Janet-Like Gröbner Bases

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. We define a new type of Gröbner bases called Janet-like, since their properties are similar to those for Janet bases. In particular, Janet-like bases also admit an explicit formula for the Hilbert function of polynomial ideals. Cardinality of a Janet-like basis never exceeds that of a Janet basis, but in many cases it is substantially less. Especially, Janet-like bases are much more compact than their Janet counterparts when reduced Gröbner bases have "sparce" leading monomials sets, e.g., for toric ideals. We present an algorithm for constructing Janet-like bases that is a slight modification of our Janet division algorithm. The former algorithm, by the reason of checking not more but often less number of nonmultiplicative prolongations, is more efficient than the latter one.

1 Introduction

In [1] we introduced the concept of noninvolutive monomial division called Janet-like due to its similarity to Janet division studied in [2]. Having possessed all merits of the latter division, the former division is algorithmically better for constructing Gröbner bases. This is because every Janet divisor is also a Janet-like divisor, and the converse may not hold.

We refer to paper [1] for the basic notations and definitions including those related to Janet-like division and its properties. In the present paper we define Janet-like bases and show that their Gröbner redundancy never exceeds that of Janet bases, but in some cases is considerably less. This effect is illustrated by a number of examples, including toric ideals, which are "unconvenient" for Janet division. We present also the underlying algorithm in its simplest form that is a straightforward modification of our involutive algorithm [3].

2 Janet-Like Bases

In this section we introduce Janet-like bases for polynomial ideals in accordance with general Definition 3 of $r-$bases in paper [1] specified for Janet-like division. However, unlike our more general definition of involutive bases [2], we restrict ourselves to consideration of minimal bases only.

First, we define the corresponding Janet-like reduction and normal form.

V.G. Ganzha, E.W. Mayr, and E.V. Vorozhtsov (Eds.): CASC 2005, LNCS 3718, pp. 184–195, 2005.

Definition 1. ($\mathcal{J}-$*reduction*). Given a monomial order $\succ$, a finite set $F \in \mathbb{R} \setminus \{0\}$ of polynomials and a polynomial $p \in \mathbb{R} \setminus \{0\}$, we shall say that:

(i). $p \in \mathbb{R}$ is $\mathcal{J}-$*reducible modulo* $f \in F$ if p has a term $t = a\,u$ ($a \in \mathbb{K}, u \in \mathbb{M}, a \neq 0$) whose monomial u is $\mathcal{J}$-multiple[1] of $\mathrm{lm}(f)$. It yields the $\mathcal{J}-$*reduction* $p \to g := p - (a/lc(f))\, f \cdot v$ where v is $\mathcal{J}-$multiplier for u ($v \in \mathcal{M}(\mathrm{lm}(f), \mathrm{lm}(F))$).

(ii). p is $\mathcal{J}-$*reducible modulo* F if there is $f \in F$ such that p is $\mathcal{J}-$reducible modulo f.

(iii). p is *in* $\mathcal{J}-$*normal form modulo* F (denotation $p = NF_{\mathcal{J}}(p, F)$) if p is not $\mathcal{J}-$reducible modulo F.

It follows that the normal form $NF_{\mathcal{J}}(g, F)$ ($g \in \mathbb{R}$) can be presented as the finite sum

$$h := NF_{\mathcal{J}}(g, F) = g - \sum_{i=1}^{\mathrm{card}(F)} f_i \sum_j \alpha_{ij} m_{ij}\,, \tag{1}$$

where $\forall i, j \;:\; \alpha_{ij} \in \mathbb{K}$, $m_{ij} \in \mathcal{M}(\mathrm{lm}(f_i), \mathrm{lm}(F))$, $\mathrm{lm}(f_i)m_{ij} \preceq \mathrm{lm}(p)$, $m_{ij} \neq m_{ik}$, $(j \neq k)$, and polynomial h is $\mathcal{J}-$irreducible modulo F.

Definition 2. ($\mathcal{J}-$*autoreduction*). A polynomial set F will be called $\mathcal{J}-$*autoreduced* if

1. The leading monomial set $\mathrm{lm}(F)$ contains distinct elements.
2. Every $f \in F$ has no (tail) terms $t = a\,u$ ($0 \neq a \in \mathbb{K}, u \in \mathbb{M}, u \neq lm(f)$) $\mathcal{J}-$reducible modulo F.

Now we can define Janet-like bases.

Definition 3. (*Janet-like basis*). Let $\mathcal{I} \subset \mathbb{R}$ be a nonzero ideal and $\succ$ be a monomial order. Then a finite $\mathcal{J}$-autoreduced subset $G \subset \mathbb{R}$ such that $\mathcal{I} = Id(G)$ is called *Janet-like basis or* $\mathcal{J}-$*basis of* $\mathcal{I}$ if

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

and set $\mathrm{lm}(G)$ is $\mathcal{J}-$compact in accordance with Definition 11 in [1].

