Contemporary Mathematics

Computation of Syzygies Over Non-Commutative Rings

Holger Bluhm and Martin Kreuzer

This paper is dedicated to Gerhard Rosenberger on occasion of his 60th birthday.

Abstract. This paper is devoted to computing modules of two-sided syzygies. Two-sided syzygies are elements $\sum_{i=1}^{s}\sum_{j=1}^{k_i} g_{ij}e_ih_{ij}$ in a free two-sided module such that $\sum_{i=1}^{s}\sum_{j=1}^{k_i} g_{ij}f_ih_{ij} = 0$. Here $(f_1,\dots,f_s)$ is a given tuple of elements of a non-commutative ring R or a free two-sided R-module. Of particular interest are two-sided syzygies of the form $ae_1 - e_2a$ such that $aw = w'a$ for a given pair of words (w,w') representing elements in a group ring $R = K[G]$ because these syzygies solve the conjugator search problem.

Our approach is to translate everything to syzygies of elements of a free two-sided module over the non-commutative polynomial ring $K[X^*]$ and to adapt the component elimination technique of [**3**] to this non-commutative setting. The computation of syzygies over residue class rings of $K[X^*]$ is then achieved by projecting the corresponding syzygies of vectors of representatives of the given elements.

1. Introduction

For non-commutative rings, there exist two essentially different ways to construct Gröbner basis theories: Ed Green and his co-workers developed theories for *basic algebras*, i.e. algebras having vector space bases which form a multiplicatively closed set that can be well-ordered (see [**4**], [**5**], [**7**], [**8**]). Typical examples are path algebras, PBW-algebras, etc. This theory does usually not apply to group rings, since their natural vector space basis (the group elements) cannot be well-ordered.

A different approach was taken by Klaus Madlener and his co-workers (see [**13**], [**14**], [**15**], [**9**]): if the algebra is decribed by generators and relations, i.e. as a residue class algebra of the non-commutative polynomial ring, one can use a system of generators of the ideal of relations which defines a convergent rewrite rule to compute effectively in the residue class algebra and to define a theory of (prefix-) Gröbner bases. This theory applies to many monoid and group rings and will be used in the present paper.

In the first theory, algorithms for the computation of modules of one-sided syzygies have been developed: Given elements $f_1,\dots,f_s$ of the non-commutative

1991 *Mathematics Subject Classification.* Primary 16-08; Secondary 16D25, 16S34, 20M05.

Key words and phrases. two-sided syzygy, Groebner basis, elimination theory, group ring.

algebra R, the left-R-module of all tuples $(g_1,\dots,g_s)\in R^s$ such that $g_1f_1+\cdots+g_sf_s=0$ has been computed (see [**5**] and [**12**]). However, for two-sided syzygies there have been only scattered attempts to achieve this goal. Here we ask for a system of generators of all tuples $((g_{11},h_{11}),\dots,(g_{1k_1},h_{1k_1}),\dots,(g_{sk_s},h_{sk_s}))$ such that $\sum_{i=1}^{s}\sum_{j=1}^{k_i} g_{ij}f_ih_{ij}=0$.

In [**16**], II.3, Teo Mora tried to generalize the commutative method of lifting the syzygies of the leading terms to the case of the non-commutative polynomial ring. However, this technique faces the problem that the syzygy module of the leading terms is almost never finitely generated and contains many "trivial" elements. For PBW-algebras, Manuel and Socorro Garcia Roman computed two-sided syzygies by shifting the problem to the enveloping algebra and using the known algorithms for one-sided syzygies (see [**6**]). In this paper, we solve the problem of computing two-sided syzygies in the case of the Gröbner basis theory of Madlener *et al.* in a direct and straightforward fashion.

The first step is to construct a Gröbner basis theory for submodules of two-sided free modules over the non-commutative polynomial ring $K[X^*]$ over a field K. For two-sided ideals in this ring, the two aforementioned Gröbner basis theories agree and yield the same results. Since two-sided syzygies are elements of the free two-sided module $F_r=(K[X^*]\otimes_K K[X^*])^r$ over this ring, we generalize the theory in the natural way and reconnect it to the case of two-sided ideals via the canonical epimorphism $\pi: F_1\longrightarrow K[X^*]$.

For the actual computation of the two-sided syzygy module we adapt the idea of Massimo Caboara and Carlo Traverso (see [**3**] and [**10**], Tut. 34) from the commutative to the non-commutative setting. They proposed to use "module component elimination" for syzygy calculations and showed that this approach is theoretically a most efficient one. Hence we introduce the non-commutative theory of component elimination is Section 3 and use it to compute intersections and two-sided syzygy modules over the non-commutative polynomial ring.

Then we bring the full force of the theory of Madlener *et al.* to bear and compute two-sided syzygy modules over non-commutative rings of the form $K[X^*]/I$. The method to do this is to compute the corresponding syzygy module over $K[X^*]$ and then to project the computed syzygies.

Finally, in the last section, we show that the algorithm we developed can be used to solve the conjugator search problem in certain finitely presented monoids and groups, a task which has been suggested as a basis for non-commutative cryptosystems (see [**1**]). Further examples are contained in the first author's diploma thesis [**2**]. Unless specified otherwise, we shall adhere to the definitions and notation used in [**10**] and [**11**].

2. Gröbner Bases for 2-Sided $K[X^*]$-Modules

In the following we let $X=\{x_1,\dots,x_n\}$ be a finite alphabet and X^* the monoid of *words* (or *terms*) $x_{i_1}\cdots x_{i_\ell}$ under concatenation. The empty word will be denoted by λ. Furthermore, let K be a field, and let

$$K[X^*]=\{c_1w_1+\cdots+c_sw_s \mid c_i\in K\setminus\{0\},\ w_i\in X^*,\ s\in\mathbb{N}\}$$

be the *non-commutative polynomial ring* (also called the *free associative algebra*) over the set of indeterminates X. To perform explicit computations in $K[X^*]$, we need to order the terms.

Definition 2.1. A *term ordering* on X^* is a complete ordering σ such that

(1) $w_1 \geq_\sigma w_2$ implies $w_3w_1w_4 \geq_\sigma w_3w_2w_4$ for $w_1, \dots, w_4 \in X^*$, and
(2) σ is a well-ordering.

For instance, the *length-lexicographic ordering* `llex` is a term ordering. It is defined by first considering the length of the two words and breaking ties by comparing them lexicographically with respect to $x_1 >_{\texttt{llex}} \cdots >_{\texttt{llex}} x_n$. Another example is the *total lexicographic ordering* `tlex` which first compares the associated commutative terms lexicographically and then breaks ties using the non-commutative lexicographic ordering. Notice that the non-commutative lexicographic ordering by itself is not a term ordering, since it is not a well-ordering.

Given a term ordering σ on X^*, we can define the *leading term* $\mathrm{LT}_\sigma(f)$ of a non-commutative polynomial $f \in K[X^*] \setminus \{0\}$ as the largest term in its support. Then we introduce the *leading term ideal* of a two-sided ideal $I \subseteq K[X^*]$ by letting

$$\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f) \mid f \in I \setminus \{0\} \rangle$$

where $\langle S \rangle$ denotes the two-sided ideal generated by S. Finally, we recall that a (two-sided) σ*-Gröbner basis* of I is a set of non-commutative polynomials G such that the set of their leading terms $\mathrm{LT}_\sigma(G)$ generates $\mathrm{LT}_\sigma(I)$.

The Gröbner basis theory for two-sided ideals in $K[X^*]$ is well-developed (see for instance [**17**] and [**18**]). Our first task in this section is to generalize it to submodules of free two-sided modules. What kind of modules are we talking about? Given a (non-commutative) K-algebra R, its *enveloping algebra* $R^{\mathrm{env}} = R \otimes_K R$ is a two-sided R-module in the natural way. For $r \geq 1$, we form the two-sided R-module $F_r = \bigoplus_{i=1}^r R^{\mathrm{env}}$. The following well-known result explains why we call it the *free two-sided R-module* of rank r.

Proposition 2.2. *For a two-sided R-module M and elements $v_1, \dots, v_r \in M$, there exists a unique homomorphism of two-sided R-modules $\varphi : F_r \longrightarrow M$ such that $\varphi(e_i) = v_i$ for $i = 1, \dots, r$. Here $e_i = (0, \dots, 0, 1 \otimes 1, 0, \dots, 0)$ is the i^{th}* standard basis vector *in F_r.*

Now we introduce the basic notions of Gröbner basis theory in this setting.

Definition 2.3. A *term* in F_r is an element of the form we_iw' where $w, w' \in X^*$ are words and $i \in \{1, \dots, r\}$. The set of all terms in F_r will be denoted by $\mathbb{T}(F_r)$.

A *module term ordering* on $\mathbb{T}(F_r)$ is a total ordering τ such that $t_1 \leq_\tau t_2$ implies $w_1t_1w_2 \leq_\tau w_1t_2w_2$ for all $t_1, t_2 \in \mathbb{T}(F_r)$ and $w_1, w_2 \in X^*$, and such that τ is a well-ordering.

Example 2.4. Let `To` be a term ordering on X^*.

(1) For terms $w_1e_iw_i', w_2e_jw_2' \in \mathbb{T}(F_r)$ such that $w_1, w_1', w_2, w_2' \in X^*$ and $i, j \in \{1, \dots, r\}$, we let

$$\begin{aligned} w_1e_iw_i' \geq_{\texttt{ToPos}} w_2e_jw_2' \quad \Longleftrightarrow \quad & w_1w_1' >_{\texttt{To}} w_2w_2' \text{ or} \\ & (w_1w_1' = w_2w_2' \text{ and } w_1 >_{\texttt{To}} w_2) \text{ or} \\ & (w_1 = w_2 \text{ and } i \leq j). \end{aligned}$$

This defines a module term ordering `ToPos` on $\mathbb{T}(F_r)$.

(2) For terms $w_1 e_i w_i', w_2 e_j w_2' \in \mathbb{T}(F_r)$ such that $w_1, w_1', w_2, w_2' \in X^*$ and $i, j \in \{1, \dots, r\}$, we let

$$\begin{aligned} w_1 e_i w_i' \geq_{\texttt{PosTo}} w_2 e_j w_2' \quad \iff \quad & i < j \text{ or} \\ & (i = j \text{ and } w_1 w_1' >_{\texttt{To}} w_2 w_2') \text{ or} \\ & (i = j \text{ and } w_1 w_1' = w_2 w_2' \text{ and } w_1 \geq_{\texttt{To}} w_2). \end{aligned}$$

Again this defines a module term ordering PosTo on $\mathbb{T}(F_r)$.

Definition 2.5. Let τ be a module term ordering on $\mathbb{T}(F_r)$.

(1) Given a vector $v \in F_r \setminus \{0\}$, there exists a unique representation $v = c_1 t_1 + \cdots + c_s t_s$ with $c_1, \dots, c_s \in K \setminus \{0\}$ and $t_1, \dots, t_s \in \mathbb{T}(F_r)$ satisfying $t_1 >_\tau \cdots >_\tau t_s$. The term $\mathrm{LT}_\tau(v) = t_1$ is called the *leading term* of v with respect to τ. The element $\mathrm{LC}_\tau(v) = c_1$ is called its *leading coefficient*. We shall also use the notation $\mathrm{LM}_\tau(v) = c_1 t_1$.

(2) For a two-sided submodule $M \subseteq F_r$, the two-sided submodule $\mathrm{LT}_\tau(M) = \langle \mathrm{LT}_\tau(v) \mid v \in M \setminus \{0\} \rangle$ of F_r is called the *leading term module* of M.

(3) A subset G of a two-sided submodule M of F_r is called a *τ-Gröbner basis* of M if the leading term module $\mathrm{LT}_\tau(M)$ is generated by the leading terms in the set $\mathrm{LT}_\tau\{G\} = \{\mathrm{LT}_\tau(f) \mid f \in G \setminus \{0\}\}$.

Based on these definitions, we can now generalize some standard results of Gröbner basis theory as follows.

