On the Relation between Pommaret and Janet Bases*

Vladimir P.Gerdt

Laboratory of Computing Techniques and Automation, Joint Institute for Nuclear Research, 141980 Dubna, Russia

Abstract. In this paper the relation between Pommaret and Janet bases of polynomial ideals is studied. It is proved that if an ideal has a finite Pommaret basis then the latter is a minimal Janet basis. An improved version of the related algorithm for computation of Janet bases, initially designed by Zharkov, is described. For an ideal with a finite Pommaret basis, the algorithm computes this basis. Otherwise, the algorithm computes a Janet basis which need not be minimal. The obtained results are generalized to linear differential ideals.

1 Introduction

Pommaret and Janet bases may be cited as typical representatives of involutive bases [1–4]. Involutive bases are Gröbner bases, though, generally redundant, and involutive methods provide an alternative approach to computation of Gröbner bases. In so doing, polynomial Pommaret bases which were first introduced in [5] have become a research subject in commutative algebra. They can be considered as generalized left Gröbner bases in the commutative ring with respect to non-commutative grading [6]. Pommaret bases of homogeneous ideals in generic position coincide with their reduced Gröbner bases [7]. The use of these bases makes more accessible the structural information of zero-dimensional ideals [8]. Pommaret bases provide an algorithmic tool for determining combinatorial decompositions of polynomial modules and for computations in the syzygy modules [9].

Linear differential Pommaret bases form the main tool in formal theory of linear partial differential equations [10, 11] whereas linear differential Janet bases form an algorithmic tool in Lie symmetry analysis of nonlinear differential equations [12, 13]. Unlike reduced Gröbner bases, Pommaret and Janet bases along with any other involutive bases lead to explicit formulae for Hilbert functions and Hilbert polynomials [3, 4, 11, 14].

Basic properties of Pommaret and Janet bases are determined by the underlying involutive divisions [1–3]. Non-noetherity of Pommaret division [1] is responsible for non-existence of finite Pommaret bases for some polynomial (linear differential) ideals of positive (differential) dimension. On the other hand, any polynomial ideal as well as any linear differential ideal has a finite Janet

* Dedicated to the memory of Alyosha Zharkov.

basis due to the noetherity of Janet division. The two divisions differ greatly by their definition: unlike Janet divisibility, Pommaret divisibility do not depend on the leading terms of generators. Given an ideal and an admissible monomial ordering, or ranking in the differential case, its monic Pommaret basis is unique whereas there are infinitely many different monic Janet bases and among them only the minimal Janet basis is uniquely defined [2].

However, in spite of the above differences, Pommaret and Janet bases are closely related, and Zharkov was the first to observe this fact in the last paper [15] of his life. He argued that if a polynomial ideal has a finite Pommaret basis and a Janet basis which is Pommaret autoreduced, then they have identical monic forms (c.f. [9]). Zharkov put also forward an algorithm for construction of Janet bases by sequential treatment of Janet nonmultiplicative prolongations followed by Pommaret autoreduction.

The goal of this paper is to study the relation between polynomial Pommaret and Janet bases in more details and to improve the Zharkov algorithm. Our analysis is based on the properties of Janet and Pommaret divisions and involutive algorithms studied in [1, 2, 4, 16].

This paper is organized as follows. The next section sketches some definitions, notations and conventions which are used in the sequel. Section 3 deals with analysis of the relationships between polynomial Pommaret and Janet bases. In particular, we prove that if an ideal has a finite Pommaret basis, then it is a minimal Janet basis. We describe here an algorithm of the combined Pommaret and Janet autoreduction which, given a Janet basis, converts it into another Janet basis. Since a minimal Janet basis is both Janet and Pommaret autoreduced, the existence of a finite Pommaret basis is equivalent to Pommaret-Janet autoreducibility of any non-minimal Janet basis into a minimal one. In Section 4 we describe an algorithm for computation of polynomial Janet bases which is an improved version of the Zharkov algorithm [15]. One of the improvements is the use of Pommaret-Janet autoreduction rather than the pure Pommaret autoreduction. Another improvement is incorporation of the involutive analogue [1] of Buchberger's chain criterion [17]. Section 5 contains generalization of the results of Sections 3 and 4 to linear differential ideals. The generalization is based on paper [4] where general involutive methods and algorithms of papers [1, 2, 16] are extended from commutative to differential algebra.

2 Basic Definitions and Notations

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. If monomial u divides monomial v we shall write $u|v$. Throughout the paper we restrict ourselves to admissible monomial orderings [18] $\succ$ which are compatible with

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

The leading monomial of the polynomial $f \in \mathbb{R}$ with respect to $\succ$ will be denoted by $lm(f)$. 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 initial ideal of an ideal $I \in \mathbb{R}$ with respect to the monomial ordering $\succ$ will be denoted by $in_{\succ}(I)$. The support of a polynomial f, that is, the set of monomials occurring in f with nonzero coefficients will be denoted by $supp(f)$. For the least common multiple of two monomials $u, v \in \mathbb{M}$ we shall use the conventional notation $lcm(u, v)$.