Theorem 1. *(Existence). A Janet-like basis exists for any nonzero ideal* $\mathcal{I} \subseteq \mathbb{R}$ *and for any admissible monomial order.*

Proof. Let G be a reduced Gröbner basis of $\mathcal{I}$. Let $U := \mathrm{lm}(G)$ be the leading monomial set of G. By Corollary 1 in [1], there exists a minimal $\mathcal{J}-$ completion $\bar{U} \supseteq U$ of U.

If $\bar{U} = U$, then G is also a Janet-like basis. First, it is $\mathcal{J}-$autoreduced, since it is conventionally autoreduced. Second, in accordance to conditions (2) and (10) of paper [1], $\mathrm{lm}(f) \in C_{\mathcal{J}}(U)$ for all $f \in \mathcal{I}$.

[1] As noted in Remark 2 of paper [1], $\mathcal{J}-$division for F is defined in terms of the monomial set $\mathrm{lm}(F)$.

Otherwise, consider $V := \bar{U} \setminus U$. For every $v \in V$ there is $u \in U$ such that $v = u \cdot w$. Note, that w belongs to the monoid ideal $\mathcal{NM}(u, U)$ defined in (4) of paper [1]. For every such v, u, w enlarge G with $g \cdot w$ ($g \in G, \mathrm{lm}(g) = u$). Denote the enlarged set by G_1. Now, if a tail term in G_1 is $\mathcal{J}$-reducible modulo G_1, then perform its $\mathcal{J}$-reduction as described in part (i) of Definition 1. This reduction process obviously terminates in a finite number of step, and we obtain $\mathcal{J}$-reduced set $\bar{G}$ such that $\mathrm{lm}(\bar{G}) = \mathrm{lm}(G_1) = \bar{U}$. Since, by the construction, $\{\mathrm{lm}(f) \mid f \in \mathcal{I}\} = C(U) = C_{\mathcal{J}}(\bar{U})$, the obtained set $\bar{G}$ is a Janet-like basis. □

From the above proof we immediately have the next result just as in theories of Gröbner bases [4] and involutive bases [2,3,5].

Corollary 1. *Given an ideal $\mathcal{I}$ and a monomial order, the following is equivalent:*

(i). G is a Janet-like basis of $\mathcal{I}$.
(ii). G is $\mathcal{J}-$autoreduced, the set $\mathrm{lm}(G)$ is $\mathcal{J}-$compact and

$$\forall f \in \mathcal{I} : NF_{\mathcal{J}}(f, G) = 0\,. \tag{3}$$

Remark 1. The above proof contains, in fact, one of possible algorithms for constructing Janet-like bases via reduced Gröbner bases. This algorithm, however, needs an algorithm for construction of the reduced Gröbner basis. Below we present another algorithm based on the characterization 3 which computes also reduced Gröbner bases as subsets of Janet-like bases.

As any $r-$basis, a Janet-like basis is a Gröbner basis since $\mathcal{J}$-reducibility implies the conventional reducibility (i.e. reducibility with respect to the conventional division). But the converse is not true in general. By this reason, Janet-like bases, similarly to involutive bases, are generally redundant as the Gröbner one.

The following corollary establishes interrelation between (minimal) Janet, Janet-like and reduced Gröbner bases.

Corollary 2. *Given a minimal Janet basis (abreviation JB), a Janet-like (abreviation JLB) and a reduced Gröbner basis (abreviation GB) of the same ideal, their cardinalities satisfy inequality*

$$\mathrm{card}(GB) \leq \mathrm{card}(JLB) \leq card(JB)\,. \tag{4}$$

Moreover, if all these bases are monic than

$$GB \subseteq JLB \subseteq JB\,. \tag{5}$$

The strict inequalities in (4) and, repectively, strict inclusions in (5) also take place for some ideals and orders.

Proof. If one considers the leading monomial sets of the three bases, then inequality (4) follows from Proposition 1 in [1] and from already shown fact that both Janet and Janet-like bases are Gröbner bases. The proof of inclusion $GB \subseteq JLB$ is contained in the proof of Theorem 1. As to inclusion $JLB \subseteq JB$, it is an easy consequence the same Proposition 1 and of the fact that Janet division satisfies [2] to property 3 in Definition 4 of paper [1]. The last implies that $\mathcal{J}-$autoreduced elements of a Janet-like basis cannot become Janet reducible after extension (completion) of the Janet-like basis to the Janet basis. At last, we illustrate below the strict inequalities and inclusions by some explicit examples. □

Example 1. Consider ideal $\mathrm{Id}(\{x^6y^3-y, x^3y^4-y\}) \in \mathbb{Q}[x,y]$. Its lexicographical $(x \succ y)$ bases are

$$JLB = GB = \{x^3y-y^2, y^5-y\}\,, \quad JB = \{x^3y-y^2, xy^5-xy, x^2y^5-x^2y, y^5-y\}\,.$$

3 Algorithm

In this section we present the simplest version of an algorithm for constructing Janet-like polynomial bases and illustrate its work by Example 1. The algorithm is a straightforward modification of its involutive counterpart [3] and based on the below theorem that gives an algorithmic characterization of Janet-like bases.