Proposition 2.6 (Macaulay's Basis Theorem).
Let M be a two-sided submodule of F_r. Then the residue classes of the elements in $\mathbb{T}(F_r) \setminus \mathrm{LT}_\tau\{M\}$ form a K-vector space basis of F^r/M.

Proof. For $v \in F_r$ let $\overline{v} \in F_r/M$ denote the corresponding residue class. First suppose that the residue classes of $\mathbb{T}(F_r) \setminus \mathrm{LT}_\tau\{M\}$ do not generate F_r/M. Then let $v \in F$ such that $\overline{v} \notin \langle \overline{t} \mid t \in \mathbb{T}(F_r) \setminus \mathrm{LT}_\tau\{M\} \rangle_K =: B$. Since τ is a well ordering, we may assume that v has a minimal leading term with respect to τ among all these elements. If $\mathrm{LT}_\tau(v) \in \mathbb{T}(F_r) \setminus \mathrm{LT}_\tau\{M\}$ then the residue class of $v - \mathrm{LM}_\tau(v)$ is also not contained in B and $\mathrm{LT}_\tau(v - \mathrm{LM}_\tau(v)) <_\tau \mathrm{LT}_\tau(v)$, a contradiction. If $\mathrm{LT}_\tau(v) \in \mathrm{LT}_\tau\{M\}$ then there exists an element $m \in M$ such that $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(v)$. Again the element $v - \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(m)} m$ has residue class not in B and a smaller leading term than v, in contradiction to the minimality of $\mathrm{LT}_\tau(v)$.

To prove the linear independence, suppose that there are elements $k \geq 1$, $c_i \in K \setminus \{0\}$ and $t_i \in \mathbb{T}(F_r) \setminus \mathrm{LT}_\tau\{M\}$ such that $\sum_{i=1}^k c_i t_i \in M$. Then we have $\mathrm{LT}_\tau(\sum_{i=1}^k c_i t_i) \in \mathrm{LT}_\tau\{M\} \cap (\mathbb{T}(F_r) \setminus \mathrm{LT}_\tau\{M\})$, a contradiction. □

Proposition 2.7 (The Division Algorithm).
Let $s \geq 1$, and let $m, f_1, \dots, f_s \in F_r \setminus \{0\}$. Consider the following sequence of instructions.

(D1) *For $i = 1, \dots, s$ let $k_i = 1$, $g_{i1} = g_{i1}' = 0$, $p = 0$ and $v = m$.*

(D2) *Find the smallest $i \in \{1, \dots, s\}$ such that $\mathrm{LT}_\tau(v) = w\, \mathrm{LT}_\tau(f_i) w'$ for some $w, w' \in X^*$. If such an i exists, increase s by 1, set $g_{ik_i} = \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(f_i)} w$, $g_{ik_i}' = w'$ and replace v by $v - \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(f_i)} w f_i w'$. If now $v \neq 0$, continue with step (D2). Otherwise, continue with step (D4).*

(D3) *Replace p by $p + \mathrm{LM}_\tau(v)$ and v by $v - \mathrm{LM}_\tau(v)$. If now $v \neq 0$, continue with step (D2).*

(D4) *Return the tuple $((g_{11}, g'_{11}), \ldots, (g_{1k_1}, g'_{1k_1}), \ldots, (g_{s1}, g'_{s1}), \ldots, (g_{sk_s}, g'_{sk_s}))$ and the vector $p \in F_r$.*

This is an algorithm which returns elements $((g_{11}, g'_{11}), \ldots, (g_{sk_s}, g'_{sk_s}))$ and p such that the following conditions are satisfied.

1. *We have $m = \sum_{i=1}^{s} \sum_{j=1}^{k_i} g_{ij} f_i g'_{ij} + p$.*
2. *No element of $\mathrm{Supp}(p)$ is contained in $\langle \mathrm{LT}_\tau(f_1), \ldots, \mathrm{LT}_\tau(f_s) \rangle$.*
3. *If $g_{ij} \neq 0 \neq g'_{ij}$ for some $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, k_i\}$ then we have $\mathrm{LT}_\tau(g_{ij} f_i g'_{ij}) \leq_\tau \mathrm{LT}_\tau(m)$.*
4. *For all $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, k_i\}$ we have*
$$g_{ij} \,\mathrm{LT}_\tau(f_i) g'_{ij} \notin \langle \mathrm{LT}_\tau(f_1), \ldots, \mathrm{LT}_\tau(f_{i-1}) \rangle.$$
5. *The elements $((g_{11}, g'_{11}), \ldots, (g_{sk_s}, g'_{sk_s}))$ and p are uniquely determined by the preceding conditions (1)-(4).*

Proof. In step (D2) and (D3) the leading term of v becomes strictly smaller with respect to τ. Since τ is a well ordering, this can happen only finitely many times and the algorithm stops after finitely many steps.

To prove (1), we consider the equation $m = \sum_{i=1}^{s} \sum_{j=1}^{k_i} g_{ij} f_i g'_{ij} + p + v$. It holds at each point in the algorithm, since in step (D2) we have $g_{ik_i} f_i g'_{ik_i} + v = \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(f_i)} w f_i w' + v - \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(f_i)} w f_i w'$, and in step (D3) we have $p + v = (p + \mathrm{LM}_\tau(v)) + (v - \mathrm{LM}_\tau(v))$. Therefore we have $m = \sum_{i=1}^{s} \sum_{j=1}^{k_i} g_{ij} f_i g'_{ij} + p$ when the algorithm stops. Moreover, in step (D3) a monomial is added to p only if it is of the form $cw \,\mathrm{LT}_\tau(f_i) w'$ for some $c \in K \setminus \{0\}$, $w, w' \in X^*$ and $i \in \{1, \ldots, s\}$, which yields (2).

Claim (3) follows from $\mathrm{LT}\,\tau(g_{ij} f_i g'_{ij}) = \mathrm{LT}_\tau(v) \leq_\tau \mathrm{LT}_\tau(m)$.

Now we prove (4). Let $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, k_i\}$. Since in the corresponding step (D2) the index i is chosen minimally, we obtain $\mathrm{LT}_\tau(v) \notin \langle \mathrm{LT}_\tau(f_1), \ldots, \mathrm{LT}_\tau(f_{i-1}) \rangle$, where $\mathrm{LT}_\tau(v) = \frac{1}{\mathrm{LC}_\tau(g_{ij}) \,\mathrm{LC}_\tau(g'_{ij})} g_{ij} \,\mathrm{LT}_\tau(f_i) g'_{ij}$.

Finally, suppose there exist other elements $((h_{11}, h'_{11}), \ldots, (h_{1l_1}, h'_{1l_1}), \ldots, (h_{s1}, h'_{s1}), \ldots, (h_{sl_s}, h'_{sl_s}))$ and p' which satisfy conditions (1)-(4). Then we have
$$0 = \sum_{i=1}^{s} (\sum_{j=1}^{k_i} g_{ij} f_i g'_{ij} - \sum_{j=1}^{l_i} h_{ij} f_i h'_{ij}) + (p - p').$$
Now condition (2) implies that $\mathrm{LT}_\tau(p - p') \notin \langle \mathrm{LT}_\tau(f_1), \ldots, \mathrm{LT}_\tau(f_s) \rangle$ and condition (4) implies that for each $i \in \{1, \ldots, s\}$ the leading term of the corresponding summand with respect to τ is pairwise different from those of smaller index. Since it is $\mathrm{LT}_\tau(g_{ij} f_i g'_{ij}) >_\tau \mathrm{LT}_\tau(g_{ik} f_i g'_{ik})$ for $k \in \{j + 1, k_i\}$, we obtain $k_i = l_i$ and $p - p' = g_{11} f_i g'_{11} - h_{11} f_i h'_{11} = \cdots = g_{sk_s} f_i g'_{sk_s} - h_{sk_s} f_i h'_{sk_s} = 0$. □

The vector p in the output of the above algorithm is called the *normal remainder* of m with respect to $\mathcal{G} = (g_1, \ldots, g_s)$. We will denote it by $\mathrm{NR}_{\tau, \mathcal{G}}(m)$.

Definition 2.8. Let $g, m \in F_r$ and $G \subseteq F_r$.

1. If there exists a term $w_1 e_i w'_1 \in \mathrm{Supp}(m)$ and elements $w_2, w'_2 \in X^*$ such that $w_2 \,\mathrm{LT}_\tau(g) w'_2 = w_1 e_i w'_1$, we say that g *reduces m in one step* to $m' = m - \frac{c}{\mathrm{LC}_\tau(g)} w_2 g w'_2$ using the *rewrite rule* defined by g, and we denote it by $m \xrightarrow{g} m'$. Here $c \in K$ is the coefficient of $w_1 e_i w'_1$ in m.

(2) The reflexive and transitive closure of $\bigcup_{g\in G} \xrightarrow{g}$ is called the *rewrite relation* defined by G and is denoted by $\xrightarrow{G}$. By $\xleftrightarrow{G}$ we will denote the reflexive, symmetric and transitive closure of $\bigcup_{g\in G} \xrightarrow{g}$.

(3) An element $m \in F_r$ is called *irreducible* with respect to $\xrightarrow{G}$ if there is no $g \in G$ and no $m' \in F_r \setminus \{m\}$ such that $m \xrightarrow{g} m'$.

(4) A rewrite relation is called *Noetherian* if there is no infinite rewriting sequence. It is called *confluent* if for all $m, m_1, m_2 \in F_r$ such that $m \xrightarrow{G} m_1$ and $m \xrightarrow{G} m_2$ there exists an element $m_3 \in F_r$ such that $m_1 \xrightarrow{G} m_3$ and $m_2 \xrightarrow{G} m_3$. It is called *locally confluent* if for all $g_1, g_2 \in G$ and all $m, m_1, m_2 \in F_r$ such that $m \xrightarrow{g_1} m_1$ and $m \xrightarrow{g_2} m_2$ there exists an element $m_3 \in F_r$ such that $m_1 \xrightarrow{G} m_3$ and $m_2 \xrightarrow{G} m_3$. A rewrite relation which is Noetherian and confluent is called *convergent.*

(5) Let I be an index set, and let $G = \{g_i \mid i \in I\} \subseteq F_r \setminus \{0\}$. A pair (i,j) such that $i,j \in I$ and $i < j$ is called a *critical pair* of G if there are terms $w_i, w_i', w_j, w_j' \in X^*$ such that $w_i \operatorname{LT}_\tau(g_i) w_i' = w_j \operatorname{LT}_\tau(g_j) w_j'$. The set of all critical pairs of G will be denoted by B. For each pair $(i,j) \in B$, we call
$$S_{ij} = \frac{1}{\operatorname{LC}_\tau(g_i)} w_i g_i w_i' - \frac{1}{\operatorname{LC}_\tau(g_j)} w_j g_j w_j'$$
the *S-vector* of g_i and g_j.

Proposition 2.9. *Let $G \subseteq F_r \setminus \{0\}$, let M be the two-sided submodule generated by G, and let $m \in F_r$. Then the following conditions are equivalent.*

(1) *The set G is a τ-Gröbner basis of M.*

(2) *The rewrite relation $\xrightarrow{G}$ is convergent.*

(3) *There exists a unique element* $\operatorname{NF}_{\tau,M}(m) \in F_r$ *which is irreducible with respect to τ such that $m \xrightarrow{G} \operatorname{NF}_{\tau,M}(m)$. This element is called the* normal form *of m with respect to τ.*

(4) *We have $m \xrightarrow{G} 0$ if and only if $m \in M$.*

Proof. First we prove (1) ⇒ (2). Since τ is a well ordering, the rewrite relation $\xrightarrow{G}$ is Noetherian. For the proof of confluence, let $m, m_1, m_2 \in F_r$ be such that $m \xrightarrow{G} m_1$ and $m \xrightarrow{G} m_2$. Then the element $m_1 - m_2 \in M$ is irreducible with respect to $\xrightarrow{G}$, and we have $m_1 - m_2 = 0$, since G is a τ-Gröbner basis of M. Now the claim follows for $m_3 = m_1 = m_2$.

