UNIVERSITÄT
PASSAU

Fakultät für Informatik und Mathematik

Dissertation

Non-Commutative Gröbner Bases and Applications

Xingqiang Xiu

Eingereicht an der Fakultät für Informatik und Mathematik
der Universität Passau als Dissertation zur Erlangung des
Grades eines Doktors der Naturwissenschaften

Submitted to the Department of Informatics and Mathematics
of the Universität Passau in Partial Fulfilment of the Requirements
for the Degree of a Doctor in the Domain of Science

Betreuer / Advisor:
Prof. Dr. Martin Kreuzer
Universität Passau

May 2012

Non-Commutative Gröbner Bases and Applications

Xingqiang Xiu

Erstgutachter:	**Prof. Dr. Martin Kreuzer**
Zweitgutachter:	**Prof. Dr. Gerhard Rosenberger**
Mündliche Prüfer:	**Prof. Dr. Franz Brandenburg**
	Prof. Dr. Tobias Kaiser

Der Fakultät für Informatik und Mathematik
der Universität Passau
vorgelegt im Mai 2012

Dedicated to my parents and grandma

Contents

Chapter 1

Introduction

In this thesis we devote ourselves to the study of non-commutative Gröbner bases in free monoid rings over fields and in free bimodules over free monoid rings, and develop applications based on Gröbner bases in these settings. In the past few decades, Gröbner bases have had great success in computational commutative algebra and its applications. Moreover, Gröbner bases and the Buchberger procedure for Gröbner basis computations have been extended successfully to various non-commutative algebras, and then found their ways into applications in those non-commutative settings. The computation of Gröbner bases is a crucial point, both in theory and in practice. Consequently, one of the essential aims of this thesis is to develop efficient (enumerating) procedures for Gröbner basis computations.

Motivation

In 1965, B. Buchberger introduced Gröbner basis theory for ideals in commutative polynomial rings over fields (see [11]). He constructed special bases, named *Gröbner bases*, of ideals. A Gröbner basis G of an ideal is a set of polynomials such that every polynomial in the polynomial ring has a unique remainder when it is divided by the polynomials in G. In particular, the remainder of each polynomial in the ideal generated by G is zero. Buchberger developed a terminating procedure, called *Buchberger's Algorithm*, to transform a finite generating set of an ideal into a finite Gröbner basis of the same ideal. In a natural way, Gröbner bases enable us to solve the membership problem for ideals, that is, to decide whether a given polynomial lies in a given ideal. Gröbner bases also solve many other algebraic problems related to ideals in a computational fashion (see [14, 16, 18]).

Since it is outstandingly important for polynomial rings, Gröbner basis theory has been generalized to several algebraic structures. For instance, in their books [43, 44], M. Kreuzer and L. Robbiano describe a more general version of Gröbner basis theory for free modules over commutative polynomial rings, and provide numerous characterizations and applications of Gröbner bases.

A concept of Gröbner bases for non-commutative polynomial rings (free monoid rings) over fields was first proposed by F. Mora [53], who formulated Buchberger's Algorithm to compute Gröbner bases of ideals in non-commutative polynomial rings. The most important difference is that, non-commutative polynomial rings are no longer Noetherian if they are generated by more then one indeterminate. Hence the procedure for Gröbner basis computations may not terminate. Further, T. Mora [55] unified Gröbner basis theory for both commutative and non-commutative algebras.

Originally, Gröbner basis theory was established by a rewriting approach, which uses polynomials as rewriting rules (see [11]). K. Madlener et al. adopted this method and defined the theory of the prefix Gröbner bases in monoid and group rings (see [52, 57, 58, 63]).

Aided by the development of computer algebra systems, Buchberger's Algorithm for computing Gröbner bases in commutative algebras has been improved and refined over several decades (see [4, 12, 13, 17, 28, 33, 34]). Today there is an implementation of Buchberger's Algorithm in virtually every computer algebra system, including CoCoA [20], GAP [31], Magma [51], SINGULAR [65], et cetera. However, there are only a few computer algebra systems providing a user with the possibility of performing computations in the non-commutative case. Besides ApCoCoA [2], we refer to [67], Section 5 for an exhaustive list of such systems.

In this thesis we start by following the approach of [43] to characterize Gröbner bases in free monoid rings over fields using the notions given by Mora [53, 55] (see Chapter 3). In full detail, we formulate an enumerating procedure, namely the *Buchberger Procedure*, for Gröbner basis computations and present several Improved Buchberger Procedures (see Chapter 4). Then, using the same approach, we investigate Gröbner basis theory in free bimodules over free monoid rings (see Chapter 5). Finally, in the last chapter (Chapter 6) we list a rich collection of useful applications of Gröbner bases. We want to mention that throughout the thesis we are adopting the notation and terminology of the books [43] and [44].

We have implemented all algorithms and procedures in this thesis in the package *gbmr* (the abbreviation for *Gröbner bases in monoid rings*) of the computer algebra system ApCoCoA. All examples provided in this thesis have been computed with this package *gbmr*. We refer to the ApCoCoA wiki page for more information on ApCoCoA and the package *gbmr*. Moreover, we refer to the *Symbolic Data Project* [68] for more examples of the applications of Gröbner bases contributed by us.

Outline

This section presents an outline of the remainder of this thesis and our contributions to the topic at hand. Since every chapter starts with an explanation of its organization, we omit such descriptions here.

Chapter 2 briefly introduces several basic algebraic categories. We need a number of definitions and notions from monoids and groups (see Section 2.1), rings (see Section 2.2) and modules (see Section 2.3). These are the basic algebraic objects in this thesis. Some important properties of these algebraic categories are reviewed. Moreover, the word problem, the membership problem and the conjugacy problem are defined.

Chapter 3 introduces Gröbner bases of ideals in free monoid rings and characterizes Gröbner bases of ideals in detail. Gröbner bases of ideals are defined with respect to a given admissible ordering σ as follows: given a two-sided ideal I, a subset $G \subseteq I$ of non-zero polynomials is a σ-Gröbner basis of I if the leading term set $\mathrm{LT}_\sigma\{G\} = \{\mathrm{LT}_\sigma(g) \mid g \in G\}$ generates the leading term set $\mathrm{LT}_\sigma\{I\} = \{\mathrm{LT}_\sigma(f) \mid f \in I\}$ as a monoid ideal. Following the approach of M. Kreuzer and L. Robbiano in [43], we characterize Gröbner bases via leading term sets and leading term ideals, Gröbner representations, and syzygy modules in great detail. In addition, Gröbner bases of one-sided ideals are defined and characterized in the last section of Chapter 3.

Chapter 4 focuses on techniques for Gröbner basis computations in free monoid rings. We check whether a set G of non-zero polynomials is a Gröbner basis via the set of obstructions of G: the set G is a Gröbner basis of the (two-sided) ideal it generates if the normal remainders with respect to G of all S-polynomials of obstructions are zero. Based on the idea of T. Mora [53, 55], we formulate a Buchberger Procedure to enumerate Gröbner bases. However, in general there exist infinitely many obstructions for a given finite set of non-zero polynomials. This fact makes Buchberger's Procedure infeasible in practice. We get rid of a large number of trivial obstructions and formulate an improved version of the Buchberger Procedure which enumerates Gröbner bases for finitely generated ideals. Later, by investigating the set of non-trivial obstructions carefully, we propose further improvements of the Buchberger Procedure by detecting unnecessary obstructions and by deleting redundant generators, respectively. In order to detect as many unnecessary obstructions as possible, we present an Interreduction Algorithm on non-trivial obstructions and propose generalizations of the *Gebauer-Müller Installation* (see [33]) in free monoid rings. The effectiveness and efficiency of our improvements are shown in examples. Moreover, given a homogenous system of generators, we tune the Buchberger Procedure carefully and propose a homogeneous version of the Buchberger Procedure to enumerate Gröbner bases degree by degree. Since every finitely generated one-sided ideal has a finite Gröbner basis, two algorithms are given for computing Gröbner bases of finitely generated one-sided ideals in the last section of Chapter 4.

Chapter 5 generalizes the notions of Gröbner basis theory from the previous two chapters to free bimodules over free monoid rings. This chapter is inspired by the suggestions of H. Bluhm and M. Kreuzer [8, 9]. Firstly, we define Gröbner bases (see Definition 5.2.1) of (two-sided) submodules with respect to a given module term ordering (see Definition 5.1.1) in the same style as Gröbner bases of ideals in free monoid rings. Then we explore the characterizations of Gröbner bases of submodules and formulate a Buchberger Procedure for enumerating Gröbner bases in free bimodules. By generalizing our methods in Chapter 4, we improve the Buchberger Procedure by detecting unnecessary obstructions and by deleting redundant generators. We show the effectiveness and efficiency of our improvements in examples. Finally, we generalize J.-C. Faugère's F4 Algorithm (see [26]) to the non-commutative case and formulate an F4 Procedure for enumerating Gröbner bases in our setting.

Chapter 6 collects many interesting applications of Gröbner bases. Even though some applications assume that there exist finite Gröbner bases, these applications are quite useful. In Section 6.1, we develop the theory of Gröbner bases in residue class rings and in free bimodule over residue class rings. Note that residue class rings contain monoid and group rings as special cases. Hence the theory developed in this section is compatible with prefix Gröbner basis theory introduced by K. Madlener et al (see [52, 57, 58, 63]). In Section 6.2, we list applications related to elimination orderings. These applications include ideal (resp. module) operations, exploring K-algebra homomorphisms, checking if an element of a residue class ring is algebraic and computing its minimal polynomial if the answer is positive, checking if a monoid element has finite order, formulating enumerating procedures to possibly solve the subalgebra membership problem and the generalized word problem, syzygy computations, and solving the decomposition search problem and the factorization problem. In Section 6.3, we exploit the K-dimension of K-algebra $K\langle X\rangle/I$ with the aid of the Ufnarovski graph

[69]. Under the assumption that the ideal I has a finite Gröbner basis, we formulate the Hilbert series of the K-algebra $K\langle X\rangle/I$ at the end of the section.

Acknowledgements

I am deeply grateful to my advisor Prof. Dr. Martin Kreuzer for supporting me continuously with advice, remarks and suggestions through the whole working period on this thesis. Many interesting topics of the thesis would not have evolved without his influence, wide scope of interests and critiques. I owe very much to Prof. Dr. Gerhard Rosenberger for fruitful discussions concerning group representation theory, for hints and suggestions that contributed greatly to many applications in this thesis.

I am thankful to Prof. Dr. Niels Schwartz for giving me a chance for completing my Ph.D. at Fakultät für Informatik und Mathematik of the Universität Passau. I would like to thank Prof. Dr. Franz Brandenburg and Prof. Dr. Tobias Kaiser for extending my knowledge about efficient algorithms and commutative algebra.

I am indebted to all my colleagues who have shared their expertise with me. In particular, I would like to thank Stefan Kasper, Stefan Schuster, Ehsan Ullah, Bilge Sipal and Anja for their advice and fruitful discussions during the development of the ApCoCoA package *gbmr* and for proof reading this thesis.

I wish to express my appreciation to my family for their love, encouragement and patience. It is hard to imagine how could this thesis be finished without them.

I would like to thank CSC (China Scholarship Council) and FORWISS Passau (Institut für Softwaresysteme in technischen Anwendungen der Informatik) for providing partial financial support for my research. Moreover, I am especially grateful to Prof. Dr. Haiyang Huang and Prof. Dr. Qing He (Beijing, China) for recommending me to study abroad and for encouraging me in all my pursuits.

Chapter 2

Preliminaries

The main tasks of this thesis are to introduce Gröbner basis theories in free monoid rings as well as in free modules over free monoid rings and to explore applications of Gröbner bases. Hence in this chapter we shall introduce several basic algebraic categories: monoids and groups (see Section 2.1), rings (see Section 2.2) and modules (see Section 2.3) which are the most fundamental objects in the thesis.

We shall review each algebraic category by following the same approach. Each algebraic category is defined as a set of elements together with operations that are closed on the set (see Definitions 2.1.1, 2.2.1 and 2.3.1). Then we define substructures of each algebraic category and their systems of generators (see Definitions 2.1.6, 2.2.6 and 2.3.4) and introduce maps (homomorphisms) that preserve algebraic structures (see Definitions 2.1.7, 2.2.7 and 2.3.6). Moreover, in Section 2.1 we introduce monoid presentations (see Definition 2.1.15) and monoid ideals (see Definition 2.1.23). Monomial ideals and monomial modules are studied in Sections 2.2 and 2.3, respectively. Finally, graded rings (see Definition 2.2.15) and graded modules (see Definition 2.3.14) are introduced in Sections 2.2 and 2.3, respectively. We refer to [40, 46] as standard textbooks for intensive study of algebraic categories, refer to [38, 66] for further information on finitely presented groups, and refer to [43], Section 1.7 and [48] for information on gradings.

2.1 Monoids and Groups

Definition 2.1.1. A **monoid** is a non-empty set $\mathcal{M}$ together with a binary operation $\cdot : \mathcal{M} \times \mathcal{M} \to \mathcal{M}$ (called **multiplication**) such that there exists an identity element, i.e. an element $1_{\mathcal{M}} \in \mathcal{M}$ satisfying $1_{\mathcal{M}} \cdot a = a \cdot 1_{\mathcal{M}} = a$ for all $a \in \mathcal{M}$, and such that the associative law is satisfied, i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathcal{M}$.

It can be shown that the identity element $1_{\mathcal{M}}$ is unique. When it is clear which monoid is considered, we simply write 1 instead of $1_{\mathcal{M}}$. We will write ab instead of $a \cdot b$ if no confusion is likely to arise. The product $\underbrace{a \cdot a \cdots a}_{\text{n times}}$ with $n \in \mathbb{N}$ is called the **n-th power** of a and denoted by a^n, where $a^0 = 1$.

Let $\mathcal{M}$ be a monoid. An element $a \in \mathcal{M}$ is called a **unit** if there exists an element $b \in \mathcal{M}$ such that $ab = ba = 1$. The element b is called the **inverse** of a and denoted by a^{-1}. Furthermore, $\mathcal{M}$ is called a **group** if every element of $\mathcal{M}$ is a unit. $\mathcal{M}$ is called **commutative** (or **abelian**) if $ab = ba$ for all $a, b \in \mathcal{M}$. Otherwise it is called **non-commutative** (or **non-abelian**). The **order** of $\mathcal{M}$ is the cardinal number $|\mathcal{M}|$. We say $\mathcal{M}$ is **finite** (resp. **infinite**) if $|\mathcal{M}|$ is finite (resp. infinite). The **order** of $a \in \mathcal{M}$, denoted by $|a|$, is the cardinal number of the set $\{a^n \mid n \in \mathbb{N}\}$. Now let $\mathcal{G}$ be a group. It is easy to verify that $a^{-n} = (a^{-1})^n$ for all $a \in \mathcal{G}$ and $n \in \mathbb{Z}$. The order of a is equal to the smallest $n \in \mathbb{N}$ such that $a^n = 1$. We say $\mathcal{G}$ is **torsion-free** if every non-identity element of $\mathcal{G}$ has infinite order.

Example 2.1.2. The set $\mathbb{N}$ of natural numbers with addition is a commutative monoid with the identity element 0. Only 0 is a unit. The set $\mathbb{N}$ with multiplication is a commutative monoid with the identity element 1. Only 1 is a unit.

Example 2.1.3. The set $\mathbb{Z}$ of integers with addition is a commutative group with the identity element 0. The inverse of n is $-n$. The set $\mathbb{Z}$ with multiplication is a commutative monoid with the identity element 1. Only 1 and -1 are units.

The most important monoid and group for our needs are as follows.

Definition 2.1.4. Let X be a set. A **word** over X is an element of the form $w = x_1 \cdots x_s$ with $s \in \mathbb{N}$ and $x_1, \ldots, x_s \in X$. We denote the **empty word**, i.e. the word with $s = 0$, by 1 and denote the **set of all words** over X by $\langle X \rangle$. Let $w' = x'_1 \cdots x'_t \in \langle X \rangle$ be another word. The multiplication of w and w' is defined by $ww' = x_1 \cdots x_s x'_1 \cdots x'_t$ which is the concatenation of w and w'. With this multiplication the set $\langle X \rangle$ becomes a monoid with the identity element 1 and is called the **free monoid** generated by X.

For a word $w = x_1 \cdots x_s \in \langle X \rangle$, the number s is called the **length** of w and denoted by $\operatorname{len}(w)$. Every word of the form $w' = x_i x_{i+1} \cdots x_j$ with $1 \leq i \leq j \leq s$ is called a

subword of w. In particular, w' is called a **prefix** of w if $i = 1$; it is called a **suffix** of w if $j = s$. For two words $w, w' \in \langle X \rangle$, we say w and w' are **coprime** is neither w is a subword of w' nor w' is a subword of w.

Definition 2.1.5. Let X be a set. A **reduced word** over X is an element of the form $w = x_1^{\lambda_1} \cdots x_s^{\lambda_s}$ with $s \in \mathbb{N}$ and $x_1, \dots, x_s \in X, \lambda_1, \dots, \lambda_s \in \{1, -1\}$ such that w contains no subword of the form $x_i x_i^{-1}$ or $x_i^{-1} x_i$ where $x_i \in X$. We denote the **set of all reduced words** over X by $F(X)$. Let $w' = y_1^{\delta_1} \cdots y_t^{\delta_t} \in F(X)$ be another word. The multiplication of w and w' is defined as follows. Let $k = \max\{l \mid x_{s-l}^{\lambda_{s-l}} = y_{1+l}^{-\delta_{1+l}}, 0 \le l \le \min\{s, t\}\}$. Then we define

$$ww' = \begin{cases} x_1^{\lambda_1} \cdots x_{s-k}^{\lambda_{s-k}} y_{k+1}^{\delta_{k+1}} \cdots y_t^{\delta_t} & \text{if } 0 \le l < \min\{s, t\}, \\ x_1^{\lambda_1} \cdots x_{s-k}^{\lambda_{s-k}} & \text{if } k = t < s, \\ y_{k+1}^{\delta_{k+1}} \cdots y_t^{\delta_t} & \text{if } k = s < t, \\ 1 & \text{if } k = s = t. \end{cases}$$

With this multiplication the set $F(X)$ becomes a group with the identity element 1 and is called the **free group** generated by X.

The free monoid $\langle X \rangle$ and free group $F(X)$ are free objects on the set X which satisfy the *universal properties* in the corresponding algebraic structures. We refer to [40, 46] for more details. Clearly, neither the free monoid $\langle X \rangle$ nor the free group $F(X)$ is commutative if $|X| \ge 2$. Moreover, the free group $F(X)$ is torsion-free.

Now we consider substructures of monoids and groups that are closed under multiplication.

Definition 2.1.6. Let $\mathcal{M}$ be a monoid.

a) A non-empty subset $N \subseteq \mathcal{M}$ is called a **submonoid** of $\mathcal{M}$ if $1 \in N$ and $ab \in N$ for all $a, b \in N$.

b) Let $Y \subseteq \mathcal{M}$ be a subset. A submonoid $N \subseteq \mathcal{M}$ is said to be **generated** by Y if N is the smallest submonoid in $\mathcal{M}$ containing Y. In this case we have $N = \{y_1^{n_1} \cdots y_s^{n_s} \mid y_1, \dots, y_s \in Y, n_1, \dots, n_s \in \mathbb{N}\}$ and write $N = \langle Y \rangle$.

Now let $\mathcal{G}$ be a group instead.

c) A non-empty subset $H \subseteq \mathcal{G}$ is called a **subgoup** of $\mathcal{G}$ if $ab^{-1} \in H$ for all $a, b \in H$.

d) Let $Y \subseteq \mathcal{G}$ be a subset. A subgroup $H \subseteq \mathcal{G}$ is said to be **generated** by Y if H is the smallest subgroup in $\mathcal{G}$ containing Y. In this case we have $H = \{y_1^{n_1} \cdots y_s^{n_s} \mid y_1, \ldots, y_s \in Y, n_1, \ldots, n_s \in \mathbb{Z}\}$ and write $H = \langle Y \rangle$.

By definition, every monoid has two trivial submonoids: the monoid itself and $\{1\}$. The same is true for every group. In Definitions 2.1.6.b and 2.1.6.d the set Y is called a **system of generators** of N and H, respectively. A monoid or a group is said to be **finitely generated** if it has a finite system of generators. A monoid or a group is said to be **cyclic** if it has a system of generators consisting of only one element.

We introduce the functions that preserve the structures of monoids and groups in the following sense.

Definition 2.1.7. Let $\mathcal{M}$ and $\mathcal{N}$ be two monoids (or groups). A map $\varphi : \mathcal{M} \to \mathcal{N}$ is called a **homomorphism** from $\mathcal{M}$ to $\mathcal{N}$ if $\varphi(1_{\mathcal{M}}) = 1_{\mathcal{N}}$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in \mathcal{M}$.

It is easy to check that in case $\mathcal{M}$ and $\mathcal{N}$ are groups we have $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in \mathcal{M}$. A homomorphism is called a **monomorphism** if it is injective, an **epimorphism** if it is surjective, and an **isomorphism** if it is a bijection. If $\varphi : \mathcal{M} \to \mathcal{N}$ is an isomorphism, then $\mathcal{M}$ and $\mathcal{N}$ are said to be isomorphic and denoted by $\mathcal{M} \cong \mathcal{N}$. A homomorphism $\mathcal{M} \to \mathcal{M}$ is called an **endomorphism** of $\mathcal{M}$. An isorphism $\mathcal{M} \to \mathcal{M}$ is called an **automorphism** of $\mathcal{M}$.

Definition 2.1.8. Let $\varphi : \mathcal{M} \to \mathcal{N}$ be a monoid (or group) homomorphism. The **kernel** of φ is the set $\{a \in \mathcal{M} \mid \varphi(a) = 1_{\mathcal{N}}\}$ and is denoted by $\ker(\varphi)$. The **image** of φ is the set $\{\varphi(a) \mid a \in \mathcal{M}\}$ and is denoted by $\mathrm{im}(\varphi)$.

If $\mathcal{M}$, $\mathcal{N}$ are monoids (resp. groups) and $\varphi : \mathcal{M} \to \mathcal{N}$ is a monoid (resp. group) homomorphism, then $\ker(\varphi) \subseteq \mathcal{M}$ and $\mathrm{im}(\varphi) \subseteq \mathcal{N}$ are submonoids (resp. subgroups).

Let $\mathcal{G}$ be a group, and let $H \subseteq \mathcal{G}$ be a subgroup. For $a \in \mathcal{G}$ we define the **left coset** $aH = \{ah \mid h \in H\}$ and the **right coset** $Ha = \{ha \mid h \in H\}$. Observe that $aH = bH$ (resp. $Ha = Hb$) if and only if $a^{-1}b \in H$ (resp. $ba^{-1} \in H$) for $a, b \in \mathcal{G}$. In this case we say a is **left congruent** (resp. **right congruent**) to b modulo H. Clearly left (resp. right) congruence modulo H is an *equivalence relation* on G. It can be shown that the set of all left cosets of H in $\mathcal{G}$ is isomorphic to the set of all right cosets of H in $\mathcal{G}$. Their cardinality is called the **index** of H in $\mathcal{G}$ and is denoted by $|\mathcal{G} : H|$.

Definition 2.1.9. Let $\mathcal{G}$ be a group. A subgroup N of $\mathcal{G}$ is called a **normal subgroup**

in $\mathcal{G}$ if $aN = Na$ for all $a \in \mathcal{G}$. In this case we write $N \trianglelefteq \mathcal{G}$.

Theorem 2.1.10. *Let $\mathcal{G}$ be a group, let $N \trianglelefteq \mathcal{G}$ be a normal subgroup, and let $\mathcal{G}/N$ be the set of all cosets of N in $\mathcal{G}$. Furthermore, for two cosets $aN, bN \in \mathcal{G}/N$ we define the multiplication by $aN \cdot bN = abN$. With this multiplication the set $\mathcal{G}/N$ is a group with the identity element N.*

Proof. See [40], Theorem 5.4 of Chapter I. □

The group $\mathcal{G}/N$ constructed as in the theorem is called the **quotient group** (or **factor group**) of $\mathcal{G}$ modulo N. It is easy to verify that for a group homomorphism $\varphi : \mathcal{G} \to \mathcal{H}$ we have $\ker(\varphi) \trianglelefteq \mathcal{G}$. Conversely, for a normal subgroup $N \trianglelefteq \mathcal{G}$ the map $\pi : \mathcal{G} \mapsto \mathcal{G}/N$ given by $a \mapsto aN$ is an epimorphism with kernel N. The map π is called the **canonical epimorphism**. The following homomorphism theorem induces a series of important isomorphism theorems of groups (see [40], Section 5 of Chapter I).

Theorem 2.1.11. *Let $\varphi : \mathcal{G} \to \mathcal{H}$ be a group homomorphism, and let $N \trianglelefteq \mathcal{G}$ be a normal subgroup contained in* $\ker(\varphi)$. *Then there is a unique homomorphism $\bar{\varphi} : \mathcal{G}/N \to \mathcal{H}$ such that $\bar{\varphi}(aN) = \varphi(a)$ for all $a \in \mathcal{G}$,* $\mathrm{im}(\bar{\varphi}) = \mathrm{im}(\varphi)$ *and* $\ker(\bar{\varphi}) = \ker(\varphi)/N$. *The map $\bar{\varphi}$ is an isomorphism if and only if φ is an epimorphism and $N = \ker(\varphi)$.*

Proof. See [40], Theorem 5.6 of Chapter I. □

We define a general form of congruence relation on monoids and groups as follows.

Definition 2.1.12. Let $\mathcal{M}$ be a monoid. A **congruence relation** $\mathcal{R}$ on $\mathcal{M}$ is an equivalence relation $\sim$ on $\mathcal{M}$ such that $a \sim b$ implies $ca \sim cb$ and $ac \sim bc$ for all $a, b, c \in \mathcal{M}$. For all $a \in \mathcal{M}$ we define the equivalence class $\bar{a} = \{a' \in \mathcal{M} \mid a' \sim a\}$. Let $\mathcal{M}/\mathcal{R}$ be the set of all equivalence classes in $\mathcal{M}$. Furthermore, for two equivalence classes $\bar{a}, \bar{b} \in \mathcal{M}/\mathcal{R}$ we define the multiplication by $\bar{a}\bar{b} = \overline{ab}$. With this multiplication the set $\mathcal{M}/\mathcal{R}$ becomes a monoid with identity element $\bar{1}_{\mathcal{M}}$. The monoid $\mathcal{M}/\mathcal{R}$ is called the **quotient monoid** of $\mathcal{M}$ modulo $\mathcal{R}$.

Obviously if $\mathcal{M}$ is a group then the quotient monoid $\mathcal{M}/\mathcal{R}$ is also a group. It is easy to see that if $N \trianglelefteq \mathcal{G}$ is a normal subgroup then the congruence modulo N satisfies the condition in Definion 2.1.12 and hence is a congruence relation on $\mathcal{G}$. We are more interested in congruence relations generated by subsets $R \subseteq \mathcal{M} \times \mathcal{M}$.

Definition 2.1.13. Let $\mathcal{M}$ be a monoid (or group), and let R be a subset of $\mathcal{M} \times \mathcal{M}$. If $\mathcal{R}$ is the smallest congruence relation on $\mathcal{M}$ containing R, then $\mathcal{R}$ is called the **congruence relation** generated by R.

The congruence relation $\mathcal{R}$ generated by $R \subseteq \mathcal{M} \times \mathcal{M}$ has the following property.

Proposition 2.1.14. *Let $\mathcal{M}$ be a monoid, let R be a subset of $\mathcal{M} \times \mathcal{M}$, and let $\mathcal{R}$ be the congruence relation generated by R. Moreover, let $\mathcal{N}$ be another monoid, and let $\varphi : \mathcal{M} \to \mathcal{N}$ be a monoid homomorphism such that $\varphi(a) = \varphi(b)$ for all $(a, b) \in R$. Then there exists a unique homomorphism $\psi : \mathcal{M}/\mathcal{R} \to \mathcal{N}$ such that $\varphi = \psi\pi$ where π is the canonical epimorphism $\pi : \mathcal{M} \to \mathcal{M}/\mathcal{R}$ defined by $a \mapsto \bar{a}$.*

Proof. See [66], Proposition 4.3 of Chapter 1. □

We are now at the point of defining monoid presentations, which is a crucial subject of rewriting systems and group presentation theory. We refer to [38, 66] as standard textbooks for more details.

Definition 2.1.15. Let X be a set, and let R be a subset of $\langle X \rangle \times \langle X \rangle$. We define the monoid $\mathcal{M}$ to be the quotient monoid of $\langle X \rangle$ modulo the congruence relation generated by R. The pair (X, R) is called a **monoid presentation** for $\mathcal{M}$ and denoted by $\mathcal{M} = \langle X \mid R \rangle$. The presentation is **finite** if both X and R are finite. A monoid is said to be **finitely presented** if it has a finite presentation.

For a finitely presented monoid $\mathcal{M} = \langle X \mid R \rangle$ with $X = \{x_1, \ldots, x_n\}$ and $R = \{(w_1, w_1'), \ldots, (w_s, w_s')\}$ we will usually write $\mathcal{M} = \langle x_1, \ldots, x_n \mid w_1 = w_1', \ldots, w_s = w_s' \rangle$. Here are some examples of monoid presentations. A rich collection of finitely presented monoids and groups are freely available at *Symbolic Data* [68].

Example 2.1.16. Let X be a set. We have $\langle X \rangle = \langle X \mid \emptyset \rangle$. Moreover, let $X^{-1} = \{x^{-1} \mid x \in X\}$, and let $R = \{xx^{-1} = x^{-1}x = 1 \mid x \in X\}$. Then we have $F(X) = \langle X \cup X^{-1} \mid R \rangle$. If the set X is finite, then $\langle X \rangle$ and $F(X)$ are finitely presented.

Example 2.1.17. Let $X = \{x_1, \ldots, x_n\}$, and let $R = \{x_j x_i = x_i x_j \mid 1 \leq i < j \leq n\}$. Then the monoid $\langle X \mid R \rangle$ is isomorphic to $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_1, \ldots, \alpha_n \in \mathbb{N}\}$.

Example 2.1.18. Here are some finitely presented groups.

a) Let $n \geq 1$. Then $\langle x \mid x^n = 1 \rangle$ is a *cyclic group*.

b) Let $n \geq 3$. Then $\langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$ is the *dihedral group* of order $2n$.

c) Let $G = \langle x, y \mid x^p = y^q = W^r(x, y) = 1\rangle$ with $p, q, r \geq 2, W(x, y) = x^{\alpha_1} y^{\beta_1} \cdots x^{\alpha_k} y^{\beta_k}$ such that $k \geq 1$ and $1 \leq \alpha_i < p, 1 \leq \beta_i < q$ for all $i \in \{1, \ldots, k\}$. Then G is a *generalized triangle group* (see [29, 64]).

d) Let $X = \{x_1, \ldots, x_n\}$, let $X^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$, let $R = \{x_i x_i^{-1} = x_i^{-1} x_i = 1 \mid i = 1, \ldots, n\}$, and let $S = \{x_i x_{(i+m) \bmod n} = x_{(i+k) \bmod n} \mid i = 1, \ldots, n\}$ with $m, k \in \{1, \ldots, n\}$ such that $m \neq k$. Then $\langle X \cup X^{-1} \mid R \cup S\rangle$ is a *(Cavicchioli-Hegenbarth-Repovš) generalized Fibonacci group* (see [15, 75]).

Remark 2.1.19. We make some remarks on monoid presentations.

a) Many algebraic problems for monoids and groups are related to finite presentations, for instance the word, conjugacy, and isomorphism problems for finitely present groups (see [22]). Below, we list some undecidable problems that will be investigated in later chapters. Note that, given a finite presentation $\mathcal{M} = \langle X \mid R\rangle$, it is generally undecidable whether or not $\mathcal{M}$ is a group (see [59]). In this thesis, given a group presentation, we shall always assume that it is indeed a group.

b) Given a finite presentation $\mathcal{M} = \langle X \mid R\rangle$, the *Knuth-Bendix Procedure* (see [41]) generates a complete rewriting system from R which is indeed a congruence relation generated by R. The Knuth-Bendix Procedure makes the undecidable word problem into a semi-decidable problem. Some useful heuristics for implementing the Knuth-Bendix Procedure are discussed in [66]. In next section we convert the word problem to the membership problem (see Remark 2.2.12.b) and use Buchberger's Procedure (see Theorem 4.1.14) to make the word problem semi-decidable. Actually the Knuth-Bendix Procedure and Buchberger's Procedure are very similar (see [74]) and we can even consider Buchberger's Procedure as a generalization of the Knuth-Bendix Procedure.

Definition 2.1.20. (The Word Problem) Let X be a finite set, and let $\mathcal{M} = \langle X \mid R\rangle$ a finitely presented monoid. Given two words $w, u \in \langle X\rangle$, decide whether or not w and u define the same element in $\mathcal{M}$.

Definition 2.1.21. (The Membership Problem) Let X be a finite set, let $\mathcal{G} = \langle X \mid R\rangle$ be a finitely presented monoid, and let $H = \langle U\rangle \subseteq \mathcal{G}$ be the submonoid generated by the set $U = \{w_1, \ldots, w_s\} \subset \langle X\rangle$. Given a word $w \in \langle X\rangle$, decide whether or not w is in H.

The membership problem is also called the *generalized word problem.*

Definition 2.1.22. **(The Conjugacy Problem)** Let X be a finite set, and let $\mathcal{G} = \langle X \mid R \rangle$ be a finitely presented group. Given two words $w, u \in \langle X \rangle$, decide whether or not there is a word $a \in \langle X \rangle$ such that aw and ua define the same element in $\mathcal{G}$.

To end this section we introduce another substructure of monoids as follows.

Definition 2.1.23. Let $\mathcal{M}$ be a monoid.

a) A non-empty subset $I \subseteq \mathcal{M}$ is called a (two-sided) **monoid ideal** of $\mathcal{M}$ if we have $\mathcal{M} \cdot I \cdot \mathcal{M} \subseteq I$.

b) A subset $B \subseteq \mathcal{M}$ is called a **system of generators** of monoid ideal $I \subseteq \mathcal{M}$ if I is the smallest monoid ideal in $\mathcal{M}$ containing B. In this case we have $I = \{a\beta b \mid \beta \in B, a, b \in \mathcal{M}\}$.

c) A system of generators B of a monoid ideal I is called **irredundant** if B does not properly contain any other system of generators of I. It is called **minimal** if the number of elements in B is minimal among all systems of generators of I.

By definition, $\mathcal{M}$ is a monoid ideal of itself and it has a system of generators $\{1\}$. In general, it is undecidable if a system of generators of a monoid ideal is irredundant. A monoid ideal may have many irredundent systems of generators. However, in the free monoid $\langle X \rangle$, every monoid ideal has a unique irredundent system of generators, which coincides with minimal system of generators.

Proposition 2.1.24. *Let I be a monoid ideal of $\langle X \rangle$, and let B be the set of all elements of I which do not contain elements of I as a proper subwords. Then B is the unique minimal system of generators of I.*

Proof. First we prove that B generates I. Let w be an element of I, and let w' be a subword of w with minimal length such that w' is still in I. By the definition of B we have $w' \in B$. Thus B is a system of generators of I. Then we prove that B is minimal. Suppose that there exists $B' \subset B$ such that B' generates I. Let $w \in B \setminus B'$. Then there exist $\beta' \in B', a, b \in \langle X \rangle$ such that $w = a\beta' b$. By the definition of B we must have $w = \beta'$ which is a contradiction. Therefore B is minimal. Finally, we prove the uniqueness. Suppose that there are two minimal systems of generators B and B' of I. By symmetry we may assume that there exists an element $\beta' \in B' \setminus B$. With the same process as before, we obtain the same contradiction that $\beta' \in B$. □

Remark 2.1.25. We make some remarks on Proposition 2.1.24.

a) The proposition shows that if there is a finite system of generators of the monoid ideal then we can obtain the minimal system of generators by deleting in this set all elements which contain another elements as proper subwords and removing all repetitions of an element.

b) Note that a monoid ideal of $\langle X \rangle$ need not have finite systems of generators. For instance the monoid ideal $I \subset \langle x, y \rangle$ generated by the set $B = \{xy^i x \mid i \in \mathbb{N}\}$ has a infinite system of generators B which is minimal. Thus *Dickson's lemma* (see [43], Corollary 1.3.6) which plays an important role in computational commutative algebra does not hold in free monoids.

2.2 Rings

Definition 2.2.1. A **ring** is a non-empty set R together with two binary operations $+, \cdot : R \times R \to R$ such that R together with the operation $+$ (called **addition**) is a commutative group with the identity element 0_R, and such that R together with the operation $\cdot$ (called **multiplication**) is a monoid with the identity element 1_R, and such that the distributive laws are satisfied, i.e. $r_3 \cdot (r_1 + r_2) = r_3 \cdot r_1 + r_3 \cdot r_2$ and $(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$ for all $r_1, r_2, r_3 \in R$.

Note that a ring does not necessarily have the multiplicative identity element. *For our purposes in this thesis we shall always assume that a ring contains the identity element under multiplication.* If no ambiguity is likely to arise, we write rr' instead of $r \cdot r'$, 0 instead of 0_R, and 1 instead of 1_R. R is called **commutative** if $rr' = r'r$ for all $r, r' \in R$. An element $r \in R \setminus \{0\}$ is called a **zero divisor** if there exists an element $r' \in R \setminus \{0\}$ such that $rr' = 0$ or $r'r = 0$. More precisely, r is called a **left zero divisor** if $rr' = 0$ and a **right zero divisor** if $r'r = 0$. An **integral domain** R is a commutative ring with no zero divisor and $1_R \neq 0$. A **division ring** R is a ring such that $1_R \neq 0$ and the set $R \setminus \{0\}$ together with multiplication is a group. A commutative division ring is called a **field**.

Example 2.2.2. Let $n \geq 1$. The set $\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\}$ of integers modulo n together with addition and multiplication forms a ring. If p is prime, then non-zero elements of $\mathbb{Z}/(p)$ form a multiplicative group of order $p - 1$ and $\mathbb{Z}/(p)$ is a field. In this case we usually denote it by $\mathbb{F}_p$.

Definition 2.2.3. Let K be a field, and let $\mathcal{M}$ be a monoid. The **monoid ring** of $\mathcal{M}$ over K is the set $K\langle\mathcal{M}\rangle$ of all elements of the form $\sum_{w\in\mathcal{M}} c_w w$ with $c_w \in K$ and $c_w \neq 0$ for only finitely many $w \in \mathcal{M}$, together with the **addition** $+$ defined by $\sum_{w\in\mathcal{M}} c_w w + \sum_{w\in\mathcal{M}} c'_w w = \sum_{w\in\mathcal{M}}(c_w + c'_w)w$ and the **multiplication** $\cdot$ defined by $\sum_{u\in\mathcal{M}} c_u u \cdot \sum_{v\in\mathcal{M}} c_v v = \sum_{w\in\mathcal{M}}(\sum_{uv=w} c_u c_v)w$. The elements in $K\langle\mathcal{M}\rangle$ are called the **polynomials**. If $\mathcal{G}$ is a group, then $K\langle\mathcal{G}\rangle$ is called the **group ring** of $\mathcal{G}$ over K.

Let K be a field, and let X be a set. The monoid ring of $\langle X\rangle$ over K is called the **free monoid ring** (or **non-commutative polynomial ring** or **free associative algebra**) generated by X over K and is denoted by $K\langle X\rangle$.

Definition 2.2.4. Let $K\langle X\rangle$ be the free monoid ring generated by X over K, and let $f = \sum_{w\in\langle X\rangle} c_w w \in K\langle X\rangle$ be a polynomial. The element $c_w \in K$ is called the **coefficient** of w in f. The set $\{w \in \langle X\rangle \mid c_w \neq 0\}$ is called the **support** of f and denoted by $\mathrm{Supp}(f)$. In particular, the free monoid $\langle X\rangle$ contains all **terms** in $K\langle X\rangle$.

It is easy to check that $K\langle X\rangle$ is an integral domain. The following is an example of a monoid ring with zero divisors.

Example 2.2.5. Let K be a field, let $n \geq 3$, and let $D_n = \langle a, b | a^n = b^2 = abab = 1\rangle$ be the dihedral group of order $2n$. Then $K\langle D_n\rangle$ is the group ring of D_n over K. Note that $b+1, b-1 \in K\langle D_n\rangle\setminus\{0\}$ are zero divisors since $(b+1)(b-1) = (b-1)(b+1) = b^2-1 = 0$.

Definition 2.2.6. Let R be a ring.

a) A non-empty subset $S \subseteq R$ is called a **subring** of R if S is closed under the addition and multiplication operations of R and S is itself a ring under these operations.

b) A non-empty subset $I \subseteq R$ is called a **left ideal** (resp. **right ideal**) of R if I is a subring in R and $R \cdot I \subseteq I$ (resp. $I \cdot R \subseteq I$). The set I is called a **two-sided ideal** (or simply an **ideal**) of R if it is both a left and a right ideal.

c) A subset $B \subseteq R$ is called a **system of generators** of left (resp. right, two-sided) ideal $I \subseteq R$ if I is the smallest left (resp. right, two-sided) ideal in R containing B. In this case we have $I = \{\sum_{i=1}^n r_i\beta_i \mid \beta_i \in B, r_i \in R\}$ (resp. $I = \{\sum_{i=1}^n \beta_i r_i \mid \beta_i \in B, r_i \in R\}$, $I = \{\sum_{i=1}^n r_i\beta_i r'_i \mid \beta_i \in B, r_i, r'_i \in R\}$) and write $I =_\lambda \langle B\rangle$ (resp. $I = \langle B\rangle_\varrho, I = \langle B\rangle$).

By definition, every ring has two trivial ideals which are the ring itself and $\{0\}$. An ideal I is said to be **finitely generated** if it has a finite system of generators. It is called **principal** if it has a system of generators consisting of a single element. A system of generators B of I is called **irredundant** if I cannot be generated by any proper subset of B. It is called **minimal** if the number of elements in B is minimal among all systems of generators of I.

Let R be a ring, and let $I \subseteq R$ be an ideal. Since R is commutative additive group, I is a normal subgroup of the additive group R. Consequently, by Theorem 2.1.10 there is a well-defined quotient group R/I where the addition is defined by $(r+I)+(r'+I) = (r+r')+I$ for all $r, r' \in R$. Furthermore, we define the multiplication by $(r+I)(r'+I) = rr'+I$ for all $r, r' \in R$. Then the quotient group R/I is a ring called the **residue class ring** (or **quotient ring**) of R modulo I. The elements of R/I are called **residue classes**. In particular, if R is commutative then so is R/I.

We define the functions that preserve the structures of rings as follows.

Definition 2.2.7. Let R and S be two rings. A map $\varphi : R \to S$ is called a **homomorphism** of rings from R to S if $\varphi(1_R) = 1_S$ and $\varphi(r + r') = \varphi(r) + \varphi(r'), \varphi(rr') = \varphi(r)\varphi(r')$ for all $r, r' \in R$.

A homomorphism of rings is a **monomorphism** (resp. **epimorphism**, **isomorphism**) if it is an injective (resp. surjective, bijective) map. A monomorphism of rings $R \to S$ is also called an **embedding** of R to S. A homorphism $R \to R$ is called an **endomorphism** of R. An isomorphism $R \to R$ is called an **automorphism** of R.

Example 2.2.8. Let $\varphi : \mathcal{M} \to \mathcal{N}$ be a homomorphism of monoids, and let K be a field. Define a map on the monoid rings $\bar{\varphi} : K\langle\mathcal{M}\rangle \to K\langle\mathcal{N}\rangle$ by $\bar{\varphi}(\sum_{w\in\mathcal{M}} c_w w) = \sum_{w\in\mathcal{M}} c_w \varphi(w)$. Then $\bar{\varphi}$ is a ring homomorphism induced by φ.

Definition 2.2.9. Let $\varphi : R \to S$ be a ring homomorphism. The **kernel** of φ is the set $\{r \in R \mid \varphi(r) = 0_S\}$ and is denoted by $\ker(\varphi)$. The **image** of φ is the set $\{\varphi(r) \mid r \in R\}$ and is denoted by $\mathrm{im}(\varphi)$.

It is easy to check that for a ring homomorphism $\varphi : R \to S$ the kernel $\ker(\varphi)$ is an ideal in R. Conversely, if I is an ideal in R then the map $\pi : R \to R/I$ given by $r \mapsto r + I$ is an epimorphism with kernel I. The map π is called the **canonical epimorphism**. We have the following homomorphism theorem for rings which plays an analogous role to Theorem 2.1.11 for groups (see [40], Section 2 of Chapter III).

Theorem 2.2.10. *Let $\varphi : R \to S$ be a ring homomorphism, and let $I \subseteq R$ be an ideal contained in $\ker(\varphi)$. Then there is a unique homomorphism $\bar{\varphi} : R/I \to S$ such that $\bar{\varphi}(r + I) = \varphi(r)$ for all $r \in R$, $\operatorname{im}(\bar{\varphi}) = \operatorname{im}(\varphi)$ and $\ker(\bar{\varphi}) = \ker(\varphi)/I$. The map $\bar{\varphi}$ is an isomorphism if and only if φ is an epimorphism and $I = \ker(\varphi)$.*

Proof. See [40], Theorem 2.9 of Chapter III. □

An immediate and useful application of Theorem 2.2.10 is the following corollary, which connects a monoid presentation with a ring.

Corollary 2.2.11. *Let X be a set, and let $\mathcal{M} = \langle X \mid R \rangle$ be a monoid presentation. Moreover, let K be a field, and let $I \subseteq K\langle X \rangle$ be the ideal generated by the set $\{w - w' \mid (w, w') \in R\} \subseteq K\langle X \rangle$. Then we have $K\langle \mathcal{M} \rangle \cong K\langle X \rangle / I$.*

Proof. Let $\mathcal{R}$ be the congruence relation generated by R. By Definition 2.1.15, it suffices to prove $K\langle \langle X \rangle / \mathcal{R} \rangle \cong K\langle X \rangle / I$. Let $\varphi : \langle X \rangle \to \langle X \rangle / \mathcal{R}$ be the canonical epimorphism of monoids defined by $\varphi(w) = \bar{w}$, and let $\bar{\varphi} : K\langle X \rangle \to K\langle \langle X \rangle / \mathcal{R} \rangle$ be the canonical epimorphism of rings induced by φ, i.e. $\bar{\varphi}(\sum_{w \in \langle X \rangle} c_w w) = \sum_{w \in \langle X \rangle} c_w \bar{w}$ for all $\sum_{w \in \langle X \rangle} c_w w \in K\langle X \rangle$. Obviously we have $\ker(\bar{\varphi}) \subseteq I$. By the definition of I we have $I \subseteq \ker(\bar{\varphi})$. Thus we have $I = \ker(\bar{\varphi})$. The claim follows from Theorem 2.2.10. □

Remark 2.2.12. Let us make some observations about Corollary 2.2.11.

a) Let K be a field, and let $\mathcal{M} = \langle X \mid R \rangle$ be a monoid presentation. Corollary 2.2.11 reveals that the monoid ring $K\langle \mathcal{M} \rangle$ is nothing but the quotient ring $K\langle X \rangle / I$ where $I \subseteq K\langle X \rangle$ is the ideal generated by the set $\{w - w' \mid (w, w') \in R\}$. Thus the computations for the monoid ring $K\langle \mathcal{M} \rangle$ can be done for the free monoid ring $K\langle X \rangle$ through the embedding $K\langle \mathcal{M} \rangle \to K\langle X \rangle$. For this reason in this thesis we can focus on the computations in free monoid rings (see Chapters 3 and 4). In Chapter 6 we will investigate the computations in quotient rings.

b) Using Corollary 2.2.11, we convert the word problem (see Definition 2.1.20) to the membership problem in the free monoid ring as follows. Let X be a finite set, let $\mathcal{M} = \langle X \mid R \rangle$ be a finitely presented monoid, and let $u, v \in \langle X \rangle$ be two words. Moreover, let K be a field, and let $I \subseteq K\langle X \rangle$ be the ideal generated by the set $\{w - w' \mid (w, w') \in R\}$. Then u and v define the same element in $\mathcal{M}$ if and only if $u - v \in I$.

Now we shall investigate further into free monoid rings which is a major object for our computations later on. In the rest of this section, we let K be a field, let X be a set, and let $K\langle X\rangle$ be the free monoid ring generated by X over K. The simplest ideals in $K\langle X\rangle$ are **monomial ideals** which are generated by sets of words. Monomial ideals have the following nice property.

Proposition 2.2.13. *Let $S \subseteq \langle X\rangle$ be a set of words which generates an ideal $I = \langle S\rangle \subseteq K\langle X\rangle$. Then I has a unique irredundant system of generators consisting entirely of words. In particular, for every word $w \in I$ there exists a word $w' \in S$ such that w is a multiple of w'.*

Proof. The first claim follows from Definition 2.2.6.c and Proposition 2.1.24. We write $w = \sum_{i=1}^{s} p_i w_i p_i'$ with $w_i \in S, p_i, p_i' \in K\langle X\rangle$ for all $i = 1, \ldots, s$. Then there must exist an index $i \in \{1, \ldots, s\}$ such that $w \in \mathrm{Supp}(p_i w_i p_i')$. Therefore the second claim holds. □

Note that a ring R is said to be **Noetherian** if it satisfies the ascending chain condition on ideals. That is, given any chain $I_1 \subseteq I_2 \subseteq \cdots$ of ideals, there exists a positive integer n such that $I_n = I_{n+1} = \cdots$. Note that the ascending chain condition defines a finiteness property, i.e. if R is a Noetherian ring then every ideal of R is finitely generated.

Remark 2.2.14. Unfortunately, $K\langle X\rangle$ is non-Noetherian if $|X| \geq 2$. The most famous example in the literature is as follows. Consider the free monoid ring $K\langle x, y\rangle$ and the infinite chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ where $I_i = \langle xyx, xy^2x, \ldots, xy^ix\rangle$. Clearly the chain is strictly increasing. Hence $K\langle x, y\rangle$ is non-Noetherian. Consequently, it brings difficulties to Gröbner basis computations in free monoid rings, i.e. we cannot guarantee the termination of Buchberger's Procedures and have to compromise with ourselves on enumerating procedures (see Chapter 4).

To end this section we introduce gradings to free monoid rings. Graded rings are defined as follows.

Definition 2.2.15. Let $(\Gamma, +)$ be a monoid. A ring R is called a **Γ-graded ring** if there exists a family of additive subgroups $\{R_\gamma\}_{\gamma\in\Gamma}$ such that $R = \oplus_{\gamma\in\Gamma} R_\gamma$ and $R_\gamma \cdot R_{\gamma'} \subseteq R_{\gamma+\gamma'}$ for all $\gamma, \gamma' \in \Gamma$.

Let R be a Γ-graded ring. If $r \in R_\gamma$ then we say r is **homogeneous** of degree γ and write $\deg(r) = \gamma$. By Definition 2.2.15 zero is a homogeneous element of every degree. For every $r \in R$ we can uniquely decompose r as $r = \sum_{\gamma\in\Gamma} r_\gamma$ with $r_\gamma \in R_\gamma$.

We call r_γ the **homogeneous component** of degree γ of r.

The following examples define two important gradings of $K\langle X\rangle$ which we will use later.

Example 2.2.16. Let $K\langle X\rangle_w = Kw$ for $w \in \langle X\rangle$. Clearly we have $K\langle X\rangle = \oplus_{w\in\langle X\rangle} Kw$ and $Kw \cdot Kw' = Kww'$ for all $w, w' \in \langle X\rangle$. Thus $K\langle X\rangle$ is a $\langle X\rangle$-graded ring.

Example 2.2.17. Let $K\langle X\rangle_d = \{f \in K\langle X\rangle \mid \operatorname{len}(w) = d \text{ for all } w \in \operatorname{Supp}(f)\}$ for $d \in \mathbb{N}$. Then we make $K\langle X\rangle$ into an $\mathbb{N}$-graded ring. This grading is called the **standard grading** of $K\langle X\rangle$. Let $f \in K\langle X\rangle \setminus \{0\}$ be a polynomial. We write the decomposition of f as $f = \sum_{i=0}^{d} f_i$ where $f_i \in K\langle X\rangle_i$ for $i = 0, \ldots, d$ and $f_d \neq 0$. Then the number d is called the **standard degree** (or simple the **degree**) of f and is denoted by $\deg(f)$. Clearly for $w \in \langle X\rangle$ we have $\deg(w) = \operatorname{len}(w)$. In particular, we have $\deg(x) = 1$ for $x \in X$ and $\deg(c) = 0$ for $c \in K \setminus \{0\}$. Moreover, using the convention for zero polynomial we define $\deg(0) = -\infty$.

Definition 2.2.18. An ideal I of the Γ-graded ring R is said to be **Γ-graded** (or **homogeneous**) if we have $I = \oplus_{\gamma\in\Gamma}(I \cap R_\gamma)$.

The following proposition characterizes graded rings nicely.

Proposition 2.2.19. *Let I be an ideal of Γ-graded ring R. Then the following conditions are equivalent.*

a) I is a Γ-graded ideal.

b) If $r \in I$ and $r = \sum_{\gamma\in\Gamma} r_\gamma$ is the decomposition of r into its homogeneous components, then $r_\gamma \in I$ for all $\gamma \in \Gamma$.

c) There is a system of generators of I which consists entirely of homogeneous elements.

Proof. Analogous to [43], Proposition 1.7.10. □

Corollary 2.2.20. *Let $I \subseteq K\langle X\rangle$ be an $\mathbb{N}$-graded ideal generated by a homogeneous system of generators G. Moreover, let $d \in \mathbb{N}$, let $G_{\leq d}$ be the set of elements in G with degree $\leq d$, and let $\langle I_{\leq d}\rangle$ be the ideal generated by the homogeneous element in I with degree $\leq d$. Then $G_{\leq d}$ generates $\langle I_{\leq d}\rangle$.*

Proof. This follows from Proposition 2.2.19 directly. □

Corollary 2.2.21. *If $I \subseteq R$ be a Γ-graded ideal, then the quotient ring R/I is also Γ-graded.*

Proof. Let $(R/I)_\gamma = R_\gamma/(I \cap R_\gamma)$ for $\gamma \in \Gamma$. Then the claim follows from Proposition 2.2.19.b. □

2.3 Modules

Definition 2.3.1. Let R be a ring. A **left R-module** M is an additive commutative group $(M, +)$ together with an operation $\cdot : R \times M \to M$ (called **scalar multiplication**) such that $1_R{\cdot}m = m$ for all $m \in M$, and such that the associative and distributive laws are satisfied, i.e. $r \cdot (r' \cdot m) = (rr') \cdot m$ and $r \cdot (m + m') = r \cdot m + r' \cdot m'$, $(r + r') \cdot m = r \cdot m + r' \cdot m$ for all $r, r' \in R, m, m' \in M$.

The scalar multiplication is usually written by juxtaposition as rm for $r \in R$ and $m \in M$. A **right R-module** M is defined symmetrically via a scalar multiplication of the form $\cdot : M \times R \to M$. Consequently, all theorems about left R-modules also hold, *mutatis mutandis*, for right R-modules.

If R is a division ring, then left R-module is called a **left R-vector space**. If K be a commutative ring, then a **K-algebra** A is a ring such that A is a left K-module and $k(ab) = (ka)b = a(kb)$ for all $k \in K, a, b \in A$.

Definition 2.3.2. Let R and S be two rings. An **R-S-bimodule** M is an additive commutative group $(M, +)$ such that M is a left R-module and a right S-module, and such that two scalar multiplications are compatible, i.e. $(rm)s = r(ms)$ for all $r \in R, s \in S$ and $m \in M$. An R-R-bimodule is called a **two-sided R-module** (or an **R-bimodule**).

Example 2.3.3. Let R be a ring. If $I \subseteq R$ is a left ideal, then I is a left R-module. If $I \subseteq R$ is an ideal, then I and R/I are R-bimodules. In particular, R is a left R-module and an R-bimodule.

In this section we focus mainly on two-sided modules for our purposes. We refer to [40], Chapter IV for an intensive study of (one-sided) modules.

Definition 2.3.4. Let R be a ring, and let M be an R-bimodule.

a) Let $N \subseteq M$ be an additive subgroup. N is called a (two-sided) **R-submodule** of M if $R \cdot N \cdot R \subseteq N$.

b) A subset $B \subseteq M$ is called a **system of generators** of R-submodule $N \subseteq M$ if N is the smallest R-submodule in M containing B. In this case we have $N = \{\sum_{i=1}^{n} r_i \beta_i r'_i \mid \beta_i \in B, r_i, r'_i \in R\}$ and write $N = \langle B \rangle$.

A module is said to be **finitely generated** if it has a finite system of generators. Clearly the empty set $\emptyset$ generates the zero module $\langle 0 \rangle$. A system of generators B of M is called **irredundant** if M cannot be generated by any proper subset of B. It is called **minimal** if the number of elements in B is minimal among all systems of generators of M.

A subset B of an R-bimodule M is said to be **linearly independent** if for distinct $\beta_1, \ldots, \beta_n \in B$ and distinct pairs $(r_{i1}, r'_{i1}), \ldots, (r_{ik_i}, r'_{ik_i}) \in R \times R$ for $i = 1, \ldots, n$ we have $\sum_{i=1}^{n} \sum_{j=1}^{k_i} r_{ij} \beta_i r'_{ij} = 0$ implies $r_{ij} = 0$ or $r'_{ij} = 0$ for each pair (r_{ij}, r'_{ij}) with $i \in \{1, \ldots, n\}, j \in \{1, \ldots, k_i\}$. A linearly independent subset of R-bimodule M that generates M is called a **basis** of M. In this case M is called a **free R-bimodule**. Observe that the empty set $\emptyset$ is linearly independent and is a basis of the zero module $\langle 0 \rangle$. We construct a non-trivial free bimodule as follows.

Example 2.3.5. Let K be a field, and let R be a K-algebra. Consider R as a *Lie algebra* in the natural way, its *universal enveloping algebra* $\mathcal{U}(R) = R \otimes_K R$ (see [23]) becomes an R-bimodule. Furthermore, let $s \geq 1$. Then the R-bimodule $\oplus_{i=1}^{s} \mathcal{U}(R)$ is a free R-bimodule with the canonical basis $\{e_1, \ldots, e_s\}$, i.e. $e_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$ with $1 \otimes 1$ occurring in the i^{th} position for $i = 1, \ldots, s$.

The functions that preserve the structures of bimodules are defined as follows.

Definition 2.3.6. Let R be a ring, and let M, N be two R-bimodules. An **R-bimodule homomorphism** is a map $\varphi : M \to N$ satisfying $\varphi(m + m') = \varphi(m) + \varphi(m'), \varphi(rm) = r\varphi(m)$ and $\varphi(mr) = \varphi(m)r$ for all $r, r' \in R, m, m' \in M$.

An R-bimodule homomorphism $\varphi : M \to N$ is called a **monomorphism** (resp. **epimorphism**, **isomorphism**) if it is injective (resp. surjective, bijective). The **kernel** of φ is the set $\ker(\varphi) = \{m \in M \mid \varphi(m) = 0\}$ which is an R-submodule of M. The **image** of φ is the set $\operatorname{im}(\varphi) = \{\varphi(m) \mid m \in M\}$ which is an R-submodule of N. Now let K be a commutative commutative ring, and let A, B be two K-algebras. A map $\varphi : A \to B$ is called a **K-algebra homomorphism** if φ is both a ring homomorphism and a K-module homomorphism.

Let N be an R-submodule of R-bimodule M. Then the quotient group M/N is an R-bimodule with scalar multiplications given by $r(m+N) = rm + N, (m+N)r = mr + N$ for all $r \in R, m \in M$. The map $\pi : M \to M/N$ given by $m \to m + N$ is an epimorphism with kernel N and is called the **canonical epimorphism**. The following homomorphism theorem induces isomorphism theorems for R-bimodules (see [40], Section 1 of Chapter IV).

Theorem 2.3.7. *Let $\varphi : M \to N$ be an R-bimodule homomorphism, and let $K \subseteq M$ be an R-submodule contained in* $\ker(\varphi)$. *Then there is a unique R-bimodule homomorphism $\bar{\varphi} : M/K \to N$ such that $\bar{\varphi}(m+K) = f(m)$ for all $m \in M$,* $\operatorname{im}(\bar{\varphi}) = \operatorname{im}(\varphi)$ *and* $\ker(\bar{\varphi}) = \ker(\varphi)/K$. *The map $\bar{\varphi}$ is an isomorphism if and only if φ is an epimorphism and $K = \ker(\varphi)$.*

Proof. See [40], Theorem 1.7 of Chapter IV. □

The following universal property shows that free R-bimodules are free objects in the category of R-modules.

Proposition 2.3.8. *Let F be a free R-bimodule with a basis B, and let $\iota : B \to F$ be an injective map. Given an R-bimodule M and a map $\varphi : B \to M$, there is a unique R-bimodule homomorphism $\bar{\varphi} : F \to M$ such that $\bar{\varphi}\iota = \varphi$.*

Proof. See [40], Theorem 2.1 of Chapter IV. □

It is straightforward to check that the R-bimodule $\oplus_{i=1}^{s}\mathcal{U}(R)$ constructed in Example 2.3.5 is a free object. In the rest of this section we study one specific instance of free bimodules which forms another major object for our computations later on. In the following, we let K be a field, let X be a set, and let $K\langle X\rangle$ be the free monoid ring generated by X over K.

Definition 2.3.9. Let $r \geq 1$. The $K\langle X\rangle$-bimodule $(K\langle X\rangle \otimes_K K\langle X\rangle)^s$, denoted by F_s, is called the **free bimodule** over $K\langle X\rangle$ of **rank** s with the canonical basis $\{e_1, \ldots, e_s\}$, i.e. $e_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$ with $1 \otimes 1$ occurring in the i^{th} position for $i = 1, \ldots, s$ and e_i is called the i^{th} **standard basis vector** in F_s. The set $\{we_iw' \mid i \in \{1, \ldots, s\}, w, w' \in \langle X\rangle\}$ is called the **set of terms** in F_s and denoted by $\mathbb{T}(F_s)$. We write element $m \in F_s$ as $m = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_iw'_{ij}$ with $c_{ij} \in K, w_{ij}, w'_{ij} \in \langle X\rangle$ for all $i \in \{1, \ldots, s\}, j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. The element $c_{ij} \in K$

is called the **coefficient** of the term $w_{ij}e_iw'_{ij}$ in m. The set $\{w_{ij}e_iw'_{ij} \in \mathbb{T}(F_s) \mid c_{ij} \neq 0\}$ is called the **support** of m and denoted by $\mathrm{Supp}(m)$.

Remark 2.3.10. Let $I \subseteq K\langle X\rangle$ be an ideal, and let $\bar{F}_s = (K\langle X\rangle/I \otimes_K K\langle X\rangle/I)^s$ be the free bimodule over the quotient ring $K\langle X\rangle/I$. Using the embeding $K\langle X\rangle/I \to K\langle X\rangle$, we are able to consider each element $\bar{m} \in \bar{F}_s$ as an element in F_s and perform computations for $\bar{F}_s$ on F_s. For this reason in this thesis we can focus on the computations for free bimodules over free monoid rings (see Chapter 5). In Chapter 6 we will investigate the computations for free bimodules over quotient rings. Note that, given a monoid presentation $\mathcal{M} = \langle X \mid R\rangle$, the free $K\langle\mathcal{M}\rangle$-bimodule $(K\langle\mathcal{M}\rangle \otimes_K K\langle\mathcal{M}\rangle)^s$ is nothing but a specific instance of $\bar{F}_s$ by Corollary 2.2.11.

Note that an **Noetherian module** is a module that satisfies the ascending chain condition on submodules, i.e. every ascending chain of submodules becomes eventually stationary. Note that a Noetherian module has a very nice property that all of its submodules are finitely generated. However, F_s is non-Noetherian if $|X| \geq 2$ since $K\langle X\rangle$ is non-Noetherian (see Remark 2.2.14). As a result Gröbner basis computations in F_s might not terminate and we have to content ourselves with enumerating procedures (see Chapter 5).

The simplest $K\langle X\rangle$-submodules in F_s are **monomial modules** which are generated by subsets of $\mathbb{T}(F_s)$. Monomial modules have similar nice property as monomial ideals in $K\langle X\rangle$ (see Proposition 2.2.13). To present this property for monomial modules the following definition and lemma prove useful.

Definition 2.3.11. Let $(\Gamma, \circ)$ be a monoid.

a) A **left Γ-monomodule** is a set Σ together with an operation $* : \Gamma \times \Sigma \to \Sigma$ such that $1_\Gamma * s = s$ and $(\gamma_1 \circ \gamma_2) * s = \gamma_1 * (\gamma_2 * s)$. A **right Γ-monomodule** is defined symmetrically. A **Γ-bimonomodule** is both a left Γ-monomodule and a right Γ-monomodule.

b) Let Σ be a Γ-bimonomodule. A non-empty subset $\Sigma' \subseteq \Sigma$ is called a (two-sided) **Γ-submonomodule** of Σ if we have $\Gamma * \Sigma' * \Gamma \subseteq \Sigma'$.

c) Let Σ be a Γ-bimonomodule. A subset $B \subseteq \Sigma$ is called a **system of generators** of Γ-submonomodule $\Sigma' \subseteq \Sigma$ if Σ' is the smallest Γ-submonomodule in Σ containing B. In this case we have $\Sigma' = \{\gamma_1 * s * \gamma_2 \mid \gamma_1, \gamma_2 \in \Gamma, s \in B\}$. The set B is called **irredundant** if B does not properly contain any other system of generators of Σ'. It is called **minimal** if the number of elements in B is minimal among all systems of generators of Σ'.

Clearly $\mathbb{T}(F_s)$ is a $\langle X\rangle$-bimonomodule. Moreover, we have the following lemma.

Lemma 2.3.12. *Every $\langle X\rangle$-submonomodule of $\mathbb{T}(F_s)$ has a unique minimal system of generators.*

Proof. Analogous to Proposition 2.1.24. □

Proposition 2.3.13. *Every monomial module in F_s has a unique irredundant system of generators consisting entirely of terms in $\mathbb{T}(F_s)$.*

Proof. Analogous to Proposition 2.2.13. □

We end this section with a brief introduction of gradings of bimodules.

Definition 2.3.14. Let $(\Gamma, \circ)$ be a monoid, let R be a Γ-graded ring, and let $(\Sigma, *)$ be a Γ-bimonomodule. An R-bimodule M is called a **Σ-graded R-bimodule** if there exists a family of subgroups $\{M_s\}_{s\in\Sigma}$ such that $M = \oplus_{s\in\Sigma} M_s$ and $R_\gamma \cdot M_s \cdot R_{\gamma'} \subseteq M_{\gamma * s * \gamma'}$ for all $\gamma, \gamma' \in \Gamma$, $s \in \Sigma$.

Let M be a Σ-graded R-bimodule. If $m \in M_s$ then we say m is **homogeneous** of degree s and write $\deg(m) = s$. By Definition 2.3.14 zero is a homogeneous element of every degree. For every $m \in M$ we can uniquely decompose m as $m = \sum_{s\in\Sigma} m_s$ with $m_s \in M_s$. We call m_s the **homogeneous component** of degree s of m. In the following example we define an important grading of F_s for our needs.

Example 2.3.15. Consider $K\langle X\rangle$ as a $K\langle X\rangle$-bimodule. Let $(t_1, \ldots, t_s) \in \langle X\rangle^s$ be a tuple of words. We define a $K\langle X\rangle$-bimodule homomorphism $\psi : F_s \to K\langle X\rangle$ by $e_i \mapsto t_i$ for $i = 1, \ldots, s$. Let $F_s(w) = \{m \in F_s \mid \psi(m) \in Kw\}$ for $w \in \langle X\rangle$. Recall that $K\langle X\rangle$ is $\langle X\rangle$-graded. It is easy to check that $F_s = \oplus_{w\in\langle X\rangle} F_s(w)$ and for all words $w, w_1, w_2 \in \langle X\rangle$ we have $Kw_1 \cdot F_s(w) \cdot Kw_2 \subseteq F_s(w_1 w w_2)$. Thus we make F_s into a $\langle X\rangle$-graded $K\langle X\rangle$-bimodule. This grading is called the **grading** defined by the tuple $(t_1, \ldots, t_s)$.

Definition 2.3.16. An R-submodule of the Σ-graded R-bimodule M is said to be **Σ-graded** (or **homogeneous**) if we have $N = \oplus_{s\in\Sigma}(N \cap M_s)$.

Proposition 2.2.19 for ideals of graded rings is also valid, *mutatis mutandis*, for submodules of graded bimodules.

Proposition 2.3.17. *Let N be an R-submodule of Σ-graded R-bimodule M. Then the following conditions are equivalent.*

a) N is a Σ-graded R-submodule.

b) If $m \in N$ and $m = \sum_{s \in \Sigma} m_s$ is the decomposition of m into its homogeneous components, then $m_s \in N$ for all $s \in \Sigma$.

c) There is a system of generators of N which consists entirely of homogeneous elements.

Proof. Analogous to [43], Proposition 1.7.10. □

Corollary 2.3.18. *If $N \subseteq M$ be a Σ-graded R-submodule, then the quotient group M/N is a Σ-graded R-module.*

Proof. Let $(M/N)_s = M_s/(N \cap M_s)$ for $s \in \Sigma$. Then the claim follows from Proposition 2.3.17.b. □

Chapter 3

Gröbner Bases in $K\langle X\rangle$

In this chapter we shall introduce Gröbner bases of ideals in free monoid rings and study the characterizations of Gröbner bases. In [53], F. Mora proposed a generalization of Gröbner bases and Buchberger's Algorithm to non-commutative polynomial rings, which was mainly built upon the work of G. Bergman [5] and B. Buchberger [13]. Few years later, T. Mora [55] unified Gröbner basis theory for both commutative and non-commutative algebras through a generalization of the Gaußian elimination algorithm. Non-commutative Gröbner basis theory was further considered by E. Green [36, 37], H. Li [48], V. Levandovskyy [47], et al. In this and next chapters we shall present Gröbner basis theory in free monoid rings: in this chapter we shall characterize Gröbner bases of ideals in great detail, and in next chapter we will study techniques for Gröbner basis computations.

Two main ingredients of Gröbner basis theory, namely admissible orderings (see Definition 3.1.1) and the Division Algorithm (see Theorem 3.2.1), are introduced in the first two sections. Section 3.1 we define admissible orderings followed by concrete examples that are implemented in the package *gbmr* of the computer algebra system ApCoCoA [2]. Further we present Macaulay's Basis Theorem (see Theorem 3.1.15) and introduce the normal form (see Definition 3.1.17) as a byproduct of Macaulay's Basis Theorem. In Section 3.2 we discuss the Division Algorithm in detail and present the Interreduction Algorithm (see Theorem 3.2.8) as an application of the Division Algorithm. Section 3.3 begins with a definition of Gröbner bases for two-sided ideals (see Definition 3.3.1). Then we shall characterize Gröbner bases through leading term sets and leading term ideals (see Propositions 3.3.3 and 3.3.4), and Gröbner representations (see Proposition 3.3.6), and study the existence and uniqueness of reduced

Gröbner bases (see Definition 3.3.16 and Proposition 3.3.17). In Section 3.4 we shall explore the characterizations of Gröbner bases through syzygy modules (see Definition 3.4.1 and Proposition 3.4.11). In Section 3.5 we shall have a short investigation of Gröbner bases of one-sided ideals.

Throughout this chapter, we let K be a field, $X = \{x_1, \ldots, x_n\}$ a finite alphabet (or set of indeterminates), and $K\langle X\rangle$ the free monoid ring generated by X over K. We shall also consider the free monoid $\langle X\rangle$ generated by X as the set of terms in $K\langle X\rangle$. By an ideal I we mean a two-sided ideal in $K\langle X\rangle$ unless specified otherwise.

3.1 Admissible Orderings

Note that a relation σ on a set S is a subset of $S \times S$. Henceforth, we shall write $a \geq_\sigma b$ or $b \leq_\sigma a$ instead of $(a, b) \in \sigma$. If $a \geq_\sigma b$ and $a \neq b$, we shall write $a >_\sigma b$ or $b <_\sigma a$.

Definition 3.1.1. An **admissible ordering** σ on $\langle X\rangle$ is a relation on $\langle X\rangle$ satisfying the following conditions for all $w_1, w_2, w_3, w_4 \in \langle X\rangle$.

a) $w_1 \geq_\sigma w_2$ or $w_2 \geq_\sigma w_1$, i.e. σ is complete.

b) $w_1 \geq_\sigma w_1$, i.e. σ is reflexive.

c) $w_1 \geq_\sigma w_2$ and $w_2 \geq_\sigma w_1$ imply $w_1 = w_2$, i.e. σ is antisymmetric.

d) $w_1 \geq_\sigma w_2$ and $w_2 \geq_\sigma w_3$ imply $w_1 \geq_\sigma w_3$, i.e. σ is transitive

e) $w_1 \geq_\sigma w_2$ implies $w_3w_1w_4 \geq_\sigma w_3w_2w_4$, i.e. σ is compatible with multiplication.

f) Every descending chain of words $w_1 \geq_\sigma w_2 \geq_\sigma \cdots$ in $\langle X\rangle$ becomes eventually stationary, i.e. σ is a well-ordering.

If σ is an admissible ordering on $\langle X\rangle$, then we must have $w \geq_\sigma 1$ for all $w \in \langle X\rangle$. Otherwise, we assume that $1 >_\sigma w$ for some word $w \in \langle X\rangle$. By condition 3.1.1.e, for all $i \in \mathbb{N}$, we have $w^i = w^i \cdot 1 >_\sigma w^i \cdot w = w^{i+1}$. Then by condition 3.1.1.d we obtain an infinite strictly descending chain $1 >_\sigma w >_\sigma w^2 >_\sigma \cdots$, which is a contradiction with condition 3.1.1.f.

Before presenting concrete admissible orderings on $\langle X\rangle$ which are available in the ApCoCoA package *gbmr*, we define the following lexicographic ordering.

Definition 3.1.2. The **lexicographic ordering** on $\langle X\rangle$, denoted by $\texttt{Lex}$, is defined as follows. For two words $w_1, w_2 \in \langle X\rangle$, we say $w_1 \geq_{\texttt{Lex}} w_2$ if we have $w_1 = w_2 w$ for some word $w \in \langle X\rangle$, or if we have $w_1 = w x_{i_1} w', w_2 = w x_{i_2} w''$ for some words $w, w', w'' \in \langle X\rangle$ and some letters $x_{i_1}, x_{i_2} \in X$ such that $i_1 < i_2$.

Remark 3.1.3. We add some remarks on the lexicographic ordering.

a) $\texttt{Lex}$ is a complete, reflexive, antisymmetric and transitive relation on $\langle X\rangle$. But it is not an admissible ordering, because $\texttt{Lex}$ does not satisfy condition 3.1.1.e or condition 3.1.1.f. For example, consider the free monoid $\langle x_1, x_2\rangle$. Since we have $x_2^2 >_{\texttt{Lex}} x_2$ and $x_2^2 x_1 = x_2^2 \cdot x_1 <_{\texttt{Lex}} x_2 \cdot x_1 = x_2 x_1$, $\texttt{Lex}$ is not compatible with multiplication. Moreover, since we have an infinite strictly descending chain $x_2 x_1 >_{\texttt{Lex}} x_2^2 x_1 >_{\texttt{Lex}} x_2^3 x_1 >_{\texttt{Lex}} \cdots$, $\texttt{Lex}$ is not a well-ordering.

b) Though it is not an admissible ordering, $\texttt{Lex}$ is still quite helpful because it usually acts as a "tie-breaker" during constructing a series of admissible orderings (see Definitions 3.1.4, 3.1.6, and 3.1.8). In the literature of rewriting theory, $\texttt{Lex}$ as in Definition 3.1.2 is called the *dictionary ordering*, or self-explanatorily, the *left-to-right lexicographic ordering*. The *right-to-left lexicographic ordering* is defined symmetrically (see [66], Section 2.1).

In the following we shall introduce admissible orderings that are implemented in the ApCoCoA package *gbmr*.

Definition 3.1.4. The **length-lexicographic ordering** on $\langle X\rangle$, denoted by $\texttt{LLex}$, is defined as follows. For two words $w_1, w_2 \in \langle X\rangle$, we say $w_1 \geq_{\texttt{LLex}} w_2$ if we have $\operatorname{len}(w_1) > \operatorname{len}(w_2)$, or if we have $\operatorname{len}(w_1) = \operatorname{len}(w_2)$ and $w_1 \geq_{\texttt{Lex}} w_2$.

Example 3.1.5. Consider the free monoid $\langle x_1, x_2\rangle$.

a) We have $x_1 >_{\texttt{LLex}} x_2$, since $\operatorname{len}(x_1) = 1 = \operatorname{len}(x_2)$ and $x_1 >_{\texttt{Lex}} x_2$.

b) We have $x_2^2 >_{\texttt{LLex}} x_2$ and $x_2^2 x_1 >_{\texttt{LLex}} x_2 x_1$, since $\operatorname{len}(x_2^2) = 2 > 1 = \operatorname{len}(x_2)$ and $\operatorname{len}(x_2^2 x_1) = 3 > 2 = \operatorname{len}(x_2 x_1)$, respectively.

c) We have $x_1 x_2^2 >_{\texttt{LLex}} x_2^2 x_1$, since $\operatorname{len}(x_1 x_2^2) = 3 = \operatorname{len}(x_2^2 x_1)$ and $x_1 x_2^2 >_{\texttt{Lex}} x_2^2 x_1$.

Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n_{\geq 0}$ (called a **weight tuple**) be a tuple of non-negative real numbers. Given a word $w = x_{i_1} \cdots x_{i_s} \in \langle X\rangle$, the number $\sum_{k=1}^{s} \alpha_{i_k}$ is called the **weight** of w defined by α and is denoted by $\mathrm{W}_\alpha(w)$. Then $\texttt{LLex}$ becomes a specific instance of the following weight-lexicographic ordering by letting $\alpha = (1, \ldots, 1)$.

Definition 3.1.6. The **weight-lexicographic ordering** defined by α on $\langle X\rangle$, denoted by `WLex`, is defined as follows. For two words $w_1, w_2 \in \langle X\rangle$, we say $w_1 \geq_{\texttt{WLex}} w_2$ if we have $\mathrm{W}_\alpha(w_1) > \mathrm{W}_\alpha(w_2)$, or if we have $\mathrm{W}_\alpha(w_1) = \mathrm{W}_\alpha(w_2)$ and $w_1 \geq_{\texttt{Lex}} w_2$.

Definition 3.1.7. The **length-reverse-lexicographic ordering** on $\langle X\rangle$, denoted by `LRLex`, is defined as follows. For two words $w_1, w_2 \in \langle X\rangle$, we say $w_1 \geq_{\texttt{LRLex}} w_2$ if we have $\mathrm{len}(w_1) > \mathrm{len}(w_2)$, or if we have $\mathrm{len}(w_1) = \mathrm{len}(w_2)$ and $w_1 < w_2$ by right-to-left lexicographic ordering.

Given a word $w \in \langle X\rangle$ and a letter $x_i \in X$, the number of occurrences of x_i in w is called the **degree** of x_i in w and is denoted by $\deg_{x_i}(w)$. For example, consider the free monoid $\langle x_1, x_2, x_3\rangle$. We have $\deg_{x_1}(x_2^2x_1) = 1, \deg_{x_2}(x_2^2x_1) = 2$ and $\deg_{x_3}(x_2^2x_1) = 0$.

Now we are going to introduce an *elimination ordering*, denoted by `Elim`, on $\langle X\rangle$ that eliminates letters in the alphabet X in the following sense. Let $j \in \{1, \ldots, n\}$, and let $L = \{x_1, \ldots, x_j\} \subseteq X$ be a subset. Then $w \in \langle x_{j+1}, \ldots, x_n\rangle$ and $w \geq_{\texttt{Elim}} w'$ imply $w' \in \langle x_{j+1}, \ldots, x_n\rangle$ for all $w, w' \in \langle X\rangle$. In other words, if the letters in L do not occur in a word $w \in \langle X\rangle$, then for every word $w' \in \langle X\rangle$ which is not larger than w with respect to `Elim` the letters in L do not occur in w' either.

Definition 3.1.8. We define an **elimination ordering** `Elim` on $\langle X\rangle$ as follows. For two words $w_1, w_2 \in \langle X\rangle$, we say $w_1 \geq_{\texttt{Elim}} w_2$ if we have $\deg_{x_i}(w_1) > \deg_{x_i}(w_2)$ for some $i \in \{1, \ldots, n\}$ and $\deg_{x_j}(w_1) = \deg_{x_j}(w_2)$ for all $j \in \{1, \ldots, i-1\}$, or if we have $\deg_{x_i}(w_1) = \deg_{x_i}(w_2)$ for all $i \in \{1, \ldots, n\}$ and $w_1 \geq_{\texttt{Lex}} w_2$.

Note that `Elim` is just a member of a large class of elimination orderings, which play a crucial role on many Gröbner bases applications (see Section 6.2).

Example 3.1.9. Consider the free monoid $\langle x_1, x_2\rangle$.

a) We have $x_1 >_{\texttt{Elim}} x_2^2$, since $\deg_{x_1}(x_1) = 1 > 0 = \deg_{x_1}(x_2^2)$.

b) We have $x_1x_2^2 <_{\texttt{Elim}} x_2^3x_1$, since $\deg_{x_1}(x_1x_2^2) = 1 = \deg_{x_1}(x_2^3x_1)$ and $\deg_{x_2}(x_1x_2^2) = 2 < 3 = \deg_{x_2}(x_2^3x_1)$.

c) We have $x_1x_2^2 >_{\texttt{Elim}} x_2^2x_1$, since $\deg_{x_1}(x_1x_2^2) = 1 = \deg_{x_1}(x_2^2x_1)$ and $\deg_{x_2}(x_1x_2^2) = 2 = \deg_{x_2}(x_2^2x_1)$ and $x_1x_2^2 >_{\texttt{Lex}} x_2^2x_1$.

Definition 3.1.10. An admissible ordering σ on $\langle X\rangle$ is called **length compatible** if $\mathrm{len}(w_1) > \mathrm{len}(w_2)$ implies $w_1 >_\sigma w_2$ for all $w_1, w_2 \in \langle X\rangle$.

For instance, `LLex` and `LRLex` are length compatible admissible orderings while `Elim` is not.

Assumption 3.1.11. *From now on, we let σ be an admissible ordering on $\langle X\rangle$.*

Definition 3.1.12. Every polynomial $f \in K\langle X\rangle \setminus \{0\}$ can be uniquely represented as

$$f = c_1 w_1 + \cdots + c_s w_s$$

with $c_1, \ldots, c_s \in K \setminus \{0\}, w_1, \ldots, w_s \in \langle X\rangle$ such that $w_1 >_\sigma w_2 >_\sigma \cdots >_\sigma w_s$. The word $\mathrm{LT}_\sigma(f) = w_1 \in \langle X\rangle$ is called the **leading term** of f with respect to σ. The element $\mathrm{LC}_\sigma(f) = c_1 \in K \setminus \{0\}$ is called the **leading coefficient** of f with respect to σ. Moreover, we let $\mathrm{LM}_\sigma(f) = \mathrm{LC}_\sigma(f) \cdot \mathrm{LT}_\sigma(f) = c_1 w_1$. The polynomial f is called **monic** if $\mathrm{LC}_\sigma(f) = 1$.

The leading term $\mathrm{LT}_\sigma(0)$ and leading coefficient $\mathrm{LC}_\sigma(0)$ of zero polynomial are undefined. Some elementary properties of leading terms are collected in the following remark.

Remark 3.1.13. Let $f, f_1, f_2 \in K\langle X\rangle \setminus \{0\}$ be polynomials.

a) Suppose that $f_1 + f_2 \neq 0$. We have $\mathrm{LT}_\sigma(f_1 + f_2) \leq_\sigma \max_\sigma\{\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2)\}$. Moreover, $\mathrm{LT}_\sigma(f_1 + f_2) = \max_\sigma\{\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2)\}$ if and only if $\mathrm{LT}_\sigma(f_1) \neq \mathrm{LT}_\sigma(f_2)$ or $\mathrm{LC}_\sigma(f_1) + \mathrm{LC}_\sigma(f_2) \neq 0$.

b) For all $w, w' \in \langle X\rangle$, we have $\mathrm{LT}_\sigma(wfw') = w\mathrm{LT}_\sigma(f)w'$.

c) We have $\mathrm{LT}_\sigma(f_1 f_2) = \mathrm{LT}_\sigma(f_1)\mathrm{LT}_\sigma(f_2)$.

Definition 3.1.14. Let $I \subseteq K\langle X\rangle$ be an ideal.

a) The (monomial) ideal $\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f) \mid f \in I \setminus \{0\}\rangle \subseteq K\langle X\rangle$ is called the **leading term ideal** of I with respect to σ.

b) The set $\mathrm{LT}_\sigma\{I\} = \{\mathrm{LT}_\sigma(f) \mid f \in I \setminus \{0\}\} \subseteq \langle X\rangle$ is called the **leading term set** of I with respect to σ.

c) The set $\mathcal{O}_\sigma(I) = \langle X\rangle \setminus \mathrm{LT}_\sigma\{I\}$ is called the **order ideal** of I with respect to σ.

By definition, we have $\mathrm{LT}_\sigma(\langle 0\rangle) = \langle 0\rangle$ and $\mathrm{LT}_\sigma\{\langle 0\rangle\} = \emptyset$. It is easy to check that $\mathrm{LT}_\sigma\{I\}$ is actually a monoid ideal of $\langle X\rangle$. In the sequel for the sake of simplicity, given a set of polynomials $G \subseteq K\langle X\rangle \setminus \{0\}$, we let $\mathrm{LT}_\sigma\{G\} = \{\mathrm{LT}_\sigma(g) \mid g \in G\} \subseteq \langle X\rangle$ be the leading term set and $\mathrm{LT}_\sigma(G) \subseteq K\langle X\rangle$ the monomial ideal generated by $\mathrm{LT}_\sigma\{G\}$.

In the literature of computational algebra, a non-empty set $\mathcal{O} \subseteq \langle X\rangle$ is called an *order ideal* if $w \in \mathcal{O}$ and $w = w_1w_2$ imply $w_1 \in \mathcal{O}$ and $w_2 \in \mathcal{O}$ for all $w, w_1, w_2 \in \langle X\rangle$ (see [44], Section 6.4). Observe that $\mathcal{O}_\sigma(I)$ satisfies the order ideal condition.

Let $I \subseteq K\langle X\rangle$ be an ideal. Then the residue class ring $K\langle X\rangle/I$ is also a K-vector space. Given an admissible ordering, we can explicitly describe a K-basis of $K\langle X\rangle/I$ as follows.

Theorem 3.1.15. (Macaulay's Basis Theorem) *Let $I \subseteq K\langle X\rangle$ be an ideal. The residue classes of the elements of $\mathcal{O}_\sigma(I)$ form a basis of the K-vector space $K\langle X\rangle/I$.*

Proof. Let $N = \mathrm{Span}_K\{\bar{w} \in K\langle X\rangle/I \mid w \in \mathcal{O}_\sigma(I)\}$. Obviously $N \subseteq K\langle X\rangle/I$. We prove that $N = K\langle X\rangle/I$. For the sake of contradiction, we suppose that $N \subset K\langle X\rangle/I$. Since σ is a well-ordering, there exists a polynomial $f \in K\langle X\rangle \setminus \{0\}$ satisfying $f \notin I$, $\bar{f} \notin N$ and having minimal leading term $\mathrm{LT}_\sigma(f)$ with respect to σ. If $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma\{I\}$, then there exists a polynomial $g \in I$ such that $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(g)$. Thus we obtain a polynomial $f' = f - \frac{\mathrm{LC}_\sigma(f)}{\mathrm{LC}_\sigma(g)}g$ satisfying $f' \notin I, \bar{f}' = \bar{f} \notin N$ and having a smaller leading term than f, in contradiction with our choice of f. Therefore we have $\mathrm{LT}_\sigma(f) \in \mathcal{O}_\sigma(I)$. However, we obtain a polynomial $f'' = f - \mathrm{LC}_\sigma(f)\mathrm{LT}_\sigma(f)$ satisfying $f'' \notin I, \bar{f}'' \notin N$ and having a smaller leading term than f, in contradiction with our choice of f again.

To prove linear independence, suppose that there exists a polynomial $f = \sum_{i=1}^{s} c_iw_i \in I \setminus \{0\}$ with $c_i \in K \setminus \{0\}, w_i \in \mathcal{O}_\sigma(I)$ for all $i \in \{1, \ldots, s\}$. Without loss of generality, we may assume that $w_1 >_\sigma w_2 >_\sigma \cdots >_\sigma w_s$. Then we have $\mathrm{LT}_\sigma(f) = w_1 \in \mathrm{LT}_\sigma\{I\} \cap \mathcal{O}_\sigma(I) = \emptyset$ which contradicts our assumption. □

For a constructive proof of the theorem, refer to [55], Theorem 1.1 and see also the proof of Theorem 5.1.9.

Corollary 3.1.16. *Let $I \subseteq K\langle X\rangle$ be an ideal.*

a) We have $K\langle X\rangle = I \oplus \mathrm{Span}_K\mathcal{O}_\sigma(I)$.

b) For every polynomial $f \in K\langle X\rangle$, there exists a unique polynomial $\hat{f} \in \mathrm{Span}_K\mathcal{O}_\sigma(I)$ such that $f - \hat{f} \in I$.

Proof. Claim a) is only another formulation of Theorem 3.1.15. For the proof of claim b), it suffices, by Theorem 3.1.15, to prove the uniqueness. Suppose that there exist two polynomials $\hat{f}_1, \hat{f}_2 \in \mathrm{Span}_K\mathcal{O}_\sigma(I)$ satisfying $f - \hat{f}_1, f - \hat{f}_2 \in I$. Then we have $(f - \hat{f}_1) - (f - \hat{f}_2) = \hat{f}_2 - \hat{f}_1 \in I \cap \mathrm{Span}_K \mathcal{O}_\sigma(I)$. By claim a) we have $I \cap \mathrm{Span}_K \mathcal{O}_\sigma(I) = \{0\}$, and hence $\hat{f}_1 = \hat{f}_2$. □

Definition 3.1.17. Let $I \subseteq K\langle X\rangle$ be an ideal. Given a polynomial $f \in K\langle X\rangle$, the unique polynomial $\hat{f} \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$ as in Corollary 3.1.16.b is called the **normal form** of f modulo I with respect to σ and is denoted by $\mathrm{NF}_{\sigma,I}(f)$.

A polynomial $f \in K\langle X\rangle$ is said to be a **normal polynomial** (or **in normal form**) modulo I with respect to σ if $f = \mathrm{NF}_{\sigma,I}(f)$. Similarly a word $w \in \langle X\rangle$ is said to be a **normal word** (or **in normal form**) modulo I with respect to σ if $w = \mathrm{NF}_{\sigma,I}(w)$. Note that a polynomial $f \in K\langle X\rangle$ is a normal polynomial if and only if $f \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$, and a word $w \in \langle X\rangle$ is a normal word if and only if $w \in \mathcal{O}_\sigma(I)$. Let's collect some rules for computing with normal forms.

Remark 3.1.18. Let $I \subseteq K\langle X\rangle$ be an ideal.

a) For $f \in K\langle X\rangle$, we have $\mathrm{NF}_{\sigma,I}(\mathrm{NF}_{\sigma,I}(f)) = \mathrm{NF}_{\sigma,I}(f)$.

b) For $f_1, f_2 \in K\langle X\rangle$, we have $\mathrm{NF}_{\sigma,I}(f_1 - f_2) = \mathrm{NF}_{\sigma,I}(f_1) - \mathrm{NF}_{\sigma,I}(f_2)$.

c) For $f_1, f_2 \in K\langle X\rangle$, we have $\mathrm{NF}_{\sigma,I}(f_1) = \mathrm{NF}_{\sigma,I}(f_2)$ if and only if $f_1 - f_2 \in I$. In particular, a polynomial $f \in K\langle X\rangle$ satisfies $f \in I$ if and only if $\mathrm{NF}_{\sigma,I}(f) = 0$.

d) For $f_1, f_2 \in K\langle X\rangle$, we have $\mathrm{NF}_{\sigma,I}(f_1 f_2) = \mathrm{NF}_{\sigma,I}(\mathrm{NF}_{\sigma,I}(f_1)\mathrm{NF}_{\sigma,I}(f_2))$.

Remark 3.1.19. The uniqueness property of the normal form reveals an algorithmic approach to possibly solve the word problem (see Definition 2.1.20) as follows. Let $\mathcal{M} = \langle X \mid R\rangle$ be a finitely presented monoid, and let $u, v \in \langle X\rangle$ be two words. Moreover, let $I \subseteq K\langle X\rangle$ be the ideal generated by the set $\{w - w' \mid (w, w') \in R\}$. Then by Remark 2.2.12.b, u and v define the same element in $\mathcal{M}$ if and only if $u - v \in I$. Choose an admissible ordering σ on $\langle X\rangle$. Then by Remark 3.1.18.c, u and v define the same element in $\mathcal{M}$ if and only if $\mathrm{NF}_{\sigma,I}(u - v) = 0$. Hence we convert the word problem into the computation of the normal form.

In this section we have introduced some notions related to some admissible ordering σ and some ideal I, for instance, for a polynomial f we have defined the leading term of f with respect to σ, the normal form of f modulo I with respect to σ, et cetera. If it is clear which admissible ordering and which ideal we are considering, we will simply call them, respectively, the leading term of f, the normal form of f, et cetera.

3.2 The Division Algorithm

Intuitively the normal form can be computed using the *Division Algorithm.* Just as division in commutative polynomial rings (see [43], Section 1.6), the Division Algorithm divides a polynomial $f \in K\langle X\rangle \setminus \{0\}$ by a tuple of polynomials $\mathcal{G} = (g_s, \ldots, g_s) \in (K\langle X\rangle \setminus \{0\})^s$ and gives a representation

$$f = \sum_{i=1}^{s}\sum_{j=1}^{k_i} c_{ij} w_{ij} g_i w'_{ij} + p$$

with $c_{ij} \in K \setminus \{0\}$, $w_{ij}, w'_{ij} \in \langle X\rangle$ for all $i \in \{1, \ldots, s\}, j \in \{1, \ldots, k_i\}$, and $p \in K\langle X\rangle$ such that $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_{ij} g_i w'_{ij})$ for all $i \in \{1, \ldots, s\}, j \in \{1, \ldots, k_i\}$, and such that $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(p)$ if $p \neq 0$, and such that no element of $\mathrm{Supp}(p)$ is contained in $\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle$. These properties of the representation make the Division Algorithm a powerful tool and an essential ingredient of Gröbner basis theory. We now present the Division Algorithm in free monoid rings more precisely.

Theorem 3.2.1. (The Division Algorithm) *Let $s \geq 1$, and let $f, g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$. Consider the following sequence of instructions.*

1) *Let $k_1 = \cdots = k_s = 0, p = 0$, and $v = f$.*

2) *Find the smallest $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(v) = w\mathrm{LT}_\sigma(g_i)w'$ for some $w, w' \in \langle X\rangle$. If such an i exists, increase k_i by 1, set $c_{ik_i} = \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_i)}, w_{ik_i} = w, w'_{ik_i} = w'$, and replace v by $v - c_{ik_i} w_{ik_i} g_i w'_{ik_i}$.*

3) *Repeat step 2) until there is no more $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(v)$ is a multiple of $\mathrm{LT}_\sigma(g_i)$. If now $v \neq 0$, then replace p by $p + \mathrm{LM}_\sigma(v)$ and v by $v - \mathrm{LM}_\sigma(v)$, continue with step 2).*

4) *Return the tuples $(c_{11}, w_{11}, w'_{11}), \ldots, (c_{sk_s}, w_{sk_s}, w'_{sk_s})$ and the polynomial $p \in K\langle X\rangle$.*

This is an algorithm which returns the tuples $(c_{11}, w_{11}, w'_{11}), \ldots, (c_{sk_s}, w_{sk_s}, w'_{sk_s})$ and the polynomial $p \in K\langle X\rangle$ such that

$$f = \sum_{i=1}^{s}\sum_{j=1}^{k_i} c_{ij} w_{ij} g_i w'_{ij} + p$$

and such that the following conditions are satisfied.

a) *No element of $\mathrm{Supp}(p)$ is contained in $\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle$.*

b) For all $i \in \{1, \ldots, s\}$ and all $j \in \{1, \ldots, k_i\}$, we have $\mathrm{LT}_\sigma(w_{ij} g_i w'_{ij}) \leq_\sigma \mathrm{LT}_\sigma(f)$. If $p \neq 0$, we have $\mathrm{LT}_\sigma(p) \leq_\sigma \mathrm{LT}_\sigma(f)$.

c) For all $i \in \{1, \ldots, s\}$ and all $j \in \{1, \ldots, k_i\}$, we have $\mathrm{LT}_\sigma(w_{ij} g_i w'_{ij}) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{i-1}) \rangle$.

Proof. Analogous to [43], Theorem 1.6.4. □

In contrast to the Division Algorithm in commutative polynomial rings, the following example shows that the resulting tuples $(c_{11}, w_{11}, w'_{11}), \ldots, (c_{sk_s}, w_{sk_s}, w'_{sk_s})$ and polynomial $p \in K\langle X \rangle$ satisfying conditions 3.2.1.a, 3.2.1.b, and 3.2.1.c are not uniquely determined by the admissible term ordering σ and the tuple $(f, g_1, \ldots, g_s) \in (K\langle X \rangle \setminus \{0\})^{s+1}$ (compare with [43], Theorem 1.6.4). This phenomenon is due to the fact that in step 2) of Theorem 3.2.1 there might exist more than one pairs (w, w') satisfying $\mathrm{LT}_\sigma(v) = w\mathrm{LT}_\sigma(g_i)w'$.

Example 3.2.2. Consider the free monoid ring $\mathbb{Q}\langle x, y, z \rangle$ equipped with the admissible ordering $\sigma =$ `LLex` such that $x >_\sigma > y >_\sigma z$. Divide $f = zx^2yx$ by the tuple (g_1, g_2) where $g_1 = xy + x$ and $g_2 = x^2 + xz$. We have $\mathrm{LT}_\sigma(g_1) = xy$ and $\mathrm{LT}_\sigma(g_2) = x^2$. The Division Algorithm gives

1) $k_1 = k_2 = 0, p = 0$, and $v = f = zx^2yx$.

2) Since $\mathrm{LT}_\sigma(v) = zx^2yx = zx\mathrm{LT}_\sigma(g_1)x$, we set $k_1 = 1, c_{11} = \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_1)} = 1, w_{11} = zx, w'_{11} = x$, and $v = v - c_{11}w_{11}g_1w'_{11} = -zx^3$.

2*) Since $\mathrm{LT}_\sigma(v) = zx^3 = z\mathrm{LT}_\sigma(g_2)x$, we set $k_2 = 1, c_{21} = \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_2)} = -1, w_{21} = z, w'_{21} = x$, and $v = v - c_{21}w_{21}g_2w'_{21} = zxzx$.

3) Since $\mathrm{LT}_\sigma(v) = zxzx$ is not a multiple of $\mathrm{LT}_\sigma(g_1)$ or $\mathrm{LT}_\sigma(g_2)$, we set $p = p + \mathrm{LM}_\sigma(v) = zxzx$ and $v = v - \mathrm{LM}_\sigma(v) = 0$.

4) Since $v = 0$, return the tuples $(c_{11}, w_{11}, w'_{11}), (c_{21}, w_{21}, w'_{21})$ and the polynomial $p = zxzx$.

Therefore we get a representation $f = zxg_1x - zg_2x + zxzx$. Observe that there is another choice for (w_{21}, w'_{21}) in step 2*), i.e. $(w_{21}, w'_{21}) = (zx, 1)$. In this case, the Division Algorithm gives $f = zxg_1x - zxg_2 + zg_2z - zxz^2$.

To get rid of this uncertainty, we shall fix a strategy in step 2) of Theorem 3.2.1 to choose a pair (w, w') from all pairs that satisfy $\mathrm{LT}_\sigma(v) = w\mathrm{LT}_\sigma(g_i)w'$. Note that different strategies will end with different division algorithms. For instance, if the strategy is to choose the pair (w, w') with minimal $\mathrm{len}(w)$, i.e. $\mathrm{LT}_\sigma(g_i)$ is the leftmost subword of $\mathrm{LT}_\sigma(v)$, then we obtain the **Leftmost Division Algorithm**. Symmetrically, by choosing the pair (w, w') with minimal $\mathrm{len}(w')$, i.e. $\mathrm{LT}_\sigma(g_i)$ is the rightmost subword of $\mathrm{LT}_\sigma(v)$, we obtain the **Rightmost Division Algorithm**. If we require that $w = 1$, then we obtain the **Right Division Algorithm** (see Theorem 3.5.1) or the **Prefix-reduction Algorithm** (see [52, 57, 58, 63]). We shall prove that once the strategy is fixed, the resulting tuples $(c_{11}, w_{11}, w'_{11})$, ..., $(c_{sk_s}, w_{sk_s}, w'_{sk_s})$ and polynomial $p \in K\langle X\rangle$ satisfying conditions 3.2.1.a, 3.2.1.b, and 3.2.1.c are uniquely determined by the admissible term ordering σ and the tuple $(f, g_1, \dots, g_s) \in (K\langle X\rangle \setminus \{0\})^{s+1}$. In the ApCoCoA package *gbmr*, we apply the Leftmost Division Algorithm.

Corollary 3.2.3. *In the setting of Theorem 3.2.1, if we fix a strategy to choose the pair (w, w') in step 2), then the resulting tuples $(c_{11}, w_{11}, w'_{11})$, ..., $(c_{sk_s}, w_{sk_s}, w'_{sk_s})$ and polynomial $p \in K\langle X\rangle$ satisfying conditions 3.2.1.a, 3.2.1.b, and 3.2.1.c are uniquely determined by the admissible term ordering σ and the tuple $(f, g_1, \dots, g_s) \in (K\langle X\rangle \setminus \{0\})^{s+1}$.*

Proof. Suppose that there exist another tuples $(d_{11}, u_{11}, u'_{11}), \dots, (d_{sl_s}, u_{sl_s}, u'_{sl_s})$ and a polynomial $p' \in K\langle X\rangle$ satisfying conditions 3.2.1.a, 3.2.1.b, and 3.2.1.c. Then we have

$$\begin{aligned} 0 \;=\; & (\sum_{j=1}^{k_1} c_{1j}w_{1j}g_1w'_{1j} - \sum_{j=1}^{l_1} d_{1j}u_{1j}g_1u'_{1j}) + \cdots + (\sum_{j=1}^{k_s} c_{sj}w_{sj}g_sw'_{sj} - \sum_{j=1}^{l_s} d_{sj}u_{sj}g_su'_{sj}) \\ & +(p - p'). \end{aligned}$$

We first show $\mathrm{LT}_\sigma(w_{ik}g_iw'_{ik}) = \mathrm{LT}_\sigma(u_{il}g_iu'_{il})$ implies $w_{ik} = u_{il}, w'_{ik} = u'_{il}$. By Remark 3.1.13.b, we have $w_{ik}\mathrm{LT}_\sigma(g_i)w'_{ik} = \mathrm{LT}_\sigma(w_{ik}g_iw'_{ik}) = \mathrm{LT}_\sigma(u_{il}g_iu'_{il}) = u_{il}\mathrm{LT}_\sigma(g_i)u'_{il}$. Then we have $w_{ik} = u_{il}, w'_{ik} = u'_{il}$ using the fixed strategy in step 2). Now let's consider the summand

$$G_s = \sum_{j=1}^{k_s} c_{sj}w_{sj}g_sw'_{sj} - \sum_{j=1}^{l_s} d_{sj}u_{sj}g_su'_{sj}.$$

Since $\mathrm{LT}_\sigma(v)$ strictly decreases in Steps 2) and 3) of Theorem 3.2.1, it follows from Remark 3.1.13.b that $\mathrm{LT}_\sigma(w_{s1}g_sw'_{s1}) >_\sigma \mathrm{LT}_\sigma(w_{sj}g_sw'_{sj})$ for all $j \in \{2, \dots, k_s\}$, and that $\mathrm{LT}_\sigma(u_{s1}g_su'_{s1}) >_\sigma \mathrm{LT}_\sigma(u_{sj}g_su'_{sj})$ for all $j \in \{2, \dots, l_s\}$. By condition 3.2.1.c, we have $\mathrm{LT}_\sigma(w_{s1}g_sw'_{s1}) \notin \langle \mathrm{LT}_\sigma(g_1), \dots, \mathrm{LT}_\sigma(g_{s-1})\rangle$ and $\mathrm{LT}_\sigma(w_{u1}g_su'_{s1}) \notin \langle \mathrm{LT}_\sigma(g_1), \dots,$

$\mathrm{LT}_\sigma(g_{s-1})\rangle$. Condition 3.2.1.a implies that $\mathrm{LT}_\sigma(p-p') \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle$. Altogether, we conclude that $\mathrm{LT}_\sigma(w_{s1}g_sw'_{s1})$ and $\mathrm{LT}_\sigma(u_{s1}g_su'_{s1})$ cancel each other in G_s, i.e. $c_{s1} = d_{s1}$ and $\mathrm{LT}_\sigma(w_{s1}g_sw'_{s1}) = \mathrm{LT}_\sigma(u_{s1}g_su'_{s1})$, and hence $w_{s1}\mathrm{LT}_\sigma(g_s)w'_{s1} = u_{s1}\mathrm{LT}_\sigma(g_s)u'_{s1}$. Therefore $(c_{s1}, w_{s1}, w'_{s1}) = (d_{s1}, u_{s1}, u'_{s1})$ and

$$G_s = \sum_{j=2}^{k_s} c_{sj}w_{sj}g_sw'_{sj} - \sum_{j=2}^{l_s} d_{sj}u_{sj}g_su'_{sj}.$$

Repeatedly applying this argument, we can show that $k_i = l_i$ for all $i \in \{1, \ldots, s\}$, and $(c_{ij}, w_{ij}, w'_{ij}) = (d_{ij}, u_{ij}, u'_{ij})$ for all $i \in \{1, \ldots, s\}$ and all $j \in \{1, \ldots, k_i\}$, and hence $p = p'$. □

From now on, by the Division Algorithm we mean the Leftmost Division Algorithm unless stated otherwise.

Definition 3.2.4. Let $s \geq 1$, let $f, g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$. Then the polynomial $p \in K\langle X\rangle$ obtained in Theorem 3.2.1 is called the **normal remainder** of f with respect to $\mathcal{G}$ and is denoted by $\mathrm{NR}_{\sigma,\mathcal{G}}(f)$.

Note that we have $\mathrm{NR}_{\sigma,\mathcal{G}}(0) = 0$ and $\mathrm{NR}_{\sigma,\emptyset}(f) = f$ for all $f \in \langle X\rangle$ using this definition. Also note that the normal remainder of f with respect to $\mathcal{G}$ is not yet the normal form of f modulo the ideal $\langle\mathcal{G}\rangle$ with respect to σ. The normal remainder of f also depends on the order of polynomials in the tuple $\mathcal{G}$.

Example 3.2.5. **(continued)** Consider Example 3.2.2 again. Recall that in the example we have $f = zx^2yx, g_1 = xy + x, g_2 = x^2 + xz$, and $\sigma =$ `LLex` such that $x >_\sigma y >_\sigma z$. Now we let $g'_1 = g_2, g'_2 = g_1$ and divide f by (g'_1, g'_2). Then the Division Algorithm gives

1) $k_1 = k_2 = 0, p = 0$, and $v = f = zx^2yx$.
2) Since $\mathrm{LT}_\sigma(v) = zx^2yx = z\mathrm{LT}_\sigma(g'_1)yx$, we set $k_1 = 1, c_{11} = \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g'_1)} = 1, w_{11} = z, w'_{11} = yx$, and $v = v - c_{11}w_{11}g'_1w'_{11} = -zxzyx$.
3) Since $\mathrm{LT}_\sigma(v) = zxzyx$ is not a multiple of $\mathrm{LT}_\sigma(g'_1)$ or $\mathrm{LT}_\sigma(g'_2)$, we set $p = p + \mathrm{LM}_\sigma(v) = -zxzyx$ and $v = v - \mathrm{LM}_\sigma(v) = 0$.
4) Since $v = 0$, return the tuple $(c_{11}, w_{11}, w'_{11})$ and the polynomial $p = -zxzyx$.

Therefore we get another representation $f = zg'_1yx - zxzyx = zg_2yx - zxzyx$, and another normal remainder which differs from the normal remainders in Example 3.2.2.

In order to compute the normal form using the Division Algorithm, we need $\mathcal{G}$ to fulfill some additional properties that make $\mathcal{G}$ into a Gröbner basis (see Definition 3.3.1). Gröbner bases are the subject matter of this thesis, which we shall study in the next section and the coming chapters in great detail.

To close this section, we would like to introduce a very useful algorithm, named the *Interreduction Algorithm*, which is an important application of the Division Algorithm.

Definition 3.2.6. Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials. We say G is **interreduced** with respect to σ if no element of $\mathrm{Supp}(g)$ is contained in $\mathrm{LT}_\sigma(G \setminus \{g\})$ for all $g \in G$.

The following lemma, which is an immediate consequence of Theorem 3.2.1, shows implicitly that we can compute an interreduced system of generators of an ideal with the help of the Division Algorithm.

Lemma 3.2.7. *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal I. Moreover, let $g \in G$, and let g' be the normal remainder of g with respect to $G \setminus \{g\}$. If $g' \neq 0$, then $(G \setminus \{g\}) \cup \{g'\}$ is still a system of generators of I.*

Now we present the Interreduction Algorithm which computes an interreduced system of generators of an ideal from a given system of generators.

Theorem 3.2.8. (Interreduction Algorithm) *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$. Consider the following sequence of instructions.*

1) Let $i = 1$ and $s = |G|$.

2) Compute the normal remainder g_i' of g_i with respect to $G \setminus \{0, g_i\}$ using the Division Algorithm given in Theorem 3.2.1.

3) If $g_i' = 0$, then replace g_i by 0, increase i by one, and continue with step 2).

4) If $g_i' \neq g_i$, then replace g_i by g_i', replace i by 1, and continue with step 2).

5) If $i = s$, return the set $\{g \mid g \in G \text{ and } g \neq 0\}$; otherwise, increase i by one and continue with step 2).

This is an algorithm which computes an interreduced system of generators of I.

Proof. We prove the termination by showing that the index i is eventually equal to s in step 5). Observe that the index i is reset to 1 in step 4) under the condition that $g_i' \neq 0$ and $g_i' \neq g_i$. The latter inequality implies that g_i is actually divided by $G \setminus \{0, g_i\}$, and $\mathrm{LT}_\sigma(g_i') \leq_\sigma \mathrm{LT}_\sigma(g_i)$ by Theorem 3.2.1.b. We consider the following two cases.

Case 1) $\mathrm{LT}_\sigma(g_i') = \mathrm{LT}_\sigma(g_i)$. Denote i by K. We observe that the index i increases by one either in step 3) under the condition that $g_i' = 0$ or in step 5) under the condition that g_i cannot be divided by $G \setminus \{0, g_i\}$. Thus for all $j \in \{1, \ldots, K-1\}$ and $g_j \neq 0$, g_j cannot be divided by $G \setminus \{0, g_j\}$, and by assumption, g_j cannot be divided by $G \setminus \{0, g_j, g_K\} \cup \{g_K'\}$ either. Thus after replacing g_K by g_K' and i by 1, the index i will increase to K without changing g_j for all $j \in \{1, \ldots, K-1\}$. Obviously g_K' cannot be divided by $G \setminus \{0, g_K'\}$. Hence the index i increases to $K+1$. Therefore the index i will keep on increasing.

Case 2) $\mathrm{LT}_\sigma(g_i') <_\sigma \mathrm{LT}_\sigma(g_i)$. Since σ is a well-ordering, for each i the leading term of g_i can only strictly decrease finitely many times. Thus there are only finitely many times that the index i can be reset to 1 caused by $\mathrm{LT}_\sigma(g_i') <_\sigma \mathrm{LT}_\sigma(g_i)$. Therefore the index i will eventually increase.

The procedure terminates as the index i will eventually be equal to s in step 5) after finitely many steps. The correctness follows from Theorem 3.2.1 and Lemma 3.2.7. □

Remark 3.2.9. We make some remarks on interreduced systems of generators.

a) An ideal may have many interreduced systems of generators. For instance, consider Example 3.2.2 again. We have $f = zx^2yx$, $g_1 = xy + x$, $g_2 = x^2 + xz$, and $\sigma = \texttt{LLex}$ such that $x >_\sigma y >_\sigma z$. Now we let $I \subseteq \mathbb{Q}\langle x, y, z\rangle$ be the ideal generated by the set $\{f, g_1, g_2\}$. Then by Example 3.2.2 and Lemma 3.2.7 the sets $\{zxzx, xy + x, x^2 + xz\}$ and $\{zxz^2, xy + x, x^2 + xz\}$ are systems of generators of I. It is easy to check that they are both interreduced.

b) An interreduced system of generators G has the property that the elements in the leading term set $\mathrm{LT}_\sigma\{G\}$ are coprime (see Definition 2.1.4). Many optimizations of Gröbner basis computations take advantage of this property (see Section 4.2). In the ApCoCoA package *gbmr*, the Interreduction Algorithm is deployed as a standard preprocessing step in many functions related to Gröbner basis computations. Moreover, if a set G is a σ-Gröbner basis of an ideal I, we can obtain the unique reduced σ-Gröbner basis of I by applying interreduction on G (see Corollary 3.3.18).

3.3 Gröbner Bases

Definition 3.3.1. Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $I = \langle G\rangle$. We say G is a **σ-Gröbner basis** of I if

$$\mathrm{LT}_\sigma\{I\} = \{w\mathrm{LT}_\sigma(g)w' \mid g \in G, w, w' \in \langle X\rangle\}.$$

In other words, G is a σ-Gröbner basis of I if the set G generates the ideal I and the set $\mathrm{LT}_\sigma\{G\}$ generates the leading term $\mathrm{LT}_\sigma\{I\}$ as a monoid ideal of $\langle X\rangle$. By definition, $I \setminus \{0\}$ is a σ-Gröbner basis of I and the empty set $\emptyset$ is a σ-Gröbner basis of the zero ideal $\langle 0\rangle$.

In contrast to the case of commutative polynomial ring, for a polynomial $g \in K\langle X\rangle\setminus\{0\}$ the set $\{g\}$ need not be a σ-Gröbner basis of the principal ideal $\langle g\rangle \subseteq K\langle X\rangle$. The following example is borrowed from [35] as a case in point.

Example 3.3.2. Consider the free monoid ring $\mathbb{Q}\langle x, y\rangle$ equipped with the admissible ordering $\sigma = \mathtt{LLex}$ such that $x >_\sigma y$ and the ideal $\langle g\rangle$ where $g = x^2 - xy$. Obviously we have $f = g(x - y) - xg = -xyx + xy^2 \in \langle g\rangle$ and $\mathrm{LT}_\sigma(f) = xyx$ is not a multiple of $\mathrm{LT}_\sigma(g) = x^2$. Thus the set $\{g\}$ is not a σ-Gröbner basis of the ideal $\langle g\rangle$. Actually, the ideal $\langle g\rangle$ has the infinite (reduced) σ-Gröbner basis $\{xy^ix - xy^{i+1} \mid i \in \mathbb{N}\}$ (see [35], Proposition 0.3.1).

The following proposition follows from Definition 3.3.1 immediately.

Proposition 3.3.3. *If G is a σ-Gröbner basis of an ideal I, then the set $\mathrm{LT}_\sigma\{G\}$ generates the leading term ideal $\mathrm{LT}_\sigma(I)$.*

The converse of Proposition 3.3.3 is also true.

Proposition 3.3.4. *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $I = \langle G\rangle$. If the set $\mathrm{LT}_\sigma\{G\}$ generates the leading term ideal $\mathrm{LT}_\sigma(I)$, then G is a σ-Gröbner basis of I.*

Proof. By assumption, we have $wgw' \in I$ for all $w, w' \in \langle X\rangle, g \in G$. Then by Remark 3.1.13.b we have $w\mathrm{LT}_\sigma(g)w' = \mathrm{LT}_\sigma(wgw') \in \mathrm{LT}_\sigma\{I\}$, and hence $\{w\mathrm{LT}_\sigma(g)w' \mid g \in G, w, w' \in \langle X\rangle\} \subseteq \mathrm{LT}_\sigma\{I\}$. Conversely, assume $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma\{I\}$ for some $f \in I \setminus \{0\}$. Clearly $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma(I)$. Since $\mathrm{LT}_\sigma\{G\}$ generates $\mathrm{LT}_\sigma(I)$, it follows from Propostion 2.2.13 that there exists $g \in G$ such that $\mathrm{LT}_\sigma(f)$ is a multiple of $\mathrm{LT}_\sigma(g)$. Thus $\mathrm{LT}_\sigma(f) \in \{w\mathrm{LT}_\sigma(g)w' \mid g \in G, w, w' \in \langle X\rangle\}$. Hence $\mathrm{LT}_\sigma\{I\} \subseteq \{w\mathrm{LT}_\sigma(g)w' \mid g \in G, w, w' \in \langle X\rangle\}$. □

Corollary 3.3.5. *Let $S \subseteq \langle X \rangle$ be a set of words which generates an ideal $\langle S \rangle \subseteq K\langle X \rangle$. Then S is a Gröbner basis of $\langle S \rangle$ with respect to every admissible ordering.*

Proof. This follows directly from Proposition 3.3.4. □

One of the most frequently used properties of Gröbner bases is as follows.

Proposition 3.3.6. *Let $G \subseteq K\langle X \rangle \setminus \{0\}$ be a set of polynomials. Then the following conditions are equivalent.*

a) The set G is a σ-Gröbner basis of I.

b) For every polynomial $f \in I \setminus \{0\}$, there exists a representation

$$f = \sum_{i=1}^{s} c_i w_i g_i w_i'$$

with $c_i \in K \setminus \{0\}, w_i, w_i' \in \langle X \rangle$, and $g_i \in G$ such that $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_i g_i w_i')$ for all $i \in \{1, \ldots, s\}$.

Proof. To prove condition a) implies condition b), consider the following sequence of instructions.

1) Let $s = 0$ and $v = f$.

2) Choose $g \in G$ such that $\mathrm{LT}_\sigma(v) = w\mathrm{LT}_\sigma(g)w'$ for some $w, w' \in \langle X \rangle$. Increase s by one, set $c_s = \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g)}, g_s = g, w_s = w, w_s' = w'$, and replace v by $v - c_s w_s g_s w_s'$.

3) If now $v = 0$, return the tuples $(c_1, w_1, g_1, w_1'), \ldots, (c_s, w_s, g_s, w_s')$. If $v \neq 0$, start again with step 2).

Clearly we have $v \in I$ at each point of the procedure. Since G is a σ-Gröbner basis of I, there always exists $g \in G$ such that $\mathrm{LT}_\sigma(v) = w\mathrm{LT}_\sigma(g)w'$ for some $w, w' \in \langle X \rangle$ in step 2). Before replacing v by $v - c_s w_s g_s w_s'$, we have $\mathrm{LT}_\sigma(c_s w_s g_s w_s') = w_s \mathrm{LT}_\sigma(g_s) w_s' = w\mathrm{LT}_\sigma(g)w' = \mathrm{LT}_\sigma(v)$ by Remark 3.1.13.b, and $\mathrm{LC}_\sigma(c_s w_s g_s w_s') = c_s \mathrm{LC}_\sigma(g_s) = \mathrm{LC}_\sigma(v)$. If $v - c_s w_s g_s w_s' \neq 0$, then by Remark 3.1.13.a we have $\mathrm{LT}_\sigma(v - c_s w_s g_s w_s') <_\sigma \mathrm{LT}_\sigma(v)$, i.e. $\mathrm{LT}_\sigma(v)$ strictly decreases with respect to σ. Since σ is a well-ordering, step 2) can be executed only finitely many times. Hence the procedure stops after finitely many steps. When the procedure stops, we have $f = \sum_{i=1}^{s} c_i w_i g_i w_i'$ and $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_i g_i w_i')$ for all $i = 1, \ldots, s$. Therefore we obtain a representation of f as claimed.

We prove condition b) implies condition a). Obviously the set G generates the ideal I. Note that $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_i g_i w_i')$ for all $i \in \{1,\ldots,s\}$ implies $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(w_i g_i w_i')$ for some $i \in \{1,\ldots,s\}$. Then condition a) follows from Remark 3.1.13.b and Definition 3.3.1. □

Definition 3.3.7. Let $f \in K\langle X\rangle \setminus \{0\}$ be a polynomial, and let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials. We say that f has a **Gröbner representation** in terms of G if there exist $c_1,\ldots,c_s \in K \setminus \{0\}, w_1,\ldots,w_s' \in \langle X\rangle$, and $g_1,\ldots,g_s \in G$ such that

$$f = \sum_{i=1}^{s} c_i w_i g_i w_i'$$

and $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_i g_i w_i')$ for all $i = 1,\ldots,s$.

Now Proposition 3.3.6 can be rephrased as follows. Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $I = \langle G\rangle$. Then G is a σ-Gröbner basis of I if and only if every polynomial $f \in I \setminus \{0\}$ has a Gröbner representation in terms of G.

Remark 3.3.8. We observe again the instructions in the proof of Proposition 3.3.6. Since in step 2) the leading term $\mathrm{LT}_\sigma(v)$ of v strictly decreases with respect to σ, the Gröbner representation of f that we obtain during the proof of Proposition 3.3.6 also satisfies the condition

$$\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(w_1 g_1 w_1') >_\sigma \mathrm{LT}_\sigma(w_2 g_2 w_2') >_\sigma \cdots >_\sigma \mathrm{LT}_\sigma(w_s g_s w_s').$$

In [55], T. Mora called a representation that also satisfies this additional condition a *Gröbner representation* of f in terms of G, which slightly differs from Definition 3.3.7.

The instructions in the proof of Proposition 3.3.6 inspire the following Weak Division Algorithm. The proof of the Weak Division Algorithm is straightforward.

Corollary 3.3.9. (The Weak Division Algorithm) *Let $f \in K\langle X\rangle \setminus \{0\}$ be a polynomial, and let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials. Consider the following sequence of instructions.*

1) *Let $s = 0$ and $v = f$.*

2) *If there is $g \in G$ such that $\mathrm{LT}_\sigma(v) = w\mathrm{LT}_\sigma(g)w'$ for some $w, w' \in \langle X\rangle$, increase s by one, set $c_s = \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g)}, w_s = w, w_s' = w, g_s = g$, and replace v by $v - c_s w_s g_s w_s'$.*

3) *Repeat step 2) until there is no more $g \in G$ such that $\mathrm{LT}_\sigma(v)$ is a multiple of $\mathrm{LT}_\sigma(g)$.*

4) Return the tuples $(c_1, w_1, g_1, w_1'), \ldots, (c_s, w_s, g_s, w_s')$ *and the polynomial* $v \in K\langle X\rangle$.

This is an algorithm which returns tuples $(c_1, w_1, g_1, w_1'), \ldots, (c_s, w_s, g_s, w_s')$ *and a polynomial* $v \in K\langle X\rangle$ *such that*

$$f = \sum_{i=1}^{s} c_i w_i g_i w_i' + v$$

and such that the following conditions are satisfied.

a) If $v \neq 0$*, we have* $\mathrm{LT}_\sigma(v) \leq_\sigma \mathrm{LT}_\sigma(f)$ *and* $\mathrm{LT}_\sigma(v) \notin \mathrm{LT}_\sigma(G)$.

b) We have $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(w_1 g_1 w_1') >_\sigma \mathrm{LT}_\sigma(w_2 g_2 w_2') >_\sigma \cdots >_\sigma \mathrm{LT}_\sigma(w_s g_s w_s')$.

In the literature, the Weak Division Algorithm is also called the **top-reduction algorithm** in the sense that it reduces only the leading terms of dividends (compare with Theorem 3.2.1). A polynomial $v \in K\langle X\rangle$ obtained in Corollary 3.3.9 is called a **weak normal remainder** of f with respect to G and is denoted by $\mathrm{WNR}_{\sigma,G}(f)$. Observe that in step 2) the algorithm chooses g from G arbitrarily. Examples 3.2.2 and 3.2.5 indicate that weak normal remainder $\mathrm{WNR}_{\sigma,G}(f)$ is not unique. If G is a σ-Gröbner basis of an ideal I, then by Proposition 3.3.6 the Weak Division Algorithm gives a Gröbner representation of f in terms of G for all $f \in I \setminus \{0\}$. On the other hand, if there exists some $f \in I \setminus \{0\}$ such that $\mathrm{WNR}_{\sigma,G}(f) \neq 0$, then G is not a σ-Gröbner basis of I. In Section 4.1 we will use the Weak Division Algorithm to check whether or not a (finite) set of polynomials is a Gröbner basis (see Corollary 4.1.18).

As we promised in last section, now we shall make a connection between the normal remainder and the normal form using Gröbner bases as follows.

Proposition 3.3.10. *Let* $G \subseteq K\langle X\rangle \setminus \{0\}$ *be a set of polynomials which generates an ideal* $I = \langle G\rangle$*. Moreover, let* G *be a* σ*-Gröbner basis of* I*, and let* $\mathcal{G}$ *be an associated tulpe of* G*, i.e.* $\mathcal{G}$ *consists of all polynomials in* G*. Then we have* $\mathrm{NR}_{\sigma,\mathcal{G}}(f) = \mathrm{NF}_{\sigma,I}(f)$ *for all* $f \in K\langle X\rangle$.

Proof. By Theorem 3.2.1.a, no element of $\mathrm{Supp}(\mathrm{NR}_{\sigma,\mathcal{G}}(f))$ is contained in $\mathrm{LT}_\sigma(G)$. By assumption and Definition 3.3.1, we have $\mathrm{LT}_\sigma\{I\} \subset \mathrm{LT}_\sigma(I) = \mathrm{LT}_\sigma(G)$. Consequently, no element of $\mathrm{Supp}(\mathrm{NR}_{\sigma,\mathcal{G}}(f))$ is contained in $\mathrm{LT}_\sigma\{I\}$. Hence $\mathrm{NR}_{\sigma,\mathcal{G}}(f) \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$. Then $\mathrm{NR}_{\sigma,\mathcal{G}}(f) = \mathrm{NF}_{\sigma,I}(f)$ follows from the fact $f - \mathrm{NR}_{\sigma,\mathcal{G}}(f) \in I$ and Corollary 3.1.16.b. □

Remark 3.3.11. Recall that the normal remainder of f with respect to the tuple $\mathcal{G}$ relies on the order of polynomials in $\mathcal{G}$, while the normal form of f with respect to the ideal $\langle G\rangle$ is unique. Proposition 3.3.10 indicates that if G is a σ-Gröbner basis of $\langle G\rangle$, then the normal remainder of f does not depend on the order of polynomials in $\mathcal{G}$ any longer. Moreover, if G is a σ-Gröbner basis of $\langle G\rangle$, then the Division Algorithm (Theorem 3.2.1) gives the same normal remainder no matter which strategy is applied to choose the pair (w, w') in step 2).

Remark 3.3.12. If G is a σ-Gröbner basis of the ideal $I = \langle X\rangle$, Proposition 3.3.10 says that for $f \in K\langle X\rangle$ the normal form $\mathrm{NF}_{\sigma,I}(f)$ can be achieved by computing the normal remainder $\mathrm{NR}_{\sigma,\mathcal{G}}(f)$. Consequently, as an important application of Gröbner bases, we may solve the word problem (see Definition 2.1.20) as follows.

1) Let $\mathcal{M} = \langle X \mid R\rangle$ be a finitely presented monoid, and let $u, v \in \langle X\rangle$ be two words. Moreover, let $I \subseteq K\langle X\rangle$ be the ideal generated by the set $\{w - w' \mid (w, w') \in R\}$.
2) Choose an admissible ordering σ on $\langle X\rangle$ and compute a σ-Gröbner basis G of I.
3) Compute the normal remainder $\mathrm{NR}_{\sigma,\mathcal{G}}(u-v)$. By Remark 3.1.19 and Proposition 3.3.10 u and v define the same element in $\mathcal{M}$ if and only if $\mathrm{NR}_{\sigma,\mathcal{G}}(u-v) = 0$.

However, the fact that the word problem is undecidable indicates that there can be no algorithm to compute Gröbner bases.

Generally, an ideal $I \subseteq K\langle X\rangle$ has many σ-Gröbner bases. For example, let G be a σ-Gröbner basis of an ideal $I \subseteq K\langle X\rangle \setminus \{0\}$, and let $f \in I \setminus G$ be a non-zero polynomial. Clearly we have $I = \langle G \cup \{f\}\rangle$. By Definition 3.3.1 $\mathrm{LT}_\sigma\{G\}$ generates $\mathrm{LT}_\sigma\{I\}$. Thus $\mathrm{LT}_\sigma\{G \cup \{f\}\} = \mathrm{LT}_\sigma\{G\} \cup \{\mathrm{LT}_\sigma(f)\}$ also generates $\mathrm{LT}_\sigma\{I\}$. Hence again by Definition 3.3.1 $G \cup \{f\}$ is a σ-Gröbner basis of I.

Definition 3.3.13. Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, and let G be a σ-Gröbner basis of I. A polynomial $f \in G$ is called **redundant** if $G \setminus \{f\}$ is also a σ-Gröbner basis of I.

Contrarily, a polynomial $f \in G$ is called **irredundant** if it is not redundant. Redundant polynomials can be detected easily by the following proposition.

Proposition 3.3.14. *Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, and let G be a σ-Gröbner basis of I. A polynomial $f \in G$ is redundant if $\mathrm{LT}_\sigma(f)$ is a multiple of $\mathrm{LT}_\sigma(g)$ for some $g \in G \setminus \{f\}$.*

To prove the proposition we need the following lemma.

Lemma 3.3.15. *Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, and let $G \subseteq I \setminus \{0\}$ be a subset. If the set $\mathrm{LT}_\sigma\{G\}$ generates the leading term set $\mathrm{LT}_\sigma\{I\}$, then G is a σ-Gröbner basis of I.*

Proof. By Definition 3.3.1, it suffices to prove that $I = \langle G\rangle$. For the sake of contradiction, we suppose that $\langle G\rangle \subset I$. Since σ is a well-ordering, there exists a polynomial $f \in I \setminus \langle G\rangle$ having minimal leading term $\mathrm{LT}_\sigma(f)$ with respect to σ among all polynomials in $I \setminus \langle G\rangle$. Since $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma\{I\}$ and $\mathrm{LT}_\sigma\{G\}$ generates $\mathrm{LT}_\sigma\{I\}$, there exist $c \in K \setminus \{0\}, w, w' \in \langle X\rangle$, and $g \in G$ such that $\mathrm{LM}_\sigma(f) = \mathrm{LM}_\sigma(cwgw')$ and $f - cwgw' \in I \setminus \langle G\rangle$. Then by Remark 3.1.13.a we have $\mathrm{LT}_\sigma(f - cwgw') <_\sigma \mathrm{LT}_\sigma(f)$, contradicting our choice of f. □

Proof. (Proof of Proposition 3.3.14) By Definition 3.3.1 $G \subseteq I$ and $\mathrm{LT}_\sigma\{G\}$ generates $\mathrm{LT}_\sigma\{I\}$. By assumption, $\mathrm{LT}_\sigma\{G \setminus \{f\}\}$ also generates $\mathrm{LT}_\sigma\{I\}$. Then the claim follows from $G \setminus \{f\} \subseteq I$, Lemma 3.3.15, and Definition 3.3.13. □

By removing redundant elements we reduce the size of a Gröbner basis. Moreover, for every ideal we define a unique Gröbner basis as follows.

Definition 3.3.16. Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, and let G be a σ-Gröbner basis of I. The set G is called the **reduced σ-Gröbner basis** of I if G is interreduced and every polynomial in G is monic.

Proposition 3.3.17. *For every ideal $I \subseteq K\langle X\rangle \setminus \{0\}$, there exists a unique reduced σ-Gröbner basis.*

Proof. We first prove the existence. Note that the leading term set $\mathrm{LT}_\sigma\{I\}$ is a monoid ideal of $\langle X\rangle$. By Proposition 2.1.24 there exists a unique minimal system of generators of $\mathrm{LT}_\sigma\{I\}$. We assume that the minimal system of generators of $\mathrm{LT}_\sigma\{I\}$ is $\mathrm{LT}_\sigma\{G\} \subseteq \langle X\rangle$ with the associated set of polynomials $G \subseteq K\langle X\rangle \setminus \{0\}$. Now we let $G' = \{\mathrm{LT}_\sigma(g) - \mathrm{NF}_{\sigma,I}(\mathrm{LT}_\sigma(g)) \mid g \in G\}$. We prove that G' is actually the reduced σ-Gröbner basis of I. By Corollary 3.1.16.b we have $\mathrm{LT}_\sigma(g) - \mathrm{NF}_{\sigma,I}(\mathrm{LT}_\sigma(g)) \in I$ for all $g \in G$, and hence $G' \subseteq I$. Clearly $\mathrm{LT}_\sigma\{G'\} = \mathrm{LT}_\sigma\{G\}$ generates $\mathrm{LT}_\sigma\{I\}$. Thus by Lemma 3.3.15 G' is a σ-Gröbner basis of I. By the definition of G' and Corollary 3.1.16, G' is interreduced and polynomials in G' are monic. Hence G' is the reduced σ-Gröbner basis of I.

To prove the uniqueness, we assume that G and H are two reduced σ-Gröbner bases of I. Clearly $\mathrm{LT}_\sigma\{G\}$ and $\mathrm{LT}_\sigma\{H\}$ are the minimal systems of generators of $\mathrm{LT}_\sigma\{I\}$. Then by Proposition 2.1.24 we must have $\mathrm{LT}_\sigma\{G\} = \mathrm{LT}_\sigma\{H\}$. Let $g \in G$ and $h \in H$ such that $\mathrm{LT}_\sigma(g) = \mathrm{LT}_\sigma(h)$. Then we have $g - h \in I$. Since G and H are interreduced, we have $g - h \subseteq \mathrm{Span}_K \mathcal{O}_\sigma(I)$. Finally, we have $g - h = 0$ by Corollary 3.1.16.a. □

Note that the reduced Gröbner basis need not be finite. Given a finite Gröbner basis, we can compute the reduced Gröbner basis by interreduction.

Corollary 3.3.18. *Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, and let G be a finite σ-Gröbner basis of I. We apply the Interreduction Algorithm as in Theorem 3.2.8 on G and obtain an interreduced set G'. Then G' is the reduced σ-Gröbner basis of I.*

Proof. This follows from Theorem 3.2.8 and Definition 3.3.16. □

Inspired by the proof of Proposition 3.3.17, we can also compute the reduced σ-Gröbner basis from a given finite σ-Gröbner basis as follows.

Corollary 3.3.19. *Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, and let G be a finite σ-Gröbner basis of I. Consider the following sequence of instructions.*

1) *Find a subset $G' \subseteq G$ such that the set $\mathrm{LT}_\sigma\{G'\}$ is the minimal system of generators of the leading term set $\mathrm{LT}_\sigma\{I\}$.*

2) *Return the set $G'' = \{\mathrm{LT}_\sigma(g) - \mathrm{NR}_{\sigma,\mathcal{G}'}(\mathrm{LT}_\sigma(g)) \mid g \in G'\}$.*

This is a algorithm which computes the σ-reduced Gröbner basis G'' of I from a given finite σ-Gröbner basis G of I.

Proof. By assumption and Lemma 3.3.15, G' is a σ-Gröbner basis of I. Then by Proposition 3.3.10 we have $\mathrm{NF}_{\sigma,I}(\mathrm{LT}_\sigma(g)) = \mathrm{NR}_{\sigma,\mathcal{G}'}(\mathrm{LT}_\sigma(g))$. The claim follows from the proof of Proposition 3.3.17. □

A set G' as in step 1) of Corollary 3.3.19 is called a **minimal σ-Gröbner basis** of the ideal I.

3.4 Syzygies

In this section we shall characterize Gröbner bases using syzygy modules. In commutative polynomial rings, Gröbner bases can be characterized by systems of generators of syzygy modules successfully (see [43], Section 2.3). This approach leads to a sequence of the most efficient optimizations of Buchberger's Algorithm (see [17, 27, 33]). Analogously, we shall use systems of generators of syzygy modules to characterize Gröbner bases in free monoid rings. We will obtain a Buchberger Criterion from syzygy modules in Section 4.1 and present our optimizations of the Buchberger Procedure in Section 4.2.

In what follows, we let $s \geq 1$, $g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$, $\mathcal{G}$ the tuple $(g_1, \ldots, g_s)$, and $\mathrm{LM}_\sigma(\mathcal{G})$ the tuple $(\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))$. Moreover, we let $F_s = (K\langle X\rangle \otimes K\langle X\rangle)^s$ be the free $K\langle X\rangle$-bimodule of rank s with the canonical basis $\{\epsilon_1, \ldots, \epsilon_s\}$, where $\epsilon_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$ with $1 \otimes 1$ occurring in the i^{th} position for $i = 1, \ldots, s$.

Definition 3.4.1. Using the notation above, we define syzygy and syzygy module as follows.

a) An element $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_s$ is called a **two-sided syzygy** of $\mathcal{G}$ if

$$\sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} = 0.$$

b) Let $\mathrm{Syz}(\mathcal{G})$ be the set of all two-sided syzygies of $\mathcal{G}$. One can remark that $\mathrm{Syz}(\mathcal{G})$ is indeed a two-sided $K\langle X\rangle$-module. The set $\mathrm{Syz}(\mathcal{G})$ is called the **two-sided syzygy module** of $\mathcal{G}$.

Similarly, a two-sided syzygy of $\mathrm{LM}_\sigma(\mathcal{G})$ is an element $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_s$ such that $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \mathrm{LM}_\sigma(g_i) w'_{ij} = 0$; the set of all two-sided syzygies of $\mathrm{LM}_\sigma(\mathcal{G})$ also forms a two-sided $K\langle X\rangle$-module and is denoted by $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. In what follows, by syzygy and syzygy module we mean two-sided syzygy and two-sided syzygy module, respectively, unless specified otherwise.

Example 3.4.2. Consider the free monoid ring $\mathbb{Q}\langle x, y, z\rangle$ equipped with the admissible ordering $\sigma = \texttt{LLex}$ such that $x >_\sigma y >_\sigma z$. Let $g_1 = 2x^2 + yx, g_2 = xy + zy$, and let $\mathcal{G}$ be the tuple (g_1, g_2). We have $\mathrm{LM}_\sigma(\mathcal{G}) = (\mathrm{LM}_\sigma(g_1), \mathrm{LM}_\sigma(g_2)) = (2x^2, xy)$. It is easy to check that $g_2\epsilon_1 - \epsilon_2 g_1, \epsilon_1 g_2 - g_1\epsilon_2 \in (\mathbb{Q}\langle x, y, z\rangle \otimes \mathbb{Q}\langle x, y, z\rangle)^2$ are syzygies of $\mathcal{G}$, and $\epsilon_1 xy - 2x^2\epsilon_2, \epsilon_1 y - 2x\epsilon_2 \in (\mathbb{Q}\langle x, y, z\rangle \otimes \mathbb{Q}\langle x, y, z\rangle)^2$ are syzygies of $\mathrm{LM}_\sigma(\mathcal{G})$.

Recall that in Example 2.3.15 we made F_s into a $\langle X\rangle$-graded $K\langle X\rangle$-bimodule by a grading defined by a tuple of words. Consider the tulpe $(\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s))$. We have $F_s(w) = \{\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_s \mid \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \mathrm{LT}_\sigma(g_i) w'_{ij} \in Kw\}$ for $w \in \langle X\rangle$. The following definition proves very useful.

Definition 3.4.3. Let $m = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\epsilon_i w'_{ij} \in F_s \setminus \{0\}$.

a) The word

$$\max_{\sigma}\{w_{ij}\mathrm{LT}_\sigma(g_i)w'_{ij} \mid i \in \{1,\dots,s\}, j \in \mathbb{N}, c_{ij} \neq 0\} \in \langle X\rangle$$

is called **σ-degree** of m and is denoted by $\deg_{\sigma,\mathcal{G}}(m)$.

b) The homogeneous component of degree $\deg_{\sigma,\mathcal{G}}(m)$ of m is called the **σ-leading form** of m and is denoted by $\mathrm{LF}_{\sigma,\mathcal{G}}(m)$, i.e. $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} \bar{c}_{ij}\bar{w}_{ij}\epsilon_i\bar{w}'_{ij} \in F_s \setminus \{0\}$ with

$$\bar{c}_{ij}\bar{w}_{ij}\epsilon_i\bar{w}'_{ij} = \begin{cases} c_{ij}w_{ij}\epsilon_i w'_{ij} & \text{if } c_{ij} \neq 0 \text{ and } w_{ij}\mathrm{LT}_\sigma(g_i)w'_{ij} = \deg_{\sigma,\mathcal{G}}(m), \\ 0 & \text{otherwise.} \end{cases}$$

c) m is called **homogeneous** of σ-degree $\deg_{\sigma,\mathcal{G}}(m)$ if $m \in F_s(\deg_{\sigma,\mathcal{G}}(m))$.

Example 3.4.4. (continued) Consider Example 3.4.2 again. Recall that in the example we have the tuple (g_1, g_2) with $g_1 = 2x^2 + yx, g_2 = xy + zy$, and $\sigma = \mathtt{LLex}$ such that $x >_\sigma y >_\sigma z$.

a) Let $m = g_2\epsilon_1 - \epsilon_2 g_1 \in (\mathbb{Q}\langle x,y,z\rangle \otimes \mathbb{Q}\langle x,y,z\rangle)^2$. We have

$$\begin{aligned} \deg_{\sigma,\mathcal{G}}(m) &= \max_{\sigma}\{xy\mathrm{LT}_\sigma(g_1), zy\mathrm{LT}_\sigma(g_1), \mathrm{LT}_\sigma(g_2)x^2, \mathrm{LT}_\sigma(g_2)yx\} \\ &= \max_{\sigma}\{xy\cdot x^2, zy\cdot x^2, xy\cdot x^2, xy\cdot yx\} = xyx^2, \\ \mathrm{LF}_{\sigma,\mathcal{G}}(m) &= xy\epsilon_1 - 2\epsilon_2 x^2 \neq m. \end{aligned}$$

The element $g_2\epsilon_1 - \epsilon_2 g_1$ is not homogeneous of σ-degree xyx^2.

b) Let $m = \epsilon_1 y - 2x\epsilon_2 \in (\mathbb{Q}\langle x,y,z\rangle \otimes \mathbb{Q}\langle x,y,z\rangle)^2$. We have

$$\begin{aligned} \deg_{\sigma,\mathcal{G}}(m) &= \max_{\sigma}\{\mathrm{LT}_\sigma(g_1)y, x\mathrm{LT}_\sigma(g_2)\} \\ &= \max_{\sigma}\{x^2\cdot y, x\cdot xy\} = x^2y, \\ \mathrm{LF}_{\sigma,\mathcal{G}}(m) &= \epsilon_1 y - 2x\epsilon_2 = m. \end{aligned}$$

The element $\epsilon_1 y - 2x\epsilon_2$ is homogeneous of σ-degree x^2y.

Now we consider the free monoid ring $K\langle X\rangle$ as a $K\langle X\rangle$-bimodule. Let $M \subseteq K\langle X\rangle$ be the two-sided $K\langle X\rangle$-submodule generated by the set $\{g_1,\dots,g_s\}$, and let $N \subseteq K\langle X\rangle$ be the two-sided $K\langle X\rangle$-submodule generated by the set $\{\mathrm{LM}_\sigma(g_1),\dots,\mathrm{LM}_\sigma(g_s)\}$. Moreover, let $\lambda : F_s \to M$ be the $K\langle X\rangle$-bimodule homomorphism given by $\epsilon_i \mapsto g_i$ for $i = 1,\dots,s$, and let $\Lambda : F_s \to N$ be the $K\langle X\rangle$-bimodule homomorphism given by $\epsilon_i \mapsto \mathrm{LM}_\sigma(g_i)$ for $i = 1,\dots,s$. Then we have $\mathrm{Syz}(\mathcal{G}) = \ker(\lambda)$ and $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) = \ker(\Lambda)$.

Lemma 3.4.5. *For all* $m \in F_s \setminus \mathrm{Syz}(\mathcal{G})$*, we have* $\mathrm{LT}_\sigma(\lambda(m)) \leq_\sigma \deg_{\sigma,\mathcal{G}}(m)$*. Moreover,* $\mathrm{LT}_\sigma(\lambda(m)) = \deg_{\sigma,\mathcal{G}}(m)$ *if and only if* $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \notin \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$*.*

Proof. Let $m = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij}$. We have $\lambda(m) = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} \neq 0$ by assumption. Then $\mathrm{LT}_\sigma(\lambda(m)) \leq_\sigma \deg_{\sigma,\mathcal{G}}(m)$ follows from Proposition 3.1.13.a and Definition 3.4.3.a. To prove the second claim, it suffices to show that $\mathrm{LT}_\sigma(\lambda(m)) <_\sigma \deg_{\sigma,\mathcal{G}}(m)$ if and only if $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Note that $\mathrm{LT}_\sigma(\lambda(m)) <_\sigma \deg_{\sigma,\mathcal{G}}(m)$ if and only if the coefficient of $\deg_{\sigma,\mathcal{G}}(m)$ in $\sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} g_i w'_{ij}$ vanishes. The latter is equivalent to $\Lambda(\mathrm{LF}_{\sigma,\mathcal{G}}(m)) = 0$, i.e. $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. □

Example 3.4.6. (continued) Consider Example 3.4.2 again. Recall that in the example we have the tuple (g_1, g_2) with $g_1 = 2x^2 + yx, g_2 = xy + zy$, and $\sigma = \texttt{LLex}$ such that $x >_\sigma y >_\sigma z$. Let $M \subseteq \mathbb{Q}\langle x, y, z\rangle$ be the ideal generated by $\{g_1, g_2\}$, and let $N \subseteq \mathbb{Q}\langle x, y, z\rangle$ be the ideal generated by $\{\mathrm{LM}_\sigma(g_1), \mathrm{LM}_\sigma(g_2)\}$.

a) Let $m = \epsilon_1 y - 2x\epsilon_2 \in (\mathbb{Q}\langle x, y, z\rangle \otimes \mathbb{Q}\langle x, y, z\rangle)^2$. We have $\lambda(m) = g_1 y - 2xg_2 = -2xzy + yxy \neq 0$. Thus $m \notin \mathrm{Syz}(\mathcal{G})$, $\mathrm{LT}_\sigma(\lambda(m)) = xzy$, and $\mathrm{LM}_\sigma(\lambda(m)) = -2xzy$. From Example 3.4.4.b, we have $\deg_{\sigma,\mathcal{G}}(m) = x^2y$ and $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \epsilon_1 y - 2x\epsilon_2 = m$. Therefore $\deg_{\sigma,\mathcal{G}}(m) >_\sigma \mathrm{LT}_\sigma(\lambda(m))$, $\Lambda(\mathrm{LF}_{\sigma,\mathcal{G}}(m)) = \mathrm{LM}_\sigma(g_1)y - 2x\mathrm{LM}_\sigma(g_2) = 2x^2 \cdot y - 2x \cdot xy = 0$, and hence $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

b) Let $m = xy\epsilon_1 x - 2x\epsilon_2 x^2 \in (\mathbb{Q}\langle x, y, z\rangle \otimes \mathbb{Q}\langle x, y, z\rangle)^2$. We have

$$\begin{aligned}\deg_{\sigma,\mathcal{G}}(m) &= \max_\sigma\{xy\mathrm{LT}_\sigma(g_1 x), x\mathrm{LT}_\sigma(g_2)x^2\} = x^2yx^2,\\ \mathrm{LF}_{\sigma,\mathcal{G}}(m) &= -2x\epsilon_2 x^2 \neq m.\end{aligned}$$

The element $xy\epsilon_1 x - 2x\epsilon_2 x^2$ is not homogeneous of σ-degree x^2yx^2. We also have $\lambda(m) = xyg_1x - 2xg_2x^2 = -2x^2yx^2 + 2xyx^3 + xy^2x^2 - 2xzyx^2$. Thus $m \notin \mathrm{Syz}(\mathcal{G})$, $\mathrm{LT}_\sigma(\lambda(m)) = x^2yx^2$, and $\mathrm{LM}_\sigma(\lambda(m)) = -2x^2yx^2$. Therefore $\deg_{\sigma,\mathcal{G}}(m) = \mathrm{LT}_\sigma(\lambda(m))$, $\Lambda(\mathrm{LF}_{\sigma,\mathcal{G}}(m)) = -2x\mathrm{LM}_\sigma(g_2)x^2 = -2x \cdot xy \cdot x^2 \neq 0$, and hence $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \notin \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

In the following we shall introduce another crucial ingredient of Gröbner basis theory, which plays an analogous role to the critical syzygy in commutative polynomial ring.

Definition 3.4.7. Let $i, j \in \{1, \ldots, s\}$ and $i \leq j$, the element

$$\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) = \frac{1}{\mathrm{LC}_\sigma(g_i)} w_i \epsilon_i w'_i - \frac{1}{\mathrm{LC}_\sigma(g_j)} w_j \epsilon_j w'_j \in F_s \setminus \{0\}$$

with $w_i, w'_i, w_j, w'_j \in \langle X\rangle$ such that $w_i\mathrm{LT}_\sigma(g_i)w'_i = w_j\mathrm{LT}_\sigma(g_j)w'_j$, is called an **obstruction** of g_i and g_j. If $i = j$, it is called a **self obstruction** of g_i. The **set of all obstructions** of g_i and g_j will be denoted by $\mathrm{o}(i,j)$.

Note that for all $i, j \in \{1,\dots,s\}$ and $i \le j$, the set $\mathrm{o}(i,j)$ is non-empty since it contains trivial elements $\mathrm{o}_{i,j}(\mathrm{LT}_\sigma(g_j)w, 1; 1, w\mathrm{LT}_\sigma(g_i)), \mathrm{o}_{i,j}(1, w\mathrm{LT}_\sigma(g_j); \mathrm{LT}_\sigma(g_i)w, 1)$ for all $w \in \langle X\rangle$.

Lemma 3.4.8. *Let $i, j \in \{1,\dots,s\}$ and $i \le j$.*

a) Every element $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$ of $\mathrm{o}(i,j)$ is a syzygy of $\mathrm{LM}_\sigma(\mathcal{G})$ and is homogeneous of σ-degree $w_i\mathrm{LT}_\sigma(g_i)w'_i = w_j\mathrm{LT}_\sigma(g_j)w'_j$.

b) We have $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) = \langle \cup_{1\le i\le j\le s}\mathrm{o}(i,j)\rangle$.

Proof. Claim a) follows immediately from Definitions 3.4.3 and 3.4.7. To prove claim b), it suffices, by a), to prove that $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) \subseteq \langle \cup_{1\le i\le j\le s}\mathrm{o}(i,j)\rangle$. Let $m = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\epsilon_i w'_{ij} \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) \setminus \{0\}$. We may assume without loss of generality that m is homogeneous of σ-degree $\deg_{\sigma,\mathcal{G}}(m)$ and all terms in the representation of m are pairwise distinct. We must have $|\mathrm{Supp}(m)| \ge 2$ since $m \ne 0$ and $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\mathrm{LM}_\sigma(g_i)w'_{ij} = 0$. Thus there exist $w_{ij}\epsilon_i w'_{ij}, w_{kl}\epsilon_k w'_{kl} \in \mathrm{Supp}(m)$ such that $w_{ij}\mathrm{LT}_\sigma(g_i)w'_{ij} = w_{kl}\mathrm{LT}_\sigma(g_k)w'_{kl}$. We may assume without loss of generality that $i \le k$. We deduce that $\mathrm{o}_{i,k}(w_{ij}, w'_{ij}; w_{kl}, w'_{il}) = \frac{1}{\mathrm{LC}_\sigma(g_i)}w_{ij}\epsilon_i w'_{ij} - \frac{1}{\mathrm{LC}_\sigma(g_k)}w_{kl}\epsilon_k w'_{kl}$ is an obstruction in $\mathrm{o}(i,k)$. Let $m' = m - c_{ij}\mathrm{LC}_\sigma(g_i)\mathrm{o}_{i,k}(w_{ij}, w'_{ij}; w_{kl}, w'_{il})$. Then we have $|\mathrm{Supp}(m')| \le |\mathrm{Supp}(m)| - 1$. We conclude the proof by induction on $|\mathrm{Supp}(m)|$. □

Remark 3.4.9. In commutative polynomial rings, $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ is finitely generated by the critical syzygies (see [43], Theorem 2.3.7). We can compute a system of generators of $\mathrm{Syz}(\mathcal{G})$ by *lifting* a system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(G))$ (see [43], Proposition 3.1.4). However, the issue is quite different in free monoid rings. In [54], II.3, T. Mora stated that one cannot hope for the existence of a finite basis of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, due to the fact that $\langle \cup_{1\le i\le j\le s}\mathrm{o}(i,j)\rangle$ cannot be finitely generated. For instance, consider Example 3.4.2 again. We have $\mathrm{LM}_\sigma(\mathcal{G}) = (2x^2, xy)$ and

$$\begin{aligned}
\mathrm{o}(1,1) &= \{x\epsilon_1 - \epsilon_1 x, \epsilon_1 x - x\epsilon_1\} \cup \{x^2 w\epsilon_1 - \epsilon_1 w x^2, \epsilon_1 w x^2 - x^2 w\epsilon_1 \mid w \in \langle X\rangle\},\\
\mathrm{o}(1,2) &= \{\frac{1}{2}\epsilon_1 y - x\epsilon_2\} \cup \{\frac{1}{2}xyw\epsilon_2 - \epsilon_2 w x^2, \frac{1}{2}\epsilon_1 wxy - x^2 w\epsilon_2 \mid w \in \langle X\rangle\},\\
\mathrm{o}(2,2) &= \{xyw\epsilon_2 - \epsilon_2 wxy, \epsilon_2 wxy - xyw\epsilon_2 \mid w \in \langle X\rangle\}.
\end{aligned}$$

One can verify that for all $k \in \mathbb{N} \setminus \{0\}$ the obstruction $\epsilon_2 y^k xy - xy^{k+1}\epsilon_2$ cannot be generated by $\cup_{1\le i\le j\le 2}\mathrm{o}(i,j) \setminus \{\epsilon_2 y^k xy - xy^{k+1}\epsilon_2\}$. Therefore the method for computing a system of generators of $\mathrm{Syz}(\mathcal{G})$ by lifting is infeasible in free monoid rings. In [8], H. Bluhm and M. Kreuzer proposed a direct and straightforward approach, which we will discuss in Section 6.2, to compute a system of generators of $\mathrm{Syz}(\mathcal{G})$. Even though it does not apply to compute a system of generators of $\mathrm{Syz}(\mathcal{G})$, the lifting still can characterize Gröbner bases in free monoid rings successfully.

