The Computation of Gröbner Bases Using an Alternative Algorithm

Joachim Apel
Institut für Informatik, Universität Leipzig,
Augustusplatz 10/11, D-04109 Leipzig, Germany
apel@informatik.uni-leipzig.de

0.1 Introduction

When Zharkov and Blinkov ([ZB93]) applied the classical ideas of involutive systems originating from the theory of partial differential equations (c.f. [Ja29],[Po78]) to the computation of Gröbner bases (c.f. [Bu65],[BW93]) their theory seemed to be a rather marginal concept. But due to the opportunity of gaining a faster version for one of the most frequently applied algorithms the method came into the focus of computer algebra research (c.f. [Ap95], [GB95], [GS95], [Ma95]). It turned out that Pommaret bases are not only of interest for fast implementations (c.f. [ZB93]) but that they are also a point of contact of different theories which were investigated intensively for a long time. So, the theory of Pommaret bases enables the exchange of useful ideas between the theories as well as it benefits itself from the relationships. A certain similarity of the Zharkov/Blinkov method and the Kandri-Rody/Weispfenning closure technique motivates the study of commutative polynomial rings from a non-commutative point of view. The theory of Pommaret bases can be presented in an algebraic way using the Gröbner theory of graded structures. Here we will present the straight forward generalization of Pommaret bases to the class of algebras of solvable type. Under the non-commutative grading most calculations are pushed back to the free non-commutative polynomial ring. This provides a link to the theory of term rewriting and the Zharkov/Blinkov method appears as an application of the prefix reduction/saturation technique of Madlener and Reinert (c.f.[MR93]) with a restricted saturation. The restricted saturation has its natural origin in the syzygy theory and heavily improves the termination behaviour in the particular case of Pommaret bases. So, it seems to be worth to investigate the effect of splitting the saturation step also for similar term rewriting problems.

The main result of this paper consists in the presentation of a termination condition for the Zharkov/Blinkov method providing an alternative algorithm for the computation of ordinary Gröbner bases which terminates for arbitrary ideals in the case of generalized degree compatible term orders.

Acknowledgement: The author is grateful to the participants of the Workshop on Symbolic Rewriting Techniques, Monte-Verita 1995, for many valuable discussions. Special thanks are to M. Kalkbrener, K. Madlener, D. Mall, T. Mora, and B. Reinert. Moreover the author is grateful to an anonymous referee for helpful remarks and suggestions.

0.2 Preliminaries

Let $R = \mathcal{K}[X]$ be the 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 terms forms a $\mathcal{K}$-vector space basis of R. An irreflexive well-order $\prec$ of T which is compatible with the multiplication $\circ_T$ of power products, i.e. $u \prec v$ implies $t \circ_T u \prec t \circ_T v$ for all terms u, v and t, is called an *admissible term order.* Furthermore, we introduce the notations $T(X_{i_1}, \ldots, X_{i_k})$ and $T(\{X_{i_1}, \ldots, X_{i_k}\})$ for the set of terms depending only on the variables $\{X_{i_1}, \ldots, X_{i_k}\} \subseteq X$. Let us fix an admissible term order $\prec$. Every 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 *support*, *leading term* and the *leading coefficient* of f by $\operatorname{supp}(f) := \{t_1, \ldots, t_m\}$, $\operatorname{lt}(f) := t_1$ and $\operatorname{lc}(f) := c_1$, respectively.

The main difference between Gröbner and Pommaret bases consists in different notions of divisibility of terms. Gröbner bases are connected with the ordinary divisibility of terms, i.e. for all $u, v \in T$ we have $u \mid v$ iff there exists $s \in T$ such that $s \circ_T u = v$. Let $\sqsubset$ be an arbitrary linear order on the set X of variables. The additional requirement of the existence of an index $1 \leq i \leq n$ such that $s \in T(\{X_j \mid X_j \sqsubseteq X_i\})$ and $u \in T(\{X_j \mid X_i \sqsubseteq X_j\})$ leads to the *Pommaret divisibility with respect to* $\sqsubset$, denoted by $u \mid_{P,\sqsubset} v$. W.l.o.g. we can assume that the variables are enumerated in such a way that $X_1 \sqsubset \cdots \sqsubset X_n$ and we will use the short cut $\mid_P$ for the Pommaret divisibility with respect to this particular order.

Definition : *Let $I \subseteq R$ be an ideal, $F \subseteq I$ a subset of I and $\prec$ an admissible term order. Then F is called a* Gröbner*, resp.* Pommaret*, basis of I with respect to $\prec$ iff for every $0 \neq g \in I$ there exists $f \in F$ such that $\operatorname{lt}(f) \mid \operatorname{lt}(g)$, resp. $\operatorname{lt}(f) \mid_P \operatorname{lt}(g)$.*