To prove the theorem we need the following lemma.

Lemma 1. *For any $\mathcal{J}-$autoreduced polynomial set F, the $\mathcal{J}-$normal form satisfies the linearity condition*

$$\forall p_1, p_2 \in \mathbb{R} \setminus \{0\} \,:\, NF_{\mathcal{J}}(p_1+p_2, F) = NF_{\mathcal{J}}(p_1, F) + NF_{\mathcal{J}}(p_2, F)\,, \quad (6)$$

Proof. First, we claim that $NF_{\mathcal{J}}(p, F) = 0$ iff p admits representation as a finite sum of the form

$$p = \sum_{i=1}^{\mathrm{card}(F)} f_i \sum_j \beta_{ij} m_{ij} f_j\,, \quad (7)$$

where $\beta_{ij} \in \mathbb{K}$, $m_{ij} \in \mathcal{M}(\mathrm{lm}(f), \mathrm{lm}(F))$, $m_{ij} \neq m_{ik}$, $(j \neq k)$. If $NF_{\mathcal{J}}(p, F) = 0$, then applying a sequence of elementary $\mathcal{J}-$reduction given in Definition 1, which is obviously terminates by admissibility of order $\succ$, we obtain representation (7) for p. Note, that Proposition 2 in [1] asserts uniqueness of every elementary reduction. Apparently, this implies uniqueness of the representation[2].

Let now $p_3 := p_1 + p_2$ and $h_1 := NF_{\mathcal{J}}(p_1, F)$, $h_2 := NF_{\mathcal{J}}(p_3, F)$, $h_3 := NF_{\mathcal{J}}(p_3, F)$. Then, by Definition 1, $NF_{\mathcal{J}}(h_3 - h_1 - h_2, F) = h_3 - h_1 - h_2$ since h_1, h_2, h_3 have no terms whose monomials belong to $C_{\mathcal{J}}(\mathrm{lm}(F))$. On the other hand, from (1) it follows that $p := h_3 - h_1 - h_2$ admits representation (7). Thus, $NF_{\mathcal{J}}(h_3 - h_1 - h_2, F) = 0$. □

[2] It implies also uniqueness of (1) exactly as in the case of involutive divisions [2].

Algorithm: Janet-like Basis $(F, \prec)$

Input: $F \in \mathbb{R} \setminus \{0\}$, a finite set; $\prec$, an order
Output: G, a Janet-like basis of $\mathrm{Id}(F)$

choose $f \in F$ with the lowest $\mathrm{lm}(f)$ w.r.t. $\succ$
$G := \{f\}$
$Q := F \setminus G$
do
  $h := 0$
  while $Q \neq \emptyset$ and $h = 0$ **do**
    choose $p \in Q$ with the lowest $\mathrm{lm}(p)$ w.r.t. $\succ$
    $Q := Q \setminus \{p\}$
    $h :=$ **NormalForm**$(p, G, \prec)$
  od
  if $h \neq 0$ **then**
    for all $\{g \in G \mid \mathrm{lm}(h) \sqsubset \mathrm{lm}(g)\}$ **do**
      $Q := Q \cup \{g\}$; $G := G \setminus \{g\}$
    od
    $G := G \cup \{h\}$
    $Q := Q \cup \{\, g \cdot t \mid g \in G,\, t \in NMP(\mathrm{lm}(g), \mathrm{lm}(G))\,\}$
  fi
od while $Q \neq \emptyset$
return G

Theorem 2. *(Algorithmic characterization). An $\mathcal{J}-$autoreduced set $F \in \mathbb{R}$ satisfies (3) for $\mathcal{I} = Id(F)$ iff*

$$\forall f \in F \;\; \forall p \in NMP(\mathrm{lm}(f), \mathrm{lm}(F)) : \; NF_{\mathcal{J}}(f \cdot p, F) = 0\,. \tag{8}$$

Proof. Implication (3) $\Longrightarrow$ (8) is obvious.