Definition 3.4.10. We say an element $\bar{m} \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))\setminus\{0\}$ has a **lifting** in $\mathrm{Syz}(\mathcal{G})$ if there is an element $m \in \mathrm{Syz}(\mathcal{G})$ such that $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \bar{m}$.

Finally, we have the following proposition from which we will obtain a Buchberger Criterion in Section 4.1.

Proposition 3.4.11. *Let $G \subseteq K\langle X\rangle\setminus\{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$. Moreover, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. The following conditions are equivalent.*

a) The set G is a σ-Gröbner basis of I.

b) Every obstruction in $\cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ has a lifting in $\mathrm{Syz}(\mathcal{G})$.

Proof. We prove condition a) implies condition b). Let $m \in \cup_{1\le i\le j\le s}\mathrm{o}(i,j)$. By Definition 3.4.7 we have $\Lambda(m) = 0$ and $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = m$. If $\lambda(m) = 0$, then m is a lifting of itself. Now assume that $\lambda(m) \neq 0$. By condition a) and Proposition 3.3.6, $\lambda(m)$ has a representation $\lambda(m) = \sum_{k=1}^{\mu} c_k w_k g_{i_k} w'_k$ with $c_k \in K\setminus\{0\}, w_k, w'_k \in \langle X\rangle$, and $g_{i_k} \in G$ such that $\mathrm{LT}_\sigma(\lambda(m)) \geq_\sigma \mathrm{LT}_\sigma(w_k g_{i_k} w'_k)$ for all $k \in \{1,\ldots,\mu\}$. Let $h = \sum_{k=1}^{\mu} c_j w_k \epsilon_{i_k} w'_k \in F_s$. We have $m-h \in \mathrm{Syz}(\mathcal{G})$ and $\mathrm{LT}_\sigma(\lambda(m)) = \mathrm{LT}_\sigma(\lambda(h)) = \deg_{\sigma,\mathcal{G}}(h)$. From $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = m \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ and Lemma 3.4.5, it follows that $\deg_{\sigma,\mathcal{G}}(m) >_\sigma \mathrm{LT}_\sigma(\lambda(m))$. Thus $\deg_{\sigma,\mathcal{G}}(m) >_\sigma \deg_{\sigma,\mathcal{G}}(h)$ and $\mathrm{LF}_{\sigma,\mathcal{G}}(m-h) = \mathrm{LF}_{\sigma,\mathcal{G}}(m)$ $= m$. We conclude that $m-h$ is a lifting of m in $\mathrm{Syz}(\mathcal{G})$.

We prove condition a) follows from condition b). Let $f \in I$. Then f has a representation $f = \sum_{k=1}^{\mu} c_k w_k g_{i_k} w'_k$ with $c_k \in K\setminus\{0\}, w_k, w'_k \in \langle X\rangle$, and $g_{i_k} \in G$ for all $k \in \{1,\ldots,\mu\}$. Since σ is a well-ordering, there exists one among all representations of f having minimal $\max_\sigma\{\mathrm{LT}_\sigma(w_k g_{i_k} w'_k) \mid k \in \{1,\ldots,\mu\}\}$. Suppose that $\max_\sigma\{\mathrm{LT}_\sigma(w_k g_{i_k} w'_k) \mid k \in \{1,\ldots,\mu\}\} >_\sigma \mathrm{LT}_\sigma(f)$. Let $m = \sum_{k=1}^{\mu} c_k w_k \epsilon_{i_k} w'_k \in F_s$ such that $\lambda(m) = f$ with minimal σ-degree. By assumption, we have $\deg_{\sigma,\mathcal{G}}(m) >_\sigma \mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(\lambda(m))$. By Lemma 3.4.5 we have $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Moreover, by Lemma 3.4.8.b $\cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ is a homogeneous system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Thus there exist $a_1,\ldots,a_\nu \in K\setminus\{0\}, \bar{w}_1,\ldots,\bar{w}'_\nu \in \langle X\rangle$, and $\bar{m}_1,\ldots,\bar{m}_\nu \in$

$\cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ such that $\mathrm{LF}_{\sigma,\mathcal{G}}(m)=\sum_{l=1}^{\nu}a_l\bar{w}_l\bar{m}_l\bar{w}_l'$. By condition b), we assume that $m_l\in\mathrm{Syz}(\mathcal{G})$ is a lifting of $\bar{m}_l$, i.e. $\mathrm{LF}_{\sigma,\mathcal{G}}(m_l)=\bar{m}_l$ for all $l\in\{1,\dots,\nu\}$. We conclude that $\mathrm{LF}_{\sigma,\mathcal{G}}(m)=\sum_{l=1}^{\nu}a_l\bar{w}_l\mathrm{LF}_{\sigma,\mathcal{G}}(m)_l\bar{w}_l'=\mathrm{LF}_{\sigma,\mathcal{G}}(\sum_{l=1}^{\nu}a_l\bar{w}_lm_l\bar{w}_l')$. Thus $\deg_{\sigma,\mathcal{G}}(m-\sum_{l=1}^{\nu}a_l\bar{w}_lm_l\bar{w}_l')<_\sigma\deg_{\sigma,\mathcal{G}}(m)$ and $\lambda(m-\sum_{l=1}^{\nu}a_l\bar{w}_lm_l\bar{w}_l')=\lambda(m)$, contradicting the minimality of the σ-degree of m. Therefore we must have $\mathrm{LT}_\sigma(f)\ge_\sigma\max_\sigma\{\mathrm{LT}_\sigma(w_kg_{i_k}w_k')\mid k\in\{1,\dots,\mu\}\}$. Hence G is a σ-Gröbner basis of I by Proposition 3.3.6.b. □

Observe that Proposition 3.4.11 also holds if G is an infinite set. To prove the proposition in this case, we first index the elements of G by an ordered set and then proceed exactly the same as the proof of Proposition 3.4.11.

3.5 Gröbner Bases of Right Ideals

In this section we shall investigate Gröbner bases of one-sided ideals in free monoid rings briefly. We only consider right ideals, since the situation of left ideals is completely symmetric and all theorems about right ideals also hold, *mutatis mutandis*, for left ideals. In this section we revise the main ingredients of Gröbner basis theory we have obtained so far in the setting of right ideals. We shall begin with two main ingredients, namely right-admissible orderings and the Right Division Algorithm.

A *right-admissible ordering* σ on $\langle X\rangle$ is defined almost the same as in Definition 3.1.1, except that it has to be compatible with right multiplication, i.e. $w_1>_\sigma w_2$ implies $w_1w_3>_\sigma w_2w_3$ for all $w_1,w_2,w_3\in\langle X\rangle$. Note that (left-to-right) Lex is compatible with right multiplication. Since we are only taking into concern the right multiplication, we introduce the following Right Division Algorithm.

Theorem 3.5.1. (The Right Division Algorithm) *let σ be a right-admissible ordering on $\langle X\rangle$, let $s\ge 1$, and let $f,g_1,\dots,g_s\in K\langle X\rangle\setminus\{0\}$. Consider the following sequence of instructions.*

1) *Let $q_1=\cdots=q_s=0,p=0$, and $v=f$.*

2) *Find the smallest $i\in\{1,\dots,s\}$ such that $\mathrm{LT}_\sigma(v)=\mathrm{LT}_\sigma(g_i)w$ for some $w\in\langle X\rangle$. If such an i exists, replace q_i by $q_i+\frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_i)}w$ and v by $v-\frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_i)}g_iw$.*

3) *Repeat step 2) until there is no more $i\in\{1,\dots,s\}$ such that $\mathrm{LT}_\sigma(g_i)$ is a prefix of $\mathrm{LT}_\sigma(v)$. If now $v\ne 0$, then replace p by $p+\mathrm{LM}_\sigma(v)$ and v by $v-\mathrm{LM}_\sigma(v)$, continue with step 2). Otherwise, return the tuple $(q_1,\cdots,q_s,p)$.*

This is an algorithm which returns the tuple $(q_1, \cdots, q_s, p)$ *such that*

$$f = \sum_{i=1}^{s} g_i q_i + p$$

and such that the following conditions are satisfied.

a) No element of $\mathrm{Supp}(p)$ *is contained in* $\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle_\varrho$.

b) If $q_i \neq 0$ *for some* $i \in \{1, \ldots, s\}$, *we have* $\mathrm{LT}_\sigma(g_i q_i) \leq_\sigma \mathrm{LT}_\sigma(f)$. *If* $p \neq 0$, *we have* $\mathrm{LT}_\sigma(p) \leq_\sigma \mathrm{LT}_\sigma(f)$.

Moreover, the tuple $(q_1, \cdots, q_s, p)$ *satisfying the above condition is uniquely determined by the tuple* $(f, g_1, \ldots, g_s)$.

Let $s \geq 1$, let $f, g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$. Then the polynomial $p \in K\langle X\rangle$ obtained in Theorem 3.5.1 is called the **right normal remainder** of f with respect to $\mathcal{G}$ and is denoted by $\mathrm{RNR}_{\sigma,\mathcal{G}}(f)$.

In the spirit of Definition 3.3.1 we define Gröbner bases of right ideals as follows.

Definition 3.5.2. A set $G \subseteq K\langle X\rangle\setminus\{0\}$ of polynomials is called a **(right)** σ**-Gröbner basis** of a right ideal $I_\varrho \subseteq K\langle X\rangle \setminus \{0\}$ if G generates I_ϱ and

$$\mathrm{LT}_\sigma\{I_\varrho\} = \{\mathrm{LT}_\sigma(g)w \mid g \in G, w \in \langle X\rangle\}.$$

Remark 3.5.3. One can show that for every polynomial $g \in K\langle X\rangle \setminus \{0\}$ the set $\{g\}$ is a σ-Gröbner basis of the right ideal $\langle g\rangle_\varrho$ as follows (compare with Example 3.3.2). Each element $f \in \langle g\rangle_\varrho \setminus \{0\}$ has a representation $f = gp$ where $p \in K\langle X\rangle \setminus \{0\}$. By Remark 3.1.13.c we have $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(g)\mathrm{LT}_\sigma(p)$. Thus $\{g\}$ is a right σ-Gröbner basis of $\langle g\rangle_\varrho$. This fact indicates that Gröbner bases of right ideals could be simpler than Gröbner bases of two-sided ideals. Indeed in Section 4.4 we will show that every finitely generated right ideal has a finite right Gröbner basis.

Gröbner bases of right ideals can be also characterized, *mutatis mutandis*, by leading term sets and leading term ideals (see Propositions 3.3.3 and 3.3.4), Gröbner representations (see Proposition 3.3.6), and syzygy modules. Since we will obtain a Buchberger Criterion for right ideals from syzygy modules, we shall spend a few words on them.

Let $s \geq 1$, and let $(K\langle X\rangle)^s$ be the right $K\langle X\rangle$-module of rank s with the canonical basis $\{\eta_1, \ldots, \eta_s\}$, i.e. $\eta_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ whose the i^{th} element is 1 and all of whose other elements are 0. Note that $(K\langle X\rangle)^s$ is not a free $K\langle X\rangle$-bimodule since the universal property (see Proposition 2.3.8) does not hold. We write an element $m \in (K\langle X\rangle)^s$ as $m = \sum_{i=1}^s \eta_i p_i$ with $p_i \in K\langle X\rangle$. Once again, we let $g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$, $\mathcal{G}$ the tuple $(g_1, \ldots, g_s)$, and $\mathrm{LM}_\sigma(\mathcal{G})$ the tuple $(\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))$.

Definition 3.5.4. Using the notation above, we define right syzygy and right syzygy module as follows.

a) A **right syzygy** of $\mathcal{G}$ is an element $\sum_{i=1}^s \eta_i p_i \in (K\langle X\rangle)^s$ such that $\sum_{i=1}^s g_i p_i = 0$.

b) Let $\mathrm{Syz}(\mathcal{G})_\varrho$ be the set of all right syzygies of $\mathcal{G}$. One can verify that $\mathrm{Syz}(\mathcal{G})_\varrho$ is a right $K\langle X\rangle$-module. We call $\mathrm{Syz}(\mathcal{G})_\varrho$ the **right syzygy module** of $\mathcal{G}$.

Similarly, a right syzygy of $\mathrm{LM}_\sigma(\mathcal{G})$ is an element $\sum_{i=1}^s \eta_i p_i \in (K\langle X\rangle)^s$ such that $\sum_{i=1}^s \mathrm{LM}_\sigma(g_i) p_i = 0$; the set of all right syzygies of $\mathrm{LM}_\sigma(\mathcal{G})$ forms a right $K\langle X\rangle$-module and is denoted by $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))_\varrho$.

Definition 3.5.5. Let $i, j \in \{1, \ldots, s\}$ and $i < j$. If there exists some $w \in \langle X\rangle$ such that $\mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(g_j)w$ or $\mathrm{LT}_\sigma(g_i)w = \mathrm{LT}_\sigma(g_j)$, then a **right obstruction** of g_i and g_j, denoted by $\mathrm{ro}_{i,j}$, is $\frac{1}{\mathrm{LC}_\sigma(g_i)}\eta_i - \frac{1}{\mathrm{LC}_\sigma(g_j)}\eta_j w$ or $\frac{1}{\mathrm{LC}_\sigma(g_i)}\eta_i w - \frac{1}{\mathrm{LC}_\sigma(g_j)}\eta_j$, respectively. Let O_ϱ be the **set of all right obstructions** of $\mathcal{G}$.

In contrast to two-sided syzygies, for each pair $i, j \in \{1, \ldots, s\}$ there exists none or only one right obstruction of g_i and g_j and there is no self right obstruction. Therefore we have

$$\mathrm{O}_\varrho = \{\mathrm{ro}_{i,j} \in (K\langle X\rangle)^s \mid 1 \le i < j \le s,\ g_i \text{ and } g_j \text{ have a right obstruction}\}.$$

Clearly we have $|\mathrm{O}_\varrho| < \infty$. Moreover, the following lemma holds.

Lemma 3.5.6. *The right syzygy module* $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))_\varrho$ *is finitely generated by* O_ϱ*.*

Proof. The proof that $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))_\varrho$ is generated by O_ϱ is proceeded analogously to the proof of Lemma 3.4.8.b. The finiteness follows from the fact that $\mathrm{O}_\varrho < \infty$. □

The following proposition is the counterpart of Proposition 3.4.11.

Proposition 3.5.7. *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates a right ideal $I_\varrho = \langle G\rangle_\varrho$. Moreover, let $\mathcal{G}$ be an associated tuple of G, and let O_ϱ be the set of all right obstructions of $\mathcal{G}$. Then G is a right σ-Gröbner basis of I_ϱ if and only if every right obstruction in O_ϱ has a lifting in* $\mathrm{Syz}(\mathcal{G})_\varrho$*.*

Proof. Analogous to Proposition 3.4.11. □

Chapter 4

Gröbner Basis Computations in $K\langle X\rangle$

In the last chapter we have taken the first step toward studying Gröbner basis theory in free monoid rings. In the process we investigated many nice properties of Gröbner bases. In this chapter we shall explore techniques for Gröbner basis computations in free monoid rings. It is known that computing Gröbner bases is not an easy task in both the commutative and the non-commutative cases. In the non-commutative case it bears the extra difficulty that Gröbner bases, even reduced Gröbner bases, may be infinite. Since Gröbner basis computations are at the heart of many applications of Gröbner bases, efficient algorithms for computing Gröbner bases are of considerable practical interest. In the literature of computational commutative algebra, Gröbner basis computations are based on either the classical Buchberger Algorithm [11] or J.-C. Faugère's F4 Algorithm [26]. In this chapter we shall study a generalization of Buchberger's Algorithm in free monoid rings. In Chapter 5 we will generalize the F4 Algorithm to free bimodules over free monoid rings.

With the intention of improving the procedures for computing Gröbner bases in free monoid rings, in Section 4.1 we shall obtain a Buchberger Criterion from a set of obstructions and formulate a Buchberger Procedure to enumerate Gröbner bases. First, we obtain prototypes of Buchberger's Criterion (see Corollary 4.1.3) and Buchberger's Procedure (see Theorem 4.1.4). Then we investigate the set of obstructions more carefully and get rid of a large number of trivial obstructions (see Lemmas 4.1.6 and 4.1.10). We obtain a finite set of non-trivial obstructions for every finite system of generators (see Definition 4.1.11 and Lemma 4.1.12). Finally, we get practical versions of Buchberger's Criterion (see Proposition 4.1.13) and Buchberger's Procedure (see Theorem 4.1.14).

In commutative settings improvements of the classical Buchberger Algorithm have been well-studied mainly for two approaches, which are to detect unnecessary critical pairs (see [12, 13, 17, 33, 43, 44]) and to play with strategies (see [4, 28, 34]). However, little is known about the improvements of Gröbner basis computations in the non-commutative case. In Section 4.2 we shall be mostly concerned with improving the Buchberger Procedure by detecting unnecessary obstructions. We investigate the set of obstructions closely and propose two methods to detect unnecessary obstructions: by interreducing on non-trivial obstructions (see Theorems 4.2.12) and by generalizing the Gebauer-Möller Installation (see [33]) to free monoid rings (see Propositions 4.2.15, 4.2.17 and 4.2.18). Then we improve the Buchberger Procedure accordingly (see Theorem 4.2.12). We also study redundant generators and improve the Buchberger Procedure by deleting redundant generators (see Theorem 4.2.24).

Since the Buchberger Procedure behaves very well for a homogenous system of generators, in Section 4.3 we shall study homogenization and dehomogenization techniques and explore the connections between $\mathbb{N}$-graded and non-graded ideals. First we define homogenization and dehomogenization for polynomials (see Definition 4.3.1) and ideals (see Definition 4.3.3) and study related properties (see Lemmas 4.3.2, 4.3.4 and 4.3.7). Then we present connections between $\mathbb{N}$-graded and non-graded ideals through Gröbner bases (see Propositions 4.3.10 and 4.3.13). We describe a homogeneous version of the Buchberger Procedure to enumerate Gröbner bases of ideals that are generated by homogeneous systems of generators (see Theorems 4.3.16 and 4.3.21).

In Section 4.4 we shall briefly study Gröbner basis computations for right ideals. Since every finitely generated right ideal has a finite Gröbner basis, we present two algorithms for computing Gröbner bases of right ideals (see Theorem 4.4.3 and Proposition 4.4.4).

Throughout this chapter, we let K be a field, $X = \{x_1, \ldots, x_n\}$ a finite alphabet (or set of indeterminates), $K\langle X\rangle$ the free monoid ring generated by X over K, $\langle X\rangle$ the free monoid generated by X, and σ an admissible ordering on $\langle X\rangle$. Moreover, for $s \geq 1$, we let $F_s = (K\langle X\rangle \otimes K\langle X\rangle)^s$ be the free $K\langle X\rangle$-bimodule of rank s with canonical basis $\{\epsilon_1, \ldots, \epsilon_s\}$, where $\epsilon_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$ with $1 \otimes 1$ occurring in the i^{th} position for $i = 1, \ldots, s$, and we let $\mathbb{T}(F_s)$ be the set of terms in F_s, i.e. $\mathbb{T}(F_s) = \{w\epsilon_i w' \mid i \in \{1, \ldots, s\}, w, w' \in \langle X\rangle\}$. By an ideal $I \subseteq K\langle X\rangle$ we mean a two-sided ideal unless specified otherwise.

4.1 The Buchberger Procedure

Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Recall that $\cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ is the set of all obstructions of $\mathcal{G}$ (see Definition 3.4.7). By Proposition 3.4.11 the set G is a σ-Gröbner basis of I if and only if every obstruction in $\cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ has a lifting in $\mathrm{Syz}(\mathcal{G})$. In this section, we shall obtain a Buchberger Criterion from Proposition 3.4.11 and construct a Buchberger Procedure for enumerating Gröbner bases of finitely generated ideals. We start by defining S-polynomials of obstructions.

Definition 4.1.1. Let $i,j \in \{1,\dots,s\}$ such that $i \le j$, and let $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j') \in \mathrm{o}(i,j)$ be an obstruction of g_i and g_j. We call the polynomial

$$S_{i,j}(w_i,w_i';w_j,w_j') = \frac{1}{\mathrm{LC}_\sigma(g_i)}w_ig_iw_i' - \frac{1}{\mathrm{LC}_\sigma(g_j)}w_jg_jw_j' \in K\langle X\rangle$$

the **S-polynomial** of $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')$.

The following proposition shows that we can check whether an obstruction has a lifting using its S-polynomial and a representation of its S-polynomial.

Proposition 4.1.2. *Let $G \subseteq K\langle X\rangle\setminus\{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Then the following conditions are equivalent.*

a) The set G is a σ-Gröbner basis of I.

b) The S-polynomial of every obstruction $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j') \in \cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ has a representation

$$S_{i,j}(w_i,w_i';w_j,w_j') = \sum_{k=1}^{\mu} c_kw_kg_{i_k}w_k'$$

with $c_k \in K, w_k, w_k' \in \langle X\rangle$, and $g_{i_k} \in G$ for all $k \in \{1,\dots,\mu\}$ such that $\mathrm{LT}_\sigma(w_kg_{i_k}w_k') \le_\sigma \mathrm{LT}_\sigma(S_{i,j}(w_i,w_i';w_j,w_j'))$ if $c_k \ne 0$ for some $k \in \{1,\dots,\mu\}$.

c) The S-polynomial of every obstruction $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j') \in \cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ has a representation

$$S_{i,j}(w_i,w_i';w_j,w_j') = \sum_{k=1}^{\mu} c_kw_kg_{i_k}w_k'$$

with $c_k \in K, w_k, w'_k \in \langle X\rangle$, *and* $g_{i_k} \in G$ *for all* $k \in \{1,\ldots,\mu\}$ *such that* $\mathrm{LT}_\sigma(w_k g_{i_k} w'_k) <_\sigma \mathrm{LT}_\sigma(w_i g_i w'_i)$ *if* $c_k \neq 0$ *for some* $k \in \{1,\ldots,\mu\}$.

Proof. From the fact $S_{i,j}(w_i, w'_i; w_j, w'_j) \in I$ and Proposition 3.3.6, it follows that condition a) implies condition b). By Definitions 3.3.7 and 4.1.1 we have $\mathrm{LT}_\sigma(wg_iw'_i) >_\sigma \mathrm{LT}_\sigma(S_{i,j}(w_i, w'_i; w_j, w'_j))$. Then condition c) immediately follows from condition b).

To prove that condition c) implies condition a), it suffices, by Proposition 3.4.11, to prove that every obstruction $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1\leq i\leq j\leq s}\mathrm{o}(i,j)$ has a lifting in $\mathrm{Syz}(\mathcal{G})$. If $S_{i,j}(w_i, w'_i; w_j, w'_j) = 0$, then $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$ is a lifting of itself. Now assume that $S_{i,j}(w_i, w'_i; w_j, w'_j) \neq 0$. Let $S_{i,j}(w_i, w'_i; w_j, w'_j) = \sum_{k=1}^{\mu} c_k w_k g_{i_k} w'_k$ be a representation of $S_{i,j}(w_i, w'_i; w_j, w'_j)$ as in condition c). Let $m = \mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) - \sum_{k=1}^{\mu} c_k w_k \epsilon_{i_k} w'_k$. Clearly $m \in F_s$. Then we have $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$ and $m \in \mathrm{Syz}(\mathcal{G})$. Hence m is a lifting of $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$. □

The representations of $S_{i,j}(w_i, w'_i; w_j, w'_j)$ as in conditions 4.1.2.b and 4.1.2.c are called **weak Gröbner representations** of $S_{i,j}(w_i, w'_i; w_j, w'_j)$ in terms of G by A. Cohen [21] and T. Mora [55], respectively. Note that the notion of a weak Gröbner representation as in condition 4.1.2.b coincides with the notion of a Gröbner representation introduced in Definition 3.3.7. Intuitively, weak Gröbner representations can be computed by the Division Algorithm.

Corollary 4.1.3. (Prototype of Buchberger's Criterion) *Let* $G \subseteq K\langle X\rangle \setminus \{0\}$ *be a finite set of polynomials which generates an ideal* $I = \langle G\rangle$, *let* $\mathcal{G}$ *be an associated tuple of* G, *and let* $s = |\mathcal{G}|$. *Then the following conditions are equivalent.*

a) The set G *is a* σ*-Gröbner basis of* I.

b) For every obstruction $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1\leq i\leq j\leq s}\mathrm{o}(i,j)$, *we have*

$$\mathrm{NR}_{\sigma,\mathcal{G}}(S_{i,j}(w_i, w'_i; w_j, w'_j)) = 0.$$

Proof. From the fact $S_{i,j}(w_i, w'_i; w_j, w'_j) \in I$, Remark 3.1.18.c and Proposition 3.3.10, it follows that condition a) implies condition b). Conversely, by Theorem 3.2.1 and Proposition 4.1.2 we have condition b) implies condition a). □

Just as Proposition 3.4.11, one can verify that Proposition 4.1.2 and Corollary 4.1.3 also hold if G is an infinite set. With Buchberger's Criterion above, we construct Buchberger's Procedure in free monoid rings, which is virtually identical to Buchberger's Algorithm in the commutative case. Buchberger's Procedure can be roughly described as follows. Given a system of generators, we construct obstructions for each pair of generators. For each obstruction we compute the normal remainder of its S-polynomial, and add non-zero normal remainder to the system of generators and construct new obstructions. At termination of the procedure, all the S-polynomials of obstructions have the zero normal remainder and the system of generators forms a Gröbner basis. More precisely we have the following prototype of Buchberger's Procedure. Note that in the following procedure as well as in procedures henceforth, by a **fair strategy** we mean a selection strategy which ensures every obstruction is eventually selected.

Theorem 4.1.4. (Prototype of Buchberger's Procedure) *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Consider the following sequence of instructions.*

1) *Let $s' = s$ and $B = \cup_{1\leq i\leq j\leq s'}\mathrm{o}(i,j)$.*

2) *If $B = \emptyset$, return the result $\mathcal{G}$. Otherwise, select an obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ $\in B$ using a fair strategy and delete it from B.*

3) *Compute the S-polynomial $S = S_{i,j}(w_i, w_i'; w_j, w_j')$ and its normal remainder $S' = \mathrm{NR}_{\sigma,\mathcal{G}}(S)$. If $S' = 0$, continue with step 2).*

4) *Increase s' by one, append $g_{s'} = S'$ to the tuple $\mathcal{G}$, and append the set of obstructions $\cup_{1\leq i\leq s'}\mathrm{o}(i,s')$ to the set B. Then continue with step 2).*

This is a procedure that enumerates a σ-Gröbner basis $\mathcal{G}$ of I.

Proof. To prove correctness, it suffices, by Corollary 4.1.3, to show that for every obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq s'}\mathrm{o}(i,j)$ the normal remainder of $S_{i,j}(w_i, w_i'; w_j, w_j')$ with respect to $\mathcal{G}$ is zero. If in step 3) $S' = 0$, then we are done. Otherwise, we ensure that the normal remainder of S with respect to $\mathcal{G}$ is zero by appending $S' = \mathrm{NR}_{\sigma,\mathcal{G}}(S)$ to $\mathcal{G}$ in step 4). □

In the literature of computational non-commutative algebra, this procedure for enumerating Gröbner bases is often called **Mora's Algorithm** since it was introduced by F. Mora [53].

Remark 4.1.5. Let us make some remarks on the preceding procedure.

a) Different selection strategies applied in step 2) can affect the behaviour and efficiency of the procedure remarkably (see [10, 34]). The *normal selection strategy*, which selects the obstruction with the minimal σ-degree, is the default selection strategy in the ApCoCoA package *gbmr*. We also use the normal selection strategy in examples henceforth in this thesis.

b) Unfortunately, even if the best selection strategy is applied, we can not guarantee the termination of Buchberger's Procedure due to the fact that Dickson's lemma, which ensures the termination of Buchberger's Algorithm in the commutative case, does not hold in free monoid rings (see Remark 2.1.25.b).

c) Besides the failure of Dickson's lemma in free monoid rings, there is still one crucial problem with the prototype of Buchberger's Procedure: there may exist infinitely many obstructions. For all $1 \leq i \leq j \leq s$, according to Definition 3.4.7, there are infinitely many obstructions in $\mathrm{o}(i,j)$ caused by the following two sources.

   c.1) If $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{o}(i,j)$, then $\mathrm{o}_{i,j}(ww_i, w_i'w'; ww_j, w_j'w') \in \mathrm{o}(i,j)$ for all $w, w' \in \langle X\rangle$.

   c.2) We have $\mathrm{o}_{i,j}(\mathrm{LT}_\sigma(g_j)w, 1; 1, w\mathrm{LT}_\sigma(g_i)), \mathrm{o}_{i,j}(1, w\mathrm{LT}_\sigma(g_j); \mathrm{LT}_\sigma(g_i)w, 1) \in \mathrm{o}(i,j)$ for all $w \in \langle X\rangle$.

   We should carefully handle this problem in order to extract a practical procedure from the prototype of Buchberger's Procedure.

Now we shall take care of the sources of infinitely many obstructions mentioned in Remark 4.1.5.c. The following lemma handles case c.1) of Remark 4.1.5.

Lemma 4.1.6. *If the S-polynomial of* $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{o}(i,j)$ *has a weak Gröbner representation in terms of* G*, then so does the S-polynomial of* $\mathrm{o}_{i,j}(ww_i, w_i'w'; ww_j, w_j'w')$ *for all* $w, w' \in \langle X\rangle$.

Proof. By assumption, we write $S_{i,j}(w_i, w_i'; w_j, w_j') = \sum_{k=1}^{\mu} c_k w_k g_{i_k} w_k'$ with $c_k \in K$, $w_k, w_k' \in \langle X\rangle, g_{i_k} \in G$ such that $w_i\mathrm{LT}_\sigma(g_i)w_i' >_\sigma w_k\mathrm{LT}_\sigma(g_{i_k})w_k'$ for all $k \in \{1,\ldots,\mu\}$. For any $w, w' \in \langle X\rangle$ we have $S_{i,j}(ww_i, w_i'w'; ww_j, w_j'w') = \sum_{k=1}^{\mu} c_k ww_k g_{i_k} w_k'w'$ using Definition 4.1.1. Since σ is compatible with multiplication, we have $ww_i\mathrm{LT}_\sigma(g_i)w_i'w' >_\sigma ww_k\mathrm{LT}_\sigma(g_{i_k})w_k'w'$ for all $k \in \{1,\ldots,\mu\}$. Thus $S_{i,j}(ww_i, w_i'w'; ww_j, w_j'w')$ has a weak Gröbner representation in terms of G. □

For the purposes of computing Gröbner bases, by Proposition 4.1.2 and Lemma

4.1.6, we only need to consider in $\mathrm{o}(i,j)$ the obstructions of the forms

$$\mathrm{o}_{i,j}(w_i,1;1,w'_j),\ \mathrm{o}_{i,j}(1,w'_i;w_j,1),\ \mathrm{o}_{i,j}(w_i,w'_i;1,1),\ \mathrm{o}_{i,j}(1,1;w_j,w'_j)$$

with $w_i,w'_i,w_j,w'_j \in \langle X\rangle$. Observe that $\mathrm{o}_{i,i}(1,1;w_i,w'_i) \in \mathrm{o}(i,i)$ implies $w_i = w'_i = 1$. Clearly $\mathrm{o}_{i,i}(1,1;1,1) = 0$. Moreover, $S_{i,i}(w_i,1;1,w'_i) = -S_{i,i}(1,w'_i;w_i,1)$. Thus we only need to consider in $\mathrm{o}(i,i)$ the self obstructions of the form

$$\mathrm{o}_{i,i}(1,w'_i;w_i,1)$$

with $w_i,w'_i \in \langle X\rangle \setminus \{1\}$.

To get rid of case c.2) of Remark 4.1.5, the following definition proves useful.

Definition 4.1.7. Let $w_1,w_2 \in \langle X\rangle$. If there exist $w,w',w'' \in \langle X\rangle$ and $w \neq 1$ such that $w_1 = w'w$ and $w_2 = ww''$, or $w_1 = ww'$ and $w_2 = w''w$, or $w_1 = w$ and $w_2 = w'ww''$, or $w_1 = w'ww''$ and $w_2 = w$, then we say w_1 and w_2 have an **overlap** at w. Otherwise, we say w_1 and w_2 have **no overlap**.

Let $\mathrm{o}_{i,j}(w_i,w'_i;w_j,w'_j) \in \mathrm{o}(i,j)$ be an obstruction. If $\mathrm{LT}_\sigma(g_i)$ and $\mathrm{LT}_\sigma(g_j)$ have an overlap at $w \in \langle X\rangle \setminus \{1\}$ and if w is a subword of $w_i\mathrm{LT}_\sigma(g_i)w'_i$, then we say $\mathrm{o}_{i,j}(w_i,w'_i;w_j,w'_j)$ has an **overlap** at w. Otherwise, we say $\mathrm{o}_{i,j}(w_i,w'_i;w_j,w'_j)$ has **no overlap**.

Case c.2) of Remark 4.1.5 shows that there are infinitely many obstructions without overlaps in each $\mathrm{o}(i,j)$. The following example is inspired by [21], Lemma 1.3.

Example 4.1.8. Consider the free monoid ring $\mathbb{F}_2\langle x,y,u,v,t,s\rangle$ equipped with the admissible ordering $\sigma = \texttt{LLex}$ such that $x >_\sigma y >_\sigma u >_\sigma v >_\sigma t >_\sigma s$. Let $I \subseteq \mathbb{F}_2\langle x,y,u,v,t,s\rangle$ be the ideal generated by the set $\{g_1,g_2\}$, where $g_1 = u(xy)^3+v(xy)^2+u+v$ and $g_2 = (yx)^3t+(yx)^2t+t+s$. We have $\mathrm{LT}_\sigma(g_1) = u(xy)^3$ and $\mathrm{LT}_\sigma(g_2) = (yx)^3t$. Let $\mathcal{G}$ be the tuple (g_1,g_2). It is easy to check that $\mathrm{o}(1,1)$ and $\mathrm{o}(2,2)$ contain only obstructions without overlaps, and

$$\begin{aligned}\mathrm{o}(1,2) &= \{\mathrm{o}_{1,2}(1,xt;ux,1),\mathrm{o}_{1,2}(1,xyxt;uxyx,1),\mathrm{o}_{1,2}(1,(xy)^2xt;u(xy)^2xt,1)\}\\ &\quad\cup\{\mathrm{o}_{1,2}(1,w(yx)^3t;u(xy)^3w,1)\mid w\in\langle X\rangle\}\\ &\quad\cup\{\mathrm{o}_{1,2}((yx)^3tw,1;1,wu(xy)^3)\mid w\in\langle X\rangle\}.\end{aligned}$$

We consider the following obstructions in $\mathrm{o}(1,2)$.

a) $\mathrm{o}_{1,2}(1,xt;ux,1)$ has an overlap at $(xy)^2x$.

$$\begin{aligned}S_{1,2}(1,xt;ux,1) &= uxs+vxt\\ \mathrm{NR}_{\sigma,\mathcal{G}}(S_{1,2}(1,xt;ux,1)) &= uxs+vxt\end{aligned}$$

We let $\mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = uxs + vxt$.

b) $\mathrm{o}_{1,2}(1, xyxt; uxyx, 1)$ has an overlap at xyx.

$$\begin{aligned} S_{1,2}(1, xyxt; uxyx, 1) &= uxyxs + vxyxt \\ \mathrm{NR}_{\sigma,\mathcal{G}}(S_{1,2}(1, xyxt; uxyx, 1)) &= uxyxs + vxyxt \end{aligned}$$

We let $\mathcal{G} = (g_1, g_2, g_3, g_4)$ with $g_4 = uxyxs + vxyxt$.

c) $\mathrm{o}_{1,2}(1, (xy)^2xt; u(xy)^2xt, 1)$ has an overlap at x.

$$\begin{aligned} S_{1,2}(1, (xy)^2xt; u(xy)^2xt, 1) &= u(xy)^2xs + v(xy)^2xt \\ \mathrm{NR}_{\sigma,\mathcal{G}}(S_{1,2}(1, (xy)^2xt; u(xy)^2xt, 1)) &= u(xy)^2xs + v(xy)^2xt \end{aligned}$$

We let $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ with $g_5 = u(xy)^2xs + v(xy)^2xt$.

d) $\mathrm{o}_{1,2}(1, (yx)^3t; u(xy)^3, 1)$ has no overlap and corresponds to case c.2) of Remark 4.1.5 with $w = 1$.

$$\begin{aligned} S_{1,2}(1, (yx)^3t; u(xy)^3, 1) &= u(xy)^3(yx)^2t + u(xy)^2(yx)^3t + u(xy)^3t \\ &\quad +u(xy)^3s + u(yx)^3t + v(yx)^3t \end{aligned}$$

By the Division Algorithm we get

$$S_{1,2}(1, (yx)^3t; u(xy)^3, 1) = g_1(yx)^2t + u(xy)^2g_2 + g_1t + ug_2 + g_1s + vg_2.$$

Thus $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{1,2}(1, (yx)^3t; u(xy)^3, 1)) = 0$.

e) $\mathrm{o}_{1,2}(1, x(yx)^3t; u(xy)^3x, 1)$ has no overlap and corresponds to case c.2) of Remark 4.1.5 with $w = x$.

$$S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1) = u(xy)^3xs + v(xy)^3xt$$

By the Division Algorithm we get

$$S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1) = g_1xs + uxg_2 + g_5 + g_3.$$

Thus $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1)) = 0$. Going the other way, we compute $S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1)$ as follows.

$$\begin{aligned} & S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1) \\ = \;& g_1x\mathrm{LT}_\sigma(g_2) + \mathrm{LT}_\sigma(g_1)xg_2 \\ = \;& g_1x(g_2 + ((yx)^2t + t + s)) + (g_1 + (u(xy)^2 + u + v))xg_2 \\ = \;& g_1x((yx)^2t + t + s) + ((u(xy)^2 + u + v))xg_2 \\ = \;& (g_1x(yx)^2t + u(xy)^2xg_2) + (g_1xt + uxg_2) + g_1xs + vxg_2 \end{aligned}$$

Observe that $g_1xt+uxg_2$ and $g_1x(yx)^2t+u(xy)^2xg_2$ are S-polynomials in a) and c), respectively, and that both obstructions in a) and b) have overlaps. Further, by a) we have $g_1xt+uxg_2 = g_3$ and $\mathrm{LT}_\sigma(g_3) = uxs <_\sigma u(xy)^3xs$, where $u(xy)^3xs$ is the leading term of $S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1)$, and by c) we have $g_1x(yx)^2t + u(xy)^2xg_2 = g_5$ and $\mathrm{LT}_\sigma(g_5) = u(xy)^2xs <_\sigma u(xy)^3xs$. Using substitution, we get again

$$S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1) = g_5 + g_3 + g_1xs + vxg_2$$

which is a weak Gröbner representation of $S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1)$ in terms of G in the sense of Proposition 4.1.2.b.

f) $\mathrm{o}_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1)$ has no overlap and corresponds to case c.2) of Remark 4.1.5 with $w = xyx$.

$$S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1) = u(xy)^4xs + v(xy)^4xt$$

By the Division Algorithm we get

$$S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1) = g_1xyxs + vxyxg_2 + g_1xs + vxg_2 + g_5 + g_4 + g_3.$$

Thus $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1)) = 0$. Going the other way, we compute $S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1)$ as follows.

$$\begin{aligned} & S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1) \\ = \;& g_1xyx\mathrm{LT}_\sigma(g_2) + \mathrm{LT}_\sigma(g_1)xyxg_2 \\ = \;& g_1xyx(g_2 + ((yx)^2t + t + s)) + (g_1 + (u(xy)^2 + u + v))xyxg_2 \\ = \;& g_1xyx((yx)^2t + t + s) + ((u(xy)^2 + u + v))xyxg_2 \\ = \;& (g_1xyx(yx)^2t + u(xy)^2xyxg_2) + (g_1xyxt + uxyxg_2) + g_1xyxs + vxyxg_2 \end{aligned}$$

Observe that $g_1xyxt + uxyxg_2$ and $g_1xyx(yx)^2t + u(xy)^2xyxg_2$ are S-polynomials in b) and e), respectively, and that the obstruction in c) has an overlap, and that $\deg_{\sigma,\mathcal{G}}(\mathrm{o}_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1)) >_\sigma \deg_{\sigma,\mathcal{G}}(\mathrm{o}_{1,2}(1, x(yx)^3t; u(xy)^3x, 1))$. Further, by b) we have $g_1xyxt + uxyxg_2 = g_4$ and $\mathrm{LT}_\sigma(g_4) = uxyxs <_\sigma u(xy)^4xs$, where $u(xy)^4xs$ is the leading term of $S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1)$, and by e) we have $g_1xyx(yx)^2t + u(xy)^2xyxg_2 = g_1xs + uxg_2 + g_5 + g_3$ and $\mathrm{LT}_\sigma(g_1xs + uxg_2 + g_5 + g_3) = u(xy)^3xs <_\sigma u(xy)^4xs$. By substitution we get again

$$S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1) = g_1xs + uxg_2 + g_5 + g_3 + g_4 + g_1xyxs + vxyxg_2$$

which is a weak Gröbner representation of $S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1)$ in terms of G in the sense of Proposition 4.1.2.b.

Remark 4.1.9. Let us make some observations about the preceding example.

a) Examples 4.1.8.d, 4.1.8.e, and 4.1.8.f show that the weak Gröbner representations of the S-polynomials of obstructions without overlaps depend on the weak Gröbner representations of the S-polynomials of obstructions with overlaps. Example 4.1.8.f also shows that larger σ-degree obstruction without overlap can be "reduced" to smaller σ-degree obstruction without overlap. A. Cohen proved in [21], Lemma 1.3 that if all the S-polynomials of obstructions with overlaps have weak Gröbner representations, then so do the S-polynomials of obstructions without overlaps. The proof was achieved by induction on the σ-degree of obstructions.

b) From another point of view, in Example 4.1.8.e we have $\mathrm{LT}_\sigma(g_1)x(yx)^3t$ larger than $\mathrm{LT}_\sigma(g_1)x(yx)^2$, $\mathrm{LT}_\sigma(g_1)xt$, $\mathrm{LT}_\sigma(g_1)xs$, $u(xy)^2x\mathrm{LT}_\sigma(g_2)$, $ux\mathrm{LT}_\sigma(g_2)$, and $vx\mathrm{LT}_\sigma(g_2)$. Thus $S_{1,2}(1, x(yx)^3t; u(xy)^3x, 1) = g_1x((yx)^2t + t + s) + ((u(xy)^2 + u + v))xg_2$ is a weak Gröbner representation in terms of $\{g_1, g_2\}$ in the sense of Proposition 4.1.2.c. Similarly, in Example 4.1.8.f we have $\mathrm{LT}_\sigma(g_1)xyx(yx)^3t$ larger than $\mathrm{LT}_\sigma(g_1)xyx(yx)^2t$, $\mathrm{LT}_\sigma(g_1)xyxt$, $\mathrm{LT}_\sigma(g_1)xyxs$, $u(xy)^2xyx\mathrm{LT}_\sigma(g_2)$, $uxyx\mathrm{LT}_\sigma(g_2)$, and $vxyx\mathrm{LT}_\sigma(g_2)$. Therefore $S_{1,2}(1, xyx(yx)^3t; u(xy)^3xyx, 1) = g_1xyx((yx)^2t + t + s) + ((u(xy)^2 + u + v))xyxg_2$ is a weak Gröbner representation in terms of $\{g_1, g_2\}$ in the sense of Proposition 4.1.2.c.

The following lemma is a generalization of the observations in Remark 4.1.9.

Lemma 4.1.10. *If $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{o}(i, j)$ has no overlap, then the S-polynomial $S_{i,j}(w_i, w_i'; w_j, w_j')$ has a weak Gröbner representation in terms of $\{g_i, g_j\}$.*

Proof. See [55], Lemma 5.4. □

By Proposition 4.1.2 and Lemma 4.1.10, for the purposes of computing Gröbner bases we can safely discard all obstructions without overlaps.

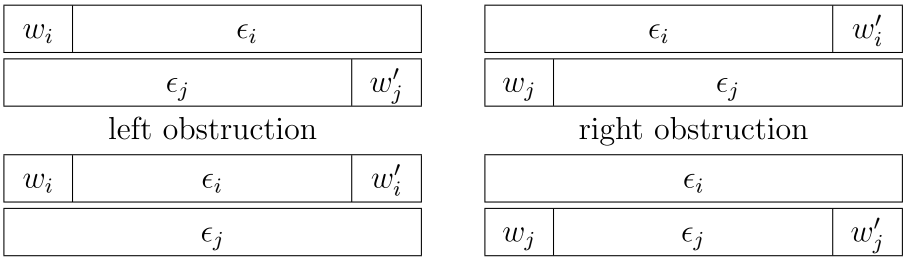
Definition 4.1.11. Let $s \geq 1$, let $g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple.

a) Let $i, j \in \{1, \ldots, s\}$ and $i < j$. An obstruction in $\mathrm{o}(i, j)$ is called **non-trivial** if it has an overlap and is of the form $\mathrm{o}_{i,j}(w_i, 1; 1, w_j')$, or $\mathrm{o}_{i,j}(1, w_i'; w_j, 1)$, or $\mathrm{o}_{i,j}(w_i, w_i'; 1, 1)$, or $\mathrm{o}_{i,j}(1, 1; w_j, w_j')$ with $w_i, w_i', w_j, w_j' \in \langle X\rangle$.

b) Let $i \in \{1, \dots, s\}$. A self obstruction in $\mathrm{o}(i,i)$ is called **non-trivial** if it has an overlap and is of the form $\mathrm{o}_{i,i}(1, w_i'; w_i, 1)$ with $w_i, w_i' \in \langle X \rangle \setminus \{1\}$.

c) Let $i, j \in \{1, \dots, s\}$ and $i \le j$. The **set of all non-trivial obstructions** of g_i and g_j is denoted by $\mathrm{O}(i,j)$.

In the literature, a non-trivial obstruction of the form $\mathrm{o}_{i,j}(w_i, 1; 1, w_j')$ is called a **left obstruction**, of the form $\mathrm{o}_{i,j}(1, w_i'; w_j, 1)$ is called a **right obstruction**, and of the form $\mathrm{o}_{i,j}(w_i, w_i'; 1, 1)$ or $\mathrm{o}_{i,j}(1, 1; w_j, w_j')$ is called a **center obstruction**. Thus every non-trivial self obstruction is a right obstruction. We picture four obstructions as follows.



left obstruction right obstruction

centre obstruction centre obstruction

Lemma 4.1.12. *For all $i, j \in \{1, \dots, s\}$ and $i \le j$, we have $|\mathrm{O}(i,j)| < \infty$.*

Proof. For any non-trivial obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{O}(i,j)$, it follows from Definition 4.1.11 that $\mathrm{len}(w_i \mathrm{LT}_\sigma(g_i) w_i') < \mathrm{len}(\mathrm{LT}_\sigma(g_i)) + \mathrm{len}(\mathrm{LT}_\sigma(g_j))$. Thus $\mathrm{len}(w_i w_i')$ $< \mathrm{len}(\mathrm{LT}_\sigma(g_j))$. Since $|X| < \infty$, there are only finitely many choices of w_i and w_i'. Hence $|\mathrm{O}(i,j)| < \infty$. □

Finally, we have the following practical versions of Buchberger's Criterion and Buchberger's Procedure.

Proposition 4.1.13. (Buchberger Criterion) *Let $G \subseteq K\langle X \rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G \rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Then the following conditions are equivalent.*

a) The set G is a σ-Gröbner basis of I.

b) For every obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1 \le i \le j \le s} \mathrm{O}(i,j)$, we have

$$\mathrm{NR}_{\sigma,\mathcal{G}}(S_{i,j}(w_i, w_i'; w_j, w_j')) = 0.$$

Proof. Follows from Corollary 4.1.3 and Lemmas 4.1.6 and 4.1.10. □

Theorem 4.1.14. (Buchberger Procedure) *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Consider the following sequence of instructions.*

1) Let $s' = s$ and $B = \cup_{1\le i\le j\le s'} \mathrm{O}(i,j)$.

2) If $B = \emptyset$, return the result $\mathcal{G}$. Otherwise, select an obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in B$ using a fair strategy and delete it from B.

3) Compute the S-polynomial $S = S_{i,j}(w_i, w_i'; w_j, w_j')$ and its normal remainder $S' = \mathrm{NR}_{\sigma,\mathcal{G}}(S)$. If $S' = 0$, continue with step 2).

4) Increase s' by one, append $g_{s'} = S'$ to the tuple $\mathcal{G}$, and append the set of obstructions $\cup_{1\le i\le s'} \mathrm{O}(i, s')$ to the set B. Then continue with step 2).

This is a procedure that enumerates a σ-Gröbner basis $\mathcal{G}$ of I. If I has a finite σ-Gröbner basis, it stops after finitely many steps and the resulting tuple $\mathcal{G}$ is a finite σ-Gröbner basis of I.

Proof. The correctness follows from Theorem 4.1.4 and Proposition 4.1.13. We prove that the procedure stops after finitely many steps if I has a finite σ-Gröbner basis. Suppose that $G' = \{g_1', \ldots, g_t'\}$ is a finite σ-Gröbner basis of I. Since the procedure enumerates a σ-Gröbner basis $\mathcal{G}$ of I, for each polynomial $g_j' \in G'$ there exists a polynomial $g_{i_j} \in \mathcal{G}$ such that $\mathrm{LT}_\sigma(g_j')$ is a multiple of $\mathrm{LT}_\sigma(g_{i_j})$. Let $k = \max\{i_1, \ldots, i_t\}$ and $\mathcal{G}_k = (g_1, \ldots, g_k) \subseteq \mathcal{G}$. Then we have $\mathrm{LT}_\sigma\{I\} = \{w\mathrm{LT}_\sigma(g_j')w' \mid g_j' \in G', w, w' \in \langle X\rangle\} \subseteq \{w\mathrm{LT}_\sigma(g_i)w' \mid g_i \in \mathcal{G}_k, w, w' \in \langle X\rangle\} \subseteq \mathrm{LT}_\sigma\{I\}$. Thus $\mathcal{G}_k$ is a σ-Gröbner basis of I. Hence all $\mathrm{NR}_{\sigma,\mathcal{G}}(S)$ in step 3) are zero after g_k being appended to $\mathcal{G}$, and the procedure terminates after finitely many steps by Proposition 4.1.12. □

Example 4.1.15. (continued) Consider Example 4.1.8 again. Recall that the ideal $I \subseteq \mathbb{F}_2\langle x, y, u, v, t, s\rangle$ is generated by the set $\{g_1, g_2\}$ with $g_1 = u(xy)^3 + v(xy)^2 + u + v, g_2 = (yx)^3t + (yx)^2t + t + s$, and that $\sigma = \mathtt{LLex}$ with $x >_\sigma y >_\sigma u >_\sigma v >_\sigma t >_\sigma s$. We have $\mathrm{O}(1,1) = \mathrm{O}(2,2) = \emptyset$ and $\mathrm{O}(1,2) = \{\mathrm{o}_{1,2}(1, xt; ux, 1), \mathrm{o}_{1,2}(1, xyxt; uxyx, 1), \mathrm{o}_{1,2}(1, (xy)^2xt; u(xy)^2xt, 1)\}$. After selecting the obstructions in $\mathrm{O}(1,2)$, we get $g_3 = uxs + vxt, g_4 = uxyxs + vxyxt, g_5 = u(xy)^2xs + v(xy)^2xt$ and $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ by Example 4.1.8. Since $\mathrm{O}(1,3) = \mathrm{O}(2,3) = \mathrm{O}(3,3) = \mathrm{O}(1,4) = \mathrm{O}(2,4) = \mathrm{O}(3,4) = \mathrm{O}(4,4) = \mathrm{O}(1,5) = \mathrm{O}(2,5) = \mathrm{O}(3,5) = \mathrm{O}(4,5) = \mathrm{O}(5,5) = \emptyset$, the set $\{g_1, g_2, g_3, g_4, g_5\}$ is a σ-Gröbner basis of the ideal I.

Remark 4.1.16. We observe again the instructions of the Buchberger Procedure. Note that at every stage of the procedure the tuple $\mathcal{G}$ is a system of generators of the ideal I. We call each such tuple $\mathcal{G}$ a **partial σ-Gröbner basis** of the ideal I. Also note that in general it is undecidable whether a finitely generated ideal has a finite Gröbner basis in free monoid rings (see [58], Theorem 2.4). In some situations we happen to know ahead of time that a finitely generated ideal has only infinite Gröbner bases or Gröbner bases consisting of a very large number of generators. Moreover, for many applications it is not necessary to compute a Gröbner basis completely. Partial Gröbner bases are the gem for these applications. Let us take the word problem (see Definition 2.1.20) as an example. In Remark 3.1.19 we converted the word problem to checking whether the normal form of a polynomial modulo an ideal is zero. We compute the normal remainder of the polynomial with respect to a partial Gröbner basis of the ideal. If the normal remainder is zero, then we get a positive answer to the word problem. Otherwise, we carry on with the Buchberger Procedure and obtain a new partial Gröbner basis and try the division again. In this way we make the word problem into a semi-decidable problem.

We end this section with an application of the Weak Division Algorithm (see Corollary 3.3.9). Recall that in Section 3.2 we constructed the Division Algorithm (see Theorem 3.2.1) with original intention of computing the normal form. Condition 3.2.1.a, i.e. no element of the support of the normal remainder is contained in the monomial ideal generated by the leading terms of divisors, is a strong requirement. Compared with the Weak Division Algorithm, further reduction steps are needed in order to satisfy condition 3.2.1.a. Note that condition 3.2.1.a is not necessary for Gröbner basis computations.

Proposition 4.1.17. (Weak Buchberger Criterion) *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Then the following conditions are equivalent.*

a) The set G is a σ-Gröbner basis of I.

b) For every obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq s}\mathrm{O}(i,j)$, we have

$$\mathrm{WNR}_{\sigma,G}(S_{i,j}(w_i, w_i'; w_j, w_j')) = 0.$$

Proof. Note that for each S-polynomial the Weak Division Algorithm gives a weak Gröbner representation in terms of G. Then the proof of the proposition is analogous to the proof of Proposition 4.1.13. □

Thus $\mathrm{WNR}_{\sigma,\mathcal{G}}(S)$ is an alternative to $\mathrm{NR}_{\sigma,\mathcal{G}}(S)$ in the Buchberger Procedure (see Theorem 4.1.14). According to our experiments the Division Algorithm and the Weak Division Algorithm have almost the same performance for Gröbner basis computations. It is still unclear which one is superior. A more practical usage of the Weak Division Algorithm is the following algorithm for checking whether a given finite system of generators is a Gröbner basis.

Corollary 4.1.18. *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Consider the following sequence of instructions.*

1) Let $B = \cup_{1\leq i\leq j\leq s}\mathrm{O}(i,j)$.

2) If $B = \emptyset$, then return "The set G is a σ-Gröbner basis of the ideal $\langle G\rangle$". Otherwise, select an obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in B$ and delete it from B.

3) Compute $S = S_{i,j}(w_i, w_i'; w_j, w_j')$ and $\mathrm{WNR}_{\sigma,\mathcal{G}}(S)$. If $\mathrm{WNR}_{\sigma,\mathcal{G}}(S) = 0$, continue with step 2). Otherwise, return "The set G is not a σ-Gröbner basis of the ideal $\langle G\rangle$".

This is an algorithm which checks if a finite set of polynomials G is a σ-Gröbner basis of the ideal $\langle G\rangle$.

Proof. The termination follows from Proposition 4.1.12 and the correctness follows from Proposition 4.1.17. □

4.2 Improved Buchberger Procedures

Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Proposition 4.1.13 states that G is a σ-Gröbner basis of I if and only if the normal remainders of all the S-polynomials of non-trivial obstructions in $\cup_{1\leq i\leq j\leq s}\mathrm{O}(i,j)$ are zero with respect to $\mathcal{G}$. The normal remainders are computed by the Division Algorithm. Note that the application of the Division Algorithm is the most time-consuming part in the Buchberger Procedure. Hence the most efficient optimization of the Buchberger Procedure is to detect as many unnecessary obstructions, i.e. the obstructions whose S-polynomials have the zero normal remainder, as possible.

In the commutative case, this problem was first studied by B. Buchberger [12, 13]. Later on, R. Gebrauer and H. Möller [33] used Taylor bases of the module generated by the critical syzygies to detect almost all unnecessary critical pairs very efficiently, and this resulted in the *Gebauer-Möller Installation.* In [43], Tutorial 25, M. Kreuzer and L. Robbiano generalized the Gebauer-Möller Installation to modules. In [17, 44], M. Kreuzer et al. applied Gröbner basis techniques to modules in the homogeneous case and obtained a minimal system of generators of the module generated by the critical syzygies. Hence they successfully detected all unnecessary critical pairs. In the non-commutative case, T. Mora [55] gave a detailed presentation of useless pairs.

In this section we shall explore techniques for detecting unnecessary obstructions in free monoid rings. To this end we shall first present an Interreduction Algorithm on non-trivial obstructions, which is based on the assumption that the elements of the leading term set $\mathrm{LT}_\sigma\{G\}$ are coprime. Then, by looking at the interreduction operations closely, we shall give straightforward generalizations of the Gebauer-Möller Installation and present improved versions of the Buchberger Procedure. Note that the method in [17, 44] is strongly related to Gröbner basis theory in modules, which we will study in Chapter 5. In this section we also improve the Buchberger Procedure by deleting redundant generators.

For our purposes we order the terms in $\mathbb{T}(F_s)$ by a relation τ as follows.

Definition 4.2.1. Let $\mathcal{G}$ be the tuple as above, and let σ be an admissible ordering on $\langle X\rangle$. For all $w_1\epsilon_i w_1', w_2\epsilon_j w_2' \in \mathbb{T}(F_s)$, we say $w_1\epsilon_i w_1' \geq_\tau w_2\epsilon_j w_2'$ if and only if $w_1\mathrm{LT}_\sigma(g_i)w_1' >_\sigma w_2\mathrm{LT}_\sigma(g_j)w_2'$, or $w_1\mathrm{LT}_\sigma(g_i)w_1' = w_2\mathrm{LT}_\sigma(g_j)w_2'$ and $i > j$, or $w_1\mathrm{LT}_\sigma(g_i)w_1' = w_2\mathrm{LT}_\sigma(g_j)w_2'$ and $i = j$ and $w_1 \geq_\sigma w_2$. The relation τ is called the **module term ordering** induced by $(\sigma, \mathcal{G})$ on $\mathbb{T}(F_s)$.

In fact, the relation τ defined above is a module term ordering on $\mathbb{T}(F_s)$ (see Definition 5.1.1). It follows from Definitions 3.4.7 and 4.1.11 that $w_i\epsilon_i w_i' <_\tau w_j\epsilon_j w_j'$ for all $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq s}\mathrm{O}(i,j)$.

4.2.1 Interreduction on Obstructions

To perform interreduction, we make some observations about operations on the set $\cup_{1\leq i\leq j\leq s}\mathrm{O}(i,j)$. Recall that two words $w, w' \in \langle X\rangle$ are called **coprime** if neither w is a subword of w' nor w' is a subword of w. The following proposition is essential for our purposes.

Proposition 4.2.2. *Suppose that the elements of the leading term set* $\mathrm{LT}_\sigma\{G\}$ *are coprime. Let* $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j'), \mathrm{o}_{k,l}(w_k, w_k'; w_l, w_l') \in \cup_{1\leq i\leq j\leq s}\mathrm{O}(i,j)$ *be two distinct* *non-trivial obstructions.*

a) *Suppose that $j = l, i \le k$, and $w_j \epsilon_j w'_j = w w_l \epsilon_l w'_l w'$ for some $w, w' \in \langle X\rangle$. Then we have*

$$\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) - w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w' = \mathrm{o}_{i,k}(w_i, w'_i; ww_k, w'_k w')$$

and $\mathrm{o}_{i,k}(w_i, w'_i; ww_k, w'_k w') \in \mathrm{O}(i,k)$ has an overlap.

b) *Suppose that $j = l, i > k$, and $w_j \epsilon_j w'_j = w w_l \epsilon_l w'_l w'$ for some $w, w' \in \langle X\rangle$. Then we have*

$$-\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) + w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w' = \mathrm{o}_{k,i}(ww_k, w'_k w'; w_i, w'_i)$$

and $\mathrm{o}_{k,i}(ww_k, w'_k w'; w_i, w'_i) \in \mathrm{O}(k,i)$ has an overlap.

c) *Suppose that $i = l$ and $w_i \epsilon_i w'_i = w w_l \epsilon_l w'_l w'$ for some $w, w' \in \langle X\rangle$. Then we have*

$$\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) + w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w' = \mathrm{o}_{k,j}(ww_k, w'_k w'; w_j, w'_j)$$

and $\mathrm{o}_{k,j}(ww_k, w'_k w'; w_j, w'_j) \in \mathrm{O}(k,j)$ has an overlap.

Proof. To prove claim a), by Definition 3.4.7, we have

$$\begin{aligned}
& \mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) - w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w' \\
= \ & (\frac{1}{\mathrm{LC}_\sigma(g_i)} w_i \epsilon_i w'_i - \frac{1}{\mathrm{LC}_\sigma(g_j)} w_j \epsilon_j w'_j) - w(\frac{1}{\mathrm{LC}_\sigma(g_k)} w_k \epsilon_k w'_k - \frac{1}{\mathrm{LC}_\sigma(g_l)} w_l \epsilon_l w'_l)w' \\
= \ & (\frac{1}{\mathrm{LC}_\sigma(g_i)} w_i \epsilon_i w'_i - \frac{1}{\mathrm{LC}_\sigma(g_k)} ww_k \epsilon_k w'_k w') - (\frac{1}{\mathrm{LC}_\sigma(g_j)} w_j \epsilon_j w'_j - \frac{1}{\mathrm{LC}_\sigma(g_l)} ww_l \epsilon_l w'_l w').
\end{aligned}$$

We have $w_i \mathrm{LT}_\sigma(g_i) w'_i = w_j \mathrm{LT}_\sigma(g_j) w'_j = ww_l \mathrm{LT}_\sigma(g_l) w'_l w' = ww_k \mathrm{LT}_\sigma(g_k) w'_k w'$ and $\frac{1}{\mathrm{LC}_\sigma(g_j)} w_j \epsilon_j w'_j - \frac{1}{\mathrm{LC}_\sigma(g_l)} ww_l \epsilon_l w'_l w' = 0$ by assumption. Then, by Definition 3.4.7, we have $\frac{1}{\mathrm{LC}_\sigma(g_i)} w_i \epsilon_i w'_i - \frac{1}{\mathrm{LC}_\sigma(g_k)} ww_k \epsilon_k w'_k w' = \mathrm{o}_{i,k}(w_i, w'_i; ww_k, w'_k w') \in \mathrm{O}(i,k)$. We show that $\mathrm{o}_{i,k}(w_i, w'_i; ww_k, w'_k w')$ has an overlap. By Definition 4.1.11 and the assumption that $\mathrm{LT}_\sigma(g_i)$ and $\mathrm{LT}_\sigma(g_j)$ are coprime, we may assume, without loss of generality, that $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) = \frac{1}{\mathrm{LC}_\sigma(g_i)} \epsilon_i w'_i - \frac{1}{\mathrm{LC}_\sigma(g_j)} w_j \epsilon_j$ with $w'_i, w_j \in \langle X\rangle \setminus \{1\}$ and $\mathrm{len}(\mathrm{LT}_\sigma(g_i)) > \mathrm{len}(w_j)$. From the assumption $w_j \epsilon_j = ww_l \epsilon_l w'_l w'$, it follows that $ww_l = w_j, w'_l w' = 1$ and hence $w'_l = w' = 1$. Note that $\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)$ is also a non-trivial obstruction. By Definition 4.1.11 we must have $\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l) = \frac{1}{\mathrm{LC}_\sigma(g_k)} \epsilon_k w'_k - \frac{1}{\mathrm{LC}_\sigma(g_l)} w_l \epsilon_l$ with $w'_k, w_l \in \langle X\rangle \setminus \{1\}$. Thus $\mathrm{o}_{i,k}(w_i, w'_i; ww_k, w'_k w') = \frac{1}{\mathrm{LC}_\sigma(g_i)} \epsilon_i w'_i - \frac{1}{\mathrm{LC}_\sigma(g_k)} w \epsilon_k w'_k$ and

$\mathrm{len}(\mathrm{LT}_\sigma(g_i)) > \mathrm{len}(w_j) = \mathrm{len}(ww_l) > \mathrm{len}(w)$. Therefore $\mathrm{o}_{i,k}(w_i, w'_i; ww_k, w'_kw')$ has an overlap.

We prove claim b). By Definition 3.4.7, we have

$$\begin{aligned}
& -\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) + w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w' \\
= \; & -(\frac{1}{\mathrm{LC}_\sigma(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_jw'_j) + w(\frac{1}{\mathrm{LC}_\sigma(g_k)}w_k\epsilon_kw'_k - \frac{1}{\mathrm{LC}_\sigma(g_l)}w_l\epsilon_lw'_l)w' \\
= \; & (\frac{1}{\mathrm{LC}_\sigma(g_k)}ww_k\epsilon_kw'_kw' - \frac{1}{\mathrm{LC}_\sigma(g_i)}w_i\epsilon_iw'_i) + (\frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_jw'_j - \frac{1}{\mathrm{LC}_\sigma(g_l)}ww_l\epsilon_lw'_lw').
\end{aligned}$$

We have $w_i\mathrm{LT}_\sigma(g_i)w'_i = w_j\mathrm{LT}_\sigma(g_j)w'_j = ww_l\mathrm{LT}_\sigma(g_l)w'_lw' = ww_k\mathrm{LT}_\sigma(g_k)w'_kw'$ and $\frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_jw'_j - \frac{1}{\mathrm{LC}_\sigma(g_l)}ww_l\epsilon_lw'_lw' = 0$ by assumption. Then, by Definition 3.4.7, we have $\frac{1}{\mathrm{LC}_\sigma(g_k)}ww_k\epsilon_kw'_kw' - \frac{1}{\mathrm{LC}_\sigma(g_i)}w_i\epsilon_iw'_i = \mathrm{o}_{k,i}(ww_k, w'_kw'; w_i, w'_i) \in \mathrm{O}(k,i)$. Proceeding exactly the same as the proof of claim a), one can show that $\mathrm{o}_{k,i}(ww_k, w'_kw'; w_i, w'_i)$ has an overlap.

Finally we prove claim c). By Definition 3.4.7, we have

$$\begin{aligned}
& \mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) + w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w' \\
= \; & (\frac{1}{\mathrm{LC}_\sigma(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_jw'_j) + w(\frac{1}{\mathrm{LC}_\sigma(g_k)}w_k\epsilon_kw'_k - \frac{1}{\mathrm{LC}_\sigma(g_l)}w_l\epsilon_lw'_l)w' \\
= \; & (\frac{1}{\mathrm{LC}_\sigma(g_k)}ww_k\epsilon_kw'_kw' - \frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_jw'_j) + (\frac{1}{\mathrm{LC}_\sigma(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\sigma(g_l)}ww_l\epsilon_lw'_lw').
\end{aligned}$$

We have $w_j\mathrm{LT}_\sigma(g_j)w'_j = w_i\mathrm{LT}_\sigma(g_i)w'_i = ww_l\mathrm{LT}_\sigma(g_l)w'_lw' = ww_k\mathrm{LT}_\sigma(g_k)w'_kw'$ and $\frac{1}{\mathrm{LC}_\sigma(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\sigma(g_l)}ww_l\epsilon_lw'_lw' = 0$ by assumption. Then, by Definition 3.4.7, we have $\frac{1}{\mathrm{LC}_\sigma(g_k)}ww_k\epsilon_kw'_kw' - \frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_jw'_j = \mathrm{o}_{k,j}(ww_k, w'_kw'; w_j, w'_j) \in \mathrm{O}(k,j)$. We show that $\mathrm{o}_{k,j}(ww_k, w'_kw'; w_j, w'_j)$ has an overlap. By Definition 4.1.11 and the assumption that $\mathrm{LT}_\sigma(g_i)$ and $\mathrm{LT}_\sigma(g_j)$ are coprime, we may assume, without loss of generality, that $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) = \frac{1}{\mathrm{LC}_\sigma(g_i)}\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_j$ with $w'_i, w_j \in \langle X\rangle\backslash\{1\}$ and $\mathrm{len}(\mathrm{LT}_\sigma(g_j)) > \mathrm{len}(w'_i)$. From the assumption $\epsilon_iw'_i = ww_l\epsilon_lw'_lw'$, it follows that $ww_l = 1, w'_lw' = w'_i$ and hence $w_l = w = 1$. Note that $\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)$ is also a non-trivial obstruction. By Definition 4.1.11 we must have $\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l) = \frac{1}{\mathrm{LC}_\sigma(g_k)}w_k\epsilon_k - \frac{1}{\mathrm{LC}_\sigma(g_l)}\epsilon_lw'_l$ with $w_k, w'_l \in \langle X\rangle \setminus \{1\}$. Thus $\mathrm{o}_{k,j}(ww_k, w'_kw'; w_j, w'_j) = \frac{1}{\mathrm{LC}_\sigma(g_k)}w_k\epsilon_kw' - \frac{1}{\mathrm{LC}_\sigma(g_j)}w_j\epsilon_j$ and $\mathrm{len}(\mathrm{LT}_\sigma(g_j)) > \mathrm{len}(w'_i) = \mathrm{len}(w'_lw') > \mathrm{len}(w')$. Therefore $\mathrm{o}_{k,j}(ww_k, w'_kw'; w_j, w'_j)$ has an overlap. □

The assumption that the elements of $\mathrm{LT}_\sigma\{G\}$ are coprime is crucial to ensure that the resulting obstructions in the proposition have overlaps. The following example shows this.

Example 4.2.3. Consider the free monoid ring $K\langle x,y\rangle$ and the tuple $\mathcal{G}=(g_1,g_2,g_3)$ with $\mathrm{LM}_\sigma(\mathcal{G})=((xy)^2,y,xyx^2y)$. We have $\mathrm{o}_{1,3}(xyx,1;1,xy)\in \mathrm{O}(1,3), \mathrm{o}_{2,3}(x,x^2y;1,1) \in \mathrm{O}(2,3)$, and $\mathrm{o}_{1,3}(xyx,1;1,xy)-\mathrm{o}_{2,3}(x,x^2y;1,1)xy=\mathrm{o}_{1,2}(xyx,1;x,x^2yxy)\in\mathrm{O}(1,2)$. But $\mathrm{o}_{1,2}(xyx,1;x,x^2yxy)\notin \mathrm{O}(1,2)$ since $\mathrm{LT}_\sigma(g_1)$ and $\mathrm{LT}_\sigma(g_2)$ have no overlap in $xyx\mathrm{LT}_\sigma(g_1)=xyx(xy)^2$.

Assumption 4.2.4. *In the rest of this subsection, we shall assume that the elements of the leading term set* $\mathrm{LT}_\sigma\{G\}$ *are coprime.*

However, even this assumption is satisfied we still cannot guarantee that the resulting obstructions in Proposition 4.2.2 are non-trivial.

Example 4.2.5. Consider the free monoid ring $K\langle x,y\rangle$ and the tuple $\mathcal{G}=(g_1,g_2,g_3)$ with $\mathrm{LM}_\sigma(\mathcal{G})=(x^2y^2,y^3,xyx^2y)$. We have $\mathrm{o}_{1,3}(xy,1;1,y)\in\mathrm{O}(1,3), \mathrm{o}_{2,3}(xyx^2,1;1,y^2)\in \mathrm{O}(2,3)$, and $-\mathrm{o}_{2,3}(xyx^2,1;1,y^2)+\mathrm{o}_{1,3}(xy,1;1,y)y=\mathrm{o}_{1,2}(xy,y;xyx^2,1)\in\mathrm{O}(1,2)$. Observe that $w_1=xy$ and $w_2=xyx^2$ have a common prefix xy. Thus by Definition 4.1.11 $\mathrm{o}_{1,2}(xy,y;xyx^2,1)\notin\mathrm{O}(1,2)$.

Definition 4.2.6. We define a **shrink map** Shk on $\cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ as follows.

$$\begin{aligned}\mathrm{Shk}:\ \cup_{1\le i\le j\le s}\mathrm{o}(i,j) &\ \rightarrow\ \cup_{1\le i\le j\le s}\mathrm{o}(i,j)\\ \mathrm{o}_{i,j}(w_i,w_i';w_j,w_j') &\ \mapsto\ \mathrm{o}_{i,j}(\tilde{w}_i,\tilde{w}_i';\tilde{w}_j,\tilde{w}_j')\end{aligned}$$

where $w_i=w\tilde{w}_i, w_j=w\tilde{w}_j, w_i'=\tilde{w}_i'w', w_j'=\tilde{w}_j'w'$ such that $w\in\langle X\rangle$ is the maximal common prefix of w_i and w_j, and such that $w'\in\langle X\rangle$ is the maximal common suffix of w_i' and w_j'.

Clearly, if $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')\in\mathrm{o}(i,j)$ is an obstruction with an overlap, then $\mathrm{Shk}(\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j'))\in\mathrm{O}(i,j)$ is a non-trivial obstruction.

Definition 4.2.7. Let $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j'), \mathrm{o}_{k,l}(w_k,w_k';w_l,w_l')\in\cup_{1\le i\le j\le s}\mathrm{O}(i,j)$ be two distinct non-trivial obstructions.

a) Suppose that $j=l, i<k$, and $ww_l\epsilon_l w_l'w'=w_j\epsilon_j w_j'$ for some $w,w'\in\langle X\rangle$. Then we let

$$\mathrm{o}_{i,k}(w_i,w_i';ww_k,w_k'w')=\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')-w\mathrm{o}_{k,l}(w_k,w_k';w_l,w_l')w'$$

and say that $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')$ is **reduced** to $\mathrm{Shk}(\mathrm{o}_{i,k}(w_i,w_i';ww_k,w_k'w'))$.

b) Suppose that $j = l, i > k$, and $ww_l\epsilon_l w'_l w' = w_j\epsilon_j w'_j$ for some $w, w' \in \langle X\rangle$. Then we let

$$\mathrm{o}_{k,i}(ww_k, w'_k w'; w_i, w'_i) = -\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) + w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w'$$

and say that $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$ is **reduced** to $\mathrm{Shk}(\mathrm{o}_{k,i}(ww_k, w'_k w'; w_i, w'_i))$.

c) Suppose that $j = l, i = k$, and $ww_l\epsilon_l w'_l w' = w_j\epsilon_j w'_j$ for some $w, w' \in \langle X\rangle$. Then we let

$$\mathrm{o}_{i,i}(w_i, w'_i; ww_k, w'_k w') = \mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) - w\mathrm{o}(i, l; w_k, w'_k; w_l, w'_l)w'$$

and say that $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$ is **reduced** to $\mathrm{Shk}(\mathrm{o}_{i,i}(w_i, w'_i; ww_k, w'_k w'))$ if $\mathrm{len}(w_i) < \mathrm{len}(ww_k)$, and to $\mathrm{Shk}(\mathrm{o}_{i,i}(ww_k, w'_k w'; w_i, w'_i))$ if $\mathrm{len}(w_i) > \mathrm{len}(ww_k)$.

d) Suppose that $i = l$ and $ww_l\epsilon_l w'_l w' = w_i\epsilon_i w'_i$ for some $w, w' \in \langle X\rangle$. Then we let

$$\mathrm{o}_{k,j}(ww_k, w'_k w'; w_j, w'_j) = \mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) + w\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)w'$$

and say that $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$ is **reduced** to $\mathrm{Shk}(\mathrm{o}_{k,j}(ww_k, w'_k w'; w_j, w'_j))$.

In the cases above, we say $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$ can be **reduced** by $\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)$. The reduction is called **one step obstruction reduction** on $\cup_{1\le i\le j\le s}\mathrm{O}(i, j)$ and is denoted by $\rightarrow_{\mathrm{Ob}}$.

Definition 4.2.8. The reflexive transitive closure of $\rightarrow_{\mathrm{Ob}}$ is called the **obstruction reduction** defined by $\cup_{1\le i\le j\le s}\mathrm{O}(i, j)$ and is denoted by $\overset{*}{\rightarrow}_{\mathrm{Ob}}$. An obstruction $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1\le i\le j\le s}\mathrm{O}(i, j)$ is called **irreducible** with respect to $\overset{*}{\rightarrow}_{\mathrm{Ob}}$ if there is no obstruction in $\cup_{1\le i\le j\le s}\mathrm{O}(i, j)$ that can reduce $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$. A set of non-trivial obstructions is called **interreduced** if every obstruction in the set is irreducible.