Next we show that (2) implies (3). Let $m \in F_r$. Since $\xrightarrow{G}$ is Noetherian, there exists an irreducible element $\operatorname{NF}_{\tau,M}(m) \in F_r$ such that $m \xrightarrow{G} \operatorname{NF}_{\tau,M}(m)$. Moreover, for each $m' \in F_r$ such that $m \xrightarrow{G} m'$ the confluence of $\xrightarrow{G}$ implies $m' \xrightarrow{G} \operatorname{NF}_{\tau,M}(m)$.

Now suppose that every element has a unique normal form. Let $m \in F_r$ be such that $m \xrightarrow{G} 0$. Thus we have a sequence $m \xrightarrow{g_1} m_1 \xrightarrow{g_2} \cdots \xrightarrow{g_{k-1}} m_{k-1} \xrightarrow{g_k} 0$ where $g_1, \dots, g_k \in G$ and $m_1, \dots, m_{k-1} \in F_r$ for some $k \in \mathbb{N}$. This yields a representation $m = \sum_{i_1}^k c_i w_i g_i w_i'$ with $c_i \in K \setminus \{0\}$, and with $w_i, w_i' \in X^*$ for $i = 1, \dots, k$. Hence $m \in \langle G \rangle = M$. Conversely, every $m \in M$ can be written as $m = \sum_{i_1}^k c_i w_i g_i w_i'$

inducing $m \xrightarrow{\{g_1,\dots,g_k\}} 0$. Now the claim follows from the uniqueness of $\mathrm{NF}_{\tau,M}(m)$ and from the fact that 0 is irreducible with respect to $\xrightarrow{G}$.

Finally, we show the implication (4) $\Rightarrow$ (1). So, let $m \in F_r$. Using (4), we get $m \xrightarrow{G} 0$. Thus there are elements $g_1, \dots, g_k \in G$ and $m_1, \dots, m_{k-1} \in M$ such that $m \xrightarrow{g_1} m_1 \xrightarrow{g_2} \cdots \xrightarrow{g_{k-1}} m_{k-1} \xrightarrow{g_k} 0$. Since in each reduction step one term is replaced by smaller ones with respect to τ and since the sequence finishes with 0, there has to be a point where the leading term of m is reduced. Therefore we have $\mathrm{LT}_\tau(m) = w_i \,\mathrm{LT}_\tau(g_i) w'_i$ for some $i \in \{1, \dots, k\}$, and this shows $\mathrm{LT}_\tau(m) \in \mathrm{LT}_\tau\{G\}$. □

At this point we can characterize Gröbner bases in the following way.

Theorem 2.10 (Buchberger's Criterion).
Let $G = \{g_i \mid i \in I\}$ be a (countable) set of elements in F_r which generate a two-sided submodule $M = \langle G \rangle$ of F_r, and let B be the set of critical pairs between elements of G. Then the set G is a τ-Gröbner basis of M if and only if $S_{ij} \xrightarrow{G} 0$ for all $(i, j) \in B$.

Proof. If G is a τ-Gröbner basis of M then Proposition 2.9 yields $m \xrightarrow{G} 0$ for every $m \in M$. Since the S-vector S_{ij} is contained in M for all $(i, j) \in B$, this implies $S_{ij} \xrightarrow{G} 0$.

Now suppose that $S_{ij} \xrightarrow{G} 0$ for every critical pair (i, j) of G. By Proposition 2.9, it suffices to show the convergence of $\xrightarrow{G}$. Since $\xrightarrow{G}$ is already Noetherian, only the local confluence of $\xrightarrow{G}$ has to be proved. Let $m, m_1, m_2 \in F_r$ and $g_i, g_j \in G$ be such that $m \xrightarrow{g_i} m_1$ and $m \xrightarrow{g_j} m_2$. Thus we have $m_1 = m - c_i w_i g_i w'_i$ and $m_2 = m - c_j w_j g_j w'_j$ for some $c_i, c_j \in K \setminus \{0\}$ and $w_i, w'_i, w_j, w'_j \in X^*$. First suppose that $w_i \,\mathrm{LT}_\tau(g_i) w'_i \neq w_j \,\mathrm{LT}_\tau(g_j) w'_j$, w.l.o.g. let $w_i \,\mathrm{LT}_\tau(g_i) w'_i >_\tau w_j \,\mathrm{LT}_\tau(g_j) w'_j$. If $w_j \,\mathrm{LT}_\tau(g_j) w'_j \notin \mathrm{Supp}(w_i g_i w'_i)$ then we obtain an element $m_3 = m - c_i w_i g_i w'_i - c_j w_j g_j w'_j$ such that $m_1 \xrightarrow{g_j} m_3$ and $m_2 \xrightarrow{g_i} m_3$. In the other case, the element $m_3 = m - c_i w_i g_i w'_i - (c_j - \frac{c c_i}{\mathrm{LC}_\tau(g_j)}) w_j g_j w'_j$ where $c \in K \setminus \{0\}$ is the coefficient of $w_j \,\mathrm{LT}_\tau(g_j) w'_j$ in $w_i g_i w'_i$ satisfies the reduction sequences $m_1 \xrightarrow{g_j} m_3$ and $m_2 \xrightarrow{g_i} m - c_i w_i g_i w'_i - c_j w_j g_j w'_j \xrightarrow{g_j} m_3$.

Now suppose that $w_i \,\mathrm{LT}_\tau(g_i) w'_i = w_j \,\mathrm{LT}_\tau(g_j) w'_j$. Then we have $m_2 - m_1 = c_i w_i g_i w'_i - c_j w_j g_j w'_j = c_i \,\mathrm{LC}_\tau(g_i) S_{ij}$, and our assumption implies $m_2 - m_1 \xrightarrow{G} 0$. Thus we obtain a reduction sequence $m_2 - m_1 \xrightarrow{g_{i_1}} m_2 - m_1 - c_{i_1} w_{i_1} g_{i_1} w'_{i_1} = f_1 \xrightarrow{g_{i_2}} \cdots \xrightarrow{g_{i_k}} f_k = 0$ with $c_{i_j} \in K \setminus \{0\}$, with $w_{i_j}, w'_{i_j} \in X^*$ and with $g_{i_j} \in G$ for $j = 1, \dots, k$. In this situation we have $c_{i_1} = c'_2 - c'_1$ where c'_1, c'_2 are the coefficients of $w_{i_1} \,\mathrm{LT}_\tau(g_{i_1}) w'_{i_1}$ in m_1 and m_2 respectively. Considering the reductions $m_1 \xrightarrow{g_{i_1}} m_1 - c'_1 w_{i_1} g_{i_1} w'_{i_1} = h_1$ and $m_2 \xrightarrow{g_{i_1}} m_2 - c'_2 w_{i_1} g_{i_1} w'_{i_1} = h'_1$, we get $f_1 = h'_1 - h_1$. By induction on k, there exist elements $h_k, h'_k \in M$ such that $m_1 \xrightarrow{G} h_k$, $m_2 \xrightarrow{G} h'_k$ and $f_k = h'_k - h_k$. Choosing $m_3 = h_k = h'_k$ yields the confluence of $\xrightarrow{G}$ which concludes the proof. □

This theorem enables us to formulate the following procedure for computing Gröbner bases of two-sided modules. Since these Gröbner bases need not be finite, we have to content ourselves with an enumerating procedure.

Corollary 2.11 (Buchberger's Procedure).
Let $G = \{g_1, \dots, g_s\} \subseteq F_r$ be a set of non-zero elements which generates a two-sided submodule $M \subseteq F_r$, and let $\mathcal{G} = (g_1, \dots, g_s)$. Consider the following sequence of instructions.

(B1) *Let B be the set of critical pairs of G and $s' = s$.*
(B2) *If $B = \emptyset$, return $\mathcal{G}$ and stop. Otherwise choose a pair $(i,j) \in B$ using a fair strategy and delete it from B.*
(B3) *Compute the S-vector S_{ij} and its normal remainder $\mathrm{NR}_{\tau,\mathcal{G}}(S_{ij})$. If the result is zero, continue with step (B2).*
(B4) *Increase s' by one. Append $g_{s'} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{ij})$ to $\mathcal{G}$, and append $\{(i,s') \mid 1 \le i < s'$ und (i,s') ist kritisches Paar$\}$ to B. Continue with step (B2).*

This is a procedure which enumerates a tuple $\mathcal{G}$ of vectors forming a τ-Gröbner basis of M. If M has a finite τ-Gröbner basis, it stops after finitely many steps and the vectors of the resulting tuple $\mathcal{G}$ form a finite τ-Gröbner basis of M.

Proof. We start by showing the correctness of the procedure. By Proposition 2.10, it suffices to show that, for every critical pair (i,j) which is appended to B at some point in the procedure, the corresponding S-vector reduces to zero. Let (i,j) be such a pair. Since we choose the next pair by a fair strategy in step (B2), the pair (i,j) is chosen at some point. Either the element $\mathrm{NR}_{\tau,\mathcal{G}}(S_{ij})$ is zero, or it is appended to $\mathcal{G}$ and the S-vector S_{ij} reduces to zero afterwards.

If there exits a finite τ-Gröbner basis $G = \{g'_1, \dots, g'_k\}$ of M, and if G is the enumerated τ-Gröbner basis of M then for each $j \in \{1, \dots, k\}$ the set G contains an element g_{i_j} such that $\mathrm{LT}_\tau(g'_j) = w \,\mathrm{LT}_\tau(g_{i_j}) w'$ with $w, w' \in X^*$. By this we obtain $\mathrm{LT}_\tau\{M\} = \{w \,\mathrm{LT}_\tau(g'_j) w' \mid j \in \{1, \dots, k\}, w, w' \in X^*\} \subseteq \{w \,\mathrm{LT}_\tau(g_{i_j}) w' \mid j \in \{1, \dots, k\}, w, w' \in X^*\} \subseteq \{w \,\mathrm{LT}_\tau(g_i) w' \mid i \in \{1, \dots, \max\{i_1, \dots, i_k\}\}, w, w' \in X^*\} \subseteq \mathrm{LT}_\tau\{M\}$. Hence $\{g_1, \dots, g_{\max\{i_1,\dots,i_k\}}\}$ forms a τ-Gröbner basis of M, and therefore we have $S_{ij} \xrightarrow{G} 0$ for all $(i,j) \in B$ after the procedure has appended the element $g_{\max\{i_1,\dots,i_k\}}$ to $\mathcal{G}$. Thus the set B is no longer enlarged and the procedure stops after treating all pairs in B. □

Our last topic in this section is to clarify the connection between the Gröbner basis theory for two-sided modules developed above and the usual Gröbner basis theory for two-sided ideals in $K[X^*]$.

Proposition 2.12. *Let σ be a term ordering on X^*, and let $I \subseteq K[X^*]$ be a two-sided ideal. Furthermore, let N be the two-sided submodule $N = \langle x_i e_1 - e_1 x_i \mid i \in \{1, \dots, n\}\rangle$ of F_1, and let τ be the module term ordering $\tau = \mathtt{Pos} - \sigma$.*

(1) *The map $\pi : F_1 \longrightarrow K[X^*]$ defined by $\pi(e_1) = 1$ induces an isomorphism of two-sided $K[X^*]$-modules $\bar{\pi} : F_1/N \xrightarrow{\sim} K[X^*]$.*
(2) *Let $I = \langle f_1, \dots, f_s\rangle$. Then we have $\pi^{-1}(I) = N + \langle e_1 f_1, \dots, e_1 f_s\rangle$.*
(3) *Let G be a τ-Gröbner basis of $\pi^{-1}(I)$. Then the set $\pi(G) \setminus \{0\}$ is a σ-Gröbner basis of I.*

Proof. To prove (1), we observe that the map π is a homomorphism of two-sided modules (see Proposition 2.2). Since π is obviously surjective and since

$\mathrm{Ker}(\pi) \supseteq N$, it suffices to show $\mathrm{Ker}(\pi) \subseteq N$. Let $m \in \mathrm{Ker}(\pi) \setminus N$ be such that m has minimal leading term with respect to τ. We write $m = \sum_{i=1}^{l} w_i e_1 w_i'$ with $c_i \in K \setminus \{0\}$, and with $w_i, w_i' \in X^*$ for $i = 1, \ldots, l$. W.l.o.g. let $w_1 e_1 w_1'$ be the leading term of m with respect to τ. Since we have $\pi(m) = \sum_{i=1}^{l} w_i w_i' = 0$, there exists an index $j \in \{2, \ldots, l\}$ such that $w_1 w_1' = w_j w_j'$. Thus $m' = m - c_1 w_1 e_1 w_1' + c_1 w_j e_1 w_j'$ is also an element of $\mathrm{Ker}(\pi)$, but is not contained in N, since we have $c_1 w_1 e_1 w_1' - c_1 w_j e_1 w_j' \in N$. This contradicts the choice of m, since $\mathrm{LT}_\tau(m') <_\tau \mathrm{LT}_\tau(m)$.

