Effective Gröbner Structures

Joachim Apel
Institut für Informatik, Universität Leipzig, Germany

Abstract

Since Buchberger introduced the theory of Gröbner bases in 1965 it has become one of the most important tools in constructive algebra and, nowadays, it is the kernel of many algorithms in the theory of polynomial ideals and algebraic geometry. Motivated by the results in polynomial rings there have been investigated a lot of possibilities to generalise Buchberger's ideas to other types of rings. The perhaps most general concept, though it does not cover all extensions reported in the literature, is the extension to graded structures due to Robbiano and Mora. But in order to obtain algorithmic solutions for the computation of Gröbner bases it needs additional computability assumptions. The subject of this paper is the presentation of some classes of effective graded structures.

1 Introduction

Buchberger's algorithm for the computation of Gröbner bases has become a central tool in the field of constructive commutative algebra and algebraic geometry during the last three decades (c.f. [Bu65],[Bu85],[BW93],[AL94]). Motivated by the achievements in polynomial rings many efforts have put towards generalisations of the Gröbner theory to other types of rings.

The concept of graded structures due to Robbiano (see [Ro86]) and Mora (see [Mo88a]) provides an excellent frame for investigating Gröbner bases in very general situations. What remains to do in a concrete application is to verify a series of computability conditions which have to be fulfilled in order to obtain not only existential statements on Gröbner bases but also constructive results such as decidability of the ideal membership problem or the computability of finite generating sets of syzygy modules.

The subject of this paper is to describe large classes of effective Gröbner structures, i.e. such graded structures which allow the algorithmic computation of Gröbner bases.

Important examples for classes of rings covered by Theorem 1 and Theorem 2 are, for instance, the polynomial rings in finitely many indeterminates over effective fields (see [Bu65]) or over effective principal ideal domains (see [KK84],[Pa85]) or, even more general, over commutative rings in which linear equations are solvable (see [Tr78],[Za78],[Sch79],[Mö88],[BW93],[AL94]), the algebras of solvable type (see [KW90]), the G-algebras (see [Ap92]), or the solvable polynomial rings (see [Kr92]). A first advantage of our approach is that different generalisations are combined and further generalised. So, e.g., also algebras of solvable type over effective non-commutative rings in which linear equations are solvable are covered. A second advantage is that we obtain subclasses of effective graded structures which are closed under adjunction of effective noetherian well-ordered monoids as well as under quotients modulo two-sided ideals. As a consequence membership decision and left syzygy problems of finitely generated left modules can be reduced to left ideal problems using Nagata's principle of idealisation (see [Na62], [Ap92]).

A different approach in the two-sided case is described in Theorem 3. There are investigated graded structures which allow the computation of two-sided but not necessarily of one-sided Gröbner bases. The most important classical examples for these effective two-sided Gröbner structures are the non-commutative algebras investigated by Mora in [Mo88b].

The paper is organised as follows. In Section 2 we present a short introduction into the theory of graded structures. Section 3 deals with conditions ensuring an effective associated graded ring with decidable membership problem for homogeneous ideals. In Section 4 we describe a very general class of effective left Gröbner structures. Finally, Section 5 presents two classes of effective two-sided Gröbner structures.

2 Graded structures

Let R be a ring with unit element and $(\Gamma, \prec)$ a well-ordered monoid. Let ϵ denote the unit element of Γ and note the well-known fact that ϵ is the minimal element of Γ with respect to $\prec$. Finally, let $\varphi : R \setminus \{0\} \to \Gamma$ be a Γ-pseudo valuation function, i.e. it satisfies

$$\begin{aligned} \varphi(u) &= \epsilon \\ a+b \neq 0 &\implies \varphi(a+b) \preceq \max(\varphi(a), \varphi(b)) \\ ab \neq 0 &\implies \varphi(ab) \preceq \varphi(a) \circ \varphi(b) \end{aligned}$$

for all invertible elements $u \in R$ and all non-zero elements $a, b \in R$. For each $\gamma \in \Gamma$ the set $\mathcal{F}_\gamma = \{a \mid \varphi(a) \preceq \gamma\} \cup \{0\}$ is an additive subgroup of R and it is easy to prove that the family $\mathfrak{F} = (\mathcal{F}_\gamma)_{\gamma\in\Gamma}$ is a filtration of R. For each $\gamma \in \Gamma$ we define the quotient $G_\gamma = \mathcal{F}_\gamma / \widehat{\mathcal{F}}_\gamma$ of $\mathcal{F}_\gamma$ by its subgroup $\widehat{\mathcal{F}}_\gamma = \{0\} \cup \bigcup_{\gamma' \prec \gamma} \mathcal{F}_{\gamma'}$. For $a \in \mathcal{F}_\gamma$ we introduce the denotation $[a]_{\widehat{\mathcal{F}}_\gamma}$ for the residue class $a + \widehat{\mathcal{F}}_\gamma \in G_\gamma$. The equation

$$\forall a, b \in R \setminus \{0\} \ : \ [a]_{\widehat{\mathcal{F}}_{\varphi(a)}} [b]_{\widehat{\mathcal{F}}_{\varphi(b)}} = [ab]_{\widehat{\mathcal{F}}_{\varphi(a)\circ\varphi(b)}}$$

determines a multiplication which makes the direct sum $G = \bigoplus_{\gamma\in\Gamma} G_\gamma$ a Γ-graded ring with unit element $[1]_{\widehat{\mathcal{F}}_\epsilon}$. G with this multiplication is called the associated graded ring of the filtered structure $(R, \mathfrak{F})$. The elements $u \in G_\gamma$ are homogeneous of degree γ (denotation $\deg(u) = \gamma$). R and G are connected via the function $\text{in} : R \to G$ assigning each element $a \in R$ its initial term $\text{in}(a) = [a]_{\widehat{\mathcal{F}}_{\varphi(a)}}$ (by definition $\text{in}(0) = 0$). Let $\hat{G} = \bigcup_{\gamma\in\Gamma} G_\gamma$ denote the set of all homogeneous elements of G and $\text{in}^* : \hat{G} \to R$ an arbitrary section of in, i.e. $\text{in}(\text{in}^*(u)) = u$ for all homogeneous elements $u \in G$.

