J. Symbolic Computation (1995) **11**, 1–000

A Gröbner Approach to Involutive Bases†

JOACHIM APEL

Institut für Informatik, Universität Leipzig, D-04109 Leipzig, Germany

(Received 2 February 1995)

Recently, Zharkov and Blinkov introduced the notion of involutive bases of polynomial ideals. This involutive approach has its origin in the theory of partial differential equations and is a translation of results of Janet and Pommaret. In this paper we present a pure algebraic foundation of involutive bases of Pommaret type. In fact, they turn out to be generalized left Gröbner bases of ideals in the commutative polynomial ring with respect to a non-commutative grading. The introduced theory will allow not only the verification of the results of Zharkov and Blinkov but it will also provide some new facts.

1. Introduction

Nowadays, the search for improvements of Buchberger's Algorithm for the computation of Gröbner bases (see Buchberger, 1965, 1985) is one of the main research directions in Computer Algebra. Recently, Zharkov and Blinkov reported about a completely new approach to the problem (Zharkov and Blinkov, 1993). They translated involutive methods originating from the theory of partial differential equations (see Janet, 1929; and Pommaret, 1978) in the language of polynomial ideals. This provides the class of so-called involutive bases (see Zharkov and Blinkov, 1993; and Zharkov, 1994*a,b*) and a constructive method for their computation. The involutive bases turned out to be special redundant Gröbner bases and, hence, they lead to a second method for the computation of Gröbner bases which at first sight is completely different from Buchberger's Algorithm (cf. Figures 1 and 2).

Comparing Gröbner bases and involutive bases of Pommaret type, also called Pommaret bases, Zharkov and Blinkov stated the latter to be superior for two reasons. They claimed that involutive bases contain more information about the structure of the ideal due to the redundancy. Furthermore, they reported a series of examples tested using both methods showed a much better time behaviour of the new method. It is a fact, however, that the method of Zharkov and Blinkov cannot have lower than a double exponential worst case complexity because this bound for Gröbner bases results from an input–output consideration. Even in the zero-dimensional case there are obvious examples for which Buchberger's Algorithm is faster than the method of Zharkov and Blinkov: e.g. $F = \{x^3 + y^2 + z - 3, y^3 + z^2 + x - 3, z^3 + x^2 + y - 3\}$. F is (reduced) Gröbner basis with respect to any degree compatible order and Buchberger's Algorithm will realize this

† In memory of A. Yu. Zharkov.

0747–7171/95/000000 + 00 $08.00/0

fact without performing any reduction since all critical pairs can be skipped according to the product criterion (see Buchberger, 1985). But 10 new polynomials have to be added to F in order to complete it to a Pommaret basis (see Zharkov and Blinkov, 1993). Taking into account all these facts, it is worth investigating the relationship between Gröbner bases and involutive bases. Some important questions are:

Which method has the better average behaviour?

Does the Zharkov–Blinkov method reflect particular strategies (e.g. pair selection, post reduction, etc.) that can be used to improve Buchberger's Algorithm at least for some width class of input ideal bases?

Assuming the previous question has a positive answer, how large is the class and can we guess whether a basis belongs to the class?

As a preparatory step towards answering these questions, in this paper we will give a completely algebraic description of Pommaret bases. Our algebraic foundation of Pommaret bases is based on two major ideas. First, we have a certain similarity of the Zharkov–Blinkov method to the Kandri-Rody–Weispfenning closure technique for two sided ideals in algebras of solvable type (see Kandri-Rody and Weispfenning, 1990). This motivates to watch the theory in a "non-commutative light". Second, the theory of graded structures introduced by Robbiano (1986) and generalized to non-commutative situations by Mora (1988) proved to be a powerful frame for generalizations of Gröbner bases. The fundamental idea in the theory of graded structures is to calculate in the associated graded ring and to lift back the results to the original ring. So, it is natural to look for gradings providing an associated graded ring having "better" (or at least not "worse") algebraic properties than the original ring (cf. Mora, 1988; and Apel, 1992). We cannot follow this line here any longer. Starting from a commutative, Noetherian integral domain, we will construct an associated graded ring that is non-commutative, non-Noetherian and contains zero-divisors. The price we pay is the loss of the termination property. Without knowing the work of Zharkov and Blinkov, in particular their statement about the comparison to Buchberger's Algorithm, this author would certainly have never investigated such an approach.

In addition to a better insight and the confirmation of all results reported by Zharkov and Blinkov (1993), our algebraic approach provides the following additional facts about Pommaret bases:

Pommaret bases are investigated with respect to arbitrary admissible term orders without requiring degree compatibility;

The method for the computation of Pommaret bases is a semi-decision procedure for the problem "Has I a finite Pommaret basis?"; i.e. it will terminate after finitely many steps if and only if the ideal I has a finite Pommaret basis;

The algorithm for the computation of Pommaret bases can be improved by criteria and selection strategies similar to those known from Buchberger's Algorithm;

There are given conditions when an ideal has a finite Pommaret basis, and answers the question concerning the linear variable changes transforming the ideal in a position ensuring a finite Pommaret basis;

The notion of the Pommaret basis of an ideal is completely decoupled from the method for its computation;

The theory of Pommaret bases can be straightforwardly generalized to algebras of solvable type.

This paper is organized as follows. In order to keep the paper self-contained we present an introduction to the theories of (ordinary) Gröbner bases, Pommaret bases and (generalized) Gröbner bases in graded structures in Sections 2 and 3. In Section 4 it is shown that the notion of Pommaret basis is an instantiation of the generalized Gröbner basis concept in graded structures. We will formulate and prove some important properties of Pommaret bases by means of algebra. Finally, in Section 5, we discuss some possible and impossible generalizations of the theory.

2. Ordinary Gröbner and Pommaret bases

Let $R = \mathcal{K}[X_1, \ldots, X_n] = \mathcal{K}[X]$ be the commutative polynomial ring in the variables $X = \{X_1, \ldots, X_n\}$ over the field $\mathcal{K}$. The set $T = \{X_1^{\nu_1} \cdots X_n^{\nu_n} | \nu_i = 0, 1, 2, \ldots\}$ of power products forms a $\mathcal{K}$-vector space basis of R. An irreflexive well-order $\prec$ of T which is compatible with the multiplication of power products, i.e. $u \prec v$ implies $tu \prec tv$ for all power products u, v and t, is called an *admissible term order*. For a description and complete classification of admissible term orders we refer to Robbiano (1985). Let $\prec$ be a fixed admissible term order. Then each non-zero polynomial $f \in R$ has a unique representation $f = \sum_{i=1}^{m} c_i t_i$ satisfying $0 \neq c_i \in \mathcal{K}, t_i \in T$ $(1 \leq i \leq m)$ and $t_m \prec t_{m-1} \prec \cdots \prec t_1$. We define the *leading power product* and the *leading coefficient* of f by $\mathrm{lp}(f) := t_1$ and $\mathrm{lc}(f) := c_1$, respectively.

2.1. GRÖBNER BASES

A brief introduction to the well-known theory of Gröbner bases follows. We will not present the improvements achieved by many different researchers during the last three decades; an overview can be found, for instance, in Buchberger (1985) or Becker *et al.* (1993).