Next we prove (2). By (1) we know that $\mathrm{Ker}(\pi) = N$, and therefore we get $\pi(N + \langle e_1 f_1, \ldots, e_1 f_s \rangle) = \pi(\langle e_1 f_1, \ldots, e_1 f_s \rangle) \subseteq I$. To show the other inclusion, let $m \in \pi^{-1}(I)$. Then we can write $\pi(m) = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} f_i w_{ij}'$ with $c_{ij} \in K$, and with $w_{ij}, w_{ij}' \in X^*$ for $i = 1, \ldots, s$ and for all $j \in \mathbb{N}$ where all but finitely many of the elements c_{ij} are zero. Then the kernel of π contains the element $m - \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 f_i w_{ij}'$. Now we conclude $m \in \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 f_i w_{ij}' + N \subseteq \langle e_1 f_1, \ldots, e_1 f_s \rangle + N$.

For the proof of (3), we first show that we have $\mathrm{LT}_\sigma(\pi(m)) = \pi(\mathrm{LT}_\tau(m))$ for every $m \in F_1 \setminus \{0\}$. Let $m \in F_1 \setminus \{0\}$, and let $w_1 e_1 w_1'$ be the leading term of m with respect to τ. For every term $t \in \mathrm{Supp}(\pi(m))$ such that $t \neq w_1 w_1'$ there exists a term $w_2 e_1 w_2' \in \mathrm{Supp}(m)$ having the image $\pi(w_2 e_1 w_2') = t$. Then the fact that we have $\tau = \mathtt{Pos} - \sigma$ implies $\pi(\mathrm{LT}_\tau(m)) = w_1 w_1' >_\sigma w_2 w_2' = t$.

Now let G be a τ-Gröbner basis of $\pi^{-1}(I)$, and let $f \in I \setminus \{0\}$. Again we write $f = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} f_i w_{ij}'$. Then the element $\tilde{f} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 f_i w_{ij}'$ is contained in $\langle e_1 f_1, \ldots, e_1 f_s \rangle$ and satisfies $\pi(\tilde{f}) = f$. Since we have $w_{ij} e_1 - e_1 w_{ij} \in N$, we obtain another element $\overline{f} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} e_1 w_{ij} f_i w_{ij}' \in \pi^{-1}(I)$. Here we let $e_1 \overline{w}$ be the leading term of $\overline{f}$ with respect to τ. Since G is a τ-Gröbner basis of $\pi^{-1}(I)$, there exist elements $g \in G$ and $w, w' \in X^*$ such that $\mathrm{LT}_\tau(\overline{f}) = w \, \mathrm{LT}_\tau(g) w'$. This yields $w = 1$ and $\mathrm{LT}_\tau(g) = e_1 w''$ for some $w'' \in X^*$. Hence we have $e_1 \overline{w} = e_1 w'' w'$ and $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(\pi(\overline{f})) = \pi(\mathrm{LT}_\tau(\overline{f})) = w'' w' = \pi(\mathrm{LT}_\tau(g)) w'$ $= \mathrm{LT}_\sigma(\pi(g)) w'$. Now the claim follows from $\pi(g) \in \pi(G) \setminus \{0\}$. □

3. Elimination and Component Elimination Modules

In the following we let L be a subset of $\{1, \ldots, r\}$, and we let $\widehat{F}_r$ denote the free two-sided $K[X^*]$-module generated by $\{e_i \mid i \in \{1, \ldots, r\} \setminus L\}$.

Definition 3.1. Let $M \subseteq F_r$ be a two-sided submodule. A module term ordering τ on $\mathbb{T}(F_r)$ is called a *component elimination ordering* for L if every element $m \in F_r \setminus \{0\}$ such that $\mathrm{LT}_\tau(m) \in \widehat{F}_r$ is contained in $\widehat{F}_r$.

The two-sided submodule $M \cap \widehat{F}_r$ of $\widehat{F}_r$ is called the *component elimination module* of M with respect to L.

Example 3.2. Let $i \in \{1, \ldots, r\}$, and let $L = \{1, \ldots, i\}$. If `To` is a term ordering on X^* then the module ordering $\tau = \mathtt{PosTo}$ is a component elimination ordering for L. Namely, let $m \in F_r \setminus \{0\}$ be such that $\mathrm{LT}_\tau(M) = w_1 e_j w_1' \in \widehat{F}_r$. Then every term $t = w_2 e_k w_2' \in \mathrm{Supp}(m)$ satisfies $t \leq_\tau \mathrm{LT}_\tau(m)$. This implies $k \geq j$, and we conclude that $t \in \widehat{F}_r$ and $m \in \widehat{F}_r$.

The following theorem shows how one can compute component elimination modules. In fact, it yields a Gröbner basis with respect to the restriction to $\widehat{F}_r$ of the given component elimination ordering.

Theorem 3.3 (Computation of Component Elimination Modules).
Let M be a two-sided submodule of F_r, let $L \subseteq \{1, \dots, r\}$, and let τ be a component elimination ordering for L. Furthermore, let G be a τ-Gröbner basis of M, and let $\widehat{\tau}$ be the restriction of τ to $\mathbb{T}(\widehat{F}_r)$. Then the set $\widehat{G} = G \cap \widehat{F}_r$ is a $\widehat{\tau}$-Gröbner basis of $M \cap \widehat{F}_r$.

Proof. Let $m \in (M \cap \widehat{F}_r) \setminus \{0\}$. Then we have $\mathrm{LT}_{\widehat{\tau}}(m) = \mathrm{LT}_\tau(m) \in \mathrm{LT}_\tau\{M\}$ because $\widehat{\tau}$ is the restriction of τ. Since G is a τ-Gröbner basis of M, there exists an element $g \in G$ such that $\mathrm{LT}_{\widehat{\tau}}(m) = w \,\mathrm{LT}_\tau(g) w'$ for some $w, w' \in X^*$. But then we have $\mathrm{LT}_\tau(g) \in \widehat{F}_r$, and the assumption that τ is a component elimination ordering for L yields $g \in \widehat{F}_r$, i.e. $g \in \widehat{G} = G \cap \widehat{F}_r$. Now the fact that $\mathrm{LT}_\tau(g) = \mathrm{LT}_{\widehat{\tau}}(g)$ concludes the proof. □

Generalizing the methods and results of M. Caboara and C. Traverso, we first show how one can compute the intersection of two two-sided submodules of F_r using component elimination. In the following let F_{2r} denote the free two-sided $K[X^*]$-module with canonical basis $\{e_1, \dots, e_r, e_{r+1}, \dots, e_{2r}\}$.

Proposition 3.4 (Intersection of Submodules).
Let M and N be two-sided submodules of F_r, let $\{g_1, \dots, g_s\}$ be a system of generators of M, and let $\{h_1, \dots, h_t\}$ be a system of generators of N. For every $m \in F_r$, let $\overline{m}$ denote the corresponding element in F_{2r}. Finally, for every $h_k = \sum_{i=1}^r \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w'_{ij}$ let $h'_k = \sum_{i=1}^r \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij}$, and let V be the two-sided submodule of F_{2r} generated by $\{\overline{g}_1, \dots, \overline{g}_s, \overline{h}_1 - h'_1, \dots, \overline{h}_t - h'_t\}$. Then we have

$$V \cap \langle e_{r+1}, \dots, e_{2r} \rangle \cong M \cap N.$$

Proof. We consider the homomorphism $\psi : \widehat{F}_{2r} = \langle e_{r+1}, \dots, e_{2r} \rangle \longrightarrow F_r$ defined by $\psi(e_{r+i}) = e_i$ for $i = 1, \dots, r$. The restriction φ of ψ to $V \cap \widehat{F}_{2r}$ is obviously an injective homomorphism. Therefore it remains to show that $\mathrm{Im}(\varphi) = M \cap N$. For every $m \in M \cap N$ we can write $\overline{m} = \sum_{i=1}^s \sum_{j \in \mathbb{N}} b_{ij} v_{ij} \overline{g}_i v'_{ij}$, but also $\overline{m} = \sum_{i=1}^t \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{h}_i w'_{ij}$ with $b_{ij}, c_{kj} \in K$, and with $v_{ij}, v'_{ij}, w_{kj}, w'_{kj} \in X^*$ for $i = 1, \dots, s$, for $k = 1, \dots, t$ and for all $j \in \mathbb{N}$ where all but finitely many of the b_{ij} and c_{kj} are zero. From this we get $\overline{m} \in V$ and the element $m' = \sum_{i=1}^t \sum_{j \in \mathbb{N}} c_{ij} w_{ij} h'_i w'_{ij} \in \widehat{F}_{2r}$ such that $m' = \sum_{i=1}^t \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (h'_i - \overline{h}_i) w'_{ij} + \sum_{i=1}^t \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{h}_i w'_{ij} \in V$. Thus we found an element $m' \in V \cap \widehat{F}_{2r}$ satisfying $\varphi(m') = m$.

Conversely, let $\overline{m} \in V \cap \widehat{F}_{2r}$, i.e. we have $\overline{m} = \sum_{i=1}^s \sum_{j \in \mathbb{N}} b_{ij} v_{ij} \overline{g}_i v'_{ij} + \sum_{i=1}^t \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (\overline{h}_i - h'_i) w'_{ij}$. Applying φ yields $\varphi(\overline{m}) = \sum_{i=1}^s \sum_{j \in \mathbb{N}} b_{ij} v_{ij} g_i v'_{ij}$, and we get $\varphi(\overline{m}) \in M$. Furthermore, since $\overline{m}$ is contained in $\widehat{F}_{2r}$, we also have $\sum_{i=1}^s \sum_{j \in \mathbb{N}} b_{ij} v_{ij} \overline{g}_i v'_{ij} + \sum_{i=1}^t \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{h}_i w'_{ij} = 0$. Consequently, this implies $\varphi(\overline{m}) = -\sum_{i=1}^t \sum_{j \in \mathbb{N}} c_{ij} w_{ij} h_i w'_{ij} \in N$. Altogether, we conclude that $\mathrm{Im}(\varphi) = M \cap N$ and obtain the claim. □

Another application is the computation of two-sided syzygies of a tuple of vectors. More precisely, we want to compute the two-sided syzygy module which is defined as follows.

Definition 3.5. Let F_s be the free two-sided $K[X^*]$-module generated by $\{\varepsilon_1, \ldots, \varepsilon_s\}$, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of vectors of F_r. The *(two-sided) syzygy module* of $\mathcal{G}$ is defined as the kernel of the homomorphism $\lambda : F_s \longrightarrow F_r$ given by $\varepsilon_i \mapsto g_i$ for $i = 1, \ldots, s$. We will denote it by $\mathrm{Syz}(\mathcal{G})$.

The computation of two-sided syzygy modules is based on the following proposition. Let F_{r+s} be the free two-sided $K[X^*]$-module generated by $\{e_1, \ldots, e_{r+s}\}$.

