Janet-Like Monomial Division

Conference Paper *in* Lecture Notes in Computer Science · September 2005

DOI: 10.1007/11555964_15 · Source: DBLP

2 authors:

Vladimir Gerdt
Joint Institute for Nuclear Research

Yuri A. Blinkov
Saratov State University

Janet-Like Monomial Division

Vladimir P. Gerdt[1] and Yuri A. Blinkov[2]

[1] Laboratory of Information Technologies,
Joint Institute for Nuclear Research, 141980 Dubna, Russia
gerdt@jinr.ru
[2] Department of Mathematics and Mechanics,
Saratov University, 410071 Saratov, Russia
BlinkovUA@info.sgu.ru

Abstract. In this paper we introduce a new type of monomial division called Janet-like, since its properties are similar to those of Janet division. We show that the former division improves the latter one. This means that a Janet divisor is always a Janet-like divisor but the converse is generally not true. Though Janet-like division is not involutive, it preserves all algorithmic merits of Janet division, including Noetherianity, continuity and constructivity. Due to superiority of Janet-like division over Janet division, the algorithm for constructing Gröbner bases based on the new division is more efficient than its Janet division counterpart.

1 Introduction

In [1] we introduced the concept of involutive division as an underlying notion for theory of involutive Gröbner bases and designed algorithms for their construction. Then, a modified concept of involutive division was introduced in [2] together with another form of involutive algorithms based on this concept.

For a given finite polynomial set and a monomial order, an involutive division partitions the variables into two disjoint subsets called multiplicative and nonmultiplicative. One of such partitions was invented by French mathematician M.Janet in his study [3] of algebraic partial differential equation by means of their transformation (often called completion) to an involutive form [1]. This partition generates Janet division [1] which is one of the most widely used among known involutive divisions. Janet division and related involutive algorithms for completion of polynomial or/and differential systems to involution have been implemented in Reduce, C/C++ [4], Mathematica [5], MuPAD [6], Maple [7], Aldor [8].

One of the main motivations for use of Janet division is its practical computational efficiency. Our present day algorithms [4,9], being optimized versions of those in [1] and implemented for Janet division, demonstrate their superiority over the best implementations [2] of the Buchberger algorithm [10]. Some of the related efficiency aspects are discussed in [9].

[1] This is where the term "involutive" came from.
[2] See our Web page http://invo.jinr.ru for experimental comparison with Singular and Magma.

V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov (Eds.): CASC 2005, LNCS 3718, pp. 174–183, 2005.

It should be noted, however, that the indicated superiority takes place for most of standard benchmarks, but not for all of them. In addition, there is a class of polynomial systems for which any Janet division algorithm is to be highly inefficient because of a very large Gröbner redundancy of Janet bases. The last means much larger cardinality of Janet bases than that of the reduced Gröbner bases. For those examples the degrees of variables which occur in the leading monomial set of a Gröbner basis form a sparse set in the resulting range of the degrees. It generates a large number of nonmultiplicative prolongations that are involutively head irreducible, and, by this reason, present in the the output Janet basis.

Among such polynomial systems are those generating toric ideals as we already demonstrated in [11]. By the maximality arguments [2], one can expect that any other involutive division will also be inefficient for those systems.

In the given paper we introduce another monomial division which also restricts the conventional division (cf. [9]) and is very similar to Janet division. By this reason we call it Janet-like. The new division, however, is not involutive. Nevertheless, it possesses all merits of Janet division. Moreover, it improves the last division by optimizing the number of operations needed to construct the output Gröbner bases called Janet-like. Janet-like bases and their algorithmic construction are considered in a separate paper [12].

2 Basics

Let $\mathbb{R} = \mathbb{K}[\mathbb{X}]$ be the polynomial ring over the field $\mathbb{K}$ in the indeterminates $\mathbb{X} = \{x_1, \ldots, x_n\}$. By $\mathbb{M}$ we denote the monoid of monomials in $\{x_1^{i_1} \cdots x_n^{i_n} \mid i_k \in \mathbb{N}_{\geq 0},\ 1 \leq k \leq n\}$ in $\mathbb{R}$. By $\deg_i(u)$ we denote the degree of x_i in $u \in \mathbb{M}$ and by $\deg(u) = \sum_{i=1}^{n} \deg_i(u)$ the total degree of u. An admissible monomial order such that

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

will be denoted by $\succ$.