Definition 1. *[10, 14] 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* Pommaret multiplicative *or* $P-$multiplicative *and the other variables as* $P-$nonmultiplicative. *For $u = 1$ all the variables are $P-$multiplicative.*

Definition 2. *[14] Let $U \subset \mathbb{M}$ be a finite monomial set. For each $1 \leq i \leq n$ divide U into groups labeled by non-negative integers $d_1, \ldots, d_i$:*

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

A variable x_i is called Janet multiplicative *or* $J-$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 $deg_i(u) = \max\{deg_i(v) \mid v \in [d_1, \ldots, d_{i-1}]\}$. If a variable is not $J-$multiplicative for $u \in U$, it is called* $J-$nonmultiplicative *for u.*

For a polynomial $f \in \mathbb{R}$ the Pommaret separation of variables into multiplicative and nonmultiplicative is done in accordance with Definition 1 where $u = lm(f)$. Analogously, for an element $f \in F$ in a finite polynomial set $F \subset \mathbb{R}$ the Janet multiplicative and nonmultiplicative variables are determined by Definition 2 with $u = lm(f) \in U = lm(F)$.

We denote by $M_P(f)$, $NM_P(f)$ and by $M_J(f, F)$, $NM_J(f, F)$, respectively, the sets of $P-$multiplicative, $P-$nonmultiplicative and $J-$multiplicative, $J-$nonmultiplicative variables for f. A set of monomials in $P-$multiplicative variables for u and $J-$multiplicative variables for $u \in U$ will be denoted by $P(u)$ and $J(u, U)$, respectively.

Remark 1. The monomial sets $P(u)$ and $J(u, U)$ for any u, U such as $u \in U$ satisfy the following axioms

(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 $u \in V$

if one takes either $P(u)$ or $J(u, U)$ as $L(u, U)$. The axioms characterize an involutive monomial division, a concept invented in [1]. Every monomial set $L(u, U)$ satisfying the axioms generates an appropriate separation of variables into ($L-$)multiplicative and ($L-$)nonmultiplicative. As this takes place, an element $u \in U$ is an $L-$divisor of a monomial $w \in \mathbb{M}$ if $w/u \in L(u, U)$. In this case w is $L-$multiple of u. Using the axioms, a number of new divisions was constructed [2, 16] which may be also used for algorithmic computation of involutive bases.

All the next definitions in this section are those in [1, 2] specified to Pommaret and Janet divisions.

Definition 3. *Given a finite monomial set U, its* cone $C(U)$, $P-$cone $C_P(U)$ *and $J-$*cone $C_J(U)$ *are the following monomial sets*

$$C(U) = \cup_{u\in U}\, u\mathbb{M}, \quad C_P(U) = \cup_{u\in U}\, uP(u), \quad C_J(U) = \cup_{u\in U}\, uJ(u,U)\,.$$

Definition 4. *Given an admissible ordering $\succ$, a polynomial set $F \subset \mathbb{R}$ is called* Pommaret autoreduced *or $P-$*autoreduced *if every $f \in F$ has no terms $P-$multiple of an element in $lm(F) \setminus lm(f)$. Similarly, a finite polynomial set F is* Janet autoreduced *or $J-$*autoreduced *if each term in every $f \in F$ has no $J-$divisors among $lm(F) \setminus lm(f)$. A finite set F will be called* Pommaret-Janet autoreduced *or $PJ-$*autoreduced *if it is both $P-$autoreduced and $J-$autoreduced.*

Remark 2. From Definition 2 it follows that any finite set U of distinct monomials is $J-$autoreduced

$$(\forall u, v \in U)\ (u \neq v)\ \ [\ uJ(u,U) \cap vJ(v,U) = \emptyset\ ]\,.$$

Definition 5. *Given an admissible ordering $\succ$ and a polynomial set $F \subset \mathbb{R}$, a polynomial $h \in \mathbb{R}$ is said to be in $P-$*normal form modulo F *if every term in h has no $P-$ divisors in $lm(F)$. Similarly, if all the terms in h have no $J-$divisors among the leading terms of a finite polynomial set F, then h is in $J-$*normal form modulo F.

A general involutive normal form algorithm is described in [1], and an involutive normal form of a polynomial modulo any involutively autoreduced set is uniquely defined. We denote by $NF_P(f, F)$ and $NF_J(f, F)$, respectively, $P-$normal and $J-$normal form of polynomial f modulo F.

Pommaret or Janet autoreduction of a finite polynomial set F may be performed [1] similarly to the conventional autoreduction [17, 18]. If H is obtained from F by the conventional, or $J-$autoreduction we shall write $H = Autoreduce(F)$ or $H = Autoreduce_J(F)$, respectively.

Definition 6. *A $P-$autoreduced set F is called a* Pommaret basis *($P-$basis) of the ideal $Id(F)$ generated by F if*

$$(\forall f \in F)\ (\forall x \in NM_P(f))\ \ [\ NF_P(f \cdot x, F) = 0\ ]\,. \qquad (2)$$

Similarly, a $J-$autoreduced set F is called a Janet basis *($J-$basis) of $Id(F)$ if*

$$(\forall f \in F)\ (\forall x \in NM_J(f, F))\ \ [\ NF_J(f \cdot x, F) = 0\ ]\,. \qquad (3)$$

In accordance with Definition 5 the nonmultiplicative prolongation $f \cdot x$ with the vanishing $P-$ or $J-$normal form modulo polynomial set $F = \{f_1, \cdots, f_m\}$ can be rewritten as

$$f \cdot x = \sum_{i=1}^{m} f_i\, h_i, \quad h_i \in \mathbb{R}, \quad lm(f) \cdot x \succeq lm(f_i\, h_i) \quad (1 \leq i \leq m)$$

where $supp(h_i) \subset P(f_i)$ or $supp(h_i) \subset J(f_i, F)$, respectively, for every polynomial product $f_i\, h_i$.