Definition 1 *With the above notation we call* $\mathfrak{R} = (R, \Gamma, \varphi, G, \text{in}, \text{in}^*)$ *a* graded structure. *Furthermore, a set $F \subset R$ is called a left (right,two-sided) Gröbner basis of the left (right,two-sided) ideal I generated by F if* $\text{in}(F)$ *and* $\text{in}(I)$ *generate the same left (right,two-sided) ideal of G.*

Note, that the definition of graded structures introduced by Robbiano and Mora (see [Ro86], [Mo88a]) consists only of the quintuple $(R, \Gamma, \varphi, G, \text{in})$. Investigating the computability of Gröbner bases it is preferable to include the function in^* in the definition.

Definition 2 *A graded structure* $\mathfrak{R} = (R, \Gamma, \varphi, G, \text{in}, \text{in}^*)$ *is called an* effective left (right) Gröbner structure *if the following conditions are satisfied:*

i) the rings with unit element R and G and the ordered monoid Γ are effective algebraic structures,

ii) φ, in *and* in^* *are computable functions,*

iii) the membership problem of homogeneous left (right) ideals of G given by an arbitrary finite homogeneous generating set is decidable,

iv) for any finite set $H \subset G$ of homogeneous elements there can be computed a finite homogeneous generating set of the left (right) syzygy module of H, and

v) G is a left (right) noetherian ring.

Before, we consider the two-sided case we will briefly discuss the syzygy problem of two-sided ideals. Let U denote the subring of G generated by the unit element $[1]_{\widehat{\mathcal{F}}_\epsilon}$. G is U-left and U-right module, so the tensor product $G \otimes_U G$ is a well-defined U-bimodule. In the following we consider $G \otimes_U G$ with its natural G-bimodule structure. Let $H = \{h_1, \ldots, h_k\} \subset G$ be a finite subset of G and $S_H : (G \otimes_U G)^k \to G$ be the G-bimodule homomorphism defined by $S_H\left(\sum_{j=1}^m a_j e_{i_j} b_j\right) = \sum_{j=1}^m a_j h_{i_j} b_j$, where $1 \le i_j \le k$ and $a_j e_{i_j} b_j$ denotes the tensor $a_j \otimes b_j$ belonging to the i_j-th copy of $G \otimes_U G$. For any H the kernel $ker(S_H)$ forms a G-submodule of $(G \otimes_U G)^k$ which is called the syzygy module $Syz(H)$ of H. Even for noetherian rings G the G-bimodule $(G \otimes_U G)^k$ will not be noetherian, in general. Therefore, a straight forward generalisation of condition *iv)* is unacceptable. Mora solved the problem by asking for the computability of a finite homogeneous non-trivial generating set of $Syz(H)$ (see [Mo88a]). A homogeneous syzygy $\sum_{j=1}^m a_j e_{i_j} b_j \in Syz(H)$ is called trivial if the element $lift_F\left(\sum_{j=1}^m a_j e_{i_j} b_j\right) = \sum_{j=1}^m \text{in}^*(a_j) f_{i_j} \text{in}^*(b_j)$ can be reduced to zero modulo F for any subset $F = \{f_1, \ldots, f_k\} \subset R$ such that $\text{in}(f_i) = h_i$ for all $i = 1, \ldots, k$.

If B together with the trivial syzygies of H generates the syzygy module $Syz(H)$ then B is called a non-trivial generating set of $Syz(H)$. The subring $A \subseteq G$ generated by the initial terms $\text{in}(a)$ of the elements a of the centre of R is contained in the centre of G. Let $\tau : (G \otimes_U G)^k \to (G \otimes_A G)^k$ be the natural G-bimodule homomorphism. Then all syzygies belonging to the intersection $ker(\tau) \cap Syz(H)$ are trivial and we can modify condition *iv)* by requiring the computability of a finite homogeneous generating set of $\tau(Syz(H))$. Finally, we define

Definition 3 *A graded structure* $\mathfrak{R} = (R, \Gamma, \varphi, G, \text{in}, \text{in}^*)$ *is called an* effective two-sided Gröbner structure *if the following conditions are satisfied:*

i) the rings with unit element R *and* G *and the ordered monoid* Γ *are effective algebraic structures,*

ii) φ, in *and* in^* *are computable functions,*

iii) the membership problem of homogeneous two-sided ideals of G *given by an arbitrary finite homogeneous generating set is decidable,*

iv) for any finite set $H \subset G$ *of homogeneous elements there can be computed a finite homogeneous generating set of* $\tau(Syz(H))$*, and*

v) G *satisfies the ascending chain condition for two-sided ideals.*

Let $\mathfrak{R} = (R, \Gamma, \varphi, G, \text{in}, \text{in}^*)$ be an effective left (right, two-sided) Gröbner structure. Then for any finite subset $F \subset R$ there can be computed a left (right, two-sided) Gröbner basis of the left (right, two-sided) ideal of R generated by F in an algorithmic way (see [Mo88a]).

The above fact is the motivation for investigating sufficient conditions for effective Gröbner structures.

3 General conditions

Let $\mathfrak{R} = (R, \Gamma, \varphi, G, \text{in}, \text{in}^*)$ be a graded structure. First obvious necessary conditions for the effectiveness of $\mathfrak{R}$ are:

Assumption 1 R *and* $(\Gamma, \prec)$ *are effective algebraic structures.* φ *is a computable function.*

Let us consider the structure of the associated graded ring G. Denote the direct summand $G_\epsilon = \mathcal{F}_\epsilon / \widehat{\mathcal{F}}_\epsilon$ of G consisting of all homogeneous elements of degree ϵ by Q. Q with the restricted multiplication of G is a ring with unit element. Moreover, there is a natural isomorphism between Q and the subring F_ϵ of R under which we will identify $Q = G_\epsilon = \mathcal{F}_\epsilon$. Since φ is computable the domain $Q = \varphi^{-1}(\epsilon)$ is decidable and hence Q is an effective subring of the effective ring R. G as well as each direct summand G_γ of G are Q-bimodules. Simple degree considerations show that if G satisfies the conditions *iii)- v)* of an effective left (right, two-sided) Gröbner structure then the subring $Q \subset G$ with the trivial grading $\forall u \in Q \setminus \{0\} \; : \; \deg(u) = \epsilon$ will satisfy these conditions, too. Instead of using the trivial grading of Q we can consider Q as a not necessarily graded ring and reformulate *iii)* and *iv)* in terms of arbitrary ideals rather than only homogeneous.