Before presenting two important properties of the obstruction reduction, we shall extend the module term ordering τ to the set of obstructions $\cup_{1\le i\le j\le s}\mathrm{o}(i, j)$. We shall commit a slight abuse of notation and use τ to denote this relation.

Definition 4.2.9. Let τ be the module term ordering defined as in Definition 4.2.1. For two obstructions $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j)$, $\mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l) \in \cup_{1\le i\le j\le s}\mathrm{o}(i, j)$, we say $\mathrm{o}_{i,j}(w_i, w'_i; w_j, w'_j) \ge_\tau \mathrm{o}_{k,l}(w_k, w'_k; w_l, w'_l)$ if we have $w_j\epsilon_j w'_j >_\tau w_l\epsilon_l w'_l$, or if we have $w_j\epsilon_j w'_j = w_l\epsilon_l w'_l$ and $w_i\epsilon_i w'_i \ge_\tau w_k\epsilon_k w'_k$.

Remark 4.2.10. We can verify easily that τ is a complete ordering on $\cup_{1\le i\le j\le s}\mathrm{o}(i,j)$ and is a well-ordering and compatible with scalar multiplication. Obviously, we have $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \ge_\tau \mathrm{Shk}(\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j'))$ for all $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\le i\le j\le s}\mathrm{o}(i,j)$.

Proposition 4.2.11. *The obstruction reduction has the following properties.*

a) *Let* $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j'), \mathrm{o}_{k,l}(w_k, w_k'; w_l, w_l') \in \cup_{1\le i\le j\le s}\mathrm{O}(i,j)$ *be two distinct non-trivial obstructions, and let*

$$\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \xrightarrow{\mathrm{o}_{k,l}(w_k,w_k';w_l,w_l')}_{\mathrm{Ob}} \mathrm{o}_{\mu,\nu}(w_\mu, w_\mu'; w_\nu, w_\nu') \in \cup_{1\le i\le j\le s}\mathrm{O}(i,j)$$

be one step obstruction reduction. Then we have

$$\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') >_\tau \mathrm{o}_{\mu,\nu}(w_\mu, w_\mu'; w_\nu, w_\nu').$$

Moreover, if the S-polynomials $S_{k,l}(w_k, w_k'; w_l, w_l')$ *and* $S_{\mu,\nu}(w_\mu, w_\mu'; w_\nu, w_\nu')$ *have weak Gröbner representations in terms of* G*, then so does the S-polynomial* $S_{i,j}(w_i, w_i'; w_j, w_j')$*.*

b) *The relation* $\xrightarrow{*}_{\mathrm{Ob}}$ *is Noetherian.*

Proof. Claim a) can be verified case by case according to Definition 4.2.7. We prove the claim for case a) of Definition 4.2.7 and one can prove the other cases similarly. In Definition 4.2.7.a), we have $i<k, j=l, ww_{jk}\epsilon_j w_{jk}'w' = w_{ji}\epsilon_j w_{ji}'$ for some $w, w' \in \langle X\rangle$, and

$$\mathrm{o}_{i,k}(w_{ij}, w_{ij}'; ww_{kj}, w_{kj}'w') = \mathrm{o}_{i,j}(w_{ij}, w_{ij}'; w_{ji}, w_{ji}') - w\mathrm{o}_{k,j}(w_{kj}, w_{kj}'; w_{jk}, w_{jk}')w'.$$

We have $w_{kj}\epsilon_k w_{kj}' <_\tau w_{jk}\epsilon_j w_{jk}'$ and hence $ww_{kj}\epsilon_k w_{kj}'w' <_\tau ww_{jk}\epsilon_j w_{jk}'w' = w_{ji}\epsilon_j w_{ji}'$ by Definition 4.2.1. Then, by Definition 4.2.9, we have $\mathrm{o}_{i,j}(w_{ij}, w_{ij}'; w_{ji}, w_{ji}') >_\tau \mathrm{o}_{i,k}(w_{ij}, w_{ij}'; ww_{kj}, w_{kj}'w') \ge_\tau \mathrm{Shk}(\mathrm{o}_{i,k}(w_{ij}, w_{ij}'; ww_{kj}, w_{kj}'w'))$.

Let $\mathrm{o}_{i,k}(w_i, w_i'; w_k, w_k') = \mathrm{Shk}(\mathrm{o}_{i,k}(w_{ij}, w_{ij}'; ww_{kj}, w_{kj}'w'))$, i.e. there exist $\tilde{w}, \tilde{w}' \in \langle X\rangle$ such that $\mathrm{o}_{i,k}(w_{ij}, w_{ij}'; ww_{kj}, w_{kj}'w') = \tilde{w}\mathrm{o}_{i,k}(w_i, w_i'; w_k, w_k')\tilde{w}'$. Thus we have

$$\mathrm{o}_{i,j}(w_{ij}, w_{ij}'; w_{ji}, w_{ji}') = w\mathrm{o}_{k,j}(w_{kj}, w_{kj}'; w_{jk}, w_{jk}')w' + \tilde{w}\mathrm{o}_{i,k}(w_i, w_i'; w_k, w_k')\tilde{w}',$$

and hence

$$S_{i,j}(w_{ij}, w_{ij}'; w_{ji}, w_{ji}') = wS_{k,j}(w_{kj}, w_{kj}'; w_{jk}, w_{jk}')w' + \tilde{w}S_{i,k}(w_i, w_i'; w_k, w_k')\tilde{w}'.$$

Without loss of generality, we assume $S_{i,j}(w_{ij}, w'_{ij}; w_{ji}, w'_{ji}), S_{k,j}(w_{kj}, w'_{kj}; w_{jk}, w'_{jk})$ and $S_{i,k}(w_i, w'_i; w_k, w'_k)$ are non-zero. Since $S_{k,j}(w_{kj}, w'_{kj}; w_{jk}, w'_{jk})$ has a weak Gröbner representation in terms of G, we have

$$S_{k,j}(w_{kj}, w'_{kj}; w_{jk}, w'_{jk}) = \sum_{s=1}^{\mu} a_s w_s g_{i_s} w'_s$$

with $a_s \in K \setminus \{0\}, w_s, w'_s \in \langle X \rangle, g_{i_s} \in G$ such that $\mathrm{LT}_\sigma(w_{jk} g_j w'_{jk}) >_\sigma \mathrm{LT}_\sigma(w_s g_{i_s} w'_s)$ for all $s \in \{1, \ldots, \mu\}$. Similarly, since $S_{i,k}(w_i, w'_i; w_k, w'_k)$ has a weak Gröbner representation in terms of G, we have

$$S_{i,k}(w_i, w'_i; w_k, w'_k) = \sum_{t=1}^{\nu} b_t w_t g_{i_t} w'_t$$

with $b_t \in K \setminus \{0\}, w_t, w'_t \in \langle X \rangle, g_{i_t} \in G$ such that $\mathrm{LT}_\sigma(w_k g_k w'_k) >_\sigma \mathrm{LT}_\sigma(w_t g_{i_t} w'_t)$ for all $t \in \{1, \ldots, \nu\}$. Therefore we have

$$\begin{aligned} S_{i,j}(w_{ij}, w'_{ij}; w_{ji}, w'_{ji}) &= w(\sum_{s=1}^{\mu} a_s w_s g_{i_s} w'_s) w' + \tilde{w}(\sum_{t=1}^{\nu} b_t w_t g_{i_t} w'_t) \tilde{w}' \\ &= \sum_{s=1}^{\mu} a_s w w_s g_{i_s} w'_s w' + \sum_{t=1}^{\nu} b_t \tilde{w} w_t g_{i_t} w'_t \tilde{w}'. \end{aligned}$$

From $w w_{jk} \epsilon_j w'_{jk} w' = w_{ji} \epsilon_j w'_{ji}$, it follows that $w w_{jk} \mathrm{LT}_\sigma(g_j) w'_{jk} w' = w_{ji} \mathrm{LT}_\sigma(g_j) w'_{ji}$. By Remark 3.1.13.b we have $\mathrm{LT}_\sigma(w_{ji} g_j w'_{ji}) = w_{ji} \mathrm{LT}_\sigma(g_j) w'_{ji} = w w_{jk} \mathrm{LT}_\sigma(g_j) w'_{jk} w' = w \mathrm{LT}_\sigma(w_{jk} g_j w'_{jk}) w' >_\tau w \mathrm{LT}_\sigma(w_s g_{i_s} w'_s) w' = \mathrm{LT}_\sigma(w w_s g_{i_s} w'_s w')$ for all $s \in \{1, \ldots, \mu\}$. It follows from $\mathrm{o}_{i,k}(w_{ij}, w'_{ij}; w w_{kj}, w'_{kj} w') = \tilde{w} \mathrm{o}_{i,k}(w_i, w'_i; w_k, w'_k) \tilde{w}'$ that $w_{ij} \mathrm{LT}_\sigma(g_i) w'_{ij} = w w_{kj} \mathrm{LT}_\sigma(g_k) w'_{kj} w' = \tilde{w} w_k \mathrm{LT}_\sigma(g_k) w'_k \tilde{w}'$. Then we have $\mathrm{LT}_\sigma(w_{ij} g_i w'_{ij}) = w_{ij} \mathrm{LT}_\sigma(g_i) w'_{ij}$ $= \tilde{w} w_k \mathrm{LT}_\sigma(g_k) w'_k \tilde{w} = \tilde{w} \mathrm{LT}_\sigma(w_k g_k w'_k) \tilde{w} >_\sigma \tilde{w} \mathrm{LT}_\sigma(w_t g_{i_t} w'_t) \tilde{w}' = \mathrm{LT}_\sigma(\tilde{w} w_t g_{i_t} w'_t \tilde{w}')$ for all $t \in \{1, \ldots, \nu\}$ by Remark 3.1.13.b. Finally, from $\mathrm{LT}_\sigma(w_{ji} g_j w'_{ji}) = w_{ji} \mathrm{LT}_\sigma(g_j) w'_{ji} = w_{ij} \mathrm{LT}_\sigma(g_i) w'_{ij} = \mathrm{LT}_\sigma(w_{ij} g_i w'_{ij})$, we conclude that

$$S_{i,j}(w_{ij}, w'_{ij}; w_{ji}, w'_{ji}) = \sum_{s=1}^{\mu} a_s w w_s g_{i_s} w'_s w' + \sum_{t=1}^{\nu} b_t \tilde{w} w_t g_{i_t} w'_t \tilde{w}'$$

is a weak Gröbner representation of $S_{i,j}(w_{ij}, w'_{ij}; w_{ji}, w'_{ji})$ in terms of G.

Claim b) directly follows from claim a) and the fact that τ is a well-ordering on $\cup_{1 \le i \le j \le s} \mathrm{O}(i,j)$. □

From Proposition 4.2.11 we construct the following Interreduction Algorithm on the set of non-trivial obstructions.

Theorem 4.2.12. (Interreduction Algorithm) *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, let $s = |\mathcal{G}|$, and let $\cup_{1\le i\le j\le s}\mathrm{O}(i,j)$ be the set of non-trivial obstructions. Moreover, suppose that Assumption 4.2.4 is satisfied. Consider the following sequence of instructions.*

1) *Let $B = \cup_{1\le i\le j\le s}\mathrm{O}(i,j)$, and let $\xrightarrow{*}_{\mathrm{Ob}}$ be the obstruction reduction defined by B.*

2) *If there is no obstruction in B that can be reduced by other obstructions in B, return the set B. Choose an obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in B$ that can be reduced by other obstructions in B, and delete it from B.*

3) *Reduce $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ by $\xrightarrow{*}_{\mathrm{Ob}}$ as much as possible until it becomes an irreducible obstruction $\mathrm{o}_{\mu,\nu}(w_\mu, w_\mu'; w_\nu, w_\nu')$ with respect to $\xrightarrow{*}_{\mathrm{Ob}}$.*

4) *If $\mathrm{o}_{\mu,\nu}(w_\mu, w_\mu'; w_\nu, w_\nu') \notin B$, insert it into B. Then continue with step 2).*

This is an algorithm that computes an interreduced set of non-trivial obstructions from $\cup_{1\le i\le j\le s}\mathrm{O}(i,j)$.

Using Theorem 4.2.12, we can delete a large number of unnecessary obstructions during the Buchberger Procedure and hence avoid many unnecessary division steps. The following example shows the effectivity of the Interreduction Algorithm.

Example 4.2.13. Consider the free monoid ring $\mathbb{Q}\langle a,b\rangle$ equipped with the admissible ordering $\sigma = \texttt{LLex}$ on $\langle a,b\rangle$ such that $a >_\sigma b$. Let $I \subseteq \mathbb{Q}\langle a,b\rangle$ be the ideal generated by the set $\{g_1, g_2, g_3\}$ with $g_1 = a^2 - 1, g_2 = b^3 - 1$, and $g_3 = (ababab^2ab^2)^2 - 1$. Note that $\langle a, b \mid a^2 = b^3 = (ababab^2ab^2)^2 = 1\rangle$ is a finite generalized triangle group of order 576 (cf. [64], Theorem 2.12). We enumerate a σ-Gröbner basis of I using the Buchberger Procedure equipped with the Interreduction Algorihtm given in Theroem 4.2.12. To satisfy Assumption 4.2.4, we equip the Buchberger Procedure with the interreduction on the system of generators (see Theorem 3.2.8). At termination of the procedure, we get the reduced σ-Gröbner basis of I which consists of 35 generators. When the number of generators changes during the Buchberger Procedure, we plot in Figure 4.1 the number of total non-trivial obstructions, the number of obstructions reduced by the Interreduction Algorithm, the number of obstructions left after applying the Interreduction Algorithm, and the number of generators. As we have marked in the figure, the maximal number of non-trivial obstructions is 2298, while the maximal number of obstructions left after applying the Interreduction Algorithm is 283. And the maximal number of generators is 36. The figure shows that the number of total non-trivial obstructions can be very large even though the number of generators is small. Note that this is a frequent phenomenon in free monoid rings. Our Interreduction Algorithm reduces a large number of unnecessary obstructions successfully.

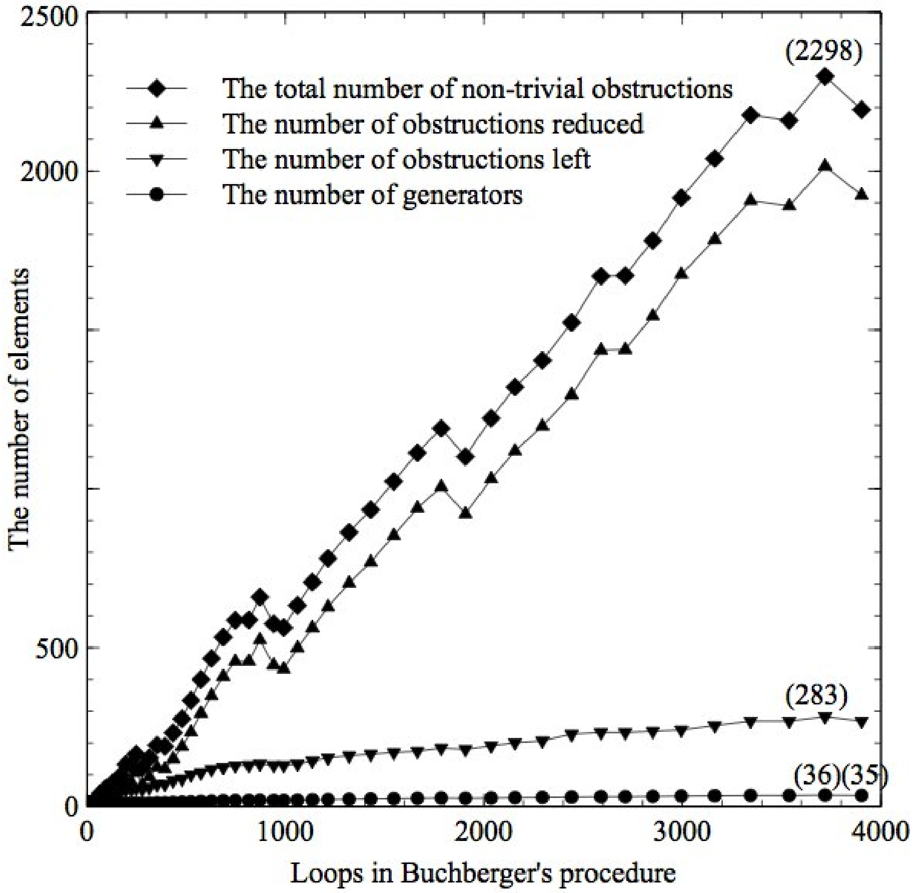


Figure 4.1: Computation of LLex-Gröbner basis of the ideal $\langle g_1, g_2, g_3\rangle \subseteq \mathbb{Q}\langle a, b\rangle$ with $g_1 = a^2 - 1, g_2 = b^3 - 1$, and $g_3 = (ababab^2ab^2)^2 - 1$.

4.2.2 Improved Buchberger Procedures

However, the drawbacks of applying the Interreduction Algorithm on the set of non-trivial obstructions are twofold. First, Assumption 4.2.4, i.e. the elements of $\mathrm{LT}_\sigma\{G\}$ are coprime, is too strict. It could be quite costly to make sure that this assumption is satisfied throughout the Buchberger Procedure: after appending a new generators, we must apply the interreduction on the system of generators and reconstruct the set of non-trivial obstructions, which is followed by the interreduction on the set of non-trivial obstructions again. Second, the interreduction on the set of non-trivial obstructions is intrinstically an interreduction process in the free $K\langle X\rangle$-bimodule F_s (see Corollary 5.1.14) together with a shrink map Shk defined on F_s, which can also be quite costly.

Now we shall overcome these drawbacks of applying the Interreduction Algorithm directly as given in Theorem 4.2.12. First of all, we shall deal with Assumption 4.2.4. As we have seen in Example 4.2.3, if the system of generators does not satisfy Assumption 4.2.4, the obstruction reduction can end with an obstruction without overlap, which violates our expectation that the obstruction reduction $\rightarrow_{\mathrm{Ob}}$ should be closed on $\cup_{1\le i\le j\le s}\mathrm{O}(i,j)$. Nonetheless, this should not cause any problem at all. By Lemma 4.1.10, the S-polynomial of obstruction without overlap has a weak Gröbner representation. Consequently, if a non-trivial obstruction $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')$ is reduced by another non-trivial obstruction $\mathrm{o}_{k,l}(w_k,w_k';w_l,w_l')$ to an obstruction $\mathrm{o}_{\mu,\nu}(w_\mu,w_\mu';w_\nu,w_\nu')$ without overlap, then, following the proof of Proposition 4.2.11.a, we can show that $S_{i,j}(w_i,w_i';w_j,w_j')$ has a weak Gröbner representation provided that $S_{k,l}(w_k,w_k';w_l,w_l')$ has a weak Gröbner representation. Henceforth we shall drop Assumption 4.2.4 safely.

Now the obstruction reduction reduces a non-trivial obstruction $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')$ by another non-trivial obstruction $\mathrm{o}_{k,l}(w_k,w_k';w_l,w_l')$ to an obstruction $\mathrm{o}_{\mu,\nu}(w_\mu,w_\mu';w_\nu,w_\nu')$, which is either a non-trivial obstruction or an obstruction without overlap. By Proposition 4.2.11.a, weak Gröbner representation of $S_{i,j}(w_i,w_i';w_j,w_j')$ depends on weak Gröbner representations of $S_{k,l}(w_k,w_k';w_l,w_l')$ and $S_{\mu,\nu}(w_\mu,w_\mu';w_\nu,w_\nu')$. Thus we are able to abandon $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')$ during the Buchberger Procedure if the S-polynomials $S_{k,l}(w_k,w_k';w_l,w_l')$ and $S_{\mu,\nu}(w_\mu,w_\mu';w_\nu,w_\nu')$ have weak Gröbner representations. In the following we shall optimize the Buchberger Procedure according to different types of obstruction reductions as in Definition 4.2.7.

Remark 4.2.14. Let $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}'),\mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}')\in\cup_{1\le i\le s'}\mathrm{O}(i,s')$ be two distinct non-trivial obstructions with some $w,w'\in\langle X\rangle$ satisfying $w_{s'i}=ww_{s'j}$ and $w_{s'i}'=w_{s'j}'w'$.

a) If $i<j$, then we have

$$\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}')=w\mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}')w'+\mathrm{o}_{i,j}(w_i,w_i';ww_j,w_j'w').$$

Following the proof of Proposition 4.2.11.a, we can show that the S-polynomial of $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}')$ has a weak Gröbner representation if the S-polynomials of $\mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}'),\mathrm{o}_{i,j}(w_i,w_i';ww_j,w_j'w')$ have weak Gröbner representations.

Clearly $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') >_\tau \mathrm{o}_{i,j}(w_i,w_i';ww_j,w_j'w')$. Further, if $ww' \neq 1$, we have $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') >_\tau \mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}')$ by $w_{s'i}\epsilon_{s'}w_{s'i}' = ww_{s'j}\epsilon_{s'}w_{s'j}'w'$ $>_\tau w_{s'j}\epsilon_{s'}w_{s'j}'$.

b) If $i > j$, then we have

$$\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') = w\mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}')w' - \mathrm{o}_{j,i}(ww_j,w_j'w';w_i,w_i').$$

The S-polynomial of $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}')$ has a weak Gröbner representation if the S-polynomials of $\mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}'), \mathrm{o}_{j,i}(ww_j,w_j'w';w_i,w_i')$ have weak Gröbner representations. Clearly $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') >_\tau \mathrm{o}_{j,i}(ww_j,w_j'w';w_i,w_i')$. Moreover, by $w_{s'i}\epsilon_{s'}w_{s'i}' = ww_{s'j}\epsilon_{s'}w_{s'j}'w'$ we have $w_i\mathrm{LT}_\sigma(g_i)w_i' = w_{s'i}\mathrm{LT}_\sigma(g_{s'})w_{s'i}'$ $= ww_{s'j}\mathrm{LT}_\sigma(g_{s'})w_{s'j}'w' = ww_j\mathrm{LT}_\sigma(g_j)w_j'w'$. Then, from $i > j$, it follows that $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') >_\tau w\mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}')w' \geq_\tau \mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}')$.

c) If $i = j$, then we have

$$\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') = w\mathrm{o}_{i,s'}(w_j,w_j';w_{s'j},w_{s'j}')w' + \mathrm{o}_{i,i}(w_i,w_i';ww_j,w_j'w').$$

The S-polynomial of $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}')$ has a weak Gröbner representation if the S-polynomials of $\mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}'), \mathrm{o}_{i,i}(w_i,w_i';ww_j,w_j'w')$ have weak Gröbner representations. Clearly $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') >_\tau \mathrm{o}_{i,i}(w_i,w_i';ww_j,w_j'w')$. Moreover, if $ww' \neq 1$ or $ww' = 1$ and $w_i >_\sigma w_j$, it is easy to verify that $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}') >_\tau \mathrm{o}_{i,s'}(w_j,w_j';w_{s'j},w_{s'j}')$.

With the investigations as in Remark 4.2.14, we can remove from $\cup_{1\leq i\leq s'}\mathrm{O}(i,s')$ some obstructions as follows.

Proposition 4.2.15. *Suppose that* $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}'), \mathrm{o}_{j,s'}(w_j,w_j';w_{s'j},w_{s'j}')$ *are two non-trivial obstructions in* $\cup_{1\leq i\leq s'}\mathrm{O}(i,s')$ *such that there exist some* $w,w' \in \langle X\rangle$ *satisfying* $w_{s'i} = ww_{s'j}$ *and* $w_{s'i}' = w_{s'j}'w'$. *Then* $\mathrm{o}_{i,s'}(w_i,w_i';w_{s'i},w_{s'i}')$ *can be removed from* $\cup_{1\leq i\leq s'}\mathrm{O}(i,s')$ *in the execution of the Buchberger Procedure if one of the following conditions is satisfied.*

a) $i > j$.

b) $i \leq j$ *and* $ww' \neq 1$.

c) $i = j$ *and* $ww' = 1$ *and* $w_i >_\sigma w_j$.

Proof. Note that condition a) corresponds to Remark 4.2.14.b, while conditions b) and c) correspond to Remarks 4.2.14.a and 4.2.14.c. Moreover, according to Remark 4.2.14, $\mathrm{o}_{i,s'}(w_i, w'_i; w_{s'i}, w'_{s'i})$ can be represented as

$$\mathrm{o}_{i,s'}(w_i, w'_i; w_{s'i}, w'_{s'i}) = w\mathrm{o}_{j,s'}(w_j, w'_j; w_{s'j}, w'_{s'j})w' + c\tilde{w}\mathrm{o}_{\mu,\nu}(w_\mu, w'_\mu; w_\nu, w'_\nu)\tilde{w}'$$

with $c \in K, \tilde{w}, \tilde{w}' \in \langle X\rangle, \mu = \min\{i,j\}, \nu = \max\{i,j\}$, and $\mathrm{o}_{\mu,\nu}(w_\mu, w'_\mu; w_\nu, w'_\nu)$ is either a non-trivial obstruction or an obstruction without overlap. If one of the conditions is satisfied, then $\mathrm{o}_{i,s'}(w_i, w'_i; w_{s'i}, w'_{s'i})$ is strictly larger than $\mathrm{o}_{j,s'}(w_j, w'_j; w_{s'j}, w'_{s'j})$ and $\mathrm{o}_{\mu,\nu}(w_\mu, w'_\mu; w_\nu, w'_\nu)$. Following the proof of Proposition 4.2.11.a, we can show that if $S_{j,s'}(w_j, w'_j; w_{s'j}, w'_{s'j})$ and $S_{\mu,\nu}(w_\mu, w'_\mu; w_\nu, w'_\nu)$ have weak Gröbner representations then $S_{i,s'}(w_i, w'_i; w_{s'i}, w'_{s'i})$ also has a weak Gröbner representation. Moreover, if $\mathrm{o}_{\mu,\nu}(w_\mu, w'_\mu; w_\nu, w'_\nu)$ has no overlap, then, by Lemma 4.1.10, $S_{\mu,\nu}(w_\mu, w'_\mu; w_\nu, w'_\nu)$ has a weak Gröbner representation. The conclusion follows from Proposition 4.1.2 and Theorem 4.1.14. □

Remark 4.2.16. Now we consider the obstruction reduction in the case of Definition 4.2.7.d. Let $\mathrm{o}_{i,j}(w_i, w'_i; w_{ji}, w'_{ji}) \in \cup_{1\le i\le j\le s'-1}\mathrm{O}(i,j)$ and $\mathrm{o}_{j,s'}(w_{js'}, w'_{js'}; w_{s'}, w'_{s'}) \in \cup_{1\le j\le s'}\mathrm{O}(j,s')$ with some $w, w' \in \langle X\rangle$ satisfying $w_{js'} = ww_{ji}$ and $w'_{js'} = w'_{ji}w'$. Then we have

$$\mathrm{o}_{j,s'}(w_{js'}, w'_{js'}; w_{s'}, w'_{s'}) = -w\mathrm{o}_{i,j}(w_i, w'_i; w_{ji}, w'_{ji})w' + \mathrm{o}_{i,s'}(ww_i, w'_iw'; w_{s'}, w'_{s'}).$$

The S-polynomial of $\mathrm{o}_{j,s'}(w_{js'}, w'_{js'}; w_{s'}, w'_{s'})$ has a weak Gröbner representation if the S-polynomials of $\mathrm{o}_{i,j}(w_i, w'_i; w_{ji}, w'_{ji}), \mathrm{o}_{i,s'}(ww_i, w'_iw'; w_{s'}, w'_{s'})$ have weak Gröbner representations, and $\mathrm{o}_{j,s'}(w_{js'}, w'_{js'}; w_{s'}, w'_{s'}) >_\tau \mathrm{o}_{i,s'}(ww_i, w'_iw'; w_{s'}, w'_{s'})$. Moreover, since $w_{s'}\epsilon_{s'}w'_{s'} >_\tau w_{js'}\epsilon_j w'_{js'} = ww_{ji}\epsilon_j w'_{ji}w \ge_\tau w_{ji}\epsilon_j w'_{ji}$, we have $\mathrm{o}_{j,s'}(w_{js'}, w'_{js'}; w_{s'}, w'_{s'})$ $>_\tau \mathrm{o}_{i,j}(w_i, w'_i; w_{ji}, w'_{ji})$. Note that $\mathrm{o}_{i,s'}(ww_i, w'_iw'; w_{s'}, w'_{s'})$ is either an obstruction without overlap or a multiple of non-trivial obstruction $\mathrm{Shk}(\mathrm{o}_{i,s'}(ww_i, w'_iw'; w_{s'}, w'_{s'}))$. It suffices for us to consider only the situation that $\mathrm{o}_{i,s'}(ww_i, w'_iw'; w_{s'}, w'_{s'})$ is an obstruction without overlap, since the other situation has been considered in Proposition 4.2.15.

Proposition 4.2.17. *Suppose that* $\mathrm{o}_{j,s'}(w_{js'}, w'_{js'}; w_{s'}, w'_{s'})$ *is a non-trivial obstruction in* $\cup_{1\le i\le s'}\mathrm{O}(i,s')$ *and* $\mathrm{o}_{i,j}(w_i, w'_i; w_{ji}, w'_{ji})$ *is a non-trivial obstruction in* $\cup_{1\le i\le j\le s'-1}\mathrm{O}(i,j)$ *such that there exist some* $w, w' \in \langle X\rangle$ *satisfying* $w_{js'} = ww_{ji}$ *and* $w'_{js} = w'_{ji}w'$. *If* ww_i *is a multiple of* $w_{s'}\mathrm{LT}_\sigma(g_{s'})$ *or* w'_iw' *is a multiple of* $\mathrm{LT}_\sigma(g_{s'})w'_{s'}$, *then* $\mathrm{o}_{j,s'}(w_{js'}, w'_{js'};$ $w_{s'j}, w'_{s'j})$ *can be removed from* $\cup_{1\le i\le s'}\mathrm{O}(i,s')$ *in the execution of the Buchberger Procedure.*

Proof. Note that if $S_{i,j}(w_i, w_i'; w_{ji}, w_{ji}'), S_{i,s'}(ww_i, w_i'w'; w_{s'}, w_{s'}')$ have weak Gröbner representations, then so does $S_{j,s'}(w_{js'}, w_{js'}'; w_{s'}, w_{s'}')$. Also note that ww_i is a multiple of $w_{s'}\mathrm{LT}_\sigma(g_{s'})$ or $w_i'w'$ is a multiple of $\mathrm{LT}_\sigma(g_{s'})w_{s'}'$ implies that the obstruction $\mathrm{o}_{i,s'}(ww_i, w_i'w'; w_{s'}, w_{s'}')$ has no overlap. By Lemma 4.1.10, $S_{i,s'}(ww_i, w_i'w'; w_{s'}, w_{s'}')$ has a weak Gröbner representation. Then the conclusion follows from Proposition 4.1.2 and Theorem 4.1.14. □

By now we have reduced non-trivial obstructions in $\cup_{1\le i\le s'}\mathrm{O}(i, s')$ with the aid of obstructions in $\cup_{1\le i\le j\le s'-1}\mathrm{O}(i, j)$. We shall also reduce non-trivial obstructions in $\cup_{1\le i\le j\le s'-1}\mathrm{O}(i, j)$ with the aid of obstructions in $\cup_{1\le i\le s'}\mathrm{O}(i, s')$. Intuitively, we are able to reduce a non-trivial obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\le i\le j\le s'-1}\mathrm{O}(i, j)$ by some non-trivial obstruction $\mathrm{o}_{k,s'}(w_k, w_k'; w_{s'}, w_{s'}') \in \cup_{1\le i\le s'}\mathrm{O}(i, s')$ if $k = i$ and $w_i\epsilon_i w_i'$ is a multiple of $w_k\epsilon_i w_k'$ or $k = j$ and $w_j\epsilon_j w_j'$ is a multiple of $w_k\epsilon_j w_k'$. Then as what we did in Definition 4.2.7, we represent $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ as a linear combination of some obstructions $\mathrm{o}_{i,s'}(w_{is'}, w_{is'}'; w_{s'i}, w_{s'i}'), \mathrm{o}_{j,s'}(w_{js'}, w_{js'}'; w_{s'j}, w_{s'j}') \in \cup_{1\le i\le s'}\mathrm{O}(i, s')$ with the property that $w_j\mathrm{LT}_\sigma(g_j)w_j' = w_{s'i}\mathrm{LT}_\sigma(g_{s'})w_{s'i}' = w_{s'j}\mathrm{LT}_\sigma(g_{s'})w_{s'j}'$. Actually, the property of the representation gives a sufficient condition for this kind of reduction. More precisely, if $w_j\mathrm{LT}_\sigma(g_j)w_j'$ is a multiple of $\mathrm{LT}_\sigma(g_{s'})$, i.e. there exist some $w_{s'}, w_{s'}' \in \langle X\rangle$ such that $w_j\mathrm{LT}_\sigma(g_j)w_j' = w_{s'}\mathrm{LT}_\sigma(g_{s'})w_{s'}'$, then we have

$$\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') = \mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}') - \mathrm{o}_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}')$$

where $\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}')$ is either an obstruction without overlap or a multiple of non-trivial obstruction in $\cup_{1\le i\le s'}\mathrm{O}(i, s')$, and similarly $\mathrm{o}_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}')$ is either an obstruction without overlap or a multiple of non-trivial obstruction in $\cup_{1\le i\le s'}\mathrm{O}(i, s')$. Following the proof of Proposition 4.2.11.a, we can show that if $S_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}')$ and $S_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}')$ have weak Gröbner representation then so does $S_{i,j}(w_i, w_i'; w_j, w_j')$.

Proposition 4.2.18. *Suppose that $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ is a non-trivial obstruction in $\cup_{1\le i\le j\le s'-1}\mathrm{O}(i, j)$. Then $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ can be removed from $\cup_{1\le i\le j\le s'-1}\mathrm{O}(i, j)$ in the execution of the Buchberger Procedure if the following conditions are satisfied.*

a) There are $w_{s'}, w_{s'}' \in \langle X\rangle$ such that $w_j\mathrm{LT}_\sigma(g_j)w_j' = w_{s'}\mathrm{LT}_\sigma(g_{s'})w_{s'}'$.

b) Under condition a), either $\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}')$ is an obstruction without overlap or the non-trivial obstruction $\mathrm{Shk}(\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}'))$ is in $\cup_{1\le i\le s'}\mathrm{O}(i, s')$.

c) Under condition a), either $\mathrm{o}_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}')$ is an obstruction without overlap or the non-trivial obstruction $\mathrm{Shk}(\mathrm{o}_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}'))$ is in $\cup_{1\le i\le s'}\mathrm{O}(i, s')$.

Proof. This follows from Lemma 4.1.10, Proposition 4.1.2, and Theorem 4.1.14. □

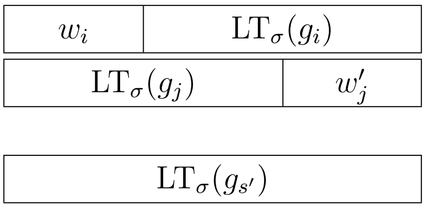
The following two remarks show that, unlike in Propositions 4.2.15 and 4.2.17, under the assumption of Proposition 4.2.18 we cannot guarantee that both non-trivial obstructions $\mathrm{Shk}(\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}'))$ and $\mathrm{Shk}(\mathrm{o}_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}'))$ are strictly smaller than $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ with respect to τ. We would like to mention that Remark 4.2.19 covers the presentation of useless pairs given by T. Mora [55].

Remark 4.2.19. (Left Obstruction) Let $i, j \in \{1, \ldots, s'-1\}$ and $i \leq j$. Suppose that the polynomials $g_i, g_j, g_{s'} \in K\langle X\rangle$ are monic and $w_i\epsilon_i - \epsilon_j w_j' \in \mathrm{O}(i,j)$ is a non-trivial obstruction with $w_i, w_j' \in \langle X\rangle \setminus \{1\}$. Let $w_i \mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(g_j)w_j' = w\mathrm{LT}_\sigma(g_{s'})w'$ with $w, w' \in \langle X\rangle$. We shall illustrate all possibilities for $\mathrm{Shk}(\mathrm{o}_{i,s'}(w_i, w_i'; w, w'))$ and $\mathrm{Shk}(\mathrm{o}_{j,s'}(w_j, w_j'; w, w'))$ as follows.

Case 1) Let $w = w' = 1$, i.e. $w_i\mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(g_j)w_j' = \mathrm{LT}_\sigma(g_{s'})$. Then we have

$$w_i\epsilon_i - \epsilon_j w_j' = (w_i\epsilon_i - \epsilon_{s'}) - (\epsilon_j w_j' - \epsilon_{s'})$$

with $w_i\epsilon_i - \epsilon_{s'} \in \mathrm{O}(i, s'), \epsilon_j w_j' - \epsilon_{s'} \in \mathrm{O}(j, s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w_j' <_\tau w_i\epsilon_i - \epsilon_{s'}$ and $w_i\epsilon_i - \epsilon_j w_j' <_\tau \epsilon_j w_j' - \epsilon_{s'}$.

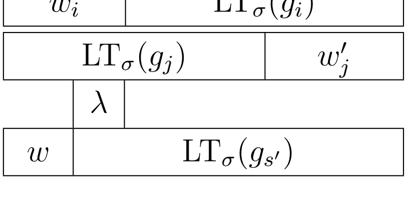

w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w_j'
$\mathrm{LT}_\sigma(g_{s'})$

Case 2) Let $w \neq 1, w' = 1$, i.e. $w_i\mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(g_j)w_j' = w\mathrm{LT}_\sigma(g_{s'})$.

Case 2.1) If $w_i = w\lambda$ with $\lambda \in \langle X\rangle$, then we have

$$w_i\epsilon_i - \epsilon_j w_j' = w(\lambda\epsilon_i - \epsilon_{s'}) - (\epsilon_j w_j' - w\epsilon_{s'})$$

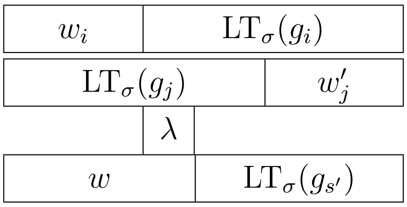
with $\lambda\epsilon_i - \epsilon_{s'} \in \mathrm{O}(i, s'), \epsilon_j w_j' - w\epsilon_{s'} \in \mathrm{O}(j, s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w_j' >_\tau \lambda\epsilon_i - \epsilon_{s'}$ and $w_i\epsilon_i - \epsilon_j w_j' <_\tau \epsilon_j w_j' - w\epsilon_{s'}$.


w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w_j'
λ
w
$\mathrm{LT}_\sigma(g_{s'})$

Case 2.2) If $w = w_i\lambda$ with $\lambda \in \langle X\rangle$ and $\mathrm{len}(w) < \mathrm{len}(\mathrm{LT}_\sigma(g_j))$, then we have

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \lambda\epsilon_{s'}) - (\epsilon_j w'_j - w\epsilon_{s'})$$

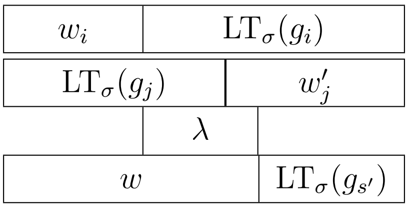
with $\epsilon_i - \lambda\epsilon_{s'} \in \mathrm{O}(i,s'), \epsilon_j w'_j - w\epsilon_{s'} \in \mathrm{O}(j,s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \lambda\epsilon_{s'}$ and $w_i\epsilon_i - \epsilon_j w'_j <_\tau \epsilon_j w'_j - w\epsilon_{s'}$.


w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
w
$\mathrm{LT}_\sigma(g_{s'})$

Case 2.3) If $w = w_i\lambda$ with $\lambda \in \langle X\rangle$ and $\mathrm{len}(w) \geq \mathrm{len}(\mathrm{LT}_\sigma(g_j))$, then $\mathrm{LT}_\sigma(g_j)$ and $\mathrm{LT}_\sigma(g_{s'})$ have no overlap. We have

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \lambda\epsilon_{s'}) - (\epsilon_j w'_j - w\epsilon_{s'})$$

with $\epsilon_i - \lambda\epsilon_{s'} \in \mathrm{O}(i,s'), \epsilon_j w'_j - w\epsilon_{s'} \in \mathrm{o}(j,s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \lambda\epsilon_{s'}$.


w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
w
$\mathrm{LT}_\sigma(g_{s'})$

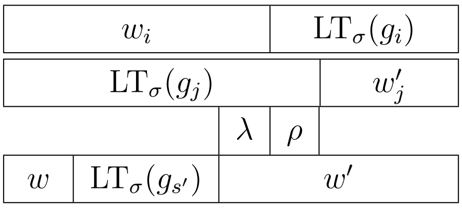
Case 3) Let $w = 1, w' \neq 1$, i.e. $w_i\mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(g_j)w'_j = \mathrm{LT}_\sigma(g_{s'})w'$. Similar to Case 2).

Case 4) Let $w \neq 1, w' \neq 1$, i.e. $w_i\mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(g_j)w'_j = w\mathrm{LT}_\sigma(g_{s'})w'$.

Case 4.1) If $w_i = w\mathrm{LT}_\sigma(g_{s'})\lambda$ with $\lambda \in \langle X\rangle$, i.e. $\mathrm{LT}_\sigma(g_{s'})$ is a subword of w_i, then $\mathrm{LT}_\sigma(g_i)$ and $\mathrm{LT}_\sigma(g_{s'})$ have no overlap. Let $\mathrm{LT}_\sigma(g_i)$ and $\mathrm{LT}_\sigma(g_j)$ have an overlap at $\rho \in \langle X\rangle$. Then we have

$$w_i\epsilon_i - \epsilon_j w'_j = w(\mathrm{LT}_\sigma(g_{s'})\lambda\epsilon_i - \epsilon_{s'}w') - (\epsilon_j - w\epsilon_{s'}\lambda\rho)w'_j$$

with $\mathrm{LT}_\sigma(g_{s'})\lambda\epsilon_i - \epsilon_{s'}w' \in \mathrm{o}(i,s'), \epsilon_j - w\epsilon_{s'}\lambda\rho \in \mathrm{O}(j,s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j - w\epsilon_{s'}\lambda\rho$.

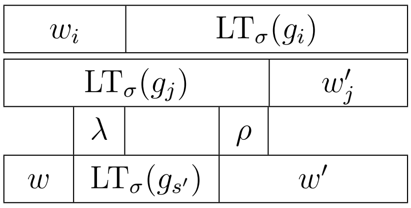

w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Case 4.2) If $w'_j = \lambda \mathrm{LT}_\sigma(g_{s'})w'$ with $\lambda \in \langle X\rangle$, i.e. $\mathrm{LT}_\sigma(g_{s'})$ is a subword of w'_j, then $\mathrm{LT}_\sigma(g_j)$ and $\mathrm{LT}_\sigma(g_{s'})$ have no overlap. Similar to Case 4.1).

Case 4.3) If $w_i = w\lambda, w' = \rho w'_j$ with $\lambda, \rho \in \langle X\rangle$, then we have

$$w_i\epsilon_i - \epsilon_j w'_j = w(\lambda\epsilon_i - \epsilon_{s'}w') - (\epsilon_j - w\epsilon_{s'}\rho)w'_j$$

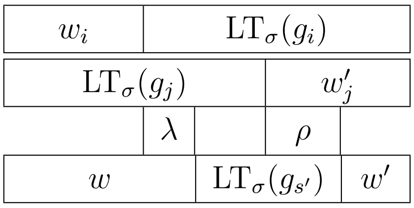
with $\lambda\epsilon_i - \epsilon_{s'}w' \in \mathrm{O}(i,s'), \epsilon_j - w\epsilon_{s'}\rho \in \mathrm{O}(j,s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w'_j >_\tau \lambda\epsilon_i - \epsilon_{s'}w'$ and $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j - w\epsilon_{s'}\rho$.


w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Case 4.4) If $w = w_i\lambda, w'_j = \rho w'$ with $\lambda, \rho \in \langle X\rangle$, then we have

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \lambda\epsilon_{s'}w') - (\epsilon_j\rho - w\epsilon_{s'})w'$$

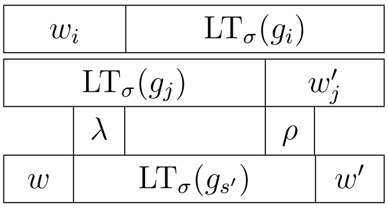
with $\epsilon_i - \lambda\epsilon_{s'}w' \in \mathrm{O}(i,s'), \epsilon_j\rho - w\epsilon_{s'} \in \mathrm{O}(j,s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \lambda\epsilon_{s'}w'$ and $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j\rho - w\epsilon_{s'}$.


w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Case 4.5) If $w_i = w\lambda, w'_j = \rho w'$ with $\lambda, \rho \in \langle X\rangle$, then we have

$$w_i\epsilon_i - \epsilon_j w'_j = w(\lambda\epsilon_i - \epsilon_{s'}w') - (\epsilon_j\rho - w\epsilon_{s'})w'$$

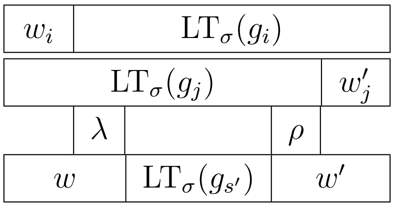
with $\lambda\epsilon_i - \epsilon_{s'}w' \in \mathrm{O}(i,s'), \epsilon_j\rho - w\epsilon_{s'} \in \mathrm{O}(j,s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w'_j >_\tau \lambda\epsilon_i - \epsilon_{s'}w'$ and $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j\rho - w\epsilon_{s'}$.


w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Case 4.6) If $w = w_i\lambda, w' = \rho w'_j$ with $\lambda, \rho \in \langle X\rangle$, then we have

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \lambda\epsilon_{s'}w') - (\epsilon_j - w\epsilon_{s'}\rho)w'_j$$

with $\epsilon_i - \lambda\epsilon_{s'}w' \in \mathrm{O}(i,s'), \epsilon_j - w\epsilon_{s'}\rho \in \mathrm{O}(j,s')$. Moreover, we have $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \lambda\epsilon_{s'}w'$ and $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j - w\epsilon_{s'}\rho$.

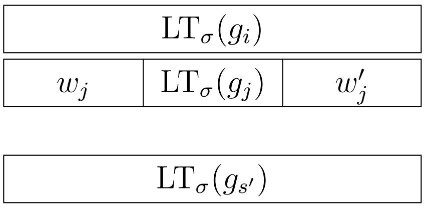

w_i
$\mathrm{LT}_\sigma(g_i)$
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Remark 4.2.20. (Center Obstruction) Let $i, j \in \{1, \dots, s'-1\}$ and $i \leq j$. Suppose that the polynomials $g_i, g_j, g_{s'} \in K\langle X\rangle$ are monic and $\epsilon_i - w_j\epsilon_j w'_j \in \mathrm{O}(i,j)$ is a non-trivial obstruction with $w_i, w'_j \in \langle X\rangle$. Let $\mathrm{LT}_\sigma(g_i) = w_j\mathrm{LT}_\sigma(g_j)w'_j = w\mathrm{LT}_\sigma(g_{s'})w'$ with $w, w' \in \langle X\rangle$. We shall illustrate all possibilities for $\mathrm{Shk}(\mathrm{o}_{i,s'}(w_i, w'_i; w, w'))$ and $\mathrm{Shk}(\mathrm{o}_{j,s'}(w_j, w'_j; w, w'))$ as follows.

Case 1) Let $w = w' = 1$, i.e. $\mathrm{LT}_\sigma(g_i) = w_j\mathrm{LT}_\sigma(g_j)w'_j = \mathrm{LT}_\sigma(g_{s'})$. Then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - \epsilon_{s'}) - (wj\epsilon_j w'_j - \epsilon_{s'})$$

with $\epsilon_i - \epsilon_{s'} \in \mathrm{o}(i, s'), wj\epsilon_j w'_j - \epsilon_{s'} \in \mathrm{O}(i, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - \epsilon_{s'}$ and $\epsilon_i - w_j\epsilon_j w'_j <_\tau w_j\epsilon_j w'_j - \epsilon_{s'}$.

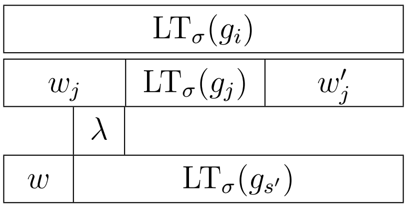

$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
$\mathrm{LT}_\sigma(g_{s'})$

Case 2) Let $w \neq 1, w' = 1$, i.e. $\mathrm{LT}_\sigma(g_i) = w_j\mathrm{LT}_\sigma(g_j)w'_j = w\mathrm{LT}_\sigma(g_{s'})$.

Case 2.1) If $w_j = w\lambda$ with $\lambda \in \langle X\rangle$, then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}) - w(\lambda\epsilon_j w'_j - \epsilon_{s'})$$

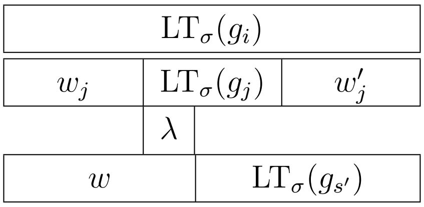
with $\epsilon_i - w\epsilon_{s'} \in \mathrm{O}(i, s'), \lambda\epsilon_j w'_j - \epsilon_{s'} \in \mathrm{O}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}$ and $\epsilon_i - w_j\epsilon_j w'_j >_\tau \lambda\epsilon_j w'_j - \epsilon_{s'} \in \mathrm{O}(j, s')$.


$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
w
$\mathrm{LT}_\sigma(g_{s'})$

Case 2.2) If $w = w_j\lambda$ with $\lambda \in \langle X\rangle$, then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}) - w_j(\epsilon_i w'_j - \lambda\epsilon_{s'})$$

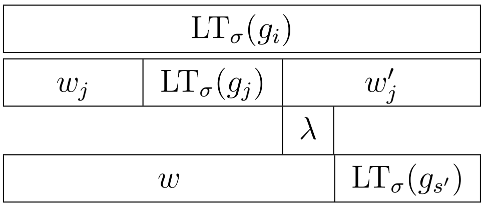
with $\epsilon_i - w\epsilon_{s'} \in \mathrm{O}(i, s'), \epsilon_i w'_j - \lambda\epsilon_{s'} \in \mathrm{O}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}$, and $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_i w'_j - \lambda\epsilon_{s'}$.


$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
w
$\mathrm{LT}_\sigma(g_{s'})$

Case 2.3) If $w = w_j\mathrm{LT}_\sigma(g_j)\lambda$ with $\lambda \in \langle X\rangle$, then $\mathrm{LT}_\sigma(g_j)$ and $\mathrm{LT}_\sigma(g_{s'})$ have no overlap. Then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}) - w_j(\epsilon_j w'_j - \mathrm{LT}_\sigma(g_j)\lambda\epsilon_{s'})$$

with $\epsilon_i - w\epsilon_{s'} \in \mathrm{O}(i, s'), \epsilon_j w'_j - \mathrm{LT}_\sigma(g_j)\lambda\epsilon_{s'} \in \mathrm{o}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}$.


$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
w
$\mathrm{LT}_\sigma(g_{s'})$

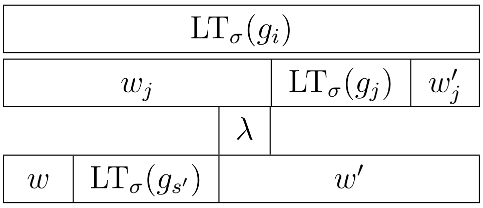
Case 3) Let $w = 1, w' \neq 1$, i.e. $\mathrm{LT}_\sigma(g_i) = w_j\mathrm{LT}_\sigma(g_j)w'_j = \mathrm{LT}_\sigma(g_{s'})w'$. Similar to Case 2).

Case 4) Let $w \neq 1, w' \neq 1$, i.e. $\mathrm{LT}_\sigma(g_i) = w_j\mathrm{LT}_\sigma(g_j)w'_j = w\mathrm{LT}_\sigma(g_{s'})w'$.

Case 4.1) If $w_j = w\mathrm{LT}_\sigma(g_{s'})\lambda$ with $\lambda \in \langle X\rangle$, i.e. $\mathrm{LT}_\sigma(g_{s'})$ is a subword of w_j, then $\mathrm{LT}_\sigma(g_j)$ and $\mathrm{LT}_\sigma(g_{s'})$ have no overlap. Then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}w') - w(\mathrm{LT}_\sigma(g_{s'})\lambda\epsilon_j - \epsilon_{s'}\lambda\mathrm{LT}_\sigma(g_j))w'_j$$

with $\epsilon_i - w\epsilon_{s'}w' \in \mathrm{O}(i, s'), \mathrm{LT}_\sigma(g_{s'})\lambda\epsilon_j - \epsilon_{s'}\lambda\mathrm{LT}_\sigma(g_j) \in \mathrm{o}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}w'$.

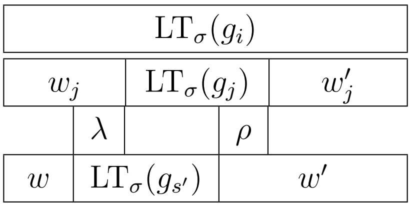

$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Case 4.2) If $w'_j = \lambda\mathrm{LT}_\sigma(g_{s'})w'$ with $\lambda \in \langle X\rangle$, i.e. $\mathrm{LT}_\sigma(g_{s'})$ is a subword of w'_j, then $\mathrm{LT}_\sigma(g_j)$ and $\mathrm{LT}_\sigma(g_{s'})$ have no overlap. Similar to Case 4.1).

Case 4.3) If $w_j = w\lambda, w' = \rho w'_j$ with $\lambda, \rho \in \langle X\rangle$, then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}w') - w(\lambda\epsilon_j - \epsilon_{s'}\rho)w'_j$$

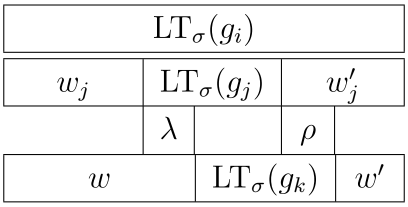
with $\epsilon_i - w\epsilon_{s'}w' \in \mathrm{O}(i, s'), \lambda\epsilon_j - \epsilon_{s'}\rho \in \mathrm{O}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}w'$ and $\epsilon_i - w_j\epsilon_j w'_j >_\tau \lambda\epsilon_j - \epsilon_{s'}\rho$.


$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Case 4.4) If $w = w_j\lambda, w'_j = \rho w'$ with $\lambda, \rho \in \langle X \rangle$, then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}w') - w_j(\epsilon_j\rho - \lambda\epsilon_{s'})w'$$

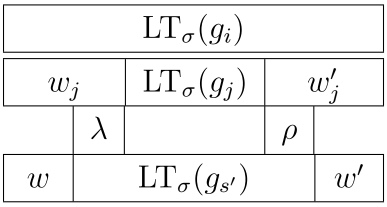
with $\epsilon_i - w\epsilon_{s'}w' \in \mathrm{O}(i, s'), \epsilon_j\rho - \lambda\epsilon_{s'} \in \mathrm{O}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}w'$ and $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_j\rho - \lambda\epsilon_{s'}$.


$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_k)$
w'

Case 4.5) If $w_j = w\lambda, w'_j = \rho w'$ with $\lambda, \rho \in \langle X \rangle$, then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}w') - w(\lambda\epsilon_j\rho - \epsilon_{s'})w'$$

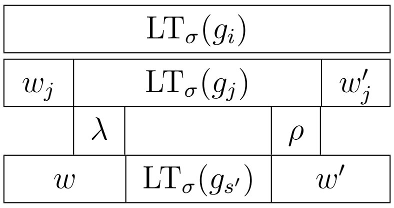
with $\epsilon_i - w\epsilon_{s'}w' \in \mathrm{O}(i, s'), \lambda\epsilon_j\rho - \epsilon_{s'} \in \mathrm{O}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}w'$ and $\epsilon_i - w_j\epsilon_j w'_j >_\tau \lambda\epsilon_j\rho - \epsilon_{s'}$.


$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Case 4.6) If $w = w_j\lambda, w' = \rho w'_j$ with $\lambda, \rho \in \langle X \rangle$, then we have

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_{s'}w') - w_j(\epsilon_j - \lambda\epsilon_{s'}\rho)w'_j$$

with $\epsilon_i - w\epsilon_{s'}w' \in \mathrm{O}(i, s'), \epsilon_j - \lambda\epsilon_{s'}\rho \in \mathrm{O}(j, s')$. Moreover, we have $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_{s'}w'$ and $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_j - \lambda\epsilon_{s'}\rho$.


$\mathrm{LT}_\sigma(g_i)$
w_j
$\mathrm{LT}_\sigma(g_j)$
w'_j
λ
ρ
w
$\mathrm{LT}_\sigma(g_{s'})$
w'

Remark 4.2.21. To apply Propositions 4.2.15, 4.2.17 and 4.2.18 to remove unnecessary obstructions, it is crucial to make sure that the S-polynomials of those removed obstructions have weak Gröbner representations.

a) Propositions 4.2.15 and 4.2.17 remove unnecessary non-trivial obstruction, say $\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}')$, from $\cup_{1\leq i\leq s'}\mathrm{O}(i, s')$. The weak Gröbner representation of $S_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}')$ depends on the weak Gröbner representations of the S-polynomials of two smaller obstructions in $\cup_{1\leq i\leq j\leq s'}\mathrm{o}(i, j)$.

b) Proposition 4.2.18 removes unnecessary obstruction, say $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$, from $\cup_{1\leq i\leq j\leq s'-1}\mathrm{O}(i, j)$. The weak Gröbner representation of $S_{i,j}(w_i, w_i'; w_j, w_j')$ depends on the weak Gröbner representations of the S-polynomials of two obstructions, say $\mathrm{o}_{k,s'}(w_k, w_k'; w_{s'k}, w_{s'k}')$ and $\mathrm{o}_{l,s'}(w_l, w_l'; w_{s'l}, w_{s'l}')$, in $\cup_{1\leq i\leq s'}\mathrm{o}(i, s')$, which are not necessarily smaller than $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ according to Examples 4.2.19 and 4.2.20. Hence before applying Proposition 4.2.18, it is important to make sure the obstructions $\mathrm{o}_{k,s'}(w_k, w_k'; w_{s'k}, w_{s'k}')$ and $\mathrm{o}_{l,s'}(w_l, w_l'; w_{s'l}, w_{s'l}')$ are still in $\cup_{1\leq i\leq s'}\mathrm{O}(i, s')$.

Observe that Propositions 4.2.15, 4.2.17 and 4.2.18 are actually generalizations of the Gebauer-Möller Installation (see [33]) in free monoid rings.

Having Propositions 4.2.15, 4.2.17 and 4.2.18 in hand, we shall improve the Buchberger Procedure as follows.

Theorem 4.2.22. (Improved Buchberger Procedure I) *In the setting of Theorem 4.1.14, we replace step 4) by the following sequence of instructions.*

4a) Increase s' by one. Append $g_{s'} = S'$ to $\mathcal{G}$, and form the set of non-trivial obstructions $\mathrm{O}(s') = \cup_{1\leq i\leq s'}\mathrm{O}(i, s')$.

4b) Remove from $\mathrm{O}(s')$ all obstructions $\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'i}, w_{s'i}')$ such that there exists $\mathrm{o}_{j,s'}(w_j, w_j'; w_{s'j}, w_{s'j}')$ in $\mathrm{O}(s')$ with the properties that there exist some $w, w' \in \langle X\rangle$ such that $w_{s'i} = ww_{s'j}, w_{s'i}' = w_{s'j}'w'$, and such that $i > j$, or $i \leq j$ and $ww' \neq 1$, or $i = j$ and $ww' = 1$ and $w_i >_\sigma w_j$.

4c) Remove from $\mathrm{O}(s')$ all obstructions $\mathrm{o}_{j,s'}(w_{js'}, w_{js'}'; w_{s'}, w_{s'}')$ such that there exists $\mathrm{o}_{i,j}(w_i, w_i'; w_{ji}, w_{ji}') \in B$ with the properties that there exist some $w, w' \in \langle X\rangle$ such that $w_{js'} = ww_{ji}, w_{js'}' = w_{ji}'w'$, and such that $\mathrm{o}_{i,s'}(ww_i, w_i'w'; w_{s'}, w_{s'}')$ has no overlap.

4d) Remove from B all obstructions $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ such that there exist $w, w' \in \langle X\rangle$ satisfying $w\mathrm{LT}_\sigma(g_{s'})w' = w_j\mathrm{LT}_\sigma(g_j)w_j'$, and such that the following conditions are satisfied.

(i) either $\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}')$ has no overlap or $\mathrm{Shk}(\mathrm{o}_{i,s'}(w_i, w_i'; w_{s'}, w_{s'}'))$ is in $\mathrm{O}(s')$.

(ii) either $\mathrm{o}_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}')$ has no overlap or $\mathrm{Shk}(\mathrm{o}_{j,s'}(w_j, w_j'; w_{s'}, w_{s'}'))$ is in $\mathrm{O}(s')$.

4f) Replace B by $B \cup \mathrm{O}(s')$ and continue with step 2).

Then the resulting set of instructions is a procedure that enumerates a σ-Gröbner basis $\mathcal{G}$ of I. If I has a finite σ-Gröber basis, it stops after finitely many steps and the resulting tuple $\mathcal{G}$ is a finite σ-Gröbner basis of I.

Proof. This follows from Theorem 4.1.14 and Propositions 4.2.15, 4.2.17 and 4.2.18. □

Now we shall present another optimization of the Buchberger Procedure related to redundant generators. Recall that, given a σ-Gröbner basis G of an ideal I, a polynomial $g \in G$ is called **redundant** if $G \setminus \{g\}$ is still a σ-Gröbner basis of I. Proposition 3.3.14 says that $g \in G$ is redundant if $\mathrm{LT}_\sigma(g)$ is a multiple of the leading term of some polynomial in $G \setminus \{g\}$. The following proposition allows us to delete redundant generators during the execution of the Buchberger Procedure.

Proposition 4.2.23. *Suppose that there exists an index $i \in \{1, \ldots, s'\}$ such that $\mathrm{LT}_\sigma(g_i)$ is a multiple of $\mathrm{LT}_\sigma(g_{s'+1})$. Then, after constructing the new set of obstructions, we can delete g_i from $\mathcal{G}$ in step 4) of the Buchberger Procedure.*

Proof. Without loss of generality, we may assume that during the Buchberger Procedure g_i is the only redundant generator which is detected by $g_{s'+1}$. Then there exist some $w, w' \in \langle X\rangle$ such that $\mathrm{LT}_\sigma(g_i) = w\mathrm{LT}_\sigma(g_{s'+1})w'$ and $\mathrm{o}_{i,s'+1}(1, 1; w, w')$ is appended to the set of obstructions. Let $\mathcal{G}$ be the resulting tuple of the Buchberger Procedure. Thus $g_i \notin \mathcal{G}$. Firstly, we prove that $\langle g_1, \ldots, g_i, \ldots, g_{s'}\rangle = \langle \mathcal{G}\rangle$. By the Buchberger Procedure, the polynomials in $\mathcal{G}$ are generated by $\{g_1, \ldots, g_i, \ldots, g_{s'}\}$ and hence we have $\langle \mathcal{G}\rangle \subseteq \langle g_1, \ldots, g_i, \ldots, g_{s'}\rangle$. To prove the other inclusion $\langle g_1, \ldots, g_i, \ldots, g_{s'}\rangle \subseteq \langle \mathcal{G}\rangle$, it suffices to show that $g_i \in \langle \mathcal{G}\rangle$. Since the Buchberger Procedure ensures that the S-polynomial of $\mathrm{o}_{i,s'+1}(1, 1; w, w')$ has a weak Gröbner basis in terms of $\mathcal{G}$, we have $\frac{1}{\mathrm{LC}_\sigma(g_i)}g_i - \frac{1}{\mathrm{LC}_\sigma(g_{s'+1})}wg_{s'+1}w' \in \langle \mathcal{G}\rangle$. Then $g_i \in \langle \mathcal{G}\rangle$ follows from the assumption that $g_{s'+1}\in\mathcal{G}$. Secondly, we prove that $\mathcal{G}$ is indeed a σ-Gröbner basis. Since the Buchberger Procedure ensures that all the S-polynomials of non-trivial obstructions in $\cup_{1\le k\le l\le|\mathcal{G}|}\mathrm{O}(k,l)$ with $k\neq i$ and $l\ge s'+1$ have weak Gröbner representations in terms of $\mathcal{G}$, it suffices to prove that, for every non-trivial obstruction $\mathrm{o}_{k,l}(w_k,w_k';w_l,w_l')\in\cup_{1\le k\le l\le s'}\mathrm{O}(k,l)$ with $k\neq i$ and $l\neq i$, its S-polynomial $S_{k,l}(w_k,w_k';w_l,w_l')$ has a weak representation in terms of $\mathcal{G}$. Note that the Buchberger Procedure ensures that $S_{k,l}(w_k,w_k';w_l,w_l')$ has a weak Gröbner basis in terms of $\mathcal{G}\cup\{g_i\}$. Thus there exist $g_{i_1},\dots,g_{i_\mu}\in\mathcal{G}\cup\{g_i\},w_1,\dots,w_\mu'\in\langle X\rangle$, and $c_1,\dots,c_\mu\in K\setminus\{0\}$ such that $S_{k,l}(w_k,w_k';w_l,w_l')=\sum_{s=1}^{\mu}c_sw_sg_{i_s}w_s'$ and $\mathrm{LT}_\sigma(w_kg_kw_k')>_\sigma\mathrm{LT}_\sigma(w_sg_{i_s}w_s')$ for all $s\in\{1,\dots,\mu\}$. If $g_i\notin\{g_{i_1},\dots,g_{i_\mu}\}$, then we are done. We assume that $g_i\in\{g_{i_1},\dots,g_{i_\mu}\}$. Since the Buchberger Procedure ensures that the S-polynomial $S_{i,s'+1}(1,1;w,w')$ has a weak Gröbner basis in terms of $\mathcal{G}$, there exist $\tilde{g}_{i_1},\dots,\tilde{g}_\nu\in\mathcal{G},\tilde{w}_1,\dots,\tilde{w}_\nu'\in\langle X\rangle$, and $\tilde{c}_1,\dots,\tilde{c}_\nu\in K\setminus\{0\}$ such that $\frac{1}{\mathrm{LC}_\sigma(g_i)}g_i-\frac{1}{\mathrm{LC}_\sigma(g_{s'+1})}wg_{s'+1}w'=\sum_{t=1}^{\nu}\tilde{c}_t\tilde{w}_t\tilde{g}_{i_t}\tilde{w}_t,\mathrm{LT}_\sigma(g_i)=\mathrm{LT}_\sigma(wg_{s'+1}w)$, and $\mathrm{LT}_\sigma(g_i)>_\sigma\mathrm{LT}_\sigma(\tilde{w}_t\tilde{g}_{i_t}\tilde{w}_t)$ for all $t\in\{1,\dots,\nu\}$. By substituting $g_i=\frac{\mathrm{LC}_\sigma(g_i)}{\mathrm{LC}_\sigma(g_{s'+1})}wg_{s'+1}w'+\sum_{t=1}^{\nu}\mathrm{LC}_\sigma(g_i)\tilde{c}_t\tilde{w}_t\tilde{g}_{i_t}\tilde{w}_t$ in the weak Gröbner representation of $S_{k,l}(w_k,w_k';w_l,w_l')$, we obtain a weak Gröbner representation of $S_{k,l}(w_k,w_k';w_l,w_l')$ in terms of $\mathcal{G}$. □

We should delete redundant generators cautiously, because we select obstructions using a fair strategy during the Buchberger Procedure and there may exist unselected obstructions that are the obstructions of redundant generators. Thus, we delay the deletion by marking each generator with a tag to indicate whether it is redundant. Moreover, as a preprocessing step we can apply interreduction on the system of generators at the beginning of the Buchberger Procedure to avoid redundancy in the system of generators.

Theorem 4.2.24. (Improved Buchberger Procedure II) *Let $G\subseteq K\langle X\rangle\setminus\{0\}$ be a finite set of polynomials which generates an ideal $I=\langle G\rangle$. Consider the following sequence of instructions.*

1) *Interreduce the system of generators G using the Interreduction Algorithm given in Theorem 3.2.8.*

2) *Let $\mathcal{G}$ be an associated tuple of G, let $s'=|\mathcal{G}|$, let $\mathcal{T}$ be the tuple $(t_1,\dots,t_{s'})$ with $t_i=\mathrm{true}$ for all $i\in\{1,\dots,s'\}$, and let $B=\cup_{1\le i\le j\le s'}\mathrm{O}(i,j)$.*

3) *If $B=\emptyset$, return the subtuple $\mathcal{G}'$ of $\mathcal{G}$ consisting of all polynomials g_i such that $t_i=\mathrm{true}$. If $B\neq\emptyset$, select an obstruction $\mathrm{o}_{i,j}(w_i,w_i';w_j,w_j')\in B$ using a fair*

strategy and delete it from B.

4) *Let $\mathcal{G}'$ be the subtuple of $\mathcal{G}$ consisting of the polynomials g_i such that $t_i = \mathrm{true}$. Compute the S-polynomial $S = S_{i,j}(w_i, w_i'; w_j, w_j')$ and its normal remainder $S' = \mathrm{NR}_{\sigma,\mathcal{G}'}(S)$. If $S' = 0$, continue with step 3).*

5) *Increase s' by one, append $g_{s'} = S'$ to the tuple $\mathcal{G}$, append $t_{s'} = true$ to the tuple $\mathcal{T}$, and append the set of non-trivial obstructions $\cup_{1\le i\le s', t_i=\mathrm{true}}\mathrm{O}(i, s')$ to the set B.*

6) *For every $i \in \{1, \dots, s'-1\}$, let $t_i = \mathrm{false}$ if $\mathrm{LT}_\sigma(g_i)$ is a multiple of $\mathrm{LT}_\sigma(g_{s'})$. Then continue with step 3).*

This is a procedure that enumerates a σ-Gröbner basis of I. If I has a finite σ-Gröber basis, it stops after finitely many steps and the resulting tuple is a finite σ-Gröbner basis of I.

Proof. This follows from Theorem 4.1.14 and Proposition 4.2.23. □

Corollary 4.2.25. *In the setting of Theorem 4.2.24, the Improved Buchberger Procedure II enumerates a minimal σ-Gröbner basis of the ideal I.*

Proof. Let G' be the resulting tuple of the Improved Buchberger Procedure II. We claim that the set $\mathrm{LT}_\sigma\{G'\}$ is the minimal system of generators of the leading term set $\mathrm{LT}_\sigma\{I\}$. It suffices to prove that $\mathrm{LT}_\sigma(g_i)$ is not a multiple of $\mathrm{LT}_\sigma(g_j)$ for all $g_i, g_j \in G'$ such that $g_i \neq g_j$. Let $g_i, g_j \in G'$ be two generators. If g_i, g_j are contained in the interreduced system of generators G in step 2) of Theorem 4.2.24, then by Definition 3.2.6 the claim is satisfied. Without loss of generality, we may assume that $i < j$. Note that g_j is the normal remainder of some S-polynomial with respect to a tuple of polynomials containing g_i. Thus $\mathrm{LT}_\sigma(g_j)$ is not a multiple of $\mathrm{LT}_\sigma(g_i)$ by Theorem 3.2.1.a. Conversely, $\mathrm{LT}_\sigma(g_i)$ is not a multiple of $\mathrm{LT}_\sigma(g_j)$ either. Otherwise, in step 6) of Theorem 4.2.24 we have $t_i = \mathrm{false}$ and hence $g_i \notin G'$, contradicting our assumption. Therefore $\mathrm{LT}_\sigma\{G'\}$ is the minimal system of generators of $\mathrm{LT}_\sigma\{I\}$ and G' is a minimal σ-Gröbner basis of I. □

We shall end this section with two examples.

Example 4.2.26. Consider the free monoid ring $\mathbb{Q}\langle a, b\rangle$ equipped with the admissible ordering $\sigma = \mathtt{LLex}$ on $\langle a, b\rangle$ such that $a >_\sigma b$. We take a list of finite generalized triangle groups from [64], Theorem 2.12 and construct a list of ideals as follows. Let $I_k = \langle G_k\rangle \subseteq \mathbb{Q}\langle a,b\rangle$ be the ideal generated by a set of polynomials $G_k \subseteq \mathbb{Q}\langle a,b\rangle$ for $k = 1,\dots,13$, where $G_1 = \{a^2-1, b^3-1, (ababab^2ab^2)^2-1\}, G_2 = \{a^2-1, b^3-1, (ababab^3)^3-1\}$, $G_3 = \{a^3-1, b^3-1, (abab^2)^2-1\}$, $G_4 = \{a^3-1, b^3-1, (aba^2b^2)^2-1\}$, $G_5 = \{a^2-1, b^5-1, (abab^2)^2-1\}$, $G_6 = \{a^2-1, b^5-1, (ababab^4)^2-1\}$, $G_7 = \{a^2-1, b^5-1, (abab^2ab^4)^2-1\}$, $G_8 = \{a^2-1, b^4-1, (ababab^3)^2-1\}$, $G_9 = \{a^2-1, b^3-1, (abab^2)^2-1\}$, $G_{10} = \{a^2-1, b^3-1, (ababab^2)^2-1\}$, $G_{11} = \{a^2-1, b^3-1, (abababab^2)^2-1\}$, $G_{12} = \{a^2-1, b^3-1, (ababab^2abab^2)^2-1\}$, $G_{13} = \{a^2-1, b^3-1, (ababababab^2ab^2)^2-1\}$. We compute σ-Gröbner bases of each ideal by the Improved Buchberger Procedure I and the Improved Buchberger Procedure II.

k	$\lvert Gb\rvert$	$\lvert SelObs\rvert$	$\lvert TolObs\rvert$	$\lvert Rule1\rvert$	$\lvert Rule2\rvert$	$\lvert RedGb\rvert$
1	60	247	6592	6122	223	35
2	131	530	30771	29752	489	96
3	49	194	2721	2397	130	40
4	66	262	5047	4544	241	28
5	36	119	1686	1466	101	21
6	199	880	51077	48994	1203	164
7	199	878	51285	49194	1213	164
8	52	190	3602	3216	196	37
9	11	31	150	106	13	5
10	22	75	741	624	42	15
11	30	117	1573	1373	83	21
12	96	365	16495	15741	389	70
13	220	1021	87507	85052	1434	194

Table 4.1: Computing Gröbner bases by the Improved Buchberger Procedure I

Table 4.1 lists the results computed by the Improved Buchberger Procedure I followed by the Interreduction Algorithm given in Theorem 3.2.8. Table 4.2 lists the results computed by the Improved Buchberger Procedures I and II, that is, a procedure combining Propositions 4.2.15, 4.2.17, 4.2.18, and 4.2.23. In the tables, $|Gb|$ is the number of generators returned by the procedure, $|SelObs|$ is the number of selected obstructions which is also the number of obstructions left after removing unnecessary obstructions, $|TolObs|$ is the total number of obstructions, $|Rule1|$ is the number of unnecessary obstructions detected by Propositions 4.2.15 and 4.2.17, $|Rule2|$ is the number of unnecessary obstructions detected by Proposition 4.2.18, $|RedGb|$ is the number of generators in the reduced σ-Gröbner basis, and $|ReduG|$ is the number of redundant generators detected by Proposition 4.2.23.

The results in the tables show that Propositions 4.2.15, 4.2.17 and 4.2.18 detect a large number of unnecessary obstructions. Observe that the numbers in column $|SelObs|$ of Tables 4.1 and 4.2 are mostly the same, while the numbers in columns $|TolObs|$ and $|Rule1|$ of Tables 4.1 and 4.2 have remarkable differences. This is because almost all unnecessary obstructions related to redundant generators are detected by the lemmas, especially by Propositions 4.2.15 and 4.2.17. Also note that the numbers in column $|RedGb|$ of Table 4.1 are equal to the numbers in column $|Gb|$ of Table 4.1. This coincidence verifies that for any ideal I the number of generators in the reduced σ-Gröbner basis and the number of generators in a minimal σ-Gröbner basis are equal.

k	$\lvert Gb\rvert$	$\lvert SelObs\rvert$	$\lvert TolObs\rvert$	$\lvert Rule1\rvert$	$\lvert Rule2\rvert$	$\lvert ReduG\rvert$
1	35	241	3456	3005	210	25
2	96	544	23419	22410	465	35
3	40	192	2268	1947	129	9
4	28	258	2693	2205	230	38
5	21	123	987	777	87	15
6	164	891	41950	39885	1174	35
7	164	884	42032	39953	1195	35
8	37	193	2420	2040	187	15
9	5	32	77	34	11	6
10	15	77	449	337	35	7
11	21	121	885	697	67	9
12	70	371	11615	10885	359	26
13	194	1023	73541	71130	1388	26

Table 4.2: Computing Gröbner bases by the Improved Buchberger Procedures I and II

As we have seen that Propositions 4.2.15, 4.2.17, 4.2.18 and 4.2.23 improve the Buchberger Procedure significantly, in the ApCoCoA package *gbmr* and in examples henceforth in this thesis we shall apply these optimizations wherever it is possible. The last example is taken from [55], where T. Mora used it to demonstrate that the selection strategy can affect the Buchberger Procedure in surprising ways. Unfortunately, T.