Proposition 3.6. *Let $G = \{g_1, \ldots, g_s\} \subseteq F_r \setminus \{0\}$, let $\mathcal{G} = (g_1, \ldots, g_s)$, and for every $m \in F_r$ let $\overline{m}$ denote the corresponding element in F_{r+s}. Let U be the two-sided submodule of F_{r+s} generated by $\{\overline{g}_1 - e_{r+1}, \ldots, \overline{g}_s - e_{r+s}\}$. Then we have*

$$U \cap \langle e_{r+1}, \ldots, e_{r+s} \rangle \cong \mathrm{Syz}(\mathcal{G}).$$

Proof. We consider the homomorphism $\psi : \widehat{F}_{r+s} = \langle e_{r+1}, \ldots, e_{r+s} \rangle \longrightarrow F_s$ given by $e_{r+i} \mapsto \varepsilon_i$ for $i = 1, \ldots, s$. Again we obtain an injective homomorphism φ by restricting ψ to $U \cap \widehat{F}_{r+s}$. Therefore it suffices to prove that $\mathrm{Im}(\varphi) = \mathrm{Syz}(\mathcal{G})$. Let $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij}$ be an element of $\mathrm{Syz}(\mathcal{G})$ with $c_{ij} \in K$, and with $w_{ij}, w'_{ij} \in X^*$ for $i = 1, \ldots, s$ and for all $j \in \mathbb{N}$ where all but finitely many of the elements c_{ij} are zero. Then the element $\overline{m} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{g}_i w'_{ij} - \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (\overline{g} - e_{r+i}) w'_{ij}$ is contained in $U \cap \widehat{F}_{r+s}$, and it satisfies $\varphi(\overline{m}) = m$.

Now let $U \cap \widehat{F}_{r+s}$ contain the element $\overline{m} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij}$. Then we have $\lambda(\varphi(\overline{m})) = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{g}_i w'_{ij} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (\overline{g} - e_{r+i}) w'_{ij} + \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij} \in U$. Moreover, none of the free generators $e_{r+1}, \ldots, e_{r+s}$ appears in the representation of $\lambda(\varphi(\overline{m}))$. Since U is generated by the elements $\{\overline{g}_1 - e_{r+1}, \ldots, \overline{g}_s - e_{r+s}\}$, this implies $\lambda(\varphi(\overline{m})) = 0$. Hence we get $\varphi(\overline{m}) \in \mathrm{Syz}(\mathcal{G})$. □

Using the result of the above proposition, we are able to formulate the following procedure for the computation of the syzygy module of a tuple of vectors in F_r.

Theorem 3.7 (Computation of Two-Sided Syzygy Modules over $K[X^*]$).
Let $G = \{g_1, \ldots, g_s\} \subseteq F_r \setminus \{0\}$ and let $\mathcal{G} = (g_1, \ldots, g_s)$. Let $\varphi : \widehat{F}_{r+s} \longrightarrow F_s$ be the homomorphism defined by $e_{r+i} \mapsto \varepsilon_i$ for $i = 1, \ldots, s$, and for every $m \in F_r$ let $\overline{m}$ denote the corresponding element in F_{r+s}. Consider the following sequence of instructions.

1. *Choose a component elimination ordering τ for $L = \{1, \ldots, r\}$ on $\mathbb{T}(F_{r+s})$.*
2. *Compute a τ-Gröbner basis G of the two-sided submodule $U = \langle \overline{g}_1 - e_{r+1}, \ldots, \overline{g}_s - e_{r+s} \rangle$ of F_{r+s}.*
3. *Compute $\widehat{G} = G \cap \widehat{F}_{r+s}$. Return $\varphi(\widehat{G})$ and stop.*

This is a procedure which enumerates a $\widehat{\tau}$-Gröbner basis of the two-sided syzygy module $\mathrm{Syz}(\mathcal{G})$ of $\mathcal{G}$ where $\widehat{\tau}$ is the restriction of τ to $\mathbb{T}(\widehat{F}_{r+s})$.

Proof. By Proposition 3.6, the two-sided module $U \cap \widehat{F}_{r+s}$ is isomorphic to $\mathrm{Syz}(\mathcal{G})$. Since $U \cap \widehat{F}_{r+s}$ is also the component elimination module of U with respect to L, Theorem 3.3 implies that the set $\widehat{G}$ computed in step (3) of the procedure forms a $\widehat{\tau}$-Gröbner basis of $U \cap \widehat{F}_{r+s}$, i.e. the set $\varphi(\widehat{G})$ is a $\widehat{\tau}$-Gröbner basis of $\mathrm{Syz}(\mathcal{G})$. □

Combining the results of Proposition 3.4 and of Proposition 3.6, we obtain a procedure for computing the intersection of two syzygy modules based on the following proposition.

Proposition 3.8. *Let $\mathcal{G} = (g_1, \dots, g_s), \mathcal{H} = (h_1, \dots, h_s) \in F_r^s$, and for every $m \in F_r$ let $\overline{m}$ denote the corresponding element in F_{2r+2s}. Furthermore, for every $h_i = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w'_{ij}$ let $h' = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij} \in F_{2r+2s}$, and let U be the two-sided submodule of F_{2r+2s} generated by $\{\overline{g}_1 - e_{2r+1}, \dots, \overline{g}_s - e_{2r+s}, h'_1 - e_{2r+1} - e_{2r+s+1}, \dots, h'_s - e_{2r+s} - e_{2r+2s}\}$. Then we have*

$$U \cap \langle e_{2r+s+1}, \dots, e_{2r+2s} \rangle \cong \operatorname{Syz}(\mathcal{G}) \cap \operatorname{Syz}(\mathcal{H}).$$

Proof. We let $\widehat{F}_{2r+2s} = \langle e_{2r+s+1}, \dots, e_{2r+2s} \rangle$ and consider the homomorphism $\psi : \widehat{F}_{2r+2s} \longrightarrow F_s$ given by $e_{2r+s+i} \mapsto \varepsilon_i$ for $i = 1, \dots, s$. We will show that $\operatorname{Syz}(\mathcal{G}) \cap \operatorname{Syz}(\mathcal{H})$ equals the image of φ where φ is the restriction of ψ to $U \cap \widehat{F}_{2r+2s}$. Since φ is obviously an injective homomorphism, this fact will conclude the proof.

First let $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij}$ be an element of $\operatorname{Syz}(\mathcal{G}) \cap \operatorname{Syz}(\mathcal{H})$ with $c_{ij} \in K$, and with $w_{ij}, w'_{ij} \in X^*$ for $i = 1, \dots, s$ and for all $j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. The element $m' = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{2r+s+i} w'_{ij}$ is contained in $\widehat{F}_{2r+2s}$ and satisfies $\varphi(m') = m$. Moreover, we can write m' as $m' = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (h'_i - e_{2r+i}) w'_{ij} - \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (h'_i - e_{2r+i} - e_{2r+s+i}) w'_{ij}$ where the second summand is an element of U. Since we have $m \in \operatorname{Syz}(\mathcal{G}) \cap \operatorname{Syz}(\mathcal{H})$, the first summand is equal to $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (\overline{g}_i - e_{2r+i}) w'_{ij} \in U$. Hence m' is already contained in U.

Now we let $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{2r+s+i} w'_{ij}$ be an element of $U \cap \widehat{F}_{2r+2s}$. The above equation yields $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (h'_i - e_{2r+i}) w'_{ij} \in U$. Using the fact that U contains the element $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (\overline{g}_i - e_{2r+i}) w'_{ij}$, we get $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (h'_i - \overline{g}_i) w'_{ij} \in U$. Since none of the generators $e_{2r+1}, \dots, e_{2r+2s}$ appears in this sum, we must have $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (h'_i - \overline{g}_i) w'_{ij} = 0$, i.e. $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} h'_i w'_{ij} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{g}_i w'_{ij}$. Now, from the facts that we have $g_i \in \langle e_1, \dots, e_r \rangle$ and $h'_i \in \langle e_{r+1}, \dots, e_{2r} \rangle$ for $i = 1, \dots, s$, it follows that both sums are zero. Hence the image of m under φ is a two-sided syzygy of $\mathcal{G}$ and of $\mathcal{H}$. □

In the same way as in Theorem 3.7, we obtain a procedure for computing the module of two-sided syzygies of tuples of polynomials instead of vectors. For this purpose we need a condition equivalent to Proposition 3.6.

Proposition 3.9. *Let $G = \{g_1, \dots, g_s\} \subseteq K[X^*] \setminus \{0\}$, let $\mathcal{G} = (g_1, \dots, g_s)$, and let U be the two-sided submodule of F_{s+1} generated by $\{e_1 g_1 - e_2, \dots, e_1 g_s - e_{s+1}, x_1 e_1 - e_1 x_1, \dots, x_n e_1 - e_1 x_n\}$. Then we have*

$$U \cap \langle e_2, \dots, e_{s+1} \rangle \cong \operatorname{Syz}(\mathcal{G}).$$

Proof. In analogy to the proof of Proposition 3.6, we consider the injective homomorphism $\varphi : U \cap \widehat{F}_{s+1} \longrightarrow F_s$ given by $\varphi(e_{i+1}) = \varepsilon_i$ for $i = 1, \dots, s$ and show $\operatorname{Im}(\varphi) = \operatorname{Syz}(\mathcal{G})$. First we let $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij} \in \operatorname{Syz}(\mathcal{G})$ with $c_{ij} \in K$, and with $w_{ij}, w'_{ij} \in X^*$ for $i = 1, \dots, s$ and for all $j \in \mathbb{N}$ where all but finitely many of the elements c_{ij} are zero. Again we have the element $\overline{m} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{i+1} w'_{ij} \in \widehat{F}_{s+1}$ such that $\varphi(\overline{m}) = m$. Now we can write $\overline{m} = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij} - \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (e_1 g_i - e_{i+1}) w'_{ij}$ where the right summand is contained in U. The left summand is equal to $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} e_1 w_{ij} g_i w'_{ij} +$

$\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}(w_{ij}e_1 - e_1w_{ij})g_iw'_{ij}$. Here the second summand is again contained in U because $w_{ij}e_1 - e_1w_{ij} \in N$ for $i = 1,\ldots,s$ and for all $j \in \mathbb{N}$. And since we have $m \in \mathrm{Syz}(\mathcal{G})$, the first summand equals zero. Altogether, we conclude that $\overline{m} \in U \cap \widehat{F}_{s+1}$.

Now let $U \cap \widehat{F}_{s+1}$ contain the element $\overline{m} = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_{i+1}w'_{ij}$, and let $m' = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_1g_iw'_{ij}$. Then we get $\lambda(\varphi(\overline{m})) = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_iw'_{ij} = \pi(m')$. If we write m' as $m' = \overline{m} + \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_1g_i - e_{i+1})w'_{ij}$, we see that $m' \in U$ and even $m' \in N$, since none of the generators $e_2,\ldots,e_{s+1}$ is contained in the representation of m'. Thus, by Proposition 2.12 (1), we deduce $\lambda(\varphi(\overline{m})) = \pi(m') = 0$ and therefore $\varphi(\overline{m}) \in \mathrm{Syz}(\mathcal{G})$. □

Corollary 3.10. *Let $G = \{g_1,\ldots,g_s\} \subseteq K[X^*] \setminus \{0\}$, let $\mathcal{G} = (g_1,\ldots,g_s)$, and let $\varphi : \widehat{F}_{s+1} \longrightarrow F_s$ be the homomorphism defined by $e_{i+1} \mapsto \varepsilon_i$ for $i = 1,\ldots,s$. Consider the following sequence of instructions.*

1. *Choose a component elimination ordering τ for $L = \{1\}$ on $\mathbb{T}(F_{s+1})$.*
2. *Compute a τ-Gröbner basis G of the two-sided submodule $U = \langle e_1g_1 - e_2,\ldots,e_1g_s - e_{s+1}, x_1e_1 - e_1x_1,\ldots,x_ne_1 - e_1x_n\rangle$ of F_{s+1}.*
3. *Compute $\widehat{G} = G \cap \widehat{F}_{s+1}$. Return $\varphi(\widehat{G})$ and stop.*

This is a procedure which enumerates a $\widehat{\tau}$-Gröbner basis of the two-sided syzygy module $\mathrm{Syz}(\mathcal{G})$ *of $\mathcal{G}$ where $\widehat{\tau}$ is the restriction of τ to $\mathbb{T}(\widehat{F}_{s+1})$.*

Proof. The claim is a direct consequence of Theorem 3.3 and Proposition 3.9. □

4. Two-Sided Syzygies over Residue Class Rings of $K[X^*]$

In this section we let $I \subseteq K[X^*]$ be a two-sided ideal, we let $G_I = \{f_1,\ldots,f_t\}$ be a σ-Gröbner basis of I, and we let $R = K[X^*]/I$. First we give a short introduction to Gröbner basis theory of two-sided R-submodules of the free two-sided R-module $\overline{F}_r = \bigoplus_{i=1}^{r} R^{\mathrm{env}}$. For this purpose we generalize the theory of prefix Gröbner bases of K. Madlener and B. Reinert.