If the ring Q is commutative then the decision of $f \in (f_1, \ldots, f_k)Q\,\Gamma$ is equivalent to the decision whether the inhomogeneous linear equation $\sum_{i=1}^{k} f_i X_i = f$ over Q is solvable. If the result of the latter decision is positive then successively testing the possible solutions according to a Gödel enumeration of Q^k will provide one particular solution. Moreover, the computation of a finite generating set of the syzygy module of $\{f_1, \ldots, f_k\}$ is equivalent to the (complete) solution of the homogeneous linear equation $\sum_{i=1}^{k} f_i X_i = 0$. Therefore, a commutative ring Q satisfying conditions *iii)-v)* is sometimes called a noetherian ring in which linear equations are solvable. Gröbner bases in polynomial rings over such rings Q have been extensively investigated in the literature. For an overview we refer to [AL94].

Note, that our investigation are not restricted to commutative rings Q. Though some results corresponding to, e.g., effective left Gröbner structures require only the properties for left ideals of Q, we assume for simplicity:

Assumption 2 *Q is noetherian and has decidable ideal membership and solvable syzygy problems for left-, right-, and two-sided ideals.*

Our goal is to find conditions on the parts of $\mathfrak{R}$ which guaranty that $\mathfrak{R}$ is an effective Gröbner structure. In any case the class of graded structures satisfying the conditions should contain the simple example $(Q\langle\Gamma\rangle, \Gamma, \text{lt}, Q\langle\Gamma\rangle, \text{in}, id)$ of a graded structure of the monoid ring $Q\langle\Gamma\rangle$ which is isomorphic to the direct sum $\bigoplus_{\gamma\in\Gamma} Q \cdot \gamma$ as a Q-bimodule and whose multiplication is determined by $\gamma \cdot \gamma' = \gamma \circ \gamma'$. The leading term $\text{lt}(\sum_{i=1}^{k} a_i \gamma_i)$ is defined in the usual way as the maximum $\max\{\gamma_i \mid 1 \leq i \leq k\}$. The function in is completely determined by the above data and $\text{in}^* = id$ is chosen as the identity on the set of homogeneous elements. The assumption that $(Q\langle\Gamma\rangle, \Gamma, \text{lt}, Q\langle\Gamma\rangle, \text{in}, id)$ is an effective left, right, or two-sided Gröbner structure provides some obvious necessary conditions on the monoid Γ. First of all Γ has to satisfy a version of Dickson's Lemma (see [Di13]). We assume the strongest generalisation of Dickson's Lemma, i.e. for any infinite sequence $\gamma_1, \gamma_2, \ldots$ of elements of Γ there must exist natural numbers $i < j$ and $k < l$ such that γ_i is a left divisor of γ_j and γ_k is a right divisor of γ_l. In this case we call Γ a noetherian monoid which reflects the fact that ascending chains of left, right, or two-sided monoid ideals, respectively, will always stabilise. We say that Γ has a decidable divisor problem if for any two elements $\gamma, \omega \in \Gamma$ it can be decided whether there exists $\gamma', \gamma'' \in \Gamma$ such that $\gamma' \circ \gamma \circ \gamma'' = \omega$. Left and right divisor problem are defined in an analogous way. Any noetherian well-ordered monoid Γ satisfies the left and right cancellation law and any element $\gamma \neq \epsilon$ of Γ has only a finite number of decompositions into irreducible factors. Furthermore, Γ has a uniquely determined minimal (monoid) generating set $X = \{x_1, \ldots, x_n\}$. All elements

x_i are irreducible, i.e. $x_i \neq \gamma_1 \circ \gamma_2$ for all $\gamma_1, \gamma_2 \in \Gamma \setminus \{\epsilon\}$. If X can be computed and the left, right, or general divisor problem of Γ is decidable then for any $\gamma \in \Gamma$ there can be computed the set of all factorizations of γ. Hence, if a finite generating set X of the effective noetherian well-ordered monoid Γ is given then the solution of the factorization problem, i.e. the computation of all decompositions into irreducible factors, is equivalent to the decidability of any of the three divisor problems. From now on we will assume that the monoid Γ satisfies the following conditions which are necessary for the effectivity of the graded structure $(Q\langle\Gamma\rangle, \Gamma, \mathrm{lt}, Q\langle\Gamma\rangle, \mathrm{in}, id)$.

Assumption 3 *The monoid Γ is noetherian, there can be computed a finite generating set X of Γ, and the factorization problem of Γ is solvable. Moreover, we require that for any finite subset $\Omega \subseteq \Gamma$ there can be computed the set of all minimal common multiples of the elements of Ω.*

Furthermore, we assume that any of the direct summands G_γ of G is a cyclic Q-bimodule generated by an element $1\!\!1_\gamma$ which, in addition, generates G_γ already as a Q-left and as a Q-right module. This condition seems the most restrictive since it is far from being necessary for effective Gröbner structures. At the other hand side the condition is fundamental for all classical Gröbner bases investigations and generalisations. In particular our investigations of the ideal membership and the syzygy problems of G will make use of the above assumption extensively. Nevertheless, at least if Q is a commutative principal ideal domain we could generalise a lot of the results to finitely generated Q-bimodules G_γ.