A polynomial $g \in R$ is called *reducible modulo* $F \subset R$ iff there exists $f \in F$ such that $\mathrm{lp}(f)$ divides $\mathrm{lp}(g)$. Otherwise, g is called *irreducible modulo* F. Let g be reducible modulo F and $f \in F$ such that $\mathrm{lp}(g) = t \cdot \mathrm{lp}(f)$ for some $t \in T$. Then we say: g *reduces to* $h = g - \frac{\mathrm{lc}(g)}{\mathrm{lc}(tf)} tf$ modulo F. A sequence $g = h_1, h_2, \ldots$ such that h_i reduces to h_{i+1} modulo F for all $i = 1, 2, \ldots$ is called a *reduction sequence* of g modulo F. Note, that any reduction sequence of g modulo F is finite since $\prec$ is well-order. If $g = h_1, h_2, \ldots, h_k$ is a reduction sequence modulo F and h_k is irreducible modulo F, then we call h_k a *normal form* of g modulo F. Given two non-zero polynomials $g, h \in R$ we define the *S-polynomial* corresponding to the pair (g, h) by

$$\mathrm{Spol}(g, h) := \mathrm{lc}(h) \frac{t}{\mathrm{lp}(g)} g - \mathrm{lc}(g) \frac{t}{\mathrm{lp}(h)} h\,, \text{ where } t = lcm(\mathrm{lp}(g), \mathrm{lp}(h))\,.$$

A set $F \subset R$ is called a *Gröbner basis* of the ideal $I = F \cdot R$ with respect to $\prec$ iff zero is a normal form of each element $g \in I$ modulo F (or equivalently, for g ranging only over all S-polynomials corresponding to pairs of elements of F).

Figure 1 presents a rough version of Buchberger's Algorithm. $\mathrm{Nf}(\mathrm{Spol}(cp), G)$ denotes a normal form of $\mathrm{Spol}(cp)$ modulo G.

Input: finite basis F of the ideal I, term order $\prec$
Output: Gröbner basis G of I with respect to $\prec$

$P :=$ set of pairs of elements of F
$G := F$
while $P \neq \emptyset$ **do**
  choose $cp \in P$
  $P := P \backslash \{cp\}$
  $h := \mathrm{Nf}(\mathrm{Spol}(cp), G)$
  if $h \neq 0$ **then**
    $P := P \cup \{(g, h) | g \in G\}$
    $G := G \cup \{h\}$

Figure 1. Buchberger's Algorithm (method 1)

2.2. POMMARET BASES

The main difference between the theories of Gröbner and involutive bases consists in the notion of division of power products and, consequently, in the notion of reduction. A variable X_i is called *Pommaret-multiplicative* for the power product $u \in T$ iff $u \in \mathcal{K}[X_i, \ldots, X_n]$. We say $u \in T$ is a *Pommaret divisor* of $t \in T$ iff u divides t and all variables occurring in $\frac{t}{u}$ are Pommaret-multiplicative for u. A finite set $F \subset R$ of non-zero polynomials whose leading power products are pairwise but not a Pommaret divisor of each other is called *P-autoreduced.* A polynomial $g \in R$ is called *P-reducible* with respect to $F \subset R$ iff there exists $f \in F$ such that $\mathrm{lp}(f)$ is a Pommaret divisor of $\mathrm{lp}(g)$. Let $g \in R$, $F \subset R$, $f \in F$ and $t \in T$ such that $\mathrm{lp}(f)$ is a Pommaret divisor of $\mathrm{lp}(g)$ and $\mathrm{lp}(g) = t \cdot \mathrm{lp}(f)$. Then, by definition, g *P-reduces to* $h = g - \frac{\mathrm{lc}(g)}{\mathrm{lc}(tf)} tf$ modulo F. Based on the notions P-reducible and P-reduces modulo F, we can introduce the appropriate notions *P-irreducible*, *P-reduction sequence* and *P-normal form* modulo F in the same way as we did for Gröbner bases. Finally, a set $F \subset R$ is called a *Pommaret basis* of $I = F \cdot R$ with respect to $\prec$ iff F is P-autoreduced and each element $g \in I$ has zero as a P-normal form modulo F.

Figure 2 shows a constructive method (method 2) for the computation of a Pommaret basis of the polynomial ideal generated by a given finite basis with respect to a given admissible term order $\prec$. The sub-algorithms *P_Autoreduce* and Nf_P can be constructed in the same way as is known from the Gröbner basis theory, only with the usual reductions being substituted by P-reductions. Each instruction step of method 2 is computable and in case of termination the method is correct. But the method is not algorithmic since, in general, termination is not ensured.

The correctness and termination proofs for zero-dimensional ideals I given by Zharkov and Blinkov make essential use of the degree compatibility of $\prec$ and of the fact that the bases involved are P-autoreduced. The termination of method 2 and the existence of finite Pommaret bases in the positive dimensional case remained open in the papers by Zharkov and Blinkov. They cited from the theory of partial differential equations only that any ideal will have a finite Pommaret basis after most linear variable changes. Our theory developed in Section 4 will overcome the above restrictions and we will be able to prove that the method is semi-algorithmic, i.e. it terminates if and only if the ideal has a finite Pommaret basis. Furthermore, we will give an explanation of "most" variable changes.

Comparing Figures 1 and 2 the first impression is that both methods are rather differ-

```
Input: finite basis F of the ideal I, term order ≺
Output in case of termination: Pommaret basis G of I with respect to ≺

G := ∅
while F ≠ ∅ do
    G := P_Autoreduce(G ∪ F)
    F := ∅
    for each g ∈ G do
        for each X_i which is not Pommaret-multiplicative for lp(g) do
            f := Nf_P(gX_i, G)
            if f ≠ 0 then F := F ∪ {f}
```

Figure 2. Method of Zharkov and Blinkov (method 2)

ent. In contrast to Buchberger's Algorithm, we do not need S-polynomials in method 2, though in some sense their reduction is replaced by P-autoreductions and P-reductions of so-called *prolongations* gX_i of basis polynomials by variables.

If we replace the subroutine *P_Autoreduce* by a left Gröbner basis algorithm and consider the right prolongations of basis elements not only by variables that are not Pommaret-multiplicative but by all variables, we obtain exactly the shape of the right closure technique for two-sided ideals in algebras of a solvable type developed by Kandri-Rody and Weispfenning (1990). So, dividing such variables that are Pommaret-multiplicative and such that are not Pommaret-multiplicative effects a certain non-commutative behaviour. Though we are in a completely commutative situation, this behaviour motivates us to watch Pommaret bases in a non-commutative light.

3. Graded structures

An introduction to the complete theory of Gröbner bases in graded structure can be found in Mora (1988). We will restrict ourselves here to some major ideas that turn out to be useful for the characterization of generalized Pommaret bases.

Definition 3.1. *Let A be an associative ring with unit element and Γ be a monoid. Furthermore, let $\prec$ be an irreflexive well-order of Γ such that*

$$\begin{gathered} \mathbb{1} \prec \gamma \ \text{ for all } \ \mathbb{1} \neq \gamma \in \Gamma \ \text{ and} \\ \alpha \prec \beta \ \text{ implies } \ \alpha \circ \gamma \prec \beta \circ \gamma \ \text{ and } \ \gamma \circ \alpha \prec \gamma \circ \beta \ \text{ for all } \ \alpha, \beta, \gamma \in \Gamma\,, \end{gathered} \tag{3.1}$$

where $\circ$ is the operation and $\mathbb{1}$ is the unit element of Γ. Finally, let $\varphi : A\backslash\{0\} \to \Gamma$ be a function satisfying:

$$\begin{gathered} \varphi(1) = \varphi(-1) = \mathbb{1}\,, \\ a + b = 0 \ \text{ or } \ \varphi(a+b) \preceq \max(\varphi(a), \varphi(b))\,, \ \text{ and} \\ a \cdot b = 0 \ \text{ or } \ \varphi(a \cdot b) \preceq \varphi(a) \circ \varphi(b)\,, \end{gathered} \tag{3.2}$$

for all non-zero elements $a, b \in A$, where $\preceq$ denotes the reflexive closure of $\prec$. Then we call the quadruple $\mathcal{A} = (A, \Gamma, \prec, \varphi)$ a graded structure.