As usual, the conventional divisibility of monomial v by monomial u will be denoted by $u \mid v$. If $u \mid v$ and $\deg(u) < \deg(v)$, i.e. u is a proper divisor of v, we shall write $u \sqsubset v$.

For a polynomial $f \in \mathbb{R} \setminus \{0\}$ its leading monomial, leading term and leading coefficient will be denoted by $\mathrm{lm}(f)$, $\mathrm{lt}(f)$ and $\mathrm{lc}(f)$, respectively. Given a polynomial set $F \subset \mathbb{R} \setminus \{0\}$ and an order $\succ$, $\mathrm{lm}(F)$ will denote the leading monomial set of F. For the ideal in $\mathcal{I} \in \mathbb{R}$ generated by a polynomial set $F \subset \mathbb{R}$ we shall write $\mathcal{I} = \mathrm{Id}(F)$.

Definition 1. *Gröbner basis* [10]. Given an order $\succ$, a finite subset $G \subset \mathbb{R}$ is called a *Gröbner basis* of ideal $\mathcal{I} = \mathrm{Id}(G) \in \mathbb{R}$ if

$$\forall f \in \mathcal{I},\ \exists g \in G \ :\ \mathrm{lm}(g) \mid \mathrm{lm}(f)\,. \tag{2}$$

The basic idea behind the involutive division approach [1,2] is to replace the conventional division in (2) by its certain restriction called involutive. In the present paper, we need, however, more general concepts defined as follows.

Definition 2. (*Restricted division* [9]). A *restricted division* r on $\mathbb{M}$ is a reflexive transitive relation, denoted by $u \mid_r v$ $(u, v \in \mathbb{M})$, such that $u \mid_r v \Longrightarrow u \mid v$. If $u \mid_r v$, then u is $r-$*divisor* of v and v is r-*multiple* of u, respectively.

Definition 3. (r-*basis* [9]). Given an order $\succ$ and a restricted division r, a finite subset $G \subset \mathbb{R}$ is called $r-$*basis* of ideal $\mathcal{I} = \mathrm{Id}(G) \in \mathbb{R}$ if

$$\forall f \in \mathcal{I},\ \exists g \in G\ :\ \mathrm{lm}(g) \mid_r \mathrm{lm}(f)\,.$$

Note, that the whole class of restricted divisions includes the conventional division as well. From Definition 2 it follows that a $r-$basis, if exists, is always a Gröbner basis. It is also easy to reformulate the concept of Gröbner reduction and normal form [10] in terms of the restricted division [9].

A natural way to introduce a restricted monomial division r is to indicate a certain subset $X(u) \subseteq \mathbb{X}$ of indeterminates for a monomial $u \in \mathbb{M}$ and to define for $v \in \mathbb{M}$

$$u \mid_r v \Longleftrightarrow v = u \cdot w,$$

where w belongs to the monoid of power products constructed from the indeterminates in $X(u)$. Besides, Definitions 1 and 3 deal with r-divisors taken from a certain finite monomial set. By this reason, for algorithmic purposes of constructing Gröbner bases, it suffices to define an r-division for an arbitrary finite set of possible monomial divisors.

Involutive divisions [1,2] form an algorithmically interesting class of this sort of restricted divisions. Our concept of involutive division is given by the folowing definition. [3]

Definition 4. (*Involutive division* [1]). We say that an *involutive division* $\mathcal{L}$ is defined on $\mathbb{M}$ if for any nonempty finite monomial set $U \subset \mathbb{M}$ and for any $u \in U$ there defined a subset $M_{\mathcal{L}}(u, U) \subseteq \mathbb{X}$ (possibly empty [4]) of indeterminates whose power products generate submonoid $\mathcal{L}(u, U)$ of $\mathbb{M}$ such that the following holds

1. $v \in U\ \wedge\ u\mathcal{L}(u, U) \cap v\mathcal{L}(v, U) \neq \emptyset \Longrightarrow u \in v\mathcal{L}(v, U)\ \vee\ v \in u\mathcal{L}(u, U)$.
2. $v \in U\ \wedge\ v \in u\mathcal{L}(u, U) \Longrightarrow \mathcal{L}(v, U) \subseteq \mathcal{L}(u, U)$.
3. $u \in V \wedge\ V \subseteq U \Longrightarrow \mathcal{L}(u, U) \subseteq \mathcal{L}(u, V)$.