Mora made a mistake at the conclusion in the example and many authors cited it carelessly without noticing the error.

Example 4.2.27. Consider the free monoid ring $K\langle a,b,c,d,e,f\rangle$ equipped with the weight-lexicographic ordering $\sigma = \mathtt{WLex}$ defined by $(3,1,1,1,1,1) \in \mathbb{R}^6$ and $a <_{\mathtt{Lex}} b <_{\mathtt{Lex}} c <_{\mathtt{Lex}} d <_{\mathtt{Lex}} e <_{\mathtt{Lex}} f$, and the ideal $I \subseteq K\langle a,b,c,d,e,f\rangle$ generated by the set $\{f_1,f_2,f_3,f_4,f_5,f_6,f_7\}$, where $f_1 = ca-ac, f_2 = da-ad, f_3 = ba-b^2c, f_4 = be-b, f_5 = bf-b, f_6 = ef-b, f_7 = bcd$. We enumerate a σ-Gröbner basis of I. Note that $\mathrm{LT}_\sigma(f_1) = ca, \mathrm{LT}_\sigma(f_2) = da, \mathrm{LT}_\sigma(f_3) = ba, \mathrm{LT}_\sigma(f_4) = be, \mathrm{LT}_\sigma(f_5) = bf, \mathrm{LT}_\sigma(f_6) = ef$, $\mathrm{LT}_\sigma(f_7) = bcd$. We found the tuple and the set of non-trivial obstructions as follows.

$$\mathcal{G} = (f_1,\ldots,f_7),\ B = \{\mathrm{o}_{4,6}(1,f;b,1), \mathrm{o}_{2,7}(bc,1;1,a)\}$$

Now we have two possibilities to proceed with the computation, i.e. first select either the obstruction $\mathrm{o}_{4,6}(1,f;b,1)$ or the obstruction $\mathrm{o}_{2,7}(bc,1;1,a)$. We note that σ-degree of $\mathrm{o}_{2,7}(bc,1;1,a)$ is $bcda$ and σ-degree of $\mathrm{o}_{4,6}(1,f;b,1)$ is bed. In the following we consider two selection strategies. Firstly, we select the obstructions with maximal σ-degree.

1) Select $\mathrm{o}_{2,7}(bc,1;1,a)$ whose σ-degree is $bcda$. We have

$$S_{2,7}(bc,1;1,a) = -bcad,\ \mathrm{NR}_{\sigma,\mathcal{G}}(-bcad) = -b^2c^2d.$$

Let $f_8 = b^2c^2d$. Append f_8 to $\mathcal{G}$ and $\{\mathrm{o}_{2,8}(b^2c^2,1;1,a)\}$ to B. Then we have

$$\mathcal{G} = (f_1,\ldots,f_7,f_8),\ B = \{\mathrm{o}_{4,6}(1,f;b,1), \mathrm{o}_{2,8}(b^2c^2,1;1,a)\}.$$

2) Select $\mathrm{o}_{2,8}(b^2c^2,1;1,a)$ whose σ-degree is b^2c^2da. We have

$$S_{2,8}(b^2c^2,1;1,a) = -b^2c^2ad,\ \mathrm{NR}_{\sigma,\mathcal{G}}(-b^2c^2ad) = -b^3c^3d.$$

Let $f_9 = b^3c^3d$. Append f_9 to $\mathcal{G}$ and $\{\mathrm{o}_{2,9}(b^3c^3,1;1,a)\}$ to B. Then we have

$$\mathcal{G} = (f_1,\ldots,f_7,f_8,f_9),\ B = \{\mathrm{o}_{4,6}(1,f;b,1), \mathrm{o}_{2,9}(b^3c^3,1;1,a)\}.$$

It is easy to check that the procedure goes on forever. At stage k) we have

$$\mathcal{G} = (f_1,\ldots,f_7,f_8,\ldots,f_{7+k})$$

with $f_{7+i} = b^{1+i}c^{1+i}d$ for all $i \in \{1,\ldots,k\}$, and

$$B = \{\mathrm{o}_{4,6}(1,f;b,1), \mathrm{o}_{2,7+k}(b^{1+k}c^{1+k},1;1,a)\}.$$

Secondly, we select the obstructions with minimal σ-degree.

1) Select $o_{4,6}(1, f; b, 1)$. We have

$$S_{4,6}(1, f; b, 1) = -bf + b^2,\ \mathrm{NR}_{\sigma,\mathcal{G}}(-bf + b^2) = b^2 - b.$$

Let $f_8 = b^2 - b$. Append f_8 to $\mathcal{G}$ and $\{o_{3,8}(b, 1; 1, a), o_{4,8}(b, 1; 1, e), o_{5,8}(b, 1; 1, f), o_{7,8}(b, 1; 1, cd), o_{8,8}(1, b; b, 1)\}$ to B. Then we have

$$\begin{aligned} \mathcal{G} &= (f_1, \ldots, f_7, f_8), \\ B &= \{o_{8,8}(1, b; b, 1), o_{4,8}(b, 1; 1, e), o_{5,8}(b, 1; 1, f), o_{7,8}(b, 1; 1, cd), \\ &\quad\ o_{3,8}(b, 1; 1, a), o_{2,7}(bc, 1; 1, a)\}. \end{aligned}$$

2) Note that σ-degrees of obstructions in B are $b^3 <_\sigma b^2e <_\sigma b^2f <_\sigma b^2cd <_\sigma b^2a <_\sigma bcda$, respectively. Select $o_{8,8}(1, b; b, 1)$. We have $S_{8,8}(1, b; b, 1) = 0$. Select $o_{4,8}(b, 1; 1, e)$. We have $S_{4,8}(b, 1; 1, e) = be - b^2$ and $\mathrm{NR}_{\sigma,\mathcal{G}}(be - b^2) = 0$. Select $o_{5,8}(b, 1; 1, f)$. We have $S_{5,8}(b, 1; 1, f) = bf - b^2$ and $\mathrm{NR}_{\sigma,\mathcal{G}}(bf - b^2) = 0$. Select $o_{7,8}(b, 1; 1, cd)$. We have $S_{7,8}(b, 1; 1, cd) = bcd$ and $\mathrm{NR}_{\sigma,\mathcal{G}}(bcd) = 0$. Select $o_{3,8}(b, 1; 1, a)$. We have $S_{3,8}(b, 1; 1, a) = -b^3c + ba$ and $\mathrm{NR}_{\sigma,\mathcal{G}}(-b^3c + ba) = 0$. At last, select $o_{2,7}(bc, 1; 1, a)$. We have

$$S_{2,7}(bc, 1; 1, a) = -bcad,\ \mathrm{NR}_{\sigma,\mathcal{G}}(-bcad) = -bc^2d.$$

Let $f_9 = bc^2d$. Append f_9 to $\mathcal{G}$ and $\{o_{2,9}(bc^2, 1; 1, a), o_{8,9}(1, c^2d; b, 1)\}$ to B. Then we have

$$\mathcal{G} = (f_1, \ldots, f_7, f_8, f_9),\ B = \{o_{8,9}(1, c^2d; b, 1), o_{2,9}(bc^2, 1; 1, a)\}.$$

3) Note that σ-degrees of obstructions in B are $b^2c^2d <_\sigma bc^2da$, respectively. Select $o_{8,9}(1, c^2d; b, 1)$. We have $S_{8,9}(1, c^2d; b, 1) = -bc^2d$ and $\mathrm{NR}_{\sigma,\mathcal{G}}(-bc^2d) = 0$. At last, select $o_{2,9}(bc^2, 1; 1, a)$. We have

$$S_{2,9}(bc^2, 1; 1, a) = -bc^2ad,\ \mathrm{NR}_{\sigma,\mathcal{G}}(-bcad) = -bc^3d.$$

Let $f_{10} = bc^3d$. Append f_{10} to $\mathcal{G}$ and $\{o_{2,10}(bc^3, 1; 1, a), o_{8,10}(1, c^3d; b, 1)\}$ to B. Then we have

$$\mathcal{G} = (f_1, \ldots, f_7, f_8, f_9, f_{10}),\ B = \{o_{2,10}(bc^3, 1; 1, a), o_{8,10}(1, c^3d; b, 1)\}.$$

It can be verified easily that the procedure goes on forever again. At stage k) we have

$$\mathcal{G} = (f_1, \ldots, f_7, f_8, \ldots, f_{7+k})$$

with $f_8 = b^2 - 1$ and $f_{7+i} = bc^i d$ for all $i \in \{2, \ldots, k\}$, and

$$B = \{\mathrm{o}_{2,7+k}(bc^k, 1; 1, a), \mathrm{o}_{8,7+k}(1, c^k d; b, 1)\}.$$

In [55], T. Mora claimed that $\{f_1, \ldots, f_7, b^2 - b\}$ is a σ-Gröbner basis of I, which is not true according to our computation.

4.3 Homogenization and Dehomogenization

Recall that the free monoid ring $K\langle X\rangle$ is naturally $\mathbb{N}$-graded (see Example 2.2.17). For a polynomial $f \in K\langle X\rangle \setminus \{0\}$, the standard degree of f is the number $\deg(f) = \max\{\mathrm{len}(w) \mid w \in \mathrm{Supp}(f)\}$ and f is homogeneous of degree d if $\deg(f) = d$ and $f \in K\langle X\rangle_d$. Note that an ideal $I \subseteq K\langle X\rangle$ is $\mathbb{N}$-graded if and only if I has a system of generators consisting of homogeneous polynomials (see Proposition 2.2.19). Every homogeneous polynomial of I can be represented nicely in terms of those homogeneous generators. As a result, $\mathbb{N}$-graded ideals possess many useful properties, see for instance Corollary 2.2.20. In this section we shall study homogenization and dehomogenization techniques and find out the connections between $\mathbb{N}$-graded and non-graded ideals of free monoid rings.

Throughout this section, we let y be a new indeterminate, $K\langle y, X\rangle$ the free monoid ring generated by $\{y\} \cup X$ over K, and $\langle y, X\rangle$ the free monoid generated by $\{y\} \cup X$. Moreover, let $C \subseteq K\langle y, X\rangle$ be the ideal generated by the set $\{yx_1 - x_1y, \ldots, yx_n - x_ny\}$. Observe that the ideal C makes the new indeterminate y commute with each word in $\langle X\rangle$. In the literature, the ideal $C = \langle yx_1 - x_1y, \ldots, yx_n - x_ny\rangle \subseteq K\langle y, X\rangle$ is call the **ideal of commutators**.

Definition 4.3.1. Let $f = \sum_{i=1}^{s} c_i w_i \in K\langle X\rangle \setminus \{0\}$ and $\widehat{f} \in K\langle y, X\rangle$ be polynomials.

a) The **homogenization** of f with respect to y is the polynomial

$$f^{\mathrm{hom}} = \sum_{i=1}^{s} c_i w_i y^{\deg(f) - \mathrm{len}(w_i)} \in K\langle y, X\rangle.$$

For the zero polynomial we set $0^{\mathrm{hom}} = 0$.

b) The **dehomogenization** of $\widehat{f}$ with respect to y is the polynomial

$$\widehat{f}^{\mathrm{deh}} = \widehat{f}(1, x_1, \ldots, x_n) \in K\langle X\rangle.$$

Obviously the dehomogenization defines a ring epimorphism $\mathrm{deh} : K\langle y, X\rangle \to K\langle X\rangle$ given by $\mathrm{deh}(y) = 1$ and $\mathrm{deh}(x_i) = x_i$ for all $i = 1, \ldots, n$. The following lemma collects some useful properties of the homogenization and dehomogenization.

Lemma 4.3.2. *Let $f, g \in K\langle X\rangle$ and $\widehat{f}, \widehat{g} \in K\langle y, X\rangle$ be polynomials.*

a) We have $f = (f^{\mathrm{hom}})^{\mathrm{deh}}$.

b) Let $d = \max\{\deg(f), \deg(g)\}$. Then we have $(f+g)^{\mathrm{hom}} y^{d-\deg(f+g)} = f^{\mathrm{hom}} y^{d-\deg(f)} + g^{\mathrm{hom}} y^{d-\deg(g)}$.

c) We have $(fg)^{\mathrm{hom}} - f^{\mathrm{hom}} g^{\mathrm{hom}} \in C$.

d) Let $\widehat{f}$ be a homogeneous polynomial. Then there exists a number $d \in \mathbb{N}$ such that $\widehat{f} - (\widehat{f}^{\mathrm{deh}})^{\mathrm{hom}} y^d \in C$.

e) We have $(\widehat{f} + \widehat{g})^{\mathrm{deh}} = \widehat{f}^{\mathrm{deh}} + \widehat{g}^{\mathrm{deh}}$ and $(\widehat{f}\widehat{g})^{\mathrm{deh}} = \widehat{f}^{\mathrm{deh}} \widehat{g}^{\mathrm{deh}}$.

Proof. The proofs of claims a), b), and e) are analogous to the proof of [44], Proposition 4.3.2. We prove claims c) and d). To prove claim c), it suffices to prove that $yw - wy \in C$ for all $w \in \langle X\rangle$. Let $\widehat{\sigma} =$ `LLex` be the admissible ordering on $\langle y, X\rangle$ such that $y >_{\widehat{\sigma}} x_i$ for all $i \in \{1, \ldots, n\}$. Then we have $\mathrm{LT}_{\widehat{\sigma}}(yx_i - x_i y) = yx_i$. Divide yw by the tuple $(yx_1 - x_1 y, \ldots, yx_n - x_n y)$ using the Division Algorithm. Clearly the normal remainder of yw with respect to $(yx_1 - x_1 y, \ldots, yx_n - x_n y)$ is wy. Therefore we have $yw - wy \in C$.

To prove claim d), we write $\widehat{f} = \sum_{i=1}^{s} c_i \widehat{w}_i$ with $c_1, \ldots, c_s \in K \setminus \{0\}, \widehat{w}_1, \ldots, \widehat{w}_s \in \langle y, X\rangle$, and $\mathrm{len}(\widehat{w}_1) = \cdots = \mathrm{len}(\widehat{w}_s)$. Clearly $yx_i = x_i y + (yx_i - x_i y)$ for all $i \in \{1, \ldots, n\}$. By recursively replacing $yx_i = x_i y + (yx_i - x_i y)$ in all terms of $\widehat{f}$, we obtain $\widehat{f} = \sum_{i=1}^{s} c_i \widehat{w}_i^{\mathrm{deh}} y^{d_i} + h$ with $h \in C$ and $d_1, \ldots, d_s \in \mathbb{N}$ satisfying $\mathrm{len}(\widehat{w_1}^{\mathrm{deh}}) + d_1 = \cdots = \mathrm{len}(\widehat{w_s}^{\mathrm{deh}}) + d_s$. Let $d = \min\{d_1, \ldots, d_t\}$. Then we have $\widehat{f} = (\sum_{i=1}^{s} \widehat{w}_i^{\mathrm{deh}} y^{d_i - d}) y^d + h = (\widehat{f}^{\mathrm{deh}})^{\mathrm{hom}} y^d + h$. □

We define the homogenization and dehomogenization of ideals as follows.

Definition 4.3.3. Let $I \subseteq K\langle X\rangle$ and $\widehat{I} \subseteq K\langle y, X\rangle$ be ideals.

a) The ideal $I^{\mathrm{hom}} = \langle f^{\mathrm{hom}} \mid f \in I\rangle + C \subseteq K\langle y, X\rangle$ is called the **homogenization** of I with respect to y.

b) The set $\widehat{I}^{\mathrm{deh}} = \{\widehat{f}^{\mathrm{deh}} \mid \widehat{f} \in \widehat{I}\} \subseteq K\langle X\rangle$ is called the **dehomogenization** of $\widehat{I}$ with respect to y.

Obviously the ideal $I^{\text{hom}} \subseteq K\langle y,X\rangle$ is $\mathbb{N}$-graded. Since the dehomogenization is a ring epimorphism, the set $\widehat{I}^{\text{deh}} \subseteq K\langle X\rangle$ is also an ideal.

Lemma 4.3.4. *Let $I \subseteq K\langle X\rangle$ and $\widehat{I} \subseteq K\langle y,X\rangle$ be ideals.*

a) We have $(I^{\text{hom}})^{\text{deh}} = I$.

b) Suppose that $\widehat{I}$ is a $\mathbb{N}$-graded ideal containing the ideal C. Let $f \in \widehat{I}^{\text{deh}}$ be a polynomial. Then there exists a number $d \in \mathbb{N}$ such that $f^{\text{hom}}y^d \in \widehat{I}$.

Proof. We prove claim a). By Definition 4.3.3 we have $I \subseteq (I^{\text{hom}})^{\text{deh}}$. Conversely, let $f \in (I^{\text{hom}})^{\text{deh}}$. By Definition 4.3.3.b there exists $\widehat{f} \in I^{\text{hom}}$ such that $f = \widehat{f}^{\text{deh}}$. By Definition 4.3.3.a we have $\widehat{f} = \sum_{i=1}^{s} \widehat{a}_i g_i^{\text{hom}} \widehat{a}'_i + \sum_{j=1}^{t} \widehat{b}_j(yx_{i_j} - x_{i_j}y)\widehat{b}'_j$ with $\widehat{a}_i, \widehat{a}'_i \in K\langle y,X\rangle, g_i \in I$ for all $i \in \{1,\dots,s\}$, and $\widehat{b}_j, \widehat{b}'_j \in K\langle y,X\rangle$ for all $j \in \{1,\dots,t\}$. By Lemma 4.3.2 we have $\widehat{f}^{\text{deh}} = \sum_{i=1}^{s} \widehat{a}_i^{\text{deh}}(g_i^{\text{hom}})^{\text{deh}}\widehat{a}_i'^{\text{deh}} = \sum_{i=1}^{s} \widehat{a}_i^{\text{deh}} g_i \widehat{a}_i'^{\text{deh}} \in I$. Therefore $f \in I$ and $(I^{\text{hom}})^{\text{deh}} \subseteq I$.

We prove claim b). By Definition 4.3.3.b there exists $\widehat{f} \in \widehat{I}$ such that $f = \widehat{f}^{\text{deh}}$. Since $\widehat{I}$ is $\mathbb{N}$-graded, without loss of generality, we may assume that $\widehat{f}$ is homogeneous. Then by Lemma 4.3.2.d there exists a number $d \in \mathbb{N}$ such that $\widehat{f} - (\widehat{f}^{\text{deh}})^{\text{hom}}y^d \in C$. From the assumption $L \subseteq \widehat{I}$, we conclude that $f^{\text{hom}}y^d = (\widehat{f}^{\text{deh}})^{\text{hom}}y^d \in \widehat{I}$. □

Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $I = \langle G\rangle$, and let the set $\widehat{G} = \{g^{\text{hom}} \mid g \in G\} \cup \{yx_1 - x_1y, \dots, yx_n - x_ny\}$ generate an ideal $\widehat{I} = \langle \widehat{G}\rangle$. The following example shows that in general we have the proper inclusion $\widehat{I} \subset I^{\text{hom}}$.

Example 4.3.5. Consider the free monoid ring $K\langle x_1,x_2\rangle$ and a set of polynomials $G = \{x_2^2 - x_1 + 3, x_2^3 - x_1x_2 - x_1 - x_2\} \subseteq K\langle x_1,x_2\rangle \setminus \{0\}$ which generates an ideal $I = \langle G\rangle$ (cf. [50]). Since $(x_2^2 - x_1 + 3)x_2 - (x_2^3 - x_1x_2 - x_1 - x_2) = x_1 + 4x_2$, we have $x_1 + 4x_2 \in I$. Note that $x_1 + 4x_2$ is homogeneous and hence $x_1 + 4x_2 \in I^{\text{hom}}$. However, we can see easily that $x_1 + 4x_2 \notin \langle x_2^2 - x_1y + 3y^2, x_2^3 - x_1x_2y - x_1y^2 - x_2y^2, yx_1 - x_1y, yx_2 - x_2y\rangle \subseteq K\langle y,x_1,x_2\rangle$.

In order to use homogenization and dehomogenization techniques to compute Gröbner bases we shall extend admissible orderings on $\langle X\rangle$ to admissible orderings on $\langle y,X\rangle$.

Definition 4.3.6. We define a relation $\widehat{\sigma}$ on $\langle y,X\rangle$ as follows. For two terms $\widehat{w}_1, \widehat{w}_2 \in \langle y,X\rangle$, we say $\widehat{w}_1 \geq_{\widehat{\sigma}} \widehat{w}_2$ if we have $\text{len}(\widehat{w}_1) > \text{len}(\widehat{w}_2)$, or if we have $\text{len}(\widehat{w}_1) = \text{len}(\widehat{w}_2)$ and $\widehat{w}_1^{\text{deh}} >_\sigma \widehat{w}_2^{\text{deh}}$, or if we have $\text{len}(\widehat{w}_1) = \text{len}(\widehat{w}_2)$ and $\widehat{w}_1^{\text{deh}} = \widehat{w}_2^{\text{deh}}$ and $\widehat{w}_1 \geq_{\texttt{Lex}} \widehat{w}_2$ where `Lex` is the lexicographic ordering on $\langle y,X\rangle$ such that $y >_{\texttt{Lex}} x_i$ for all $i \in \{1,\dots,n\}$. We call $\widehat{\sigma}$ the **extension** of σ.

It is straightforward to check that $\widehat{\sigma}$ is an admissible ordering on $\langle y, X\rangle$. The following lemma is crucial for our purposes.

Lemma 4.3.7. *Let $f \in K\langle X\rangle \setminus \{0\}$ and $\widehat{f} \in K\langle y, X\rangle \setminus \{0\}$ be polynomials.*

a) If σ is length-compatible, then we have $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}) = \mathrm{LT}_\sigma(f) \in \langle X\rangle$.

b) If $\widehat{f}$ is homogeneous and $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f})$ is not a multiple of yx_i for all $i \in \{1,\dots,n\}$, then we have $(\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}))^{\mathrm{deh}} = \mathrm{LT}_\sigma(\widehat{f}^{\mathrm{deh}})$ and $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}) = \mathrm{LT}_\sigma(\widehat{f}^{\mathrm{deh}})y^d$ for some $d \in \mathbb{N}$.

Proof. Claim a) follows directly from Definitions 3.1.12, 4.3.1.a, and 4.3.6. To prove claim b), we note that $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}) = wy^d$ with some $w \in \langle X\rangle, d \in \mathbb{N}$ by assumption. Let $\widehat{f} = c_1wy^d + \sum_{i=2}^s c_2\widehat{w}_i$ with $c_1,\dots,c_s \in K \setminus \{0\}, \widehat{w}_2,\dots,\widehat{w}_s \in \langle y, X\rangle$ such that $\mathrm{len}(wy^d) = \mathrm{len}(\widehat{w}_2) = \cdots = \mathrm{len}(\widehat{w}_s)$. By Definition 4.3.6 we have $w \geq_\sigma \widehat{w}_i^{\mathrm{deh}}$ for all $i \in \{2,\dots,s\}$. We conclude the proof of claim b) by showing that $w >_\sigma \widehat{w}_i^{\mathrm{deh}}$ for all $i \in \{2,\dots,s\}$. For a contradiction, suppose that there exists an index $k \in \{2,\dots,s\}$ such that $w = \widehat{w}_k^{\mathrm{deh}}$. Since $\mathrm{len}(wy^d) = \mathrm{len}(\widehat{w_k})$ and $w = \widehat{w_k}^{\mathrm{deh}}$, there must be a letter y at position before $\mathrm{len}(w) + 1$ in $\widehat{w_k}$. Then by Definition 4.3.6 we have $wy^d <_{\mathtt{Lex}} \widehat{w_k}$ and hence $wy^d <_{\widehat{\sigma}} \widehat{w_k}$, which contradicts $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}) = wy^d$. Therefore $\mathrm{LT}_\sigma(\widehat{f}^{\mathrm{deh}}) = w = (\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}))^{\mathrm{deh}}$ and $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}) = wy^d = \mathrm{LT}_\sigma(\widehat{f}^{\mathrm{deh}})y^d$. □

Note that Lemma 4.3.7.a does not hold if σ is not length-compatible. A counterexample is as follows.

Example 4.3.8. Consider the free monoid ring $K\langle x_1, x_2\rangle$ equipped with the admissible ordering $\sigma = \mathtt{Elim}$ on $\langle x_1, x_2\rangle$ such that $x_1 >_\sigma x_2$, and a polynomial $f = -x_1 + x_2^2 + 3 \in K\langle x_1, x\rangle$. Let $\widehat{\sigma}$ be the extension of σ. Then we have $f^{\mathrm{hom}} = -x_1y + x_2^2 + 3y^2$ and $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}) = x_1y \neq x_1 = \mathrm{LT}_\sigma(f)$.

Assumption 4.3.9. *In the rest of this section, we shall assume that σ is a length-compatible admissible ordering on $\langle X\rangle$.*

Now we are ready to study the relations between $\mathbb{N}$-graded and non-graded ideals. The following propositions, i.e. Propositions 4.3.10 and 4.3.13, present the connections between $\mathbb{N}$-graded with non-graded ideals by Gröbner bases.

Proposition 4.3.10. *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $I = \langle G\rangle$. Then G is a σ-Gröbber basis of I if and only if the set $\widehat{G} = \{g^{\mathrm{hom}} \mid g \in G\} \cup \{yx_1 - x_1y, \dots, yx_n - x_ny\}$ is a homogeneous $\widehat{\sigma}$-Gröbner basis of the ideal $I^{\mathrm{hom}} \subseteq K\langle y, X\rangle$.*

Proof. Assume that G is a σ-Gröbber basis of I. Clearly $\widehat{G} \subseteq I^{\mathrm{hom}}$. To prove that $\widehat{G}$ is a homogeneous $\widehat{\sigma}$-Gröbner basis of I^{hom}, by Lemma 3.3.15 it suffices to show that for every polynomial $\widehat{f} \in I^{\mathrm{hom}} \setminus \{0\}$ there exists a polynomial $\widehat{g} \in \widehat{G}$ such that $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f})$ is a multiple of $\mathrm{LT}_{\widehat{\sigma}}(\widehat{g})$. Let $\widehat{f} \in I^{\mathrm{hom}} \setminus \{0\}$. Since I^{hom} is $\mathbb{N}$-graded, without loss of generality, we may assume that $\widehat{f}$ is homogeneous. Note that we have $\mathrm{LT}_{\widehat{\sigma}}(yx_i - x_iy) = yx_i$ for all $i \in \{1, \ldots, n\}$ by Definition 4.3.6. If $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f})$ is a multiply of yx_i for some $i \in \{1, \ldots, n\}$, then we are done. Now we assume that $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f})$ is not a multiply of yx_i for all $i \in \{1, \ldots, n\}$. Then by Lemma 4.3.7.b we have $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}) = \mathrm{LT}_{\sigma}(\widehat{f}^{\mathrm{deh}})y^d$ for some $d \in \mathbb{N}$. On the other hand, we have $\widehat{f}^{\mathrm{deh}} \in I$ by Lemma 4.3.4.a. Since G is a σ-Gröbner basis of I, there exist $g \in G, w, w' \in \langle X\rangle$ such that $\mathrm{LT}_{\sigma}(\widehat{f}^{\mathrm{deh}}) = w\mathrm{LT}_{\sigma}(g)w'$. By Lemma 4.3.7.a we have $\mathrm{LT}_{\sigma}(g) = \mathrm{LT}_{\widehat{\sigma}}(g^{\mathrm{hom}})$. Altogether, we have $\mathrm{LT}_{\widehat{\sigma}}(\widehat{f}) = \mathrm{LT}_{\sigma}(\widehat{f}^{\mathrm{deh}})y^d = w\mathrm{LT}_{\sigma}(g)w'y^d = w\mathrm{LT}_{\widehat{\sigma}}(g^{\mathrm{hom}})w'y^d$.

Conversely, assume that $\widehat{G}$ is a homogeneous $\widehat{\sigma}$-Gröbner basis of I^{hom}. To prove G is a σ-Gröbber basis of I, by Lemma 3.3.15 it suffices to show that for every polynomial $f \in I\backslash\{0\}$ there exists a polynomial $g \in G$ such that $\mathrm{LT}_{\sigma}(f)$ is a multiple of $\mathrm{LT}_{\sigma}(g)$. Let $f \in I\backslash\{0\}$. Clearly $f^{\mathrm{hom}} \in I^{\mathrm{hom}}$. By assumption, there exist $\widehat{g} \in \widehat{G}, \widehat{w}, \widehat{w}' \in \langle y, X\rangle$ such that $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}) = \widehat{w}\mathrm{LT}_{\widehat{\sigma}}(\widehat{g})\widehat{w}'$. By Lemma 4.3.7.a we have $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}) = \mathrm{LT}_{\sigma}(f) \in \langle X\rangle$. Thus $\widehat{w}\mathrm{LT}_{\widehat{\sigma}}(\widehat{g})\widehat{w}' \in \langle X\rangle$. Therefore we must have $\widehat{w}, \widehat{w}' \in \langle X\rangle$ and $\widehat{g} = g^{\mathrm{hom}}$ for some $g \in G$. Again by Lemma 4.3.7.a we have $\mathrm{LT}_{\sigma}(g) = \mathrm{LT}_{\widehat{\sigma}}(g^{\mathrm{hom}})$. Altogether, we have $\mathrm{LT}_{\sigma}(f) = \widehat{w}\mathrm{LT}_{\sigma}(g)\widehat{w}'$ with $\widehat{w}, \widehat{w}' \in \langle X\rangle$ and $g \in G$. □

Remark 4.3.11. Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be a finitely generated ideal. We compute a homogeneous $\widehat{\sigma}$-Gröbner basis of the ideal $I^{\mathrm{hom}} \subseteq K\langle y, X\rangle$ via the following approach.

1) Enumerate a σ-Gröbner basis $G \subseteq K\langle X\rangle$ of I.

2) Then $\{g^{\mathrm{hom}} \mid g \in G\} \cup \{yx_1 - x_1y, \ldots, yx_n - x_ny\}$ is a homogeneous $\widehat{\sigma}$-Gröbner basis of I^{hom} by Proposition 4.3.10.

Example 4.3.12. Consider the free monoid ring $K\langle x_1, x_2\rangle$ equipped with the admissible ordering σ = `LLex` on $\langle x_1, x_2\rangle$ such that $x_1 >_{\sigma} x_2$, and a set of polynomials $G = \{x_2^2 - x_1 + 3, x_2^3 - x_1x_2 - x_1 - x_2\} \subseteq K\langle x_1, x_2\rangle \setminus \{0\}$ which generates an ideal $I = \langle G\rangle$. We compute a σ-Gröbner basis of I using the ApCoCoA package *gbmr* and get a set $\{x_2^2 - x_1 + 3, x_1 + 4x_2\}$. Then the set $\{x_2^2 - x_1y + 3y^2, x_1 + 4x_2, yx_1 - x_1y, yx_2 - x_2y\}$ is a homogeneous $\widehat{\sigma}$-Gröbner basis of the ideal $I^{\mathrm{hom}} \subseteq K\langle y, x_1, x_2\rangle$.

Proposition 4.3.13. *Let $\widehat{I} \subseteq K\langle y, X\rangle \setminus \{0\}$ be an $\mathbb{N}$-graded ideal containing the ideal C, and let the set $\widehat{G} \subseteq K\langle y, X\rangle \setminus \{0\}$ be a homogeneous $\widehat{\sigma}$-Gröbner basis of $\widehat{I}$.*

Then the set $\{\widehat{g}^{\mathrm{deh}} \mid \widehat{g} \in \widehat{G}\} \setminus \{0\}$ *is a* σ*-Gröbner basis of the ideal* $\widehat{I}^{\mathrm{deh}}$*.*

Proof. Obviously $\{\widehat{g}^{\mathrm{deh}} \mid \widehat{g} \in \widehat{G}\} \setminus \{0\} \subseteq I^{\mathrm{deh}}$ for all $\widehat{g} \in \widehat{G}$. By Lemma 3.3.15 it suffices to prove that for every polynomial $f \in \widehat{I}^{\mathrm{deh}} \setminus \{0\}$ there exists a polynomial $\widehat{g} \in \widehat{G}$ such that $\mathrm{LT}_\sigma(f)$ is a multiple of $\mathrm{LT}_\sigma(\widehat{g}^{\mathrm{deh}})$. Let $f \in \widehat{I}^{\mathrm{deh}} \setminus \{0\}$. By Lemma 4.3.4.b we have $f^{\mathrm{hom}}y^d \in \widehat{I}$ for some $d \in \mathbb{N}$. Since $\widehat{G}$ is a $\widehat{\sigma}$-Gröbner basis of $\widehat{I}$, there exist $\widehat{g} \in \widehat{G}, \widehat{w}, \widehat{w}' \in \langle y, X\rangle$ such that $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}y^d) = \widehat{w}\mathrm{LT}_{\widehat{\sigma}}(\widehat{g})\widehat{w}'$. By Remark 3.1.13.b and Lemma 4.3.7.a we have $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}y^d) = \mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}})y^d = \mathrm{LT}_\sigma(f)y^d$. Thus $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}y^d)$ is not a multiple of yx_i for all $i \in \{1, \ldots, n\}$. By Lemma 4.3.7.b we have $\mathrm{LT}_{\widehat{\sigma}}(f^{\mathrm{hom}}y^d) = \mathrm{LT}_\sigma((f^{\mathrm{hom}}y^d)^{\mathrm{deh}})y^{d'}$ for some $d' \in \mathbb{N}$. By Lemmas 4.3.2.a and 4.3.2.e we have $\mathrm{LT}_\sigma((f^{\mathrm{hom}}y^d)^{\mathrm{deh}}) = \mathrm{LT}_\sigma(f)$. Hence $\widehat{w}\mathrm{LT}_{\widehat{\sigma}}(\widehat{g})\widehat{w}' = \mathrm{LT}_\sigma(f)y^{d'}$. Therefore $\mathrm{LT}_{\widehat{\sigma}}(\widehat{g})$ must have the form $wy^{d''}$ with $w \in \langle X\rangle$ and $d'' \in \mathbb{N}$. Again by Lemma 4.3.7.b we have $(\mathrm{LT}_{\widehat{\sigma}}(\widehat{g}))^{\mathrm{deh}} = \mathrm{LT}_\sigma(\widehat{g}^{\mathrm{deh}})$. Altogether, we have $\mathrm{LT}_\sigma(f) = (\mathrm{LT}_\sigma(f)y^{d'})^{\mathrm{deh}} = (\widehat{w}\mathrm{LT}_{\widehat{\sigma}}(\widehat{g})\widehat{w}')^{\mathrm{deh}} = \widehat{w}^{\mathrm{deh}}(\mathrm{LT}_{\widehat{\sigma}}(\widehat{g}))^{\mathrm{deh}}\widehat{w}'^{\mathrm{deh}} = \widehat{w}^{\mathrm{deh}}\mathrm{LT}_\sigma(\widehat{g}^{\mathrm{deh}})\widehat{w}'^{\mathrm{deh}}$. □

Remark 4.3.14. Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $I = \langle G\rangle$. Then we can compute a σ-Gröbner basis of I via the following approach.

1) Consider the $\mathbb{N}$-graded ideal $\widehat{I} = \langle g^{\mathrm{hom}} \mid g \in G\rangle + C$. (Note that $\widehat{I}^{\mathrm{deh}} = I$.)

2) Enumerate a homogeneous $\widehat{\sigma}$-Gröbner basis $\widehat{G} \subseteq K\langle y, X\rangle$ of $\widehat{I}$.

3) Then, by Proposition 4.3.13, $\{\widehat{g}^{\mathrm{deh}} \mid \widehat{g} \in \widehat{G}\} \setminus \{0\} \subseteq K\langle X\rangle$ is a σ-Gröbner basis of I.

Note that the normal remainder of a homogeneous polynomial of degree $d \in \mathbb{N}$ with respect to a tuple of homogeneous polynomials is still homogeneous of degree d. Also note that the S-polynomial $S_{i,j}(w_i, w_i'; w_j, w_j')$ of the obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ of two homogeneous polynomials g_i and g_j is again homogeneous. Moreover, the S-polynomial has a degree not less than $\max\{\deg(g_i), \deg(g_j)\}$. With these facts, given a homogeneous system of generators, we are able to compute Gröbner bases degree by degree. To this end we introduce some basic terminology.

Definition 4.3.15. Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of homogeneous polynomials which generates an ideal $I = \langle G\rangle$, let $\mathcal{G}$ be an associative tuple of G, and let $s = |\mathcal{G}|$.

a) Given a degree $d \in \mathbb{N}$, let $G_{\leq d} = \{g \in G \mid \deg(g) \leq d\}$ and $G_d = \{g \in G \mid \deg(g) = d\}$.

b) The tuple $\mathcal{G}$ is said to be **degree-ordered** if $\deg(g_1) \leq \cdots \leq \deg(g_s)$.

c) Given a degree $d \in \mathbb{N}$, we let $\mathcal{G}_{\leq d}$ be the subtuple of $\mathcal{G}$ consisting of all polynomials g_i such that $\deg(g_i) \leq d$, and $\mathcal{G}_d$ the subtuple of $\mathcal{G}$ consisting of all polynomials g_i such that $\deg(g_i) = d$.

d) The **degree** of an obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq s}\mathrm{O}(i,j)$ is defined to be the degree of its S-polynomial, i.e. $\deg(S_{i,j}(w_i, w_i'; w_j, w_j'))$.

e) Let B be a set of obstructions. Given a degree $d \in \mathbb{N}$, we let $B_{\leq d}$ be the subset of B containing all obstructions whose degrees are not larger than d, and B_d the subset of B containing all obstructions whose degrees are equal to d.

Given a homogeneous system of generators, we compute a homogeneous Gröbner basis degree by degree as follows.

Theorem 4.3.16. (Homogeneous Buchberger Procedure) *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of homogeneous polynomials which generates an ideal $I = \langle G\rangle$. Consider the following sequence of instructions.*

1) Let $B = \emptyset, \mathcal{G} = \emptyset$, and $s = 0$.

2) Let d be the smallest degree of a polynomial in G or an obstruction in B. Form the subsets G_d of G and B_d of B, and delete their entries from G and B, respectively.

3) If $G_d = \emptyset$, continue with step 6). Otherwise, select a polynomial $g \in G_d$ and delete it from G_d.

4) Compute $g' = \mathrm{NR}_{\sigma,\mathcal{G}}(g)$. If $g' = 0$, continue with step 3).

5) Increase s by one, append $g_s = g'$ to the tuple $\mathcal{G}$, and append the set of non-trivial obstructions $\cup_{1\leq i\leq s}\mathrm{O}(i,s)$ to the set B. Continue with step 3).

6) If $B_d = \emptyset$, continue with step 9). Otherwise, select an obstruction $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$ $\in B_d$ and delete it from B_d.

7) Compute the S-polynomial $S = S_{i,j}(w_i, w_i'; w_j, w_j')$ and its normal remainder $S' = \mathrm{NR}_{\sigma,\mathcal{G}}(S)$. If $S' = 0$, continue with step 6).

8) Increase s by one, append $g_s = S'$ to the tuple $\mathcal{G}$, and append the set of non-trivial obstructions $\cup_{1\leq i\leq s}\mathrm{O}(i,s)$ to the set B. Continue with step 6).

9) If $G = \emptyset$ and $B = \emptyset$, return the tuple $\mathcal{G}$. Otherwise, continue with step 2).

This is a procedure that enumerates a degree-ordered homogeneous σ-Gröbner basis $\mathcal{G}$ of I. If I has a finite homogeneous σ-Gröbner basis, it stops after finitely many steps and the resulting degree-ordered tuple $\mathcal{G}$ is a homogeneous σ-Gröbner basis of I.

Proof. Observe that the normal remainder of a homogeneous polynomial with respect to a tuple of homogeneous polynomials is also homogeneous. Thus the tuple $\mathcal{G}$ consists of entirely homogeneous polynomials. Note that in step 4) $\deg(g') = \deg(g)$ if $g' \neq 0$, and in step 7) $\deg(S') = \deg(S)$ if $S' \neq 0$, and that the degree of an obstruction of g_i and g_j is larger or equal to the degrees of g_i and g_j. Then the tuple $\mathcal{G}$ is degree-ordered by choosing the smallest degree d in step 2). The proof of the claim that the procedure enumerates a σ-Gröbner basis $\mathcal{G}$ of I and stops after finitely many steps if I has a finite σ-Gröbner basis proceeds exactly the same as the proof of Theorem 4.1.14. □

Remark 4.3.17. Let $\mathcal{G}$ be the resulting tuple of Theorem 4.3.16. Obviously G is a homogeneous system of generators of the $\mathbb{N}$-graded ideal I. Moreover, let $d \in \mathbb{N}$, and let $\langle I_{\leq d}\rangle$ be the ideal generated by the homogeneous polynomials in I with degree $\leq d$. By Corollary 2.2.20, the set $G_{\leq d}$ is a system of generators of $\langle I_{\leq d}\rangle$. We call $\mathcal{G}_{\leq d}$ a **d-truncated σ-Gröbner basis** of I.

Just like partial Gröbner bases (see Remark 4.1.16), truncated Gröbner bases are sufficient to handle many applications. In some situations we happen to know the maximal degree of generators in a homogeneous Gröbner basis beforehand. Thus it is necessary for us to terminate the Homogeneous Buchberger Procedure properly. We shall therefore slightly modify the Homogeneous Buchberger Procedure given in Theorem 4.3.16 and make it more flexible for our purposes.

Corollary 4.3.18. *In the setting of Theorem 4.3.16 and given a degree $d_0 \in \mathbb{N}$, we replace steps 2), 5), and 8) by the following instructions.*

2') Let d be the smallest degree of a polynomial in G or an obstruction in B. If $d > d_0$, return the tuple $\mathcal{G}$. Form the subsets G_d of G and B_d of B, and delete their entries from G and B, respectively.

5') Increase s by one, append $g_s = S'$ to the tuple $\mathcal{G}$, and append the set

$$\{\mathrm{o}_{i,j}(w_i, w_i'; w_s, w_s') \in \cup_{1\leq i\leq s}\mathrm{O}(i,s) \mid \deg(S_{i,j}(w_i, w_i'; w_s, w_s')) \leq d_0\}$$

to the set B. Continue with step 3).

8') Increase s by one, append $g_s = S'$ to tuple $\mathcal{G}$, and append the set

$$\{\mathrm{o}_{i,j}(w_i, w_i'; w_s, w_s') \in \cup_{1\le i\le s}\mathrm{O}(i,s) \mid \deg(S_{i,j}(w_i, w_i'; w_s, w_s')) \le d_0\}$$

to the set B. Continue with step 6).

Then the resulting set of instructions defines an algorithm that computes a d_0-truncated σ-Gröbner basis of I.

Proof. Note that it is not necessary to consider polynomials and obstructions whose degrees are larger than d_0, since the non-zero normal remainder of a homogeneous polynomial of degree d with respect to a tuple of homogeneous polynomials is also a homogeneous polynomial of degree d. The correctness follows from Theorem 4.3.16. We prove the finiteness. When a polynomial g_s is appended to $\mathcal{G}$, the leading term set $\mathrm{LT}_\sigma\{\mathcal{G}\}$ is strictly enlarged. Since $\mathrm{len}(\mathrm{LT}_\sigma(g_s))$ is bounded by d_0 and $|\langle X\rangle_{\le d_0}| < \infty$, there are only finitely many g_s can be appended to $\mathcal{G}$. Therefore the procedure terminates after finitely many steps. □

Given a homogeneous system of generators, well-behaved Homogeneous Buchberger Procedure allows us to enumerate Gröbner bases degree by degree. Given an inhomogeneous system of generators G, by Remark 4.3.14 we can compute a σ-Gröbner basis as follows. First we construct an $\mathbb{N}$-graded ideal $\widehat{I} \subseteq K\langle X\rangle$ generated by a homogeneous system of generators $\widehat{G} = \{g^{\mathrm{hom}} \mid g \in G\} \cup \{yx_1 - x_1y, \ldots, yx_n - x_ny\}$. Then we apply the Homogeneous Buchberger Procedure given in Theorem 4.3.16 to enumerate a homogeneous $\widehat{\sigma}$-Gröbner basis $\widehat{G}$ of $\widehat{I}$. Finally, by Proposition 4.3.13 we obtain a σ-Gröbner basis of the ideal $\langle G\rangle$ by dehomogenizing generators in $\widehat{G}$ with respect to y. However, the following example shows that we shall avoid using homogenization and dehomogenization techniques naïvely.

Example 4.3.19. (continued) Consider Example 4.3.12 again. Recall that in this example we have the free monoid ring $K\langle x_1, x_2\rangle$ equipped with the admissible ordering $\sigma = \texttt{LLex}$ on $\langle x_1, x_2\rangle$ such that $x_1 >_\sigma x_2$, and an ideal $I = \langle G\rangle \subseteq K\langle x_1, x_2\rangle \setminus \{0\}$ generated by a set of polynomials $G = \{x_2^2 - x_1 + 3, x_2^3 - x_1x_2 - x_1 - x_2\}$. We construct the homogeneous system of generators $\widehat{G} = \{x_2^2 - x_1y + 3y^2, x_2^3 - x_1x_2y - x_1y^2 - x_2y^2, yx_1 - x_1y, yx_2 - x_2y\}$ which generates the ideal $\widehat{I} = \langle\widehat{G}\rangle \subseteq K\langle y, x_1, x_2\rangle$. We enumerate a $\widehat{\sigma}$-Gröbner basis of $\widehat{I}$ by the Homogeneous Buchberger Procedure given in Theorem 4.3.16 and obtain an infinite set $\{yx_2 - x_2y, yx_1 - x_1y, x_2^2 - x_1y + 3y^2, x_1y^2 + 4x_2y^2\} \cup \{x_1x_2x_1^iy - x_2x_1^{i+1}y \mid i \in \mathbb{N}\}$. Note that $x_2^3 - x_1x_2y - x_1y^2 - x_2y^2$ is removed because of redundancy.

But Example 4.3.12 shows that the ideal I should have a finite σ-Gröbner basis. By tracing the enumerating procedure in Example 4.3.19, we find out that the new indeterminate y is the source of the infiniteness. It is a general phenomenon that a new indeterminate can induce infinite loops in Buchberger's Procedure (see [67, 72]). Observe that in Example 4.3.19 the polynomial $x_1y^2 + 4x_2y^2$ has the new indeterminate y on the right side of each term. If we can cancel y in each term of $x_1y^2 + 4x_2y^2$ and get $x_1 + 4x_2$, then we can remove redundant polynomials $yx_1 - x_1y, x_1y^2 + 4x_2y^2$ and $x_1x_2x_1^iy - x_2x_1^{i+1}y$ and hence obtain a finite homogeneous $\widehat{\sigma}$-Gröbner basis. Actually it is valid to do so. We rephrase the cancellation mentioned above in terms of a dehomogenization.

Definition 4.3.20. Let $\widehat{f} \in K\langle y, X\rangle \setminus \{0\}$ be a polynomial, and let $k \in \mathbb{N}$ be the maximal number satisfying $\widehat{f} = \widehat{f'}y^k$ with $\widehat{f'} \in K\langle y, X\rangle$. The polynomial $\widehat{f'}$ is called the **right dehomogenization** of $\widehat{f}$ with respect to y and is denoted by $\widehat{f}^{\mathrm{rdeh}}$.

Theorem 4.3.21. *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $I = \langle G\rangle$. We construct a homogeneous system of generators $\{g^{\mathrm{hom}} \mid g \in G\} \cup \{yx_1 - x_1y, \dots, yx_n - x_ny\} \subseteq K\langle y, X\rangle$ and apply the Buchberger Procedure given in Theorem 4.1.14 with step 4) replaced by the following instruction.*

4') Increase s' by one, append $g_{s'} = (S')^{\mathrm{rdeh}}$ to the tuple $\mathcal{G}$, and append the set of obstructions $\cup_{1\le i\le s'}\mathrm{O}(i, s')$ to the set B. Then continue with step 2).

Then we obtain a procedure which enumerates a homogeneous $\widehat{\sigma}$-Gröbner basis of I^{hom}.

Proof. See [72], Theorem 2. □

A modification similar to the one in Theorem 4.3.21 applies to the Homogeneous Buchberger Procedure given in Theorem 4.3.16. We shows it in the following example.

Example 4.3.22. (continued) Consider Example 4.3.12 again. Recall that in this example we have the free monoid ring $K\langle x_1, x_2\rangle$ equipped with the admissible ordering $\sigma = \texttt{LLex}$ on $\langle x_1, x_2\rangle$ such that $x_1 >_\sigma x_2$, and the ideal $I = \langle G\rangle \subseteq K\langle x_1, x_2\rangle$ generated by the set $G = \{x_2^2 - x_1 + 3, x_2^3 - x_1x_2 - x_1 - x_2\}$. We construct the homogeneous system of generators $\widehat{G} = \{x_2^2 - x_1y + 3y^2, x_2^3 - x_1x_2y - x_1y^2 - x_2y^2, yx_1 - x_1y, yx_2 - x_2y\}$. We enumerate a $\widehat{\sigma}$-Gröbner basis of I^{hom} using the Homogeneous Buchberger Procedure given in Theorem 4.3.16 deployed with right dehomogenization.

1) Let $B = \emptyset, \mathcal{G} = \emptyset$, and $s = 0$.

2) Let $d = 2, G_2 = \{yx_2 - x_2y, yx_1 - x_1y, x_2^2 - x_1y + 3y^2\}, B_2 = \emptyset, \widehat{G} = \{x_2^3 - x_1x_2y - x_1y^2 - x_2y^2\}$, and $B = \emptyset$.

3) Select $g = yx_2 - x_2y$ and let $G_2 = \{yx_1 - x_1y, x_2^2 - x_1y + 3y^2\}$.

4) Compute $g' = \mathrm{NR}_{\widehat{\sigma},\mathcal{G}}(g) = yx_2 - x_2y$.

5) Let $s = 1, \mathcal{G} = (g_1)$ with $g_1 = g' = yx_2 - x_2y$, and $B = \emptyset$. Continue with step 3).

3) Select $g = yx_1 - x_1y$ and let $G_2 = \{x_2^2 - x_1y + 3y^2\}$.

4) Compute $g' = \mathrm{NR}_{\widehat{\sigma},\mathcal{G}}(g) = yx_1 - x_1y$.

5) Let $s = 2, \mathcal{G} = (g_1, g_2)$ with $g_2 = yx_1 - x_1y$, and $B = \emptyset$. Continue with step 3).

3) Select $g = x_2^2 - x_1y + 3y^2$ and let $G_2 = \emptyset$.

4) Compute $g' = \mathrm{NR}_{\widehat{\sigma},\mathcal{G}}(g) = x_2^2 - x_1y + 3y^2$.

5) Let $s = 3, \mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = x_2^2 - x_1y + 3y^2$, and $B = \{\mathrm{o}_{1,3}(1, x_2; y, 1); \mathrm{o}_{3,3}(1, x_2; x_2, 1)\}$.

3) Since $G_2 = \emptyset$, continue with step 6).

6) Since $B_2 = \emptyset$, continue with step 9).

9) Since $\widehat{G} \neq \emptyset, B \neq \emptyset$, continue with step 2).

2) Let $d = 3, G_3 = \{x_2^3 - x_1x_2y - x_1y^2 - x_2y^2\}, B_3 = \{\mathrm{o}_{1,3}(1, x_2; y, 1); \mathrm{o}_{3,3}(1, x_2; x_2, 1)\}$, $\widehat{G} = \emptyset$, and $B = \emptyset$.

3) Select $g = x_2^3 - x_1x_2y - x_1y^2 - x_2y^2$ and let $G_3 = \emptyset$.

4) Compute $g' = \mathrm{NR}_{\widehat{\sigma},\mathcal{G}}(g) = x_1y^2 + 4x_2y^2$.

5) Let $s = 4, \mathcal{G} = (g_1, g_2, g_3, g_4)$ with $g_4 = (g')^{\mathrm{rdeh}} = x_1 + 4x_2$, and $B = \{\mathrm{o}_{2,4}(1, 1; y, 1)\}$. Note that $g_2 = yx_1 - x_1y$ is redundant since $\mathrm{LT}_{\widehat{\sigma}}(g_2) = yx_1 = y\mathrm{LT}_{\widehat{\sigma}}(g_4)$.

3) Since $G_2 = \emptyset$, continue with step 6).

6) Select $\mathrm{o}_{1,3}(1, x_2; y, 1)$ and let $B_3 = \{\mathrm{o}_{3,3}(1, x_2; x_2, 1)\}$.

7) Compute $S = S_{1,3}(1, x_2; y, 1) = -x_2yx_2 + yx_1y - 3y^3$ and $S' = \mathrm{NR}_{\widehat{\sigma},\mathcal{G}}(S) = 0$.

6) Select $o_{3,3}(1, x_2; x_2, 1)$ and let $B_3 = \emptyset$.

7) Compute $S = S_{3,3}(1, x_2; x_2, 1) = -x_1yx_2 + x_2x_1y + 3y^2x_2 - 3x_2y^2$ and $S' = \mathrm{NR}_{\widehat{\sigma},\mathcal{G}}(S) = 0$.

6) Since $B_3 = \emptyset$, continue with step 9).

9) Since $B \neq \emptyset$, continue with step 2).

2) Let $d = 2, G_2 = \emptyset, B_2 = \{o_{2,4}(1, 1; y, 1)\}, \widehat{G} = \emptyset$, and $B = \emptyset$.

3) Since $G_2 = \emptyset$, continue with step 6).

6) Select $o_{2,4}(1, 1; y, 1)$ and let $B_2 = \emptyset$.

7) Compute $S = S_{2,4}(1, 1; y, 1) = -x_1y - 4yx_2$ and $S' = \mathrm{NR}_{\widehat{\sigma},\mathcal{G}}(S) = 0$.

6) Since $B_3 = \emptyset$, continue with step 9).

9) Since $\widehat{G} = \emptyset$ and $B = \emptyset$, return $\mathcal{G} = (g_1, g_3, g_4)$ with $g_1 = yx_2 - x_2y, g_3 = x_2^2 - x_1y + 3y^2$, and $g_4 = x_1 + 4x_2$. Note that g_2 is removed because of redundancy.

The set $\{g_1, g_3, g_4\}$ is a $\widehat{\sigma}$-Gröbner basis of I^{hom} where $g_1 = yx_2 - x_2y, g_3 = x_2^2 - x_1y + 3y^2$, and $g_4 = x_1 + 4x_2$. Thus by Proposition 4.3.13 the set $\{x_2^2 - x_1 + 3, x_1 + 4x_2\}$ is a σ-Gröbner basis of I. Note that the results are exactly the same as in Example 4.3.12 except for a removed redundant polynomial.

We end this section with a remark on selection strategies.

Remark 4.3.23. Observe that in Example 4.3.22 the degree d is initialized to 2 and then increases to 3 and then decreases to 2 again. The degree d does not keep increasing because of right dehomogenization. This jumping back of the degree is called the **rabbit strategy** (see [72]). Note that in commutative settings the *sugar cube strategy* is widely used in most of the implementations of Buchberger's Algorithm because of great practical merits. The sugar cube strategy marks each generator with a phantom degree and then plays normal selection strategy. We refer to [4, 34] for more details. In the ApCoCoA package *gbmr*, we use the sugar cube strategy with non-commutative flavor for both inhomogeneous and homogeneous system of generators. More precisely, during the Buchberger Procedure and the Homogeneous Buchberger Procedure, we first select the obstruction with the minimal degree and then break tie by selecting the obstruction with the minimal σ-degree as mentioned in Remark 4.1.5. Consequenctly, the rabbit strategy becomes inherent in the ApCoCoA package *gbmr*.

4.4 Gröbner Basis Computations for Right Ideals

In this section we shall study Gröbner basis computations for right ideals in free monoid rings shortly. It is understood that all results in this section can be applied to left ideals symmetrically.

Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite set of polynomials which generates a right ideal $I_\varrho = \langle G\rangle_\varrho$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Moreover, let $s \geq 1$, and let $(K\langle X\rangle)^s$ be the right $K\langle X\rangle$-module of rank s with the canonical basis $\{\eta_1, \ldots, \eta_s\}$, i.e. $\eta_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ whose the i^{th} element is 1 and all of whose other elements are 0. Recall that O_ϱ is the set of all right obstructions of $\mathcal{G}$ (see Definition 3.5.5). By Proposition 3.5.7 the set G is a right σ-Gröbner basis of I_ϱ if and only if every right obstruction in O_ϱ has a lifting in $\mathrm{Syz}(\mathcal{G})_\varrho$. Recall that for each pair $i, j \in \{1, \ldots, s\}$ such that $i < j$ there exists none or only one right obstruction of g_i and g_j. Just as what we did in Section 4.1 for two-sided ideals, we define S-polynomials of right obstructions.

Definition 4.4.1. Let $i, j \in \{1, \ldots, s\}$ and $i < j$, and let $\mathrm{ro}_{i,j} \in \mathrm{O}_\varrho$ be the right obstruction of g_i and g_j. The **S-polynomial** of $\mathrm{ro}_{i,j}$ is defined as follows.

$$S_{i,j} = \begin{cases} \frac{1}{\mathrm{LC}_\sigma(g_i)} g_i - \frac{1}{\mathrm{LC}_\sigma(g_j)} g_j w & \text{if } \mathrm{ro}_{i,j} = \frac{1}{\mathrm{LC}_\sigma(g_i)} \eta_i - \frac{1}{\mathrm{LC}_\sigma(g_j)} \eta_j w, \\ \frac{1}{\mathrm{LC}_\sigma(g_i)} g_i w - \frac{1}{\mathrm{LC}_\sigma(g_j)} g_j & \text{if } \mathrm{ro}_{i,j} = \frac{1}{\mathrm{LC}_\sigma(g_i)} \eta_i w - \frac{1}{\mathrm{LC}_\sigma(g_j)} \eta_j. \end{cases}$$

Clearly we have $\max_\sigma\{\mathrm{LT}_\sigma(g_i), \mathrm{LT}_\sigma(g_j)\} >_\sigma \mathrm{LT}_\sigma(S_{i,j})$ for all $\mathrm{ro}_{i,j} \in \mathrm{O}_\varrho$. Keep in mind that to compute Gröbner bases of right ideals we should apply the Right Division Algorithm (see Theorem 3.5.1) as far as the division takes place.

Proposition 4.4.2. (Buchberger Criterion for Right Ideals) *Let $G \subseteq K\langle X\rangle$ be a finite set of non-zero polynomials which generates a right ideal $I_\varrho = \langle G\rangle_\varrho$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Then the following conditions are equivalent.*

a) The set G is a right σ-Gröbner basis of I_ϱ.

b) For every right obstruction $\mathrm{ro}_{i,j} \in \mathrm{O}_\varrho$, *we have* $\mathrm{RNR}_{\sigma,\mathcal{G}}(S_{i,j}) = 0$.

Proof. Analogous to Proposition 4.1.13. □

We have the following Buchberger Algorithm for computing Gröbner bases of right ideals.

Theorem 4.4.3. (Buchberger Algorithm for Right Ideals) *Let $G \subseteq K\langle X\rangle$ be a finite set of non-zero polynomials which generates a right ideal $I_\varrho = \langle G\rangle_\varrho$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Consider the following sequence of instructions.*

1) *Let $s' = s$ and $B = \mathrm{O}_\varrho$.*

2) *If $B = \emptyset$, return the result $\mathcal{G}$. Otherwise, select a right obstruction $\mathrm{ro}_{i,j} \in B$ and delete it from B.*

3) *Compute the S-polynomial $S = S_{i,j}$ and its normal remainder $S' = \mathrm{RNR}_{\sigma,\mathcal{G}}(S)$. If $S' = 0$, continue with step 2).*

4) *Increase s' by one, append $g_{s'} = S'$ to the tuple $\mathcal{G}$, and append the set of right obstructions $\{\mathrm{ro}(i,s') = \frac{1}{\mathrm{LC}_\sigma(g_i)}\eta_i - \frac{1}{\mathrm{LC}_\sigma(g_{s'})}\eta_{s'}w \mid i \in \{1,\ldots,s'-1\}, w \in \langle X\rangle, \mathrm{LT}_\sigma(g_i) = \mathrm{LT}_\sigma(g_{s'})w\}$ to the set B. Then continue with step 2).*

This is an algorithm that computes a right σ-Gröbner basis $\mathcal{G}$ of I_ϱ.

Proof. To prove correctness, by Proposition 4.4.2 it suffices to prove that for every right obstruction $\mathrm{ro}_{i,j} \in \mathrm{O}_\varrho$ its S-polynomial $S_{i,j}$ satisfies $\mathrm{RNR}_{\sigma,\mathcal{G}}(S_{i,j}) = 0$. Assume that in step 4) $g_{s'} \neq 0$. Note that none of $\{\mathrm{LT}_\sigma(g_1),\ldots,\mathrm{LT}_\sigma(g_{s'-1})\}$ is a prefix of $\mathrm{LT}_\sigma(g_{s'})$ by Theorem 3.5.1.a. Thus for some $i \in \{1,\ldots,s'-1\}$ the polynomials g_i and $g_{s'}$ have a right obstruction if and only if $\mathrm{LT}_\sigma(g'_s)$ is a proper prefix of $\mathrm{LT}_\sigma(g_i)$. Therefore step 1) together with step 2) ensures that all possible right obstructions of $\mathcal{G}$ are considered by the procedure. If in step 3) we have $S' = 0$, then we are done. Otherwise, $\mathrm{RNR}_{\sigma,\mathcal{G}}(S_{i,j}) = 0$ is guaranteed by appending $g_{s'} = S'$ to $\mathcal{G}$ in step 4).

To prove finiteness, we let $w_{\max} = \max_\sigma\{\mathrm{LT}_\sigma(g_i) \mid g_i \in G\}$. If in step 3) $S' \neq 0$, then by Theorem 3.5.1.b we have $\mathrm{LT}_\sigma(S) \geq_\sigma \mathrm{LT}_\sigma(S')$. Note that for all $\mathrm{ro}_{i,j} \in \mathrm{O}_\varrho$ we have $\max_\sigma\{\mathrm{LT}_\sigma(g_i), \mathrm{LT}_\sigma(g_j)\} >_\sigma \mathrm{LT}_\sigma(S_{i,j})$. Thus $w_{\max} >_\sigma \mathrm{LT}_\sigma(g_{s'})$ in step 4). When a polynomial $g_{s'}$ is appended to $\mathcal{G}$, the leading term set $\mathrm{LT}_\sigma\{\mathcal{G}\}$ is strictly enlarged. This can happen only finitely many times since σ is a well-ordering. Therefore the procedure terminates after finitely many steps. □

From Theorem 4.4.3 we conclude that *every finitely generated right ideal in free monoid rings has a finite Gröbner basis.* The following proposition shows that Gröbner bases of right ideals can be computed by operating interreduction on systems of generators.

Proposition 4.4.4. *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates a right ideal $I_\varrho = \langle G\rangle_\varrho$. We apply the Interreduction Algorithm on G given in Theorem 3.2.8 with the Division Algorithm replaced by the Right Division Algorithm given in Theorem 3.5.1. Then the resulting interreduced set G' is a right σ-Gröbner basis of I_ϱ.*

Proof. We have $I_\varrho = \langle G'\rangle_\varrho$ by Theorem 3.2.8. We prove that every polynomial $f \in I_\varrho \setminus \{0\}$ has a Gröbner representation in terms of G'. Since $I_\varrho = \langle G'\rangle_\varrho$, there exist $g_1, \ldots, g_s \in G', p_1, \ldots, p_s \in K\langle X\rangle \setminus \{0\}$ such that $f = \sum_{i=1}^s g_i p_i$. By Remark 3.1.13.b we have $\mathrm{LT}_\sigma(g_i p_i) = \mathrm{LT}_\sigma(g_i)\mathrm{LT}_\sigma(p_i)$. Since G' is interreduced, $\mathrm{LT}_\sigma(g_i)$ is not a prefix of $\mathrm{LT}_\sigma(g_j)$ for all $i, j \in \{1, \ldots, s\}$ and $i \neq j$. Thus $\mathrm{LT}_\sigma(g_i p_i) = \mathrm{LT}_\sigma(g_i)\mathrm{LT}_\sigma(p_i) \neq \mathrm{LT}_\sigma(g_j)\mathrm{LT}_\sigma(p_j) = \mathrm{LT}_\sigma(g_j p_j)$ for all $i, j \in \{1, \ldots, s\}$ and $i \neq j$. By Remark 3.1.13.a we have $\mathrm{LT}_\sigma(f) = \max_\sigma\{\mathrm{LT}_\sigma(g_i p_i) \mid i \in \{1, \ldots, s\}\}$. Therefore $f = \sum_{i=1}^s g_i p_i$ is a Gröbner representation of f in terms of G'. □

Chapter 5

Gröbner Basis Theory in $(K\langle X\rangle \otimes K\langle X\rangle)^r$

In this chapter we shall extend the notions of Gröbner basis theory to free bimodules over free monoid rings. In [8, 9], H. Bluhm and M. Kreuzer generalized Gröbner basis theory to free bimodules over K-algebras in order to compute two-sided syzygies. Inspired by their ideas, we shall explore the characterizations of Gröbner bases of two-sided submodules in free bimodules over free monid rings, and formulate procedures for enumerating Gröbner bases in this setting. We refer to [1] for Gröbner bases of one-sided submodules in free bimodules over free monoid rings.

We shall study Gröbner basis theory in free bimodules over free monoid rings by following the same approach as in Chapters 3 and 4. In Section 5.1 we shall introduce two main ingredients of Gröber basis theory: module term orderings (see Definition 5.1.1) and the Division Algorithm (see Theorem 5.1.12). We present Macaulay's Basis Theorem (see Theorem 5.1.9) as a consequence of the module term ordering and introduce the Interreduction Algorithm (see Corollary 5.1.14) as an application of the Division Algorithm.

We shall start Section 5.2 with a definition of Gröbner bases of two-sided submodules (see Definition 5.2.1). Then we shall characterize Gröbner bases through Gröbner representations (see Proposition 5.2.2) and syzygy modules (see Definition 5.2.4 and Proposition 5.2.10). Using critical pairs and critical syzygies (see Definition 5.2.7), we obtain a Buchberger Criterion (see Corollary 5.2.11) and formulate a Buchberger Procedure (see Theorem 5.2.12) for enumerating Gröbner bases.

In Section 5.3 we shall devote ourselves to improving the Buchberger Procedure.

We generalize our methods in Section 4.2 to the setting in this chapter. More precisely, we shall improve the Buchberger Procedure by detecting unnecessary critical pairs (see Proposition 5.3.3 and Theorem 5.3.5) and by deleting redundant generators (see Theorem 5.3.10).

In Section 5.4 we shall generalize Faugère's F4 Algorithm by investigating ingredients of the F4 Algorithm. After founding a connection between a set of elements in a free bimodule and a linear system over K (see Definition 5.4.1) and studying the Reduction Algorithm (see Theorem 5.4.7), we shall propose an F4 Procedure (see Theorem 5.4.10) for enumerating Gröbner bases in our setting.

Throughout this chapter, we let K be a field, $X = \{x_1, \ldots, x_n\}$ a finite alphabet (or set of indeterminates), $K\langle X\rangle$ the free monoid ring generated by X over K, $\langle X\rangle$ the free monoid generated by X, and σ an admissible ordering on $\langle X\rangle$. Moreover, for $r \geq 1$, we let $F_r = (K\langle X\rangle \otimes K\langle X\rangle)^r$ be the free $K\langle X\rangle$-bimodule of rank r with the canonical basis $\{e_1, \ldots, e_r\}$, where $e_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$ with $1 \otimes 1$ occurring in the i^{th} position for $i = 1, \ldots, r$, and we let $\mathbb{T}(F_r)$ be the set of terms in F_r, i.e. $\mathbb{T}(F_r) = \{we_iw' \mid i \in \{1, \ldots, r\}, w, w' \in \langle X\rangle\}$. By a $K\langle X\rangle$-submodule $M \subseteq F_r$ we mean a two-sided $K\langle X\rangle$-submodule unless stated otherwise.

5.1 Module Term Orderings and the Division Algorithm

Definition 5.1.1. A **module term ordering** τ on $\mathbb{T}(F_r)$ is a relation on $\mathbb{T}(F_r)$ satisfying the following conditions for all $s_1, s_2, s_3 \in \mathbb{T}(F_r)$ and all $w, w' \in \langle X\rangle$.

a) $s_1 \geq_\tau s_2$ or $s_2 \geq_\tau s_1$, i.e. τ is complete.

b) $s_1 \geq_\tau s_1$, i.e. τ is reflexive.

c) $s_1 \geq_\tau s_2$ and $s_2 \geq_\tau s_1$ imply $s_1 = s_2$, i.e. τ is antisymmetric.

d) $s_1 \geq_\tau s_2$ and $s_2 \geq_\tau s_3$ imply $s_1 \geq_\tau s_3$, i.e. τ is transitive.

e) $s_1 \geq_\tau s_2$ implies $ws_1w' \geq_\tau ws_2w'$, i.e. τ is compatible with scalar multiplication.

f) Every descending chain of terms $s_1 \geq_\tau s_2 \geq_\tau \cdots$ in $\mathbb{T}(F_r)$ becomes eventually stationary, i.e. τ is a well-ordering.

If τ is a module term ordering on $\mathbb{T}(F_r)$, then we have $wsw' \geq_\tau s$ for all $s \in \mathbb{T}(F_r)$ and all $w, w' \in \langle X \rangle$. In particular, $we_iw' \geq_\tau e_i$ for all $i \in \{1, \ldots, r\}$ and all $w, w' \in \langle X \rangle$. Recall that we introduced the following module term ordering in Definition 4.2.1, which plays an important role in the optimizations of the Buchberger Procedure in free monoid rings.

Example 5.1.2. Let $\mathcal{G} = (g_1, \ldots, g_r) \in (K\langle X \rangle \setminus \{0\})^r$ be a tuple of polynomials. The **module term ordering** τ induced by $(\sigma, \mathcal{G})$ on $\mathbb{T}(F_r)$ is defined as follows. For all $w_1e_iw_1', w_2e_jw_2' \in \mathbb{T}(F_r)$ with $i, j \in \{1, \ldots, r\}$ and $w_1, w_1', w_2, w_2' \in \langle X \rangle$, we say that $w_1e_iw_1' \geq_\tau w_2e_jw_2'$ if we have $w_1\mathrm{LT}_\sigma(g_i)w_1' >_\sigma w_2\mathrm{LT}_\sigma(g_j)w_2'$, or if we have $w_1\mathrm{LT}_\sigma(g_i)w_1' = w_2\mathrm{LT}_\sigma(g_j)w_2'$ and $i > j$, or if we have $w_1\mathrm{LT}_\sigma(g_i)w_1' = w_2\mathrm{LT}_\sigma(g_j)w_2'$ and $i = j$ and w_2 is a prefix of w_1.

In Section 5.3 we will follow the same approach to define a module term ordering which is useful for improving the Buchberger Procedure in F_r. The following are two very important module term orderings that are related to many applications of Gröbner bases (see Section 6.2).

Example 5.1.3. Let `To` be an admissible ordering on $\langle X \rangle$, and let $w_1e_iw_1', w_2e_jw_2' \in \mathbb{T}(F_r)$ with $i, j \in \{1, \ldots, r\}$ and $w_1, w_1', w_2, w_2' \in \langle X \rangle$.

a) The module term ordering `ToPos` on $\mathbb{T}(F_r)$ is defined as follows. If we have $w_1w_1' >_{\mathtt{To}} w_2w_2'$, or if we have $w_1w_1' = w_2w_2'$ and $w_1 >_{\mathtt{To}} w_2$, or if we have $w_1 = w_2$ and $w_1' = w_2'$ and $i \leq j$, then we say that $w_1e_iw_1' \geq_{\mathtt{ToPos}} w_2e_jw_2'$.

b) The module term ordering `PosTo` on $\mathbb{T}(F_r)$ is defined as follows. If we have $i < j$, or if we have $i = j$ and $w_1w_1' >_{\mathtt{To}} w_2w_2'$, or if we have $i = j$ and $w_1w_1' = w_2w_2'$ and $w_1 >_{\mathtt{To}} w_2$, then we say that $w_1e_iw_1' \geq_{\mathtt{PosTo}} w_2e_jw_2'$.

Definition 5.1.4. Let σ be an admissible ordering on $\langle X \rangle$, and let τ be a module term ordering on $\mathbb{T}(F_r)$. We say that τ is **compatible** with σ if $w \geq_\sigma w'$ implies $ws \geq_\tau w's$ and $sw \geq_\tau sw'$ for all $s \in \mathbb{T}(F_r)$ and $w, w' \in \langle X \rangle$.

For instance, the module term ordering τ induced by $(\sigma, \mathcal{G})$ is compatible with σ. Both `ToPos` and `PosTo` are compatible with `To`.

Assumption 5.1.5. *In what follows, we let τ be a module term ordering on $\mathbb{T}(F_r)$.*

Definition 5.1.6. Every element $m \in F_r \setminus \{0\}$ can be uniquely represented as

$$m = c_1w_1e_{\gamma_1}w_1' + \cdots + c_sw_se_{\gamma_s}w_s'$$

with $c_1,\dots,c_s \in K\backslash\{0\}, \gamma_1,\dots,\gamma_s \in \{1,\dots,r\}, w_1,\dots,w'_s \in \langle X\rangle$ such that $w_1e_{\gamma_1}w'_1 >_\tau w_2e_{\gamma_2}w'_2 >_\tau \cdots >_\tau w_se_{\gamma_s}w'_s$. The term $\mathrm{LT}_\tau(m) = w_1e_{\gamma_1}w'_1 \in \mathbb{T}(F_r)$ is called the **leading term** of m with respect to τ. The element $\mathrm{LC}_\tau(m) = c_1 \in K\setminus\{0\}$ is called the **leading coefficient** of m with respect to τ. The element m is called **monic** if $\mathrm{LC}_\tau(m) = 1$. Moreover, we let $\mathrm{LM}_\tau(m) = \mathrm{LC}_\tau(m)\cdot\mathrm{LT}_\tau(m) = c_1w_1e_{\gamma_1}w'_1$.

Note that the leading term $\mathrm{LT}_\tau(0)$ and leading coefficient $\mathrm{LC}_\tau(0)$ of zero element are undefined. The following remark lists some useful rules for computing with leading terms.

Remark 5.1.7. Let $m, m_1, m_2 \in F_r \setminus \{0\}$ be elements.

a) Suppose that $m_1+m_2 \neq 0$. We have $\mathrm{LT}_\tau(m_1+m_2) \leq_\tau \max_\tau\{\mathrm{LT}_\tau(m_1), \mathrm{LT}_\tau(m_2)\}$. Moreover, $\mathrm{LT}_\tau(m_1+m_2) = \max_\tau\{\mathrm{LT}_\tau(m_1), \mathrm{LT}_\tau(m_2)\}$ if and only if $\mathrm{LT}_\tau(m_1) \neq \mathrm{LT}_\tau(m_2)$ or $\mathrm{LC}_\tau(m_1) + \mathrm{LC}_\tau(m_2) \neq 0$.

b) For all $w, w' \in \langle X\rangle$, we have $\mathrm{LT}_\tau(wmw') = w\mathrm{LT}_\tau(m)w'$.

Definition 5.1.8. Let $M \subseteq F_r$ be a $K\langle X\rangle$-submodule.

a) The $K\langle X\rangle$-submodule $\mathrm{LT}_\tau(M) = \langle \mathrm{LT}_\tau(m) \mid m \in M \setminus \{0\}\rangle \subseteq F_r$ is called the **leading term module** of M with respect to τ.

b) The set $\mathrm{LT}_\tau\{M\} = \{\mathrm{LT}_\tau(m) \mid m \in M\setminus\{0\}\} \subseteq \mathbb{T}(F_r)$ is called the **leading term set** of M with respect to τ.

c) The set $\mathcal{O}_\tau(M) = \mathbb{T}(F_r)\backslash\mathrm{LT}_\tau\{M\}$ is called the **order module** of M with respect to τ.

We have $\mathrm{LT}_\tau(\langle 0\rangle) = \langle 0\rangle$ and $\mathrm{LT}_\tau\{\langle 0\rangle\} = \emptyset$ using this definition. Observe that $\mathrm{LT}_\tau\{M\}$ is actually a $\langle X\rangle$-submonomodule of $\mathbb{T}(F_r)$. We call $\mathcal{O}_\tau(M)$ the order module in the following sense. If $s, s' \in \mathbb{T}(F_r)$ such that $s \in \mathcal{O}_\tau(M)$ and s is a multiple of s', then we also have $s' \in \mathcal{O}_\tau(M)$. Now we are able to present Macaulay's Basis Theorem in F_r as follows.

Theorem 5.1.9. (Macaulay's Basis Theorem) *Let $M \subseteq F_r$ be a $K\langle X\rangle$-submodule. We have $F_r = M \oplus \mathrm{Span}_K\mathcal{O}_\tau(M)$. Moreover, for every element $m \in F_r$, there exists a unique element $\hat{m} \in \mathrm{Span}_K\mathcal{O}_\tau(M)$ such that $m - \hat{m} \in M$.*

Proof. First we prove that $F_r = M + \mathrm{Span}_K\mathcal{O}_\tau(M)$. It suffices to prove $F_r \subseteq M + \mathrm{Span}_K\mathcal{O}_\tau(M)$. Given an element $m \in F_r \setminus \{0\}$, we consider the following sequence of instructions.