3.1. Related algebraic objects

Let $\mathcal{A} = (A, \Gamma, \prec, \varphi)$ be a fixed graded structure. In this section we will construct algebraic objects related to $\mathcal{A}$ which justify the above definition. To each element $\gamma \in \Gamma$

we associate the set $F_\gamma = \{a|\varphi(a) \preceq \gamma\} \cup \{0\}$. Clearly, $\delta \prec \gamma$ implies $F_\delta \subseteq F_\gamma$. For each non-zero element $a \in A$ there exists a unique $\gamma \in \Gamma$, namely $\gamma = \varphi(a)$, such that $a \in F_\gamma$ and $a \notin F_\delta$ for all $\delta \prec \gamma$. It is an easy observation that the F_γ are additive subgroups of A and that $F_\gamma F_\delta \subseteq F_{\gamma\circ\delta}$ for all $\gamma, \delta \in \Gamma$. Hence, the family $(F_\gamma)_{\gamma\in\Gamma}$ is a filtration of A. For each $\gamma \in \Gamma$ let $\hat{F}_\gamma$ be the additive subgroup of F_γ defined by $\hat{F}_\gamma := \{0\} \cup \bigcup_{\delta\prec\gamma} F_\delta$ and let G_γ be the factor group $F_\gamma/\hat{F}_\gamma$. The elements $g \in G_\gamma$ are called *homogeneous of degree* γ (notation: $\deg(g) = \gamma$). Let $G_\Gamma = \bigcup_{\gamma\in\Gamma} G_\gamma$ be the set of all homogeneous elements. φ induces a function $\mathrm{in} : A \to G_\Gamma$ by defining

$$\mathrm{in}(0) := 0 \ \text{ and } \ \mathrm{in}(a) := [a]_{\hat{F}_{\varphi(a)}} \ \text{ for } \ 0 \neq a \in A\,.$$

Since in is surjective, we can fix a function $\mathrm{in}^* : G_\Gamma \to A$ such that

$$\mathrm{in}(\mathrm{in}^*(g)) = g$$

for all $g \in G_\Gamma$. The mapping $\_\bullet\_ : G_\Gamma \times G_\Gamma \to G_\Gamma$ given by

$$\mathrm{in}(a) \bullet \mathrm{in}(b) = [ab]_{\hat{F}_{\varphi(a)\circ\varphi(b)}}$$

is well defined and can be uniquely extended to multiplication, making the direct sum $G = \bigoplus_{\gamma\in\Gamma} G_\gamma$ an associative ring. This Γ-graded ring G is called the *associated graded ring* of A with respect to the graded structure $\mathcal{A} = (A, \Gamma, \prec, \varphi)$.

3.2. LEFT $\mathcal{A}$-GRÖBNER BASES

Let $\mathcal{A} = (A, \Gamma, \prec, \varphi)$ be a graded structure and G be the associated graded ring of A with respect to $\mathcal{A}$. The function "in" is extended to subsets $F \subseteq A$ in the usual way by setting $\mathrm{in}(F) := \{\mathrm{in}(f)|f \in F\}$ and the left ideal generated by $\mathrm{in}(F)$ in G is called the $\mathcal{A}$-*initial left ideal* of F (notation: $\mathrm{LIn}(F)$). A basis F of the left ideal $I \subset A$ which satisfies

$$\mathrm{LIn}(F) = \mathrm{LIn}(I)$$

is called a *left* $\mathcal{A}$-*Gröbner basis* of I.

This is an elegant and frequently used definition of Gröbner bases. However, it is neither similar to the definition in Section 2 nor does it show an algorithmic way for Gröbner basis construction. In order to bridge this gap we need some further preparation. A non-zero element $h \in A$ is called $\mathcal{A}$-*reducible* modulo F if $\mathrm{in}(h) \in \mathrm{LIn}(F)$ and $\mathcal{A}$-*irreducible* modulo F, otherwise. By definition 0 is $\mathcal{A}$-irreducible modulo F. Let be $h \in A$ and $F \subset A$. Then a representation

$$h = \sum_{i=1}^{m} g_i f_i\,,$$

where $g_i \in A$, $f_i \in F$ and $\varphi(g_i) \circ \varphi(f_i) \preceq \varphi(h)$ for $i = 1, \ldots, m$, is called a *left* $\mathcal{A}$-*representation* of h in terms of F. Furthermore, an element $h' \in A$ which is $\mathcal{A}$-irreducible modulo F and for which $h - h'$ has a left $\mathcal{A}$-representation in terms of F is called a *left* $\mathcal{A}$-*normal form* of h modulo F. By definition 0 is left $\mathcal{A}$-normal form of 0 modulo F.

The natural generalization of Buchberger's critical pairs to graded structures are homogeneous syzygies. Let $H = \{h_1, \ldots, h_m\} \subset G_\Gamma\backslash\{0\}$ and G^m be the left G-module freely generated by $\{e_1, \ldots, e_m\}$ and graded by assigning

$$\deg(e_i) := \deg(h_i) \ \text{ for all } \ 1 \leq i \leq m.$$

The kernel of the homogeneous homomorphism $S : G^m \to G$ defined by

$$S\left(\sum_{i=1}^{m} k_i e_i\right) := \sum_{i=1}^{m} k_i h_i$$

is a homogeneous left submodule of G^m, the so-called *left syzygy module* $\mathrm{LSyz}(H)$ of H. Its elements are called *left syzygies* of H. Let $F = \{f_1, \ldots, f_m\}$ be a finite set of non-zero elements of A and let $s = \sum_{i=1}^{m} h_i e_i$ be a left syzygy of $\mathrm{in}(F)$. Then we define the *critical element* of F corresponding to s by:

$$c(s) := \sum_{i=1}^{m} \mathrm{in}^*(h_i) f_i \in A\,. \tag{3.3}$$

We close this section with a theorem summarizing some important equivalent properties for left $\mathcal{A}$-Gröbner bases.

Theorem 3.1. *Let $I \subset A$ be a left ideal, $F = \{f_1, \ldots, f_m\} \subset I$ be a finite set of non-zero elements of I, and B be a homogeneous basis of the left syzygy module* $\mathrm{LSyz}(\mathrm{in}(F))$. *Then the following conditions are equivalent:*

(i) F is a left $\mathcal{A}$-Gröbner basis of I;
(ii) Each $h \in I$ has 0 as (only) left $\mathcal{A}$-normal form modulo F;
(iii) F generates I and for each $s \in B$ the critical element $c(s)$ of F corresponding to s has 0 as (only) left $\mathcal{A}$-normal form modulo F.

Proof. We refer to Mora (1988).

3.3. effectiveness conditions

The third condition of Theorem 3.1 shows a way of generalizing Buchberger's Algorithm to left ideals in graded structures. In order to get a constructive method, the graded structure has to satisfy some effectiveness conditions.