In the following we denote the residue class of an element $f \in K[X^*]$ in R by $\overline{f}$. Since G_I is a σ-Gröbner basis of I by assumption, the rewrite relation $\xrightarrow{G_I}$ is convergent (see Proposition 2.9). Therefore every element in $K[X^*]$ has a unique normal form. Hence we let a residue class $\overline{f} \in R$ always be represented by an irreducible element $f \in K[X^*]$ with respect to $\xrightarrow{G_I}$.

Now we let $\mathbb{T}(R) = \{\overline{w} \mid w \in X^*, w \text{ irreducible with respect to } \xrightarrow{G_I}\}$ denote the set of all terms in R. The product of two terms $w_1, w_2 \in \mathbb{T}(R)$ will be written as w_1w_2 and the concatenation of the corresponding elements in $K[X^*]$ as $w_1 \cdot w_2$. Moreover, we will denote the identity in $K[X^*]$ by $\equiv$.

In order to define a Gröbner basis we need a module term ordering on $\mathbb{T}(\overline{F}_r)$. But in our setting we can have $wt_1w' >_\tau wt_2w'$ for terms $t_1, t_2 \in \mathbb{T}(\overline{F}_r)$ and $w, w' \in \mathbb{T}(R)$ where $t_1 \leq_\tau t_2$. Therefore we use rewrite relations to introduce Gröbner bases. Then for elements $m, g \in \overline{F}_r$ we have to decide whether there exists a term $t \in \mathrm{Supp}(m)$ such that $t = w\,\mathrm{LT}_\tau(g)w'$ for some $w, w' \in \mathbb{T}(R)$. Since this is not solvable in $\mathbb{T}(R)$, we consider $t \equiv w \cdot \mathrm{LT}_\tau(g) \cdot w'$ instead of the equation $t = w\,\mathrm{LT}_\tau(g)w'$ in analogy to the theory of prefix rewriting.

Definition 4.1. Let $g, m \in \overline{F}_r$, and let $G \subseteq \overline{F}_r$. If there exists a term $w_1 e_i w'_1 \in \operatorname{Supp}(m)$ and elements $w_2, w'_2 \in \mathbb{T}(R)$ such that $w_2 \cdot \operatorname{LT}_\tau(g) \cdot w'_2 \equiv w_1 e_i w'_1$, we say that *$g$ reduces m in a two-sided reduction step* to $m' = m - \frac{c}{\operatorname{LC}_\tau(g)} w_2 g w'_2$, and we denote it by $m \xrightarrow{g}_* m'$. Here $c \in K$ is the coefficient of $w_1 e_i w'_1$ in m.

The reflexive and transitive closure of $\bigcup_{g \in G} \xrightarrow{g}_*$ will be denoted by $\xrightarrow{G}_*$ and the reflexive, symmetric and transitive closure by $\xleftrightarrow{G}_*$.

For every two-sided reduction step, we have $\operatorname{LT}_\tau(m) >_\tau \operatorname{LT}_\tau(m')$ because of the following lemma.

Lemma 4.2. *Let $m = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} e_i \overline{w}'_{ij}$ be a non-zero element of $\overline{F}_r$ with $c_{ij} \in K$, and with $\overline{w}_{ij}, \overline{w}'_{ij} \in \mathbb{T}(R)$ such that w_{ij} and w'_{ij} are irreducible with respect to $\xrightarrow{G_I}$ for $i = 1, \ldots, r$ and for all $j \in \mathbb{N}$. Furthermore, let $\overline{w}_1 e_k \overline{w}'_1$ be the leading term of m with respect to τ, and let $\overline{w}, \overline{w}' \in \mathbb{T}(R)$ be such that $w w_1$ and $w'_1 w'$ are irreducible with respect to $\xrightarrow{G_I}$. Then we have*

$$\overline{w} \cdot \operatorname{LT}_\tau(m) \cdot \overline{w}' \equiv \overline{w} \operatorname{LT}_\tau(m) \overline{w}' = \operatorname{LT}_\tau(\overline{w} m \overline{w}').$$

Proof. Since $w w_1$ and $w'_1 w'$ are irreducible with respect to $\xrightarrow{G_I}$, we already know $\overline{w} \cdot \operatorname{LT}_\tau(m) \cdot \overline{w}' \equiv \overline{w} \operatorname{LT}_\tau(m) \overline{w}'$. Moreover, for every term $t = \overline{w}_2 e_l \overline{w}'_2 \in \operatorname{Supp}(m)$ we get $\overline{w} t \overline{w}' \leq_\tau \overline{w} \cdot t \cdot \overline{w}' \equiv w w_2 e_l w'_2 w' \leq_\tau w w_1 e_k w'_1 w' \equiv \overline{w w_1} e_k \overline{w'_1 w'}$. We deduce that every term in $\overline{w} m \overline{w}'$ is smaller than or equal to $\overline{w} \operatorname{LT}_\tau(m) \overline{w}'$ which concludes the proof. □

For every subset G of $\overline{F}_r$ the rewrite relation $\xrightarrow{G}_*$ is again Noetherian. However, it is not true that $m \xleftrightarrow{G}_* 0$ for every element m of the two-sided R-module generated by G. Hence we define a Gröbner basis in the following way.

Definition 4.3. Let M be a two-sided R-submodule of $\overline{F}_r$. A set $G \subseteq M$ is called a *(two-sided) Gröbner basis* of M if the rewrite relation $\xrightarrow{G}_*$ is confluent and if we have $m \xleftrightarrow{G}_* 0$ for all $m \in M$.

The following proposition shows that two-sided Gröbner bases defined in this way share many of the nice properties of normal Gröbner bases.

Proposition 4.4. *Let M be a two-sided R-submodule of $\overline{F}_r$, and let $G \subseteq M$. Then the following conditions are equivalent.*

1. *The set G is a Gröbner basis of M.*
2. *Every non-zero element $m \in M$ can be written as $m = \sum_{i=1}^{k} c_i w_i g_i w'_i$ with $c_i \in K \setminus \{0\}$, with $w_i, w'_i \in \mathbb{T}(R)$ and with $g_i \in G$ such that $\operatorname{LT}_\tau(m) \geq_\tau w_i \cdot \operatorname{LT}_\tau(g_i) \cdot w'_i \geq_\tau \operatorname{LT}_\tau(w_i g_i w'_i)$ for $i = 1, \ldots, k$.*
3. *We have $\operatorname{LT}_\tau\{M\} = \{w \cdot \operatorname{LT}_\tau(g) \cdot w' \mid g \in G, w, w' \in \mathbb{T}(R)\}$.*

Proof. First we prove (1) ⇒ (2). For every $m \in M \setminus \{0\}$ we have $m \xleftrightarrow{G}_* 0$, since G is a Gröbner basis of M. From the facts that zero is always irreducible and that the normal form of an element is unique we can even conclude that $m \xrightarrow{G}_* 0$. Thus we can write m as $m = \sum_{i=1}^{k} c_i w_i g_i w'_i$ with $c_i \in K \setminus \{0\}$, with $w_i, w'_i \in \mathbb{T}(R)$, and with $g_i \in G$ for $i = 1, \ldots, k$. But then we already have $\operatorname{LT}_\tau(m) \geq_\tau w_i \cdot \operatorname{LT}_\tau(g_i) \cdot w'_i \equiv \operatorname{LT}_\tau(w_i g_i w'_i)$.

To show that (2) implies (3), we assume that $m \in M$ has a representation as in (2). Then there must be an index $i \in \{1, \dots, k\}$ such that $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(w_i g_i w_i')$. By Lemma 4.1, we obtain $\mathrm{LT}_\tau(m) \equiv w_i \cdot \mathrm{LT}_\tau(g_i) \cdot w_i'$.

Finally, we prove the implication (3) $\Rightarrow$ (1). Let $m \in M \setminus \{0\}$. By condition (3), there exist elements $w_1, w_1' \in \mathbb{T}(R)$ and $g_1 \in G$ such that $\mathrm{LT}_\tau(m) \equiv w_1 \cdot \mathrm{LT}_\tau(g_1) \cdot w_1'$. The corresponding two-sided reduction of m by g_1 yields an element $m_1 = m - \frac{\mathrm{LC}_\tau(m)}{\mathrm{LC}_\tau(g_1)} w_1 g_1 w_1' \in M$ where $\mathrm{LT}_\tau(m) >_\tau \mathrm{LT}_\tau(m_1)$. If m_1 is not zero, we find another element $g_2 \in G$ which reduces m_1 in a two-sided step to $m_2 \in M$. Again we have $\mathrm{LT}_\tau(m_1) >_\tau \mathrm{LT}_\tau(m_2)$. Since the rewrite relation $\xrightarrow{G}_*$ is Noetherian, this can be done only finitely many times. Hence we obtain elements $g_1, \dots, g_l \in G$ and $m_1, \dots, m_l \in M$ such that $m \xrightarrow{g_1}_* m_1 \xrightarrow{g_2}_* \cdots \xrightarrow{g_l}_* m_l$. Now m_l is irreducible with respect to $\xrightarrow{G}_*$. This implies $m = 0$, i.e. $m \xrightarrow{G}_* 0$. The confluence of $\xrightarrow{G}_*$ follows in the same way as in the proof of Proposition 2.9. □

The computation of the two-sided syzygy module of a tuple $(\overline{g}_1, \dots, \overline{g}_s) \in R^s$, which is again defined as the kernel of the homomorphism $\overline{\lambda} : \overline{F}_s \longrightarrow R$, $\varepsilon_i \mapsto g_i$, consists of two steps. First we compute the corresponding syzygy module over $K[X^*]$ by Corollary 3.9. Then we project the result to our setting via the following mapping. The canonical surjective homomorphism $\eta : K[X^*] \longrightarrow R$, $f \mapsto \overline{f}$ induces a homomorphism $\tilde{\eta} = \eta \otimes_K \eta : F_1 \longrightarrow \overline{F}_1$ of two-sided modules which can be extended to the free $K[X^*]$-module F_s generated by $\{\varepsilon_1, \dots, \varepsilon_s\}$. In the following we let $\psi : F_{s+t} \longrightarrow \overline{F}_s$ be the homomorphism given by $\sum_{i=1}^{s+t} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w_{ij}' \mapsto \sum_{i=s+1}^{s+t} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \varepsilon_{i-s} \overline{w}_{ij}'$. We still have $R = K[X^*]/I$ where I is the two-sided ideal generated by $\{f_1, \dots, f_t\}$.

Proposition 4.5. *Let* $\overline{\mathcal{G}} = (\overline{g}_1, \dots, \overline{g}_s) \in R^s$*, and let* $\mathcal{G} = (g_1, \dots, g_s, f_1, \dots, f_t)$ *be a tuple in* $K[X^*]^{s+t}$*. Furthermore, let* $\tilde{\tau}$ *be a module term ordering on* $\mathbb{T}(F_{s+t})$ *such that* τ *is the restriction of* $\tilde{\tau}$ *to* $\mathbb{T}(F_s)$ *and such that we have* $\varepsilon_i >_{\tilde{\tau}} \varepsilon_j$ *for all* $i \in \{1, \dots, s\}$ *and for all* $j \in \{s+1, \dots, s+t\}$*. If* G *is a* $\tilde{\tau}$*-Gröbner basis of* $\mathrm{Syz}(\mathcal{G})$ *then* $\psi(G) \setminus \{0\}$ *is a Gröbner basis of* $\mathrm{Syz}(\overline{\mathcal{G}})$.