Indeterminates in $M_{\mathcal{L}}(u, U)$ are called $\mathcal{L}-$ *multiplicative* for u and the remaining indeterminates in $NM_{\mathcal{L}}(u, U) := \mathbb{X} \setminus M_{\mathcal{L}}(u, U)$ are called $\mathcal{L}-$*nonmultiplicative* for u, respectively. If $w \in u\mathcal{L}(u, U)$, then u is called $\mathcal{L}-$*(involutive) divisor* of w.

[3] Another concept [2] also satisfies conditions 1 and 2 for any given monomial set but not necessarily condition 3.

[4] If $M_{\mathcal{L}}(u, U) = \emptyset$, then $\mathcal{L}(u, U) = \{1\}$.

A typical and computationally good [9] representative of involutive division is Janet division.

Definition 5. *Janet division* [1]. Let $U \subset \mathbb{M}$ be a finite set. For each $0 \leq i \leq n$ partition U into groups labeled by non-negative integers $d_0, \ldots, d_i$ [5]

$$[d_0, d_1, \ldots, d_i] := \{u \in U \mid d_0 = 0, d_1 = \deg_1(u), \cdots, d_i = \deg_i(u)\}. \quad (3)$$

Indeterminate x_i is *J(anet)-multiplicative* for $u \in U$ if $u \in [d_0, \ldots, d_{i-1}]$ and $\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_0, \ldots, d_{i-1}]\}$.

Below, in accordance to the notations used in Definition 4, we shall write $M_J(u, U)$ and $NM_J(u, U)$ for the sets of J-multiplicative and J-nonmultiplicative indeterminates for monomial $u \in U$, and write $u \mid_J w$ if u is a $J-$divisor of w.

3 Janet-Like Division

In this section we introduce a non-involutive restricted division which improves algorithmic properties of Janet division. In the following, unless mentioned, the monomial subsets of $\mathbb{M}$ are assumed to be finite and nonempty, and polynomial subsets of $\mathbb{R}$ are also assumed to be finite and without zero polynomials.

Definition 6. (*Nonmultiplicative power*). Let $U \subset \mathbb{M}$ be a monomial set and its elements be partitioned into groups as in (3). For every $u \in U$ and $1 \leq i \leq n$ consider $h_i(u, U) \in \mathbb{N}_{\geq 0}$ given by

$$h_i(u, U) := \max\{\deg_i(v) \mid u, v \in [d_0, \ldots, d_{i-1}]\} - \deg_i(u).$$

If $h_i(u, U) > 0$, then the power $x_i^{k_i}$ where

$$k_i := \min\{\deg_i(v) - \deg_i(u) \mid v, u \in [d_0, \ldots, d_{i-1}],\ \deg_i(v) > \deg_i(u)\}$$

will be called a *nonmultiplicative power* for u.

We shall denote by $NMP(u, U)$ the set of all nonmultiplicative powers for $u \in U$.

Definition 7. (*Janet-like division*). Given a set $U \subset \mathbb{M}$ and $u \in U$, elements of the monoid ideal

$$\mathcal{NM}(u, U) := \{v \in \mathbb{M} \mid \exists w \in NMP(u, U) : w \mid v\} \quad (4)$$

will be called *$\mathcal{J}$-nonmultipliers* for $u \in U$. Elements in $\mathcal{M}(u, U) := \mathbb{M} \backslash \mathcal{NM}(u, U)$ will be correspondingly called *$\mathcal{J}$-multipliers* for u. Element $u \in U$ will be called a *Janet-like divisor or $\mathcal{J}-$divisor* of $w \in \mathbb{M}$ (denotation $u \mid_{\mathcal{J}} w$) if $w = u \cdot v$ with $v \in \mathcal{M}(u, U)$.