Let $I_\gamma = ann_L(G_\gamma) \subseteq Q$ denote the annihilating left ideal of the Q-left module G_γ. Since G_γ is cyclic we have the isomorphism $G_\gamma \cong Q/I_\gamma$ of Q-left modules. Hence, as a Q-left module G is isomorphic to the direct sum $\bigoplus_{\gamma\in\Gamma} Q/I_\gamma$. Finally, we add assumptions which are essential for the computability of the functions in and in* and, hence, provide the linkage between R and the associated graded ring G.

Assumption 4 *For any $\gamma \in \Gamma$ there exists $1\!\!1_\gamma \in G_\gamma$ generating G_γ as left and as right Q-module. Moreover, for given $\gamma \in \Gamma$ it is possible to compute a finite generating set $B_\gamma \subset Q = \mathcal{F}_\epsilon \subset R$ of the annihilating left ideal $ann_L(Q_\gamma)$ and a representant $g_\gamma \in R$ such that $[g_\gamma]_{\widehat{\mathcal{F}}_{\varphi(g_\gamma)}} = 1\!\!1_\gamma$.*

Each summand Q/I_γ is an effective Q-left module since Q has decidable membership problem for left ideals given by finite generating sets. Hence, the direct sum $\bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ over the recursively enumerable set Γ is an effective Q-left module, too. Moreover, any element of $\bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ can be algorithmically decomposed into its homogeneous parts. A Q-left module isomorphism $\psi : G \to \bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ induces a multiplication on $\bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ such that ψ becomes a ring isomorphism. By assumption 1 we can compute $\varphi(f)$ for arbitrary non-zero $f \in R$. Successively testing the elements of Q according to a Gödel enumeration after a finite number of steps we will find an element

$c \in Q$ satisfying $f - cg_{\varphi(f)} \in \widehat{\mathcal{F}}_{\varphi(f)}$. Hence, $f \mapsto c + I_{\varphi(f)}$ defines a computable function $\text{in}' : R \to \bigoplus_{\gamma\in\Gamma} Q/I_\gamma$. There exists a uniquely determined isomorphism $\psi : G \to \bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ such that $\psi(\text{in}(f)) = \text{in}'(f)$ for all $f \in R$. From now we identify G and $\bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ under ψ. This leads also to an identification of the functions in$'$ and in. Now, let $d + I_\gamma \in G$, where $d \in Q$, be an arbitrary homogeneous element of degree γ. The definition $\text{in}^*(d + I_\gamma) = \hat{d}g_\gamma$, where $\hat{d}$ is the canonical representant of $d + I_\gamma$ with respect to an arbitrary fixed canonical simplifier of Q/I_γ, defines a section of the function in which is computable since R is effective and the existence of canonical simplifiers of Q/I_γ is ensured by the decidability of the left ideal membership problem of Q. Finally, the computability of the multiplication of G follows from the relations $uv = 0 \iff \varphi(\text{in}^*(u)\text{in}^*(v)) \neq \deg(u) \circ \deg(v)$ and $uv \neq 0 \Rightarrow uv = \text{in}(\text{in}^*(u)\text{in}^*(v))$ for all non-zero homogeneous elements $u, v \in G$.

In summary, up to now we proved that the associated graded ring $G = \bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ is effective and connected to R by computable functions in and in* if $\mathfrak{R}$ satisfies the conditions 1,2,3, and 4.

Next we consider the ideal membership problem of homogeneous ideals of G. Let $H = \{h_1, \ldots, h_k\} \subset G$ be a set of homogeneous elements, I the left ideal of G generated by H and $h \in G$ a homogeneous element. According to condition 3 the set $M = \{(\gamma, i) \mid 1 \leq i \leq k \wedge \gamma \circ \deg(h_i) = \deg(h)\}$ is finite and can be computed. We have $h \in I$ if and only if there exist elements $c_{\gamma,i} \in Q$ such that $h = \sum_{(\gamma,i)\in M} c_{\gamma,i} \mathbb{1}_\gamma h_i$. The latter problem can be reduced to a left ideal membership problem of Q and, hence, is decidable according to condition 2.

Now, let us consider the two-sided ideal J generated by H and ask whether $h \in J$. The same arguments as above provide finiteness and computability of the set $M = \{(\gamma, i, \gamma') \mid 1 \leq i \leq k \wedge \gamma \circ \deg(h_i) \circ \gamma' = \deg(h)\}$. However, in general the decision about the solvability of the equation

$$h = \sum_{(\gamma,i,\gamma')\in M} c_{\gamma,i,\gamma'} \mathbb{1}_\gamma h_i d_{\gamma,i,\gamma'} \mathbb{1}_{\gamma'} \tag{1}$$

in the variables $c_{\gamma,i,\gamma'}, d_{\gamma,i,\gamma'} \in Q$ is not reducible to an ideal membership problem of Q. Using condition 4 we could transform the problem 1 into solving

$$a\mathbb{1}_{\deg(h)} = h = \sum_{(\gamma,i,\gamma')\in M} c_{\gamma,i,\gamma'} \mathbb{1}_\gamma h_i \mathbb{1}_{\gamma'} e_{\gamma,i,\gamma'} = \sum_{(\gamma,i,\gamma')\in M} c_{\gamma,i,\gamma'} a_{\gamma,i,\gamma'} \mathbb{1}_{\deg(h)} e_{\gamma,i,\gamma'} \ ,$$

where $c_{\gamma,i,\gamma'}, e_{\gamma,i,\gamma'} \in Q$ are variables and $a, a_{\gamma,i,\gamma'} \in Q$ are constants. In general, this requires the decision of a Q-subbimodule problem. Such a decidabiltiy is not ensured by the assumptions made so far. Let $Z(G)$ denote the centre of G and Z a generating set of Q considered as $Z(G) \cap Q$-left module. Then we can transform 1 in the form

$$h = \sum_{(\gamma,i,\gamma')\in M} \sum_{z\in Z} p_{\gamma,i,\gamma',z} \mathbb{1}_\gamma h_i z \mathbb{1}_{\gamma'} \ , \tag{2}$$

where the $p_{\gamma,i,\gamma',z} \in Q$ are variables. If Q is finitely generated as $Z(G) \cap Q$-left module and a finite generating set Z can be computed then the solution of 2 can be reduced to the decision of a left ideal membership problem of Q.