Definition 3.2. *A graded structure $\mathcal{A} = (A, \Gamma, \prec, \varphi)$ having the following three properties is called a left effective graded structure:*

(i) A, G and Γ are effective and φ, in *and* in^* *are computable functions,*
(ii) For any given non-zero homogeneous elements $h_1, \ldots, h_m, h \in G$ the left ideal membership problem $h \in G \cdot (h_1, \ldots, h_m)$ is decidable and in case of membership it is possible to compute a homogeneous representation $h = \sum_{i=1}^{m} g_i h_i$, i.e. for all $1 \le i \le m$ we have $g_i \in G_\Gamma$ and $g_i = 0$ or $\deg g_i \circ \deg h_i = \deg h$.
(iii) For each finite subset H of non-zero homogeneous elements of G the left syzygy module $\mathrm{LSyz}(H)$ *is finitely generated and it is possible to compute a finite homogeneous basis of* $\mathrm{LSyz}(H)$.

All ground instructions appearing in the methods presented in Figures 3 and 4 are computable for left effective graded structures $\mathcal{A}$. Correctness in case of termination of method 3 is obvious; method 4 follows condition (iii) of Theorem 3.1. It remains for us to check the termination. Method 3 is algorithmic since termination is ensured by the

```
Input: graded structure A, h ∈ A, F = {f_1, ..., f_m} ⊂ A\{0}
Output: left G-normal form h' of h in terms of F

h' := h
while  h' ≠ 0 and in(h') ∈ LIn(F) do
      compute a homogeneous representation in(h') = Σ_{i=1}^m g_i in(f_i)
      h' := h' − Σ_{i=1}^m in*(g_i) f_i
```

Figure 3. Computation of left G-normal forms (method 3)

```
Input: graded structure A, Basis F = {f_1, ..., f_m} ⊂ A\{0} of the left ideal I
Output: left A-Gröbner basis H of I

H := ∅
while F ≠ ∅ do
      H := H ∪ F
      B := finite homogeneous basis of LSyz(in(H))
      F := ∅
      while B ≠ ∅ do
            choose s ∈ B
            B := B\{s}
            f := left A-normal form of c(s) in terms of H
            if f ≠ 0 then F := F ∪ {f}
```

Figure 4. Computation of left $\mathcal{A}$-Gröbner bases (method 4)

well-order property of $\prec$. The computation of left $\mathcal{A}$-Gröbner bases is semi-algorithmic in the following sense:

THEOREM 3.2. *Let $\mathcal{A} = (A, \Gamma, \prec, \varphi)$ be a graded structure, I a left ideal of A and F a finite basis of I which does not contain zero. Then method 4 terminates for input $\mathcal{A}$ and F if and only if* $\mathrm{LIn}(I)$ *is finitely generated.*

PROOF. The non-termination of method 4 in the case of a not-finitely generated $\mathcal{A}$-initial left ideal $\mathrm{LIn}(I)$ is a trivial consequence of the correctness. So, let us assume that $\mathrm{LIn}(I)$ is finitely generated by non-zero homogeneous elements $u_1, \ldots, u_k \in G$. First we introduce the notations $H(\mu)$ and $B(\mu)$ for the values assigned to H and B, respectively, at the beginning of the μ-th run of the outer loop of method 4. We fix $1 \le i \le k$ and look for an index $\mu_{0,i}$ such that $u_i \in \mathrm{LIn}(H(\mu_{0,i}))$. There exists $g \in I$ such that $\mathrm{in}(g) = u_i$. Let

$$g = \sum_{j=1}^{l} f_j h_j$$

be a representation of g in terms of $H(1)$ such that $h_1, \ldots, h_l \in H(1)$ and $f_1, \ldots, f_l \neq 0$. Let γ be the maximum of the $\varphi(f_j) \circ \varphi(h_j)$, where $1 \le j \le l$. If $\gamma = \deg u_i$ then $\mu_{0,i} = 1$ has the desired property. It remains the case that $\deg u_i \prec \gamma$. Then

$$s = \sum_{\{j \mid \varphi(f_j) \circ \varphi(h_j) = \gamma\}} \mathrm{in}(f_j) e_j \in \mathrm{LSyz}(\mathrm{in}(H(1)))\,.$$

Hence, $s = \sum_{j=1}^{q} a_j s_j$, where $s_j \in B(1)$. Each element $c(s_j)$ has a left $\mathcal{A}$-representation p_j in terms of $H(2)$. Hence, performing some obvious manipulations on

$$g = \sum_{j=1}^{l} f_j h_j + \sum_{j=1}^{q} \mathrm{in}^*(a_j)\,(p_j - c(s_j))\,,$$

where $c(s_j)$ stands for its defining representation (3.3), leads to a new representation

$$g = \sum_{j=1}^{l'} f'_j h'_j$$

of g in terms of $H(2)$ such that $h'_j \in H(2)$, $f'_j \neq 0$, $\varphi(f'_j) \circ \varphi(h'_j) \prec \gamma$ for all $1 \leq j \leq l'$. Repeating these arguments and taking into account that $\prec$ is well-order, we finally deduce the existence of $\mu_{0,i}$ such that g has a left $\mathcal{A}$-representation in terms of $H(\mu_{0,i})$.

Let μ_0 be the maximum of $\mu_{0,1}, \ldots, \mu_{0,k}$. Then $u_1, \ldots, u_k \in \mathrm{LIn}(H(\mu))$ for all $\mu \geq \mu_0$. Hence, $H(\mu_0)$ is a left $\mathcal{A}$-Gröbner basis of I. By Theorem 3.1 we deduce that all left critical elements of left syzygies of $B(\mu_0)$ will only have 0 as a left $\mathcal{A}$-normal form. Therefore, the outer loop of method 4 will terminate after μ_0 runs at most. Each inner loop terminates since each $B(\mu)$ is finite by construction. □

The semi-algorithm presented in Figure 4 has one serious restriction: it requires to consider all left syzygies associated to an intermediate basis $H(\mu)$ before any left syzygy involving basis elements computed afterwards. Recalling the sensitivity of Buchberger's Algorithm against the pair selection strategy, it is natural to ask for possible strategy improvements in the situation of graded structures. While the correctness of method 4 is independent of the syzygy selection strategy, it can lead to non-termination even in the case of finitely generated $\mathcal{A}$-initial left ideals. Checking the proof of Theorem 3.2 it turns out that we used only the fact that the syzygy selection strategy is fair, i.e. any created left syzygy has to be considered after finitely many steps. Hence, we can alter method 4 by allowing an arbitrary fair left syzygy selection strategy. The importance of fair selection strategies is well-known from the non-Noetherian situations of free non-commutative rings (Mora, 1986) and differential algebras (Ollivier, 1990). If the associated graded ring G is Noetherian, the situation is even better: we could use a completely different termination proof which is independent on the syzygy selection strategy.

3.4. Quotients of graded structures

Let $\mathcal{A} = (A, \Gamma, \prec, \varphi)$ be a graded structure and $I \subset A$ be a two-sided ideal of A. Then we can construct a graded structure $\mathcal{A}_I = (A/I, \Gamma, \prec, \varphi_I)$ for the quotient ring A/I, where the function φ_I is defined by

$$\varphi_I(a) := \min\{\varphi(f) | f \in a\}\,.$$

φ_I is well-defined since $\prec$ is well-order. It is an easy exercise to verify the validity of conditions (3.2).

4. Pommaret bases in graded structures

The theory of graded structures provides an excellent framework for generalizations of the theory of Gröbner bases. What remains for us is to introduce a suitable grading and to check the effectiveness conditions in particular cases.