Remark 1. From comparison of Definitions 5 and 7 it follows immediately that every nonmultiplicative power is nothing else then the power of $J-$nonmultiplicative indeterminate. The following example illustrates this obvious fact.

Example 1. $U = \{x_1^5, x_1^2x_2^2x_3, x_1^2x_3^2, x_2^4x_3, x_2x_3^2, x_3^5\} \subset \mathbb{K}[x_1, x_2, x_3]$.

[5] Note that $U = [0]$.

Table 1. Comparison of Janet and Janet-like divisions

Element in U	Division		
	Janet		Janet-like
	M_J	NM_J	NMP
x_1^5	x_1, x_2, x_3	$-$	$-$
$x_1^2 x_2^2 x_3$	x_2, x_3	x_1	x_1^3
$x_1^2 x_3^2$	x_3	x_1, x_2	x_1^3, x_2^2
$x_2^4 x_3$	x_2, x_3	x_1	x_1^2
$x_2 x_3^2$	x_3	x_1, x_2	x_1^2, x_2^3
x_3^5	x_3	x_1, x_2	x_1^2, x_2

Proposition 1. *Let $U \subset \mathbb{M}$ be a set, $u \in U$ be its element and $w \in \mathbb{M}$ be a monomial. Then Janet-divisibility of w by u implies its Janet-like divisibility, i.e.*

$$u \mid_J w \Longrightarrow u \mid_{\mathcal{J}} w\,.$$

The converse is generally not true.

Proof. By Definition 5, w/u is a power product of $J-$multiplicative variables for u. Since any element in $NMP(u,U)$ is a power of a $J-$nonmultiplicative variable, w is $\mathcal{J}-$multiplier. On the other side, if $x_i^{k_i} \in NMP(u,U)$ and $k_i > 1$, then, in accordance with Definition 7, $u \mid_{\mathcal{J}} u \cdot x_i^{k_i-1}$ whereas $x_i \in NM_J(u,U)$. □

In the rest of this paper we show that Janet-like division, whereas providing a wider divisibility then Janet division, as the Proposition 1 states, possesses all algorithmic merits of the last division. First, we show that as well as a Janet divisor, a Janet-like divisor is unique.

Proposition 2. *A monomial w cannot have two distinct $\mathcal{J}-$divisors in any monomial set.*

Proof. Suppose there are two $\mathcal{J}-$divisors $u, v \in U$ and $u \neq v$. Let i be the lowest index such that $\deg_i(u) \neq \deg_i(v)$. Without the loss of generality assume that $\deg_i(u) < \deg_i(v)$. Then $u, v \in [d_0, \ldots, d_{i-1}]$ and, in accordance with Definition 6, $x_i^{k_i} \in NMP(u,U)$ where $0 < k_i \leq \deg_i(v) - \deg_i(u)$. Since $v \mid w$, w/u is a multiple of $x_i^{k_i}$, and u cannot $\mathcal{J}-$divide w, a contradiction. □

Definition 8. (*Completeness*). A monomial set U is called $\mathcal{J}-$*complete* if the equality

$$C_{\mathcal{J}}(U) = C(U) \tag{5}$$

holds, where

$$C_{\mathcal{J}}(U) := \{u \cdot v \mid u \in U, v \in \mathcal{M}(u,U)\}\,, \tag{6}$$

$$C(U) := \{u \cdot w \mid u \in U, w \in \mathbb{M}\}\,. \tag{7}$$

Equality (5) means that any element in the monoid ideal (7) generated by elements in the complete set U has a $\mathcal{J}-$divisor in U. If U contains only distinct monomials, then, by Proposition 2, this ideal is partitioned into the disjoint subsets generated by $\mathcal{J}-$multiples of elements in U.