4 Effective left Gröbner structures

Assumption 1 to 4 influence mainly the Q-module structure of G. Until now there are to many freedoms in the multiplication of G than we could hope to solve the syzygy problem algorithmically. In particular, we have not yet any control about the zero divisors of G.

Let us illustrate this at an example. Let $k[X]$ be the polynomial ring in a finite set X of indeterminates over a field k. Furthermore, let $T(X)$ be the set of terms in X, $\mathbb{N}$ the natural numbers and $\prec$ a monoid well-order of $T(X) \times \mathbb{N}$ comparing the first components with respect to an arbitrary fixed admissible term order of $T(X)$ and breaking ties by comparing the second components with respect to the usual order $<$ of natural numbers. Finally, for all $0 \neq a \in k$ and $1 \neq t \in T(X)$ let $\varphi(a) = (1, 0)$ and $\varphi(at) = (t, 1)$. We consider the graded structure $(k[X], (T(X) \times \mathbb{N}, \prec), \varphi, G, \mathrm{in}, \mathrm{in}^*)$, where in^* is arbitrary admissible. Then $Q = k$ and G is isomorphic to $k[X]$ as a k-vector space. But any two non-constant terms have product 0 in G. So, obviously G is not noetherian and syzygy modules of finite sets of non-constant homogeneous elements are not finitely generated. We glue together the multiplications of G and Γ by requiring:

Assumption 5 *for all* $\gamma, \omega \in \Gamma$ *let* $G_\gamma G_\omega = G_{\gamma \circ \omega}$.

Lemma 1 *If* $\mathfrak{R}$ *satisfies the assumptions 4 and 5 and* Q *is noetherian then for any* $\gamma \in \Gamma$ *the set*

$$\Gamma_\gamma = \{\omega \in \Gamma \mid Q/I_\gamma \ncong Q/I_{\omega \circ \gamma}\} \tag{3}$$

is either empty or a left monoid ideal of Γ.

Proof: For arbitrary $\gamma, \omega \in \Gamma$ and $c \in Q$ we have $c\mathbb{1}_\omega \mathbb{1}_\gamma = 0$ if and only if $c \in ann_L(G_{\omega \circ \gamma}) = I_{\omega \circ \gamma}$ according to the assumptions 4 and 5. Hence, $I_\omega \subseteq I_{\omega \circ \gamma}$ and, consequently, the Q-left module $Q/I_{\omega \circ \gamma}$ is a homomorphic image of the Q-left module Q/I_ω. Similar to the annihilating left ideal I_γ we can introduce the annihilating right ideal $J_\gamma = ann_R(G_\gamma) \subseteq Q$ of the Q-left module G_γ. The same arguments as above show that $Q/J_{\omega \circ \gamma}$ is a homomorphic image of Q/J_γ considered as Q-right modules. Since annihilating left and right ideals are always two-sided we can apply even ring homomorphisms. From the Q-left module isomorphism $Q/I_\gamma \cong G_\gamma$, the Q-right module isomorphism $Q/J_\gamma \cong G_\gamma$ and the properties of $\mathbb{1}_\gamma$ it follows that the residue class rings Q/I_γ and Q/J_γ are isomorphic. Hence, there exists a surjective ring homomorphism $\sigma_{\omega,\gamma} : Q/I_\gamma \to Q/I_{\omega \circ \gamma}$. Since Q is noetherian we have $\omega \in \Gamma_\gamma$ if and only if $\sigma_{\omega,\gamma}$ is not injective. But if $\sigma_{\omega,\gamma}$ is not injective then for any $\omega' \in \Gamma$ also the surjective homomorphism $\sigma_{\omega,\gamma} \circ \sigma_{\omega',\omega \circ \gamma} : Q/I_\gamma \to Q/I_{\omega' \circ \omega \circ \gamma}$ is not injective. □

For graded structures $\mathfrak{R}$ satisfying the previous assumptions the above lemma justifies to require:

Assumption 6 *the subset* $\{\gamma \mid \Gamma_\gamma = \emptyset\} \subseteq \Gamma$ *is decidable and for arbitrary given* γ *such* $\Gamma_\gamma \neq \emptyset$ *there can be computed a finite generating set* Δ_γ *of the left monoid ideal* Γ_γ*.*

Theorem 1 *Any graded structure* $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in}, \mathrm{in}^*)$ *satisfying the assumptions 1 to 6 is an effective left Gröbner structure.*

Proof: Conditions *i),ii)* and *iii)* of effective left Gröbner structure have been proved already.
v) Assume there exists an infinite strictly ascending chain of homogeneous left ideals of G then one can construct an infinite sequence of homogeneous elements such that no element of the sequence belongs to the left ideal generated in G by all previous elements. We will prove that G is left noetherian by showing that any infinite sequence of non-zero homogeneous elements $h_1 = \mathbb{1}_{\gamma_1} c_1, h_2 = \mathbb{1}_{\gamma_2} c_2, \ldots$ of G contains $h_l \in G \cdot (h_1, \ldots, h_{l-1})$.

Since Γ is noetherian there exists an infinite subsequence $h_{i_1}, h_{i_2}, \ldots$ such that the degree of h_{i_k} is a right multiple of the degree of h_{i_j} for all $j < k$. Moreover, from assumption 5 for all $j < k$ it follows the existence of a homogeneous element $u_{j,k}$ satisfying $\mathbb{1}_{\gamma_{i_k}} = u_{j,k} \mathbb{1}_{\gamma_{i_j}}$. Furthermore, from the noetherianity of Q we deduce the existence of an index $l > 1$ such that c_{i_l} belongs to the left ideal of Q generated by the elements $c_{i_1}, \ldots, c_{l-1}$. Consequently, there exist $a_1, \ldots, a_{l-1} \in Q$ such that $h_{i_l} = \mathbb{1}_{\gamma_{i_l}} c_{i_l} = \sum_{r=1}^{l-1} u_{r,l} \mathbb{1}_{\gamma_{i_r}} a_r c_{i_r}$. According to assumption 4 we have $h_{i_l} = \sum_{r=1}^{l-1} u_{r,l} b_r \mathbb{1}_{\gamma_{i_r}} c_{i_r} = \sum_{r=1}^{l-1} (u_{r,l} b_r) h_{i_r}$ for some $b_r \in Q$. Hence, h_{i_l} belongs to the left ideal of G generated by $h_1, \ldots, h_{i_l - 1}$.