Note that the definition of Pommaret bases depends on the order $\sqsubset$ of variables induced by their enumeration. Furthermore, we remark that the term order $\prec$ needs not to be compatible with $\sqsubset$. A comprehensive overview of the theory of Gröbner bases can be found e.g. in [BW93]. For the theory of Pommaret bases we refer to [ZB93] and [Ap95]. It is a well-known fact that the ordinary Gröbner basis theory is an instance of the theory of Göbner bases in graded structures (c.f. [Ro86], [Mo88]). In [Ap95] it was proved that the same holds also for Pommaret bases. While the ordinary Gröbner basis theory is based on a T-grading of the polynomial ring we have to use a S-grading of R in order to obtain the Pommaret theory. Here, S denotes the free non-commutative monoid generated by X. Let $comm : S \to S$ be the function defined by $comm(X_{i_1} X_{i_2} \cdots X_{i_m}) := X_{i_{\pi(1)}} X_{i_{\pi(2)}} \cdots X_{i_{\pi(m)}}$, where π is a permutation of $(1, 2, \ldots, m)$ such that $i_{\pi(1)} \leq i_{\pi(2)} \leq \cdots \leq i_{\pi(m)}$. Then we can consider T as a subset of S by identifying the elements of T and $\{t \mid t = comm(t)\} \subseteq S$. An order $\prec$ of S will be called an *admissible term order* if it is an irreflexive well-order of S which is compatible with the multiplication $\circ_S$ of S and satisfies the conditions $comm(t) \preceq t$ and $comm(s) \prec comm(t) \Rightarrow s \prec t$ for all $s, t \in S$.

0.3 Pommaret Bases in Graded Structures

In this section we will sketch the non-commutative grading providing exactly the Pommaret bases as the Gröbner bases of left ideals in the corresponding graded structure. In [Ap95] it was remarked that the theory of Pommaret bases can be generalized to left ideals of algebras of solvable type [KW90] without any trouble. Here, we will use the more general setting explicitly.

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 $\mathcal{K}$. S is $\mathcal{K}$-vector space basis of P. Let us fix an admissible term order $\prec$ of S for the remainder of this section. Then we can define the notions of support $\mathrm{supp}(f)$, leading word $\mathrm{lw}(f)$, and leading coefficient $\mathrm{lc}(f)$ of an element $f \in P$ with respect to $\prec$ in the same way as we did for polynomials. Note, here we use the notion "word" instead of "term" since S is isomorphic to the free word semi-group generated by X.

Let $I \subset P$ be a two-sided ideal such that for all numbers $1 \leq i < j \leq n$ there exists an element $X_jX_i - c_{i,j}X_iX_j + p_{i,j} \in I$ with $0 \neq c_{i,j} \in \mathcal{K}$ and $p_{i,j} = 0$ or $\mathrm{lw}(p_{i,j}) \prec X_iX_j$. Furthermore, we assume that for every $0 \neq f \in I$ there exists $t = X_{i_1}X_{i_2}\cdots X_{i_k} \in \mathrm{supp}(f)$ such that $i_{j+1} < i_j$ for some $1 \leq j < k$. This property corresponds to condition (H) in [KW90] and the class of all quotient algebras of P modulo a two-sided ideal I satisfying the above conditions consists exactly of the algebras of solvable type. Let $A = P/I$. The well-order property of $\prec$ ensures that the function $\mathrm{lt} : A \to S$ given by $\mathrm{lt}(f+I) := \min\{\mathrm{lw}(g) \mid g - f \in I\}$ is well-defined for all residue classes $f + I \neq I$. Since lt satisfies the conditions $a + b = 0 \vee \mathrm{lt}(a+b) \preceq \max(\mathrm{lt}(a), \mathrm{lt}(b))$ and $\mathrm{lt}(ab) \preceq \mathrm{lt}(a) \circ_S \mathrm{lt}(b)$ for all non-zero elements $a, b \in A$ the family $\left(\mathcal{F}_S^{(u)}\right)_{u\in S}$, where $\mathcal{F}_S^{(u)} := \{a \in A \mid \mathrm{lt}(a) \preceq u\} \cup \{0\}$, is a filtered structure. So, we can define a graded structure $\mathcal{A}_S = (A, S, \prec, \mathrm{lt})$ and associate to A a S-graded algebra $\mathcal{G}_S = \bigoplus_{u\in S}\mathcal{G}_S^{(u)}$. Here $\mathcal{G}_S^{(u)}$ denotes the quotient group of $\mathcal{F}_S^{(u)}$ by $\hat{\mathcal{F}}_S^{(u)} := \bigcup_{v\prec u}\mathcal{F}_S^{(v)}$ and the multiplication $\bullet_S$ of $\mathcal{G}_S$ is defined in the usual way. The elements of $h \in \mathcal{G}_S^{(u)}$ are called *homogeneous* of S-degree u (denotation: $\deg_S(h) = u$). The image of $f \in A$ under the function $in_S : A \to \mathcal{G}_S$ defined by $in_S(0) := 0$ and $in_S(f) := f + \hat{\mathcal{F}}_S^{(\mathrm{lt}(f))}$ for all $f \neq 0$ will be called the *initial part* (with respect to $\mathcal{A}_S$) of f. The left ideal generated in $\mathcal{G}_S$ by the set $in_S(F)$ of all initial parts of elements of $F \subseteq A$ will be denoted by $LIn_S(F)$. The image of A under the mapping in_S is the set $\bigcup_{u\in S}\mathcal{G}_S^{(u)}$ of all homogeneous elements. Therefore, we can fix a function $in_S^* : \bigcup_{u\in S}\mathcal{G}_S^{(u)} \to A$ such that $in_S(in_S^*(h)) = h$ for all homogeneous elements $h \in \mathcal{G}_S$.