Lemma 1. *Let $u, v \in U$ and $u \mid_{\mathcal{J}} v \cdot p$, $p \in NMP(u, U)$. Then $u \succ_{lex} v$ where $\succ_{lex}$ is the lexicographical monomial order induced by (1).*

Proof. Assume that $p = x_i^{k_i}$ $(1 \leq i \leq n, k_i > 0)$. If $i = 1$, then $\deg_1(u) > \deg_1(v)$. Indeed, if $d_1 := \deg_1(u) = \deg_1(v)$, then $u, v \in [d_0, d_1]$. Since $p \in NMP(v, U)$, by Definition 6, $p \in NMP(u, U)$ what contradicts $\mathcal{J}$-divisibility $v \cdot p$ by u. If $\deg_1(u) < \deg_1(v)$, then again, by Definitions 6 and 7, $x_1^{\deg_1(v)-\deg_1(u)} \notin \mathcal{M}(u, U)$. Thus, for $i = 1$ $u >_{lex} v$.

Let now $i > 1$ and $0 \leq j < i$ will be the minimal such that $\deg_j(u) < \deg_j(v)$. Then $x_j^{d_j} \in NMP(u, U)$ where $0 < d_j \leq \deg_j(v) - \deg_j(u)$. Since $(v \cdot p)/u$ is multiple of such $x_j^{d_j}$, u cannot $\mathcal{J}-$divide $v \cdot p$. Thereby, both u and v belong to the same monomial group $[d_0, \ldots, d_{i-1}]$. Then one can apply the same reasoning as for $i = 1$ to show that $\deg_i(u) > \deg_i(v)$. □

4 Algorithmic Properties

The following theorem gives an algorithmic characterization of completeness for Janet-like division much like that for Janet and other involutive divisions. Thereby, it establishes a property of Janet-like division which we shall call *continuity* by analogy with that for involutive divisions [1].

Theorem 1. *(Continuity). A monomial set U is $\mathcal{J}-$complete iff*

$$\forall u \in U,\ \forall p \in NMP(u, U),\ \exists v \in U\ :\ v \mid_{\mathcal{J}} u \cdot p. \tag{8}$$

Proof. (5) $\Longrightarrow$ (8) is trivial since the equality (5) is equivalent to

$$\forall u \in U,\ \forall t \in \mathbb{M},\ \exists v \in U\ :\ v \mid_{\mathcal{J}} u \cdot t\,.$$

(8) $\Longrightarrow$ (5) Consider $u \cdot t$ with $u \in U$ and $t \in \mathcal{NM}(u, U)$ as defined in (4). Then $\exists q_1 \in NMP(u, U)\ :\ q_1 \mid t$. From (8) it follows that $\exists u_1 \in U\ :\ u_1 \mid_{\mathcal{J}} q_1$. By Lemma 1, $u_1 \succ_{lex} u$. Thus we have $u \cdot t = u_1 \cdot t_1$. If $t_1 \in \mathcal{M}(u_1, U)$ we are done. Otherwise, $\exists q_2 \in NMP(u, U)\ :\ q_2 \mid t_1$. Again we deduce that $u_1 \cdot t_1 = u_2 \cdot t_2$ where $u_2 \mid_{\mathcal{J}} q_2$ and $u_2 \succ_{lex} u_1$. Repeating this reasoning we obtain the chain of elements in U satisfying

$$u \cdot t = u_1 \cdot t_1 = u_2 \cdot t_2 = \cdots$$

and, by Lemma 1, such that

$$u \prec_{lex} u_1 \prec_{lex} u_2 \prec_{lex} \cdots$$

Since U is finite, the last chain is terminated with a $\mathcal{J}-$divisor of $u \cdot t$. □

Show that Janet-like division satisfies also a property which is the straightforward analogue of property 3 in Definition 4.

Proposition 3. *For every $U \subset \mathbb{M}$ and $u \in U$, the set of $\mathcal{J}-$nonmultipliers $\mathcal{NM}(u,U)$ introduced in Definition 7 satisfies the condition*

$$\forall v \in \mathbb{M} \ : \ \mathcal{NM}(u, U \cup \{v\}) \supseteq \mathcal{NM}(u,U). \tag{9}$$

Proof. From Definition 6 it follows that $NMP(u,U) \neq NMP(u,U \cup \{v\})$ only if there is $1 \leq i \leq n$ such that $u, v \in [d_0, \ldots, d_{i-1}]$ and $\deg_i(v) > \deg_i(u)$. Now, if $\deg_i(u) = \max\{\deg_i(w) \mid w \in [d_0, \ldots, d_{i-1}]\}$ we have

$$NMP(u, U \cup \{v\}) = NMP(u,U) \cup \{x_i^{\deg_i(v)-\deg_i(u)}\}\,,$$

and, hence, $\mathcal{NM}(u,U) \subset \mathcal{NM}(u, U \cup \{v\})$.