Starting from representations $h_i = c_i' \mathbb{1}_{\gamma_i}$ we can prove in the same way that G is right noetherian and, hence, noetherian.
iv) Let $H \subset G$ be a finite set of non-zero homogeneous elements. Our aim is to construct a finite set $A(H)$ of homogeneous left syzygies of H such that $A(H) \cup \bigcup_{H' \subsetneq H} LSyz(H')$ generates the left syzygy module $LSyz(H)$ of H.

Let $\gamma \in \Gamma$ be a common right multiple of the degrees of the elements of H. Then there can be computed a finite generating set D_γ of the left syzygy module of $\{d + I_\gamma \mid \exists h \in H \; \exists \omega \in \Gamma \, : \, \mathbb{1}_\omega h = d \mathbb{1}_\gamma\} \subset Q/I_\gamma$. Multiplying each component of $s \in D_\gamma$ from the right by the corresponding $\mathbb{1}_\omega$ yields a homogeneous left syzygy $t(s)$ of H of degree γ and the G-left module generated by the set $A_\gamma = \{t(s) \mid s \in D_\gamma\} \subset LSyz(H)$ contains all homogeneous left syzygies of H of degree γ. Let $\gamma \in \Gamma$ be a common right multiple of the degrees of the elements of H, $\omega \in \Gamma$ arbitrary, and $s = \sum_{h \in H} u_h e_h$ a homogeneous left syzygy of degree $\omega \circ \gamma$ of H. By assumption 5 for all $h \in H$ it follows the existence of a homogeneous element v_h such that $\mathbb{1}_\omega v_h = u_h$. Hence, s can be written in the form $s = \mathbb{1}_\omega \sum_{h \in H} v_h e_h$. Let $d \in Q$ be such that $\sum_{h \in H} v_h h = \mathbb{1}_\gamma d$. It follows $d \in ann_R(G_{\omega \circ \gamma}) \supseteq ann_R(G_\gamma)$. If $d \in ann_R(G_\gamma)$ then $s \in G \cdot A_\gamma$. In particular, the equality $ann_R(G_{\omega \circ \gamma}) = ann_R(G_\gamma)$ always implies $s \in G \cdot A_\gamma$. Let $\Omega(H)_0 \subset \Gamma$

denote the set of all minimal common right multiples of the degrees of the elements of H. Recursively we define $\Omega(H)_{i+1} = \{\gamma' \circ \gamma \mid \gamma \in \Omega(H)_i \wedge \gamma' \in \Delta_\gamma\}$. Assumptions 3 and 6 ensure that each set $\Omega(H)_i$ is finite and can be computed in an algorithmic way. Obviously, $\Omega(H)_i = \emptyset$ implies $\Omega(H)_j = \emptyset$ for all $j > i$. There must exist a natural number i_0 such that $\Omega(H)_{i_0} = \emptyset$, otherwise it would follow the existence of an infinite sequence $Q/I_{\gamma_0} \longrightarrow Q/I_{\gamma_1} \longrightarrow \cdots$ of epimorphisms which are not injective in contradiction to assumption 2. Hence, the sets $\Omega(H) = \bigcup_{i=1}^{\infty} \Omega(H)_i = \bigcup_{i=1}^{i_0-1} \Omega(H)_i$ and $A(H) = \bigcup_{\gamma \in \Omega(H)} A_\gamma$ are finite and can be computed in an algorithmic way. The above investigations show that $A(H) \cup \bigcup_{H' \subsetneq H} LSyz(H')$ generates $LSyz(H)$ and induction on the number of elements of H finally yields that a finite homogeneous generating set of $LSyz(H)$ can be constructed algorithmically. □

5 Effective two-sided Gröbner structures

There is a large class of graded structures where a generalised Kandri-Rody/Weispfenning closure technique (see [KW90]) can be applied to the computation of Gröbner bases of two-sided ideals of R.

Assumption 7 *Let $\hat{Q} = Q \cap Z(R)$ denote the subring of Q consisting of all elements which commute with the elements of R. Assume that Q is finitely generated as $\hat{Q}$-module and that a finite generating set Z can be constructed in an algorithmic way. Furthermore, let there exist computable functions $\delta : Q \times Q \to Q$ and $\delta_X : X \times Q \to Q$ satisfying $c \cdot d = \delta(c,d) \cdot c$ respectively $c \cdot \mathbb{1}_x = \delta_X(x,c) \cdot \mathbb{1}_x \cdot c$ for all $c, d \in Q$ and $x \in X$. Finally, assume that the monoid Γ is commutative.*

The requirement of the existence of δ and δ_X might seem rather technical. It could be replaced by one of the stronger conditions that Q is a skew field or that $Q = \hat{Q} \subseteq Z(R)$. In fact these both situations are the most interesting applications.

Theorem 2 *If the graded structure $\mathfrak{R} = (R, \Gamma, \varphi, G, \mathrm{in}, \mathrm{in}^*)$ satisfies the assumptions 1 to 6 and 7 then it is an effective two-sided Gröbner structure.*

Moreover, a two-sided Gröbner basis F of an arbitrary two-sided ideal $I \subseteq R$ is also a left Gröbner basis of I.

Proof: We verified already conditions *i)*, *ii)* and *v)* of effective two-sided Gröbner structures. Condition *iii)* follows immediately from the trivial observation $\hat{Q} \subseteq Q \cap Z(G)$ and the discussion at the end of Section 3.

So it remains to consider the syzygy problem *iv)*. Let $H \subset G$ be a finite set of non-zero homogeneous elements. Recall from Definition 3 that we need to consider the image $\tau(Syz(H))$ of the syzygy module of H under the natural homomorphism $\tau : (G \otimes_U G)^{|H|} \to (G \otimes_A G)^{|H|}$, where A is the subring of G generated by the initial terms of the elements of $Z(R)$. From now, for simplicity, we denote the image $\tau(Syz(H))$ by $Syz(H)$.