Definition : *Let $F \subseteq J$ be a subset of the left ideal $J \subseteq A$. Then F is called a* Gröbner basis of J with respect to the graded structure $\mathcal{A}_S = (A, S, \prec, \mathrm{lt})$ *iff $LIn_S(F) = LIn_S(J)$.*

In the particular case $c_{i,j} = 1$ and $p_{i,j} = 0$ for all $1 \leq i < j \leq n$ the ring A is isomorphic to the polynomial ring $R = \mathcal{K}[X]$ and the definitions of lt given here and in Section 0.2 coincide when A and R are identified under the natural isomorphism. Hence, the following notion is a straight forward generalization of the Pommaret bases of polynomial ideals defined in Section 0.2.

Definition : *Let A be an algebra of solvable type, $J \subseteq A$ a left ideal, $F \subseteq J$ a subset, $\prec_T$ an admissible term order of T, and $\sqsubset$ a linear order of the set of variables X. F is called a* Pommaret basis of J with respect to $\prec_T$ and $\sqsubset$ *iff for any non-zero $g \in J$ there exists $f \in F$ such that* $\mathrm{lt}(f) \mid_{P,\sqsubset} \mathrm{lt}(g)$.

Figure 0.1: Pommaret basis semi-algorithm

Input: $A \cdots$ algebra of solvable type
$\prec \cdots$ admissible term order of S
Basis $F = \{f_1, \ldots, f_m\} \subset A \backslash \{0\}$ of the left ideal J
Output: Pommaret basis G of J.

$l := m$
$g_i := f_i/\mathrm{lc}(f_i)$ for $1 \leq i \leq l$
$G := \{g_1, \ldots, g_l\}$
$B := \left\{X_i \bullet_S e_{in_S(g_j)} \mid 1 \leq i \leq n, 1 \leq j \leq l, \mathrm{lt}(g_j) \notin T(X_i, \ldots, X_n)\right\}$
$\quad \cup \left\{u \bullet_S e_{in_S(g_j)} - e_{in_S(g_i)} \mid 1 \leq i \neq j \leq l, \mathrm{lt}(g_j) \mid_P \mathrm{lt}(g_i), u = \frac{\mathrm{lt}(g_i)}{\mathrm{lt}(g_j)}\right\}$
while $B \neq \emptyset$ **do**
  choose $s \in B$ w.r.t. a fair selection strategy
  $B := B \backslash \{s\}$
  $f := PNF(c(s), G)$
  if $f \neq 0$ **then**
    $l := l + 1$
    $g_l := f/\mathrm{lc}(f)$
    $G := G \cup \{g_l\}$
    $B := B \cup \left\{X_i \bullet_S e_{in_S(g_l)} \mid \mathrm{lt}(g_l) \notin T(X_i, \ldots, X_n)\right\}$
    $\quad \cup \left\{u \bullet_S e_{in_S(g_l)} - e_{in_S(g_i)} \mid 1 \leq i < l, \mathrm{lt}(g_l) \mid_P \mathrm{lt}(g_i), u = \frac{\mathrm{lt}(g_i)}{\mathrm{lt}(g_l)}\right\}$

Let $\iota : T \to S$ be the natural set embedding identifying the commutative terms with the non-commutative words belonging to the image of the above defined function *comm*. Then for any $u, v \in T$ we have $u \mid_P v$ if and only if $\iota(u)$ is a postfix of $\iota(v)$. Therefore, the Pommaret divisibility (with respect to the variable order $X_1 \sqsubset \cdots \sqsubset X_n$) and the postfix relation on the image $im(comm)$ of the *comm*-mapping can be identified in a natural way. From this and some well-known properties of Gröbner bases in graded structures we deduce the following equivalence.

Theorem 1 ([Ap95, Theorem 4.1]) *Let $\mathcal{A}_S = (A, S, \prec, \mathrm{lt})$ be the above defined graded structure of the algebra A of solvable type. Furthermore, let $J \subseteq A$ be a left ideal of A and $G \subseteq J$ a subset of this left ideal. Then G is a Gröbner basis of J with respect to $\mathcal{A}_S$ if and only if G is a Pommaret basis of J with respect to $\prec_T$ and $\sqsubset$, where $X_1 \sqsubset \cdots \sqsubset X_n$ and $\prec_T$ denotes the restriction of $\prec$ to $T = im(comm)$.*

Since $X_i \sqsubset X_j \iff X_i \circ_S X_j \prec X_j \circ_S X_i$ the graded structure $\mathcal{A}_S$ carries not only the information on the restricted order $\prec_T$ but also that on the variable order $\sqsubset$. Generalizing the definition of *comm* it is easy to construct a graded structure $\mathcal{A}_{S,\sqsubset}$ where the postfix relation of elements of $im(comm)$ corresponds to $\mid_{P,\sqsubset}$ and, consequently, Gröbner bases with respect to $\mathcal{A}_{S,\sqsubset}$ coincide with Pommaret bases with respect to $\prec_T$ and $\sqsubset$. Gröbner reduction with respect to $\prec$ modulo I provides a canonical simplifier of the residue class ring $A = P/I$. By this means the elements are represented in terms of the Poincaré-Birkhoff-Witt basis of the solvable algebra A which consists of the elements of $im(comm)$. It might seem that the variable order $\sqsubset$ defining the Pommaret divisibility and the Poincaré-Birkhoff-Witt basis in which the elements of A are represented depend on each other via the graded structure $\mathcal{A}_{S,\sqsubset}$. Since changing the Poincaré-Birkhoff-Witt basis may heavily influence the size of the representation of a given element we emphasize that there is neither a theoretical nor a practical necessity to use the above canonical simplifier. Any effective representation of A will be suitable, one has only to take care about the correct computation of the function lt.