Proof. We start by showing $\psi(G) \subseteq \mathrm{Syz}(\overline{\mathcal{G}})$. Let g be an element of G. We can write $g = \sum_{i=1}^{s+t} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w_{ij}'$ with $c_{ij} \in K$, and with $w_{ij}, w_{ij}' \in X^*$ for $i = 1, \dots, s+t$ and for all $j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. Then we have $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w_{ij}' + \sum_{i=s+1}^{s+t} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} f_{i-s} w_{ij}' = 0$. From this we can see that $\psi(g) = \sum_{i=1}^{s} c_{ij} \overline{w}_{ij} \overline{g}_i \overline{w}_{ij}' = \overline{0}$ and therefore $\psi(g) \in \mathrm{Syz}(\overline{\mathcal{G}})$.

Now let G be a $\tilde{\tau}$-Gröbner basis of $\mathrm{Syz}(\mathcal{G})$, and let $m \in \mathrm{Syz}(\overline{\mathcal{G}}) \setminus \{0\}$. The element m can be written as $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \varepsilon_i \overline{w}_{ij}'$ with $c_{ij} \in K$, and with $\overline{w}_{ij}, \overline{w}_{ij}' \in \mathbb{T}(R)$ for $i = 1, \dots, s$ and for all $j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. The equation $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \overline{g}_i \overline{w}_{ij}' = \overline{0}$ implies $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \cdot \overline{g}_i \cdot \overline{w}_{ij}' \in I$. Thus there are elements $b_{ij} \in K$ and $v_{ij}, v_{ij}' \in X^*$ for $i = 1, \dots, t$ and for $j \in \mathbb{N}$ such that $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \cdot \overline{g}_i \cdot \overline{w}_{ij}' = \sum_{i=1}^{t} \sum_{j \in \mathbb{N}} b_{ij} v_{ij} f_i v_{ij}'$. In other words, we have $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w_{ij}' - \sum_{i=1}^{t} \sum_{j \in \mathbb{N}} b_{ij} v_{ij} f_i v_{ij}' = 0$. Hence the element $m' = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w_{ij}' - \sum_{i=1}^{t} \sum_{j \in \mathbb{N}} b_{ij} v_{ij} \varepsilon_{s+i} v_{ij}'$ is contained in $\mathrm{Syz}(\mathcal{G})$ and satisfies $\psi(m') = m$. Since G is a $\tilde{\tau}$-Gröbner basis of $\mathrm{Syz}(\mathcal{G})$ and since the leading monomial of m' is a summand in the first sum, there exist elements $g \in G$ and $w, w' \in X^*$ such that $w \, \mathrm{LT}_{\tilde{\tau}}(g) w' = \mathrm{LT}_{\tilde{\tau}}(m') \equiv \mathrm{LT}_\tau(m)$. The claim is proved if we show the validity of the relation $\overline{w} \cdot \mathrm{LT}_\tau(\psi(g)) \cdot \overline{w}' \equiv \mathrm{LT}_\tau(m)$. Let $\mathrm{LT}_{\tilde{\tau}}(m') = w_{ij}\varepsilon_i w'_{ij}$ for some $i \in \{1, \dots, s\}$ and some $j \in \mathbb{N}$, and let $\mathrm{LT}_{\tilde{\tau}}(g) = w_1 \varepsilon_i w_2$ with $w_1, w_2 \in X^*$. Since w_{ij} and w'_{ij} are irreducible with respect to $\xrightarrow{G_I}$, the elements w_1 and w_2 are also irreducible. Thus we have $\mathrm{LT}_\tau(\psi(g)) = \psi(\mathrm{LT}_{\tilde{\tau}}(g))$. Now the claim follows from $\mathrm{LT}_\tau(m) \equiv \overline{w} \cdot \mathrm{LT}_{\tilde{\tau}}(g) \cdot \overline{w}' \equiv \overline{w} \cdot \psi(\mathrm{LT}_{\tilde{\tau}}(g)) \cdot \overline{w}' \equiv \overline{w} \cdot \mathrm{LT}_\tau(\psi(g)) \cdot \overline{w}'$. □

Finally, by combining the preceding results we obtain the following procedure for computing the module of two-sided syzygies of a tuple of elements of R.

Proposition 4.6 (Computation of Two-Sided Syzygy Modules over R). *Let $\overline{\mathcal{G}} = (\overline{g}_1, \dots, \overline{g}_s) \in R^s$, and let U be the two-sided $K[X^*]$-submodule of F_{s+1} generated by $\{\varepsilon_1 g_1 - \varepsilon_2, \dots, \varepsilon_1 g_s - \varepsilon_{s+1}, \varepsilon_1 f_1, \dots, \varepsilon_1 f_t, x_1\varepsilon_1 - \varepsilon_1 x_1, \dots, x_n \varepsilon_1 - \varepsilon_1 x_n\}$. Consider the following sequence of instructions.*

(1) *Choose a component elimination ordering $\tilde{\tau}$ for $L = \{1\}$ on $\mathbb{T}(F_{s+1})$ such that τ is the restriction of $\tilde{\tau}$ on $\mathbb{T}(F_s)$.*
(2) *Compute a $\tilde{\tau}$-Gröbner basis G of U.*
(3) *Compute $\widehat{G} = G \cap \widehat{F}_{s+1}$. Return $\psi(\widehat{G}) \setminus \{0\}$ and stop.*

This is a procedure which enumerates a Gröbner basis of the two-sided syzygy module of $\overline{\mathcal{G}}$.

Proof. First we prove that $\psi(U \cap \widehat{F}_{s+1}) \subseteq \mathrm{Syz}(\overline{\mathcal{G}})$. Let $m \in U \cap \widehat{F}_{s+1}$. Here we can write m as $m = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \varepsilon_{i+1} w'_{ij}$ with $c_{ij} \in K$, and with $w_{ij}, w'_{ij} \in X^*$ for $i = 1, \dots, s$ and for all $j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. If we let $m' = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \varepsilon_1 g_i w'_{ij}$, we get the equation $m = m' - \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} (\varepsilon_1 g_i - \varepsilon_{i+1}) w'_{ij}$. Since the second summand is contained in U, we also have $m' \in U$. Moreover, none of the generators $\varepsilon_2, \dots, \varepsilon_{s+1}$ appears in the representation of m'. Thus m' is even an element of the two-sided $K[X^*]$-submodule of F_{s+1} generated by $\{\varepsilon_1 f_1, \dots, \varepsilon_1 f_t, x_1 \varepsilon_1 - \varepsilon_1 x_1, \dots, x_n \varepsilon_1 - \varepsilon_1 x_n\}$, and we can write m' as $m' = \sum_{i=1}^t \sum_{j\in\mathbb{N}} b_{ij} v_{ij} \varepsilon_1 f_i v'_{ij} + m''$ with $m'' \in N$, with $b_{ij} \in K$, and with $v_{ij}, v'_{ij} \in X^*$ for $i = 1, \dots, t$ and for all $j \in \mathbb{N}$ where all but finitely many of the b_{ij} are zero. By applying the homomorphisms $\overline{\lambda}$ and ψ to m, we get $\overline{\lambda}(\psi(m)) = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} \overline{w}_{ij} \overline{g}_i \overline{w}'_{ij} = \overline{\pi(m')} = \sum_{i=1}^t \sum_{j\in\mathbb{N}} b_{ij} \overline{v}_{ij} \overline{f}_i \overline{v}'_{ij} = \overline{0}$. Hence we can conclude that $\psi(m) \in \mathrm{Syz}(\overline{\mathcal{G}})$.

Now we prove that the set $\psi(\widehat{G})$ is in fact a Gröbner basis of $\mathrm{Syz}(\overline{\mathcal{G}})$. By Theorem 3.3, the set $\widehat{G}$ computed in steps (2) and (3) is a τ-Gröbner basis of $U \cap \widehat{F}_{s+1}$. We take an element $m \in \mathrm{Syz}(\overline{\mathcal{G}}) \setminus \{0\}$, i.e. $m = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} \overline{w}_{ij} \varepsilon_i \overline{w}'_{ij}$ with $c_{ij} \in K$, and with $\overline{w}_{ij}, \overline{w}'_{ij} \in \mathbb{T}(R)$ for $i = 1, \dots, s$ and for all $j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. Then the element $m' = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \varepsilon_{i+1} w'_{ij}$ is contained in $\widehat{F}_{s+1}$ and it satisfies $\psi(m') = m$. Again we can write $m' = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \varepsilon_1 g_i w'_{ij} - \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} (\varepsilon_1 g_i - \varepsilon_{i+1}) w'_{ij}$ where the second summand is contained in U. The first summand equals $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} \varepsilon_1 w_{ij} g_i w'_{ij} + \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} (w_{ij} \varepsilon_1 - \varepsilon_1 w_{ij}) g_i w'_{ij}$. Since m is a two-sided syzygy of $\overline{\mathcal{G}}$, we get $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} \in I$, i.e. $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} \varepsilon_1 w_{ij} g_i w'_{ij}$ is an element of the two-sided $K[X^*]$-submodule $\langle \varepsilon_1 f_1, \dots, \varepsilon_1 f_t, x_1 \varepsilon_1 - \varepsilon_1 x_1, \dots, x_n \varepsilon_1 - \varepsilon_1 x_n \rangle$ of U. Altogether, we obtain $m' \in U \cap \widehat{F}_{s+1}$. Thus there exist elements $g \in \widehat{G}$ and $w, w' \in X^*$ such that $\mathrm{LT}_\tau(m') = w \, \mathrm{LT}_\tau(g) w'$. Let $w_1 \varepsilon_i w_2$ be the leading term of m' for some $w_1, w_2 \in X^*$ and some $i \in \{2, \dots, s+1\}$. Then w_1 and w_2 are irreducible with respect to $\xrightarrow{G_I}$ by assumption. This yields $\mathrm{LT}_\tau(m) \equiv \mathrm{LT}_\tau(m') = w\,\mathrm{LT}_\tau(g)w' \equiv \overline{w} \cdot \psi(\mathrm{LT}_\tau(g)) \cdot \overline{w}' \equiv \overline{w} \cdot \mathrm{LT}_\tau(\psi(g)) \cdot \overline{w}'$. Therefore the claim follows from $\psi(g) \in \psi(\widehat{G}) \setminus \{0\}$. □

For the next corollary we let $\psi : F_{2s+2} \longrightarrow \overline{F}_s$ be the homomorphism given by $\sum_{i=1}^{2s+2} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij} \mapsto \sum_{i=s+3}^{2s+2} \sum_{j\in\mathbb{N}} c_{ij} \overline{w}_{ij} \varepsilon_{i-s-2} \overline{w}'_{ij}$.

Corollary 4.7. *Let $\overline{\mathcal{G}} = (\overline{g}_1, \ldots, \overline{g}_s), \overline{\mathcal{H}} = (\overline{h}_1, \ldots, \overline{h}_s) \in R^s$, and let U be the two-sided $K[X^*]$-submodule of F_{2s+2} generated by the set $\{\varepsilon_1 g_1 - \varepsilon_3, \ldots, \varepsilon_1 g_s - \varepsilon_{s+2}, \varepsilon_2 h_1 - \varepsilon_3 - \varepsilon_{s+3}, \ldots, \varepsilon_2 h_s - \varepsilon_{s+2} - \varepsilon_{2s+2}, \varepsilon_1 f_1, \ldots, \varepsilon_1 f_t, \varepsilon_2 f_1, \ldots, \varepsilon_2 f_t, x_1\varepsilon_1 - \varepsilon_1 x_1, \ldots, x_n\varepsilon_1 - \varepsilon_1 x_n, x_1\varepsilon_2 - \varepsilon_2 x_1, \ldots, x_n\varepsilon_2 - \varepsilon_2 x_n\}$. Consider the following sequence of instructions.*

1. *Choose a component elimination ordering $\tilde{\tau}$ for $\{1,2\}$ on $\mathbb{T}(F_{2s+2})$ which is also a component elimination ordering for $\{1,\ldots,s+2\}$ such that τ is the restriction of $\tilde{\tau}$ on $\mathbb{T}(F_s)$.*
2. *Compute a $\tilde{\tau}$-Gröbner basis G of U.*
3. *Compute $\widehat{G} = G \cap \langle \varepsilon_{s+3}, \ldots, \varepsilon_{2s+2} \rangle$. Return $\psi(\widehat{G}) \setminus \{0\}$ and stop.*

This is a procedure which enumerates a Gröbner basis of the intersecton of the two-sided syzygy modules $\mathrm{Syz}(\overline{\mathcal{G}})$ and $\mathrm{Syz}(\overline{\mathcal{H}})$.