Let $a \in Q$ and $h = c\mathbb{1}_\gamma \in H$ be arbitrary. By assumption 4 there exists $a' \in Q$ such that $\mathbb{1}_\gamma a = a'\mathbb{1}_\gamma$. Hence $ha = \delta(c, a')h$ and $s_{a,h} = e_h a - d_{a,h} e_h \in Syz(H)$, where $d_{a,h} = \delta(c, a') \in Q$. In a similar way for arbitrary $x \in X$ and $h \in H$ it can be proved the existence of a syzygy $s_{x,h} = e_h \mathbb{1}_x - c_{x,h}\mathbb{1}_x e_h \in Syz(H)$. Let $A_Z = \{s_{z,h} \mid (z,h) \in Z \times H\}$ and $A_X = \{s_{x,h} \mid (x,h) \in X \times H\}$. Our aim is to prove that $A_Z \cup A_X \cup LSyz(H) \otimes_A 1$ generates $Syz(H)$. It is easy to observe that $s_{a,h} \in GA_Z G$ for all $a \in Q$ and $h \in H$. Next consider arbitrary $\gamma \in \Gamma$ and $h \in H$. Let $\gamma = x_1 \circ \cdots \circ x_k$ be an arbitrary representation of γ in the generating set X. Using induction on k we will prove the existence of a syzygy $s_{\gamma,h} = e_h \mathbb{1}_\gamma - c_{\gamma,h}\mathbb{1}_\gamma e_h \in G(A_Z \cup A_X)G$. The initial step $k = 1$ is obvious. Consider $k > 1$ and set $\gamma' = x_1 \circ \cdots \circ x_{k-1}$. We have $e_h \mathbb{1}_{\gamma' \circ x_k} = e_h \mathbb{1}_{x_k}\mathbb{1}_{\gamma'} a = s_{x_k,h}\mathbb{1}_{\gamma'} a + c_{x_k,h}\mathbb{1}_{x_k} e_h \mathbb{1}_{\gamma'} a$ for some $a \in Q$. By induction hypothesis there exists $s_{\gamma',h} = e_h \mathbb{1}_{\gamma'} - c_{\gamma',h}\mathbb{1}_{\gamma'} e_h \in G(A_Z \cup A_X)G$. Hence, $e_h \mathbb{1}_{\gamma' \circ x_k} = s_{x_k,h}\mathbb{1}_{\gamma'} a + c_{x_k,h}\mathbb{1}_{x_k} s_{\gamma',h} a + c_{x_k,h}\mathbb{1}_{x_k} c_{\gamma',h}\mathbb{1}_{\gamma'} e_h a = s_{x_k,h}\mathbb{1}_{\gamma'} a + c_{x_k,h}\mathbb{1}_{x_k} s_{\gamma',h} a + c_{x_k,h}\mathbb{1}_{x_k} c_{\gamma',h}\mathbb{1}_{\gamma'} s_{a,h} + c_{x_k,h}\mathbb{1}_{x_k} c_{\gamma',h}\mathbb{1}_{\gamma'} d_{a,h} e_h$. This finishes the induction proof. As an immediate consequence we obtain that for any homogeneous syzygy $s \in Syz(H)$ there exists a homogeneous left syzygy $s' \in LSyz(H)$ such that $s - s' \otimes 1 \in G(A_Z \cup A_X)G$. Hence, $Syz(H)$ is finitely generated since A_Z and A_X are finite by construction and $LSyz(H)$ is finitely generated according to Theorem 1. The computability assumptions ensure that the sets A_Z and A_X and a finite homogeneous generating set of $LSyz(H)$ can be computed.

From the above investigations it follows that for any homogeneous elements $h, u \in G$ there exists a homogeneous element $v \in G$ of the same degree as u such that $hu = vh$. Hence, any homogeneous left ideal of G is even two-sided and, consequently, a two-sided Gröbner basis of the two-sided ideal I is also a left Gröbner basis of I. □

Roughly, the nature of the Kandri-Rody/Weispfenning closure technique consists in computing left Gröbner bases and checking whether the generated left ideal is closed under multiplying variables from the right. If this is not the case then the process is repeated after adding the non-zero remainders to the basis. In our situation the generating set $A_Z \cup A_X \cup LSyz(H) \otimes_A 1$ of the syzygy module allows a similar procedure. The syzygies contained in A_Z and A_X represent the multiples against which the left ideal generated by the Gröbner basis has to be closed.

In [Mo88b] Mora considers a class of non-commutative algebras which allow the computation of two-sided but not necessarily of one-sided Gröbner bases. The reason is that the associated graded ring satisfies the ascending chain condition for two-sided but not for one-sided ideals. Weakening assumption 5 and sharpening assumption 7 we obtain a class of effective two-sided but not necessarily one-sided Gröbner structures which covers also the class of Mora.

Assumption 8 *Let Γ be commutative and $Q = \hat{Q}$ a subring of the centre of R. For all $\gamma, \omega \in \Gamma$ such that γ divides ω let there exist $\gamma', \gamma'' \in \Gamma$ having the properties $\gamma' \circ \gamma \circ \gamma'' = \omega$ and $G_{\rho'} G_\rho G_{\rho''} = G_{\rho' \circ \rho \circ \rho''}$ for any divisors $\rho' \mid \gamma'$, $\rho \mid \gamma$, and $\rho'' \mid \gamma''$.*

Let $\gamma \mid \omega$ and γ', γ'' be as above. In particular we have $G_{\gamma'} G_\gamma G_{\gamma''} = G_\omega$ and $G_{\gamma'} G_\gamma = G_{\gamma' \circ \gamma}$. Applying the same arguments as in Lemma 1 for arbitrary $\omega', \omega'' \in \Gamma$ we obtain an epimorphism sequence $Q/I_\gamma \to Q/I_{\gamma' \circ \gamma} \to Q/I_\omega \to Q/I_{\omega' \circ \omega \circ \omega''}$. Hence, any of the sets

$$\widehat{\Gamma}_\gamma = \{\omega \in \Gamma \ : \ \gamma \mid \omega \wedge Q/I_\gamma \ncong Q/I_\omega\} \tag{4}$$

is either empty or a monoid ideal of Γ.