4.1. The Gröbner grading of polynomial rings

Before we consider Pommaret bases we will show how the classical theory of Gröbner bases due to Buchberger (1965, 1985) can be formulated in terms of graded structures. Let T be the free commutative monoid generated by X, i.e. the monoid of commutative power products, and $\prec_T$ be an admissible term order of T. We easily observe that $\prec_T$ satisfies conditions (3.1) and that the function lp, assigning it to each non-zero polynomial its leading power product, satisfies conditions (3.2). Hence, $\mathcal{R}_T = (R, T, \prec_T, \mathrm{lp})$ is a graded structure. We hold that $F \subset I$ is (ordinary) Gröbner basis with respect to $\prec_T$ of the ideal $I \subset R$ if and only if it is left $\mathcal{R}_T$-Gröbner basis of I considered as left ideal. Therefore, we call $\mathcal{R}_T$ the *Gröbner grading* of R defined by $\prec_T$. Furthermore, the algorithm presented in Figure 1 turns out to be an instantiation of the semi-algorithm given in Figure 4. Of course, in the particular situation $\mathcal{A} = \mathcal{R}_T$ the latter is algorithmic, too.

4.2. A grading of free non-commutative algebras

Starting from results of Bergmann (1978), Mora developed a theory of Gröbner bases of one- and two-sided ideals of free non-commutative algebras (Mora, 1986). This theory can also be interpreted as an instantiation of the theory of graded structures (see Mora, 1988). Let S be the free non-commutative monoid generated by X and $\prec_S$ be an irreflexive well-order of S satisfying conditions (3.1). The free non-commutative $\mathcal{K}$-algebra $P = \mathcal{K}\langle S\rangle$ in the variables X is the algebra obtained by monoid adjunction of S to the field $\mathcal{K}$. Since S is isomorphic to a free word semi-group, we will call an element of S a *word*. S is $\mathcal{K}$-vector space basis of P. Hence, the function $\mathrm{lw}{:}P\backslash\{0\} \to S$ assigning to each non-zero element $f \in P$ the largest word (with respect to $\prec_S$) which appears in f with non-zero coefficient is well-defined and satisfies conditions (3.2). Consequently, $\mathcal{P} = (P, S, \prec_S, \mathrm{lw})$ is a graded structure. The notions of left-, right- and two-sided $\mathcal{P}$-Gröbner basis of $F \subset P$ as well as the algorithms for their computation correspond to those introduced in Mora (1986).

4.3. The Pommaret grading of polynomial rings

In the terminology of graded structures, algebras of solvable type are non-commutative rings graded by a commutative monoid (cf. Kandri-Rody and Weispfenning, 1990; and Apel, 1992). Now we show how Pommaret bases can be described by an opposite approach. Let $R, P, T, S, \prec_T, \prec_S, \mathrm{lp}$ and lw be as above and let $\circ$ denote the concatenation of words, i.e. the monoid operation in S. Identifying the commutative power products with the *ordered* words, words such as $X_{i_1} \cdots X_{i_k} \in S$ for which $i_1 \le i_2 \le \cdots \le i_k$, the set T can be embedded into S. Note, however, that this is not a monoid embedding. Furthermore, we assume that $\prec_S$ satisfies the following two conditions:

(i) $s \prec_S t \Longleftrightarrow s \prec_T t$ for all $s, t \in T$;
(ii) For each $X_{i_1} \cdots X_{i_k} \in T$ and each permutation π of the numbers $1, \ldots, k$ it holds that $X_{i_1} \cdots X_{i_k} \preceq_S X_{i_{\pi(1)}} \cdots X_{i_{\pi(k)}}$.

That means $\prec_S$ coincides with $\prec_T$ on T and among all words which differ only in the sequence of variables for which the ordered is minimal with respect to $\prec_S$. It is easy to observe that such an admissible order $\prec_S$ exists for any given admissible term order $\prec_T$. Let J be the two-sided ideal of P generated by $\{X_iX_j - X_jX_i | 1 \leq j < i \leq n\}$ and consider the graded structure $\mathcal{P}_J = (P/J, S, \prec_S, \mathrm{lw}_J)$ as introduced in Section 3. Identifying P/J and R via the canonical isomorphism, we see that $\mathcal{P}_J$ is equal to $\mathcal{R}_S = (R, S, \prec_S, \mathrm{lp})$. So, we obtain a second class of gradings of the commutative polynomial ring R which appears as its natural non-commutative gradings. A simple example shall illustrate the connection between $\mathcal{P}_J$ and $\mathcal{R}_S$.

EXAMPLE 4.1. Let $R = Q[X,Y,Z]$ be the polynomial ring in the indeterminates X, Y and Z over the rationals and $\prec_T$ be the lexicographical order $\prec_{X,Y,Z}$ extending $X \prec_{X,Y,Z} Y \prec_{X,Y,Z} Z$. Further, consider the free non-commutative algebra $P = Q\langle X,Y,Z\rangle$. The words generated by X, Y and Z are ordered by $\prec_S$ in such a way that first the number of occurrences of Z are compared; in case of equality the number of occurrences of Y are compared. If we have equality again then we compare the number of occurrences of X. So we have, for instance, $XY \prec_S YZ$ and $ZXZ \prec_S YZZ$. No decision, though, can be made if both words contain the same number of Z, Y and X, i.e. they are equal in any permutation of letters, e.g. XZZ, ZXZ and ZZX. We will break these ties by the lexicographical order $\prec_{X,Y,Z}$ for words. For the above example this yields $XZZ \prec_S ZXZ \prec_S ZZX$. Clearly this is a suitable order $\prec_S$ since it is admissible and satisfies the above conditions (i) and (ii). But we could break the ties also in another way, e.g. $XZZ \prec_S' ZZX \prec_S' ZXZ$. Consider the two-sided ideal $J \subset P$ generated by $XY - YX, ZX - XZ$ and $ZY - YZ$. Let $f \in P$. The residue class $f + J$ contains a unique element $\tilde{f}$ which is linear combination of ordered words. By definition $\mathrm{lw}_J(f + J)$ is the minimum (with respect to $\prec_S$) among all leading words of representants of $f + J$. In particular,

$$\mathrm{lw}_J(f + J) \preceq \mathrm{lw}(\tilde{f})\,.$$

But, obviously, the support of any representant of $f + J$ contains at least one word which is equal to $\mathrm{lw}(\tilde{f})$ up to permutation. Hence, by condition (ii) on $\prec_S$, we deduce the equation

$$\mathrm{lw}_J(f + J) = \mathrm{lw}(\tilde{f}).$$

According to the identification of ordered words and commutative power products we can interpret $\tilde{f}$ as an element of the polynomial ring R. The canonical isomorphism defined by $P/J \ni f + J \mapsto \tilde{f} \in R$ provides an identification of P/J and R which justifies the equation

$$\mathrm{lw}_J(f + J) = \mathrm{lp}(\tilde{f}). \tag{4.1}$$

Before we prove that the grading $\mathcal{R}_S$ is good for the computation of Pommaret bases, we will have to look at the associated graded ring G_S of R with respect to $\mathcal{R}_S$. Let $G_{S,t}$ denote the additive group of all elements of G_S of degree $t \in S$. Clearly, $G_{S,t} = \{0\}$ for all $t \notin T$ and $G_{S,t}$ is a one-dimensional $\mathcal{K}$-vector space for each $t \in T$. Consequently, G_S is isomorphic to R as $\mathcal{K}$-vector space and we can represent G_S as the polynomial ring R with a new multiplication $\bullet$. Unless we want to stress the residue class property of the elements of G_S, we will abbreviate the residue class $[u]_{\hat{F}_u} \in G_S$ by u for elements $u \in T$. In particular, we write $\mathrm{in}(u) = u$ for all $u \in T$. Given two words $u, v \in T$ we have