Next, if $\deg_i(v) < k_i$ where k_i defined as in Definition 6, then

$$NMP(u, U \cup \{v\}) = NMP(u,U) \cup \{x_i^{\deg_i(v)}\} \setminus \{x_i^{k_i}\}.$$

This implies again $\mathcal{NM}(u,U) \subset \mathcal{NM}(u, U \cup \{v\})$.

At last, if $\deg_i(v) \geq k_i$ the enlargement of U with v does not change the set $NMP(u,U)$. □

Definition 9. (*Completion*). For a given set U, a $\mathcal{J}-$complete set $\bar{U}$ will be called $\mathcal{J}-$*completion* of U if $U \subseteq \bar{U}$ and

$$C_{\mathcal{J}}(\bar{U}) = C(U)\,. \tag{10}$$

Definition 10. (*Prolongation*). The product $u \cdot v$ where $u \in U \subset \mathbb{M}$ and $v \in NMP(u,U)$ will be called a *nonmultiplicative prolongation* of u. Similarly, the product $u \cdot v$ with $v \in \mathcal{M}(u,U)$ will be called a *multiplicative prolongation* of u.

Remark 2. Exactly as in the theory of involutive polynomial bases [1], the above defined notion of prolongation is extended to polynomial sets. Given a monomial order $\succ$ and a polynomial set $F \subset \mathbb{R}$, the product $p \cdot v$ is called nonmultiplicative (multiplicative) prolongation of p if it is such for $\mathrm{lm}(p) \in \mathrm{lm}(F)$.

The following theorem extends the property of constructivity of Janet division [1] to Janet-like division.

Theorem 2. *(Constructivity). A nonmultiplicative prolongation $u \cdot t$, $u \in U, t \in NMP(u,U)$ satisfying $u \cdot t \notin C_{\mathcal{J}}(U)$ and*

$$\forall v \in U,\ \forall s \in NMP(v,U) \ \textit{such that}\ v \cdot s \sqsubset u \cdot t \ : \ v \cdot s \in C_{\mathcal{J}}(U) \tag{11}$$

belongs to $\bar{U}$, a $\mathcal{J}-$completion of U.

Proof. Assume for a contradiction that $u \cdot t \notin \bar{U}$. This implies $\exists v \in \bar{U} \ : \ v \mid_{\mathcal{J}} u \cdot t$. From Proposition 3 it follows that $v \notin U$ and $u \cdot t \in \mathcal{M}(v, U \cup \{v\})$. Then $v \sqsubset u \cdot t$ and $\exists u_1 \in U \wedge \exists v_1 \in \mathcal{M}(u_1, U) \ : \ v = u_1 v_1$. Since extension of a monomial set U with $\mathcal{J}-$multiplicative prolongation v of u_1 does not affect the group partition (3) of elements in U, it follows that $u \cdot t = u_1 \cdot w_1$ where $w_1 \in \mathcal{M}(u_1, U)$ and $w_1 \notin \mathcal{M}(u_1, \bar{U})$. We deduce that $\exists t_1 \in NMP(u_1, \bar{U}) \ : \ t_1 \mid w_1$. Completeness of $\bar{U}$ implies $\exists u_2 \in \bar{U} \ : \ u_2 \mid_{\mathcal{J}} u_1 \cdot t_1$. In the obtained equality

$$u \cdot t = u_1 \cdot w_1 = u_2 \cdot w_2$$

$u_2 \succ_{lex} u_1 \succ_{lex} u$, by Lemma 1. Again, $\exists t_2 \in NMP(u_2, \bar{U}) \ : \ t_2 \mid w_2$, and $\exists u_3 \in \bar{U} \ : \ u_3 \mid_{\mathcal{J}} u_2 \cdot t_2$. By repetition of this reasoning, we obtain the infinite chain of elements in $\bar{U}$ satisfying

$$u \prec_{lex} u_1 \prec_{lex} u_2 \prec_{lex} u_3 \prec_{lex} \cdots ,$$

a contradiction. □

The next important property of Janet division - Noetherianity [1,9] is also easily extended to Janet-like division.