Assumption 9 *The subset* $\left\{\gamma \mid \widehat{\Gamma}_\gamma = \emptyset\right\} \subseteq \Gamma$ *is decidable and for arbitrary given* γ *such* $\widehat{\Gamma}_\gamma \neq \emptyset$ *there can be computed a finite generating set* Δ_γ *of the monoid ideal* $\widehat{\Gamma}_\gamma$.

Theorem 3 *Let* $\mathfrak{R}$ *be a graded structure satisfying conditions 1 to 4 and 8 to 9. Then* $\mathfrak{R}$ *is a two-sided Gröbner structure.*

Proof: Conditions *i) - iii)* are obvious.
v) We will show that any infinite sequence $h_1 = \mathbb{1}_{\gamma_1} c_1, h_2 = \mathbb{1}_{\gamma_2} c_2, \ldots$ of homogeneous elements of G contains an element $h_k \in G(h_1, \ldots, h_{k-1})G$. Since Γ is noetherian it is sufficient to prove the assertion for sequences satisfying $\gamma_i \mid \gamma_j$ for all $i < j$. By noetherianity of Q there exists k such that $c_k \in (c_1, \ldots, c_{k-1})Q$. For all $i < k$ we deduce the existence of $\gamma_i', \gamma_i'' \in \Gamma$ and $b_i \in Q$ such that $b_i \mathbb{1}_{\gamma_i'} \mathbb{1}_{\gamma_i} \mathbb{1}_{\gamma_i''} = \mathbb{1}_{\gamma_k}$ from assumption 8. Hence, $h_k \in G(h_1, \ldots, h_{k-1})G$.
iv) For the rather technical and lengthy proof we refer to [Ap97]. Let us sketch the main ideas. For any $x \in X$ and $h \in H$ there exists a homogeneous syzygy $s_{x,h} = a_{x,h} e_h \mathbb{1}_x - b_{x,h} \mathbb{1}_x e_h \in Syz(H)$ where at least one of the elements $a_{x,h}, b_{x,h} \in Q$ is a unit. Let $B_X = \{s_{x,h} \mid (x,h) \in X \times H\}$. For any homogeneous syzygy $s = \sum_{i=1}^k u_i e_{h_i} v_i \in Syz(H)$ whose degree is a multiple of the degrees of all $h \in H$ there exists a homogeneous syzygy $s' = \mathbb{1}_\delta \left(\sum_{i=1}^k u_i' e_{h_i} v_i'\right) \mathbb{1}_{\delta'}$ such that $s - s' \in G B_X G$ and $\deg(u_i') \circ \deg(h_i) \circ \deg(v_i')$ is a minimal common multiple of the degrees of the elements of H. Let $\Omega(H)_0$ be the set of all minimal common multiples of the degrees of $h \in H$ and define recursively $\Omega(H)_{i+1} = \bigcup_{\gamma \in \Omega(H)_i} \Delta_\gamma$. Then the set $\Omega(H) = \bigcup_{i=0}^\infty \Omega(H)_i$ is finite and can be constructed algorithmically. Finally, the set $B_X \cup \bigcup_{\gamma \in \Omega(H)} A_\gamma \cup \bigcup_{H' \subsetneqq H} Syz(H')$, where the A_γ are finite generating sets of the Q-modules of all homogeneous syzygies of H of degree γ, generates $Syz(H)$. □

References

[AL94] Adams, W.W., Loustaunau, P., An Introduction to Gröbner Bases. Graduate Studies in Mathematics, Vol. 3, AMS Press, 1994.

[Ap92] Apel, J., A relationship between Gröbner bases of ideals and vector modules of G-algebras. Contemporary Mathematics, Band **131**, Vol. 2, pp. 195–204, 1992.

[Ap97] Apel, J., Habilitation Thesis. Submitted at the University of Leipzig.

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

[Bu65] Buchberger, B., Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD-Thesis, Univ. Innsbruck, 1965.

[Bu85] Buchberger, B., An Algorithmic Method in Polynomial Ideal Theory. Chapter 6 in: Recent Trends in Multidimensional System Theory (ed.: N.K. Bose), D. Reidel Publ. Comp., 1985.

[Di13] Dickson, L.E., Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *Am.J.of Math.* **35**, pp. 413–426, 1913.

[KK84] Kandri-Rody, A., Kapur, D., Algorithms for computing Gröbner bases of polynomial ideals over various Euclidean rings. *L.N.C.S.* **174**, pp. 193–206, 1984.

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

[Kr92] Kredel, H., Solvable polynomial rings. PhD-Thesis, Univ. Passau, Shaker-Verlag, 1992.

[Mö88] Möller, H.M., On the construction of Gröbner bases using syzygies. *J.Symb.Comp.* **6** pp. 345–359, 1988.

[Mo88a] Mora, T., Seven Variations on Standard Bases. Preprint, Univ. di Genova, Dip. di Mathematica, N. 45, 1988.

[Mo88b] Mora, T., Gröbner Bases in Non-Commutative Algebras. *L.N.C.S.* **358**, pp. 150–161, 1988.

[Na62] Nagata, M., Local rings. Interscience, New York, 1962.

[Pa85] Pan, L., Application of Rewriting Techniques. PhD Thesis, Univ. Santa Barbara, 1985.

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

[Sch79] Schaller, S.C., Algorithmic aspects of polynomial residue class rings. PhD Thesis, Univ. Wisconsin at Madison, 1979.

[Tr78] Trinks, W., Über Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Theory* **10** pp. 475–488, 1978.

[Za78] Zacharias, G., Generalized Gröbner Bases in Commutative Polynomial Rings. Bachelor Thesis. MIT, Boston, 1978.