Let G_P and G_J be Pommaret and Janet bases of an ideal I, respectively. Then, from Definition 6 it follows [1] that

$$h \in I \quad \text{iff} \quad NF_P(h, G_P) = 0 \quad \text{and} \quad h \in I \quad \text{iff} \quad NF_J(h, G_J) = 0\,. \tag{4}$$

This implies, in particular, the equalities

$$C_P(lm(G_P)) = C(lm(G_P))\,, \quad C_J(lm(G_J)) = C(lm(G_J))\,. \tag{5}$$

It is immediate from (5) that $lm(G_P)$ and $lm(G_J)$ are $P-$ and $J-$bases of the initial ideal $in_{\succ}(I)$.

Corollary 1. *If for a $P-$autoreduced set G_P the equality (5) of its cone and $P-$cone holds and $lm(G_P)$ is a basis of the initial ideal $in\,(Id(G_P))\}$, then G_P is a $P-$ basis of $Id(G_P)$. Analogous statement holds for a $J-$basis.*

Whereas monic Pommaret bases much like to reduced Gröbner bases are unique, every ideal, by property (2), has infinitely many monic Janet bases. Among them there is the unique $J-$basis defined as follows.

Definition 7. *A Janet basis G of ideal $Id(G)$ is called* minimal *if for any other $J-$basis F of the ideal the inclusion $lm(G) \subseteq lm(F)$ holds.*

Remark 3. Every zero-dimensional polynomial ideal has a finite Pommaret basis, and for a positive dimensional ideal the existence of finite Pommaret basis can be always achieved by means of an appropriate linear transformation of variables [5, 6, 10, 11].

3 Relation Between Polynomial Pommaret and Janet Bases

Given a finite monomial set U, Definitions 1 and 2 generally give different separations of variables for elements in U.

Example 1. $U = \{x_1x_2, x_2x_3, x_3^2\}$.

monomial	Pommaret		Janet	
	M_P	NM_P	M_J	NM_J
x_1x_2	x_2, x_3	x_1	x_1, x_2, x_3	$-$
x_2x_3	x_3	x_1, x_2	x_2, x_3	x_1
x_3^2	x_3	x_1, x_2	x_3	x_1, x_2

Here is, however, an important relation between Pommaret and Janet separations:

Proposition 1. [15](see also [1]). *If a finite monomial set U is $P-$autoreduced, then for any $u \in U$ the following inclusions hold*

$$M_P(u,U) \subseteq M_J(u,U), \quad NM_J(u,U) \subseteq NM_P(u,U)\,.$$

For U in Example 1 the minimal Janet basis U_J and the Pommaret basis U_P of the monomial ideal $Id(U)$ are

$$U_J = U \cup \{x_1 x_3^2\}, \quad U_P = U_J \cup_{i=2}^{\infty} \{x_1^i x_2\} \cup_{j=2}^{\infty} \{x_1^j x_3^2\} \cup_{k=2}^{\infty} \{x_2^k x_3\}\,. \tag{6}$$

Note that U_P is infinite and $U_J \subset U_P$. Below we show that the inclusion $G_J \subseteq G_P$ holds for any minimal Janet basis G_J and Pommaret basis G_P if both of them are monic and generate the same ideal. Furthermore, the proper inclusion $G_J \subset G_P$ holds iff P is infinite.

The following algorithm, given a finite polynomial set $F \in \mathbb{R}$ and an admissible ordering $\succ$, performs $PJ-$autoreduction of F and outputs a PJ-autoreduced set H. In this case we shall write $H = Autoreduce_{PJ}F$.

Since the involutive $P-$ and $J-$reductions which are performed in the course of the algorithm form subsets of the conventional reductions [1], the algorithm terminates. Furthermore, the **while**-loop generates the $P-$autoreduced monomial set $lm(H)$. In accordance with Remark 2 the Janet autoreduction in line 12 does not affect the leading terms, and, hence, the output polynomial set is both Pommaret and Janet autoreduced.

Algorithm: **Pommaret-JanetAutoreduction**$(F, \succ)$

Input: $F \in \mathbb{R}$, a finite set; $\succ$, an admissible ordering
Output: $H = Autoreduce_{PJ}(F)$
begin
1 $G := \emptyset$; $H := F$
2 **repeat**
3 $\tilde{H} := H$
4 **while** exist $h \in H$ such that
5 $lm(h) \in C_P\,(lm(H \setminus \{h\}))$ **do**
6 $H := H \setminus \{h\}$; $G := G \cup \{h\}$
7 **for each** $g \in G$ **do**
8 $G \setminus \{g\}$; $f := NF_J(g,H)$
9 **if** $f \neq 0$ **then**
10 $H := H \cup \{f\}$
11 **until** $H = \tilde{H}$
12 $H := Autoreduce_J(H)$
end

Proposition 2. *If algorithm* **Pommaret-JanetAutoreduction** *takes a Janet basis F as an input its output H is also a Janet basis of the same ideal, and $H \subseteq F$.*

Proof. Let F be a Janet basis of the ideal $Id(F)$ and H be a polynomial set which is computed by the algorithm. Apparently, $Id(H) = Id(F)$. Consider $U = lm(F)$. If U is $P-$autoreduced, then H initiated as F in line 1 does not change in the process of the algorithm, and, hence, $H = F = Autoreduce_{PJ}(F)$. Otherwise, consider the output polynomial sets H. Denote $lm(H)$ by V. Then, by construction, $V \subset U$.