The method for the computation of Pommaret bases in algebras of solvable type presented in Figure 0.1 requires the introduction of some additional notions and denotations. Let $G = \{g_1, \ldots, g_m\} \subset A$ be a finite set of non-zero elements. Then the *critical element* of the homogeneous left syzygy $s = \sum h_i \bullet_S e_{in_S(g_i)}$ of $in_S(G)$ is defined by $c(s) := \sum in_S^*(h_i) g_i$. We say that $\bar{f} \in A$ is *Pommaret irreducible* modulo G if $\mathrm{lt}(g_i) \nmid_P u$ for all $u \in \mathrm{supp}(\bar{f})$ and $i = 1, \ldots, m$. An element $\bar{f}$ which is Pommaret irreducible modulo G will be called a (left) *Pommaret normal form* of $f \in A$ in terms of G (denotation $\bar{f} = PNF(f, G)$) if there exist $c_1, \ldots, c_l \in \mathcal{K}\backslash\{0\}$, $u_1, \ldots, u_l \in T$ and $g_{i_1}, \ldots, g_{i_l} \in G$ such that $\mathrm{lt}(u_1 g_{i_1}) = u_1 \circ_S \mathrm{lt}(g_{i_1}) \prec \cdots \prec \mathrm{lt}(u_l g_{i_l}) = u_l \circ_S \mathrm{lt}(g_{i_l})$ and $f - \bar{f} = \sum_{i=1}^{l} c_j u_j g_{i_j}$.

Next, we will sketch the correctness and termination proof of the method presented in Figure 0.1. $\mathcal{A}_S$ is a (left-) effective graded structure. Hence, all instructions of Method 0.1 are effective computable. The correctness of the method follows from the theory of graded structures and the fact that, roughly spoken, the left syzygies passing through B form a homogeneous basis of the left syzygy module of $in_S(G)$ (see [Ap95, Lemma 4.1]). A left syzygy selection strategy is called *fair* if it ensures that no left syzygy can stay in B for an infinite number of runs of the **while**-loop. The assumed fair selection strategy makes Method 0.1 semi-algorithmic, i.e. it terminates if and only if a finite Pommaret basis of J exists (see [Ap95]).

From the assumed properties of an admissible term order $\prec$ of S it follows that the restriction to the subset $im(comm) = T$, which for simplicity will be also denoted by $\prec$, is an admissible term order of the abealian monoid T. So, we can construct the graded structure $\mathcal{A}_T = (A, T, \prec, \mathrm{lt})$ and all associated objects in the same way as we did for $\mathcal{A}_S$. It is well-known that the Gröbner bases with respect to the graded structure $\mathcal{A}_T$ are just the classical Gröbner bases with respect to $\prec$.

0.4 An Alternative Gröbner Basis Algorithm

Mall observed that every set of monomials generating an ideal J which is in stable position with respect to an admissible term order $\prec$ is a Pommaret basis of J with respect to $\prec$ (see [Ma95]). An equivalent formulation is to say that the reduced

Pommaret and the reduced Gröbner basis of J with respect to $\prec$ are equal in this situation. Nevertheless, it is also well-known that a monomial ideal needs not to have a finite Pommaret basis, in general. However, an infinite reduced Pommaret basis has a very regular structure and starting from a Gröbner basis G it is easy to construct a Pommaret basis, e.g.

$$P = G \cup \{ug_j | g_j \in G, \exists 1 \leq i \leq n \, : \, \mathrm{lt}(g_j) \notin T(X_i, \ldots, X_n) \wedge u \in T(X_i, \ldots, X_n)\} \quad .$$

Subsequent minimalization of a so-constructed Pommaret basis is not difficult. Our subject will be the more delicate problem: How to use the regular structure in order to find a stronger termination condition for Method 0.1 ensuring that the truncated Pommaret basis computed at termination time is already an ordinary Gröbner basis of the input ideal? The phenomenon is similar to the generalized FGLM-algorithm for higher dimensions. Roughly, the conversion of a Gröbner basis to another term order by means of linear algebra requires a walk along a border basis of the ideal. In spite of the infiniteness of the border basis of a positive dimensional ideal Licciardi and Mora presented an always terminating procedure (see [LM94]).

Consider the left ideal $J \subseteq A$ generated by the set $F = \{f_1, \ldots, f_m\}$ of non-zero elements of A. Let U_S be a homogeneous minimal basis of the left ideal $LIn_S(J) \subseteq \mathcal{G}_S$. There exists a finite subset $U_T \subseteq U_S$ such that $in_T(in^*_S(U_T))$ is a homogeneous minimal basis of $LIn_T(J) \subseteq \mathcal{G}_T$. Let $u \in U_S$. According to the fair selection strategy there exists an index j_u such that the element g_{j_u} computed by Method 0.1 has the property $\mathrm{lt}(g_{j_u}) = \deg_S(u)$. Hence, it needs only a finite execution time of Method 0.2 until the value of G will contain the (ordinary) Gröbner basis $\{g_i \mid i \leq \max_{u \in U_T} j_u\}$ of J with respect to $\prec$ as a subset and, therefore, is a Gröbner basis of J with respect to $\prec$, too. But, it remains the problem to recognize that the value of G became a Gröbner basis of J. The time comparisons of Zharkov and Blinkov (c.f. [ZB93]) support the hope that a truncated Pommaret basis algorithm could be (sometimes) faster than Buchberger's algorithm. But in order to gain a fast truncated algorithm the check of the termination condition must not be very costly. For this reason, the trivial approach of checking the Gröbner basis property using Buchberger's algorithm makes no sense.