(8) $\Longrightarrow$ (3) By Lemma 1, it suffices to show that

$$\forall u \in \mathbb{M},\, \forall f \in F \; : \; NF_{\mathcal{J}}(f \cdot u, F) = 0\,. \tag{9}$$

Assume, without the loss of generality, that all polynomials in F are monic. Then conditions (9) together with Theorem 1 in [1] imply $\mathcal{J}-$completeness of $\mathrm{lm}(F)$. Thus, $f \cdot u$ can be rewritten as

$$f \cdot u = g \cdot v + \sum_{i=1}^{\mathrm{card}(F)} f_i \sum_j v_{ij}\,, \tag{10}$$

where $g \in F$ is uniquely defined by f and u, $v \in \mathcal{M}(\mathrm{lm}(g), \mathrm{lm}(F))$, $v_{ij} \in \mathbb{M}$, and $\forall i, j \; : \; lm(f)u = lm(g)v \succ lm(f_i)v_{ij}$. Similarly, we can further rewrite every $f_i \cdot v_{ij}$ in (10) until we obtain for the right-hand side of (10) representation (7). Admissibility of $\succ$ provides termination of this rewriting procedure. □

The above algorithm is an adaptation of our general involutive division algorithm [3] to Janet-like division. Its input consists of a polynomial set F and a monomial order $\succ$. To output a minimal and $\mathcal{J}-$autoreduced set, in accordance to Definition 2, the intermediate polynomial data are separated into subsets G and Q.

Set G contains a part of the intermediate basis. It is initialized at step 2 as a set with the single element $f \in F$ selected at step 1. The rest of the input basis is contained in the set Q initialized at step 3 as $F \setminus \{f\}$.

When the outer **do-while** loop 4-18 is executed, set Q can be enlarged with some elements of G at step 13 and with nonmultiplicative prolongations of polynomials in G. The algorithm terminates when Q becomes empty during execution of the inner **while** loop that signals that all conditions (8) satisfied, and the last $\mathcal{J}-$normal form h computed at step 9, if nonzero, does not have proper divisors of $\mathrm{lm}(h)$ in $\mathrm{lm}(G)$. This condition is verified at step 12.

The choice made at steps 1 and 7 and execution of the **for** loop 12-13 provide correctness of the algorithm. To show this and to show also the algorithm termination, first, consider subalgorithm **Normal Form**. It is invoked in line 9 of the main algorithm and computes $\mathcal{J}-$normal form in the full correspondence with Definition 1 and formula (1). Its termination is an obvious consequence of that for the conventional reductions [4].

Algorithm: Normal Form$(p, G, \prec)$

Input: $p \in \mathbb{R} \setminus \{0\}$, a polynomial; $G \subset \mathbb{R} \setminus \{0\}$, a finite set; $\prec$, an order
Output: $h = NF_{\mathcal{J}}(p, G)$, the $\mathcal{J}-$normal form of p modulo G
1: $h := p$
2: **while** $h \neq 0$ **and** h has a term t $\mathcal{J}-$reducible modulo G **do**
3: **take** $g \in G$ such that $\mathrm{lm}(g) \mid_{\mathcal{J}} t$
4: $h := h - g \cdot t / \mathrm{lt}(g)$
5: **od**
6: **return** h

Show now *termination* of algorithm **Janet-like Basis**. By the choice done at steps 1 and 7 and by displacement of elements from G to Q at step 13, the elements in $\mathrm{lm}(G)$ occurring right before execution of step 15 have no proper divisors in $\mathrm{lm}(Q)$. Thereby, when the leading monomial $\mathrm{lm}(p)$ of the nonmultiplicative prolongation $g \cdot t \in Q$ with $(g \in G, t \in NMP(\mathrm{lm}(g), \mathrm{lm}(G))$ chosen at step 7 has no $\mathcal{J}-$divisor in $\mathrm{lm}(G)$, the constructivity property (11) in [1] implies that $\mathrm{lm}(p) = \mathrm{lm}(h)$ belongs to any completion of $\mathrm{lm}(G)$. Noetherianity ascertained by Theorem 3 of paper [1] guarantees termination of this completion process.

There are finitely many cases when an element of the input polynomial set F is selected from Q at step 7. Besides, there can only be a finitely many cases when a $\mathcal{J}-$head reducible polynomial p taken from Q has $0 \neq h = NF_{\mathcal{J}}(p, G)$ computed at step 9. This is because in every such case $\mathrm{lm}(h) \notin C(\mathrm{lm}(G))$.

Indeed, assume that there are $g \in G$ and $v \in \mathcal{NM}(\mathrm{lm}(g), \mathrm{lm}(G))$ satisfying $\mathrm{lm}(g) \cdot v = lm(h)$. In that case all nonmultiplicative prolongations of the form $g \cdot t$ with $t \in NMP(\mathrm{lm}(g), \mathrm{lm}(G))$, $t \mid v$, $\mathrm{lm}(g) \cdot t \notin C_{\mathcal{J}}(\mathrm{lm}(G))$ must be added to Q at step 16 of a previous run of the main loop. But then, since $\mathrm{lm}(h) \prec \mathrm{lm}(p)$, all these prolongations must be selected at step 7 and further processed earlier than p. As a result, the leading monomials of these prolongations must belong to $C_{\mathcal{J}}(\mathrm{lm}(G))$ when p is under processing. However, the same arguments as we used in the proof of Theorem 1 in [1], bring us to a contradiction with the assumption made.

