clearer view of the most optimal computational procedures.

There is no question that any algorithmic improvement of the Gröbner basis and involutive techniques at the algebraic level has an analogous optimization at the differential level, at least for linear partial differential equations (Gerdt, 1995).

10 Acknowledgements

The initial version of this paper was written on the eve of the first anniversary of death of our mutual friend and coauthor Alyosha Zharkov who made invaluable contribution to the formation of the involutive approach to commutative algebra. We devote the present work to his memory. The authors are grateful to J.Apel for numerous fruitful discussions. This work was supported in part by the RFBR grant No. 96-01-01860.

References

[1] Apel, J. (1995). A Gröbner Approach to Involutive Bases. *J. Symb. Comp.* **19**, 441-457.

[2] Becker, T., Weispfenning, V., Kredel, H. (1993). *Gröbner Bases. A Computational Approach to Commutative Algebra.* Graduate Texts in Mathematics **141**, Springer-Verlag, New York.

[3] Buchberger, B. (1965). 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.

[4] Buchberger, B. (1979). A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases. *Proc. EUROSAM 79, International Symposium on Symbolic and Algebraic Manipulation*, Ng, E.W. (ed.), Springer-Verlag, Berlin, pp.3-21.

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

[6] Carra'Ferro, G. (1987). Gröbner Bases and Differential Algebra. *Lec. Not. in Comp. Sci.* **356**, 129-140.

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

[8] Janet, M. (1920). Sur les Systèmes d'Equations aux Dérivées Partielles. *J. Math. Pure et Appl.* **3**, 65-151.

[9] Kandri-Rody, A., Weispfenning, V. (1990). Non-commutative Gröbner bases in Algebras of Solvable Type. *J. Symb. Comp.* **9**, 1-26.

[10] Mora, T. (1988). Seven Variations on Standard Bases. Preprint No.45, Dip. di Mathematica, Univ. di Genova.

[11] Ollivier, F. (1990). Standard Bases of Differential Ideals, *Lec. Not. in Comp. Sci.* **508**, 304-321.

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

[13] Riquier C. (1910). *Les Systèmes d'Equations aux Dérivées Partielles.* Gauthier-Villars, Paris.

[14] Thomas, J. (1937). *Differential Systems.* American Mathematical Society, New York.

[15] Zharkov, A.Yu., Blinkov, Yu.A. (1993). Involutive Approach to Solving Systems of Algebraic Equations. In: *Proceedings of "SC 93", International IMACS Symposium on Symbolic Computation: New Trends and Developments*, Jacob, G., Oussous, N.E., Steiberg S. (eds.), Laboratoire d'Informatique Fondamentale de Lille, Lille, pp.11-16.

[16] Zharkov, A.Yu., Blinkov, Yu.A. (1994). Involutive Bases of Zero-Dimensional Ideals. Preprint No. E5-94-318, Joint Institute for Nuclear Research, Dubna.

[17] Zharkov, A.Yu. (1994*a*). Solving Zero-Dimensional Involutive Systems. In: *Algorithms in Algebraic Geometry and Applications*, Gonzales-Vega, L., Recio, T. (eds.). Progress in Mathematics, Vol. 143, Birkhäuser, Basel, pp.389-399.

[18] Zharkov A.Yu. (1994*b*). Private communication.

Received by Publishing Department
on January 14, 1997.