Consider a monomial $t \in C_J(U)$ and show that $t \in C_J(V)$. Let $u \in U$ be a $J-$divisor of t, that is, $t \in uJ(u,U)$, and $v \in V$ be such that $v|u$. If $u = v$, by property (d) of Janet division in Remark 1, we are done. Let now $u \in U \setminus V$. The **while**-loop provides that $u \in vP(v)$. If $v = x_1^{d_1} \cdots x_k^{d_k}$ with $d_k > 0$ $(1 \leq k \leq n)$, then from Definition 1 it follows that $u = x_1^{d_1} \cdots x_k^{d_k+e_k} \cdots x_n^{e_n}$.

We have to prove that any variable $x_i \in J(u,U)$ $(1 \leq i \leq n)$ satisfy $x_i \in J(v,V)$. Consider two alternative cases: $i < k$ and $i \geq k$. In the first case, by Definition 2, both u, v belong to the same group $[d_1, \cdots, d_{i-1}]$ of monomials in U. It follows that $x_i \in J(v,V)$. In the second case, by Definition 1, $x_i \in P(v)$ and Proposition 1 we find again that x_i is $J-$multiplicative for v as an element in V.

Therefore, V is a Janet monomial basis of $Id(U)$. Thus, by Corollary 1, H is a $J-$basis. In so doing, every $J-$normal form computed in line 8 of the algorithm apparently vanishes. This implies the inclusion $H \subseteq F$. □

Corollary 2. *A minimal Janet basis is Pommaret autoreduced.*

Proof. Let G be a minimal Janet basis. From Proposition 2 and Definition 7 it follows that $lm(G)$ is $P-$autoreduced. Thus, G is $P-$autoreduced. □

It is clear that, given a Janet basis, its $PJ-$autoreduction yields, generally, more compact basis than the pure $P-$autoreduction.

Example 2. Consider polynomial set

$$F = \{xyzt - xz, xyz + z^2, xzt + x^2, xy + z, zt + x\}$$

which is a Janet basis of the ideal $Id(F)$ with respect to the degree-reverse-lexicographical ordering $\succ$ such that $x \succ y \succ z \succ t$. Given F and $\succ$ as input, the algorithm **Pommaret-JanetAutoreduction**$(F, \succ)$ outputs the minimal $J-$basis

$$G_1 = \{xzt + x^2, xy + z, zt + x\}\,.$$

If one uses the Pommaret normal form computation in line 7 instead of that of Janet, then the algorithm leads to the output

$$G_2 = \{xzt + x^2, z^2t + xz, xy + z, zt + x\} = G_1 \cup \{z^2t + xz\}\,.$$

The following theorem is the main theoretical result of the present paper and forms a basis of an algorithm for construction of Janet and Pommaret bases described in the next section.

Theorem 1. *Given an ideal $I \subseteq R$ and an admissible monomial ordering $\succ$ compatible with (1), the following are equivalent:*

(i) *I has a finite Pommaret basis.*
(ii) *A minimal Janet basis of I is its Pommaret basis.*
(iii) *If F is a Janet basis of I, then $G = Autoreduce_{JP}(F)$ is its Pommaret basis.*

Proof. $(i) \Longrightarrow (iii)$: Suppose $G = \{g_1, \ldots, g_m\}$ which, by Proposition 2, is also a $J-$basis of I, is not its $P-$basis. Our goal is to prove that a Pommaret basis of I is an infinite polynomial set. From Corollary 1 it follows that

$$(\exists g \in G)\ (\exists x_k \in NM_P(g))\ \ [\ lm(g) \cdot x_k \notin C_P\,(lm(G))\ ]\,. \tag{7}$$

Among nonmultiplicative prolongations $g \cdot x_k$ satisfying (7) choose one with the lowest $lm(g) \cdot x_k$ with respect to the pure lexicographical ordering $\succ_{Lex}$ generated by (1). If there are several such prolongations choose that with the lexicographically lowest x_k, that is, with the lexicographically highest g. This choice is unique since G is $J-$autoreduced.

We claim that $x_k \in M_J(g, G)$. Assume for a contradiction that $x_k \in NM_J(g, G)$. Then from Janet involutivity conditions (3) we obtain

$$(\exists f \in G)\ \ [\ lm(g) \cdot x_k = lm(f) \cdot w \mid w \in J\,(lm(f), lm(G))\ ]\,. \tag{8}$$

In accordance with condition (7) w contains $P-$nonmultiplicative variables for f and from (8) it follows [1] that $f \succ_{Lex} g$. If $w = x_j$, then $x_j \succ x_k$, and both $lm(f) \cdot x_j$ and $lm(g)$ belong to the same monomial group $[\,deg_1(g), \ldots, deg_{k-1}(g)]$ appearing in Definition 2. Hence, $x_j \in NM_J(f, G)$ in contradiction to (8). Therefore, $deg(w) \geq 2$ and (8) can be rewritten as