The additional costs caused by the termination condition of Figure 0.2 are reasonable low. Moreover, for the sake of lucidity we did not care about tricks leading to an efficient implementation, e.g. the degree bound needs not to be completely recomputed before every run. The notations used in the method have the following meaning. $lcm_T(u, v)$ denotes the least common multiple of $u, v \in T$ with respect to the multiplication $\circ_T$. A standard selection strategy chooses the left syzygy $s \in B$ to be considered next only among those of minimal (w.r.t. $\prec$) S-degree. Let $\omega = (\omega_1, \ldots, \omega_n)$ be a vector of positive real numbers. If $X_{i_1} \cdots X_{i_m} \prec X_{j_1} \cdots X_{j_k}$ for all $X_{i_1} \cdots X_{i_m}, X_{j_1} \cdots X_{j_k} \in S$ such that $\sum_{\nu=1}^{m} \omega_{i_\nu} < \sum_{\nu=1}^{k} \omega_{j_\nu}$ then the admissible term order $\prec$ is called *ω-degree compatible*. An important property of ω-degree compatible orders is that for any term $t \in S$ there exist

Figure 0.2: Alternative Gröbner basis algorithm

Input: $A \cdots$ algebra of solvable type
$\prec \cdots \omega$-degree compatible term order of S
Basis $F = \{f_1, \ldots, f_m\} \subset A \backslash \{0\}$ of the left ideal J
Output: Gröbner basis G of J.

$l := m$
$g_i := f_i / \mathrm{lc}(f_i)$ for $1 \leq i \leq l$
$H := \{1, \ldots, l\}$
$G := \{g_1, \ldots, g_l\}$
$B := \left\{X_i \bullet_S e_{ins_S(g_j)} \mid 1 \leq i \leq n, 1 \leq j \leq l, \mathrm{lt}(g_j) \notin T(X_i, \ldots, X_n)\right\}$
$\cup \left\{u \bullet_S e_{ins_S(g_j)} - e_{ins_S(g_i)} \mid 1 \leq i \neq j \leq l, \mathrm{lt}(g_j) \mid_P \mathrm{lt}(g_i), u = \frac{\mathrm{lt}(g_i)}{\mathrm{lt}(g_j)}\right\}$
while $\exists s \in B : comm(\deg_S(s)) \preceq \max_{i,j \in H} (lcm_T(\mathrm{lt}(g_i), \mathrm{lt}(g_j)))$ **do**
choose $s \in B$ w.r.t. a standard selection strategy
if $s = u \bullet_S e_{ins_S(g_j)} - e_{ins_S(g_i)}$ and $m < i$ **then** $H := H \backslash \{i\}$
$B := B \backslash \{s\}$
$f := PNF(c(s), G)$
if $f \neq 0$ **then**
$l := l + 1$
$g_l := f / \mathrm{lc}(f)$
$G := G \cup \{g_l\}$
$B := B \cup \left\{X_i \bullet_S e_{ins_S(g_l)} \mid \mathrm{lt}(g_l) \notin T(X_i, \ldots, X_n)\right\}$
$\cup \left\{u \bullet_S e_{ins_S(g_l)} - e_{ins_S(g_i)} \mid 1 \leq i < l, \mathrm{lt}(g_l) \mid_P \mathrm{lt}(g_i), u = \frac{\mathrm{lt}(g_i)}{\mathrm{lt}(g_l)}\right\}$
if $\mathrm{lt}(g_l) \prec comm(\deg_S(s))$ **then** $H := H \cup \{l\}$

only finitely many terms $s \in S$ satisfying $s \prec t$. As a simple consequence we have that standard selection strategies for choosing left syzygies are fair for ω-degree compatible term orders.

The following theorems show that the termination condition is weak enough to ensure the Gröbner basis property of the output and strong enough to ensure termination at least in the case of ω-degree compatible admissible term orders.

Theorem 2 *The value of G at termination time of Method 0.2 is an (ordinary) Gröbner basis of the input left ideal J with respect to the input term order $\prec$.*

Proof: Assume that the execution of Method 0.2 terminates for input A, $\prec$ and F. In the following all references to variables occurring in the algorithm will concern their value at termination time.

First of all, we introduce some notations. Set $\tau(i,j) := lcm_T(\mathrm{lt}(g_i), \mathrm{lt}(g_j))$ and $\tau := \max_{i,j \in H} \tau(i,j)$. By $J^{(G',t)}$ we denote the subset of J consisting of 0 and all elements f which can be represented in the form $f = \sum_{j=1}^{k} h_j g_{i_j}$, where

$h_1, \ldots, h_k \in A\backslash\{0\}$, $g_{i_1}, \ldots, g_{i_k} \in G'$ and $\mathrm{lt}(h_j g_{i_j}) \prec t$ for all $j = 1, \ldots, k$. Furthermore, let $G_H := \{g_i \in G \mid i \in H\}$.