Proof. The claim follows in the same way as in the proof of Proposition 3.8 using the idea of Proposition 4.6. □

At the beginning of this section we assumed that $\{f_1, \ldots, f_t\}$ forms a σ-Gröbner basis of the two-sided ideal I. This assumption can be replaced by a weaker condition. It suffices that there exists a finite σ-Gröbner basis of I containing the set $\{f_1, \ldots, f_t\}$, since we have $\mathrm{Syz}(g_1, \ldots, g_s, f_1, \ldots, f_t) \subseteq \mathrm{Syz}(g_1, \ldots, g_s, f_1, \ldots, f_{t+u})$ for all $u \geq 0$.

5. Applications

In this section we want to show that one can apply the above methods to solve the *Conjugator Search Problem* (CSP) in certain finitely presented groups.

Problem 5.1 (CSP). Given a group G and two elements $g, h \in G$ which are known to be conjugated to each other (i.e. such that there exists an element $a \in G$ for which $ag = ha$), find a conjugator (i.e. find such an element a).

To this end, we make the following assumptions.

1. The group G is finitely presented as a monoid by generators and relations. In other words, there exists a finite alphabet $X = \{x_1, \ldots, x_n\}$ and an equivalence relation $\sim_W$ which is the normal closure of finitely many relations $w_1 \sim w'_1, \ldots, w_t \sim w'_t$ such that $G = X^*/\sim_W$.
2. There exists a term ordering σ on X^* such that $w_i >_\sigma w'_i$ for $i = 1, \ldots, t$.
3. The word rewriting system $\xrightarrow{W}$ generated by $w_i \xrightarrow{W} w'_i$ for $i = 1, \ldots, t$ is convergent, i.e. it is terminating and confluent.

Thus we can use $\xrightarrow{W}$ to present the residue class of a word $w \in X^*$ in G uniquely by its normal form $\mathrm{NF}_W(w)$. In particular, we can use $\xrightarrow{W}$ to solve the word problem in G. In the following, we shall frequently identify elements of G with the normal form of words representing them. For elements $w, w' \in X^*$ we denote the product of their images in G by ww'. Their product in X^*, i.e. their concatenation, will be denoted by $w \cdot w'$. Equality of elements in G will be denoted by $=$ while for equality of words in X^* we will use the symbol $\equiv$.

Finally, we let K be an arbitrary field.

Remark 5.2.

(1) The *group ring*

$$K[G] = \left\{ \sum_{i=1}^{k} c_i w_i \mid k \geq 0, c_i \in K \setminus \{0\}, w_i \in G \right\}$$

satisfies $K[G] = K[X^*]/I$ where $K[X^*]$ is the non-commutative polynomial ring and I is the two-sided ideal in $K[X^*]$ generated by $\{w_i - w_i' \mid i = 1, \dots, t\}$.

(2) The elements $\{w_i - w_i' \mid i = 1, \dots, t\}$ form a two-sided σ-Gröbner basis of I. In particular, I is a binomial ideal.

(3) Let $w, w' \in X^*$ be words representing conjugated elements in G. The solutions of CSP correspond uniquely to the two-sided syzygies of $(w, w') \in K[X^*]^2$ of the form $a\varepsilon_1 - \varepsilon_2 a$ where $(\varepsilon_1, \varepsilon_2)$ denotes the canonical basis of the free two-sided $K[G]$-module of rank two and where $a \in G$.

To compute this syzygy module, we can use Proposition 4.6. Hence the remaining task is to find an element f of the form $a\varepsilon_1 - \varepsilon_2 a$ in this module. This task can be solved as follows.

Proposition 5.3 (The Conjugator Search Algorithm).
In the setting described above, let $w, w' \in X^*$ be two words representing conjugated elements of the group G. Consider the following sequence of instructions.

(1) *Let F_6 be the free two-sided module of rank 6 over $K[X^*]$. In F_6 form the two-sided submodule $U = \langle \varepsilon_1 w - \varepsilon_3, \varepsilon_1 w' - \varepsilon_4, \varepsilon_2 - \varepsilon_3 - \varepsilon_5, \varepsilon_2 + \varepsilon_4 + \varepsilon_6, \varepsilon_1(w_1 - w_1'), \dots, \varepsilon_1(w_t - w_t'), \varepsilon_2(w_1 - w_1'), \dots, \varepsilon_2(w_t - w_t'), x_1\varepsilon_1 - \varepsilon_1 x_1, \dots, x_n\varepsilon_1 - \varepsilon_1 x_n, x_1\varepsilon_2 - \varepsilon_2 x_1, \dots, x_n\varepsilon_2 - \varepsilon_2 x_n \rangle$.*

(2) *Choose the following module term ordering τ on F_5: for $t_1, t_1', t_2, t_2' \in X^*$, let*

$$t_1 e_i t_1' >_\tau t_2 e_j t_2' \iff \begin{array}{l} i < j \text{ or} \\ (i = j \text{ and } t_1' >_\sigma t_2') \text{ or} \\ (i = j \text{ and } t_1' = t_2' \text{ and } t_1 >_\sigma t_2). \end{array}$$

Compute an interreduced two-sided τ-Gröbner basis $\mathfrak{A}$ von U.

(3) *In $\mathfrak{A}$, there exist elements whose leading term is of the form $t_i\varepsilon_5$ where $t_i \in X^*$ is the normal form with respect to $\xrightarrow{W}$. Return the words t_i and stop.*

This is an algorithm which solves the conjugator search problem in G.

Proof. It is clear that the module term ordering τ defined in step (2) is an elimination ordering for both $L = \{1, 2\}$ and $L' = \{1, 2, 3, 4\}$. Hence Corollary 4.7 shows that the elements of $\mathfrak{A} \cap \langle \varepsilon_5, \varepsilon_6 \rangle$ form a Gröbner basis of the intersection of $\mathrm{Syz}_{K[G]}(w, w')$ and $\mathrm{Syz}_{K[G]}(1, -1)$.

By assumption, there exists a word $a \in X^*$ representing a conjugator such that $aw = w'a$. Hence $a\varepsilon_5 - \varepsilon_6 a$ represents a syzygy in $\mathrm{Syz}_{K[G]}(w, w')$ and is contained in U. In particular, there exists an element $u \in \mathfrak{A}$ whose leading term is of the form $\mathrm{LT}_\tau(u) = t\varepsilon_5$ with $t \in X^*$. Since the elements $(w_i - w_i')\varepsilon_5$ are all contained in U, we may assume that the word t is in normal form with respect to $\xrightarrow{W}$.

Now observe that the proof of Proposition 3.8 (and then of Corollary 4.7) shows that one can consider the computation of $\mathrm{Syz}_{K[G]}(w, w') \cap \mathrm{Syz}_{K[G]}(1, -1)$ as the composition of the computation of the two individual syzygy moduls using Theorem 3.7 with the computation of the intersection of two submodules using Proposition 3.4. For all three Gröbner basis computations, we start with a system of generators consisting of binomials. Hence also the computed Gröbner bases consists of binomials. Consequently, the element $u \in \mathfrak{A}$ found above is of the form $u = t\varepsilon_5 + b\varepsilon_5 c$ or $u = t\varepsilon_5 + b'\varepsilon_6 c'$. In the first case, the definition of τ yields $c = 1$ and $t >_\sigma b$. This contradicts the fact that we assumed t to be in normal form with respect to $\xrightarrow{W}$. Therefore only $u = t\varepsilon_5 + b'\varepsilon_6 c'$ is possible. Here $u \in \mathrm{Syz}_{K[G]}(1, -1)$ yields $t = b'c'$. Hence the element $a = (b')^{-1}t$ satisfies $a\varepsilon_5 - \varepsilon_6 a = (b')^{-1}u \in \mathrm{Syz}_{K[G]}(w, w')$. Thus the word $a \in X^*$ represents the desired conjugator.

Let us recall that the computation of the Gröbner basis necessary in step (2) is an enumerating procedure. After a new Gröbner basis element has been found and fully interreduced, we can check whether it has the shape required by step (3). Since we assume that w and w' are conjugates, a suitable element u will be discovered eventually, i.e. our instructions can be performed in such a manner that they define an algorithm. □

References

[1] I. Anshel, M. Anshel, D. Goldfeld, *An algebraic method for public key cryptography*, Meth. Res. Lett. **6** (1999), 287-291.

[2] H. Bluhm, *Syzygienberechnung über nicht-kommutativen Polynomringen* (in German), diploma thesis, Fachbereich Mathematik, Universität Dortmund, 2005.

[3] M. Caboara, C. Traverso, *Efficient algorithms for ideal operations*, in: V. Weispfenning, B. Trager, *International conference on symbolic and algebraic computation*, Rostock 1998, ACM Press, New York, 1998, 147-152.

[4] D. Farkas, C. Feustel, E.L. Green, *Synergy in the theories of Gröbner bases and path algebras*, Can. J. Math. **45** (1993), 727-739.

[5] C. Feustel, E.L. Green, E. Kirkman, J. Kuzmanovich, *Constructing projective resolutions*, Commun. Algebra **21** (1993), 1869-1887.

[6] M. Garcia Roman, S. Garcia Roman, *Gröbner bases and syzygies on bimodules*, J. Symb. Comput. **40** (2005), 1039-1052.

[7] E.L. Green, *Non-commutative Gröbner bases and projective resolutions*, in: G. Dräxler, G.O. Michler, C.M. Ringel (eds.), *Computational methods for representations of groups and algebras*, Progress in Math. **173**, Birkhäuser, Basel, 1999, 29-60.

[8] E.L. Green, *Noncommutative Gröbner bases and projective resolutions*, J. Symb. Comput. **29** (2000), 601-623.

[9] D. Hofbauer, C. Kögl, K. Madlener, F. Otto, *XSSR: an experimental system for string rewriting - decision problems, algorithms, and implementation*, in: A.M. Cohen, X-S. Gao, N. Takayama (eds.), *Mathematical Software*, Proc. Conf. Beijing 2002, World Scientific, Singapore, 2002, 126-135.

[10] M. Kreuzer, L. Robbiano, *Computational commutative algebra 1*, Springer, Heidelberg, 2000.

[11] M. Kreuzer, L. Robbiano, *Computational commutative algebra 2*, Springer, Heidelberg, 2005.

[12] V. Levandovsky, *Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation*, doctoral thesis, Fachbereich Mathematik, Technische Universität Kaiserslautern, 2005.

[13] K. Madlener, B. Reinert, *Computing Gröbner bases in monoid and group rings*, in: M. Bronstein (ed.), Proc. ISSAC 1993, ACM Press, New York, 1993, 254-263.

[14] K. Madlener, B. Reinert, *Relating rewriting techniques on monoids and rings: congruences on monoids and ideals in monoid rings*, Theor. Comp. Sci. **208** (1998), 3-31.

[15] K. Madlener, B. Reinert, *String rewriting and Gröbner bases – a general approach to monoid and group rings*, in: M. Bronstein, J. Grabmeier, V. Weispfenning, *Workshop on symbolic rewriting techniques*, Monte Verita 1995, Birkhäuser, Basel, 1998, 127-180.

[16] T. Mora, *Seven variations on standard bases*, Technical Report No. 54, Dipartimento die Matematica, Università di Genova, 1988.

[17] T. Mora, *Gröbner basis for non-commutative polynomial rings*, Proc. Conf. AAECC-3, Lecture Notes in Comp. Sci. **229** (1986), 353-362.

[18] T. Mora, *An introduction to commutative and non-commutative Gröbner bases*, Theor. Comp. Sci. **134** (1994), 131-173.

Fachbereich Mathematik, Universität Dortmund, D-44221 Dortmund, Germany
E-mail address: `Holger.Bluhm@uni-dortmund.de`

Fachbereich Mathematik, Universität Dortmund, D-44221 Dortmund, Germany
E-mail address: `Martin.Kreuzer@uni-dortmund.de`