To prove *correctness* of algorithm **Janet-like Basis** it suffices to show that the following is a **do-while** loop invariant:

1. $\mathrm{lm}(G)$ is $\mathcal{J}-$compact,
2. The tail monomials in G are not in $C_{\mathcal{J}}(\mathrm{lm}(G))$.

G trivially satisfies both conditions at the initialization step 2. Suppose that this is true after execution of the **while** loop 6-10, and let $G_1 := G \cup \{h\}$ be a set obtained at step 15.

If $\mathrm{lm}(p) = \mathrm{lm}(h)$, as we already seen, $\mathrm{lm}(G_1)$ is compact. Furthermore, by property (9) in [1], the elements in G remain $\mathcal{J}-$reduced after enlargement of G with h. As to the last polynomial, it is in the normal form modulo G, by its construction at step 9.

Consider now the case when $h \neq 0$ and $\mathrm{lm}(p) \succ \mathrm{lm}(h)$. Let G_0 be the value of the intermediate set G right after execution of the **while** loop 6-10, and G_1 be the set obtained at step 15.

Assume that $\mathrm{lm}(G_1)$ is not compact. Then G_1 has a proper subset $G_2 \subset G_1$ with compact $\mathrm{lm}(G_2)$. Then, for any $f \in G_1$ there exists $g \in G_2$ such that $\mathrm{lm}(g) \mid_{\mathcal{J}} \mathrm{lm}(f)$ with respect to the set G_2. At all that $g \neq h$ in accordance to the displacement condition in line 12. Since $\mathrm{Id}(\mathrm{lm}(G_2) = \mathrm{Id}(\mathrm{lm}(G_1))$, polynomial f might only had been added to G as a result of processing a head irreducible nonmultiplicative prolongation of a polynomial $s \in G_0$ which has been displaced at step 13. In this case, however, polynomial f must be also displaced to Q since $\mathrm{lm}(h) \mid \mathrm{lm}(s) \mid \mathrm{lm}(f)$. The obtained contradiction shows compactness of $\mathrm{lm}(G_1)$.

Similarly, if a tail monomial $u \in \mathbb{M}$ of a polynomial $g \in G_1$ became $\mathcal{J}-$reducible modulo $\mathrm{lm}(G_1)$, then it could happen only if u were a nonmultiplicative prolongation $u = \mathrm{lm}(f) \cdot t \prec \mathrm{lm}(g)$ where polynomial f has been moved from G to Q. But in such a case, by the selection strategy of steps 1 and 7, the prolongation $f \cdot t$ must be processed earlier than the nonmultiplicative prolongation of the element in Q whose processing created g. Then, processing of g would lead to $\mathcal{J}-$reduction of u. Thus, $\mathcal{J}-$reducible tail monomials cannot occur in G_1. As to the polynomial h itself, the impossibility of its tail $\mathcal{J}-$reduction after the displacement follows also from the fact that $\mathrm{lm}(h)$ cannot divide its tail monomials.

As an illustration to the internal processing in algorithm **Janet-like Basis**, Table 1 shows intermediate polynomial data for Example 1. The second column of the table contains elements of set G. Their $\mathcal{J}-$nonmultiplicative powers NMP are shown in the third column. The set Q is given in the fourth column. Rows

of the table contain these values obtained at the initialization and after every interation of the **do-while** loop. In this case at steps 1 and 7 we selected the lexicographically smallest elements.

Table 1. Intermediate basis elements for Example 1

Steps of algorithm	Sets G and Q		
	elements in G	NMP	Q
initialization	$x^3y^4 - y$	–	$\{x^6y^3 - y\}$
iteration	$x^6y^3 - y$ $x^3y^4 - y$	– x^3	$\{x^6y^4 - x^3y\}$
	$x^3y - y^2$	–	$\{x^3y^4 - y, x^6y^3 - y\}$
	$x^3y - y^2$ $y^5 - y$	– x^3	$\{x^3y^5 - x^3y, x^6y^3 - y\}$
	$x^3y - y^2$ $y^5 - y$	– x^3	$\{\ \}$