There are two possibilities for $1 \leq i \leq l$ and $i \notin H$. *(i)* i was removed from H in connection with the treatment of a syzygy of type $u \bullet_S e_{in_S(g_j)} - e_{in_S(g_i)}$ and since $i > m$ we have $u \notin \mathcal{K}$. *(ii)* i was not inserted into H because of $comm(\deg_S(s)) \preceq \mathrm{lt}(g_i)$, where s is the syzygy from which g_i was produced. From $\mathrm{lt}(g_i) \preceq \mathrm{lt}(c(s)) \prec \deg_S(s)$ it follows $\mathrm{lt}(g_i) = \mathrm{lt}(c(s)) = comm(\deg_S(s))$. Hence, s must be of the type $X_k \bullet_S e_{in_S(g_j)}$ and $\mathrm{lt}(g_i) = X_k \circ_T \mathrm{lt}(g_j)$. In both cases it follows the existence of $1 \leq j \leq l$ and $h \in A\backslash\mathcal{K}$ such that $g_i + hg_j \in J^{(G,\mathrm{lt}(g_i))}$. Applying an inductive argument on $\mathrm{lt}(g_i)$ yields the existence of $j' \in H$ and $h' \in A\backslash\mathcal{K}$ satisfying $g_i + h' g_{j'} \in J^{(G_H,\mathrm{lt}(g_i))}$. Consequently,

$$J^{(G,t)} = J^{(G_H,t)} \text{ for all } t \in T \tag{0.1}$$

and, therefore, G is an ordinary Gröbner basis of J if and only if G_H has this property. In order to prove that G_H is a Gröbner basis, it is sufficient to show

$$s(i,j) := c_{i,j} u_{i,j} g_i - d_{i,j} v_{i,j} g_j \in J^{(G_H,\tau(i,j))} \tag{0.2}$$

for all $i, j \in H$, where $u_{i,j}, v_{i,j} \in T$ are such that $\mathrm{lt}(u_{i,j} g_i) = \mathrm{lt}(v_{i,j} g_j) = \tau(i,j)$ and $c_{i,j} := \mathrm{lc}(v_{i,j} g_j), d_{i,j} := \mathrm{lc}(u_{i,j} g_i)$. Before we prove the relations 0.2 we sketch how they together with some well-known facts imply the Gröbner basis property of G_H. The elements $s(i,j)$ are exactly the critical elements, which Buchberger called S-polynomials in the case of polynomial rings A. Hence, G_H is a Gröbner basis of the left ideal it generates if and only if any of these finitely many critical elements can be represented in the form $s(i,j) = \sum_{k \in H} h_k g_k$, where $h_k = 0$ or $\mathrm{lt}(h_k g_k) \prec \tau_{i,j}$ for all $k \in H$. This means exactly that condition 0.2 has to be satisfied for any pair $(i,j) \in H \times H$.

Now, we are going to prove 0.2. If $1 \leq i \leq l$ and $1 \leq j \leq n$ are such that $\mathrm{lt}(g_i) \notin T(X_j, \ldots, X_n)$, and $\mathrm{lt}(X_j g_i) \preceq \tau$ then the left syzygy $X_j \bullet_S e_{in_S(g_i)}$ had been considered during the execution of Method 0.2. Hence, there exist $g_{l_{i,j}} \in G$ and $h_{i,j} \in A$ such that $\mathrm{lt}(g_{l_{i,j}}) \mid_P \mathrm{lt}(X_j g_i)$ and

$$p(i,j) := X_j g_i + h_{i,j} g_{l_{i,j}} \in J^{(G,\mathrm{lt}(X_j g_i))} \quad . \tag{0.3}$$

Let $1 \leq i, j \leq l$ satisfy $\mathrm{lt}(g_j) \mid_P \mathrm{lt}(g_i)$ and $\mathrm{lt}(g_i) \preceq \tau$. In the same way as above we deduce the existence of $f_{i,j} \in A$ such that

$$q(i,j) := g_i + f_{i,j} g_j \in J^{(G,\mathrm{lt}(g_i))} \quad . \tag{0.4}$$

Next we prove that for all $g_i \in G$ and $u \in T$ such that $\mathrm{lt}(ug_i) \preceq \tau$ there exists an element $r(i,u) \in J^{(G,\mathrm{lt}(ug_i))}$ having a representation

$$r(i,u) = ug_i + k_{i,u} g_{m_{i,u}} \quad , \tag{0.5}$$

where $k_{i,u} \in A$, $1 \leq m_{i,u} \leq l$, $\mathrm{lt}(g_{m_{i,u}}) \mid_P \mathrm{lt}(ug_i)$ and $\mathrm{lt}(g_j) \nmid_P \mathrm{lt}(ug_i)$ for all $1 \leq j < m_{i,u}$.