$\text{in}(u) \bullet \text{in}(v) = \text{in}(uv)$ if $u \circ v \in T$ and $\text{in}(u) \bullet \text{in}(v) = 0$, otherwise. Recall Example 4.1. We have

$$\text{in}(XY) \bullet \text{in}(YZ) = [XY]_{\hat{F}_{XY}} \bullet [YZ]_{\hat{F}_{YZ}} = [XY^2Z]_{\hat{F}_{XYYZ}} = \text{in}(XY^2Z).$$

But since $XYYZ \prec_S XZYY$, it holds that

$$\text{in}(XZ) \bullet \text{in}(Y^2) = [XZ]_{\hat{F}_{XZ}} \bullet [Y^2]_{\hat{F}_{YY}} = [XY^2Z]_{\hat{F}_{XZYY}} = 0.$$

In conclusion we can deduce some properties of G_S. In the univariate case we have the trivial relationship $G_S = G_T = R$. If X contains at least two variables then G_S is non-commutative (e.g. $XY = X \bullet Y \neq Y \bullet X = 0$), contains zero-divisors (e.g. $Y \bullet X = 0$) and is not left Noetherian (e.g. the left ideal generated by XY^μ, where $\mu = 1, 2, \ldots$, is not finitely generated). Furthermore, we observe that $\text{in}(u) \in \text{LIn}(t)$ if and only if u is right subword of t, i.e. there exists $v \in S$ such that $v \circ u = t$. Summarizing this, we can state the main theorem of this paper:

Theorem 4.1. *Let $\prec_T$ be an admissible term order and $\mathcal{R}_S = (R, S, \prec_S, \text{lp})$ be a graded structure, where $\prec_S$ satisfies conditions (i) and (ii). Furthermore, let $I \subset R$ be a polynomial ideal. Then each Pommaret basis F of I with respect to $\prec_T$ is a left $\mathcal{R}_S$-Gröbner basis of I. Moreover, F is Pommaret basis of I with respect to $\prec_T$ if and only if it is minimal left $\mathcal{R}_S$-Gröbner basis of I.*

Proof. The statement follows on immediately from the trivial observation that $u \in T$ is Pommaret divisor of $t \in T$ if and only if $\text{in}(u) \in \text{LIn}(t)$. The fact that the Pommaret bases defined by Zharkov and Blinkov correspond only to the minimal left $\mathcal{R}_S$-Gröbner bases is due to their assumption that a Pommaret basis has to be P-autoreduced. □

The theorem justifies calling $\mathcal{R}_S$ a *Pommaret grading* of R which extends $\prec_T$. Note that the order $\prec_S$ is not necessarily uniquely determined by $\prec_T$. For instance, both orders $\prec_S$ and $\prec_S^{'}$ would be suitable in Example 4.1. However, the freedom in the choice of $\prec_S$ has no influence on the leading power product of a polynomial. Therefore, initial ideals and the property of being a Gröbner basis are not influenced. In the sequel we will show that not only the notions of Pommaret and left $\mathcal{R}_S$-Gröbner bases coincide but that also the semi-algorithms for their computation are the same. First, we have to verify the left effectiveness of the Pommaret grading $\mathcal{R}_S$. Clearly, condition (i) of Definition 3.2 is satisfied. Let $h_1, \ldots, h_m, h \in G_S$ be non-zero homogeneous elements. Then h is member of the left ideal $I = G_S \bullet H$ if and only if there exist $1 \leq i \leq m$ and $v \in T$ such that $\deg h = v \circ \deg h_i$. This question is decidable and if $h \in I$ then

$$h = \frac{\text{lc}(h)}{\text{lc}(v \bullet h_i)} v \bullet h_i$$

is a homogeneous representation of h in terms of H. Hence, $\mathcal{R}_S$ also satisfies condition (ii) of Definition 3.2. The following lemma proves condition (iii).

Lemma 4.1. *Let $H = \{h_1, \ldots, h_m\} \subset G_S$ be a finite set of homogeneous non-zero elements. Then $B = B_1 \cup B_2$ is a finite basis of $\text{LSyz}(H)$, where*

$$B_1 = \left\{X_i \bullet e_{h_j} | 1 \leq j \leq m, 1 \leq i \leq n, X_i \circ \deg h_j \notin T\right\},$$

$$B_2 = \left\{u \bullet e_{h_j} + e_{h_k} | 1 \leq j, k \leq m, \deg u \circ \deg h_j = \deg h_k, \text{lc}(u \bullet h_j) = -\text{lc}(h_k)\right\}.$$

PROOF. Let $s = \sum_{j=1}^{m} f_j \bullet e_{h_j}$ be a non-zero homogeneous left syzygy of H of degree $u \in S$. We distinguish two cases.

(i) Let $u \notin T$. Then each non-zero element f_j has a decomposition $f_j = t_j \bullet X_{i_j}$, where t_j is a non-zero homogeneous element and $1 \leq i_j \leq n$. Clearly, $X_{i_j} \circ \deg h_j \notin T$. Hence, $s_j = X_{i_j} \bullet e_{h_j} \in B_1$ and $s = \sum_{f_j \neq 0} t_j \bullet s_j$ is a representation of s in terms of B_1.

(ii) Let $u \in T$. Then $f_j \bullet h_j = 0$ implies $f_j = 0$. Therefore, there exist $1 \leq j \neq k \leq m$ such that $f_j, f_k \neq 0$. The equality $\deg f_j \circ \deg h_j = \deg f_k \circ \deg h_k = u$ implies that, without loss of generality, $\deg h_j$ is right subword of $\deg h_k$. Hence, there exists a homogeneous non-zero element $v \in G_S$ such that $v \bullet h_j + h_k = 0$. Set $s' := s - f_k \bullet (v \bullet e_{h_j} + e_{h_k})$. s' is homogeneous left syzygy of H of degree u having less non-zero summands than s. Repeating these arguments, finally, we obtain a representation of s in terms of B_2.

□

In summary, $\mathcal{R}_S$ is a left effective graded structure and the method presented in Figure 4 is semi-algorithmic. It follow three properties which prove that the Zharkov/Blinkov method presented in Figure 2 is an instantiation of the semi-algorithm 4.

(i) Any P-normal form of a polynomial f modulo $H \subset R$ is also left $\mathcal{R}_S$-normal form of f modulo H.

(ii) The prolongations occurring in Figure 2 are critical elements of left syzygies contained in B_1.

(iii) The result of a P-autoreduction is a left $\mathcal{R}_S$-normal form of the critical element of some left syzygy contained in B_2.

The most important consequence of these observations is that we can apply all results obtained by many researchers in the theory of Gröbner bases within the last 30 years in order to improve the method for the computation of Pommaret bases. As usual we can look for criteria for detecting unnecessary reductions; in particular, we can minimize the basis B of left syzygies. A second, important way for obtaining speed is the choice of a "good" syzygy selection strategy. Recall that we can use any fair selection strategy for choosing the next left syzygy to be considered. Examples of fair selection strategies are those that choose a left syzygy of minimal weight with respect to some fixed weight vector assigning each variable a positive weight. If $\prec_S$ is a refinement of the partial order defined by such a positive weight vector, then we can apply the standard selection strategy, i.e. we always choose a left syzygy which has minimal degree with respect to $\prec_S$. Note, however, that the standard selection strategy is not fair, for example, for the lexicographical order. Sugar-like selection strategies (see Giovini *et al.,* 1991) are fair.