1) Let $s = 0, \hat{m} = 0$, and $v = m$.

2) If $\mathrm{LT}_\tau(v) \in \mathrm{LT}_\tau(M)$, then increase s by one, choose an element $g \in M$ such that $\mathrm{LT}_\tau(v) = \mathrm{LT}_\tau(g)$, set $g_s = \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(g)}g$, and replace v by $v - g_s$. If $\mathrm{LT}_\tau(v) \notin \mathrm{LT}_\tau(M)$, replace $\hat{m}$ by $\hat{m} + \mathrm{LM}_\sigma(v)$ and v by $v - \mathrm{LM}_\sigma(v)$.

3) If now $v \neq 0$, start again with step 2). If $v = 0$, return $g_1, \dots, g_s$ and $\hat{m}$.

Observe that the following equation holds at each stage of the procedure.

$$m = g_1 + \cdots + g_s + \hat{m} + v$$

Moreover, in step 2) one of two things can happen. If $\mathrm{LT}_\tau(v) \in \mathrm{LT}_\tau(M)$, then $\mathrm{LM}_\tau(v) = \mathrm{LC}_\tau(v)\mathrm{LT}_\tau(v) = \mathrm{LC}_\tau(v)\mathrm{LT}_\tau(g) = \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(g)}\mathrm{LC}_\tau(g)\mathrm{LT}_\tau(g) = \mathrm{LM}_\tau(g_s)$. If $v - g_s \neq 0$, then by Remark 5.1.7.a we have $\mathrm{LT}_\tau(v) >_\tau \mathrm{LT}_\tau(v - g_s)$. On the other hand, if $\mathrm{LT}_\tau(v) \notin \mathrm{LT}_\tau(M)$, then $\mathrm{LM}_\tau(v)$ is subtracted from v. By Remark 5.1.7.a we have $\mathrm{LT}_\tau(v) >_\tau \mathrm{LT}_\tau(v - \mathrm{LM}_\tau(v))$ if $v - \mathrm{LM}_\tau(v) \neq 0$. In a word, the leading term of v strictly decreases in step 2). Since τ is a well-ordering, the procedure terminates after finitely many steps. When the procedure returns, we have $v = 0$ and $m = (g_1 + \cdots + g_s) + \hat{m}$ with $g_1, \cdots, g_s \in M$ and $\hat{m} \in \mathrm{Supp}_K\mathcal{O}_\tau(M)$. Therefore $F_r = M + \mathrm{Span}_K\mathcal{O}_\tau(M)$.

We prove that $M \cap \mathrm{Span}_K\mathcal{O}_\tau(M) = \{0\}$. Suppose that there exists a non-zero element $m \in M \cap \mathrm{Span}_K\mathcal{O}_\tau(M)$. Then we have $\mathrm{LT}_\tau(m) \in \mathrm{LT}_\sigma\{M\} \cap \mathcal{O}_\tau(M)$, which contradicts Definition 5.1.8.c. Altogether, we have $F_r = M \oplus \mathrm{Span}_K\mathcal{O}_\tau(M)$.

It is clear that when the procedure returns we have $m - \hat{m} \in M$. To prove the uniqueness of $\hat{m}$, we assume that there exist $\hat{m}_1, \hat{m}_2 \in \mathrm{Span}_K\mathcal{O}_\tau(M)$ such that $m - \hat{m}_1, m - \hat{m}_2 \in M$. Then we have $(m - \hat{m}_1) - (m - \hat{m}_2) = \hat{m}_2 - \hat{m}_1 \in M \cap \mathrm{Span}_K\mathcal{O}_\tau(M)$. Therefore $\hat{m}_1 = \hat{m}_2$. □

The unique element $\hat{m} \in \mathrm{Span}_K\mathcal{O}_\tau(M)$ as in Theorem 5.1.9 is called the **normal form** of m modulo M with respect to σ and is denoted by $\mathrm{NF}_{\sigma,M}(m)$. The following corollary follows from Theorem 5.1.9 immediately.

Corollary 5.1.10. *We have* $\dim_K(F_r/M) = \dim_K(F_r/\mathrm{LT}_\tau(M))$ *for any* $K\langle X\rangle$*-submodule* $M \subseteq F_r$.

We have the following rules for computing with normal forms.

Remark 5.1.11. Let $M \subseteq F_r$ be a $K\langle X\rangle$-submodule.

a) For $m \in F_r$, we have $\mathrm{NF}_{\tau,M}(\mathrm{NF}_{\tau,M}(m)) = \mathrm{NF}_{\tau,M}(m)$.

b) For $m_1, m_2 \in F_r$, we have $\mathrm{NF}_{\tau,M}(m_1 - m_2) = \mathrm{NF}_{\tau,M}(m_1) - \mathrm{NF}_{\tau,M}(m_2)$.

c) For $m_1, m_2 \in F_r$, we have $\mathrm{NF}_{\tau,M}(m_1) = \mathrm{NF}_{\tau,M}(m_2)$ if and only if $m_1 - m_2 \in M$. In particular, an element $m \in F_r$ satisfies $m \in M$ if and only if $\mathrm{NF}_{\tau,M}(m) = 0$.

From the proof of Theorem 5.1.9, we shall now construct the following Division Algorithm with the intention of computing the normal form algorithmically.

Theorem 5.1.12. (The Division Algorithm) *Let $m \in F_r \setminus \{0\}$ be an element, and let $G \subseteq F_r \setminus \{0\}$ be a set elements. Consider the following sequence of instructions.*

1) Let $t = 0, p = 0,$ and $v = m$.

2) If there exists an element $g \in G$ such that $\mathrm{LT}_\tau(v) = w\mathrm{LT}_\tau(g)w'$ for some $w, w' \in \langle X\rangle$, then increase t by 1, set $c_t = \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(g)}, w_t = w, w'_t = w', g_t = g$, and replace v by $v - c_t w_t g_t w'_t$.

3) Repeat step 2) until there is no more element $g \in G$ such that $\mathrm{LT}_\tau(v)$ is a multiple of $\mathrm{LT}_\tau(g)$. If $v \neq 0$, then replace p by $p + \mathrm{LM}_\tau(v)$ and v by $v - \mathrm{LM}_\tau(v)$, and continue with step 2).

4) Return the tuples $(c_1, w_1, w'_1, g_1), \ldots, (c_t, w_t, w'_t, g_t)$ and the element $p \in F_r$.

This is an algorithm which returns tuples $(c_1, w_1, w'_1, g_1), \ldots, (c_t, w_t, w'_t, g_t)$ and an element $p \in F_r$ such that

$$m = \sum_{i=1}^{t} c_i w_i g_i w'_i + p$$

and such that the following conditions are satisfied.

a) No element of $\mathrm{Supp}(p)$ is contained in $\mathrm{LT}_\tau(G)$.

b) If $t > 0$, then we have $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(w_1 g_1 w'_1) >_\tau \cdots >_\tau \mathrm{LT}_\tau(w_t g_t w'_t)$.

c) If $p \neq 0$, then we have $\mathrm{LT}_\tau(m) \geq_\tau \mathrm{LT}_\tau(p)$.

Proof. We first show that the following equation holds at each stage of the procedure.

$$m = \sum_{i=1}^{t} c_i w_i g_i w_i' + p + v$$

It is obviously true at the outset. Then we should consider two cases. If in step 2) there is an element $g \in G$ such that $\mathrm{LT}_\tau(v) = w\mathrm{LT}_\tau(g)w'$, then $c_t w_t g w_t'$ is added to the summation of the right hand side of the equation and meanwhile subtracted from v. Otherwise, in step 2) $\mathrm{LM}_\tau(v)$ is added to p and meanwhile subtracted from v. Thus the equation is preserved in both cases.

Observe that v changes only in steps 2) and 3). In step 2) we have $\mathrm{LT}_\tau(c_t w_t g_t w_t') = w_t\mathrm{LT}_\tau(g_t)w_t' = \mathrm{LT}_\tau(v)$ using Remark 5.1.7.b, and $\mathrm{LC}_\tau(c_t w_t g_t w_t') = c_t\mathrm{LC}_\tau(g_t) = \mathrm{LC}_\tau(v)$. If $v - c_t w_t g_t w_t' \neq 0$, then by Remark 5.1.7.a we have $\mathrm{LT}_\tau(v - c_t w_t g_t w_t') <_\tau \mathrm{LT}_\tau(v)$. If in step 3) $v - \mathrm{LM}_\tau(v) \neq 0$, then by Remark 5.1.7.a we have $\mathrm{LT}_\tau(v - \mathrm{LM}_\tau(v)) <_\tau \mathrm{LT}_\tau(v)$. Therefore $\mathrm{LT}_\tau(v)$ strictly decreases. Since τ is a well-ordering, $\mathrm{LT}_\tau(v)$ can decreases finitely many times and the procedure terminates after finitely many steps. Condition a) holds because in step 3) $\mathrm{LM}_\tau(v)$ is added to p only if $\mathrm{LT}_\tau(v)$ is not a multiple of any terms in $\mathrm{LT}_\tau\{G\}$. Conditions b) and c) hold because $\mathrm{LT}_\tau(v)$ is strictly decreasing. □

Definition 5.1.13. Let $m \in F_r \setminus \{0\}$ be an element, and let $G \subseteq F_r \setminus \{0\}$ be a set of elements. Then an element $p \in F_r$ obtained in Theorem 5.1.12 is called a **normal remainder** of m with respect to G and is denoted by $\mathrm{NR}_{\tau,G}(m)$.

Observe that normal remainder $\mathrm{NR}_{\tau,G}(m)$ is not unique, for in step 2) of the Division Algorithm there might exist more that one $g \in G$ satisfying $\mathrm{LT}_\tau(v) = w\mathrm{LT}_\tau(g)w'$ for some $w, w' \in \langle X \rangle$ (compare with Corollary 3.3.9). Note that we have $\mathrm{NR}_{\tau,G}(0) = 0$ and $\mathrm{NR}_{\tau,\emptyset}(m) = m$ for all $m \in F_r$ using this definition. Also note that $\mathrm{NR}_{\tau,G}(m)$ is not equal to $\mathrm{NF}_{\tau,\langle G \rangle}(m)$ in general. In Section 5.2 we will see that if G is a Gröbner basis (see Definition 5.2.1) of the $K\langle X \rangle$-submodule $\langle G \rangle \subseteq F_r$ then the Division Algorithm computes normal forms (see Proposition 5.2.2).

At the end of this section, we present interreduction on a set of elements $G \subseteq F_r \setminus \{0\}$ as an important application of the Division Algorithm. Note that a set of elements $G \subseteq F_r \setminus \{0\}$ is called **interreduced** with respect to τ if no element of $\mathrm{Supp}(m)$ is contained in $\mathrm{LT}_\tau(G \setminus \{m\})$ for all $m \in G$.

Corollary 5.1.14. (Interreduction Algorithm) *Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements which generates a $K\langle X \rangle$-submodule $M = \langle G \rangle$. In this setting, we apply* *the Interreduction Algorithm as in Theorem 3.2.8 with step 2) replaced by the following instruction.*

2') Compute the normal remainder g_i' of g_i with respect to $G \setminus \{0, g_i\}$ using the Division Algorithm given in Theorem 5.1.12.

Then we obtain an algorithm that computes an interreduced system of generators of M.

Proof. Analogous to Theorem 3.2.8. □

5.2 Gröbner Bases and Gröbner Basis Computations

In the spirit of Definition 3.3.1 we define Gröbner bases of $K\langle X\rangle$-submodules as follows.

Definition 5.2.1. Let $M \subseteq F_r \setminus \{0\}$ be a $K\langle X\rangle$-submodule. A subset $G \subseteq M \setminus \{0\}$ is called a **τ-Gröbner basis** of M if

$$\mathrm{LT}_\tau\{M\} = \{w\mathrm{LT}_\tau(g)w' \mid g \in G, w, w' \in \langle X\rangle\}.$$

Note that $M \setminus \{0\}$ is a τ-Gröbner basis of M using this definition. In particular, the empty set $\emptyset$ is a τ-Gröbner basis of the zero module $\langle 0\rangle$. The most frequently used properties of Gröbner bases are as follows.

Proposition 5.2.2. *Let $M \subseteq F_r \setminus \{0\}$ be a $K\langle X\rangle$-submodule, and let $G \subseteq M \setminus \{0\}$ be a subset. Then the following conditions are equivalent.*

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

b) For every element $m \in F_r$, we have $\mathrm{NR}_{\tau,G}(m) = \mathrm{NF}_{\tau,M}(m)$.

c) For every element $m \in M \setminus \{0\}$, there exists a Gröbner representation in terms of G, i.e.

$$m = \sum_{i=1}^{s} c_i w_i g_i w_i'$$

with $c_1, \ldots, c_s \in K \setminus \{0\}, g_1, \ldots, g_s \in G, w_1, \ldots, w_s' \in \langle X\rangle$ such that $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(w_1 g_1 w_1') >_\tau \mathrm{LT}_\tau(w_2 g_2 w_2') >_\tau \cdots >_\tau \mathrm{LT}_\tau(w_s g_s w_s')$.

Proof. To prove condition a) implies condition b), we let $\mathrm{NR}_{\tau,G}(m)$ be a normal remainder of m with respect to G. By Theorem 5.1.12.a, no element of $\mathrm{Supp}(\mathrm{NR}_{\tau,G}(m))$ is contained in $\mathrm{LT}_\tau(G)$. By Definition 5.2.1 we have $\mathrm{LT}_\tau\{M\} \subset \mathrm{LT}_\tau(G)$. Hence no element of $\mathrm{Supp}(\mathrm{NR}_{\tau,G}(m))$ is contained in $\mathrm{LT}_\tau\{M\}$. Thus $\mathrm{NR}_{\tau,G}(m) \in \mathrm{Span}_K \mathcal{O}_\tau(M)$. Obviously $m - \mathrm{NR}_{\tau,G}(m) \in \langle G \rangle \subseteq M$. Then condition b) holds by Theorem 5.1.9. Condition c) follows from condition b) by Theorem 5.1.12 and Remark 5.1.11.c. By Remark 5.1.7 condition c) implies condition a) . □

If a set $G \subseteq F_r$ is a Gröbner basis of a $K\langle X\rangle$-submodule $M \subseteq F_r$, then by Proposition 5.2.2.b every element $m \in F_r$ has a unique normal remainder with respect to G. By Proposition 5.2.2.c, τ-Gröbner basis G of M is also a system of generators of M.

As Gröbner bases in free monoid rings, there exist more than one Gröbner bases for every non-zero $K\langle X\rangle$-submodule in F_r. The following proposition specifies a unique Gröbner basis for every non-zero $K\langle X\rangle$-submodule.

Proposition 5.2.3. *For every $K\langle X\rangle$-submodule $M \subseteq F_r \setminus \{0\}$, there exists a unique τ-Gröbner basis G satisfying the following conditions.*

a) The set $\mathrm{LT}_\tau(G)$ is the minimal system of generators of the $\langle X\rangle$-submonomodule $\mathrm{LT}_\tau\{M\} \subseteq \mathbb{T}(F_r)$.

b) For all $g \in G$, we have $\mathrm{LC}_\tau(g) = 1$.

c) For all $g \in G$, we have $\mathrm{Supp}(g - \mathrm{LT}_\tau(g)) \cap \mathrm{LT}_\tau\{M\} = \emptyset$.

Proof. Analogous to Proposition 3.3.17. □

The unique τ-Gröbner basis G as in Proposition 5.2.3 is called the **reduced τ-Gröbner basis of M**. A τ-Gröbner basis satisfying condition 5.2.3.a is called a **minimal τ-Gröbner basis**.

We shall mention that Gröbner bases in F_r can be characterized through the leading term modules and the leading term sets as follows. Given a $K\langle X\rangle$-submodule $M \subseteq F_r \setminus \{0\}$ and a subset $G \subseteq M \setminus \{0\}$, G is a τ-Gröbner basis of M if and only if the set $\mathrm{LT}_\tau\{G\}$ generates the leading term module $\mathrm{LT}_\tau(M)$. The proof of this characterization proceeds as the proofs of Propositions 3.3.3 and 3.3.4. We shall also mention that Gröbner bases can be successfully characterized through rewrite rules (see [8, 9]). For the purposes of computing Gröbner bases, we shall now consider Gröbner bases from the point of view of syzygy modules.

In what follows, we let $s \geq 1, g_1, \ldots, g_s \in F_r\backslash\{0\}$, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$, and $\mathrm{LM}_\tau(\mathcal{G})$ the tuple $(\mathrm{LM}_\tau(g_1), \ldots, \mathrm{LM}_\tau(g_s))$. Moreover, we let $F_s = (K\langle X\rangle \otimes K\langle X\rangle)^s$ be the free $K\langle X\rangle$-bimodule of rank s with the canonical basis $\{\epsilon_1, \ldots, \epsilon_s\}$. We define the $K\langle X\rangle$-bimodule homomorphisms $\lambda : F_s \to F_r$ given by $\lambda(\epsilon_i) = g_i$ for $i = 1, \ldots, s$, and $\Lambda : F_s \to F_r$ given by $\Lambda(\epsilon_i) = \mathrm{LM}_\tau(g_i)$ for $i = 1, \ldots, s$.

Definition 5.2.4. Using the notation above, we define syzygy and syzygy module as follows.

a) The kernel of the module homomorphism $\lambda : F_s \to F_r$, i.e.

$$\ker(\lambda) = \{\sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_s \mid \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} = 0\},$$

is called the **two-sided syzygy module** of $\mathcal{G}$ and is denoted by $\mathrm{Syz}(\mathcal{G})$. An element in $\mathrm{Syz}(\mathcal{G})$ is called a **two-sided syzygy** of $\mathcal{G}$.

b) Similarly, the kernel of the module homomorphism $\Lambda : F_s \to F_r$, i.e.

$$\ker(\Lambda) = \{\sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_s \mid \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \mathrm{LT}_\tau(g_i) w'_{ij} = 0\},$$

is called the **two-sided syzygy module** of $\mathrm{LM}_\tau(\mathcal{G})$ and is denoted by $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$. An element in $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ is called a **two-side syzygy** of $\mathrm{LM}_\tau(\mathcal{G})$.

Recall that $K\langle X\rangle$ is $\langle X\rangle$-graded (see Example 2.2.16). Obviously F_r is a $\mathbb{T}(F_r)$-graded $K\langle X\rangle$-bimodule. The tuple $\mathcal{G}$ together with the module term ordering τ induces a $\mathbb{T}(F_r)$-grading on F_s as follows. For $t \in \mathbb{T}(F_r)$, we let

$$F_s(t) = \{\sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_s \mid \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \mathrm{LT}_\tau(g_i) w'_{ij} \in Kt\}.$$

Then F_s becomes a $\mathbb{T}(F_r)$-graded $K\langle X\rangle$-bimodule.

We have the following definitions and lemmas which are similar to the corresponding definitions and lemmas in Section 3.4.

Definition 5.2.5. Let $m = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_s \setminus \{0\}$.

a) The term

$$\max_\tau\{\mathrm{LT}_\tau(w_{ij} g_i w'_{ij}) \mid i \in \{1, \ldots, s\}, j \in \mathbb{N}, c_{ij} \neq 0\} \in \mathbb{T}(F_r)$$

is called **τ-degree** of m and is denoted by $\deg_{\tau,\mathcal{G}}(m)$.

b) The element $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} \bar{c}_{ij}\bar{w}_{ij}\epsilon_i\bar{w}'_{ij} \in F_s \setminus \{0\}$ given by

$$\bar{c}_{ij}\bar{w}_{ij}\epsilon_i\bar{w}'_{ij} = \begin{cases} c_{ij}w_{ij}\epsilon_i w'_{ij} & \text{if } c_{ij} \neq 0 \text{ and } \mathrm{LT}_\tau(w_{ij}g_iw'_{ij}) = \deg_{\tau,\mathcal{G}}(m), \\ 0 & \text{otherwise} \end{cases}$$

is called **τ-leading form** of m and is denoted by $\mathrm{LF}_{\tau,\mathcal{G}}(m)$.

c) m is called **homogeneous** of τ-degree $\deg_{\tau,\mathcal{G}}(m)$ if $\deg_{\tau,\mathcal{G}}(c_{ij}w_{ij}\epsilon_iw'_{ij}) = \deg_{\tau,\mathcal{G}}(m)$ for all $i \in \{1,\dots,s\}$ and all $j \in \mathbb{N}$ such that $c_{ij} \neq 0$.

Lemma 5.2.6. *For all $m \in F_s \setminus \mathrm{Syz}(\mathcal{G})$, we have $\mathrm{LT}_\tau(\lambda(m)) \leq_\tau \deg_{\tau,\mathcal{G}}(m)$. Moreover, $\mathrm{LT}_\tau(\lambda(m)) <_\tau \deg_{\tau,\mathcal{G}}(m)$ if and only if $\mathrm{LF}_{\tau,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$.*

Proof. Analogous to Lemma 3.4.5. □

Definition 5.2.7. A pair (i,j) with $i,j \in \{1,\dots,s\}$ and $i < j$ is called a **critical pair** of $\mathcal{G}$ if there exist $w_i, w'_i, w_j, w'_j \in \langle X\rangle$ such that $w_i\mathrm{LT}_\tau(g_i)w'_i = w_j\mathrm{LT}_\tau(g_j)w'_j$, and such that the common prefix of w_i and w_j is 1, and such that the common suffix of w'_i and w'_j is 1. The **set of all critical pairs** of $\mathcal{G}$ will be denoted by B. For critical pair $(i,j) \in B$, the element $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\tau(g_j)}w_j\epsilon_jw'_j \in F_s$ is called the **critical syzygy** of g_i and g_j, and the element $S_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)}w_ig_iw'_i - \frac{1}{\mathrm{LC}_\tau(g_j)}w_jg_jw'_j \in F_r$ is called the **S-element** of g_i and g_j.

It is clear that, for each pair $i,j \in \{1,\dots,s\}$ satisfying $i < j$, there exists at most one critical pair. Thus $|B| < \infty$. By Definitions 5.2.5 and 5.2.7, for each critical pair $(i,j) \in B$ the critical syzygy σ_{ij} is a syzygy of $\mathrm{LM}_\tau(\mathcal{G})$ and is homogeneous of τ-degree $\deg_{\tau,\mathcal{G}}(\sigma_{ij})$. Moreover, the following lemma holds.

Lemma 5.2.8. *We have $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G})) = \langle \sigma_{ij} \mid (i,j) \in B\rangle$.*

Proof. Analogous to Lemma 3.4.8.b. □

The following is the last ingredient we need for the purpose of characterizing Gröbner bases through syzygy modules.

Definition 5.2.9. An element $m \in F_s\setminus\{0\}$ is called a **lifting** of an element $\bar{m} \in F_s\setminus\{0\}$ if we have $\mathrm{LF}_{\tau,\mathcal{G}}(m) = \bar{m}$.

Proposition 5.2.10. *Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements which generates a $K\langle X\rangle$-submodule $M = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Then the following conditions are equivalent.*

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

b) There exists a homogeneous system of generators of $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ *with the property that every generator has a lifting in* $\mathrm{Syz}(\mathcal{G})$.

Proof. Let B be the set of all critical pairs of $\mathcal{G}$. The set $\{\sigma_{ij} \mid (i,j) \in B\}$ is a homogeneous system of generators of $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ by Lemma 5.2.8. Then the proof proceeds exactly as the proof of Proposition 3.4.11. □

Consequently, we obtain the following Buchberger Criterion.

Corollary 5.2.11. (Buchberger Criterion) *Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements which generates a $K\langle X\rangle$-submodule $M = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Moreover, let B be the set of all critical pairs of $\mathcal{G}$. Then the following conditions are equivalent.*

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

b) For all critical pairs $(i,j) \in B$, we have $\mathrm{NR}_{\tau,G}(S_{ij}) = 0$.

Proof. To prove condition a) implies condition b), note that by Proposition 5.2.2.b we have $\mathrm{NR}_{\tau,G}(S_{ij}) = \mathrm{NF}_{\tau,M}(S_{ij})$. It is clear that $S_{ij} \in M$. Thus we have $\mathrm{NF}_{\tau,M}(S_{ij}) = 0$ by Remark 5.1.11.c. Therefore $\mathrm{NR}_{\tau,G}(S_{ij}) = 0$.

To prove condition b) implies condition a), it suffices, by Lemma 5.2.8 and Proposition 5.2.10, to prove that the critical syzygy $\sigma_{ij} \in F_s$ has a lifting in $\mathrm{Syz}(\mathcal{G})$ for all critical pairs $(i,j) \in B$. By assumption and Theorem 5.1.12, there exist $c_1, \cdots, c_t \in K \setminus \{0\}, g_{i_1}, \ldots, g_{i_t} \in G, w_1, \ldots, w_t' \in \langle X\rangle$ such that $S_{ij} = \sum_{k=1}^t c_k w_k g_{i_k} w_k'$ and $\mathrm{LT}_\tau(S_{ij}) = \mathrm{LT}_\tau(w_1 g_{i_1} w_1') >_\tau \mathrm{LT}_\tau(w_2 g_{i_2} w_2') >_\tau \cdots >_\tau \mathrm{LT}_\tau(w_t g_{i_t} w_t')$. Let $h = \sigma_{ij} - \sum_{k=1}^t c_k w_k \epsilon_{i_k} w_k' \in F_s$. Since σ_{ij} is homogeneous and $\deg_{\tau,\mathcal{G}}(\sigma_{ij}) >_\tau \mathrm{LT}_\tau(S_{ij}) = \deg_{\tau,\mathcal{G}}(\sum_{k=1}^t c_k w_k \epsilon_{i_k} w_k')$, we have $\mathrm{LF}_{\tau,\mathcal{G}}(h) = \sigma_{ij}$. Clearly $\lambda(h) = 0$. Hence h is a lifting of σ_{ij} in $\mathrm{Syz}(\mathcal{G})$. □

One can check easily that Proposition 5.2.10 and Corollary 5.2.11 also hold if G is an infinite set. We formulate a Buchberger Procedure for enumerating Gröbner bases of finitely generated submodules in F_r as follows.

Theorem 5.2.12. (Buchberger Procedure) *Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements which generates a $K\langle X\rangle$-module $M = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Consider the following sequence of instructions.*

1) Let $s' = s$ and let B be the set of all critical pairs.

2) If $B = \emptyset$, return the result $\mathcal{G}$. Otherwise, select a critical pair $(i,j) \in B$ using a fair strategy and delete it from B.

3) Compute the S-element S_{ij} and its normal remainder $S'_{ij} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 2).

4) Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid i \in \{1,\dots,s'-1\},\ (i,s')$ is a critical pair$\}$ to the set B. Then continue with step 2).

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

Proof. See [8], Corollary 2.11. □

We shall end this section with an example, which shows that a finitely generated submodule need not have a finite Gröbner basis.

Example 5.2.13. Consider the free $\mathbb{Q}\langle x_1, x_2\rangle$-module F_2 of rank 2 and the module term ordering $\tau = \texttt{PosLLex}$ on $\mathbb{T}(F_2)$. Let $M \subseteq F_2$ be the $\mathbb{Q}\langle x_1, x_2\rangle$-submodule generated by the set $G = \{g_1, g_2\}$, where $g_1 = x_2x_1e_1x_2 + e_2, g_2 = e_1x_2^2 + x_1e_1$. We enumerate a τ-Gröbner basis of M using the Buchberger Procedure given in Theorem 5.2.12.

1) Let $\mathcal{G} = (g_1, g_2), s' = 2$, and $B = \{(1,2)\}$.

2) Select $(1,2)$ and let $B = \emptyset$.

3) Compute $S_{12} = g_1x_2 - x_2x_1g_2 = -x_2x_1^2e_1 + e_2x_2$ and $S'_{12} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{12}) = -x_2x_1^2e_1 + e_2x_2$.

4) Let $s' = 3, \mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = -x_2x_1^2e_1 + e_2x_2$, and $B = \{(2,3)\}$.

2) Select $(2,3)$ and let $B = \emptyset$.

3) Compute $S_{23} = x_2x_1^2g_2 + g_3x_2^2 = x_2x_1^3e_1 + e_2x_2^3$ and $S'_{23} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{23}) = x_2x_1^3e_1 + e_2x_2^3$.

4) Let $s' = 4, \mathcal{G} = (g_1, g_2, g_3, g_4)$ with $g_4 = x_2x_1^3e_1 + e_2x_2^3$, and $B = \{(2,4)\}$.

2) Select $(2,4)$ and let $B = \emptyset$.

3) Compute $S_{24} = x_2x_1^3g_2 - g_4x_2^2 = x_2x_1^4e_1 - e_2x_2^5$ and $S'_{24} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{24}) = x_2x_1^4e_1 - e_2x_2^5$.

4) Let $s' = 5, \mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ with $g_5 = x_2x_1^4e_1 - e_2x_2^5$, and $B = \{(2,5)\}$.

It is easy to check that the procedure goes on forever. We want to show that M has the infinite reduced τ-Gröbner basis $G = \{g_1, g_2\} \cup \{g_k \mid k \geq 3\}$ with $g_k = x_2x_1^{k-1}e_1 + (-1)^k e_2x_2^{2k-5}$. It is clear that $M \subseteq \langle G\rangle$. From $g_3 = -g_1x_2 + x_2x_1g_2$ and $g_k = x_2x_1^{k-2}g_2 - g_{k-1}x_2^2$ for all $k \geq 4$, we conclude that $\langle G\rangle \subseteq M$. Therefore $M = \langle G\rangle$. It is easy to check that the set of all critical pairs of G is $B = \{(1,2),(2,k) \mid k \geq 3\}$. We are going to show that $\mathrm{NR}_{\tau,G}(S_{12}) = 0$ and $\mathrm{NR}_{\tau,G}(S_{2k}) = 0$ for all $k \geq 3$, and then G is a τ-Gröbner basis of M using Corollary 5.2.11. The critical syzygy of $(1,2)$ is $\sigma_{12} = \epsilon_1x_2 - x_2x_1\epsilon_2$ and the S-element $S_{12} = -x_2x_1^2e_1 + e_2x_2 = -g_3$. Thus $\mathrm{NR}_{\tau,G}(S_{12}) = 0$. For $k \geq 3$, the critical syzygy of $(2,k)$ is $\sigma_{2k} = x_2x_1^{k-1}\epsilon_2 - \epsilon_kx_2^2$ and the S-element $S_{2k} = x_2x_1^{k-1}(e_1x_2^2 + x_1e_1) - (x_2x_1^{k-1}e_1 + (-1)^k e_2x_2^{2k-5})x_2^2 = x_2x_1^ke_1 + (-1)^{k+1}e_2x_2^{2k-3} = g_{k+1}$. Thus $\mathrm{NR}_{\tau,G}(S_{2k}) = 0$. Finally, G is the infinite reduced τ-Gröbner basis of M, because $\mathrm{LT}_\tau\{G\} = \{x_2x_1e_1x_2, e_1x_2^2, x_2x_1^{k-1}e_1 \mid k \geq 3\} \subseteq \mathbb{T}(F_2)$ and G are interreduced sets and $\mathrm{LT}_\tau(g_i) = 1$ for all $g_i \in G$.

5.3 Improved Buchberger Procedures

Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements which generates a $K\langle X\rangle$-submodule $M = \langle G\rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Moreover, let B be the set of all critical pairs of $\mathcal{G}$, and let $\Sigma = \{\sigma_{ij} \mid (i,j) \in B\}$ be the set of critical syzygies. By Proposition 5.2.10, G is a τ-Gröbner basis of M if and only if there is a homogeneous system of generators of the syzygy module $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ consisting entirely of elements which have a lifting in the syzygy module $\mathrm{Syz}(\mathcal{G})$. By Lemma 5.2.8, Σ is a homogeneous system of generators of $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$. During the Buchberger Procedure (see Theorem 5.2.12), the existence of a lifting of each element in Σ is checked by the Division Algorithm, which tends to be expensive. Our main goal in this section is to improve the Buchberger Procedure by detecting unnecessary critical pairs, i.e. the critical pairs whose associated critical syzygies are redundant (see Definition 5.3.7). We shall achieve this goal by generalizing our methods for improving the Buchberger Procedure in free monoid rings (see Section 4.2) to F_r. We also present an improvement of the Buchberger Procedure related to redundant generators.

In what follows, we let $F_s = (K\langle X\rangle \otimes K\langle X\rangle)^s$ be the free $K\langle X\rangle$-bimodule of rank s with the canonical basis $\{\epsilon_1, \ldots, \epsilon_s\}$. For our purposes, we shall define the module term ordering $\widehat{\tau}$ on $\mathbb{T}(F_s)$ induced by $(\tau, \mathcal{G})$ as follows (compare with Example 5.1.2).

Definition 5.3.1. Let τ be a module term ordering on $\mathbb{T}(F_r)$, and let $\mathcal{G} = (g_1, \ldots, g_s) \in (F_r \setminus \{0\})^s$ be a tuple of elements. The module term ordering $\widehat{\tau}$ on $\mathbb{T}(F_s)$ induced by $(\tau, \mathcal{G})$ as follows. For all $w_1\epsilon_i w_1', w_2\epsilon_j w_2' \in \mathbb{T}(F_s)$ with $i, j \in \{1, \ldots, s\}$ and $w_1, w_1', w_2, w_2' \in \langle X\rangle$, we say that $w_1\epsilon_i w_1' \geq_{\widehat{\tau}} w_2\epsilon_j w_2'$ if we have $w_1\mathrm{LT}_\tau(g_i)w_1' >_\tau w_2\mathrm{LT}_\tau(g_j)w_2'$, or if we have $w_1\mathrm{LT}_\tau(g_i)w_1' = w_2\mathrm{LT}_\tau(g_j)w_2'$ and $i \geq j$.

By Definitions 5.2.7 and 5.3.1, for each critical pair $(i, j) \in B$ the critical syzygy $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)} w_i\epsilon_i w_i' - \frac{1}{\mathrm{LC}_\tau(g_j)} w_j\epsilon_j w_j' \in F_s$ satisfies $\mathrm{LT}_{\widehat{\tau}}(\sigma_{ij}) = w_j\epsilon_j w_j'$. Furthermore, we order critical syzygies in Σ with respect to $\widehat{\tau}$ as follows. For two critical syzygies $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)} w_i\epsilon_i w_i' - \frac{1}{\mathrm{LC}_\tau(g_j)} w_j\epsilon_j w_j', \sigma_{kl} = \frac{1}{\mathrm{LC}_\tau(g_k)} w_k\epsilon_k w_k' - \frac{1}{\mathrm{LC}_\tau(g_l)} w_l\epsilon_l w_l' \in \Sigma$, we say that $\sigma_{ij} \geq_{\widehat{\tau}} \sigma_{kl}$ if we have $w_j\epsilon_j w_j' >_{\widehat{\tau}} w_l\epsilon_l w_l'$, or if we have $w_j\epsilon_j w_j' = w_l\epsilon_l w_l'$ and $w_i\epsilon_i w_i' \geq_{\widehat{\tau}} w_k\epsilon_k w_k'$. It is easy to verify that $\widehat{\tau}$ is a well-ordering on Σ.

The crucial idea of our method is to detect critical pairs whose associated critical syzygies can be generated by smaller critical syzygies with respect to $\widehat{\tau}$. Then by Lemma 5.2.8 we get a smaller homogeneous system of generator of $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$. Finally, using Proposition 5.2.10 we achieve our desired improvement of the Buchberger Procedure.

Remark 5.3.2. Let us collect some observations.

a) Let $(i, k), (j, k) \in B$ be two distinct critical pairs with associated critical syzygies $\sigma_{ik} = \frac{1}{\mathrm{LC}_\tau(g_i)} w_i\epsilon_i w_i' - \frac{1}{\mathrm{LC}_\tau(g_k)} w_{ki}\epsilon_k w_{ki}'$ and $\sigma_{jk} = \frac{1}{\mathrm{LC}_\tau(g_j)} w_j\epsilon_j w_j' - \frac{1}{\mathrm{LC}_\tau(g_k)} w_{kj}\epsilon_k w_{kj}'$, respectively. If there exist $w, w' \in \langle X\rangle$ such that $w_{ki} = ww_{kj}, w_{ki} = w_{kj}'w'$, then we have
$$\sigma_{ik} - w\sigma_{jk}w' = \frac{1}{\mathrm{LC}_\tau(g_i)} w_i\epsilon_i w_i' - \frac{1}{\mathrm{LC}_\tau(g_j)} ww_j\epsilon_j w_j' w'$$
where $\frac{1}{\mathrm{LC}_\tau(g_i)} w_i\epsilon_i w_i' - \frac{1}{\mathrm{LC}_\tau(g_j)} ww_j\epsilon_j w_j' w'$ is a multiple of $\sigma_{i'j'}$, where $i' = \min\{i, j\}$, $j' = \max\{i, j\}$. Obviously $\sigma_{ik} >_{\widehat{\tau}} \sigma_{i'j'}$. By the definition of $\widehat{\tau}$ on Σ, we have $\sigma_{ik} >_{\widehat{\tau}} \sigma_{jk}$ if and only if $i > j$ or $i < j$ and $ww' \neq 1$.

b) Let $(j, i), (i, k) \in B$ be two distinct critical pairs with associated critical syzygies $\sigma_{ji} = \frac{1}{\mathrm{LC}_\tau(g_j)} w_j\epsilon_j w_j' - \frac{1}{\mathrm{LC}_\tau(g_i)} w_{ij}\epsilon_i w_{ij}'$ and $\sigma_{ik} = \frac{1}{\mathrm{LC}_\tau(g_i)} w_{ik}\epsilon_i w_{ik}' - \frac{1}{\mathrm{LC}_\tau(g_k)} w_k\epsilon_k w_k'$, respectively. If there exist $w, w' \in \langle X\rangle$ such that $w_{ik} = ww_{ij}, w'_{ik} = w_{ij}w'$, then we have

$$\sigma_{ik} + w\sigma_{ji}w' = \frac{1}{\mathrm{LC}_\tau(g_j)}ww_j\epsilon_jw'_jw' - \frac{1}{\mathrm{LC}_\tau(g_k)}w_k\epsilon_kw'_k$$

where $\frac{1}{\mathrm{LC}_\tau(g_j)}ww_j\epsilon_jw'_jw' - \frac{1}{\mathrm{LC}_\tau(g_k)}w_k\epsilon_kw'_k$ is a multiple of σ_{jk}. Clearly $\sigma_{ik} >_{\widehat{\tau}} \sigma_{ji}$ and $\sigma_{ik} >_{\widehat{\tau}} \sigma_{jk}$. However, we shall show later that this case is unlikely to happen after removing unnecessary critical pairs detected by a) (see Proposition 5.3.4).

c) Let $(i,j) \in B$ be a critical pair with associated critical syzygy $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\tau(g_j)}w_j\epsilon_jw'_j$, and let $g_k \in \mathcal{G}$ with $k > j$. If there exist $w, w' \in \langle X\rangle$ such that $w_j\mathrm{LT}_\tau(g_j)w'_j = w\mathrm{LT}_\tau(g_k)w'$, then we have

$$\sigma_{ij} = (\frac{1}{\mathrm{LC}_\tau(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\tau(g_k)}w\epsilon_kw') - (\frac{1}{\mathrm{LC}_\tau(g_j)}w_j\epsilon_jw'_j - \frac{1}{\mathrm{LC}_\tau(g_k)}w\epsilon_kw')$$

where $\frac{1}{\mathrm{LC}_\tau(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\tau(g_k)}w\epsilon_kw'$ and $\frac{1}{\mathrm{LC}_\tau(g_j)}w_j\epsilon_jw'_j - \frac{1}{\mathrm{LC}_\tau(g_k)}w\epsilon_kw'$ are multiples of σ_{ik} and σ_{jk}, respectively. By the definition of $\widehat{\tau}$ on Σ, we have $\sigma_{ij} >_{\widehat{\tau}} \sigma_{ik}$ and $\sigma_{ij} >_{\widehat{\tau}} \sigma_{jk}$ if and only if $w\epsilon_kw'$ is a proper multiple of $\mathrm{LT}_{\widehat{\tau}}(\sigma_{ik})$ and $\mathrm{LT}_{\widehat{\tau}}(\sigma_{jk})$.

Based on these observations we have the following proposition.

Proposition 5.3.3. *Let B be the set of all critical pairs of $\mathcal{G}$. Consider the following sequence of instructions.*

a) Remove from B all pairs (i,k) with the property that there exist $w, w' \in \langle X\rangle$ and a pair $(j,k) \in B$ such that $\mathrm{LT}_{\widehat{\tau}}(\sigma_{ik}) = w\mathrm{LT}_{\widehat{\tau}}(\sigma_{jk})w'$ and such that either $i > j$ or $i < j$ and $ww' \neq 1$. Denote the resulting set of critical pairs by B'.

b) Remove from B' all pairs (i,j) with associated critical syzygy $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)}w_i\epsilon_iw'_i - \frac{1}{\mathrm{LC}_\tau(g_j)}w_j\epsilon_jw'_j$ and with the property that there exist $w, w' \in \langle X\rangle$ and $g_k \in \mathcal{G}$ with $k > j$ such that $w_j\mathrm{LT}_\tau(g_j)w'_j = w\mathrm{LT}_\tau(g_k)w'$ and such that $w\epsilon_kw'$ is a proper multiple of $\mathrm{LT}_{\widehat{\tau}}(\sigma_{ik})$ and $\mathrm{LT}_{\widehat{\tau}}(\sigma_{jk})$. Denote the resulting set of critical pairs by B''.

Then we have $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G})) = \langle \sigma_{ij} \mid (i,j) \in B''\rangle$.

Proof. This follows immediately from Lemma 5.2.8 and Remark 5.3.2. □

It is clear that, for any two elements σ_{ij}, σ_{kl} of $\{\sigma_{ij} \mid (i,j) \in B'\}$, neither $\mathrm{LT}_{\widehat{\tau}}(\sigma_{ij})$ is a multiple of $\mathrm{LT}_{\widehat{\tau}}(\sigma_{kl})$ nor $\mathrm{LT}_{\widehat{\tau}}(\sigma_{kl})$ is a multiple of $\mathrm{LT}_{\widehat{\tau}}(\sigma_{ij})$. Moreover, the following proposition shows that the set $\{\sigma_{ij} \mid (i,j) \in B'\}$ is actually interreduced.

Proposition 5.3.4. *Let B' be the set of critical pairs as in Proposition 5.3.3.a, and let $(i,k) \in B'$ be a critical pair whose critical syzygy is $\sigma_{ik} = \frac{1}{\mathrm{LC}_\tau(g_i)} w_{ik}\epsilon_i w'_{ik} - \frac{1}{\mathrm{LC}_\tau(g_k)} w_k \epsilon_k w'_k$. Then there is no critical pair $(j,i) \in B'$ such that $w_{ik}\epsilon_i w'_{ik}$ is a multiple of $\mathrm{LT}_{\hat{\tau}}(\sigma_{ji})$.*

Proof. For a contradiction, suppose that there exists a critical pair $(j,i) \in B'$ with associated critical syzygy $\sigma_{ji} = \frac{1}{\mathrm{LC}_\tau(g_j)} w_j \epsilon_j w'_j - \frac{1}{\mathrm{LC}_\tau(g_i)} w_{ij}\epsilon_i w'_{ij}$ such that $ww_{ij}\epsilon_i w'_{ij}w' = w_{ik}\epsilon_i w'_{ik}$ for some $w, w' \in \langle X \rangle$. Then we have $\sigma_{ik} + w\sigma_{ji}w' = \frac{1}{\mathrm{LC}_\tau(g_j)} ww_j\epsilon_j w'_j w' - \frac{1}{\mathrm{LC}_\tau(g_k)} w_k\epsilon_k w'_k$, which is a multiple of $\sigma_{jk} \in B$. Obviously $\sigma_{jk} <_{\hat{\tau}} \sigma_{ik}$. Thus σ_{ik} is removed from B in Proposition 5.3.3.a due to σ_{jk}: a contradiction. □

Note that Proposition 5.3.3 is a generalization of the *Gebauer-Möller Installation* (see [33]) in F_r. Using Proposition 5.3.3, we shall improve the Buchberger Procedure as follows.

Theorem 5.3.5. (Improved Buchberger Procedure I) *In the situation of Theorem 5.2.12, we replace step 4) by the following sequence of instructions.*

4a) Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and form the set $B(s') = \{(i,s') \mid i \in \{1,\dots,s'-1\}, (i,s')$ is a critical pair$\}$.

4b) Remove from $B(s')$ all pairs (i,s') with the property that there exist $w, w' \in \langle X \rangle$ and $(j,s') \in B(s')$ such that $\mathrm{LT}_{\hat{\tau}}(\sigma_{is'}) = w\mathrm{LT}_{\hat{\tau}}(\sigma_{js'})w'$ and such that either $i > j$ or $i < j$ and $ww' \neq 1$.

4c) Remove from B all pairs (i,j) with associated critical syzygy $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)} w_i\epsilon_i w'_i - \frac{1}{\mathrm{LC}_\tau(g_j)} w_j\epsilon_j w'_j$, which has the property that there exist $w, w' \in \langle X \rangle$ such that $w_j \mathrm{LT}_\tau(g_j) w'_j = w\mathrm{LT}_\tau(g_{s'})w'$ and such that $w\epsilon_{s'}w'$ is a proper multiple of $\mathrm{LT}_{\hat{\tau}}(\sigma_{is'})$ and $\mathrm{LT}_{\hat{\tau}}(\sigma_{js'})$.

4d) Replace B by $B \cup B(s')$ and continue with step 2).

Then the resulting set of instructions is a procedure that enumerates a τ-Gröbner basis $\mathcal{G}$ of M. If M has a finite τ-Gröber basis, it stops after finitely many steps and the resulting tuple $\mathcal{G}$ is a finite τ-Gröbner basis of M.

Proof. This follows from Propositions 5.2.10 and 5.3.3 and Theorem 5.2.12. □

The following example shows the effectiveness of our improvement.

Example 5.3.6. Consider the free $\mathbb{Q}\langle x_1, x_2 \rangle$-module F_2 of rank 2 equipped with the module term ordering $\tau = \mathtt{PosLLex}$ on $\mathbb{T}(F_2)$. Let $M \subseteq F_2$ be the $\mathbb{Q}\langle x_1, x_2 \rangle$-submodule generated by the set $G = \{g_1, g_2\}$, where $g_1 = x_2x_1e_1x_2 + e_1, g_2 = e_1x_2^2 + x_1e_2$ (cf. [9]). We enumerate a τ-Gröbner basis of M using the Improved Buchberger Procedure I given in Theorem 5.3.5.

1) Let $\mathcal{G} = (g_1, g_2), s' = 2$, and $B = \{(1, 2)\}$ with $\sigma_{12} = \epsilon_1x_2 - x_2x_1\epsilon_2$.

2) Select $(1, 2)$ and let $B = \emptyset$.

3) Compute $S_{12} = e_1x_2 - x_2x_1^2e_2$ and $S'_{12} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{12}) = e_1x_2 - x_2x_1^2e_2$.

4a) Let $s' = 3, \mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = e_1x_2 - x_2x_1^2e_2$, and $B(3) = \{(1, 3), (2, 3)\}$ with $\sigma_{13} = \epsilon_1 - x_2x_1\epsilon_3, \sigma_{23} = \epsilon_2 - \epsilon_3x_2$.

4d) Let $B = \{(1, 3), (2, 3)\}$. Note that $\sigma_{13} >_{\widehat{\tau}} \sigma_{23}$.

2) Select $(2, 3)$ and let $B = \{(1, 3)\}$.

3) Compute $S_{23} = x_2x_1^2e_2x_2 + x_1e_2$ and $S'_{23} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{23}) = x_2x_1^2e_2x_2 + x_1e_2$.

4a) Let $s' = 4, \mathcal{G} = (g_1, g_2, g_3, g_4)$ with $g_4 = x_2x_1^2e_2x_2 + x_1e_2$, and $B(4) = \emptyset$.

2) Select $(1, 3)$ and let $B = \emptyset$.

3) Compute $S_{13} = e_1 + x_2x_1x_2x_1^2e_2$ and $S'_{13} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{13}) = e_1 + x_2x_1x_2x_1^2e_2$.

4a) Let $s' = 5, \mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ with $g_5 = e_1 + x_2x_1x_2x_1^2e_2$, and $B(5) = \{(1, 5), (2, 5), (3, 5)\}$ with $\sigma_{15} = \epsilon_1 - x_2x_1\epsilon_5x_2, \sigma_{25} = \epsilon_2 - \epsilon_5x_2^2, \sigma_{35} = \epsilon_3 - \epsilon_5x_2$.

4b) Remove $(1, 5), (2, 5)$ from $B(5)$, since $\mathrm{LT}_{\widehat{\tau}}(\sigma_{15}) = x_2x_1\epsilon_5x_2, \mathrm{LT}_{\widehat{\tau}}(\sigma_{25}) = \epsilon_5x_2^2$ are proper multiples of $\mathrm{LT}_{\widehat{\tau}}(\sigma_{35}) = \epsilon_5x_2$.

4d) Let $B = \{(3, 5)\}$.

2) Select $(3, 5)$ and let $B = \emptyset$.

3) Compute $S_{35} = -x_2x_1x_2x_1^2e_2x_2 - x_2x_1^2e_2$ and $S'_{35} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{35}) = 0$.

2) Since $B = \emptyset$, return the tuple $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$.

Hence $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ is a τ-Gröbner basis of M. During the computation, the total number of critical pairs is 6, and 2 unnecessary critical pairs are detected. We conclude that our method improves the Buchberger Procedure efficiently.

Our next improvement of the Buchberger Procedure is related to redundant generators. In Section 3.3 we defined redundant generators through Gröbner bases (see Definition 3.3.13). In the literature, a more standard and precise meaning of the adjective "redundant" should be as follows.

Definition 5.3.7. Let $G \subseteq F_r \setminus \{0\}$ be a set of elements which generates a $K\langle X\rangle$-submodule $M = \langle G\rangle$. An element $g \in G$ is called **redundant** if the set $G \setminus \{g\}$ still generates M.

In general it is not a trivial task to determine whether or not a generator is redundant. Given a Gröbner basis, the following proposition enables us to detect redundant generators of some pattern.

Proposition 5.3.8. *Let $M \subseteq F_r \setminus \{0\}$ be a $K\langle X\rangle$-submodule, and let G be a τ-Gröbner basis of M. If $g \in G$ has the property that there exists an element $g' \in G \setminus \{g\}$ such that $\mathrm{LT}_\tau(g)$ is a multiple of $\mathrm{LT}_\tau(g')$, then g is redundant. Furthermore, the set $G \setminus \{g\}$ is still a τ-Gröbner basis of M.*

Proof. Analogous to Proposition 3.3.14. □

Example 5.3.9. **(continued)** Consider Example 5.3.6 again. In this example we obtain a τ-Gröbner basis $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ of M, where $g_1 = x_2x_1e_1x_2 + e_1, g_2 = e_1x_2^2 + x_1e_2, g_3 = e_1x_2 - x_2x_1^2e_2, g_4 = x_2x_1^2e_2x_2 + x_1e_2$, and $g_5 = e_1 + x_2x_1x_2x_1^2e_2$. Since $\mathrm{LT}_\tau(g_1) = x_2x_1e_1x_2, \mathrm{LT}_\tau(g_2) = e_1x_2^2, \mathrm{LT}_\tau(g_3) = e_1x_2$ are multiples of $\mathrm{LT}_\tau(g_5) = e_1$, the generators g_1, g_2, g_3 are redundant and the set $\{g_4, g_5\}$ is again a τ-Gröbner basis of M.

Using Proposition 5.3.8, we have the following straightforward generalization of Theorem 4.2.24 and Corollary 4.2.25. The proofs of the correctness and the termination proceed exactly as the proofs of Theorem 4.2.24 and Corollary 4.2.25.

Theorem 5.3.10. **(Improved Buchberger Procedure II)** *Let $G \subseteq F_r \setminus \{0\}$ be a set of elements which generates a $K\langle X\rangle$-submodule $M = \langle G\rangle$. Consider the following sequence of instructions.*

1) *Interreduce the system of generators G using the Interreduction Algorithm given in Corollary 5.1.14.*

2) *Let $\mathcal{G}$ be an associated tuple of G, let $s' = |\mathcal{G}|$, let $\mathcal{T}$ be the tuple $(t_1, \ldots, t_{s'})$ with $t_i =$ true for all $i \in \{1, \ldots, s'\}$, and let B be the set of all critical pairs.*

3) *If $B = \emptyset$, return the subtuple $\mathcal{G}'$ of $\mathcal{G}$ consisting of the elements g_i such that $t_i = \text{true}$. Otherwise, select a critical pair $(i,j) \in B$ using a fair strategy and delete it from B.*

4) *Let $\mathcal{G}'$ be the subtuple of $\mathcal{G}$ consisting of the elements g_i such that $t_i = \text{true}$. Compute the S-element S_{ij} and its normal remainder $S'_{ij} = \mathrm{NR}_{\tau,\mathcal{G}'}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).*

5) *Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, append $t_{s'} = true$ to the tuple $\mathcal{T}$, and append the set $\{(i,s') \mid i \in \{1,\ldots,s'-1\}, t_i = \text{true}, (i,s')$ is a critical pair$\}$ to the set B.*

6) *For every $i \in \{1,\ldots,s'-1\}$, let $t_i = \text{false}$ if $\mathrm{LT}_\tau(g_i)$ is a multiple of $\mathrm{LT}_\tau(g_{s'})$. Then continue with step 3).*

This is a procedure that enumerates a minimal τ-Gröbner basis of M. If M has a finite τ-Gröber basis, it stops after finitely many steps and the resulting tuple is a finite minimal τ-Gröbner basis of M.

We end this section by applying the Improved Buchberger Procedure II to Example 5.3.6.

Example 5.3.11. (continued) Consider Example 5.3.6 again. Recall that in the example we have $\mathbb{Q}\langle x_1,x_2\rangle$-submodule $M = \langle g_1, g_2\rangle \subseteq F_2$ with $g_1 = x_2x_1e_1x_2 + e_1, g_2 = e_1x_2^2 + x_1e_2$ and the module term ordering $\tau = \texttt{PosLLex}$. Now we enumerate a τ-Gröbner basis of M using the Improved Buchberger Procedure II given in Theorem 5.3.10.

1) $G = \{g_1, g_2\}$ is an interreduced system of generators.

2) Let $\mathcal{G} = (g_1, g_2), s' = 2, \mathcal{T} = (t_1, t_2)$ with $t_1 = t_2 = \text{true}$, and $B = \{(1,2)\}$ with $\sigma_{12} = \epsilon_1x_2 - x_2x_1\epsilon_2$.

3) Select $(1,2)$ and let $B = \emptyset$.

4) Let $\mathcal{G}' = (g_1, g_2)$. Compute $S_{12} = e_1x_2 - x_2x_1^2e_2$ and $S'_{12} = \mathrm{NR}_{\tau,\mathcal{G}'}(S_{12}) = e_1x_2 - x_2x_1^2e_2$.

5) Let $s' = 3, \mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = e_1x_2 - x_2x_1^2e_2$, $\mathcal{T} = (t_1, t_2, t_3)$ with $t_3 = \text{true}$, and $B = \{(1,3),(2,3)\}$ with $\sigma_{13} = \epsilon_1 - x_2x_1\epsilon_3, \sigma_{23} = \epsilon_2 - \epsilon_3x_2$.

6) Let $t_1 = t_2 =$ false, since $\mathrm{LT}_\tau(g_1) = x_2x_1e_1x_2, \mathrm{LT}_\tau(g_2) = e_1x_2^2$ are multiples of $\mathrm{LT}_\tau(g_3) = e_1x_2$.

3) Select $(2, 3)$ and let $B = \{(1, 3)\}$.

4) Let $\mathcal{G}' = (g_3)$. Compute $S_{23} = x_2x_1^2e_2x_2 + x_1e_2$ and $S'_{23} = \mathrm{NR}_{\tau,\mathcal{G}'}(S_{23}) = x_2x_1^2e_2x_2 + x_1e_2$.

5) Let $s' = 4, \mathcal{G} = (g_1, g_2, g_3, g_4)$ with $g_4 = x_2x_1^2e_2x_2 + x_1e_2$, $\mathcal{T} = (t_1, t_2, t_3, t_4)$ with $t_4 =$ true.

3) Select $(1, 3)$ and let $B = \emptyset$.

4) Let $\mathcal{G}' = (g_3, g_4)$. Compute $S_{13} = e_1 + x_2x_1x_2x_1^2e_2$ and $S'_{13} = \mathrm{NR}_{\tau,\mathcal{G}'}(S_{13}) = e_1 + x_2x_1x_2x_1^2e_2$.

5) Let $s' = 5, \mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ with $g_5 = e_1 + x_2x_1x_2x_1^2e_2$, $\mathcal{T} = (t_1, t_2, t_3, t_4, t_5)$ with $t_5 =$ true, and $B = \{(3, 5)\}$ with $\sigma_{35} = \epsilon_3 - \epsilon_5x_2$.

6) Let $t_s =$ false, since $\mathrm{LT}_\tau(g_3) = e_1x_2$ is a multiple of $\mathrm{LT}_\tau(g_5) = e_1$.

3) Select $(3, 5)$ and let $B = \emptyset$.

4) Let $\mathcal{G}' = (g_4, g_5)$. Compute $S_{35} = -x_2x_1x_2x_1^2e_2x_2 - x_2x_1^2e_2$ and $S'_{35} = \mathrm{NR}_{\tau,\mathcal{G}'}(S_{35}) = 0$.

3) Since $B = \emptyset$, return the tuple $\mathcal{G} = (g_4, g_5)$.

Hence $\mathcal{G} = (g_4, g_5)$ is a minimal τ-Gröbner basis of M. During the computation, redundant generators g_1, g_2, g_3 are detected. Consequently, unnecessary critical pairs $(1, 5)$ and $(2, 5)$ are "removed" because of the redundancy of g_1 and g_2.

5.4 The F4 Procedure

Since the sixties of the past century, great efforts have been made to improve the classical Buchberger Algorithm (or Procedure) for computing (or enumerating) Gröbner bases effectively and efficiently in both the commutative and the non-commutative cases. There are mainly two directions. One is to develop powerful criteria to remove unnecessary critical pairs (or obstructions). In the commutative case, we refer to

[12, 13, 17, 33, 43, 44] for more details. In the non-commutative case, we refer to Sections 4.2 and 5.3 of this thesis for details. Another direction is to play with strategies during Gröbner basis computations, for instance, the sugar cube strategy (see [4, 34]), FGLM techniques (see [3, 28]), et cetera. In [26], J.-C. Faugère described a new efficient algorithm, called the *F4 Algorithm*, for computing Gröbner bases in commutative polynomial rings. The main idea of the F4 Algorithm is to represent several polynomials in a matrix form by a symbolic preprocessing step, then compute a row echelon form of the matrix, and hence reduce several polynomials by a list of polynomials simultaneously. The F4 Algorithm takes advantage of sophisticated techniques in linear algebra as well as rapidly developing techniques in parallel computing. As a result, it is able to handle many previously untractable problems. Later, J.-C. Faugère [27] also took into account unnecessary critical pairs and proposed the F5 Algorithm.

In this section we shall generalize the F4 Algorithm to the non-commutative case. Since Gröbner bases of submodules may be infinite (see Example 5.2.13), we have to content ourselves with the F4 Procedure which enumerates Gröbner bases. Note that the main goal of this section is to explicitly show the viability of this generalization. Hence we shall not concern ourselves with further optimizations of the F4 Procedure except for the improvements we obtained in the last section.

The fundamental step to formulate an F4 Procedure is to build a connection between a (finite) set of elements in F_r and a linear system of equations over K. We construct this connection in the following definition and illustrate it through a concrete example. Recall that we let τ is a module term ordering on $\mathbb{T}(F_r)$ (see Assumption 5.1.5).

Definition 5.4.1. Let $\mathcal{T} = (t_1, \ldots, t_m) \in (\mathbb{T}(F_r))^m$ be an ordered tuple of terms with respect to τ, i.e. $t_1 >_\tau \cdots >_\tau t_m$, and let K^m be the vector space of rank m over K. We define a bijective linear map $\Psi : \mathrm{Span}_K(\mathcal{T}) \to K^m$ given by $\Psi(t_i) = \eta_i$, where η_i is the i^{th} canonical basis of K^m, i.e. $\eta_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 occurring in the i^{th} position for $i = 1, \ldots, m$.

a) Let $G = \{g_1, \ldots, g_s\} \subseteq F_r$ be a set of elements. Assume that $\mathcal{T}$ consists of all terms in $\cup_{i=1}^s \mathrm{Supp}(g_i)$. We construct a matrix $M_G \in \mathrm{Mat}_{s\times m}(K)$ whose j^{th} row vector is $\Psi(g_j)$, and we call M_G a **matrix form** of G with respect to τ.

b) Conversely, let $M \in \mathrm{Mat}_{s\times m}(K)$ be a matrix. We construct a set $G_M \subseteq F_r$ consisting of the elements $\Psi^{-1}(m_j)$ where m_j is the j^{th} row vector of M, and we call G_M a **polynomial form** of M with respect to τ.

Example 5.4.2. Consider the free $\mathbb{Q}\langle x_1, x_2\rangle$-module F_2 of rank 2 equipped with the module term ordering $\tau = \texttt{PosLLex}$ on $\mathbb{T}(F_2)$. Let $G = \{g_1, g_2\} \subseteq F_2$ be a set where $g_1 = x_2x_1e_1x_2^2 + e_1x_2, g_2 = x_2x_1e_1x_2^2 + x_2x_1^2e_2$, and let $\mathcal{T} = (x_2x_1e_1x_2^2, e_1x_2, x_2x_1^2e_2)$. The matrix form of G with respect to τ is as follows.

$$\begin{array}{cc} & \begin{array}{ccc} x_2x_1e_1x_2^2 & e_1x_2 & x_2x_1^2e_2 \end{array} \\ \begin{array}{c} g_1 \\ g_2 \end{array} & \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right) = M_G \end{array}$$

Recall that a matrix is in *row echelon form* if all non-zero rows are above any rows of all zeros, and the pivot of a non-zero row is always strictly to the right of the pivot of the row above it. A row echelon form can be achieved by Gaußian elimination.

Definition 5.4.3. Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements, and let M_G be a matrix form of G with respect to τ. Moreover, let $\widetilde{M_G}$ be a row echelon form of M_G. Then a polynomial form of $\widetilde{M_G}$ is called a **row echelon form** of G with respect to τ and is denoted by $\widetilde{G}$.

Example 5.4.4. (continued) Consider Example 5.4.2 again. In this example we have $G = \{g_1, g_2\}$ where $g_1 = x_2x_1e_1x_2^2 + e_1x_2, g_2 = x_2x_1e_1x_2^2 + x_2x_1^2e_2$, $\tau = \texttt{PosLLex}$, and $\mathcal{T} = (x_2x_1e_1x_2^2, e_1x_2, x_2x_1^2e_2)$. The matrix form M_G of G with respect to τ and a row echelon form $\widetilde{M_G}$ of M_G are as follows.

$$M_G = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \Rightarrow \widetilde{M_G} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

Hence $\widetilde{G} = \{x_2x_1e_1x_2^2 + e_1x_2, e_1x_2 - x_2x_1^2e_2\}$ is a row echelon form of G with respect to τ.

The following proposition is a straightforward generalization of [26], Corollary 2.1, which describes elementary properties of row echelon forms.

Proposition 5.4.5. *Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements, let $\widetilde{G}$ be a row echelon form of G with respect to τ, and let $\widetilde{G}^+ = \{g \in \widetilde{G} \mid \mathrm{LT}_\tau(g) \notin \mathrm{LT}_\tau\{G\}\}$. Moreover, let $G_- \subseteq G$ be a subset such that $\mathrm{LT}_\tau\{G_-\} = \mathrm{LT}_\tau\{G\}$ and such that the leading terms of elements in G_- are pairwise distinct. Then $\widetilde{G}^+ \cup G_-$ is a K-basis of $\mathrm{Span}_K(G)$, i.e. for every element $m \in \mathrm{Span}_K(G) \setminus \{0\}$ there exist $c_1, \ldots, c_s \in K \setminus \{0\}, g_1, \ldots, g_s \in \widetilde{G}^+ \cup G_-$ such that $m = \sum_{i=1}^s c_ig_i$ and $\mathrm{LT}_\tau(m) = \mathrm{LT}(g_1) >_\tau \cdots >_\tau \mathrm{LT}_\tau(g_s)$.*

Proof. It is clear that the leading terms of elements in $\widetilde{G}^+ \cup G_-$ are pairwise distinct, thus the elements in $\widetilde{G}^+ \cup G_-$ are linearly independent. We prove that $\mathrm{Span}_K(\widetilde{G}^+ \cup G_-) = \mathrm{Span}_K(G)$. Obviously $\mathrm{Span}_K(\widetilde{G}^+ \cup G_-) \subseteq \mathrm{Span}_K(G)$. For a contradiction, suppose that $\mathrm{Span}_K(\widetilde{G}^+ \cup G_-) \subset \mathrm{Span}_K(G)$. Since τ is a well-ordering, there exists a non-zero element $m \in \mathrm{Span}_K(G) \setminus \mathrm{Span}_K(\widetilde{G}^+ \cup G_-)$ having a minimal leading term with respect to τ. If $\mathrm{LT}_\tau(m) \in \mathrm{LT}_\tau\{G\}$, then by the definition of G_- there is $m' \in G_- \subseteq \widetilde{G}^+ \cup G_-$ such that $\mathrm{LT}_\tau(m') = \mathrm{LT}_\tau(m)$ and we get an element $m - \frac{\mathrm{LT}_\tau(m)}{\mathrm{LT}_\tau(m')} m'$ which is still in $\mathrm{Span}_K(G) \setminus \mathrm{Span}_K(\widetilde{G}^+ \cup G_-)$ and has a smaller leading term: a contradiction. Thus we have to have $\mathrm{LT}_\tau(m) \notin \mathrm{LT}_\tau\{G\}$. Since $\widetilde{G}$ is a row echelon form of G, the leading terms of elements in $\widetilde{G}$ are pairwise distinct and $\mathrm{Span}_K(\widetilde{G}) = \mathrm{Span}_K(G)$. Thus there exist $c'_1, \ldots, c'_t \in K \setminus \{0\}, g'_1, \ldots, g'_t \in \widetilde{G}$ such that $m = \sum_{j=1}^t c'_j g'_j$ and $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(g'_1) >_\tau \cdots >_\tau \mathrm{LT}_\tau(g'_t)$. Therefore $\mathrm{LT}_\tau(g'_1) = \mathrm{LT}_\tau(m) \notin \mathrm{LT}_\tau\{G\}$. By the definition of $\widetilde{G}$ we have $g'_1 \in \widetilde{G}^+ \subseteq \widetilde{G}^+ \cup G_-$. Again we get an element $m - c'_1 g'_1$ which is still in $\mathrm{Span}_K(G) \setminus \mathrm{Span}_K(\widetilde{G}^+ \cup G_-)$ and has a smaller leading term: a contradiction again. □

Example 5.4.6. (continued) We consider again Example 5.4.4. In this example we have $G = \{g_1, g_2\}$ where $g_1 = x_2x_1e_1x_2^2 + e_1x_2, g_2 = x_2x_1e_1x_2^2 + x_2x_1^2e_2$, and $\widetilde{G} = \{\tilde{g}_1, \tilde{g}\}$ where $\tilde{g}_1 = g_1 = x_2x_1e_1x_2^2 + e_1x_2, \tilde{g}_2 = e_1x_2 - x_2x_1^2e_2$. Thus $\widetilde{G}^+ = \{g \in \widetilde{G} \mid \mathrm{LT}_\tau(g) \notin \mathrm{LT}_\tau\{G\}\} = \{\tilde{g}_2\}$. Let $G_- = \{g_2\}$. We show that $\widetilde{G}^+ \cup G_- = \{\tilde{g}_2, g_2\}$ is a K-basis of $\mathrm{Span}_K(G)$ and hence verify Proposition 5.4.5. Clearly $\{\tilde{g}_2, g_2\}$ is a linearly independent set. From $g_1 = g_2 + \tilde{g}_2$ it follows that $g_1 \in \mathrm{Span}_K\{\tilde{g}_2, g_2\}$. Therefore $\{\tilde{g}_2, g_2\}$ is a K-basis of $\mathrm{Span}_K(G)$.

In the following we shall introduce the Reduction Algorithm, which is the main ingredient of the F4 Procedure and is comparable to the Division Algorithm in the Buchberger Procedure.

Theorem 5.4.7. (The Reduction Algorithm) *Let $L, G \subseteq F_r \setminus \{0\}$ be two finite subsets. Consider the following sequence of instructions.*

1) *Let $F = L$ and $T = \cup_{f \in F} \mathrm{Supp}(f)$.*

2) *If $T = \emptyset$, continue with step 4). Otherwise, select a term $t \in T$ and delete it from T.*

3) *If there exist $w, w' \in \langle X\rangle, g \in G$ such that $t = w\mathrm{LT}_\tau(g)w'$, then append wgw' to F and append* $\mathrm{Supp}(wgw') \setminus \{t\}$ *to T. Continue with step 2).*

4) *Compute a row echelon form $\widetilde{F}$ of F with respect to τ.*

5) Return the set $\widetilde{F}^{+} = \{f \in \widetilde{F} \setminus \{0\} \mid \mathrm{LT}_\tau(f) \notin \mathrm{LT}_\tau\{F\}\}$.

This is an algorithm. When it stops, we have $\mathrm{LT}_\tau(h) \notin \mathrm{LT}_\tau(G)$ *for all* $h \in \widetilde{F}^{+}$.

Proof. To prove termination, observe that each time step 2) executes one term t is deleted from T. The set T is enlarged only in step 3). From $t = w\mathrm{LT}_\tau(g)w'$ and Remark 5.1.7, we conclude that terms in $\mathrm{Supp}(wgw') \setminus \{t\}$ are strictly smaller than t with respect to τ. Thus in step 3) only those terms which are strictly smaller than t are appended to T. Since τ is a well-ordering, this can happen only finitely many times. Therefore the procedure terminates after finitely many steps.

We show that $\mathrm{LT}_\tau(h) \notin \mathrm{LT}_\tau(G)$ for all $h \in \widetilde{F}^{+}$. For the sake of contradiction, suppose that there exists an element $h \in \widetilde{F}^{+}$ such that $\mathrm{LT}_\tau(h) \in \mathrm{LT}_\tau(G)$. Then there exist $w, w' \in \langle X \rangle, g \in G$ satisfying $\mathrm{LT}_\tau(h) = w\mathrm{LT}_\tau(g)w'$. On the other hand, we have $\mathrm{LT}_\tau(h) \in \mathrm{Supp}(h) \subseteq \mathrm{Supp}(\widetilde{F}^{+}) \subseteq \mathrm{Supp}(\widetilde{F}) \subseteq \mathrm{Supp}(F)$. Thus wgw' is appended to F in step 2). By Remark 5.1.7 we have $\mathrm{LT}_\tau(h) = \mathrm{LT}_\tau(wgw') \in \mathrm{LT}_\tau\{F\}$ which contradicts the definition of $\widetilde{F}^{+}$. □

A set $\widetilde{F}^{+}$ obtained in Theorem 5.4.7 is called a **reduction remainder** of L with respect to G and is denoted by $\mathrm{RR}_{\tau,G}(L)$. In the literature, steps 1), 2), and 3) form the so-called *symbolic preprocessing* (see [26]). Observe that if the set L consists of only one element, the Reduction Algorithm is compared to the Division Algorithm as in Theorem 5.1.12. Otherwise, it can be considered as a division algorithm which simultaneously computes normal remainders of a set of elements and is followed by some interreduction steps on the normal remainders.

Example 5.4.8. Consider the free $\mathbb{Q}\langle x_1, x_2\rangle$-module F_2 of rank 2 equipped with the module term ordering $\tau = \texttt{PosLLex}$. Let $G = \{g_1, g_2, g_3\} \subseteq F_2$ where $g_1 = x_2x_1e_1x_2 + e_1$, $g_2 = e_1x_2^2 + x_1e_2$, $g_3 = e_1x_2 - x_2x_1^2e_2$, and $L = \{g_1x_2, x_2x_1g_2, g_1, x_2x_1g_3, g_2, g_3x_2\}$. We compute a reduction remainder of L with respect to G using the Reduction Algorithm given in Theorem 5.4.7.

1) $F = L$ and $T = \{x_2x_1e_1x_2^2, x_2x_1e_1x_2, e_1x_2^2, e_1x_2, e_1, x_2x_1x_2x_1^2e_2,\ x_2x_1^2e_2x_2, x_2x_1^2e_2, x_1e_2\}$.

2) Select $x_2x_1e_1x_2^2$ and let $T = \{x_2x_1e_1x_2, e_1x_2^2, e_1x_2, e_1, x_2x_1x_2x_1^2e_2, x_2x_1^2e_2x_2, x_2x_1^2e_2, x_1e_2\}$.

3) Since $x_2x_1\mathrm{LT}_\tau(g_3)x_2$, let $F = F \cup \{x_2x_1g_3x_2\} = \{g_1x_2, x_2x_1g_2, g_1, x_2x_1g_3, g_2,\ g_3x_2, x_2x_1g_3x_2\}$ and $T = T \cup \{x_2x_1x_2x_1^2e_2x_2\} = \{x_2x_1e_1x_2, e_1x_2^2, e_1x_2, e_1, x_2x_1x_2x_1^2e_2x_2,$

$x_2x_1x_2x_1^2e_2,\ x_2x_1^2e_2x_2,\ x_2x_1^2e_2,\ x_1e_2\}$.

2) Select $x_2x_1e_1x_2$ and let $T = \{e_1x_2^2, e_1x_2, e_1, x_2x_1x_2x_1^2e_2x_2,\ x_2x_1x_2x_1^2e_2,\ x_2x_1^2e_2x_2,$ $x_2x_1^2e_2, x_1e_2\}$.

3) Since $x_2x_1\mathrm{LT}_\tau(g_3)$, let $F = F \cup \{x_2x_1g_3\} = \{g_1x_2, x_2x_1g_2, g_1, x_2x_1g_3, g_2, g_3x_2,$ $x_2x_1g_3x_2\}$ and $T = T \cup \{x_2x_1x_2x_1^2e_2\} = \{e_1x_2^2, e_1x_2, e_1, x_2x_1x_2x_1^2e_2x_2,\ x_2x_1x_2x_1^2e_2,$ $x_2x_1^2e_2x_2,\ x_2x_1^2e_2, x_1e_2\}$.

2) Select $e_1x_2^2$ and let $T = \{e_1x_2, e_1, x_2x_1x_2x_1^2e_2x_2, x_2x_1x_2x_1^2e_2, x_2x_1^2e_2x_2, x_2x_1^2e_2,\ x_1e_2\}$.

3) Since $\mathrm{LT}_\tau(g_3)x_2$, let $F = F \cup \{g_3x_2\} = \{g_1x_2, x_2x_1g_2, g_1, x_2x_1g_3, g_2, g_3x_2,\ x_2x_1g_3x_2\}$ and $T = T \cup \{x_2x_1^2e_2x_2\} = \{e_1x_2, e_1, x_2x_1x_2x_1^2e_2x_2,\ x_2x_1x_2x_1^2e_2,\ x_2x_1^2e_2x_2,\ x_2x_1^2e_2,$ $x_1e_2\}$.

2) Select e_1x_2 and let $T = \{e_1, x_2x_1x_2x_1^2e_2x_2, x_2x_1x_2x_1^2e_2, x_2x_1^2e_2x_2, x_2x_1^2e_2, x_1e_2\}$.

3) Since $\mathrm{LT}_\tau(g_3)$, let $F = F \cup \{g_3\} = \{g_1x_2, x_2x_1g_2, g_1, x_2x_1g_3, g_2, g_3x_2,\ x_2x_1g_3x_2,\ g_3\}$ and $T = T \cup \{x_2x_1^2e_2\} = \{e_1,\ x_2x_1x_2x_1^2e_2x_2, x_2x_1x_2x_1^2e_2, x_2x_1^2e_2x_2,\ x_2x_1^2e_2,\ x_1e_2\}$.

2) Note that no element in T is a multiple of the leading term of element in G. Let $T = \emptyset$.

4) We have $F = \{g_1x_2, x_2x_1g_2, g_1, x_2x_1g_3, g_2, g_3x_2, x_2x_1g_3x_2, g_3\}$. Let $\mathcal{T} = (x_2x_1e_1x_2^2,$ $x_2x_1e_1x_2, e_1x_2^2, e_1x_2, e_1, x_2x_1x_2x_1^2e_2x_2,\ x_2x_1x_2x_1^2e_2,\ x_2x_1^2e_2x_2, x_2x_1^2e_2,\ x_1e_2)$. Then the matrix form M_F of F and a row echelon form $\widetilde{M_F}$ of M_F are as follows.

$$\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0
\end{pmatrix}
\Rightarrow
\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Thus F has a row echelon form $\widetilde{F} = \{x_2x_1e_1x_2^2 + e_1x_2, x_2x_1e_1x_2 + e_1, e_1x_2^2 + x_1e_2, e_1x_2 - x_2x_1^2e_2, e_1 + x_2x_1x_2x_1^2e_2, x_2x_1x_2x_1^2e_2x_2 + x_2x_1^2e_2, x_2x_1^2e_2x_2 + x_1e_2, 0\}$.