Let $v(i,u)$ be the longest prefix of u such that $\mathrm{lt}(g_i) \mid_P \mathrm{lt}(v(i,u)g_i)$ and let $w(i,u)$ be the corresponding postfix of u, i.e. $u = v(i,u) \circ_S w(i,u)$. We will show the existence of an element $r(i,u)$ by induction on the length of $w(i,u)$. So, first consider the case $length(w(i,u)) = 0$, i.e. $w(i,u) = 1$. If $\mathrm{lt}(g_j) \nmid_P \mathrm{lt}(ug_i)$ for all $1 \le j < i$ then $r(i,u) := ug_i - ug_i = 0$ satisfies the conditions of (0.5). Otherwise, let $1 \le j < i$ be minimal with the property $\mathrm{lt}(g_j) \mid_P \mathrm{lt}(ug_i) = u \circ_S \mathrm{lt}(g_i)$. In this case $\mathrm{lt}(g_j) \mid_P \mathrm{lt}(g_i)$ or $\mathrm{lt}(g_i) \mid_P \mathrm{lt}(g_j)$. If $\mathrm{lt}(g_j) \mid_P \mathrm{lt}(g_i)$ then $r(i,u) := uq(i,j) = ug_i + (uf_{i,j})g_j$, where $q(i,j)$ is of type (0.4), satisfies the conditions of (0.5). The case $\mathrm{lt}(g_i) \mid_P \mathrm{lt}(g_j)$ can be handled in a similar way. Now, consider the case $w(i,u) \neq 1$. We decompose $u = u' \circ_S X_j = v(i,u) \circ_S w' \circ_S X_j$ and consider the element $u'p(i,j) = ug_i + u'h_{i,j}g_{l_{i,j}} \in J^{(G,\mathrm{lt}(ug_i))}$, where $p(i,j)$ is of type (0.3). We observe that $w\left(l_{i,j}, \mathrm{lt}\left(u'h_{i,j}\right)\right)$ must be shorter than $w(i,u)$ since it is a subword of w'. Hence, by induction assumption there exists $r\left(l_{i,j}, \mathrm{lt}\left(u'h_{i,j}\right)\right)$ and $r(i,u) := u'p(i,j) - \mathrm{lc}\left(u'h_{i,j}\right) \cdot r\left(l_{i,j}, \mathrm{lt}\left(u'h_{i,j}\right)\right) \in J^{(G,\mathrm{lt}(ug_i))}$ is of type (0.5).

Let $i,j \in H$ and $f := s(i,j) - c_{i,j}r(i,u_{i,j}) + d_{i,j}r(j,v_{i,j})$, where $s(i,j)$ is of type (0.2) and $r(i,u_{i,j})$ and $r(j,v_{i,j})$ are of type (0.5). Simplification of the sum shows $f = hg_\mu$ for some $h \in A$ and $\mu := m_{i,u_{i,j}} = m_{j,v_{i,j}}$. Furthermore, from $r(i,u_{i,j}), r(j,v_{i,j}) \in J^{(G,\tau(i,j))}$ and $s(i,j) = 0$ or $\mathrm{lt}(s(i,j)) \prec \tau(i,j)$ we deduce $f = 0$ or $\mathrm{lt}(f) = \mathrm{lt}(hg_\mu) \prec \tau(i,j)$. So, in any case we have $f = hg_\mu \in J^{(G,\tau(i,j))}$ and it follows $s(i,j) = f + c_{i,j}r(i,u_{i,j}) - d_{i,j}r(j,v_{i,j}) \in J^{(G,\tau(i,j))}$. Finally, using 0.1 we conclude the validity of membership 0.2. $\square$

Theorem 3 *Method 0.2 terminates for any A, $\prec$ and F satisfying the input specification.*

Proof: Let G_μ be the value of G, H_μ the value of H, and B_μ the value of B before the μ-th run of the **while**-loop. By fairness of the selection strategy there exists μ_0 such that G_μ is an ordinary Gröbner basis of J for all $\mu \geq \mu_0$.

Assume that there exists $k \in H_{\mu+1} \backslash H_\mu$ for some $\mu > \mu_0$. Since G_μ is a Gröbner basis of J the set $D := \{g_i \in G_\mu | \exists u \in T : u \circ_T \mathrm{lt}(g_i) = \mathrm{lt}(g_k)\}$ is not empty. Let g_j be the element of D whose leading term with respect to $\prec$ is maximal with respect to the lexicographical order extending $X_1 \prec_{lex} \cdots \prec_{lex} X_n$ and let $1 \le i_1 \le \cdots \le i_m \le n$ be such that $X_{i_1} \cdots X_{i_m} \circ_T \mathrm{lt}(g_j) = \mathrm{lt}(g_k)$. Let $s \in B_\mu \backslash B_{\mu+1}$ be the left syzygy used for the construction of g_k. We have $\mathrm{lt}(X_{i_m} g_j) \preceq \mathrm{lt}(g_k) \prec comm(\deg_S(s))$. According to the applied standard selection strategy the left syzygy $X_{i_m} \bullet_S e_{in(g_j)}$ had to be considered before s, therefore, $PNF(X_{i_m} g_j, G_\mu) = 0$. Hence, there exist $g_i \in G_\mu$ and $v \in T$ such that $v \circ_S \mathrm{lt}(g_i) = X_{i_m} \circ_T \mathrm{lt}(g_j)$. But $v \in T(X_1, \ldots, X_{i_m - 1})$ contradicts the maximal choice of g_j and $v \notin T(X_1, \ldots, X_{i_m - 1})$ implies $\mathrm{lt}(g_i) \mid_P \mathrm{lt}(g_k)$ in contradiction to the construction of g_k. Consequently, $H_\mu \subseteq H_{\mu_0}$ and

$$\max_{i,j \in H_\mu} \left(lcm_T(\mathrm{lt}(g_i), \mathrm{lt}(g_j))\right) \preceq \max_{i,j \in H_{\mu_0}} \left(lcm_T(\mathrm{lt}(g_i), \mathrm{lt}(g_j))\right) =: \tau$$

for all $\mu \geq \mu_0$.