Now let us consider the termination problem of method 4 for our particular graded structure $\mathcal{R}_S$. According to Theorem 3.2, it is sufficient to investigate under which conditions the $\mathcal{R}_S$-initial left ideal of a given polynomial ideal is finitely generated. Assume I is a zero-dimensional polynomial ideal. Then there exist positive natural numbers $\nu_1, \ldots, \nu_n$ such that $X_i^{\nu_i} \in \mathrm{in}(I)$. For each $1 \leq i \leq n$ we define the set H_i consisting of all power products $X_1^{\mu_1} \cdots X_n^{\mu_n}$ such that $\mu_j = 0$ for $1 \leq j < i$, $\mu_i = \nu_i$ and $0 \leq \mu_j < \nu_j$ for $i < j \leq n$. All sets H_i are finite subsets of $\mathrm{in}(I)$. The left ideal of G_S generated by

$H = \bigcup_{i=1}^{n} H_i$ contains all but finitely many power products of T. Hence, a homogeneous basis of the $\mathcal{R}_S$-initial left ideal $\mathrm{LIn}_S(I)$ can be obtained by adding at most finitely many power products to H. This proves the well-known fact, that $\mathrm{LIn}_S(I)$ is finitely generated with respect to any Pommaret grading of R in case $\dim I = 0$.

There are positive dimensional ideals I for which $\mathrm{LIn}_S(I)$ is not finitely generated, for example, each principal ideal generated by a monomial not having the form X_n^{μ} (such as Y under the setting of Example 4.1) has this property. Though we will be unable to give a complete description of the termination behaviour in the positive dimensional case, we can characterize the situation up to a large extend. Let us consider the relationship between the initial ideals of I with respect to the graded structures $\mathcal{R}_T$ and $\mathcal{R}_S$. For the moment we forget about multiplication and consider only the $\mathcal{K}$-vector spaces $R = G_S = G_T$. Then the function $\mathrm{in} : R \to R$ is the same for both graded structures $\mathcal{R}_T$ and $\mathcal{R}_S$. However, in general, the left ideals $\mathrm{In}_T(F)$ and $\mathrm{LIn}_S(F)$ generated by $\mathrm{in}(F)$ in G_T and G_S, respectively, will be different because of the different multiplications. Note the $\mathcal{K}$-vector space equality of $\mathrm{In}_T(I)$ and $\mathrm{LIn}_S(I)$ for ideals I. Nevertheless, an ideal basis of $\mathrm{In}_T(I)$ need not to generate $\mathrm{LIn}_S(I)$. Recall that the associated graded ring with respect to a Gröbner grading is the polynomial ring R itself. We can thus consider $\mathcal{R}_S$-initial left ideals of $\mathcal{R}_T$-initial ideals. For a given admissible term order $\prec_T$, the initial ideals of I corresponding to the Gröbner grading defined by $\prec_T$ and a Pommaret grading extending $\prec_T$ are connected by the equation

$$\mathrm{LIn}_S(I) = \mathrm{LIn}_S(\mathrm{In}_T(I)). \tag{4.2}$$

It follows a necessary condition for finitely generated $\mathcal{R}_S$-initial left ideals:

LEMMA 4.2. *Let $\prec_T$ be an admissible term order, $\mathcal{R}_T$ be the Gröbner grading of R defined by $\prec_T$, and $\mathcal{R}_S$ be a Pommaret grading of R extending $\prec_T$. Also, let $I \subset R$ be a d-dimensional ideal such that $\mathrm{LIn}_S(I)$ is generated by the finite homogeneous basis $B \subset T$. Then I satisfies the following equivalent conditions:*

(i) for each $d < i \leq n$ there exists $\nu_i > 0$ such that $X_i^{\nu_i} \in \mathrm{LIn}_S(I)$;
(ii) $\{X_1, \ldots, X_d\}$ is the only maximal independent set of variables for I; and
(iii) $\{X_1, \ldots, X_d\}$ is a system of parameters for the R_T-initial ideal $\mathrm{In}_T(I)$, i.e. for each $1 \leq i \leq d$ we have

$$\dim\left(\mathrm{In}_T(I) + (X_1, \ldots, X_i)R\right) = d - i\,.$$

PROOF. For $d = n$ the statement is trivial. So let us assume $d < n$. $\dim(I) = d$ implies $I \cap \mathcal{K}[X_1, \ldots, X_{d+1}] \neq \{0\}$. Let $f \in I \cap \mathcal{K}[X_1, \ldots, X_{d+1}]$. For each $d < j \leq n$ and each natural number μ there exist $v_{j,\mu} \in T$ and $u_{j,\mu} \in B$ such that $v_{j,\mu} \circ u_{j,\mu} = \mathrm{lp}(X_j^{\mu} f) = \mathrm{lp}(f) \circ X_j^{\mu} \in \mathrm{in}(I)$. B is finite; hence, for each $d < j \leq n$ there exists an element $u_j \in B$ which is right subword of almost all powers X_j^{μ} $(\mu = 1, 2, \ldots)$. This proves condition (i). It is an easy exercise to prove the equivalence of all three conditions. □

The converse of Lemma 4.2 does not hold: consider the ideal $I \subset R$ generated by $\{XYZ, Z^2\}$ under the settings of Example 4.1. Obviously, I is two-dimensional and satisfies conditions (i)–(iii) of Lemma 4.2. However, the $\mathcal{R}_S$-initial left ideal

$$\mathrm{LIn}_S(I) = G_S \bullet (Z^2) + G_S \bullet (XYZ, XY^2Z, \ldots, XY^{\mu}Z, \ldots)$$

is not finitely generated. There is a straightforward generalization of the zero-dimensional case to higher dimensions that will provide a first sufficient condition.

LEMMA 4.3. *Let $\prec_T$ be an admissible term order, $\mathcal{R}_T$ be the Gröbner grading of R defined by $\prec_T$, and $\mathcal{R}_S$ be a Pommaret grading of R extending $\prec_T$. Furthermore, let $I \subset R$ be a d-dimensional polynomial ideal. If the $\mathcal{R}_T$-initial ideal $\mathrm{In}_T(I)$ satisfies*

$$(\mathrm{In}_T(I) \cap \mathcal{K}[X_{d+1}, \ldots, X_n])\, R = \mathrm{In}_T(I) \tag{4.3}$$

then $\mathrm{LIn}_S(I)$ is finitely generated.

PROOF. Let S' be the free non-commutative monoid generated by $\{X_{d+1}, \ldots, X_n\}$. Since I is d-dimensional and satisfies equation (4.3), the elimination ideal $\mathrm{In}_T(I) \cap \mathcal{K}[X_{d+1}, \ldots, X_n]$ is zero-dimensional. Hence, $\mathrm{LIn}_{S'}(\mathrm{In}_T(I) \cap \mathcal{K}[X_{d+1}, \ldots, X_n])$ is finitely generated. Using equations (4.2) and (4.3), we deduce $\mathrm{LIn}_S(I) = G_S \bullet \mathrm{LIn}_{S'}(\mathrm{In}_T(I) \cap \mathcal{K}[X_{d+1}, \ldots, X_n])$ and the assertion will follow. □

We say that $I \subset R$ is in *generic position* with respect to the admissible term order $\prec_T$ iff $t = X_1^{\mu_1} \cdots X_n^{\mu_n} \in \mathrm{in}(I)$ implies $u \in \mathrm{in}(I)$ for all monomials $u = X_1^{\nu_1} \cdots X_n^{\nu_n}$ satisfying

$$\textstyle\sum_{i=1}^n \mu_i = \sum_{i=1}^n \nu_i \text{ and}$$
$$\textstyle\sum_{i|X_j \prec_T X_i} \mu_i \le \sum_{i|X_j \prec_T X_i} \nu_i \text{ for all } 1 \le j \le n.$$

For any admissible term order $\prec_T$ and any ideal I there exists a Zariski open subset U of the group $Gl(n)$ of all non-degenerated linear variable changes such that any element of U transforms I in generic position with respect to $\prec_T$. If, in addition, $X_1 \prec_T X_2 \prec_T \cdots \prec_T X_n$ then the Borel group (i.e. the group of linear variable changes defined by upper triangular regular matrices) already contains a Zariski open subset U with the above property. For details we refer to Bayer and Stillman (1987).