Theorem 3. *(Noetherianity). Every set $U \in \mathbb{M}$ admits a $\mathcal{J}-$completion.*

Proof. Follows trivially from the observation that every Janet complete set is also a Janet-like complete, and from Noetherianity of Janet division [1]. The observation is a consequence of Definitions 5, 6 and Janet conditions of completeness. Indeed, for a Janet complete set all the $\mathcal{J}-$nonmultiplicative power products are just $J-$nonmultiplicative indeterminates. An explicit completion of a set U is as follows

$$\bar{U} := \{u \cdot x_1^{i_1} \cdots x_n^{i_n} \mid u \in U, \, 0 \leq i_j \leq h_j(u, U), \, 1 \leq j \leq n\} \, , \tag{12}$$

where $h_j(u, U)$ are as in Definition 6. Set $\bar{U}$ is both $\mathcal{J}$- and $J-$complete since $\forall v \in \bar{U} \ : \ h_i(v, \bar{U}) \leq 1$, and if $h_i(v, \bar{U}) = 1$, then $\exists w \in \bar{U} \ : \ w = v \cdot x_i$. □

Now we are going to show that among different $\mathcal{J}$-complete sets generating the same monomial ideal in $\mathbb{R}$ there is minimal such set.

Proposition 4. *Let $U, V \subset \mathbb{M}$ be $\mathcal{J}$-complete sets such that* $\mathrm{Id}(U) = \mathrm{Id}(V)$. *Then the set $W := U \cap V$ is also $\mathcal{J}$-complete.*

Proof. Since both sets U and V generate the same monomial ideal, W also generates this ideal and U, V are $\mathcal{J}-$completions of W. Assume that W is not $\mathcal{J}$-complete. This implies $\exists u \in W, t \in NMP(u, W) \ : \ u \cdot t \notin C_{\mathcal{J}}(W)$. Choose such a pair of u, t without proper divisors among all other nonmultiplicative prolongations that are not in $C_{\mathcal{J}}(W)$. Then Theorem 2 asserts that $u \cdot t$ must belong to any $\mathcal{J}$-completion of W. Thus, $u \cdot t \in U$ and $u \cdot t \in V$, a contradiction. □

As an immediate consequence of Proposition 4 we have the following result.

Corollary 1. *Given a monomial set U, there exists a minimal $\mathcal{J}$-completion of U, that is, such that it is a subset of any other $\mathcal{J}$-completion of U.*

The next definition is used in [12] for defining Janet-like bases and for proving correctness of the underlying algorithm.

Definition 11. *(Compactness).* A monomial set U will be called *$\mathcal{J}-$compact* if $U \subseteq V$ where V is a minimal $\mathcal{J}-$completion of the reduced Gröbner basis of $\mathrm{Id}(U)$.

5 Conclusion

In this paper we give an explicit receipt of improvement of Janet division. Though the improvement breaks the properties of Janet division as involutive one, the new division called Janet-like inherits all the attractive features of Janet division. At the same time the new division decreases Gröbner redundancy of the output bases.

Recently we analyzed [9] some issues of practical superiority of our Janet division algorithms over the Buchberger algorithm. All those issues are apparently preserved by Janet-like division too. In particular, the new division also admits a tree structure providing a very fast search of Janet-like divisor. Moreover, trees for the new division are more compact than Janet trees.

Our Janet-like division algorithm in its simplest form presented in [12] together with some examples demonstrating its superiority over Janet division algorithms.

We are planning to experiment on Janet-like division to find heuristically best strategies for selection of nonmultiplicative prolongations. For the Buchberger algorithm such a strategy is well-known [13]. For Janet division we already detected some good strategies mentioned in [9]. However, a strategy being good for Janet division may be not always that good for Janet-like division, since the latter provides generally another sequence of intermediate reduction than the former. This important aspect needs further experimental study.