$$lm(g) \cdot x_k = (lm(f) \cdot v) \cdot x_j$$

with $w = v \cdot x_j$. Show that $lm(f) \cdot v \in P\,(lm(f))$. If $v \in C_P\,(lm(G))$ we are done. Otherwise there is $x_m | v$ such that $x_m \in NM_P\,(lm(f))$. Since $lm(f) \cdot x_m \prec_{Lex} lm(g) \cdot x_k$, our choice of g and x_k implies the existence $g_1 \in G$ such that $f \cdot x_m = g_1 \cdot v_1$ and $v/x_m \in P\,(lm(g_1))$. If $v_1 = v/x_m \in P\,(lm(g_1))$ we are done. Otherwise we select again a $P-$nonmultiplicative variable for g_1 occurring in v_1 and rewrite the corresponding prolongation in terms of its $P-$divisor $lm(g_2) \in lm(G)$. Continuity of Pommaret division [1] provides termination of the rewriting process with an element in $\tilde{g} \in G \setminus \{g\}$ such that $lm(\tilde{g})$ is a $P-$divisor of $lm(f) \cdot v$. Because G is $P-$autoreduced, by Proposition 1 $lm(\tilde{g})$ is also a $J-$divisor of $lm(f) \cdot v$. By this means there are two different Janet divisors $lm(f)$ and $lm(\tilde{g})$ of the same monomial that contradicts Remark 2 and proves the claim.

Let now H be a $P-$basis of $Id(G)$. Denote $lm(g) \cdot x_k$ by u and show that $u \in lm(H)$. Suppose there is an element $h \in H \setminus G$, such that $u = lm(h) \cdot v$ with $v \in P\,(lm(h))$. Then $h \prec_{Lex} u$ and there is $q \in G$ satisfying $lm(h) = lm(q) \cdot w$ where $w \notin P\,(lm(q))$. Thus, there is a $P-$nonmultiplicative prolongation $q \cdot x_j$ with $x_j | w$ such that $lm(q) \cdot x_j \prec_{Lex} u$ and $lm(q) \cdot x_j \notin C_P\,(lm(G))$ that contradicts the above choice of g and x_k.

Now consider monomial set $U = lm(G) \cup \{u\} \subseteq lm(H)$. By Definition 2, $x_k \in NM_P(u)$ and $u \cdot x_k$ is obviously the lexicographically lowest $P-$nonmultiplicative prolongation of elements in U. It is easy to see that $u \cdot x_k \notin C_P(U)$. Indeed, since $x_k \in M_J(g, G)$, it follows that $u \cdot x_k \notin U$, and a $P-$divisor of $u \cdot x_k$ would also $P-$divide $lm(g)$ that is impossible as G is $P-$autoreduced. Thus, we find that $u \cdot x_k \in lm(H)$. By sequential repetition of this reasoning for $u \cdot x_k^i$ $(i = 2, 3 \ldots)$ we deduce that every such monomial is an element in $lm(H)$, and, therefore, H is infinite.

$(iii) \Longrightarrow (ii)$: If G is a minimal Janet basis of $Id(G)$, then Corollary 2 implies $G = Autoreduce_{JP}(G)$, and the above arguments show that either G is also a $P-$basis or the latter is infinite.

$(ii) \Longrightarrow (i)$: This implication is obvious. □

Corollary 3. *Let G_J be a monic minimal Janet basis and G_P be a monic Pommaret basis for the same polynomial ideal and monomial ordering. Then $G_J \subseteq G_P$ and $G_J \subset G_P$ iff G_P is infinite.*

Proof. This follows from the above proof of Theorem 1. □

Corollary 4. *If a polynomial ideal I is in generic position [6] with respect to the given admissible monomial ordering, then a minimal Janet basis of I is also its Pommaret basis. Additionally, if I is homogeneous, then every of these bases is the reduced Gröbner basis.*

Proof. I has a finite Pommaret basis [6, 7]. If I is homogeneous, then its Pommaret basis is the reduced Gröbner basis [7]. □

4 Algorithm for Construction of Janet Bases

In this section we present an algorithm for constructing $J-$bases of polynomial ideals which is based on Theorem 1 and will be called **JanetBasis**. Whenever the ideal generated by an input polynomial set has a finite $P-$basis for a given admissible ordering, the algorithm outputs just this basis which is also a minimal $J-$basis. Otherwise, the $J-$basis computed by the algorithm is not necessarily minimal as we demonstrate below by the explicit example.

Algorithm: **JanetBasis**$(F, \succ)$

Input: $F \in \mathbb{R}$, a finite set; $\succ$, an admissible ordering
Output: G, an involutive basis of the ideal $Id(F)$
begin
1 $\quad G := Autoreduce(F)$
2 $\quad T := \emptyset$
3 $\quad$ **for each** $g \in G$ **do**
4 $\quad\quad T := T \cup \{(g, lm(g), \emptyset)\}$
5 $\quad$ **while** exist $(g, u, D) \in T$ and $x \in NM_J(g, G) \setminus D$ **do**
6 $\quad\quad$ **choose** such $(g, u, D), x$ with the lowest $lm(g) \cdot x$ w.r.t. $\succ$
7 $\quad\quad T := T \setminus \{(g, u, D)\} \cup \{(g, u, D \cup \{x\})\}$
8 $\quad\quad$ **if** $Criterion(g \cdot x, u, T)$ is false **then**
9 $\quad\quad\quad h := NF_J(g \cdot x, G)$
10 $\quad\quad\quad$ **if** $h \neq 0$ **then**
11 $\quad\quad\quad\quad$ **if** $lm(h) = lm(g \cdot x)$ **then**
12 $\quad\quad\quad\quad\quad T := T \cup \{(h, u, \emptyset)\}$
13 $\quad\quad\quad\quad$ **else**
14 $\quad\quad\quad\quad\quad T := T \cup \{(h, lm(h), \emptyset)\}$
15 $\quad\quad\quad\quad\quad G := Autoreduce_{PJ}(G \cup \{h\})$
16 $\quad\quad Q := T$
17 $\quad\quad T := \emptyset$
18 $\quad\quad$ **for each** $g \in G$ **do**
19 $\quad\quad\quad$ **if** exist $(f, u, D) \in Q$ s.t. $lm(f) = lm(g)$ **then**
20 $\quad\quad\quad\quad$ **choose** $\tilde{g} \in G$ s.t. $u \in lm(\tilde{g})J(lm(\tilde{g}), lm(G))$
21 $\quad\quad\quad\quad T := T \cup \{(g, lm(\tilde{g}), D \cap NM_J(g, G))\}$
22 $\quad\quad\quad$ **else**
23 $\quad\quad\quad\quad T := T \cup \{(g, lm(g), \emptyset)\}$
end