Let U be a homogeneous minimal basis of $LIn_S(J)$. Since $\prec$ is ω-degree compatible the subset $U_\tau = \{u \in U | \deg_S(u) \preceq \tau\}$ is finite. Hence, the fair selection strategy ensures the existence of ν_0 such that $\mathcal{G}_S \cdot U_\tau \subseteq LIn_S(G_\nu)$ for all $\nu \geq \nu_0$. Therefore, $PNF(f, G_\nu) = 0$ for all $\nu \geq \nu_0$ and $f \in J$ such that $\mathrm{lt}(f) \preceq \tau$. Consequently, no left syzygy s with $comm(\deg_S(s)) \preceq \tau$ will be added to B after the ν_0-th run of the **while**-loop. In conclusion, the fairness of the selection strategy implies the termination of the algorithm. □

0.5 Concluding Remarks

Note, that the correctness of Algorithm 0.2 will be valid even for arbitrary admissible term orders and arbitrary selection strategies. However, the following discussion shows that our restrictions have an essential influence on the termination behaviour.

A first remark concerns term orders which are not ω-degree compatible, e.g. lexicographical orders. The reduced Pommaret basis can contain infinitely many basis elements whose leading terms are smaller than the maximal leading term of the elements of the reduced Gröbner basis. Hence, in general Method 0.2 will not terminate for such orders since all these elements had to be contained in G at termination time.

The following example illustrates that the use of a standard selection strategy is essential. Consider $G = \{Z^3 - Y^2Z, XYZ^2 + XY^2Z\}$ and the ideal $I \subset \mathcal{K}[X, Y, Z]$ generated by G. Terms are ordered first with respect to the total degree and lexicographical according to $X \prec Y \prec Z$ within the same degree. Then G is the reduced Gröbner basis and $G \cup \{XY^kZ^2 + XY^{k+1}Z | k = 2, 3, \ldots\}$ the reduced Pommaret basis of I with respect to $\prec$. If we use a selection strategy choosing $s \in B$ such that $i + 3j + k$, where $comm(\deg_S(s)) = X^iY^jZ^k$, is minimal then Method 0.2 will not terminate though the selection strategy is fair. Probably, the restriction to only standard selection strategies is to strong. The most important open question is the behaviour of sugar strategies.

The last remark concerns the definition of H. In general, we would loose termination for setting H such that $G_H = G$ and correctness for H defined such that $in(G_H)$ is minimal generating set of $LIn_T(G)$. But termination will be preserved also if we alter the algorithm by skipping the step where elements of H can be removed. At the one hand side sometimes the number of investigated critical elements can be reduced by shrinking H. At the other hand side the overhead caused by the termination condition becomes smaller without the step. If the leading terms of the elements $f_1, \ldots, f_m$ are made pairwise different during a preparatorily step then the additional condition $m < i$ for deleting i from H is not necessary.

Bibliography

[Ap95] Apel, J. (1995). A Gröbner Approach to Involutive Bases. *J.Symb.Comp.* **19**/5, pp. 441–457.

[BW93] Becker, T., Weispfenning, V., in cooperation with Kredel, H. (1993). Gröbner Bases, A Computational Approach to Commutative Algebra. Springer, New York, Berlin, Heidelberg.

[Bu65] Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. Thesis, Univ. Innsbruck.

[GB95] Gerdt, V.P., Blinkov, Yu.A. (1995). Bases Involutives de Polynômes. LIFL USTL, Preprint IT-95-271, Lille.

[KW90] Kandri-Rody, A., Weispfenning, V. (1990). Non-Commutative Gröbner Bases in Algebras of Solvable Type. *J.Symb.Comp.* **9**/1, pp. 1–26.

[Ja29] Janet, M. (1929). Lecons sur les systèmes d'equations aux dérivées partielles. Gauthier-Villars, Paris.

[LM94] Licciardi, S., Mora, T. (1994). Implicitization of Hypersurfaces and Curves by the Primbasissatz and Basis Conversion. Proc. ISSAC'94, ACM-Press, pp 191–196.

[MR93] Madlener, K., Reinert, B. (1993). Computing Gröbner Bases in Monoid and Group Rings. Proc. ISSAC'93, ACM-Press, pp 254–263.

[Ma95] Mall, D. (1995). A Note on Pommaret Bases. submitted to J.Symb.Comp.

[Mo88] Mora, T. (1988). Seven Variations on Standard Bases. Preprint, Univ. di Genova, Dip. di Mathematica, N. 45.

[Po78] Pommaret, J.F. (1978). Systems of Partial Differential Equations and Lie Pseudogroups. Gordan and Breach, New York.

[Ro86] Robbiano, L. (1986). On the Theory of Graded Structures. *J. Symb. Comp.* **2**, pp. 139–170.

[GS95] Garcia-Sanchez, P.A. (1995). Gröbner and Involutive Bases for Zero-dimensional Ideals. SIGSAM Bulletin **29**/2, pp.12–15.

[ZB93] Zharkov, A.Yu., Blinkov, Yu.A. (1993). Involution Approach to Solving Systems of Algebraic Equations. Proc. IMACS'93, pp. 11–16.