In spite of often redundancy of Janet-like bases as Gröbner ones, as well as in the case of involutive bases [5,6], just this redundancy provides more accessibility to information on polynomial ideals and modules. In particular, Janet-like bases also give explicit formulae for the Hilbert function (cf. [5]) and Hilbert polynomial (cf. [3]) of a polynomial ideal $\mathcal{I}$ in terms of binomial coefficients. If G is a $\mathcal{J}-$ basis of $\mathcal{I}$, then the (affine) Hilbert function $HF_{\mathcal{I}}(s)$ and the Hilbert polynomial $HP_{\mathcal{I}}(s)$ are

$$HF_{\mathcal{I}}(s) = \binom{n+s}{s} - \sum_{i=0}^{s} \sum_{u \in \mathrm{lm}(G)} \sum_{i_1=0}^{d_1-1} \cdots \sum_{i_k=0}^{d_k-1} \binom{i - \sum_j i_j - deg(u) + \mu(u) - 1}{\mu(u) - 1},$$

$$HP_{\mathcal{I}}(s) = \binom{n+s}{s} - \sum_{u \in \mathrm{lm}(G)} \sum_{i_1=0}^{d_1-1} \cdots \sum_{i_k=0}^{d_k-1} \binom{s - \sum_j i_j - deg(u) + \mu(u)}{\mu(u)}.$$

Here, if $NMP(u, \mathrm{lm}(G)) \neq \emptyset$, then $NMP(u, \mathrm{lm}(G)) := \{x_1^{d_1}, \ldots, x_k^{d_k}\}$ with $d_j \neq 0$ $(1 \leq j \leq k)$ and $\mu(u) := n - k$. Otherwise, $k := 1, d_1 := 0, \mu(u) := n$. The first term in the right hand sides of these formulae is the total number of monomials in $\mathbb{M}$ of degree $\leq s$. The sum in the expression for $HF_{\mathcal{I}}(s)$ counts the number of monomials of degree $\leq s$ in the set $C_{\mathcal{J}}(\mathrm{lm}(G))$ defined in (6) of paper [1]. In accordance to the completeness condition (5) in [1], this number coincides with the number of such monomials in the monoid ideal $C(\mathrm{lm}(G))$ as defined in (7) of paper [1].

4 Illustrative Examples

In this section we consider four more nontrivial examples than small Example 1. Our goal is to compare their Janet-like bases with minimal involutive Janet bases

and reduced Gröbner bases. We present these examples in the increasing order with respect to the cardinalities of Janet bases. Two of examples generating toric ideals we took from [7] and [8] and already used in [9] to show limitations in applicability of Janet bases. In the last paper we also shortly noted the approach described in the present paper. One more toric ideal was taken from [10] where it was presented already in the Gröbner basis form. One of the examples [11] is not toric ideal, but also demonstrates deficiency in application of Janet bases to certain problems.

The below examples have compact input and comparatively compact (reduced) Gröbner bases whereas their Janet bases are much larger. For all the examples we used the degree-reverse-lexicographical monomial order induced by the explicitly indicated order on the variables.

Computations were performed with our C++ code implementing Janet division algorithm [3]. We extended the package with our first implementation of Janet-like division. The actual algorithm that has been implemented is an improved version of the above algorithm **Janet-like Basis**. The improvement is similar to that described in [3] for involutive division.

The reduced Gröbner bases given explicitly whereas Janet and Janet-like bases given only for the first rather small example. In addition, for the listed examples we computed their Hilbert polynomials via Janet-like bases (see Sect.5).

Example 2. (*Toric ideal I*) [7] $\{ x^7 - y^2 z, x^4 w - y^3, x^3 y - zw \}$ $(x \succ y \succ z \succ w)$.

Gröbner basis: $\{ x^7 - y^2 z, x^4 w - y^3, x^3 y - zw, y^4 - xzw^2 \}$.

Janet-like basis: $\{ x^7 - y^2 z, x^4 y - xzw, x^4 w - y^3, x^3 y - zw, y^4 - xzw^2 \}$.

Janet basis: $\{ x^7 - y^2 z, x^6 y - x^3 zw, x^6 w - x^2 y^3, x^5 y - x^2 zw, x^2 y^4 - x^3 zw^2, x^5 w - xy^3, x^4 y - xzw, x^2 zw^2 - xy^4, x^4 w - y^3, x^3 y - zw, y^4 - xzw^2 \}$.

Hilbert Polynomial : $\dfrac{39}{6}\, s^2 - \dfrac{21}{2}\, s + 5$.

Example 3. (*Polynomial ideal*) [11] $(w \succ x \succ y \succ z)$

$$\{ z^{20} + z^{10} - x^2, z^{30} + z^{10} - x\, y^3, w^{40} x^4 - y^6 \}.$$

Gröbner basis:

$\{ 16w^{40}z^{10} - 16w^{40}x^2 + y^{18} - x^{12} + 9x^9y^3 - 24y^{12} - 33x^{10} + 150x^7y^3 + 8z^{10}$
$-219x^8 + 627x^5y^3 - 470 * x^6 + 690x^3y^3 + 16y^6 - 502x^4 + 188xy^3 - 196x^2,$
$16w^{40}y^9 - 16w^{40}x^3 - y^{27} + 32y^{21} + x^16y^3 - 12x^17 + 98x^{14}y^3 - 374x^{15} +$
$1875x^{12}y^3 - 160y^{15} - 3778x^{13} + 13743x^{10}y^3 - 17179x^{11} + 45923x^8y^3$
$-41148x^9 + 74362x^6y^3 + 120y^9 - 57702x^7 + 60452x^4y^3 - 1760xy^6 - 45324x^5$
$+18416x^2y^3 - 16728x^3,\ w^{40}x^4 - y^6,\ 8w^{40}xy^3 - 8w^{40}x^2 + y^{18} - x^{12} + 9x^9y^3$
$-22y^{12} - 33x^{10} + 150x^7y^3 + 8xy^9 - 221x^8 + 631x^5y^3 - 472x^6 + 688x^3y^3 +$
$8y^6 - 506x^4 + 192xy^3 - 192x^2,\ z^{20} + z^{10} - x^2,\ xy^{12} - x^9 + 6x^6y^3 + 2y^9$
$-13x^7 + 41x^4y^3 - 8xy^6 - 24x^5 + 28x^2y^3 - 22x^3,\ 2y^3z^{10} + 2xz^{10} - xy^6 + x^5$
$-3x^2y^3, x^2z^{10} + 2z^{10} - xy^3 - x^2,\ x^2y^6 - x^6 + 3x^3y^3 - 2x^4 + 2xy^3 - 2x^2 \}$.

Hilbert Polynomial: $2980\, s - 76460$.

Example 4. (*Toric ideal II*) [8,9] $(x_0 \succ x_1 \succ x_2 \succ x_3 \succ x_4)$

$$\{\, x_0x_1x_2x_3x_4 - 1, x_2^{29}x_3^5 - x_1^{14}x_4^{20}, x_1^{39} - x_2^{25}x_3^{14} \,\}.$$

Gröbner basis:

$$\{\, x_0{x_1}^2x_3{x_4}^{281} - {x_2}^{280}, {x_2}^{281} - x_1{x_4}^{280}, x_0{x_3}^2{x_4}^{221} - x_1{x_2}^{218},$$
$${x_1}^2{x_2}^{219} - x_3{x_4}^{220}, x_0{x_3}^3{x_4}^{161} - {x_1}^4{x_2}^{156}, {x_1}^5{x_2}^{157} - {x_3}^2{x_4}^{160},$$
$$x_0{x_3}^4{x_4}^{101} - {x_1}^7{x_2}^{94}, {x_1}^8{x_2}^{95} - {x_3}^3{x_4}^{100}, x_0{x_1}^4{x_4}^{61} - {x_2}^{61},$$
$${x_2}^{62}x_3 - {x_1}^3{x_4}^{60}, x_0{x_3}^5{x_4}^{41} - {x_1}^{10}{x_2}^{32}, {x_1}^{11}{x_2}^{33} - {x_3}^4{x_4}^{40},$$
$$x_0{x_2}^{26}{x_3}^{15}x_4 - {x_1}^{38}, {x_1}^{39} - {x_2}^{25}{x_3}^{14}, x_0{x_1}^{15}{x_4}^{21} - {x_2}^{28}{x_3}^4,$$
$${x_2}^{29}{x_3}^5 - {x_1}^{14}{x_4}^{20}, x_0{x_3}^{10}{x_4}^{21} - {x_1}^{24}{x_2}^3, {x_1}^{25}{x_2}^4 - {x_3}^9{x_4}^{20},$$
$$x_0x_1x_2x_3x_4 - 1 \,\}.$$

Hilbert Polynomial : $\dfrac{3905}{2}\,s^2 - \dfrac{177005}{2}\,s + 178805\,.$

Example 5. (*Toric ideal III*) [10] $(x \succ y \succ z \succ w)$

Gröbner basis:

$$\{\, y^{250} - x^{239}z^{11},\ x^{150}z^{12} - y^{161}w,\ y^{89}z - x^{89}w\,x^{61}z^{13} - y^{72}w^2,$$
$$x^{33}z^{27} - y^{55}w^5,\ z^{55} - x^{23}y^{21}w^{11},\ x^5z^{41} - y^{38}w^8,\ y^{17}z^{14} - x^{28}w^3 \,\}.$$

Hilbert Polynomial : $\dfrac{1229}{2}\,s^2 - \dfrac{73855}{2}\,s + 546272\,.$

Table 2. Cardinalities of bases in Examples 2-5

Example	Cardinality		
	Gröbner basis	Janet-like basis	Janet basis
2	4	5	11
3	9	14	983
4	19	190	7769
5	8	18	37901

In Table 2 we show cardinalities of Gröbner, Janet-like and Janet bases for the above examples. As one sees, Janet-like bases are much more compact than Janet bases. In other words, they have much less Gröbner redundancy. This higher redundancy of Janet bases has an effect on the running times.