$Criterion(g, u, T)$ is true provided that if there is $(f, v, D) \in T$ such that $lcm(u, v) \prec lm(g)$ and $lm(g) \in lm(f)J(lm(f), lm(G))$.

The structure of algorithm **JanetBasis** is very close to that of the algorithm **InvolutiveBasis** devised in [1] for construction of involutive bases for arbitrary constructive involutive divisions, and, hence, applicable to Janet division. The main difference between the algorithms is the form of their intermediate autoreduction. Whereas the previous algorithm, when specified for Janet division, uses the pure Janet autoreduction which do not affect the leading terms, the below one uses the above algorithm **Pommaret-JanetAutoreduction**. By this reason, the algorithm **InvolutiveBasis**, unlike the below one, almost never outputs a minimal Janet basis or a Pommaret basis if the latter is finite. In paper [2] we designed the algorithm **MinimalInvolutiveBasis** which always outputs a minimal involutive basis whenever the latter exists. As we now see from Theorem 1, this algorithm in the case of Janet division outputs also a Pommaret basis if it is finite.

Besides, in the algorithm **InvolutiveBasis** the involutive autoreduction is performed whenever nonzero normal form is obtained in the **while**-loop. In the algorithm **JanetBasis** the subalgorithm **Pommaret-JanetAutoreduction** is caused by a nonzero $J-$normal form h in line 15 only if the leading term of the related prolongation is $J-$reducible. Otherwise, since G is always $P-$autoreduced before its enlargement with h, $lm(h)$ cannot $P-$divide, in accordance with Definition 1, any other element in $lm(G)$.

Note that we indicated the intersection in line 21 to emphasize that elements in D must be nonmultiplicative variables for the corresponding polynomial that is always understood in algorithms of papers ([1, 2, 4, 16]).

Noetherity of Janet division provides termination of the algorithm **JanetBasis** [1]. To show this consider the intermediate bases $G_0 = Autoreduce(F)$ and G_i $(i = 1, 2, \ldots)$ generated after the $i - th$ iteration of the **while**-loop. It is clear that

$$Id\,(lm(G_0)) \subseteq Id\,(lm(G_1)) \subseteq Id\,(lm(G_2)) \subseteq \cdots \tag{9}$$

and this chain is stabilized after finitely many steps. Namely, the stabilization starts when the intermediate polynomial set G becomes a (non-necessarily reduced) Gröbner basis of $Id(F)$. By partial involutivity of G [1], the proper inclusion in chain (9) holds only when G is enlarged by h in line 15. In between of such proper inclusions and after the chain stabilization $lm(G)$ is completed with $lm(h) = lm(g \cdot x)$ as stands in line 11, and this completion cannot be infinite by noetherity of Janet division [1]. Once algorithm terminates, it produces, by Proposition 2, a $PJ - autoreduced$ Janet basis of F because the involutivity conditions (3) are satisfied as is checked in lines 6 and 9 where $h = 0$. In so doing, correctness of the criterion which is verified in line 8 is proved exactly as done in [1] for the algorithm **InvolutiveBasis**.

Remark 4. In line 6 of the algorithm **JanetBasis** one can use any admissible ordering for selection of the current $J-$nonmultiplicative prolongation $g \cdot x$ to be treated in the following lines. This selection ordering may not only be different from the main ordering $\succ$ but also may vary at every step when the selection is done. Correctness of this arbitrariness in the choice of selection ordering follows from the correctness of this arbitrariness for the monomial completion procedure [16].

As mentioned above, the algorithm **JanetBasis** for an ideal of positive dimension may not output its minimal $J-$basis. We demonstrate this by the following example.

Example 3. Let F be a set $\{x^2y - z, x\,y^2 - y\}$ generating one-dimensional ideal, and $\succ$ be the degree-reverse-lexicographical ordering with $x \succ y \succ z$. Then the algorithm **JanetBasis**$(F, \succ)$ outputs the following Janet basis

$$G = \{x^2y - z, x^2z - z^3, x\,y - y\,z, x\,z - z^2, y^2z - y, y\,z^2 - z\}$$

whereas the minimal Janet basis coinciding with the reduced Gröbner basis is

$$\{x\,y - y\,z, x\,z - z^2, y^2z - y, y\,z^2 - z\}\,.$$

Remark 5. The algorithm **JanetBasis** is an improved version of the algorithm designed by Zharkov [15]. The first improvement is the use of the mixed Pommaret-Janet autoreduction instead of the pure Pommaret autoreduction as Zharkov proposed. Let G_1 and G_2 be output Janet bases computed with the use of $PJ-$ and $P-$autoreduction, respectively. Then, Proposition 1 implies $G_1 \subseteq G_2$ and below we give an example when the proper inclusion holds. The second improvement is the criterion used in line 7. This criterion is an involutive analogue [1] of the Buchberger's chain criterion [17] and is superior to the criterion used in [15].