5) $\widetilde{F}^+ = \{e_1 + x_2x_1x_2x_1^2e_2, x_2x_1x_2x_1^2e_2x_2 + x_2x_1^2e_2, x_2x_1^2e_2x_2 + x_1e_2\}$.

Proposition 5.4.9. *In the situation of Theorem 5.4.7, we let $L \subseteq \{wgw' \mid g \in G, w, w' \in \langle X \rangle\}$ be a subset. Then for every element $m \in \mathrm{Span}_K(L) \setminus \{0\}$ there exists a Gröbner representation in terms of $G \cup \widetilde{F}^+$.*

Proof. In step 4) of Theorem 5.4.7, we let $F_- \subseteq F$ be a subset such that $\mathrm{LT}_\tau\{F_-\} = \mathrm{LT}_\tau\{F\}$ and the leading terms of elements in F_- are pairwise distinct. Then by Proposition 5.4.5 the set $\widetilde{F}^+ \cup F_-$ is a K-basis of $\mathrm{Span}_K(F)$ and the leading terms of elements in $\widetilde{F}^+ \cup F_-$ are pairwise distinct. It is clear that $\mathrm{Span}_K(L) \subseteq \mathrm{Span}_K(F)$. Hence by Proposition 5.4.5 for every element $m \in \mathrm{Span}_K(L) \setminus \{0\}$ there exist $c_1, \ldots, c_s \in K \setminus \{0\}, f_1, \ldots, f_s \in \widetilde{F}^+ \cup F_-$ such that $m = \sum_{i=1}^s c_i f_i$ and $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(f_1) >_\tau \cdots >_\tau \mathrm{LT}_\tau(f_s)$. By the assumption $L \subseteq \{wgw' \mid w, w' \in \langle X \rangle, g \in G\}$ and the construction of F as in Theorem 5.4.7, for every element $f \in F_- \subseteq F$ there exist $w, w' \in \langle X \rangle, g \in G$ such that $f = wgw'$. Hence $m = \sum_{i=1}^s c_i f_i$ is a Gröbner representation of m in terms of $G \cup \widetilde{F}^+$. □

Theorem 5.4.7 together with Proposition 5.4.9 enables us to formulate the following F4 Procedure for enumerating Gröbner bases in F_r.

Theorem 5.4.10. (F4 Procedure) *Let $G \subseteq F_r \setminus \{0\}$ be a finite set of elements which generates a $K\langle X \rangle$-submodule $M = \langle G \rangle$, let $\mathcal{G}$ be an associated tuple of G, and let $s = |\mathcal{G}|$. Consider the following sequence of instructions.*

1) *Let $s' = s$ and let B be the set of all critical pairs.*

2) *If $B = \emptyset$, return the tuple $\mathcal{G}$. Otherwise, select a subset $B' \subseteq B$ using a fair strategy and delete the corresponding entries from B.*

3) *Let $L = \cup_{(i,j) \in B'} \{\frac{1}{\mathrm{LC}_\tau(g_i)} w_i g_i w_i', \frac{1}{\mathrm{LC}_\tau(g_j)} w_j g_j w_j'\}$. Compute $\widetilde{F}^+ = \mathrm{RR}_{\tau,\mathcal{G}}(L)$.*

4) *If $\widetilde{F}^+ = \emptyset$, continue with step 2). Otherwise, select an element $m \in \widetilde{F}^+$ and delete it from $\widetilde{F}^+$. Increase s' by one, append $g_{s'} = m$ to $\mathcal{G}$, and append the set $\{(i, s') \mid i \in \{1, \ldots, s'-1\}, (i, s')$ is a critical pair$\}$ to the set B. Continue with step 4).*

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

Proof. We prove the correctness. Observe that all critical pairs of $\mathcal{G}$ are constructed in steps 1) and 4). The fair selection strategy in Step 2) makes sure that all critical pairs are eventually selected. In step 3) we have $S_{ij} \in \mathrm{Span}_K(L)$. Then by appending $\widetilde{F}^+$ to $\mathcal{G}$ and by Proposition 5.4.9, S_{ij} has a Gröbner representation in terms of $\mathcal{G}$, i.e. there exist $c_1, \cdots, c_t \in K \setminus \{0\}, w_1, \ldots, w'_t \in \langle X\rangle, g_{i_1}, \ldots, g_{i_t} \in G$ such that $S_{ij} = \sum_{k=1}^t c_k w_k g_{i_k} w'_k$ and $\mathrm{LT}_\tau(S_{ij}) = \mathrm{LT}_\tau(w_1 g_{i_1} w'_1) >_\tau \mathrm{LT}_\tau(w_2 g_{i_2} w'_2) >_\tau \cdots >_\tau \mathrm{LT}_\tau(w_t g_{i_t} w'_t)$. We let $h = \sigma_{ij} - \sum_{k=1}^t c_k w_k \epsilon_{i_k} w'_k$, which is a lifting of σ_{ij} in $\mathrm{Syz}(\mathcal{G})$. Thus $\mathcal{G}$ is a τ-Gröbner basis of M by Lemma 5.2.8 and Proposition 5.2.10. The proof of the termination proceeds exactly as the proof of the termination of Theorem 5.2.12. □

Remark 5.4.11. Let us make some observations about this F4 Procedure.

a) Clearly the F4 Procedure turns into the classical Buchberger Procedure if we select exactly one critical pair in step 2). Note that different selection strategies can distinctly affect the performance of the F4 Procedure as in commutative settings (see [26], Section 2.5).

b) We prove the correctness of the F4 Procedure by showing that every critical syzygy has a lifting in $\mathrm{Syz}(\mathcal{G})$. As a result, we can apply our methods for improving the Buchberger Procedure in the last section to improve the F4 Procedure. In [26], J.-C. Faugère proposed a *Simplify function* to improve the F4 Algorithm in the commutative case. Our experiments show that, after deleting redundant generators and applying Proposition 5.3.3, the Simplify function is unlikely to be executed.

c) The last observation should influence the Reduction Algorithm in step 3). Let $B' = \{(i_1, j_1), \ldots, (i_\mu, j_\mu)\} \subseteq B$ be the selected subset. Without loss of generality, we may assume that elements in $\mathcal{G}$ are monic. We arrange L as the tuple

$$(w_{i_1} g_{i_1} w'_{i_1}, \ldots, w_{i_\mu} g_{i_\mu} w'_{i_\mu}, w_{j_1} g_{j_1} w'_{j_1}, \ldots, w_{j_\mu} g_{j_\mu} w'_{j_\mu}).$$

Moreover, we assume that the leading terms $\mathrm{LT}_\tau(w_{i_1} g_{i_1} w'_{i_1}), \ldots, \mathrm{LT}_\tau(w_{i_\mu} g_{i_\mu} w'_{i_\mu})$ are pairwise distinct by a proper selection strategy. Without loss of generality, we may assume that $\mathrm{LT}_\tau(w_{i_1} g_{i_1} w'_{i_1}) >_\tau \cdots >_\tau \mathrm{LT}_\tau(w_{i_\mu} g_{i_\mu} w'_{i_\mu})$. We arrange F in step 4) of Theorem 5.4.7 as the tuple

$$(w_{i_1} g_{i_1} w'_{i_1}, \ldots, w_{i_\mu} g_{i_\mu} w'_{i_\mu}, w_{j_1} g_{j_1} w'_{j_1}, \ldots, w_{j_\mu} g_{j_\mu} w'_{j_\mu}, w_{k_1} g_{k_1} w'_{k_1}, \ldots, w_{k_\nu} g_{k_\nu} w'_{k_\nu})$$

where $w_{k_1} g_{k_1} w'_{k_1}, \ldots, w_{k_\nu} g_{k_\nu} w'_{k_\nu}$ are elements appended to F during the symbolic preprocessing. We divide the matrix form M_F of F into 3 blocks as follows.

$$M_F = \left(\begin{array}{cccccc}
* & \cdots & \cdots & * & & \\
 & \ddots & \ddots & \ddots & \ddots & \\
 & & * & \cdots & \cdots & * \\
\hline
* & \cdots & \cdots & * & & \\
 & \ddots & \ddots & \ddots & \ddots & \\
 & & * & \cdots & \cdots & * \\
\hline
* & & \cdots & \cdots & & * \\
\vdots & & \ddots & \ddots & & \vdots \\
* & & \cdots & \cdots & & *
\end{array}\right)$$

The first block is the matrix form of $(w_{i_1}g_{i_1}w'_{i_1}, \ldots, w_{i_\mu}g_{i_\mu}w'_{i_\mu})$, the second block is the matrix form of $(w_{j_1}g_{j_1}w'_{j_1}, \ldots, w_{j_\mu}g_{j_\mu}w'_{j_\mu})$, and the third block is the matrix form of $(w_{k_1}g_{k_1}w'_{k_1}, \ldots, w_{k_\nu}g_{k_\nu}w'_{k_\nu})$. Observe that the first and third blocks are already in row echelon form. To compute the reduction remainder of L it is sufficient to only eliminate rows in the second and third blocks. In [30], J.-C. Faugère et al. remarked:

> *The matrices occurring in the Gröbner basis computation have the following common properties: sparse, several rows are monomial multiples of the same polynomial, not necessary full rank, and almost block triangular.*

In practice, the matrices can be very large during intermediate computations. Instead of using naïve Gaußian elimination, row echelon forms should be computed ingeniously. Direct methods for sparse matrices are intensively studied in [25] by I. S. Duff et al. We refer to [49], Section 5 and [62] for details about Gaußian elimination of huge and sparse matrices over finite fields. Parallel Gaußian elimination for Gröbner basis computations in finite fields is studied in [30].

To end this section, we apply the F4 Procedure to Example 5.4.8.

Example 5.4.12. (continued) Consider Example 5.4.8 again. In this example we have $G = \{g_1, g_2, g_3\}$ where $g_1 = x_2x_1e_1x_2 + e_1, g_2 = e_1x_2^2 + x_1e_2, g_3 = e_1x_2 - x_2x_1^2e_2$ and the module term ordering $\tau = \texttt{PosLLex}$. Let $M \subseteq F_2$ be $\mathbb{Q}\langle x_1, x_2\rangle$-submodule generated by G. We enumerate a τ-Gröbner basis of M using the F4 Procedure given in Theorem 5.4.10.

1) Let $\mathcal{G} = (g_1, g_2, g_3), s' = 3$, and $B = \{(1,2),(1,3),(2,3)\}$.

2) Select $B' = \{(1,2),(1,3),(2,3)\}$ and let $B = \emptyset$.

3) Let $L = \{g_1x_2, x_2x_1g_2, g_1, x_2x_1g_3, g_2, g_3x_2\}$. Observe that L and G are identical to the corresponding sets in Example 5.4.8. Thus we have $\widetilde{F}^+ = \mathrm{RR}_{\tau,\mathcal{G}}(L) = \{e_1 + x_2x_1x_2x_1^2e_2, x_2x_1x_2x_1^2e_2x_2 + x_2x_1^2e_2, x_2x_1^2e_2x_2 + x_1e_2\}$.

4) Let $s' = 4, \mathcal{G} = (g_1, g_2, g_3, g_4)$ with $g_4 = e_1 + x_2x_1x_2x_1^2e_2$, and $B = \{(1,4),(2,4),(3,4)\}$. Let $s' = 5, \mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ with $g_5 = x_2x_1x_2x_1^2e_2x_2 + x_2x_1^2e_2$, and $B = \{(1,4),(2,4),(3,4)\}$. Let $s' = 6, \mathcal{G} = (g_1, g_2, g_3, g_4, g_5, g_6)$ with $g_6 = x_2x_1^2e_2x_2 + x_1e_2$, and $B = \{(1,4),(2,4),(3,4),(5,6)\}$. Since $\mathrm{LT}_{\widehat{\tau}}(\sigma_{14}) = x_2x_1\epsilon_4x_2, \mathrm{LT}_{\widehat{\tau}}(\sigma_{24}) = \epsilon_4x_2^2$ are multiples of $\mathrm{LT}_{\widehat{\tau}}(\sigma_{34}) = \epsilon_4x_2$, we can remove $(1,4),(2,4)$ from B. Thus $B = \{(3,4),(5,6)\}$.

2) Select $B' = \{(3,4),(5,6)\}$ and let $B = \emptyset$.

3) Let $L = \{g_3, g_4x_2, g_5, x_2x_1g_6\}$. We shall compute $\widetilde{F}^+ = \mathrm{RR}_{\tau,\mathcal{G}}(L)$. Now we let $L = (g_3, g_5, g_4x_2, x_2x_1g_6)$ be a tuple. Applying steps 1), 2) and 3), we obtain the tuple $F = (g_3, g_5, g_4x_2, x_2x_1g_6)$ and $\mathcal{T} = (e_1x_2, x_2x_1x_2x_1^2e_2x_2, x_2x_1^2e_2)$. Then the matrix form M_F of F and a row echelon form of $\widetilde{M_F}$ of M_F are as follows.

$$\begin{array}{cccc} & e_1x_2 & x_2x_1x_2x_1^2e_2x_2 & x_2x_1^2e_2 \\ g_3 & 1 & 0 & -1 \\ g_5 & 0 & 1 & 1 \\ g_4x_2 & 1 & 1 & 0 \\ x_2x_1g_6 & 0 & 1 & 1 \end{array} \Rightarrow \begin{array}{cccc} & e_1x_2 & x_2x_1x_2x_1^2e_2x_2 & x_2x_1^2e_2 \\ g_3 & 1 & 0 & -1 \\ g_5 & 0 & 1 & 1 \\ g_4x_2 - g_3 - g_5 & 0 & 0 & 0 \\ x_2x_1g_6 - g_5 & 0 & 0 & 0 \end{array}$$

Thus $\widetilde{F}^+ = \mathrm{RR}_{\tau,\mathcal{G}}(L) = \emptyset$.

2) Since $B = \emptyset$, return the tuple $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5, g_6)$.

Hence the set $\{g_1, g_2, g_3, g_4, g_5, g_6\}$ is a τ-Gröbner basis of M.

Chapter 6

Applications

In the previous chapters we have studied Gröbner basis theories in free monoid rings (see Chapters 3 and 4) and in free bimodules over free monoid rings (see Chapter 5). In this chapter we explore the applications of Gröbner bases in both settings.

Let $I \subseteq K\langle X\rangle$ be a two-sided ideal. We assume that the ideal I has a finite Gröbner basis. Under this assumption, in Section 6.1 we shall exploit Gröbner bases in the residue class rings $K\langle X\rangle/I$ (see Subsections 6.1.1 and 6.1.2) and in the free $K\langle X\rangle/I$-bimodule $\bar{F}_r = (K\langle X\rangle/I \otimes K\langle X\rangle/I)^r$ with $r \geq 1$ (see Subsection 6.1.3). Due to Theorem 6.1.3, we define Gröbner bases of two-sided and one-sided ideals in $K\langle X\rangle/I$ (see Definitions 6.1.4 and 6.1.8) in the spirit of the corresponding definitions in $K\langle X\rangle$. In Subsection 6.1.1 we present the properties and the computation of Gröbner bases of two-sided ideals in $K\langle X\rangle/I$ (see Proposition 6.1.5 and Remark 6.1.6). In Subsection 6.1.2 we give the Right Division Algorithm in $K\langle X\rangle/I$ (see Theorem 6.1.9) and present the properties of Gröbner bases of right ideals in $K\langle X\rangle/I$ (see Proposition 6.1.10). Through investigating the representation of elements of right ideals, we obtain a Buchberger Criterion (see Proposition 6.1.12) and a Buchberger Procedure (see Corollary 6.1.13) for the computation of Gröbner bases of right ideals in $K\langle X\rangle/I$. We use a variant of the Buchberger Procedure to check whether an element of $K\langle X\rangle/I$ is invertible, and to compute its inverse if it is invertible (see Corollary 6.1.16). In Subsection 6.1.3 we review Gröbner basis theory in free $K\langle X\rangle/I$-bimodule $\bar{F}_r$ introduced by H. Bluhm and M. Kreuzer [8], and give the Division Algorithm in $\bar{F}_r$ (see Theorem 6.1.23).

In Section 6.2 we shall study elimination of variables in the free monoid ring $K\langle X\rangle$ (see Subsection 6.2.1) and component elimination in the free $K\langle X\rangle$-bimodule $F_r =$

$(K\langle X\rangle \otimes K\langle X\rangle)^r$ with $r \geq 1$ (see Subsection 6.2.2). In Subsection 6.2.1 we define the elimination ordering and the elimination ideal in $K\langle X\rangle$ (see Definition 6.2.1). Based on the computation of elimination ideals (see Theorem 6.2.3), we compute the intersection of ideals in $K\langle X\rangle$ (see Proposition 6.2.4), and investigate the kernels and images of K-algebra homomorphisms (see Propositions 6.2.7 and 6.2.13). Furthermore, we give a condition for an element of $K\langle X\rangle/I$ to be algebraic over K and compute its minimal polynomial (see Corollary 6.2.9). In particular, we propose a procedure to check if a monoid element has finite order (see Remark 6.2.11). We also propose procedures to possibly solve the subalgebra membership problem and the generalized word problem in Remarks 6.2.14 and 6.2.15, respectively. In Subsection 6.2.2 we define the component elimination ordering and the component elimination module in F_r (see Definition 6.2.17). Based on the computation of component elimination modules (see Theorem 6.2.19), we present the computation of the intersection of modules (see Proposition 6.2.20) and the computation of syzygy modules (see Proposition 6.2.24, Corollaries 6.2.27 and 6.2.28). The latter evokes further applications, such as solving the decomposition search problem and the factorization problem (see Remark 6.2.30), Bluhm-Kreuzer's Conjugator Search Algorithm (see Remarks 6.2.32 and 6.2.33), and the computation of colon modules (see Definition 6.2.34, Corollaries 6.2.35 and 6.2.37).

In Section 6.3 we shall study the K-dimension of K-algebra $K\langle X\rangle/I$ with the help of Gröbner bases and the Ufnarovski graph. After introducing $\mathbb{N}$-grading filtration to $K\langle X\rangle/I$, we define affine Hilbert function, Hilbert function and Hilbert series (see Definition 6.3.2) that represent the information about the K-dimension of $K\langle X\rangle/I$. Given a Gröbner basis, we restate Macaulay's Basis Theorem in Lemma 6.3.7. Further, given a (finite) Gröbner basis of the ideal I with respect to a length compatible admissible ordering, we compute the values of the affine Hilbert function as well as Hilbert function of $K\langle X\rangle/I$ sequentially (see Proposition 6.3.10 and Corollary 6.3.11). We introduce the Ufnarovski graph in Definition 6.3.21 which was initially used to check the finiteness and to compute the growth of the K-dimension of a K-algebra (see Theorem 6.3.25). Through representing the Ufnarovski graph as an adjacency matrix, we give a superior algorithm to compute the values of affine Hilbert function of $K\langle X\rangle/I$ (see Theorem 6.3.27), which allows to compute the values of Hilbert function independently. Finally, we formulate the Hilbert series of $K\langle X\rangle/I$ in Theorem 6.3.29.

Throughout this chapter, we let K be a field, $X = \{x_1, \ldots, x_n\}$ a finite alphabet (or set of indeterminates), $K\langle X\rangle$ the free monoid ring generated by X over K, $\langle X\rangle$ the free monoid generated by X, and σ an admissible ordering on $\langle X\rangle$. Moreover, for $r \geq 1$, we let $F_r = (K\langle X\rangle \otimes K\langle X\rangle)^r$ be the free $K\langle X\rangle$-bimodule of rank r with canonical basis $\{e_1, \ldots, e_r\}$, where $e_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$ with $1 \otimes 1$ occurring in the i^{th} position for $i = 1, \ldots, r$, and we let $\mathbb{T}(F_r)$ be the set of terms in F_r, i.e. $\mathbb{T}(F_r) = \{we_iw' \mid i \in \{1, \ldots, r\}, w, w' \in \langle X\rangle\}$. Unless otherwise specified, by an ideal $I \subseteq K\langle X\rangle$ we mean a finitely generated two-sided ideal, and by a $K\langle X\rangle$-submodule $M \subseteq F_r$ we mean a finitely generated two-sided $K\langle X\rangle$-submodule.

6.1 Gröbner Bases in $K\langle X\rangle/I$ and $(K\langle X\rangle/I \otimes K\langle X\rangle/I)^r$

Let $I \subseteq K\langle X\rangle$ be an ideal, and let $r \geq 1$. In this section we shall generalize Gröbner basis theory to the residue class ring $K\langle X\rangle/I$ and to the free $K\langle X\rangle/I$-bimodule $\bar{F}_r = (K\langle X\rangle/I \otimes K\langle X\rangle/I)^r$ under the assumption that the ideal I has a finite σ-Gröbner basis. This section is motivated by the following. Let $\mathcal{M} = \langle X \mid R\rangle$ be a finitely presented monoid. K. Madlener and B. Reinert [57] exploited Gröbner basis theory in monoid rings. They established the theory of prefix Gröbner bases in monoid and group rings (see [52, 57, 58, 63]). With the intention of computing two-sided syzygies over residue class rings, H. Bluhm and M. Kreuzer [8] generalized the prefix Gröbner basis theory to free bimodules over the residue class rings. Recall that the monoid ring $K\langle \mathcal{M}\rangle$ is isomorphic to the residue class ring $K\langle X\rangle/I$ where $I \subseteq K\langle X\rangle$ is the two-sided ideal generated from the set R of relations (see Corollary 2.2.11). Thus we can consider monoid rings as a specific case of residue class rings.

Assumption 6.1.1. *Throughout this section, we shall assume that the ideal I has a finite σ-Gröbner basis $G_I \subseteq K\langle X\rangle$.*

Remark 6.1.2. Recall that the elements in the residue class ring $K\langle X\rangle/I$ are equivalence classes. For a polynomial $f \in K\langle X\rangle$, the residue class of f, denoted by $\bar{f}$, is the class of all those polynomials of $K\langle X\rangle$ that are equivalent to f modulo I. By Proposition 3.3.10 we have $\mathrm{NF}_{\sigma,I}(f) = \mathrm{NR}_{\sigma,G_I}(f)$ which can be computed using the Division Algorithm given in Theorem 3.2.1. Thus we let the normal form $\mathrm{NF}_{\sigma,I}(f)$ be the representative of the equivalence class of f, i.e. $\bar{f} = \mathrm{NF}_{\sigma,I}(f)$. By Macaulay's Basis Theorem (see Theorem 3.1.15) the residue classes of the elements of the order ideal $\mathcal{O}_\sigma(I)$, which consists of all normal words modulo I with respect to σ, form a K-basis of $K\langle X\rangle/I$. We consider the set $\mathcal{O}_\sigma(I)$ as the set of all words in $K\langle X\rangle/I$. Thus we can represent elements in $\bar{F}_r$ in the form of $\sum_{i=1}^r \sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_iw'_{ij}$ with $c_{ij} \in K, w_{ij}, w'_{ij} \in \mathcal{O}_\sigma(I)$ for all $i \in \{1, \ldots, r\}, j \in \mathbb{N}$.

Due to Remark 6.1.2, in the following subsections we shall define Gröbner bases in the residue class ring $K\langle X\rangle/I$ and in the free $K\langle X\rangle/I$-bimodule $\bar{F}_r$ with the same style as Gröbner bases in free monoid rings. For our needs we distinguish two multiplications as follows. Given two polynomials $\bar{f}, \bar{g} \in K\langle X\rangle/I$, we let $\bar{f} \cdot \bar{g}$ denote the product of $\bar{f}$ and $\bar{g}$ in $K\langle X\rangle$, and $\bar{f}\bar{g} = \mathrm{NF}_{\sigma,I}(\bar{f} \cdot \bar{g})$ the product of $\bar{f}$ and $\bar{g}$ in $K\langle X\rangle/I$. In particular, for two words $w_1, w_2 \in \mathcal{O}_\sigma(I)$, the word $w_1 \cdot w_2$ is the concatenation of w_1 and w_2 in $\langle X\rangle$, while $w_1w_2 = \mathrm{NF}_{\sigma,I}(w_1 \cdot w_2)$ could be a polynomial in $K\langle X\rangle/I$. Moreover, we will denote the identity in $\langle X\rangle$ by $\equiv$. Note that the ordering σ is not compatible with multiplication in $K\langle X\rangle/I$, since for $w_1, w_2, w_3, w_4 \in \mathcal{O}_\sigma(I)$ such that $w_1 >_\sigma w_2$ we might have $\mathrm{LT}_\sigma(w_3w_1w_2) \leq_\sigma \mathrm{LT}_\sigma(w_3w_2w_4)$.

6.1.1 Gröbner Bases of Two-Sided Ideals in $K\langle X\rangle/I$

The following theorem describes the relation between ideals in the free monoid ring $K\langle X\rangle$ and ideals in the residue class ring $K\langle X\rangle/I$.

Theorem 6.1.3. *Let $I \subseteq K\langle X\rangle$ be a two-sided ideal. Then there is a one-to-one correspondence between the set of all two-sided (or one-sided) ideals in $K\langle X\rangle$ containing I and the set of all two-sided (or one-sided) ideals in $K\langle X\rangle/I$, given by $J \mapsto J/I$.*

Proof. See [40], Chapter III Theorem 2.13. □

Hence every two-sided (or one-sided) ideal in $K\langle X\rangle/I$ is of the form J/I where $J \subseteq K\langle X\rangle$ is a two-sided (or one-sided) ideal containing I. We shall investigate Gröbner bases of two-sided ideals in $K\langle X\rangle/I$ in this subsection and of right-sided ideals in next subsection.

In this subsection, we let $J \subseteq K\langle X\rangle$ be a two-sided ideal containing I. Then J/I becomes a two-sided ideal in $K\langle X\rangle/I$. Since for every polynomial $f \in I$ we have $\mathrm{NF}_{\sigma,I}(f) = 0$ (see Remark 3.1.18.c), to define Gröbner bases of the ideal J/I it suffices to consider the polynomials in $J \setminus I$.

Definition 6.1.4. Let $J \subseteq K\langle X\rangle$ be a two-sided ideal containing I, and let $G_J \subseteq J$ be a set of non-zero normal polynomials modulo I with respect to σ. The set G_J is called a **σ-Gröbner basis** of the two-sided ideal J/I if for every polynomial $f \in J \setminus I$ there exists a polynomial $g \in G_J$ such that $\mathrm{LT}_\sigma(g)$ is a subword of $\mathrm{LT}_\sigma(\bar{f})$ where $\bar{f} = \mathrm{NF}_{\sigma,I}(f)$.

Since G_I is a σ-Gröbner basis of the ideal I, for every polynomial $f \in I \setminus \{0\}$ there exists a polynomial $g \in G_I$ such that $\mathrm{LT}_\sigma(f)$ is a multiple of $\mathrm{LT}_\sigma(g)$. Then we use Gröbner bases to connect the ideal $J/I \subseteq K\langle X\rangle/I$ with the ideal $J \subseteq K\langle X\rangle$ as follows.

Proposition 6.1.5. *Let $J \subseteq K\langle X\rangle$ be a two-sided ideal containing I, and let $G_J \subseteq K\langle X\rangle$ be a set of non-zero normal polynomials modulo I with respect to σ. Then the following conditions are equivalent.*

a) The set G_J is a σ-Gröbner basis of the ideal $J/I \subseteq K\langle X\rangle/I$.

b) The set $G_J \cup G_I$ is σ-Gröbner basis of the ideal J.

c) Every normal polynomial $f \in J\backslash I$ modulo I with respect to σ has a representation

$$f = \sum_{j=1}^{s} c_j w_j g_j w_j' + h$$

with $c_1, \ldots, c_s \in K \setminus \{0\}, w_1, \ldots, w_s' \in \langle X\rangle, g_1, \ldots, g_s \in G_J, h \in I$ such that $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_j g_j w_j') \equiv w_j \cdot \mathrm{LT}_\sigma(g_j) \cdot w_j'$ for all $j \in \{1, \ldots, s\}$ and such that $\mathrm{LT}_\sigma(f) >_\sigma \mathrm{LT}_\sigma(h)$ if $h \neq 0$.

Proof. We prove condition a) implies condition b). Let $f \in J \setminus \{0\}$. We have $\bar{f} = \mathrm{NF}_{\sigma,I}(f) = \mathrm{NR}_{\sigma,G_I}(f)$ where the second equality follows from Assumption 6.1.1 and Proposition 3.3.10. If $\bar{f} = 0$ or $\bar{f} \neq 0$ and $\mathrm{LT}_\sigma(\bar{f}) \not\equiv \mathrm{LT}_\sigma(f)$, then, by Theorem 3.2.1 and Remark 3.1.13, there exists a polynomial $g \in G_I$ such that $\mathrm{LT}_\sigma(f)$ is a multiple of $\mathrm{LT}_\sigma(g)$. If $\bar{f} \neq 0$ and $\mathrm{LT}_\sigma(\bar{f}) \equiv \mathrm{LT}_\sigma(f)$, then by Definition 6.1.4 there exists a polynomial $g \in G_J$ such that $\mathrm{LT}_\sigma(f)$ is a multiple of $\mathrm{LT}_\sigma(g)$. Therefore the set $G_J \cup G_I$ is a σ-Gröbner basis of the ideal J.

We prove condtion b) implies condition a). Let $f \in J\backslash I$. Clearly $\bar{f} = \mathrm{NF}_{\sigma,I}(f) \in J$. There exists a polynomial $g \in G_J \cup G_I$ such that $\mathrm{LT}_\sigma(\bar{f})$ is a multiple of $\mathrm{LT}_\sigma(g)$. Since G_I is a σ-Gröbner basis of I and $\bar{f}$ is a normal polynomial, we must have $g \notin G_I$. Thus $g \in G_J$, and hence the set G_J is a σ-Gröbner basis of the ideal J/I. The equivalence between conditions b) and c) follows from Proposition 3.3.6 and Remark 3.1.13. □

Proposition 6.1.5 shows that Gröbner bases of two-sided ideals in $K\langle X\rangle/I$ share many of nice properties of Gröbner bases of two-sided ideals in $K\langle X\rangle$ (see Section 3.3). Using Proposition 6.1.5, we compute Gröbner bases in $K\langle X\rangle/I$ as follows.

Remark 6.1.6. Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of polynomials which generates an ideal $J/I \subseteq K\langle X\rangle/I$. We compute a σ-Gröbner basis of J/I via the following procedure.

1) Enumerate a σ-Gröbner basis G_J of the ideal $\langle G \cup G_I \rangle \subseteq K\langle X \rangle$.

2) Let $G_J = G_J \setminus G_I$. For each polynomial $g \in G_J$, compute $\bar{g} = \mathrm{HF}_{\sigma,I}(g)$ using the Division Algorithm given in Theorem 3.2.1. If $\bar{g} \neq 0$, replace g by $\bar{g}$. Otherwise, delete g from G_J.

3) Return the set G_J which is a σ-Gröbner basis of the ideal J/I.

We shall remark that the procedure above might not terminate since the ideal $\langle G \cup G_I \rangle$ in step 1) might not have a finite Gröbner basis. As a result the ideal J/I may not have a finite Gröbner basis. Recall that in commutative polynomial rings the existence of finite Gröbner bases is guaranteed by Dickson's lemma. P. Nordbeck [60] generalized Dickson's lemma to $K\langle X \rangle/I$, suggested so-called *D-property* and showed that every ideal in $K\langle X \rangle/I$ has a finite Gröbner basis if the residue class ring $K\langle X \rangle/I$ fulfils the D-property. We refer to [60] for details. Note that in general it is undecidable whether or not a given ideal $J/I \subseteq K\langle X \rangle/I$ has a finite Gröbner basis.

Example 6.1.7. Consider the *dihedral group* $D_6 = \langle a, b | a^3 = b^2 = (ab)^2 = 1 \rangle$ of order 6 and the group ring $\mathbb{F}_2\langle D_6 \rangle$. Note that $\mathbb{F}_2\langle D_6 \rangle \cong \mathbb{F}_2\langle a, b \rangle/I$ where $I \subseteq \mathbb{F}_2\langle a, b \rangle$ is the two-sided ideal generated by the set $\{a^3+1, b^2+1, (ab)^2+1\}$. Let $\bar{J} \subseteq \mathbb{F}_2\langle D_6 \rangle$ be the ideal generated by the set $\{g_1, g_2\}$ where $g_1 = aba+b+a+1$ and $g_2 = ab+ba+b+a$. Equivalently, $\bar{J} = J/I \subseteq \mathbb{F}_2\langle a, b \rangle/I$ where $J \subseteq \mathbb{F}_2\langle a, b \rangle$ is the ideal generated by the set $\{g_1, g_2, a^3+1, b^2+1, (ab)^2+1\}$. Let $\sigma = \texttt{LRLex}$ be the length-reverse-lexicographic ordering on $\langle a, b \rangle$ induced by $a >_{\texttt{Lex}} b$. We compute a σ-Gröbner basis of the ideal $\bar{J}$ as follows. Firstly we compute a σ-Gröbner basis G_I of the ideal I. We get $G_I = \{b^2+1, a^3+1, ba^2+ab, aba+b, a^2b+ba, bab+a^2, abab+1\}$. Then we compute a σ-Gröbner basis G_J of the ideal J. We get $G_J = \{a+1, a^2+a, ba+a^2+b+a, ab+b, b^2+1, a^3+1, aba+b+a+1, abab+1\}$. Let $G_J = G_J \setminus G_I = \{a+1, a^2+a, ba+a^2+b+a, ab+b, aba+b+a+1\}$. We compute the normal forms of elements of G_J modulo I with respect to σ and remove zero normal form. We obtain the set $G_J = \{a+1, a^2+a, ba+a^2+b+a, ab+b\}$ which is a σ-Gröbner basis of the ideal $\bar{J}$.

6.1.2 Gröbner Bases of Right Ideals in $K\langle X \rangle/I$

Now we shall investigate Gröbner bases of right ideals in $K\langle X \rangle/I$. It is understood that all theorems about right ideals also hold, *mutatis mutandis*, for left ideals. In this subsection, we let $J \subseteq K\langle X\rangle$ be a right ideal containing I. Then J/I is a right ideal in $K\langle X\rangle/I$. We define Gröbner bases of right ideals in $K\langle X\rangle/I$ as follows.

Definition 6.1.8. Let $J \subseteq K\langle X\rangle$ be a right ideal containing I, and let $G_J \subseteq J$ be a set of non-zero normal polynomials modulo I with respect to σ. We call the set G_J a **σ-Gröbner basis** of the right ideal $J/I \subseteq K\langle X\rangle/I$ if for every polynomial $f \in J \setminus I$ there exists a polynomial $g \in G_J$ such that $\mathrm{LT}_\sigma(g)$ is a prefix of $\mathrm{LT}_\sigma(\bar{f})$.

Gröbner bases of right ideals in $K\langle X\rangle/I$ possess similar properties as in Proposition 6.1.5. To describe these properties precisely, we first generalize the Right Division Algorithm (see Theorem 3.5.1) to the residue class ring $K\langle X\rangle/I$. Recall that we represent elements of $K\langle X\rangle/I$ by their normal forms. However, as we mentioned before, the product of two normal words need not be normal. For the sake of keeping operands in normal form during all computations we shall add an ingredient, which is the normal form computation in $K\langle X\rangle$, to the Right Division Algorithm in $K\langle X\rangle/I$.

Theorem 6.1.9. (The Right Division Algorithm) *Let $f \in K\langle X\rangle$, let $s \geq 1$, and let $g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$ be normal polynomials modulo I with respect to σ. Consider the following sequence of instructions.*

1) *Let $q_1 = \cdots = q_s = 0$ and $v = \mathrm{NF}_{\sigma,I}(f)$.*

2) *If there exists an index $j \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(v) \equiv \mathrm{LT}_\sigma(g_j) \cdot w$ for some word $w \in \langle X\rangle$, then replace q_j by $q_j + \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} w$ and v by $v - \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} g_j w$.*

3) *Repeat step 2) until there is no more $j \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(g_j)$ is a prefix of $\mathrm{LT}_\sigma(v)$. Return the tuple $(v, q_1, \ldots, q_s)$.*

This is an algorithm which returns a tuple $(v, q_1, \ldots, q_s)$ such that

$$f - (\sum_{j=1}^{s} g_j q_j + v) \in I$$

and such that the following conditions are satisfied.

a) *The polynomial v is a normal polynomial modulo I with respect to σ.*

b) *For all $j \in \{1, \ldots, s\}$, q_j is in normal form modulo I with respect to σ. If $q_j \neq 0$ for some $j \in \{1, \ldots, s\}$, then $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(g_j q_j) \equiv \mathrm{LT}_\sigma(g_j) \cdot \mathrm{LT}_\sigma(q_j)$.*

c) *If $v \neq 0$, then $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(v)$ and there is no $j \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(g_j)$ is a prefix of $\mathrm{LT}_\sigma(v)$.*

Proof. First we show that at each stage of the right division procedure we have

$$f - (\sum_{j=1}^{s} g_j q_j + v) \in I.$$

Obviously it is true in step 1). We have $g_j q_j + v = g_j(q_j + \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} w) + (v - \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} g_j w)$ in step 2). Therefore $f - (\sum_{j=1}^{s} g_j q_j + v) \in I$.

We prove the termination. In step 1) if $\mathrm{NF}_{\sigma,I}(v) \neq 0$, then by Theorem 3.2.1.b we have $\mathrm{LT}_\sigma(v) \geq_\sigma \mathrm{LT}_\sigma(\mathrm{NF}_{\sigma,I}(v))$. Clearly in step 2) we have $\mathrm{LM}_\sigma(v) = \mathrm{LM}_\sigma(\frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} g_j w)$. If $v - \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} g_j w \neq 0$, then by Remark 3.1.13.a we have $\mathrm{LT}_\sigma(v) >_\sigma \mathrm{LT}_\sigma(v - \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} g_j w)$. Thus $\mathrm{LT}_\sigma(v)$ strictly decreases. Since σ is a well-ordering, the right division procedure stops after finitely many steps.

Condition a) holds because v is set to the normal form of f in step 1) and is set to $v - \frac{\mathrm{LC}_\sigma(v)}{\mathrm{LC}_\sigma(g_j)} g_j w$ in step 2), which is again in normal form by Remark 3.1.18.b.

Since v as an input of step 2) is a normal polynomial, the leading term $\mathrm{LT}_\sigma(v)$ is a normal word. Since $\mathrm{LT}_\sigma(v) \equiv \mathrm{LT}_\sigma(g_j) \cdot w$, the word w is also a normal word. By Remark 3.1.18.b q_j is a normal polynomial for all $j \in \{1, \ldots, s\}$. The second part of condition b) follows from the fact that $\mathrm{LT}_\sigma(v)$ strictly decreases and from Remarks 3.1.13.a and 3.1.13.c.

The first part of condition c) follows from the fact that $\mathrm{LT}_\sigma(v)$ strictly decreases. The second part of condition c) holds because the right division procedure stops if and only if $v = 0$ or there is no $j \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(g_j)$ is a prefix of $\mathrm{LT}_\sigma(v)$. □

Let $f \in K\langle X \rangle$, let $s \geq 1$, let $g_1, \ldots, g_s \in K\langle X \rangle \setminus \{0\}$ be normal polynomials, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_s)$. We denote a polynomial $v \in K\langle X \rangle$ obtained in Theorem 6.1.9 by $\mathrm{RNR}_{\sigma,I,\mathcal{G}}(f)$. The following promising proposition follows directly from Definition 6.1.8 and Theorem 6.1.9.

Proposition 6.1.10. *Let $J \subseteq K\langle X \rangle$ be a right ideal containing I, let $G \subseteq K\langle X \rangle$ be a set of non-zero normal polynomials modulo I with respect to σ, and let $\mathcal{G}$ be an associated tuple of G. Then the following conditions are equivalent.*

a) The set G is a σ-Gröbner basis of the ideal $J/I \subseteq K\langle X \rangle/I$.

b) Every normal polynomial $f \in J \backslash I$ modulo I with respect to σ has a representation

$$f = \sum_{j=1}^{s} g_j q_j + h$$

with $q_1, \ldots, q_s \in K\langle X\rangle \setminus \{0\}, h \in I$ *such that* $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(g_j q_j) \equiv \mathrm{LT}_\sigma(g_j) \cdot \mathrm{LT}_\sigma(q_j)$ *for all* $j \in \{1, \ldots, s\}$ *and* $\mathrm{LT}_\sigma(f) >_\sigma \mathrm{LT}_\sigma(h)$ *if* $h \neq 0$*.*

c) A polynomial $f \in K\langle X\rangle$ *satisfies* $f \in J$ *if and only if* $\mathrm{RNR}_{\sigma,I,\mathcal{G}}(f) = 0$*.*

Let $G \subseteq K\langle X\rangle$ be a set of non-zero normal polynomials which generates a right ideal $J/I \subseteq K\langle X\rangle/I$. The set G is a σ-Gröbner basis of the ideal J/I if and only if every non-zero normal polynomial $f \in J\backslash I$ has a representation as given in Proposition 6.1.10.b, which can be obtained using the Right Division Algorithm given in Theorem 6.1.9. Obviously it is impossible for us to check the above condition for all normal polynomials. Luckily, just like in free monoid rings it is possible for us to only consider finitely many pairs of generators whose leading terms have overlaps. We are going to exploit a Buchberger Criterion for the computation of Gröbner bases of right ideals in $K\langle X\rangle/I$.

Remark 6.1.11. Since the set G generates the right ideal J/I and the set G_I is a σ-Gröbner basis of the ideal I, every normal polynomial $f \in J \setminus I$ has a representation

$$f = \sum_{j=1}^{s} g_j q_j + \sum_{i=1}^{t} c_i w_i g_i' w_i'$$

with $g_j \in G, q_j \in K\langle X\rangle \setminus \{0\}$ for all $j \in \{1, \ldots, s\}$, and with $c_i \in K \setminus \{0\}, g_i' \in G_I$, $w_i, w_i' \in \langle X\rangle$ for all $i \in \{1, \ldots, t\}$. Observe that the representation does not satisfy Proposition 6.1.10.b if there exists an index $j \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(g_j) \cdot \mathrm{LT}_\sigma(q_j) >_\sigma \mathrm{LT}_\sigma(f)$ or if there exists an index $i \in \{1, \ldots, t\}$ such that $w_i \cdot \mathrm{LT}_\sigma(g_i') \cdot w_i' >_\sigma \mathrm{LT}_\sigma(f)$. Clearly those terms which are larger than $\mathrm{LT}_\sigma(f)$ should be cancelled from the representation. There are three possibilities.

a) There exist $j, j' \in \{1, \ldots, s\}$ such that $j \neq j'$ and $\mathrm{LT}_\sigma(g_j) \cdot \mathrm{LT}_\sigma(q_j) \equiv \mathrm{LT}_\sigma(g_{j'}) \cdot \mathrm{LT}_\sigma(q_{j'}) >_\sigma \mathrm{LT}_\sigma(f)$. In this case g_j and $g_{j'}$ have a right obstruction (see Definition 3.5.5).

b) There exist $i, i' \in \{1, \ldots, t\}$ such that $i \neq i'$ and $w_i \cdot \mathrm{LT}_\sigma(g_i') \cdot w_i' \equiv w_{i'} \cdot \mathrm{LT}_\sigma(g_{i'}') \cdot w_{i'}' >_\sigma \mathrm{LT}_\sigma(f)$. In this case g_i' and $g_{i'}'$ have an obstruction (see Definition 3.4.7). Indeed it is not necessary to consider this case. Since G_I is a σ-Gröbner basis of I, we can avoid this case by simply replacing $\sum_{i=1}^{t} c_i w_i g_i' w_i'$ with its Gröbner representation in terms of G_I in the sense of T. Mora [55] (see also Remark 3.3.8).

c) There exist $j \in \{1, \ldots, s\}, i \in \{1, \ldots, t\}$ such that $\mathrm{LT}_\sigma(g_j) \cdot \mathrm{LT}_\sigma(q_j) \equiv w_i \cdot \mathrm{LT}_\sigma(g_i') \cdot w_i' >_\sigma \mathrm{LT}_\sigma(f)$. Since g_j is a normal polynomial modulo I with respect to σ and G_I is a σ-Gröbner basis of I, there exists some $w \in \langle X\rangle \setminus \{1\}$ such that $\mathrm{LT}_\sigma(g_j) \cdot w \equiv w_j \cdot \mathrm{LT}_\sigma(g'_i)$.

Thus to check if the set G is a σ-Gröbner basis of the ideal J/I, we only need to take care of situations a) and c). We let

$$\begin{aligned} SO_G &= \{\frac{1}{\mathrm{LC}_\sigma(g)}g - \frac{1}{\mathrm{LC}_\sigma(g')}g'w \mid g, g' \in G, g \neq g', w \in \langle X\rangle, \mathrm{LT}_\sigma(g) \equiv \mathrm{LT}_\sigma(g') \cdot w\}, \\ SO_{GG_I} &= \{\frac{1}{\mathrm{LC}_\sigma(g)}gw - \frac{1}{\mathrm{LC}_\sigma(g')}w'g' \mid g \in G, g' \in G_I, w, w' \in \langle X\rangle, \mathrm{LT}_\sigma(g) \cdot w \equiv w' \cdot \mathrm{LT}_\sigma(g')\}. \end{aligned}$$

From Remark 6.1.11 we have the following Buchberger Criterion for the computation of Gröbner bases of right ideals in $K\langle X\rangle/I$.

Proposition 6.1.12. (Buchberger Criterion) *Let $G \subseteq K\langle X\rangle$ be a set of non-zero normal polynomials modulo I with respect to σ, let $\mathcal{G}$ be an associated tuple of G, and let $J/I \subseteq K\langle X\rangle/I$ be the right ideal generated by G. Then G is a σ-Gröbner basis of J/I if and only if* $\mathrm{RNR}_{\sigma,I,\mathcal{G}}(f) = 0$ *for all $f \in SO_G \cup SO_{GG_I}$.*

Proof. If G is a σ-Gröbner basis of J/I, then $\mathrm{RNR}_{\sigma,I,\mathcal{G}}(f) = 0$ for all $f \in SO_G \cup SO_{GG_I}$ follows from the fact that $f \in J$ and Proposition 6.1.10. Conversely, suppose that $\mathrm{RNR}_{\sigma,I,\mathcal{G}}(f) = 0$ for all $f \in SO_G \cup SO_{GG_I}$. To prove G is a σ-Gröbner basis of J/I, by Definition 6.1.8 it suffices to prove that for any non-zero normal polynomial $f \in J \setminus I$ there exists a polynomial $g \in G$ such that $\mathrm{LT}_\sigma(g)$ is a prefix of $\mathrm{LT}_\sigma(f)$. Note that f has a representation $f = \sum_{j=1}^{s} g_j q_j + \sum_{i=1}^{t} c_i w_i g'_i w'_i$ with $g_j \in G, q_j \in K\langle X\rangle \setminus \{0\}$ for all $j \in \{1, \ldots, s\}$, and with $c_i \in K \setminus \{0\}, g'_i \in G_I, w_i, w'_i \in \langle X\rangle$ for all $i \in \{1, \ldots, t\}$. Then it suffices to show that there exists such representation satisfying $\mathrm{LT}_\sigma(f) \equiv \max_\sigma\{\mathrm{LT}_\sigma(g_j) \cdot \mathrm{LT}_\sigma(q_j) \mid j \in \{1, \ldots, s\}\}$. The existence of the representation follows from Remark 3.1.13.a and Theorem 6.1.9. □

Now we formulate a Buchberger Procedure to enumerate σ-Gröbner bases of the right ideals $J/I \subseteq K\langle X\rangle/I$ as follows.

Corollary 6.1.13. (Buchberger Procedure) *Let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a set of normal polynomials modulo I with respect to σ, let $\mathcal{G}$ be an associated tuple of G, and let $J \subseteq K\langle X\rangle$ be the right ideal generated by the set G. Consider the following sequence of instructions.*

1) Let $S = \{\frac{1}{\mathrm{LC}_\sigma(g)}g - \frac{1}{\mathrm{LC}_\sigma(g')}g'w \mid g, g' \in \mathcal{G}, g \neq g', w \in \langle X\rangle, \mathrm{LT}_\sigma(g) \equiv \mathrm{LT}_\sigma(g') \cdot w\} \cup \{\frac{1}{\mathrm{LC}_\sigma(g)}gw - \frac{1}{\mathrm{LC}_\sigma(g')}w'g' \mid g \in \mathcal{G}, g' \in G_I, w, w' \in \langle X\rangle, \mathrm{LT}_\sigma(g) \cdot w \equiv w' \cdot \mathrm{LT}_\sigma(g')\}$.

2) *If $S = \emptyset$, return the result $\mathcal{G}$. Otherwise, select a polynomial $s \in S$ using a fair strategy and delete it from S.*

3) *Compute $\bar{s} = \mathrm{RNR}_{\sigma,I,\mathcal{G}}(s)$ by the Right Division Algorithm given in Theorem 6.1.9. If $\bar{s} = 0$, continue with step 2).*

4) *Append the set $\{\frac{1}{\mathrm{LC}_\sigma(g)}g - \frac{1}{\mathrm{LC}_\sigma(\bar{s})}\bar{s}w \mid g \in \mathcal{G}, w \in \langle X\rangle, \mathrm{LT}_\sigma(g) \equiv \mathrm{LT}_\sigma(\bar{s}) \cdot w\} \cup \{\frac{1}{\mathrm{LC}_\sigma(\bar{s})}\bar{s}w - \frac{1}{\mathrm{LC}_\sigma(g')}w'g' \mid g' \in G_I, w, w' \in \langle X\rangle, \mathrm{LT}_\sigma(\bar{f}) \cdot w \equiv w' \cdot \mathrm{LT}_\sigma(g')\}$ to the set S, and append $\bar{s}$ to $\mathcal{G}$. Then continue with step 2).*

This is a procedure that enumerates a σ-Gröbner basis $\mathcal{G}$ of the right ideal $J/I \subseteq K\langle X\rangle/I$. If J/I has a finite σ-Gröbner basis, it stops after finitely many steps and the resulting tuple $\mathcal{G}$ is a finite σ-Gröbner basis of J/I.

Proof. Analogous to Theorem 4.1.14. □

Remark 6.1.14. Let us make some observations about this procedure.

a) The set $SO_G \cup SO_{GG_I}$ works similarly to the set of obstructions in that the former is actually the set of S-polynomials of the corresponding obstructions. Thus the methods for improving the Buchberger Procedure in free monoid rings (see Section 4.2) can also be applied, *mutatis mutandis*, to the Buchberger Procedure given in Corollary 6.1.13.

b) Recall that every finitely generated right ideal of $K\langle X\rangle$ has a finite Gröbner basis (see Section 4.4). However, a finitely generated right ideal in $K\langle X\rangle/I$ may not have a finite Gröbner basis. For instance, consider the right ideal $\langle x\rangle/\langle xy-yx\rangle \subseteq K\langle x,y\rangle/\langle xy-yx\rangle$ and the admissible ordering $\sigma = \texttt{LLex}$ such that $x >_\sigma y$. Then the ideal $\langle x\rangle/\langle xy-yx\rangle$ has an infinite (reduced) σ-Gröbner basis $G = \{y^k x \mid k \in \mathbb{N}\}$. Therefore we should content ourselves with an enumerating procedure as in Corollary 6.1.13.

To end this section we present a meaningful application of Gröbner bases of right ideals in $K\langle X\rangle/I$ which checks for a polynomial $f \in K\langle X\rangle \setminus I$ whether $\bar{f} \in K\langle X\rangle/I$ is invertible. Note that $\bar{f} \in K\langle X\rangle/I$ is invertible if there exists an element $\bar{q} \in K\langle X\rangle/I$ such that $\bar{f}\bar{q} = \bar{1}$. Consider the right ideal $\langle f\rangle/I \subseteq K\langle X\rangle/I$. Then $\bar{f}$ is invertible indicates that $\bar{1} \in \langle f\rangle/I$, which implies that $1 \in \langle f\rangle \setminus I$. Let G be a σ-Gröbner basis of J/I. Then by Definition 6.1.8 there exists a polynomial $g \in G$ such that $\mathrm{LT}_\sigma(g)$ is a prefix of 1. Thus g must be a non-zero constant and hence G contains a constant.

Conversely assume that G contains a non-zero constant $c \in K$. Since c is contained in $\langle f \rangle$, there exists a polynomial $q \in K\langle X \rangle$ such that $fq - c \in I$. Thus $\bar{f}\bar{q} = \bar{c}$ and hence $\bar{f} \in K\langle X \rangle / I$ is invertible. Therefore we can conclude as follows.

Proposition 6.1.15. *Let $f \in K\langle X \rangle \setminus I$ be a polynomial. Then $\bar{f} \in K\langle X \rangle / I$ is invertible if and only if every Gröbner basis of the right ideal $\langle f \rangle / I \subseteq K\langle X \rangle / I$ contains a non-zero constant $c \in K$. In this case the right ideal $\langle f \rangle / I \subseteq K\langle X \rangle / I$ has finite Gröbner bases.*

From another point of view, if the right ideal $\langle f \rangle / I \subseteq K\langle X \rangle / I$ does not have a finite Gröbner basis, then $\bar{f} \in K\langle X \rangle / I$ is non-invertible. In the following we present explicitly a variation of the Buchberger Procedure to check whether $\bar{f} \in K\langle X \rangle / I$ is invertible and to compute the inverse of $\bar{f}$ if it is invertible.

Corollary 6.1.16. *Let $f \subseteq K\langle X \rangle \setminus I$ be a polynomial. Consider the following sequence of instructions.*

1) *Compute $\bar{f} = \mathrm{HF}_{\sigma,I}(f)$. If $\bar{f} = 0$, then return "$\bar{f}$ is not invertible".*

2) *Let $s = 1, g_1 = \hat{g}_1 = \bar{f}, \mathcal{G} = (g_1)$, and $S = \{\frac{1}{\mathrm{LC}_\sigma(g_1)} g_1 w - \frac{1}{\mathrm{LC}_\sigma(g_i)} w' g_i \mid g_i \in G_I, w, w' \in \langle X \rangle, \mathrm{LT}_\sigma(g_1) \cdot w \equiv w' \cdot \mathrm{LT}_\sigma(g_i)\}$.*

3) *If $S = \emptyset$, then return "$\bar{f}$ is not invertible" and the tuple $\mathcal{G}$. Otherwise, select a polynomial $g \in S$ using a fair strategy and delete it from S.*

4) *Compute $\bar{g} = \mathrm{RNR}_{\sigma,I,\mathcal{G}}(g)$ by the Right Division Algorithm given in Theorem 6.1.9. If $\bar{g} = 0$, continue with step 3). If $\bar{g} \neq 0$, increase s by one, let $g_s = \bar{g}$. Assume that we have $g - (\sum_{j=1}^{s-1} g_j q_{sj} + \bar{g}) \in I$. If in step 3) we have $g = \frac{1}{\mathrm{LC}_\sigma(g_j)} g_j - \frac{1}{\mathrm{LC}_\sigma(g_{j'})} g_{j'} w$ with $g_j, g_{j'} \in \mathcal{G}$, then let $\hat{g}_s = \sum_{j=1}^{s-1} \hat{g}_j q_{sj} - (\frac{1}{\mathrm{LC}_\sigma(\hat{g}_j)} \hat{g}_j - \frac{1}{\mathrm{LC}_\sigma(\hat{g}_{j'})} \hat{g}_{j'} w)$. If $g = \frac{1}{\mathrm{LC}_\sigma(g_j)} g_j w - \frac{1}{\mathrm{LC}_\sigma(g_i)} w' g_i$ with $g_j \in \mathcal{G}$ and $g_i \in G_I$, then let $\hat{g}_s = \sum_{j=1}^{s-1} \hat{g}_j q_{sj} - (\frac{1}{\mathrm{LC}_\sigma(\hat{g}_j)} \hat{g}_j w - \frac{1}{\mathrm{LC}_\sigma(g_i)} w' g_i)$.*

5) *If $\hat{g}_s = 1$, then we apply forward substitution and obtain $1 = \bar{f} \cdot q + h$ with $q \in K\langle X \rangle, h \in I$, compute $\bar{q} = \mathrm{HF}_{\sigma,I}(q)$, append g_s to $\mathcal{G}$, and return $\bar{q}$ and the tuple $\mathcal{G}$. If $\hat{g}_s \neq 1$, append the set $\{\frac{1}{\mathrm{LC}_\sigma(g_j)} g_j - \frac{1}{\mathrm{LC}_\sigma(g_s)} g_s w \mid g_j \in \mathcal{G}, w \in \langle X \rangle, \mathrm{LT}_\sigma(g_j) \equiv \mathrm{LT}_\sigma(g) \cdot w\} \cup \{\frac{1}{\mathrm{LC}_\sigma(g_s)} g_s w - \frac{1}{\mathrm{LC}_\sigma(g_i)} w' g_i \mid g_i \in G_I, w, w' \in \langle X \rangle, \mathrm{LT}_\sigma(g_s) \cdot w \equiv w' \cdot \mathrm{LT}_\sigma(g_i)\}$ to the set S, and append g_s to $\mathcal{G}$. Then start again with step 3).*

This is a procedure that enumerates a σ-Gröbner basis $\mathcal{G}$ of the right ideal $\langle g \rangle / I \subseteq K\langle X \rangle / I$. If $\langle f \rangle / I$ has a finite σ-Gröbner basis, it stops after finitely many steps and *the resulting tuple $\mathcal{G}$ is a finite σ-Gröbner basis of $\langle f\rangle/I$. Moreover, if $\bar{f} \in K\langle X\rangle/I$ is invertible, the procedure returns the inverse $\bar{q}$ of $\bar{f}$.*

Proof. Observe that $\hat{g}_j = g_j$ and the procedure above is nothing but the Buchberger Procedure given in Corollary 6.1.13 along with extra data $\hat{g}_j$ for tracking the enumerating procedure. The claim follows from Corollary 6.1.13 and Proposition 6.1.15. □

Example 6.1.17. We consider the *dihedral group* $D_6 = \langle a, b | a^3 = b^2 = (ab)^2 = 1\rangle$ of order 6 and the residue class ring $\mathbb{F}_2\langle a, b\rangle/I$ where $I \subseteq \mathbb{F}_2\langle a, b\rangle$ is the two-sided ideal generated by the set $\{a^3+1, b^2+1, (ab)^2+1\}$. Let $\sigma = \texttt{LLex}$ be the length-lexicographic ordering on $\langle a, b\rangle$ such that $a >_\sigma b$. The ideal I has the reduced σ-Gröbner basis $G_I = \{b^2+1, bab+a^2, ba^2+ab, aba+b, a^2b+ba, a^3+1\}$. We want to compute the inverse of $\overline{a^2b} \in \mathbb{F}_2\langle a, b\rangle/I$. Applying the procedure given in Cororllary 6.1.16, we have

1) Compute $\overline{a^2b} = \mathrm{NF}_{\sigma,I}(a^2b) = ba$.

2) Let $s = 1, g_1 = \hat{g}_1 = ba, \mathcal{G} = (g_1)$, and $S = \{bab - (bab + a^2), baa - (ba^2 + ab), baba - b(aba + b), baab + b(a^2b + ba), baa^2 - b(a^3 + 1)\}$.

3) We select $g = bab - (bab + a^2) = a^2$ and delete it from S.

4) Compute $\bar{g} = \mathrm{NR}_{\sigma,G,I}(g) = a^2$. Let $s = 2, g_2 = a^2$, and $\hat{g}_2 = \hat{g}_1 b - (bab + a^2)$.

5*) Append $\{a^2ba - a(aba + b), a^2b - (a^2b + ba), a^2a - (a^3 + 1)\}$ to S, and append g_2 to $\mathcal{G}$.

3) Select $g = baa - (ba^2 + ab) = ab$ and delete it from S.

4) Compute $\bar{g} = \mathrm{RNR}_{\sigma,I,\mathcal{G}}(g) = ab$. Let $s = 3, g_3 = ab$, and $\hat{g}_3 = \hat{g}_1 a - (ba^2 + ab)$.

5) Append $\{abb - a(b^2 + 1), abab - a(bab + a^2), aba^2 - a(ba^2 + ab), aba - (aba + b)\}$, and append g_3 to $\mathcal{G}$.

3) Select $g = abb - a(b^2 + 1)$ and delete it from S.

4) Compute $\bar{g} = \mathrm{RNR}_{\sigma,I,\mathcal{G}}(g) = a$. Let $s = 4, g_4 = a$, and $\hat{g}_4 = \hat{g}_3 b - a(b^2 + 1)$.

5) Note that $g_2 - aa = 0, g_3 - ab = 0$. Append $\{aba - (aba + b), aab - (a^2b + ba), aa^2 - (a^3 + 1)\}$ to S, and append g_4 to $\mathcal{G}$.

3) Select $g = aba - (aba + b)$ and delete it from S.

4) Compute $\bar{g} = \mathrm{RNR}_{\sigma,I,\mathcal{G}}(g) = b$. Let $s = 5, g_5 = b$, and $\hat{g}_5 = \hat{g}_3 a - (aba + b)$.

5) Note that $g_1 - ba = 0, g_3 - ab = 0$. Append $\{bb - (b^2+1), bab - (bab + a^2), ba^2 - (ba^2 + ab)\}$ to S, and append g_5 to $\mathcal{G}$.

3) Select $g = bb - (b^2 + 1)$ and delete it from S.

4) Compute $\bar{g} = \mathrm{RNR}_{\sigma,I,\mathcal{G}}(g) = 1$. Let $s = 6, g_6 = 1$, and $\hat{g}_6 = \hat{g}_5 b - (b^2 + 1)$.

5) Since $\hat{g}_5 = 1$, we apply forward substitution and obtain $1 = \overline{a^2b}a^2b + h$ where $h = (ba^2+ab)ab + (aba+b)b + (b^2+1) \in I$. Return $\overline{a^2b}$ and the tuple $\mathcal{G} = (g_1, \ldots, g_6)$.

Therefore $\overline{a^2b}$ is the inverse of itself. It is easy to verify that we have $\mathrm{NF}_{\sigma,I}(a^2b \cdot a^2b) = 1$.

Remark 6.1.18. Observe that in Example 6.1.17 some polynomials are added to the set S repeatedly, for instance $baa - (ba^2 + ab)$ in step 2) and $a^2ba - a(aba + b)$ in step 5*) are both equal to ab. Also observe that some polynomials added to S are multiples of others and should be removed from S because of redundancy, for instance in step 2) $baba - b(aba + b) = b^2, baab + b(a^2b + ba) = b^2a$ are multiples of $baa^2 - b(a^3 + 1) = b$. Moreover, in step 5*) we even added 1 to S. These observations indicate that it could be a good idea to simplify polynomials before adding them to S. In Corollary 6.1.16 if some polynomial is equal to 1 after simplifying, then we can do forward substitution immediately and get the required inverse. For instance in Example 6.1.17 we obtain $1 = \hat{g}_2 a - (a^3 + 1)$ in step 5*). By forward substitution, we obtain $1 = \overline{a^2b}ba + (bab + a^2)a + (a^3 + 1)$. Thus $\overline{ba}$ is the inverse of $\overline{a^2b}$. Indeed we have $\overline{a^2b} = \overline{ba}$. However, it is still unclear whether this kind of simplification can be used to improve the Buchberger Procedure in the general case.

6.1.3 Gröbner bases of Submodules in $(K\langle X\rangle/I \otimes K\langle X\rangle/I)^r$

In this short subsection we shall quickly revise Gröbner basis theory in free $K\langle X\rangle/I$-bimodule $\bar{F}_r = (K\langle X\rangle/I \otimes K\langle X\rangle/I)^r$ introduced by H. Bluhm and M. Kreuzer [8], and present the Division Algorithm in $\bar{F}_r$. Recall that we consider the set $\mathcal{O}_\sigma(I)$ as the set of all words in $K\langle X\rangle/I$ and represent elements in $\bar{F}_r$ in the form of $\sum_{i=1}^r \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e_i w'_{ij}$ with $c_{ij} \in K, w_{ij}, w'_{ij} \in \mathcal{O}_\sigma(I)$ for all $i \in \{1, \ldots, r\}, j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. The following lemma (compared with [8], Lemma 4.2) is the foundation stone of Gröbner basis theory in $\bar{F}_r$.

Lemma 6.1.19. *Let τ be compatible with σ, and let $m = \sum_{i=1}^{r}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_iw'_{ij} \in \bar{F}_r \setminus \{0\}$ with $c_{ij} \in K$ and $w_{ij}, w'_{ij} \in \mathcal{O}_\sigma(I)$ for all $i \in \{1,\ldots,r\}, j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. Furthermore, let $\mathrm{LT}_\tau(m) = w_1e_kw'_1$, and let $w, w' \in \mathcal{O}_\sigma(I)$ such that $w\cdot w_1, w'_1 \cdot w' \in \mathcal{O}_\sigma(I)$. Then we have $w \cdot \mathrm{LT}_\tau(m) \cdot w' \equiv w\mathrm{LT}_\tau(m)w' \equiv \mathrm{LT}_\tau(wmw')$.*

Proof. The first equivalence follows from $w \cdot w_1, w'_1 \cdot w' \in \mathcal{O}_\sigma(I)$. To prove the second equivalence it suffices to prove $ww_1e_kw'_1w' \geq_\tau \mathrm{LT}_\sigma(ww_2)e_l\mathrm{LT}_\sigma(w'_2w')$ for all $w_2e_lw'_2 \in \mathrm{Supp}(m)$. Since $w_1e_kw'_1 \geq_\tau w_2e_lw'_2$ and τ is compatible with multiplication, we have $w \cdot w_1e_kw'_1 \cdot w' \geq_\tau w \cdot w_2e_lw'_2 \cdot w'$. Since $w \cdot w_2 \geq_\sigma \mathrm{LT}_\sigma(ww_2)$ and τ is compatible with σ, we have $w \cdot w_2e_l \geq_\tau \mathrm{LT}_\sigma(ww_2)e_l$. Since τ is compatible with multiplication, we have $w \cdot w_2e_lw'_2 \cdot w' \geq_\tau \mathrm{LT}_\sigma(ww_2)e_lw'_2 \cdot w'$. Similarly we have $\mathrm{LT}_\sigma(ww_2)e_lw'_2 \cdot w' \geq_\tau \mathrm{LT}_\sigma(ww_2)e_l\mathrm{LT}_\sigma(w'_2w')$. Altogether we have $ww_1e_kw'_1w' \geq_\tau \mathrm{LT}_\sigma(ww_2)e_l\mathrm{LT}_\sigma(w'_2w')$. □

Observe that the assumption that τ is compatible with σ, which was not explicitly mentioned in [8], is crucial to the proof of Lemma 6.1.19.

Assumption 6.1.20. *In the rest of this subsection, we shall assume that the module term ordering τ is compatible with the admissible ordering σ.*

We shall define Gröbner bases in free $K\langle X\rangle/I$-bimodule $\bar{F}_r$ as follows.

Definition 6.1.21. Let $M \subseteq \bar{F}_r$ be a $K\langle X\rangle/I$-submodule. A subset $G \subseteq M \setminus \{0\}$ of elements is called a **τ-Gröbner basis** of M if

$$\mathrm{LT}_\tau\{M\} = \{w \cdot \mathrm{LT}_\tau(g) \cdot w' \mid g \in G, w, w' \in \mathcal{O}_\sigma(I)\}.$$

Gröbner bases defined in this way share many of nice properties of Gröbner bases in other settings. The following is the most promising one.

Proposition 6.1.22. *Let $M \subseteq \bar{F}_r$ be a $K\langle X\rangle/I$-submodule, and let $G \subseteq M \setminus \{0\}$ be a subset of elements. Then the following conditions are equivalent.*

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

b) Every element $m \in M \setminus \{0\}$ has a representation

$$m = \sum_{i=1}^{s} c_iw_ig_iw'_i$$

with $c_1,\ldots,c_s \in K\setminus\{0\}, w_1,\ldots,w'_s \in \mathcal{O}_\sigma(I), g_1,\ldots,g_s \in G$ such that $\mathrm{LT}_\tau(m) \geq_\tau w_i \cdot \mathrm{LT}_\tau(g_i) \cdot w'_i \geq \mathrm{LT}_\tau(w_ig_iw'_i)$ for all $i \in \{1,\ldots,s\}$.

Proof. See [8], Proposition 4.3. □

Intuitively, the Division Algorithm should be one of the necessary tools for Gröbner basis computations in $\bar{F}_r$. By integrating the Division Algorithm in F_r (see Theorem 5.1.12) with the normal form computation in $K\langle X\rangle$, we present the following division algorithm in $\bar{F}_r$.

Theorem 6.1.23. (The Division Algorithm) *Let $m \in \bar{F}_r \setminus \{0\}$ be an element, and let $G \subseteq \bar{F}_r \setminus \{0\}$ be a set elements. Consider the following sequence of instructions.*

1) *Let $t = 0$ and $v = m$.*

2) *If there exists an element $g \in G$ such that $\mathrm{LT}_\tau(v) \equiv w \cdot \mathrm{LT}_\tau(g) \cdot w'$ for some $w, w' \in \mathcal{O}_\sigma(I)$, then increase t by 1, set $c_t = \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(g)}, w_t = w, w'_t = w', g_t = g$, and replace v by $v - c_t w_t g_t w'_t$.*

3) *Repeat step 2) until there is no more element $g \in G$ such that $\mathrm{LT}_\tau(v)$ is a multiple of $\mathrm{LT}_\tau(g)$. Return the tuples $(c_1, w_1, w'_1, g_1), \ldots, (c_t, w_t, w'_t, g_t)$ and the element $v \in \bar{F}_r$.*

This is an algorithm which returns tuples $(c_1, w_1, w'_1, g_1), \ldots, (c_t, w_t, w'_t, g_t)$ and an element $v \in \bar{F}_r$ such that

$$m - (\sum_{i=1}^{t} c_i w_i g_i w'_i + v) \in (I \otimes K\langle X\rangle/I)^r \oplus (K\langle X\rangle/I \otimes I)^r \oplus (I \otimes I)^r$$

and such that the following conditions are satisfied.

a) *For all $i \in \{1, \ldots, t\}$, we have $\mathrm{LT}_\tau(w_i g_i w'_i) = w_i \cdot \mathrm{LT}_\tau(g_i) \cdot w'_i$.*

b) *If $t > 0$, then we have $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(w_1 g_1 w'_1) >_\tau \cdots >_\tau \mathrm{LT}_\tau(w_t g_t w'_t)$.*

c) *If $v \neq 0$, then we have $\mathrm{LT}_\tau(m) \geq_\tau \mathrm{LT}_\tau(v)$.*

Proof. Analogous to Theorem 6.1.9. □

Remark 6.1.24. Unfortunately, we haven't succeeded in obtaining an effective Buchberger Criterion for the computation of Gröbner bases in $\bar{F}_r$. One possible approach is to follow the previous subsections by embedding the computations in F_r. However, as indicated by the representation obtained in Theorem 6.1.23, we also have to "embed" the system of generators of I to each component of F_r. Consequently, the system of generators of the $K\langle X\rangle/I$-submodule expands rapidly. It is still unclear which generators are redundant for Gröbner basis computations in $\bar{F}_r$.

6.2 Elimination

In this section we shall work on Gröbner bases applications related to two types of eliminations: elimination of variables in the free monoid ring $K\langle X\rangle$ and component elimination in the free $K\langle X\rangle$-bimodule $F_r = (K\langle X\rangle \otimes K\langle X\rangle)^r$.

6.2.1 Elimination of Variables in $K\langle X\rangle$

In this subsection we study applications of Gröbner bases related to elimination of variables in the free monoid ring $K\langle X\rangle$. In particular, we formulate the computation of the intersection of ideals and investigate the presentations of the kernels and images of K-algebra homomorphisms. Recall that $X = \{x_1, \ldots, x_n\}$ is a finite alphabet (or set of indeterminates). In the following, we let $L \subseteq X$ be a subset, $\widehat{X} = X \setminus L$, and $K\langle\widehat{X}\rangle$ a free monoid ring generated by $\widehat{X}$ over K. Recall that the free monoid $\langle X\rangle$ generated by X is the set of terms in $K\langle X\rangle$. Similarly, we consider the free monoid $\langle\widehat{X}\rangle$ generated by $\widehat{X}$ as the set of terms in $K\langle\widehat{X}\rangle$.

Definition 6.2.1. Let $L \subseteq X$ be a subset of the alphabet.

a) An admissible ordering σ on $\langle X\rangle$ is called an **elimination ordering** for L if every polynomial $f \in K\langle X\rangle \setminus \{0\}$ such that $\mathrm{LT}_\sigma(f) \in \langle\widehat{X}\rangle$ is contained in $K\langle\widehat{X}\rangle$.

b) Given an ideal $I \subseteq K\langle X\rangle$, the ideal $I \cap K\langle\widehat{X}\rangle$ in $K\langle\widehat{X}\rangle$ is called the **elimination ideal** of I with respect to L.

It is easy to check that for any $j \in \{1, \ldots, n\}$, the elimination ordering `Elim` on $\langle X\rangle$, as given in Definition 3.1.8, is an elimination ordering for $L = \{x_1, \ldots, x_j\}$.

Lemma 6.2.2. *Let σ be an admissible ordering on $\langle X\rangle$. Then the restriction $\hat{\sigma}$ of σ to $\langle\widehat{X}\rangle$ is also an admissible ordering.*

Proof. Consider $\langle\widehat{X}\rangle$ as a subset of $\langle X\rangle$. Observe that for any two words $\hat{w}_1, \hat{w}_2 \in \langle\widehat{X}\rangle$, we have $\hat{w}_1 \leq_\sigma \hat{w}_2$ if and only if $\hat{w}_1 \leq_{\hat{\sigma}} \hat{w}_2$. Then it is straightforward to check that $\hat{\sigma}$ on $\langle\widehat{X}\rangle$ satisfies conditions a)-f) of Definition 3.1.1. □

As shown in the following theorem, using Gröbner bases with respect to some elimination ordering, we can obtain Gröbner bases of elimination ideals easily. The following theorem is the key to the applications we shall consider in this subsection.

Theorem 6.2.3. (Computation of Elimination Ideals) *Let $I \subseteq K\langle X\rangle$ be an ideal, let $L \subseteq X$ be a subset of alphabet, and let σ be an elimination ordering for L. Furthermore, let $\widehat{X} = X\backslash L$, let $K\langle \widehat{X}\rangle$ be the free monoid ring generated by $\widehat{X}$, and let $\hat{\sigma}$ be the restriction of σ to $\langle \widehat{X}\rangle$. If G is a σ-Gröbner basis of I, then the set $G \cap K\langle \widehat{X}\rangle$ is a $\hat{\sigma}$-Gröbner basis of the elimination ideal $I \cap K\langle \widehat{X}\rangle$.*

Proof. Clearly $G \cap K\langle \widehat{X}\rangle \subseteq I \cap K\langle \widehat{X}\rangle$. To prove $G \cap K\langle \widehat{X}\rangle$ is a $\hat{\sigma}$-Gröbner basis of $I \cap K\langle \widehat{X}\rangle$, by Lemma 3.3.15 it suffices to show that the set $\mathrm{LT}_{\hat{\sigma}}\{G \cap K\langle \widehat{X}\rangle\}$ generates the leading term set $\mathrm{LT}_{\hat{\sigma}}\{I \cap K\langle \widehat{X}\rangle\}$. Let $f \in I \cap K\langle \widehat{X}\rangle$ be a non-zero polynomial. As $\hat{\sigma}$ is the restriction of σ to $\langle \widehat{X}\rangle$, we have $\mathrm{LT}_\sigma(f) = \mathrm{LT}_{\hat{\sigma}}(f) \in \langle \widehat{X}\rangle$. Since G is a σ-Gröbner basis of I, there exist $w, w' \in \langle X\rangle$ and $g \in G$ such that $\mathrm{LT}_\sigma(f) = w\mathrm{LT}_\sigma(g)w'$. Clearly $w, w', \mathrm{LT}_\sigma(g) \in \langle \widehat{X}\rangle$. Then $g \in K\langle \widehat{X}\rangle$ follows from the assumption that σ is an elimination ordering for L. Thus $g \in G \cap K\langle \widehat{X}\rangle$. Therefore $\mathrm{LT}_{\hat{\sigma}}\{G \cap K\langle \widehat{X}\rangle\}$ generates $\mathrm{LT}_{\hat{\sigma}}\{I \cap K\langle \widehat{X}\rangle\}$, and hence $G \cap K\langle \widehat{X}\rangle$ is a $\hat{\sigma}$-Gröbner basis of $I \cap K\langle \widehat{X}\rangle$. □

With the notation given in Theorem 6.2.3, it is obvious that if G is the reduced σ-Gröbner basis of I then $G \cap K\langle \widehat{X}\rangle$ is the reduced $\hat{\sigma}$-Gröbner basis of $I \cap K\langle \widehat{X}\rangle$.

The first application we shall study in this subsection is the computation of the intersection of ideals in $K\langle X\rangle$. Let $G_I, G_J \subseteq K\langle X\rangle \setminus \{0\}$ be two sets of polynomials which generate ideals $I, J \subseteq K\langle X\rangle$, respectively. It is easy to check that the ideal $I + J \subseteq K\langle X\rangle$ is generated by the set $G_I \cup G_J$. The following proposition formulates the computation of the intersection $I \cap J$.