THEOREM 4.2. *Let $\prec_T$ be an admissible term order such that $X_1 \prec_T X_2 \prec_T \cdots \prec_T X_n$ and let $\mathcal{R}_S$ be a Pommaret grading of R extending $\prec_T$. If the ideal $I \subset R$ is in generic position with respect to $\prec_T$ then the $\mathcal{R}_S$-initial left ideal $\mathrm{LIn}_S(I)$ is finitely generated.*

PROOF. Let $H \subset T$ be a minimal basis of $\mathrm{LIn}_S(I)$. Fix $1 \le j < n$. Each element $t \in H \cap \mathcal{K}[X_j, \ldots, X_n]$ can be represented in the form $t = X_j^{\nu_j} \circ u(t)$, where $u(t) \in T \cap \mathcal{K}[X_{j+1}, \ldots, X_n]$ and $\nu_j \ge 0$. Since I is in generic position with respect to $\prec_T$ we have $X_{j+1}^{\nu_j} \circ u(t) \in \mathrm{in}(I)$. Since H is minimal basis of $\mathrm{LIn}_S(I)$ there exist uniquely determined elements $v(t) \in T$ and $w(t) \in H \cap \mathcal{K}[X_{j+1}, \ldots, X_n]$ such that $X_{j+1}^{\nu_j} \circ u(t) = v(t) \circ w(t)$. Hence, the relation $\sim \subseteq (H \cap \mathcal{K}[X_j, \ldots, X_n]) \times (H \cap \mathcal{K}[X_j, \ldots, X_n])$ defined by $t \sim s \Longleftrightarrow w(t) = w(s)$ is an equivalence relation and

$$H \cap \mathcal{K}[X_j, \ldots, X_n] = \bigcup_{t \in H \cap \mathcal{K}[X_{j+1}, \ldots, X_n]} [t]_\sim .$$

Consider $t = X_{j+1}^{\mu_{j+1}} \cdots X_n^{\mu_n} \in H \cap \mathcal{K}[X_{j+1}, \ldots, X_n]$. Since H is minimal basis the class $[t]_\sim$ contains $\mu_{j+1} + 1$ elements at most. Hence, finiteness of $H \cap \mathcal{K}[X_{j+1}, \ldots, X_n]$ will imply finiteness of $H \cap \mathcal{K}[X_j, \ldots, X_n]$ for all $1 \le j < n$. The trivial observation that $H \cap \mathcal{K}[X_n]$ is finite completes the proof. □

Theorem 4.2 provides a second sufficient condition on positive dimensional ideals ensuring a finitely generated $\mathcal{R}_S$-initial left ideal. Any polynomial ideal will satisfy this condition after a suitable linear change of variables and the set of suitable transformations is Zariski open.

5. Possible and impossible generalizations

An obvious and easy to perform generalization of Pommaret bases in graded structures is to consider two-sided R_S-Gröbner bases.

For the sake of generalization we strictly avoid making use of the relation $\mathrm{lc}(f)\mathrm{lc}(g) = \mathrm{lc}(fg)$ for non-zero polynomials f and g and the fact that a polynomial ring is commutative. So, the theory can be extended to algebras of solvable type in a straightforward manner. Only the statements involving ideal dimensions have to be reformulated in a convenient way; we can consider the dimension of the ideal generated by $\mathrm{in}(I)$ in the polynomial ring over $\mathcal{K}$ in the same indeterminates.

Note that the calculations $g - ctf$ and $g - cf_t$, where $f_t = tf$, have almost the same cost in polynomial rings. But in algebras of solvable type the first calculation is often much more expensive than the second. Hence, the Pommaret basis approach for algebras of solvable type seems to be even more promising than for polynomial rings.

We will close this paper with a remark concerning other types of involutive bases. Recall that the basic idea of involutive bases is the restriction of the divisibility of power products. In the theory of Janet bases, introduced in Zharkov (1994*b*), the set of divisors of a power product depends not only on the power product itself but also it is defined relative to a set of non-zero polynomials. While the notions of divisibility used in the theories of Gröbner and Pommaret bases can be described in suitable associated graded rings, a similar approach will not work for Janet bases.

Acknowledgements

The author is grateful to A. Yu. Zharkov, V. P. Gerdt, U. Klaus and T. Mora for valuable discussions on the subject of involutive bases.

References

Apel, J. (1992). A relationship between Gröbner bases of ideals and vector modules of G-algebras. *Contemporary Mathematics* **131**, 195–204.

Bayer, D., Stillman, M., M. (1987). A theorem on refining division orders by the reverse lexicographic order. *Duke Mathematical J.* **55**, 321–328.

Becker, T., Weispfenning, V., Kredel, H. (1993). *Gröbner Bases: A Computational Approach to Commutative Algebra.* New York: Springer-Verlag.

Bergmann, G. M. (1978). The diamond lemma in ring theory. *Adv. Math.* **29**, 178–218.

Buchberger, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph.D. Thesis, Universität Innsbruck, Innsbruck, Austria.

Buchberger, B. (1985). An algorithmic method in polynomial ideal theory. In (Bose, N. K., ed.) *Recent Trends in Multidimensional System Theory.* Dordrecht: D. Reidel, chapter 6.

Giovini, A., Mora, T., Niesi, G., Robbiano, L., Traverso, C. (1991). "One sugar cube, please," or selection strategies in the Buchberger Algorithm. In (Watt, S. M., ed.) *Proc. ISSAC'91.* New York: ACM Press, pp. 49–54.

Janet, M. (1929). *Lecons sur les systémes d'équations aux deriveés partielles.* Paris: Gauthier-Villars.

Kandri-Rody, A., Weispfenning, V. (1990). Non-Commutative Gröbner bases in algebras of solvable type. *J. Symbolic Computation* **9**, 1–26.

Mora, T. (1986). Gröbner bases for non-commutative polynomial rings. Lecture Notes for Computer Science **229**, 353–362. Berlin: Springer-Verlag.

Mora, T. (1988). Seven variations on standard bases. University di Genova, Dip. di Mathematica, N. 45.
Ollivier, F. (1990). *Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité*. Ph.D. Thesis, École Polytechnique, Paris, France.
Pommaret, J. F. (1978). Systems of partial differential equations and Lie pseudogroups. New York: Gordon & Breach.
Robbiano, L. (1985). Term orderings on the polynomial ring. Lecture Notes in Computer Science **204**, 513–517. Berlin: Springer-Verlag.
Robbiano, L. (1986). On the theory of graded structures. *J. Symbolic Computation* **2**, 139–170.
Zharkov, A. Yu., Blinkov, Yu. A. (1993). Involution approach to solving systems of algebraic equations. *Proc. IMACS'93*, Lille. Preprint.
Zharkov, A. Yu. (1994*a*). Solving zero-dimensional involutive systems. *Proc. ISEMAG'94*. Preprint.
Zharkov, A. Yu. (1994*b*). Involutive polynomial bases: general case. Personal communication.