Example 4. [20] The following polynomial set generates three-dimensional ideal

$$F = \left\{ \begin{array}{l} 4x_5(x_6+2a_1-8x_1)(a_2-a_3)-x_2x_3x_4+x_2+x_4 \\ 4x_5(x_6+2a_1-8x_2)(a_2-a_3)-x_1x_3x_4+x_1+x_3 \\ 4x_5(x_6+2a_1-8x_3)(a_2-a_3)-x_1x_2x_4+x_2+x_4 \\ 4x_5(x_6+2a_1-8x_4)(a_2-a_3)-x_1x_2x_3+x_1+x_3 \end{array} \right\} \qquad (10)$$

where

$$a_1 = x_1+x_2+x_3+x_4,\ a_2 = x_1x_2x_3x_4,\ a_3 = x_1x_2+x_2x_3+x_3x_4+x_4x_1\,.$$

For the polynomial set (10) and the degree-reverse-lexicographical ordering compatible with (1) the algorithm **JanetBasis** outputs set G_1 with 71 polynomials. The pure Pommaret autoreduction in line 15 generates set $G_2 \supset G_1$ of 75 elements. Note that a minimal Janet basis contains 49 polynomials whereas the reduced Gröbner basis contains 44 polynomials.

5 Linear Differential Bases

Let $\mathbb{K}$ be a zero characteristic differential field with a finite number of mutually commuting derivation operators $\partial/\partial x_1,\ldots,\partial/\partial x_n$. Consider the differential polynomial ring $\mathbb{DR} = \mathbb{K}\{y_1,\ldots,y_m\}$ with the set of differential indeterminates $\{y_1,\ldots,y_m\}$. Elements in $\mathbb{DR}$ are differential polynomials in $\{y_1,\ldots,y_m\}$. An ideal in $\mathbb{DR}$ generated by linear differential polynomials is called linear differential ideal [23].

In [4], by exploiting the well-known algorithmic similarities between polynomial and linear differential systems and the association between monomials and the derivatives, we extended the general involutive methods and algorithms designed in [1, 2, 16] for polynomial ideals to linear differential ideals. The statements and algorithms of Sect. 3 and 4 admit similar extension. As this takes place, all the statements proved above for the polynomial case are proved by parallel arguments for the differential case. In the following table we give a short correspondence between these two cases. In particular, this correspondence allows one to rewrite the algorithms **Pommaret-JanetAutoreduction** and **JanetBasis** for linear differential bases.

Commutative Algebra	Differential Algebra
$\mathbb{R} = K[x_1, \ldots, x_n]$	$\mathbb{DR} = \mathbb{K}\{y_1, \ldots, y_m\}$
$f, g, h \in \mathbb{R}$	$f, g, h \in \mathbb{DR}$
$F, G, H \subset \mathbb{R}$	$F, G, H \subset \mathbb{DR}$
$x^\alpha \equiv x_1^{\alpha_1} \cdot x_n^{\alpha_n}$	$\partial_\alpha y_j \equiv \frac{\partial^{\alpha_1+\cdots+\alpha_n} y_j}{\partial x_1^{\alpha_1} \cdots \partial x_n^{\alpha_n}} \Longleftrightarrow [x^\alpha]_j$
$g \cdot x$	$\partial_x g$
monomial ordering	ranking
$lm(g)$	leading derivative $ld(g)$
$lm(G)$	$ld(G) = \cup_{g\in G}\{ld(g)\}$

6 Conclusion

As we have seen finite Pommaret bases of polynomial and linear differential ideals are minimal Janet bases. The above proof of Theorem 1 shows that, given a $P-$autoreduced Janet basis G, it is easy to verify the existence of a finite Pommaret basis. One suffices to check the condition (7). Another check which may be even easier in practice is to look at the Pommaret and Janet separation of variables for elements in G. As shown in [9], the existence of a finite Pommaret basis implies coincidence of both separations for every element in G. Moreover, the leading monomial structure of an infinite Pommaret basis can be read off the structure of $lm(G)$ (cf. (6) for Example 1).

Therefore, minimal Janet bases can be used in commutative and differential algebra as well as Pommaret bases with the advantage of finiteness. For example, in the formal theory of differential equations [9–11] infinity of a Pommaret basis signals on δ-singularity of the coordinate system chosen, and the condition (7) gives the same signal for Janet bases.

On the face of it, Pommaret division looks like more attractive than Janet one since its separation is easier to compute than the Janet separation. Besides, Pommaret division, unlike that of Janet, is globally defined [2]. Hence, after enlargement of the intermediate polynomial set with an irreducible $P-$nonmultiplicative prolongation there are no needs to recompute the Pommaret separation for other elements in the set. However, the careful implementation of both divisions do not reveal any notable advantage of Pommaret division over Janet division in construction of polynomial bases. This rather surprising fact was firstly observed by Zharkov [15]. One of the explanations of this experimental phenomenon is given by Proposition 1: one must generally treat more $P-$nonmultiplicative prolongations than $J-$nonmultiplicative ones. In so doing, the search for an involutive divisor in the process of involutive reduction can be done similarly for both divisions as we show in our forthcoming paper [21].