We see also another, pure theoretical, direction of research. Namely, to formulate general properties of a restricted monomial division providing its algorithmic applicability to construction of Gröbner bases. We expect that axioms for involutive division given in Definition 4 or in [2] can be properly modified to characterize such good, though noninvolutive, divisions as Janet-like.

Acknowledgements

The first author thanks A.S.Semenov for useful remarks relating to the proof of Theorem 2. The research presented in this paper was partially supported by the grants 04-01-00784 and 05-02-17645 from the Russian Foundation for Basic Research and the grant 2339.2003.2 from the Russian Ministry of Science and Education.

References

1. Gerdt, V.P. and Blinkov,Yu.A.: Involutive Bases of Polynomial Ideals. *Mathematics and Computers in Simulation* 45 (1998) 519–542, http://arXiv.org/math.AC/9912027; *Minimal Involutive Bases.* Ibid., 543–560, http://arXiv.org/math.AC/9912029.
2. Apel, J.: Theory of Involutive Divisions and an Application to Hilbert Function Computations. *Journal of Symbolic Computation* 25 (1998) 683–704.
3. Janet, M.: *Leçons sur les Systèmes d'Equations aux Dérivées Partielles*, Cahiers Scientifiques, IV, Gauthier-Villars, Paris (1929).
4. Gerdt, V.P., Blinkov,Yu.A. and Yanovich, D.A.: Construction of Janet Bases. I. Monomial Bases. In: *Computer Algebra in Scientific Computing / CASC'01*, V.G.Ganzha, E.W.Mayr and E.V.Vorozhtsov (eds.), Springer, Berlin (2001) 233–247; II. Polynomial bases, ibid., 249–263.
5. Berth, M. and Gerdt, V. Computation of Involutive Bases with Mathematica. In: *Proceedings of the Third International Workshop on Mathematica System in Teaching and Research*, Institute of Mathematics & Physics, University of Podlasie (2001) 29–34.
6. Hausdorf, M. and Seiler, W.M.: Involutive Bases in MuPAD - Part I: Involutive Divisions. *mathPAD* 11 (2002) 51–56.
7. Blinkov, Yu.A., C.F.Cid, C.F., Gerdt, V.P., Plesken, W. and Robertz, D.: The Maple Package "Janet": I.Polynomial Systems. In: *Computer Algebra in Scientific Computing / CASC 2003*, V.G.Ganzha, E.W.Mayr and E.V.Vorozhtsov (eds.). Institute of Informatics, Technical University of Munich, Garching (2003)31–40; II. Linear Partial Differential Equations, ibid., 41–54.
8. Hemmecke, R: *Involutive Bases for Polynomial Ideals.* PhD Thesis, RISC Linz, 2003.
9. Gerdt, V.P.: Involutive Algorithms for Computing Gröbner Bases. IIn "Computational Commutative and Non-Commutative algebraic geometry", S.Cojocaru, G.Pfister and V.Ufnarovski (Eds.), NATO Science Series, IOS Press, 2005, pp.199–225. http://arXiv.org/math.AC/0501111.
10. Buchberger, B.: Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, In: *Recent Trends in Multidimensional System Theory*, N.K. Bose (ed.), Reidel, Dordrecht (1985) 184–232.
11. Gerdt, V.P. and Blinkov,Yu.A.: Janet Bases of Toric Ideals. In *Proceedings of the 8th Rhine Workshop on Computer Algebra*, H.Kredel and W.K.Seiler (Eds.), University of Mannheim (2002) 125-135. http://arXiv.org/math.AC/0501180.
12. Gerdt, V.P. and Blinkov,Yu.A.: Janet-like Gröbner Bases. Submitted to CASC'05 (Kalamata, Greece, September 12 - 16, 2005).
13. Giovinni, A., Mora, T., Niesi, G., Robbiano, L. and Traverso, C.: One sugar cube, please, or selection strategies in the Buchberger algorithm. In: *Proceedings of ISSAC'91*, ACM Press, New York (1991) 49–54.