The timings for construction of Janet bases for Examples 3, 4 and 5 [3], as measured on a AthlonXP 1600 computer with 256 Mb RAM running under Gentoo Linux 2004.3, are 0.04, 3.73 and 427.52 seconds, respectively. As to the

[3] Example 2 is too small for our code.

timings for Janet-like bases, because of their very small value (certainly less that 0.01 second) we were not able to measure them.

It is clear that for the case of Janet bases those computing times are wasted for constructing, analyzing and adding to the output basis a large number of $J-$head irreducible nonmultiplicative prolongations. Janet-like division is much more optimized in this respect.

5 Conclusion

It should be noted that, given a Janet-like basis G of a polynomial ideal $\mathcal{I} := \mathrm{Id}(G)$, the set

$$\{\ tg \mid g \in G, t \in \mathcal{M}(\mathrm{lm}(g), \mathrm{lm}(G))\ \} \tag{11}$$

can be considered as a staggered linear basis of $\mathcal{I}$ as $\mathbb{K}-$vector space. Similarly, any involutive basis G generates a staggered linear basis if one replaces $\mathcal{M}(\mathrm{lm}(g), \mathrm{lm}(G))$ in (11) by $\mathcal{L}(\mathrm{lm}(g), \mathrm{lm}(G))$ in accordance with Definition 4 in [1].

The notion of staggered linear basis was introduced in [13] (see also [14]) together with the appropriate modification of the Buchberger algorithm for computing Gröbner bases. Based upon relation (11), one can consider algorithm **Janet-like Basis**, as well as involutive algorithms [2,5,3], as improvements of the Gebauer-Möller staggered linear basis algorithm [13]. Another and very efficient imrovement of the last algorithm is the Faugère algorithm F_5 described in [15] for the case of homogeneous input polynomials. The most impressive feature of F_5 is detecting practically all useless, i.e., zero-redundant critical pairs.

The radical distinction of algorithm **Janet-like Basis** and involutive algorithms from the Gebauer-Möller staggered linear basis algorithm and the Faugère algorithm F_5 is partition of monomials for every of intermediate polynomials into two disjoint sets: multiplicative and nonmultiplicative. These two sets play fundamentally different algorithmic role. Whereas nonmultiplicative monomials are used for construction of prolongations including critical pairs, the multiplicative ones are used for reduction only. As a result, both intermediate and output bases generally have some extra Gröbner redundant elements that are nonmultiplicative prolongations of other elements in the basis. In doing so, the reduced Gröbner basis is the internally fixed subset of the output basis, and can be output without any extra computational costs.

On the other hand, experimental study of Janet division presented in [3] shows that the presence of extra polynomials provided by the partition of monomials smoothes growth of intermediate coefficients, and thereby increases practical efficiency of computation. Other efficiency aspects of the partition observed in [3] are: weakened role of the Buchberger criteria, fast search of a reductor, natural and effective parallelism. By its similarity to Janet division, Janet-like division preserves all these efficiency issues. The experimental evidence of this fact will be described elsewhere.

There are grounds to believe that the new criterion of paper [15] can be adopted to our algorithms too.

Acknowledgements

The research presented in this paper was supported in part 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.: Janet-like Monomial Division. Submitted to CASC'05 (Kalamata, Greece, September 12 - 16, 2005).
2. 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.
3. 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.
4. 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.
5. Apel, J.: Theory of Involutive Divisions and an Application to Hilbert Function Computations. *Journal of Symbolic Computation* 25 (1998) 683–704.
6. Seiler, W.M. *Involution - The formal theory of differential equations and its applications in computer algebra and numerical analysis*, Habilitation thesis, Dept. of Mathematics, University of Mannheim (2002).
7. Bigatti, A.M., La Scala, R. and Robbiano, L.: Computing Toric Ideals. *Journal of Symbolic Computation* 27 (1999) 351-365.
8. Pottier, L.: *Computation of toric Gröbner bases, Gröbner bases of lattices and integer point sof polytopes*. http://www-sop.inria.fr/safir/SAM/Bastat/doc/doc.html
9. 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.
10. Morales, M.: Equations des Variétés Monomiales en codimension deaux. *Journal of Algebra* 175 (1995) 1082-1095.
11. Hemmecke, R.: Private communication.
12. 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.
13. Gebauer, R. and Möller, H.M.: Buchberger's Algorithm and Staggered Linear Bases. In: *Proceedings of SYMSAC '86*, ACM Press, New York (1986) 218–221.
14. Möller, H.M., Mora, T. and Traverso, C.: Gröbner Bases Computation Using Syzygies. In: *Proceedings of ISSAC'92*, ACM Press, New York (1992) 320–328.
15. Faugère, J.C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In: *Proceedings of Issac 2002*, ACM Press, New York (2002) 75–83.