The algorithm **JanetBasis** presented above is now under implementation in C in parallel with the algorithm **MinimalInvolutiveBasis** [2] specified for

Janet division. Our first experimentation with the codes shows that sometimes the former algorithm runs faster than the latter one and needs less computer memory. For example, modular computation of the degree-reverse-lexicographic Janet basis for the Cyclic 7 example [22] is about twice faster with the algorithm **JanetBasis** than with the algorithm **MinimalInvolutiveBasis**. Currently, the timings for computation modulo 31013 are about 5 and 10 minutes, respectively, on a Pentium Pro 333 Mhz computer.

7 Acknowledgements

I am grateful to W.M.Seiler for useful discussions and for providing me with his recent paper [9]. I would also like to thank D.A.Yanovich for his assistance in computing the above examples. This work was partially supported by grant INTAS-99-1222 and grants No. 98-01-00101 and 00-15-96691 from the Russian Foundation for Basic Research.

References

1. Gerdt, V.P., Blinkov, Yu.A.: Involutive Bases of Polynomial Ideals. *Math. Comp. Sim.* **45** (1998) 519-542.
2. Gerdt, V.P., Blinkov, Yu.A.: Minimal Involutive Bases. *Math. Comp. Simul.* **45** (1998) 543-560.
3. Apel, J.: Theory of Involutive Divisions and an Application to Hilbert Function. *J. Symb. Comp.* **25** (1998) 683-704.
4. Gerdt, V.P.: Completion of Linear Differential Systems to Involution. In: *Computer Algebra in Scientific Computing / CASC'99*, V.G.Ganzha, E.W.Mayr and E.V.Vorozhtsov (Eds.), Springer-Verlag, Berlin, 1999, pp. 115-137.
5. Zharkov, A.Yu., Blinkov, Yu.A.: Involutive Approach to Investigating Polynomial Systems. In: Proceedings of "SC 93", International IMACS Symposium on Symbolic Computation: New Trends and Developments (Lille, June 14-17, 1993). *Math. Comp. Simul.* **42** (1996), 323-332.
6. Apel, J.: A Gröbner Approach to Involutive Bases. *J. Symb. Comp.* **19** (1995) 441-458.
7. Mall, D.: On the Relation Between Gröbner and Pommaret Bases. *AAECC* **9** (1998) 117-123.
8. Zharkov, A.Yu.: 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, 1996, pp. 389-399.
9. Seiler, W.M.: A Combinatorial Approach to Involution and δ-Regularity. *Preprint*, University of Mannheim, 2000.
See **www.ira.uka.de/iaks-calmet/werner/publ.html**.
10. Pommaret, J.F.: *Systems of Partial Differential Equations and Lie Pseudogroups*, Gordon & Breach, New York, 1978.
11. Pommaret J.-F.: *Partial Differential Equations and Group Theory. New Perspectives for Applications*, Kluwer, Dordrecht, 1994.
12. Schwarz, F.: An Algorithm for Determining the Size of Symmetry Groups. *Computing* **49** (1992) 95-115.

13. Schwarz, F.: Janet Bases of 2^{nd} Order Ordinary Differential Equations. In: *Proceedings of the ISSAC'96*, Lakshman Y.N. (ed.), ACM Press, 1996, pp.179-188.
14. Janet, M.: *Leçons sur les Systèmes d'Equations aux Dérivées Partielles*, Cahiers Scientifiques, IV, Gauthier-Villars, Paris, 1929.
15. Zharkov, A.Yu.: Involutive Polynomial Bases: General Case. *Preprint JINR E5-94-224*, Dubna, 1994. Submitted to ISSAC'94.
16. Gerdt, V.P.: Involutive Division Technique: Some Generalizations and Optimizations, *Zapiski Nauchnykh Seminarov POMI (St.Petersburg)* **258** (1999) 185-207. To appear in *J. Math. Sci.* **258** (2000).
17. Buchberger, B.: Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory. In: *Recent Trends in Multidimensional System Theory*, Bose, N.K. (ed.), Reidel, Dordrecht, 1985, pp. 184-232.
18. Becker, T., Weispfenning, V., Kredel, H.: *Gröbner Bases. A Computational Approach to Commutative Algebra.* Graduate Texts in Mathematics **141**, Springer-Verlag, New York, 1993.
19. Gerdt, V.P., Kornyak, V.V., Berth, M., Czichowsky G.: Construction of Involutive Monomial Sets for Different Involutive Divisions. In: *Computer Algebra in Scientific Computing / CASC'99*, V.G.Ganzha, E.W.Mayr and E.V.Vorozhtsov (Eds.), Springer-Verlag, Berlin, 1999, pp. 147-157.
20. Verschelde, J., Gaterman, K.: Symmetric Newton Polytopes for Solving Polynomial Systems, *Preprint SC 94-3*, Konrad-Zuse-Zentrum für Informationstechnik, Berlin, 1994.
21. Gerdt, V.P., Blinkov, Yu.A., Yanovich D.A. *Computation of Monomial Janet Bases.* In preparation.
22. Bini, D., Mourrain, B.: *Polynomial Test Suite*, 1996. See **www-sop.inria.fr/saga/POL**.
23. Kolchin, E.R.: *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.