Proposition 6.2.4. *Let $G_I, G_J \subseteq K\langle X\rangle \setminus \{0\}$ be two sets of polynomials which generate ideals $I, J \subseteq K\langle X\rangle$, respectively. We choose a new indeterminate y, and form the free monoid ring $K\langle y, X\rangle$ generated by $\{y\} \cup X$ over K. Furthermore, let $N \subseteq K\langle y, X\rangle$ be the ideal generated by the set $\{yf \mid f \in G_I\} \cup \{(1-y)g \mid g \in G_J\}$, and let $C \subseteq K\langle y, X\rangle$ be the ideal of commutators, i.e. the ideal C is generated by the set $\{yx_1 - x_1y, \ldots, yx_n - x_ny\}$. Then we have $I \cap J = (N + C) \cap K\langle X\rangle$.*

Proof. For a polynomial $v \in I \cap J$, there exist not necessarily pairwise distinct $f_1, \ldots, f_s \in G_I$, $g_1, \ldots, g_t \in G_J$, and $p_1, \ldots, p_s'$, $q_1, \ldots, q_t' \in K\langle X\rangle$, such that $v = \sum_{i=1}^s p_i f_i p_i' = \sum_{j=1}^t q_j g_j q_j'$. Then we have $v = yv + (1-y)v = \sum_{i=1}^s yp_i f_i p_i' + \sum_{j=1}^t (1-y)q_j g_j q_j'$. Clearly $yx_i = x_iy + (yx_i - x_iy)$ and $(1-y)x_i = x_i(1-y) - (yx_i - x_iy)$ for all $i \in \{1, \ldots, n\}$. By replacing yx_i with $x_iy + (yx_i - x_iy)$ and $(1-y)x_i$ with $x_i(1-y) - (yx_i - x_iy)$ for all $i \in \{1, \ldots, n\}$, we get $v = \sum_{i=1}^s p_i y f_i p_i' + \sum_{j=1}^t q_j(1-y)g_j q_j' + p$ with $p \in C$. Thus we have $v \in (N + C) \cap K\langle X\rangle$.

Conversely, suppose that $v \in (N + C) \cap K\langle X\rangle$. By the definitions of N and C, there exist not necessarily pairwise distinct $f_1, \dots, f_s \in G_I$, $g_1, \dots, g_t \in G_J$, and $p_1, \dots, p'_s, q_1, \dots, q'_t \in K\langle y, X\rangle, p \in C$, such that $v = \sum_{i=1}^{s} p_i y f_i p'_i + \sum_{j=1}^{t} q_j(1-y)g_j q'_j + p$. Since $v \in K\langle X\rangle$, the polynomial v is invariant under the substitution $y \mapsto 1$, i.e. we have $v = \sum_{i=1}^{s} p_i(1, X)f_i(X)p'_i(1, X) \in I$. Similarly, the polynomial v is invariant under the substitution $y \mapsto 0$, i.e. we have $v = \sum_{j=1}^{t} q_j(0, X)g_j(X)q'_j(0, X) \in J$. Altogether, we get $v \in I \cap J$. □

Remark 6.2.5. With the notation given in Proposition 6.2.4, we compute the intersection $I \cap J$ using the following sequence of instructions.

1) Let $H \subseteq K\langle y, X\rangle$ be the ideal generated by the set $\{yf \mid f \in G_I\} \cup \{(1-y)g \mid g \in G_J\} \cup \{yx_1 - x_1y, \dots, yx_n - x_ny\}$.

2) Choose an elimination ordering σ on $\langle y, X\rangle$ for $\{y\}$. Enumerate a σ-Gröbner basis G of the ideal H.

3) By Proposition 6.2.4 and Theorem 6.2.3 the set $G \cap K\langle X\rangle$ is a $\hat{\sigma}$-Gröbner basis of the ideal $I \cap J \subseteq K\langle X\rangle$.

Proposition 6.2.4 can be easily generalized for the computation of the intersection of $s \geq 2$ ideals in $K\langle X\rangle$ as follows.

Corollary 6.2.6. *Let $s \geq 2$, and let $I_i \subseteq K\langle X\rangle$ be the ideal generated by the set of polynomials $G_i \subseteq K\langle X\rangle$ for $i = 1, \dots, s$. We choose a set of new indeterminates $Y = \{y_1, \dots, y_{s-1}\}$, and form the free monoid ring $K\langle Y, X\rangle$. Moreover, let $N \subseteq K\langle Y, X\rangle$ be the ideal generated by the set $\cup_{i=1}^{s-1}\{y_i g_{ij} \mid g_{ij} \in G_i\} \cup \{(1-y_1-\cdots-y_{s-1})g_{sj} \mid g_{sj} \in G_s\}$, and let $C' \subseteq K\langle Y, X\rangle$ be the ideal generated by the set $\{y_i x_j - x_j y_i \mid i \in \{1, \dots, s-1\}, j \in \{1, \dots, n\}\}$. Then we have $\cap_{i=1}^{s} I_i = (N + C') \cap K\langle X\rangle$.*

The next application we shall consider in this subsection is to investigate the kernels and images of K-algebra homomorphisms. The following proposition computes the kernel of a given K-algebra homomorphism.

Proposition 6.2.7. *Let $I \subseteq K\langle X\rangle$ be an ideal, let $Y = \{y_1, \dots, y_m\}$ be another alphabet, let $K\langle Y\rangle$ be the free monoid ring generated by Y over K, and let $J \subseteq K\langle Y\rangle$ be an ideal. Moreover, let $g_1, \dots, g_m \in K\langle X\rangle$ be polynomials, and let $\varphi : K\langle Y\rangle/J \to K\langle X\rangle/I$ be a homomorphism of K-algebras defined by $\bar{y}_i \mapsto \bar{g}_i$ for $i = 1, \dots, m$. We form the free monoid ring $K\langle X, Y\rangle$ generated by $X \cup Y$ over K, and let $D \subseteq K\langle X, Y\rangle$*

be the diagonal ideal generated by the set $\{y_1 - g_1, \dots, y_m - g_m\}$. *Then we have* $\ker(\varphi) = ((D+I) \cap K\langle Y\rangle) + J$.

Proof. Let $h \in K\langle Y\rangle$ be a polynomial such that $h + J \in \ker(\varphi)$, i.e. $\varphi(h+J) = h(g_1, \dots, g_m) \in I$. Clearly $y_i = (y_i - g_i) + g_i$ for all $i \in \{1, \dots, m\}$. By replacing y_i with $(y_i - g_i) + g_i$ for all $i \in \{1, \dots, m\}$, we get $h(y_1, \dots, y_n) = p + h(g_1, \dots, g_m)$ with $p \in D$. Therefore we have $h + J \in ((D+I) \cap K\langle Y\rangle) + J$. Conversely, suppose that $h + J \in ((D+I) \cap K\langle Y\rangle) + J$. By the definition of D, there exist not necessarily pairwise distinct $y_{i_1} - g_{i_1}, \dots, y_{i_s} - g_{i_s} \in \{y_1 - g_1, \dots, y_m - g_m\}$, and $p_1, \dots, p'_s \in K\langle X, Y\rangle, q \in I$, such that $h + J = \sum_{k=1}^{s} p_k(y_{i_k} - g_{i_k})p'_k + q + J$. Now we substitute $y_i + J \mapsto g_i + I$ for all $i \in \{1, \dots, m\}$, we get $\varphi(h+J) \in I$. Therefore $h + J \in \ker(\varphi)$. □

Remark 6.2.8. In the setting of Proposition 6.2.7, we assume that $G_I \subseteq K\langle X\rangle$ and $G_J \subseteq K\langle Y\rangle$ are systems of generators of the ideals I and J, respectively. Then we can compute the kernel of K-algebra homomorphism φ using the following sequence of instructions.

1) Let $H \subseteq K\langle X, Y\rangle$ be the ideal generated by the set $\{y_1 - g_1, \dots, y_m - g_m\} \cup G_I$.

2) Choose an elimination ordering σ on $\langle X, Y\rangle$ for X. Enumerate a σ-Gröbner basis G of the ideal H.

3) By Proposition 6.2.7 and Theorem 6.2.3 the set $G \cap K\langle Y\rangle$ is a $\hat{\sigma}$-Gröbner basis of the ideal $(D+I) \cap K\langle Y\rangle$. Hence the set $(G \cap K\langle Y\rangle) \cup G_J$ is a system of generators of $\ker(\varphi)$.

Let $I \subseteq K\langle X\rangle$ be an ideal, let $g \in K\langle X\rangle$ be a polynomial, and let $\bar{g} \in K\langle X\rangle/I$ be the residue class of f. Moreover, let y be a new indeterminate, and let $K[y]$ be the *univariate polynomial ring*. If there exists a polynomial $\mu \in K[y]$ such that $\mu(\bar{g}) = \bar{0}$, then $\bar{g}$ is called **algebraic** over K; otherwise $\bar{g}$ is called **transcendental** over K. In the former case the monic polynomial $\mu \in K[y]$ of least degree such that $\mu(\bar{g}) = \bar{0}$ is called the **minimal polynomial** of $\bar{g}$. As an immediate application of Proposition 6.2.7, the following corollary gives a condition for an element of $K\langle X\rangle/I$ to be algebraic over K and computes its minimal polynomial.

Corollary 6.2.9. *Let* $\varphi : K[y] \to K\langle X\rangle/I$ *be a* K*-algebra homomorphism given by* $y \mapsto \bar{g}$. *Then an element* $\bar{g} \in K\langle X\rangle/I$ *is algebraic over* K *if and only if* $\ker(\varphi) \neq \{0\}$. *Moreover, if an element* $\bar{g} \in K\langle X\rangle/I$ *is algebraic over* K, *then the unique monic generating polynomial of the ideal* $\ker(\varphi) \subseteq K[y]$ *is the minimal polynomial of* $\bar{g}$ *over* K.

Proof. Analogous to [43], Corollary 3.6.4. □

Remark 6.2.10. In the setting of Corollary 6.2.9, we choose an elimination ordering σ on $\langle X, y\rangle$ for X and compute a σ-Gröbner basis G of the ideal $\{y-g\}+I \subseteq K\langle X, y\rangle$. If $G \cap K[y] \neq \{0\}$, then by Corollary 6.2.9 the element $\bar{g} \in K\langle X\rangle/I$ is algebraic over K. However, since the ideal $\{y-g\}+I$ may not have a finite σ-Gröbner basis, it is only semi-decidable whether an element of $K\langle X\rangle/I$ is algebraic over K.

Remark 6.2.11. Furthermore, we can use Corollary 6.2.9 to semi-decide if a monoid element has finite order. Let $\mathcal{M} = \langle X \mid R\rangle$ be a finitely presented monoid, and let $I \subseteq K\langle X\rangle$ be the ideal generated by the set $\{l-r \mid (l,r) \in R\}$. Recall that we have $K\langle\mathcal{M}\rangle \cong K\langle X\rangle/I$ (see Corollary 2.2.11). Let $\bar{w} \in \mathcal{M}$ be a monoid element, and let $H \subseteq K\langle X, y\rangle$ be the ideal generated by the set $\{y-w\} \cup \{l-r \mid (l,r) \in R\}$. Choose an elimination ordering σ on $\langle X, y\rangle$ for X, and compute a σ-Gröbner basis G of the ideal H.

1) By Corollary 6.2.9, the order of $\bar{w}$ is infinite if and only if $G \cap K[y] = \emptyset$. In this case the order of $\mathcal{M}$ is also infinite. However the ideal H may not have a finite σ-Gröbner basis. Instead of computing a complete σ-Gröbner basis G, we can compute partial σ-Gröbner bases G' (see Remark 4.1.16) step by step using the Buchberger Procedure given in Theorem 4.1.14 and check whether $G' \cap K[y]$ is empty. If $G' \cap K[y] \neq \emptyset$, then we claim that the order of $\bar{w}$ is finite. Otherwise, we continue with next iteration of the loop of the Buchberger Procedure. In another way, we choose other polynomials $h_1, \ldots, h_k \in K\langle X, y\rangle$, and consider the ideal $H^+ = H + \langle h_1, \ldots, h_k\rangle \subseteq K\langle X, y\rangle$. Clearly $H^+ \cap K[y] = \emptyset$ implies $H \cap K[y] = \emptyset$. By chance H^+ has a finite σ-Gröbner basis. Thus to check whether $\bar{w}$ has infinite order we can compute a σ-Gröbner basis G^+ of H^+ and check whether $G^+ \cap K[y] = \emptyset$ (see [45], Remark 6.5).

2) If $G \cap K[y] \neq \emptyset$, then by Corollary 6.2.9 the element $\bar{w} \in K\langle X\rangle/I$ is algebraic over K. Since the generators of the ideal H are binomials, the polynomials in G and $G \cap K[y]$ are also binomials. Thus the minimal polynomial $\mu(y)$ of $\bar{w}$ is a binomial. Let $K = \mathbb{F}_2$. Then the minimal polynomial of $\bar{w}$ is of the form $\mu(y) = y^k + y^l$ with $k > l$, i.e. $\bar{w}^k = \bar{w}^l$. Moreover, if $\mathcal{M}$ is a group, then by the cancellation law we have $\bar{w}^{k-l} = 1$, i.e. the order of $\bar{w}$ is $k-l$.

Example 6.2.12. Consider the infinite *dihedral group* $D_\infty = \langle a, b \mid b^2 = (ab)^2 = 1\rangle$. We want to check the order of $\bar{a}$. We choose a new indeterminate t and form the free monoid ring $\mathbb{F}_2\langle a, b, t\rangle$. Let $\sigma = \texttt{Elim}$ be the elimination ordering induced by $a >_\sigma b >_\sigma t$ as given in Definition 3.1.8. We compute the reduced σ-Gröbner basis G of the ideal $\langle a - t, b^2 - 1, (ab)^2 - 1\rangle \subseteq K\langle a, b, t\rangle$ and obtain $G = \{tbt + b, b^2 + 1, a + t\}$. Since $G \cap K[t]$ is empty, the order of $\bar{a}$ is infinite and so is the order of D_∞. Now we consider the dihedral group $D_6 = \langle a, b \mid a^3 = b^2 = (ab)^2 = 1\rangle$. We want to check the order of $\overline{bab}$. Thus we compute the reduced σ-Gröbner basis H of the ideal $\langle bab - t, a^3 - 1, b^2 - 1, (ab)^2 - 1\rangle \subseteq K\langle a, b, t\rangle$ and obtain $H = \{t^3 + 1, t^2b + bt, tbt + b, bt^2 + tb, b^2 + 1, btb + t^2, a + t^2\}$. Since $H \cap K[t] = \{t^3 + 1\}$, the polynomial $t^3 + 1$ is the minimal polynomial of $\overline{bab}$ and hence the order of $\overline{bab}$ is 3.

Given a K-algebra homomorphism as in Proposition 6.2.7, the following proposition enables us to semi-decide whether an element is in the image of homomorphism.

Proposition 6.2.13. *In the setting of Proposition 6.2.7, we consider the ideal $H = D + I \subseteq K\langle X, Y\rangle$. Let σ be an elimination ordering on $\langle X, Y\rangle$ for X. Then for a polynomial $f \in K\langle X\rangle$, we have $\bar{f} \in \mathrm{im}(\varphi)$ if and only if we have $\mathrm{NF}_{\sigma,H}(f) \in K\langle Y\rangle$.*

Proof. Let $f \in K\langle Y\rangle$ be a polynomial such that $f + I \in \mathrm{im}(\varphi)$. Then there exists a polynomial $h \in K\langle X\rangle$ satisfying $\varphi(h + J) = h(g_1, \ldots, g_m) + I = f + I$. Clearly $g_i = y_i - (y_i - g_i)$ for all $i \in \{1, \ldots, m\}$. By replacing g_i with $y_i - (y_i - g_i)$ for all $i \in \{1, \ldots, m\}$, we have $h(g_1, \ldots, g_m) = h(y_1, \ldots, y_m) + p$ with $p \in D$. Thus we have $f - h(y_1, \ldots, y_m) \in H$, and hence $\mathrm{NF}_{\sigma,H}(f) = \mathrm{NF}_{\sigma,H}(h(y_1, \ldots, y_m))$ by Remark 3.1.18.c. Since σ is an elimination ordering on $\langle X, Y\rangle$ for X and $h(y_1, \ldots, y_m) \in K\langle Y\rangle$, we have $\mathrm{NF}_{\sigma,H}(h(y_1, \ldots, y_m)) \in K\langle Y\rangle$. Therefore we have $\mathrm{NF}_{\sigma,H}(f) \in K\langle Y\rangle$.

Conversely, let $f \in K\langle X\rangle$ be a polynomial such that $\mathrm{NF}_{\sigma,H}(f) \in K\langle Y\rangle$. By Corollary 3.1.16.b we have $f - \mathrm{NF}_{\sigma,H}(f) \in H$. By the definition of H, there exist not necessarily pairwise distinct $y_{i_1} - g_{i_1}, \ldots, y_{i_s} - g_{i_s} \in \{y_1 - g_1, \ldots, y_m - g_m\}$, and $p_1, \ldots, p'_s \in K\langle X, Y\rangle, p \in I$, such that $f - \mathrm{NF}_{\sigma,H}(f) = \sum_{k=1}^{s} p_k(y_{i_k} - g_{i_k})p'_k + p$. Now we substitute $y_i \mapsto g_i$ for all $i \in \{1, \ldots, m\}$, we have $f - \mathrm{NF}_{\sigma,H}(f)(g_1, \ldots, g_m) \in I$. Therefore $f + I = \varphi(\mathrm{NF}_{\sigma,H}(f))$ and $f + I \in \mathrm{im}(\varphi)$. □

Remark 6.2.14. We can use Proposition 6.2.13 to semi-decide the *subagebra membership problem.* Assume that $G_I \subseteq K\langle X\rangle$ is a system of generators of the ideal I. Let $f, g_1, \ldots, g_m \in K\langle X\rangle$ be polynomials, and let $S = K\langle \bar{g}_1, \ldots, \bar{g}_m\rangle \subseteq K\langle X\rangle/I$ be the subalgebra generated by $\{\bar{g}_1, \ldots, \bar{g}_m\}$. We can semi-decide whether $\bar{f} \in K\langle \bar{g}_1, \ldots, \bar{g}_m\rangle$ via the following sequence of instructions.

1) Construct the ideal $H \subseteq K\langle X, Y\rangle$ generated by the set $\{y_1 - g_1, \ldots, y_m - g_m\} \cup G_I$.

Choose an elimination ordering σ on $\langle X, Y\rangle$ for X.

2) Let $G = \{y_1 - g_1, \ldots, y_m - g_m\} \cup G_I$. Note that G is a partial σ-Gröbner basis of H (see Remark 4.1.16).

3) Compute $\mathrm{NR}_{\sigma,G}(f)$ using the Division Algorithm given in Theorem 3.2.1. If $\mathrm{NR}_{\sigma,H}(f) \in K\langle Y\rangle$, then by Proposition 6.2.13 we have $\bar{f} \in S$, and return $\bar{f} = \mathrm{NR}_{\sigma,G}(f)(\bar{g}_1, \ldots, \bar{g}_m)$ which is an explicit representation of $\bar{f}$ as an element of S.

4) Using the Buchberger Procedure given in Theorem 4.1.14, we compute a new partial σ-Gröbner basis G' of H that contains G. Let $G = G'$. Then continue with step 3).

Since the ideal H may not have a finite σ-Gröbner basis, the loop in the instructions above may not terminate. Hence the subagebra membership problem is semi-decidable.

Remark 6.2.15. In particular, we can also semi-decide the generalized word problem (see Definition 2.1.21). Let $\mathcal{M} = \langle X \mid R\rangle$ be a finitely presented monoid, and let $H \subseteq \mathcal{M}$ be the submonoid generated by the set of words $\{w_1, \ldots, w_m\} \subseteq \langle X\rangle \setminus \{1\}$. Given a word $w \in \langle X\rangle$, the generalized word problem is to decide whether $\bar{w} \in H$. We consider the residue class ring $K\langle X\rangle/I$ where $I \subseteq K\langle X\rangle$ is the ideal generated by the set $\{l - r \mid (l, r) \in R\}$. Note that we have $H = \langle \bar{w}_1, \ldots, \bar{w}_m\rangle$. Then $\bar{w} \in H$ if and only if $\bar{w} - 1 \in K\langle \bar{w}_1 - 1, \ldots, \bar{w}_m - 1\rangle \subseteq K\langle X\rangle/I$. Therefore we can semi-decide whether $\bar{w} \in H$ via the following sequence of instructions.

1) Construct the ideal $H \subseteq \langle X, Y\rangle$ generated by the set $\{y_1 - w_1 + 1, \ldots, y_m - w_m +1\} \cup \{l - r \mid (l, r) \in R\}$. Choose an elimination ordering σ on $\langle X, Y\rangle$ for X.

2) Let $G = \{y_1 - w_1 + 1, \ldots, y_m - w_m +1\} \cup \{l - r \mid (l, r) \in R\}$. Note that G is a partial σ-Gröbner basis of H (see Remark 4.1.16).

3) Compute $\mathrm{NR}_{\sigma,G}(w - 1)$ using the Division Algorithm given in Theorem 3.2.1. If $\mathrm{NR}_{\sigma,G}(w - 1) \in K\langle Y\rangle$, then by Proposition 6.2.13 we have $\bar{w} - 1 \in K\langle \bar{w}_1 - 1, \ldots, \bar{w}_m - 1\rangle$, and we conclude that $\bar{w} \in H$ and stop.

4) Using the Buchberger Procedure given in Theorem 4.1.14, we compute a new partial σ-Gröbner basis G' of H that contains G. Let $G = G'$. Then continue with step 3).

As in the previous remark, the ideal H may not have a finite σ-Gröbner basis and the loop in the instructions above may not terminate. Therefore the generalized word problem is also semi-decidable.

By Proposition 6.2.13 and the definition of the reduced Gröbner basis (see Definition 3.3.16), we give a sufficient and necessary condition for a K-algebra homomorphism to be surjective in the following corollary.

Corollary 6.2.16. *In the setting of Proposition 6.2.7, let G be the reduced σ-Gröbner basis of the ideal $H = D + I \subseteq K\langle X, Y\rangle$. Then the homomorphism φ is surjective if and only if G contains polynomials of the form $x_i - h_i$, where $h_i \in K\langle Y\rangle$ for all $i \in \{1, \ldots, n\}$.*

Proof. Analogous to [43], Proposition 3.6.6.d. □

6.2.2 Component Elimination in $(K\langle X\rangle \otimes K\langle X\rangle)^r$

In this subsection we shall study applications of Gröbner bases related to component elimination in free $K\langle X\rangle$-bimodule $F_r = (K\langle X\rangle \otimes K\langle X\rangle)^r$. In [8], H. Bluhm and M. Kreuzer developed component elimination technique in F_r and proposed methods to compute two-sided syzygies in non-commutative settings. In this subsection we shall revise their results with slight adaptations, highlight our observations and extensions in remarks, and apply their technique to the computation of colon modules. In the following, we let $L \subseteq \{1, \ldots, r\}$ be a subset, $\widehat{F}_r$ the free $K\langle X\rangle$-bimodule generated by $\{e_i \mid i \in \{1, \ldots, r\} \setminus L\}$, i.e. $\widehat{F}_r = \bigoplus_{i\in\{1,\ldots,r\}\setminus L} K\langle X\rangle e_i K\langle X\rangle$, and $\mathbb{T}(\widehat{F}_r)$ the set of terms in $\widehat{F}_r$.

Definition 6.2.17. Let $L \subseteq \{1, \ldots, r\}$ be a subset as above.

a) 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 $\mathrm{LT}_\tau(m) \in \mathbb{T}(\widehat{F}_r)$ is contained in $\widehat{F}_r$.

b) Given a $K\langle X\rangle$-submodule $M \subseteq F_r$, the $K\langle X\rangle$-submodule $M \cap \widehat{F}_r$ in $\widehat{F}_r$ is called the **component elimination module** of M with respect to L.

It is easy to verify that for any $j \in \{1, \ldots, r\}$, the module term ordering `PosTo` on $\mathbb{T}(F_r)$ defined as in Example 5.1.3.b is a component elimination ordering for $L =$

$\{1,\dots,j\}$. Component elimination ordering has the following properties that are analogous to Lemma 6.2.2 and Theorem 6.2.3. The proofs of the following lemma and theorem proceed similarly to the proofs of Lemma 6.2.2 and Theorem 6.2.3, respectively.

Lemma 6.2.18. *Let τ be a module term ordering on $\mathbb{T}(F_r)$, then the restriction $\hat{\tau}$ of τ to $\mathbb{T}(\widehat{F}_r)$ is also a module term ordering.*

Theorem 6.2.19. (Computation of Component Elimination Submodules) *Let $M \subseteq F_r$ be a $K\langle X\rangle$-submodule, let $L \subseteq \{1,\dots,r\}$ be a subset, let τ be a component elimination ordering for L, and let $\hat{\tau}$ be the restriction of τ to $\mathbb{T}(\widehat{F}_r)$. If G is a τ-Gröbner basis of M, then the set $G \cap \widehat{F}_r$ is a $\hat{\tau}$-Gröbner basis of the component elimination module $M \cap \widehat{F}_r$.*

The first application we shall introduce in this subsection is the computation of the intersection of $K\langle X\rangle$-submodules in F_r. The following proposition formulates the intersection of two submodules.

Proposition 6.2.20. *Let $G_M, G_N \subseteq F_r \setminus \{0\}$ be two sets of elements which generate $K\langle X\rangle$-submodules $M, N \subseteq F_r$, respectively. Let F_{2r} be the free $K\langle X\rangle$-bimodule with the canonical basis $\{\bar{e}_1,\dots,\bar{e}_{2r}\}$. For every element $m = \sum_{i=1}^r \sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_iw'_{ij} \in F_r$, we denote $\sum_{i=1}^r \sum_{j\in\mathbb{N}} c_{ij}w_{ij}\bar{e}_iw'_{ij} \in F_{2r}$ by $\bar{m}$ and $\sum_{i=1}^r \sum_{j\in\mathbb{N}} c_{ij}w_{ij}\bar{e}_{r+i}w'_{ij} \in F_{2r}$ by m'. Consider the submodule $V \subseteq F_{2r}$ generated by the set $\{\bar{g}+g' \mid g \in G_M\} \cup \{h' \mid h \in G_N\}$. Then we have $M \cap N = V \cap \langle \bar{e}_1,\dots,\bar{e}_r\rangle$.*

Proof. Analogous [8], Proposition 3.4. □

Remark 6.2.21. We can illustrate Proposition 6.2.20 as follows. Assume that $G_M = \{g_1,\dots,g_s\}$ and $G_N = \{h_1,\dots,h_t\}$. Consider elements g_i, h_k for all $i \in \{1,\dots,s\}, k \in \{1,\dots,t\}$ as column vectors and construct the following matrix $\mathcal{V}$ of size $2r \times (s+t)$

$$\mathcal{V} = \begin{pmatrix} g_1 & \cdots & g_s & 0 & \cdots & 0 \\ g_1 & \cdots & g_s & h_1 & \cdots & h_t \end{pmatrix}.$$

Let v be an element of the $K\langle X\rangle$-submodule generated by the column vectors of $\mathcal{V}$. We divide v into two halves: the first half of v, denoted by v^+, belongs to the $K\langle X\rangle$-submodule M; the second half of v, denoted by v^-, belongs to the $K\langle X\rangle$-submodule $M+N$. Assume that $v^- = \sum_{i=1}^s \sum_{j\in\mathbb{N}} a_{ij}w_{ij}g_iw'_{ij} + \sum_{k=1}^t \sum_{l\in\mathbb{N}} b_{kl}u_{kl}h_ku'_{kl}$ with $a_{ij} \in K, w_{ij}, w'_{ij} \in \langle X\rangle$ for all $i \in \{1,\dots,s\}, j \in \mathbb{N}$ and $b_{kl} \in K, u_{kl}, u'_{kl} \in \langle X\rangle$ for all $k \in \{1, \ldots, t\}, l \in \mathbb{N}$. Then we have $v^+ = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} a_{ij} w_{ij} g_i w'_{ij}$. Clearly $v^- = 0$ if and only if $v^+ = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} a_{ij} w_{ij} g_i w'_{ij} = -\sum_{k=1}^{t} \sum_{l \in \mathbb{N}} b_{kl} u_{kl} h_k u'_{kl} \in M \cap N$.

In what follows, for $r' > r$, by abusing the notation we shall consider an element $m \in F_r$ as an element of F_r whose components at $e_{r+1}, \ldots, e_{r'}$ are zero, and conversely, consider an element $m' \in F_{r'}$ whose components at $e_{r+1}, \ldots, e_{r'}$ are zero as an element of F_r.

Remark 6.2.22. With the notation given in Proposition 6.2.20, we compute the intersection $M \cap N$ using the following sequence of instructions.

1) Let $V \subseteq F_{2r}$ be the $K\langle X\rangle$-submodule generated by the set $\{\bar{g} + g' \mid g \in G_M\} \cup \{h' \mid h \in G_N\}$.

2) Choose a component elimination ordering τ on $\mathbb{T}(F_{2r})$ for $\{r+1, \ldots, 2r\}$. Enumerate a τ-Gröbner basis G of the $K\langle X\rangle$-submodule V.

3) By Proposition 6.2.20 and Theorem 6.2.19 the set $G \cap F_r$ is a $\hat{\tau}$-Gröbner basis of the intersection $M \cap N$.

We can easily construct the required component elimination ordering τ through a slight modification on the module term ordering PosTo (see Example 5.1.3.b) as follows. Let To be an admissible ordering on $\langle X\rangle$, and let $w_1 e_i w'_1, w_2 e_j w'_2 \in \mathbb{T}(F_{2r})$. We say $w_1 e_i w'_1 >_\tau w_2 e_j w'_2$ if we have $i > j$, or if we have $i = j$ and $w_1 w'_1 >_{\texttt{To}} w_2 w'_2$, or if we have $i = j$ and $w_1 w'_1 = w_2 w'_2$ and $w_1 >_{\texttt{To}} w_2$.

It is straightforward to generalize Proposition 6.2.20 for the computation of the intersection of more than two $K\langle X\rangle$-submodules in F_r.

Corollary 6.2.23. *Let $s \geq 2$, and let $M_k \subseteq F_r$ be the $K\langle X\rangle$-submodule generated by the set $G_k \subseteq F_r$ for $k = 1, \ldots, s$. For every element $m = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w'_{ij} \in F_r$ we denote $\sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{i+(k-1)r} w'_{ij} \in F_{sr}$ by $m^{(k)}$. Consider the $K\langle X\rangle$-submodule $V \subseteq F_{sr}$ generated by the set $\cup_{i=1}^{s-1} \{g^{(i)} + g^{(i+1)} \mid g \in G_i\} \cup \{g^{(s)} \mid g \in G_s\}$. Then we have $\cap_{k=1}^{s} M_k = V \cap \langle e_1, \ldots, e_r\rangle$.*

The most important and useful application we shall introduce next is the computation of syzygy modules of a tuple of elements in F_r which gives rise to further applications. Recall that for a tuple of non-zero elements $\mathcal{G} = (g_1, \ldots, g_s) \in F_r^s$ the syzygy module $\mathrm{Syz}(\mathcal{G})$ is the set $\{\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w'_{ij} \in F_s \mid \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} = 0\}$. The following proposition formulates the computation of syzygy modules.

Proposition 6.2.24. *Let $\mathcal{G} = (g_1, \ldots, g_s) \in F_r^s$ be a tuple of non-zero elements. For every element $m = \sum_{i=1}^{r} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e_i w'_{ij} \in F_r$, we write $m' = \sum_{i=1}^{r} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e_{i+s} w'_{ij}$ as an element of F_{r+s}. Let $U \subseteq F_{r+s}$ be the $K\langle X\rangle$-submodule generated by the set $\{e_1 + g'_1, \ldots, e_s + g'_s\}$. Then we have $\mathrm{Syz}(\mathcal{G}) = U \cap \langle e_1, \ldots, e_s\rangle$.*

Proof. Analogous [8], Proposition 3.6. □

Remark 6.2.25. We can visualize Proposition 6.2.24 as follows. Consider elements g_i for all $i \in \{1, \ldots, s\}$ as column vectors and construct the following matrix $\mathcal{U}$ of size $(s + r) \times s$

$$\mathcal{U} = \begin{pmatrix} 1\otimes 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1\otimes 1 \\ g_1 & g_2 & \cdots & g_s \end{pmatrix}.$$

Let u be an element of the $K\langle X\rangle$-submodule generated by the column vectors of $\mathcal{U}$. We divide u into two parts: the first part consists of the first s components of u, denoted by u^+, belongs to the $K\langle X\rangle$-submodule generated by $\{e_1, \ldots, e_s\}$; the second part consists of the last r components of u, denoted by u^-, belongs to the $K\langle X\rangle$-submodule generated by $\{g_1, \ldots, g_s\}$. Assume that $u^+ = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e_i w'_{ij}$ with $c_{ij} \in K, w_{ij}, w'_{ij} \in \langle X\rangle$ for all $i \in \{1, \ldots, s\}, j \in \mathbb{N}$. Then we have $u^- = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} g_i w'_{ij}$. Clearly $u^- = 0$ if and only if $u^+ \in \mathrm{Syz}(\mathcal{G})$.

Remark 6.2.26. With the notation given in Proposition 6.2.24, we compute the syzygy module $\mathrm{Syz}(\mathcal{G})$ using the following sequence of instructions.

1) Let $U \subseteq F_{s+r}$ be the $K\langle X\rangle$-submodule generated by the set $\{e_1 + g'_1, \ldots, e_s + g'_s\}$.

2) Choose a component elimination ordering τ on $\mathbb{T}(F_{s+r})$ for $\{s+1, \ldots, s+r\}$. Enumerate a τ-Gröbner basis G of the $K\langle X\rangle$-submodule U.

3) By Proposition 6.2.24 and Theorem 6.2.19 the set $G \cap F_s$ is a $\hat{\tau}$-Gröbner basis of the syzygy module $\mathrm{Syz}(\mathcal{G})$.

In [8], H. Bluhm and M. Kreuzer constructed the $K\langle X\rangle$-submodule $U = \langle g_1 - e_{r+1}, \ldots, g_s - e_{r+s}\rangle \subseteq F_{r+s}$ and showed that $\mathrm{Syz}(\mathcal{G}) \cong U \cap \langle e_{r+1}, \ldots, e_{r+s}\rangle$. For the computation of $\mathrm{Syz}(\mathcal{G})$, they chose a component elimination ordering τ for $\{1, \ldots, r\}$ on $\mathbb{T}(F_{r+s})$, computed a τ-Gröbner basis of the $K\langle X\rangle$-submodule U, let $\widehat{F}_{r+s}$ be the $K\langle X\rangle$-bimodule generated by the set $\{e_{r+1}, \ldots, e_{r+s}\}$, and defined the homomorphism $\varphi : \widehat{F}_{r+s} \to F_s$

given by $e_{r+i} \mapsto e_i$ for $i = 1, \dots, s$. Then they claimed that $\varphi(G \cap \widehat{F}_{r+s})$ is a $\hat{\tau}$-Gröbner basis of $\mathrm{Syz}(\mathcal{G})$ (see [8], Theorem 3.7). However, to make the claim correct the ordering τ should satisfy a strict condition that $\mathrm{LT}_\tau(\varphi(m)) = \varphi(\mathrm{LT}_{\hat{\tau}}(m))$ for every element $m \in \widehat{F}_{r+s} \setminus \{0\}$. Consider a generalization of the module term ordering `PosTo` (see Example 5.1.3.b) as follows. Let $\sigma_1, \dots, \sigma_{r+s}$ be pairwise distinct admissible orderings on $\langle X \rangle$. For $w_1 e_i w_1', w_2 e_j w_2' \in \mathbb{T}(F_{r+s})$ we say that $w_1 e_i w_1' > w_2 e_j w_2'$ if we have $i < j$, or if we have $i = j$ and $w_1 w_1' >_{\sigma_i} w_2 w_2'$, or if $i = j$ and $w_1 w_1' = w_2 w_2'$ and $w_1 >_{\sigma_i} w_2$. It can be verified that the ordering defined in this way is a component elimination ordering for $\{1, \dots, r\}$ on $\mathbb{T}(F_{r+s})$ but it does not satisfy the condition that $\mathrm{LT}_\tau(\varphi(m)) = \varphi(\mathrm{LT}_{\hat{\tau}}(m))$ for every element $m \in \widehat{F}_{r+s} \setminus \{0\}$. The advantage of our constructions in Proposition 6.2.24 as well as Proposition 6.2.20 is that we compute a $\hat{\tau}$-Gröbner basis of the desired submodule by component elimination directly and avoid the effect of the homomorphism φ. Meanwhile we also simplify the computation.

Recall that, for a tuple of non-zero polynomials $\mathcal{G} = (g_1, \dots, g_s) \in K\langle X \rangle^s$, the syzygy module $\mathrm{Syz}(\mathcal{G})$ is the set $\{\sum_{i=1}^s \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w_{ij}' \in F_s \mid \sum_{i=1}^s \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w_{ij}' = 0\}$. Using the same approach as Proposition 6.2.24, we can compute the syzygy module of a tuple of polynomials as follows. For $i = 1, \dots, s$, we consider polynomial $g_i \in K\langle X \rangle$ as an element $g_i e_{s+1} \in F_{s+1}$ and construct the $K\langle X \rangle$-submodule generated by the set $\{e_1 + g_1 e_{s+1}, \dots, e_s + g_s e_{s+1}\}$. To eliminate the effect of canonical basis e_{s+1}, we introduce a *set of commutators* $\{x_1 e_{s+1} - e_{s+1} x_1, \dots, x_n e_{s+1} - e_{s+1} x_n\}$ which makes e_{s+1} commute with each word in $\langle X \rangle$. Altogether we have the following corollary.

Corollary 6.2.27. *Let $\mathcal{G} = (g_1, \dots, g_s) \in K\langle X \rangle^s$ be a tuple of non-zero polynomials, and let $U \subseteq F_{s+1}$ be the $K\langle X \rangle$-submodule generated by the set $\{e_1 + g_1 e_{s+1}, \dots, e_s + g_s e_{s+1}, x_1 e_{s+1} - e_{s+1} x_1, \dots, x_n e_{s+1} - e_{s+1} x_n\}$. Then we have* $\mathrm{Syz}(\mathcal{G}) = U \cap \langle e_1, \dots, e_s \rangle$.

Proof. Analogous to [8], Proposition 3.9. □

Furthermore, we compute syzygy modules of a tuple of elements in residue class rings. Let $I \subseteq K\langle X \rangle$ be the two-sided ideal generated by the set $\{f_1, \dots, f_t\} \subseteq K\langle X \rangle$, let $K\langle X \rangle / I$ be a residue class ring, and for $s \geq 1$ let $\bar{F}_s = (K\langle X \rangle / I \otimes K\langle X \rangle / I)^s$ be the free $K\langle X \rangle / I$-bimodule of rank s with the canonical basis $\{e_1, \dots, e_s\}$. As in Section 6.1, we represent elements in $\bar{F}_s$ of the form $\sum_{i=1}^r \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w_{ij}'$ with $c_{ij} \in K, w_{ij}, w_{ij}' \in \mathcal{O}_\sigma(I)$ for all $i \in \{1, \dots, r\}, j \in \mathbb{N}$. Moreover, let $g_1, \dots, g_s \in K\langle X \rangle \setminus I$ be polynomials, and let $\bar{\mathcal{G}} = (\bar{g}_1, \dots, \bar{g}_s) \in (K\langle X \rangle / I)^s$ be the tuple where $\bar{g}_i$ is the residue class of g_i for $i = 1, \dots, s$. The syzygy module of $\bar{\mathcal{G}}$ is the set $\mathrm{Syz}(\bar{\mathcal{G}}) = \{\sum_{i=1}^s \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w_{ij}' \in$

$\bar{F}_s \mid \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_iw'_{ij} \in I\}$.

Corollary 6.2.28. *Using the notation as above, we let* $U \subseteq F_{s+1}$ *be the* $K\langle X\rangle$*-submodule generated by the set* $\{e_1+g_1e_{s+1},\ldots,e_s+g_se_{s+1},f_1e_{s+1},\ldots,f_te_{s+1},x_1e_{s+1} -e_{s+1}x_1,\ldots,x_ne_{s+1}-e_{s+1}x_n\}$. *Then we have* $\mathrm{Syz}(\bar{\mathcal{G}}) = \psi(U\cap\langle e_1,\ldots,e_s\rangle)$ *where* $\psi : F_s \to \bar{F}_s$ *is the map defined by* $m \mapsto \bar{m}$.

Proof. Analogous to [8], Proposition 4.6. □

Remark 6.2.29. Using the same notation as above, we can compute the syzygy module $\mathrm{Syz}(\bar{\mathcal{G}})$ via the following sequence of instructions.

1) Let $U \subseteq F_{s+1}$ be the $K\langle X\rangle$-submodule generated by the set $\{e_1+g_1e_{s+1},\ldots, e_s+g_se_{s+1},f_1e_{s+1},\ldots,f_te_{s+1},x_1e_{s+1}-e_{s+1}x_1,\ldots,x_ne_{s+1}-e_{s+1}x_n\}$.

2) Choose a component elimination ordering τ on $\mathbb{T}(F_{s+1})$ for $\{s+1\}$. Enumerate a τ-Gröbner basis G of the $K\langle X\rangle$-submodule U.

3) By Theorem 6.2.19 and Corollary 6.2.28 the set $G\cap F_s$ is a $\hat{\tau}$-Gröbner basis of the $K\langle X\rangle$-submodule $U\cap F_s$ and the set $\psi(G\cap F_s)$ generates the syzygy module $\mathrm{Syz}(\bar{\mathcal{G}})$.

4) Moreover, if τ is compatible with σ, then the set $\psi(G\cap F_s)$ is a $\hat{\tau}$-Gröbner basis of the syzygy module $\mathrm{Syz}(\bar{\mathcal{G}})$.

We show the correctness of step 4). Let $\bar{m} = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_iw'_{ij} \in \mathrm{Syz}(\bar{\mathcal{G}})$ with $c_{ij}\in K$ and $w_{ij},w'_{ij}\in\mathcal{O}_\sigma(I)$ for all $i\in\{1,\ldots,s\}$ and for all $j\in\mathbb{N}$ where all but finitely many of the c_{ij} are zero. We can prove that $\bar{m}\in U\cap F_s$ in the same way as the proof of [8], Proposition 4.6. Let $\mathrm{LT}_{\hat{\tau}}(\bar{m}) \equiv w_1e_iw'_1$. Since $G\cap F_s$ is a $\hat{\tau}$-Gröbner basis of $U\cap F_s$, there exist $w,w'\in\langle X\rangle, g\in G\cap F_s$ such that $\mathrm{LT}_{\hat{\tau}}(\bar{m}) \equiv w\cdot\mathrm{LT}_{\hat{\tau}}(g)\cdot w'$. Since $w_1,w'_1\in\mathcal{O}_\sigma(I)$ and τ is compatible with σ, we have $\mathrm{LT}_{\hat{\tau}}(g)\equiv\mathrm{LT}_{\hat{\tau}}(\bar{g})$. Therefore we have $\mathrm{LT}_{\hat{\tau}}(\bar{m}) \equiv w\cdot\mathrm{LT}_{\hat{\tau}}(\bar{g})\cdot w'$ and hence $\psi(G\cap F_s)$ is a $\hat{\tau}$-Gröbner basis of $\mathrm{Syz}(\bar{\mathcal{G}})$.

Remark 6.2.30. M. Kreuzer [45] proposed that we can attack the *decomposition search problem* and the *factorization search problem* by using syzygy computations. We explicitly present steps to attack these problems.

a) Let $G=\langle X \mid R\rangle$ be a finitely presented group, let $v,w\in G$ be two elements, and let $A,B\subseteq G$ be two submonoids such that there exist $a\in A, b\in B$ satisfying $avb=w$. The *decomposition search problem* is to find $a\in A$ and $b\in B$ such that $avb = w$. Assume that $R = \{(w_1, w_1'), \dots, (w_t, w_t')\}$. Consider the residue class ring $K\langle X\rangle/I$ where $I \subseteq K\langle X\rangle$ is the two-sided ideal generated by the set $\{w_1 - w_1', \dots, w_t - w_t'\}$. Using the following sequence of instructions, we compute $\mathrm{Syz}(v, -w) \subseteq K\langle G\rangle e_1 K\langle G\rangle \oplus K\langle G\rangle e_2 K\langle G\rangle$ and find in it the unique element of the form $ae_1b + e_2$ with $a \in A$ and $b \in B$ satisfying $avb = w$.

1) Let $U \subseteq F_3$ be the $K\langle X\rangle$-submodule generated by the set $\{e_1 + ve_3, e_2 - we_3, (w_1 - w_1')e_3, \dots, (w_t - w_t')e_3, x_1e_3 - e_3x_1, \dots, x_ne_3 - e_3x_n\}$.

2) Choose the following module term ordering τ on $\mathbb{T}(F_3)$. For $w_1e_iw_1', w_2e_jw_2' \in \mathbb{T}(F_3)$, we say $w_1e_iw_1' >_\tau w_2e_jw_2'$ if we have $i > j$, or if we have $i = j$ and $w_1w_1' >_\sigma w_2w_2'$, or if we have $i = j$ and $w_1w_1' = w_2w_2'$ and $w_1 >_\sigma w_2$. Compute the reduced τ-Gröbner basis G of the $K\langle X\rangle$-submodule U.

3) In G there exists a unique element of the form $ae_1b + e_2$ where $a, b \in \langle X\rangle$. Then $a \in A$ and $b \in B$ represent the desired elements.

We prove the correctness of step 3). By assumption there exist $a, b \in \langle X\rangle$ representing elements in A, B respectively such that $avb = w$. Thus ae_1b+e_2 represents an element in $Syz_{K\langle G\rangle}(v, -w)$ and is contained in U by Corollary 6.2.29. By the definition of τ the leading term of $ae_1b + e_2$ is e_2 and G contains an element whose leading term is e_2. Observe that U is generated by a system of generators consisting of only binomials. Thus G also consists of only binomials. In particular, G contains an element of the form $ae_1b + e_2$ with $a, b \in \langle X\rangle$. Since it is the reduced τ-Gröbner basis, G contains a unique elements of the form ae_1b+e_2 with $a, b \in \langle X\rangle$. The fact that $a \in A, b \in B$ follows from the uniqueness. Note that in step 2) the Gröbner basis computation is an enumerating procedure. After a new Gröbner basis element has been added, we fully interreduce the Gröbner basis and check whether it contains the element of the form as in step 3). Since by assumption the elements $a \in A, b \in B$ exist, they will be found eventually.

b) Let $G = \langle X \mid R\rangle$ be a finitely presented group, let $w \in G$ be a group element, and let $A, B \subseteq G$ be two submonoids such that there exist $a \in A, b \in B$ satisfying $ab = w$. The *factorization search problem* is to find elements $a \in A$ and $b \in B$ such that $ab = w$. We solve it by computing $\mathrm{Syz}(1, -w) \subseteq K\langle G\rangle e_1 K\langle G\rangle \oplus K\langle G\rangle e_2 K\langle G\rangle$ and finding in it the unique element of the form $ae_1b + e_2$ with $a \in A$ and $b \in B$ satisfying $ab = w$. Clearly, this is just a specific case of the *decomposition search problem.*

By combining the results of Proposition 6.2.20 and Corollary 6.2.28, we compute the intersection of two syzygy modules over the residue class ring $K\langle X\rangle/I$ as follows.

Corollary 6.2.31. *Let $g_1,\dots,g_s,h_1,\dots,h_s \in K\langle X\rangle \setminus I$ be polynomials, and let $\bar{\mathcal{G}} = (\bar{g}_1,\dots,\bar{g}_s), \bar{\mathcal{H}} = (\bar{h}_1,\dots,\bar{h}_s) \in (K\langle X\rangle/I)^s$ be two tuples where $\bar{g}_i$ is the residue class of g_i and $\bar{h}_i$ is the residue class of h_i for $i = 1,\dots,s$. Furthermore, let $U \subseteq F_{2s+2}$ be the $K\langle X\rangle$-submodule generated by the set $\{e_1+e_{s+1}+g_1e_{2s+1},\dots,e_s+e_{2s}+g_se_{2s+1}, f_1e_{2s+1}, \dots, f_te_{2s+1}, x_1e_{2s+1} - e_{2s+1}x_1,\dots,x_ne_{2s+1} - e_{2s+1}x_n, e_{s+1} + h_1e_{2s+2},\dots,e_{2s} + h_se_{2s+2}, f_1e_{2s+2},\dots,f_te_{2s+2}, x_1e_{2s+2} - e_{2s+2}x_1,\dots,x_ne_{2s+2} - e_{2s+2}x_n\}$. Then we have $\mathrm{Syz}(\bar{\mathcal{G}}) \cap \mathrm{Syz}(\bar{\mathcal{H}}) = \psi(U \cap \langle e_1,\dots,e_s\rangle)$ where $\psi : F_s \to \bar{F}_s$ is the map defined by $m \mapsto \bar{m}$.*

Proof. Let $\bar{m} = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}\bar{w}_{ij}e_i\bar{w}'_{ij} \in \mathrm{Syz}(\bar{\mathcal{G}}) \cap \mathrm{Syz}(\bar{\mathcal{H}})$ with $c_{ij} \in K$ and $\bar{w}_{ij}, \bar{w}'_{ij} \in \mathcal{O}_\sigma(I)$ for all $i \in \{1,\dots,s\}$ and for all $j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. Let $m = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_iw'_{ij}$. Clearly we have $\psi(m) = \bar{m}$ and $m \in \langle e_1,\dots,e_s\rangle$. We want to prove that $m \in U$. We write m as $m = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_i + e_{s+i} + g_ie_{2s+1})w'_{ij} - \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_{s+i} + g_ie_{2s+1})w'_{ij}$ where the first summand is contained in U. Thus to prove $m \in U$ it suffices to prove that $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_{s+i} + g_ie_{2s+1})w'_{ij} \in U$. Since we have $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_{s+i} + h_ie_{2s+2})w'_{ij} \in U$, it suffices to show that $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_{s+i} + g_ie_{2s+1})w'_{ij} - \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_{s+i} + h_ie_{2s+2})w'_{ij} = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_ie_{2s+1}w'_{ij} - \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}h_ie_{2s+2}w'_{ij} \in U$. In the following we show that both $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_ie_{2s+1}w'_{ij}$ and $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}h_ie_{2s+2}w'_{ij}$ are contained in U. Since $\bar{m} \in \mathrm{Syz}(\bar{\mathcal{G}})$ and $I = \langle f_1,\dots,f_t\rangle$, we have $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_iw'_{ij} = \sum_{k=1}^t \sum_{l\in\mathbb{N}} a_{kl}u_{kl}f_ku'_{kl}$ with $a_{kl} \in K$ and $u_{kl}, u'_{kl} \in \langle X\rangle$ for all $k \in \{1,\dots,t\}$ and for all $l \in \mathbb{N}$ where all but finitely many of the a_{kl} are zero. Thus $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_iw'_{ij}e_{2s+1} - \sum_{k=1}^t \sum_{l\in\mathbb{N}} a_{kl}u_{kl}f_ku'_{kl}e_{2s+1} = 0 \in U$. Note that the set $\{x_1e_{2s+1} - e_{2s+1}x_1,\dots,x_ne_{2s+1} -e_{2s+1}x_n\} \subseteq U$ makes e_{2s+1} commutative with every word in $\langle X\rangle$. Therefore we have $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_ie_{2s+1}w'_{ij} - \sum_{k=1}^t \sum_{l\in\mathbb{N}} a_{kl}u_{kl}f_ke_{2s+1}u'_{kl} \in U$. Since the second summand is contained in U, so is $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_ie_{2s+1}w'_{ij}$. Similarly we can prove that $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}h_ie_{2s+2}w'_{ij} \in U$.

Conversely, let $m = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_iw'_{ij} \in U \cap \langle e_1,\dots,e_s\rangle$ with $c_{ij} \in K$ and $w_{ij}, w'_{ij} \in \langle X\rangle$ for all $i \in \{1,\dots,s\}$ and for all $j \in \mathbb{N}$ where all but finitely many of the c_{ij} are zero. Since $\{e_1+e_{s+1}+g_1e_{2s+1},\dots,e_s+e_{2s}+g_se_{2s+1}, e_{s+1}+h_1e_{2s+2},\dots,e_{2s}+h_se_{2s+2}\} \subseteq U$, we have $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_i+e_{s+i}+g_ie_{2s+1})w'_{ij} - \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_{s+i}+h_ie_{2s+2})w'_{ij} - m = \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_ie_{2s+1}w'_{ij} - \sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}h_ie_{2s+2}w'_{ij} \in U$. Observe that none of the generators $e_1,\dots,$ e_{2s} appears in the sum. Therefore we must have $\sum_{i=1}^s \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_ie_{2s+1}w'_{ij} \in \langle f_1e_{2s+1},\dots,f_te_{2s+1}, x_1e_{2s+1}-e_{2s+1}x_1,\dots,x_ne_{2s+1}-$

$e_{2s+1}x_n\rangle$ and $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}h_ie_{2s+2}w'_{ij} \in \langle f_1e_{2s+2},\dots,f_te_{2s+2}, x_1e_{2s+2}-e_{2s+2}x_1,\dots, x_ne_{2s+2}-e_{2s+2}x_n\rangle$. Using the result of [8], Proposition 2.12 we have $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_iw'_{ij}$, $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}h_iw'_{ij} \in \langle f_1,\dots,f_t\rangle$. Hence we have $\psi(m) = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}\bar{w}_{ij}e_i\bar{w}'_{ij} \in \mathrm{Syz}(\bar{\mathcal{G}})\cap\mathrm{Syz}(\bar{\mathcal{H}})$. □

Remark 6.2.32. With the notation given in Corollary 6.2.31, we can compute the intersection $\mathrm{Syz}(\bar{\mathcal{G}})\cap\mathrm{Syz}(\bar{\mathcal{H}})$ of two syzygy modules using the following sequence of instructions.

1) Let $U \subseteq F_{2s+2}$ be the $K\langle X\rangle$-submodule generated by the set $\{e_1+e_{s+1}+g_1e_{2s+1},\dots,e_s+e_{2s}+g_se_{2s+1}, f_1e_{2s+1},\dots,f_te_{2s+1}, x_1e_{2s+1}-e_{2s+1}x_1,\dots,x_ne_{2s+1}-e_{2s+1}x_n, e_{s+1}+h_1e_{2s+2},\dots,e_{2s}+h_se_{2s+2}, f_1e_{2s+2},\dots,f_te_{2s+2}, x_1e_{2s+2}-e_{2s+2}x_1,\dots, x_ne_{2s+2}-e_{2s+2}x_n\}$.

2) Choose a component elimination ordering τ on $\mathbb{T}(F_{2s+2})$ for $\{s+1,\dots,2s+2\}$. Enumerate a τ-Gröbner basis G of the $K\langle X\rangle$-submodule U. By Theorem 6.2.19 the set $G\cap F_s$ is a $\hat{\tau}$-Gröbner basis of the $K\langle X\rangle$-submodule $U\cap F_s$.

3) By Corollary 6.2.31 and by using the similar method as in Remark 6.2.29 we can show that the set $\psi(G\cap F_s)$ is a $\hat{\tau}$-Gröbner basis of the intersection $\mathrm{Syz}(\bar{\mathcal{G}})\cap\mathrm{Syz}(\bar{\mathcal{H}})$ if τ is compatible with σ.

Remark 6.2.33. One outstanding application of Corollary 6.2.31 is *Bluhm-Kreuzer's Conjugator Search Algorithm* (see [8, 45]). Let $G=\langle X \mid R\rangle$ be a finitely presented group, and let $w, w' \in G$ be two conjugated elements. The *conjugacy search problem* is to find an element $a\in G$ such that $aw = w'a$. H. Bluhm and M. Kreuzer [8, 45] converted the problem to the computation of $\mathrm{Syz}(w,w')\cap\mathrm{Syz}(1,-1)\subseteq K\langle G\rangle e_1 K\langle G\rangle \oplus K\langle G\rangle e_2 K\langle G\rangle$. There is a unique element of the form $ae_1 - e_2a$ with $a\in G$. Then the element a represents the desired conjugator.

To end this subsection we shall present the computation of colon modules by using syzygy computations.

Definition 6.2.34. Let R be a ring, let U be an R-bimodule, and let $M, N \subseteq U$ be two R-submodules. The set

$$N :_{R\otimes R} M = \{\sum_{i\in\mathbb{N}} r_i\otimes r'_i \in R\otimes R \mid \sum_{i\in\mathbb{N}} r_i\cdot M\cdot r'_i \subseteq N\}$$

is a two-sided R-submodule in $R\otimes R$. It is called the **colon module** of N by M.

In the following we let $R = K\langle X\rangle$ be the free monoid ring and $U = F_r$ be the free $K\langle X\rangle$-bimodule of rank r.

Corollary 6.2.35. *Let $M = \langle g\rangle$ and $N = \langle h_1, \dots, h_t\rangle$ be two $K\langle X\rangle$-submodules in F_r, and let $\{v_1, \dots, v_s\} \subseteq F_{t+1}$ be a system of generators of $\mathrm{Syz}(g, h_1, \dots, h_t)$. For every $k \in \{1, \dots, s\}$, we write v_k as $v_k = \sum_{i=1}^{t+1} \sum_{j\in\mathbb{N}} c_{kij} w_{kij} e_i w'_{kij}$ with $c_{kij} \in K, w_{kij}, w'_{kij} \in \langle X\rangle$ where all but finitely many of the c_{kij} are zero. Then we have*

$$N :_{F_1} M = \langle \sum_{j\in\mathbb{N}} c_{11j} w_{11j} e_1 w'_{11j}, \dots, \sum_{j\in\mathbb{N}} c_{s1j} w_{s1j} e_1 w'_{s1j}\rangle.$$

Proof. Let $\sum_{l\in\mathbb{N}} a_l w_l e_1 w'_l \in N :_{F_1} M$. Then we have $\sum_{l\in\mathbb{N}} a_l w_l g w'_l \in N$. Since N is generated by the set $\{h_1, \dots, h_t\}$, there exist $b_{ij} \in K, w_{ij}, w'_{ij} \in \langle X\rangle$ for all $i \in \{1, \dots, t\}, j \in \mathbb{N}$ such that $\sum_{l\in\mathbb{N}} a_l w_l g w'_l = \sum_{i=1}^{t} \sum_{j\in\mathbb{N}} b_{ij} w_{ij} h_i w'_{ij}$. Thus $\sum_{k\in\mathbb{N}} a_k w_k e_1 w'_k - \sum_{i=1}^{t} \sum_{j\in\mathbb{N}} b_{ij} w_{ij} e_{i+1} w_{ij} \in \mathrm{Syz}(g, h_1, \dots, h_t)$. Since $\{v_1, \dots, v_s\}$ is a system of generators of $\mathrm{Syz}(g, h_1, \dots, h_t)$, there exist $d_{kj} \in K, u_{kj}, u'_{kj} \in \langle X\rangle$ for $k \in \{1, \dots, s\}, j \in \mathbb{N}$ such that $\sum_{l\in\mathbb{N}} a_l w_l e_1 w'_l - \sum_{i=1}^{t} \sum_{j\in\mathbb{N}} b_{ij} w_{ij} e_{i+1} w_{ij} = \sum_{k=1}^{s} \sum_{j\in\mathbb{N}} d_{kj} u_{kj} v_k u'_{kj}$. By substituting $v_k = \sum_{i=1}^{t+1} \sum_{j\in\mathbb{N}} c_{kij} w_{kij} e_i w'_{kij}$ and comparing the first component of the equation, we obtain $\sum_{l\in\mathbb{N}} a_l w_l e_1 w'_l = \sum_{k=1}^{s} \sum_{j\in\mathbb{N}} d_{kj} u_{kj} (\sum_{j\in\mathbb{N}} c_{k1j} w_{k1j} e_1 w'_{k1j}) u'_{kj}$. Therefore we have $\sum_{l\in\mathbb{N}} a_l w_l e_1 w'_l \in \langle \sum_{j\in\mathbb{N}} c_{11j} w_{11j} e_1 w'_{11j}, \dots, \sum_{j\in\mathbb{N}} c_{s1j} w_{s1j} e_1 w'_{s1j}\rangle$.

Conversely, to prove $\langle \sum_{j\in\mathbb{N}} c_{11j} w_{11j} e_1 w'_{11j}, \dots, \sum_{j\in\mathbb{N}} c_{s1j} w_{s1j} e_1 w'_{s1j}\rangle \subseteq N :_{F_1} M$ it is sufficient to show that $\sum_{j\in\mathbb{N}} c_{k1j} w_{k1j} e_1 w'_{k1j} \in N :_{F_1} M$ for all $k \in \{1, \dots, s\}$. Since $v_k \in \mathrm{Syz}(g, h_1, \dots, h_t)$, we have $\sum_{j\in\mathbb{N}} c_{k1j} w_{kij} g w'_{k1j} + \sum_{i=2}^{t+1} \sum_{j\in\mathbb{N}} c_{kij} w_{kij} h_{i-1} w'_{kij} = 0$. Therefore we have $\sum_{j\in\mathbb{N}} c_{k1j} w_{kij} g w'_{k1j} = -\sum_{i=2}^{t+1} \sum_{j\in\mathbb{N}} c_{kij} w_{kij} h_{i-1} w'_{kij} \in N$, and hence $\sum_{j\in\mathbb{N}} c_{k1j} w_{k1j} e_1 w'_{k1j} \in N :_{F_1} M$. □

Remark 6.2.36. Using the notion given in Corollary 6.2.35, we define the homomorphism $\pi : F_{t+1} \to F_1$ given by $\sum_{i=1}^{t+1} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e_i w'_{ij} \mapsto \sum_{j\in\mathbb{N}} c_{1j} w_{1j} e_1 w'_{1j}$. Then we compute the colon module $N :_{F_1} M$ by the following sequence of instructions.

1) Compute a system of generators G of $\mathrm{Syz}(g, h_1, \dots, h_t)$ using the instructions as in Remark 6.2.26.

2) Then the set $\{\pi(g) \mid g \in G\}$ is a system of generators $N :_{F_1} M$.

Using Corollary 6.2.35, we compute colon modules in general situation as follows.

Corollary 6.2.37. *Let $M = \langle g_1, \dots, g_s\rangle$ and $N = \langle h_1, \dots, h_t\rangle$ be two $K\langle X\rangle$-submodules in F_r. Then we have*

$$N :_{F_1} M = \cap_{i=1}^{s} (N :_{F_1} \langle g_i\rangle).$$

To put it another way, we consider elements g_i, h_j for all $i \in \{1, \ldots, s\}, j \in \{1, \ldots, t\}$ as column vectors, and let $\mathcal{H} = (h_1, \ldots, h_t) \in F_r^t$ be a tuple. Construct the following block matrix of size $sr \times (st+1)$

$$\mathcal{M} = \begin{pmatrix} g_1 & \mathcal{H} & 0 & \cdots & 0 \\ g_2 & 0 & \mathcal{H} & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ g_s & 0 & \cdots & 0 & \mathcal{H} \end{pmatrix}.$$

Let $\{v_1, \ldots, v_\mu\} \subseteq F_{st+1}$ be a system of generators of $\mathrm{Syz}(\mathcal{M})$*. For $k = 1, \ldots, \mu$, we write v_k as $v_k = \sum_{i=1}^{st+1} \sum_{j \in \mathbb{N}} c_{kij} w_{kij} e_i w'_{kij}$ with $c_{kij} \in K, w_{kij}, w'_{kij} \in \langle X \rangle$ where all but finitely many of the c_{kij} are zero. Then we have*

$$N :_{F_1} M = \langle \sum_{j \in \mathbb{N}} c_{11j} w_{11j} e_1 w'_{11j}, \ldots, \sum_{j \in \mathbb{N}} c_{\mu 1j} w_{\mu 1j} e_1 w'_{\mu 1j} \rangle.$$

Proof. Analogous to [43], Proposition 3.2.15. □

Remark 6.2.38. Recall that every ideal of a ring R is a two-sided R-submodule. Let I and J be two ideals of R. The set

$$I :_{R \otimes R} J = \{ \sum_{i \in \mathbb{N}} r_i \otimes r'_i \in R \otimes R \mid \sum_{i \in \mathbb{N}} r_i \cdot J \cdot r'_i \subseteq I \}$$

is a two-sided R-submodule in $R \otimes R$. It is called the **colon module** of I by J. In particular, if $R = K\langle X \rangle$ is the free monoid ring and $I, J \subseteq K\langle X \rangle$ are finitely generated ideals, then we can compute the colon module $I :_{R \otimes R} J$ by adapting Corollaries 6.2.35 and 6.2.37 and by combining the results of Corollary 6.2.27 and Proposition 6.2.20.

6.3 The K-Dimension of $K\langle X \rangle / I$

Let $I \subseteq K\langle X \rangle$ be a finitely generated ideal. The residue class ring $K\langle X \rangle / I$ is a finitely generated K-algebra. Considering $K\langle X \rangle / I$ as a K-vector space, we wish to study the K-dimension of the K-algebra $K\langle X \rangle / I$. It is natural to ask the following motivating questions.

(i) Is the K-dimension $\dim_K(K\langle X \rangle / I)$ of $K\langle X \rangle / I$ finite?

(ii) How can one compute $\dim_K(K\langle X \rangle / I)$ if it is finite?

(iii) What is the growth of $\dim_K(K\langle X\rangle/I)$ if it is infinite?

In this section we intend to answer these questions with the aid of Gröbner bases and the *Ufnarovski graph* which is named after V. Ufnarovski [69].

Remark 6.3.1. The last question is related to the *Gelfand-Kirillov dimension* which measures the rate of the growth of finitely generated K-algebras. Let A be a finitely generated K-algebra. Choose a finite dimensional K-subspace $V \subseteq A$ which generates A as a K-algebra. Then A has a standard finite dimensional filtration $\{A_i \mid i \in \mathbb{N}\}$ where $A_0 = V^0 = K$ and $A_i = \sum_{j=0}^{i} V^j$ for all $i \geq 1$. The **Gelfand-Kirillov dimension** of K-algebra A is

$$\mathrm{GKdim}(A) = \overline{\lim}_{i\to\infty} \log_i \dim_K(A_i).$$

The Gelfand-Kirillov dimension of K-algebra A is an invariant in the sense that, given any finite dimensional K-subspace $V \subseteq A$ generating A as a K-algebra, the number $\mathrm{GKdim}(A)$ is unchanged. It is clear that $\dim_K(A) < \infty$ if and only if $\mathrm{GKdim}(A) = 0$. It can be shown that $\dim_K(A) = \infty$ if and only if $\mathrm{GKdim}(A) \geq 1$ (see [42], Proposition 1.4). Moreover, G. Bergman [6] showed that there is no algebra A with $1 < \mathrm{GKdim}(A) < 2$. W. Borho and H. Kraft [7] proved that for every real number $r \geq 2$ there exists an algebra A with $\mathrm{GKdim}(A) = r$. R.B. Warfield [73] gave a construction of an algebra A with $\mathrm{GKdim}(A) \geq 2$. We refer to [42, 56] for more details about the Gelfand-Kirillov dimension.

Recall that the free monoid ring $K\langle X\rangle$ is $\mathbb{N}$-graded. We introduce a filtration of the K-algebra $K\langle X\rangle/I$ as follows. For $i \in \mathbb{N}$, let $\mathcal{F}_i \subseteq K\langle X\rangle$ be the K-vector subspace generated by the words of length less than or equal to i, i.e. let $\mathcal{F}_i = \oplus_{d=0}^{i} K\langle X\rangle_i$. It is easy to check that $K\langle X\rangle = \cup_{i\in\mathbb{N}}\mathcal{F}_i$ and $\mathcal{F}_i \cdot \mathcal{F}_j \subseteq \mathcal{F}_{i+j}$ for all $i, j \in \mathbb{N}$. Thus the set $\{\mathcal{F}_i \mid i \in \mathbb{N}\}$ is a filtration of $K\langle X\rangle$. Furthermore, it induces a filtration $\{\mathcal{F}_i/(\mathcal{F}_i \cap I) \mid i \in \mathbb{N}\}$ of $K\langle X\rangle/I$. Clearly we have $\dim_K(\mathcal{F}_i/(\mathcal{F}_i \cap I)) < \infty$ for all $i \in \mathbb{N}$. In the literature, the set $\{\mathcal{F}_i/(\mathcal{F}_i \cap I) \mid i \in \mathbb{N}\}$ is called **$\mathbb{N}$-grading filtration** of $K\langle X\rangle/I$. We refer to [48] for more information on grading filtrations.

Definition 6.3.2. Let $\{\mathcal{F}_i/(\mathcal{F}_i \cap I) \mid i \in \mathbb{N}\}$ be $\mathbb{N}$-grading filtration of $K\langle X\rangle/I$.

a) The function $\mathrm{HF}^a_{K\langle X\rangle/I} : \mathbb{N} \to \mathbb{N}$ given by

$$\mathrm{HF}^a_{K\langle X\rangle/I}(i) = \dim_K(\mathcal{F}_i/(\mathcal{F}_i \cap I))$$

is called the **affine Hilbert function** of $K\langle X\rangle/I$. For the sake of convenience we define $\mathrm{HF}^a_{K\langle X\rangle/I}(i) = 0$ for all $i < 0$.

b) The function $\mathrm{HF}_{K\langle X\rangle/I} : \mathbb{N} \to \mathbb{N}$ given by

$$\mathrm{HF}_{K\langle X\rangle/I}(i) = \mathrm{HF}^a_{K\langle X\rangle/I}(i) - \mathrm{HF}^a_{K\langle X\rangle/I}(i-1)$$

is called the **Hilbert function** of $K\langle X\rangle/I$.

c) Moreover, let z be a new indeterminate. The power series

$$\mathrm{HS}_{K\langle X\rangle/I}(z) = \sum_{i\geq 0} \mathrm{HF}_{K\langle X\rangle/I}(i) z^i$$

is called the **Hilbert series** of $K\langle X\rangle/I$.

By definition, we have $\dim_K(K\langle X\rangle/I) = \lim_{i\to\infty} \mathrm{HF}^a_{K\langle X\rangle/I}(i) = \mathrm{HS}_{K\langle X\rangle/I}(1)$ and $\mathrm{GKdim}(K\langle X\rangle/I) = \overline{\lim}_{i\to\infty} \log_i \dim_K(\mathrm{HF}^a_{K\langle X\rangle/I}(i))$. In the following, for simplicity of notation, we will sometimes drop the index $K\langle X\rangle/I$ and write $\mathrm{HF}^a(i)$, $\mathrm{HF}(i)$ and $\mathrm{HS}(z)$ instead of $\mathrm{HF}^a_{K\langle X\rangle/I}(i)$, $\mathrm{HF}_{K\langle X\rangle/I}(i)$ and $\mathrm{HS}_{K\langle X\rangle/I}(z)$, respectively, if no confusion is likely to arise.

Remark 6.3.3. The Hilbert series $\mathrm{HS}_{K\langle X\rangle/I}(z)$ is actually a generating function that encodes the information on the values of the Hilbert function $\mathrm{HF}_{K\langle X\rangle/I}(i)$ for all $i \geq 0$. In the literature of combinatorial theory, generating functions are introduced to solve the general linear recurrence problem. Indeed, at the end of this section we will encounter the recurrence relation of the Hilbert function $\mathrm{HF}_{K\langle X\rangle/I}(i)$. Therefore we have a chance to investigate the dimensions of $K\langle X\rangle/I$ using techniques from combinatorial theory.

Observe that $\mathrm{HF}^a_{K\langle X\rangle/I}(i)$ is a monotonically increasing function. We use the notions from sophisticated complexity theory (see [61]) to classify monotonically increasing functions.

Definition 6.3.4. Let Φ be the set of all eventually monotonically increasing functions $f : \mathbb{N} \to \mathbb{R}^+$, i.e. for $f \in \Phi$ there exists an integer $n_f \in \mathbb{N}$ such that $f(n+1) \geq f(n)$ for all $n \geq n_f$. We define the relations on Φ as follows.

a) For all $f, g \in \Phi$, we say $f \preceq g$ if and only if there exist a number $c > 0$ and $k \in \mathbb{N} \setminus \{0\}$ such that $f(n) \leq cg(kn)$ for almost all $n \in \mathbb{N}$. Moreover, we say f and g are equivalent and denote it by $f \sim g$ if and only if $f \preceq g$ and $g \preceq f$.

b) For $f \in \Phi$ the equivalence class $G(f) \in \Phi/\sim$ is called the **growth** of f. The partial ordering on the set $\Phi/\sim$ induced by $\preceq$ is denoted by $\leq$.

If a function is in $G(1)$ we call it **constant**. If a function is in $G(\log(n))$, we call it **logarithmic**. If a function is in $G(n^\gamma)$ with $\gamma \geq 1$, we call it **polynomial**. In particular, it is called **linear** if $\gamma = 1$ and it is called **quadratic** if $\gamma = 2$. If a function is in $G(2^n)$, we call it **exponential**. The following lemma is essential to prove the invariance of Gelfand-Kirillov dimension (see [42], Chapter 2).

Lemma 6.3.5. *Let $f, g \in \Phi$. Then $G(f) = G(g)$ if and only if $\overline{\lim}_{n\to\infty} \log_n f(n) = \overline{\lim}_{n\to\infty} \log_n g(n)$.*

Proof. See [42], Lemma 2.1. □

Due to Lemma 6.3.5, we define the **growth** of the K-algebra $K\langle X\rangle/I$ to be the growth of the affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/I}(i)$, which is also referred by the *growth* of $\dim_K(K\langle X\rangle/I)$.

Example 6.3.6. Consider the free monoid ring $K\langle X\rangle$ as a K-algebra. Since $\mathrm{HF}_{K\langle X\rangle}(i) = n^i$, we have $\mathrm{HF}^a_{K\langle X\rangle}(i) = \frac{1-n^{i+1}}{1-n}$. It is easy to check that $G(\mathrm{HF}^a_{K\langle X\rangle}(i)) = G(2^i)$. Thus the growth of $K\langle X\rangle$ is exponential. Moreover, we have $\mathrm{GKdim}(K\langle X\rangle) = \infty$.

In the following we let $I \subseteq K\langle X\rangle$ be a non-zero ideal. In the rest of this section, we shall investigate the K-dimension of $K\langle X\rangle/I$ by using Gröbner bases. Recall that Macaulay's Basis Theorem (see Theorem 3.1.15) states that the residue classes of the words in the order ideal $\mathcal{O}_\sigma(I)$ form a basis of the K-vector space $K\langle X\rangle/I$. Thus we have $\dim_K(K\langle X\rangle/I) = |\mathcal{O}_\sigma(I)|$. Moreover, given a Gröbner basis G of the ideal I, we can rephrase Macaulay's Basis Theorem as follows.

Lemma 6.3.7. *Let $I \subseteq K\langle X\rangle\backslash\{0\}$ be an ideal, let σ be an admissible ordering on $\langle X\rangle$, let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a σ-Gröbner basis of I, and let $B \subseteq \langle X\rangle$ be the set of all words which are not a multiple of any word in the set $\mathrm{LT}_\sigma\{G\}$. Then the residue classes of the words in B form a K-basis $K\langle X\rangle/I$.*

Proof. This follows directly from Theorem 3.1.15 and Definition 3.3.1. □

The following proposition gives a connection between $\dim_K(K\langle X\rangle/I)$ and minimal Gröbner bases of the ideal I.

Proposition 6.3.8. *Let $I \subseteq K\langle X\rangle\backslash\{0\}$ be an ideal, let $G \subseteq K\langle X\rangle\setminus\{0\}$ be a minimal σ-Gröbner basis of I*

a) If G is infinite, then so is $\dim_K(K\langle X\rangle/I)$.

b) If $\dim_K(K\langle X\rangle/I)$ *is finite, then so is* G.

Proof. We prove claim a). To prove claim a), let $B \subseteq \langle X\rangle$ be the set of all words which are not multiples of any word in the set $\mathrm{LT}_\sigma\{G\}$. By Lemma 6.3.7 we have $\dim_K(K\langle X\rangle/I) = |B|$. Since G is a minimal σ-Gröbner basis of I, for all $g \in G$ every subword of $\mathrm{LT}_\sigma(g)$ is contained in B. Then claim a) follows from assumption. Claim b) is the contraposition of claim a). □

The converse of Proposition 6.3.8.b is not true, i.e. $\dim_K(K\langle X\rangle/I)$ need not be finite even if the ideal I has a finite Gröbner basis.

Example 6.3.9. Consider the free monoid ring $\mathbb{Q}\langle x,y\rangle$ and the ideal $I = \langle x^2, y^2\rangle$. By Corollary 3.3.5 the set $\{x^2, y^2\}$ is a σ-Gröbner basis of I for any admissible ordering σ on $\langle X\rangle$. Observe that $\mathcal{O}_\sigma(I) = \{xy,\ yx,\ y(xy)^n,\ x(yx)^n \mid n \in \mathbb{N}\}$ has infinitely many elements. Therefore we have $\dim_{\mathbb{Q}}(\mathbb{Q}\langle x,y\rangle/I) = \infty$.

The example implies that many useful finiteness criteria in the commutative case (see for instance [43], Proposition 3.7.1) are infeasible in the non-commutative case. However, given a Gröbner basis G of I with respect to a length compatible admissible ordering, we can effectively compute the values of the affine Hilbert function of $K\langle X\rangle/I$ and explore information on $\dim_K(K\langle X\rangle/I)$. The following proposition proves very helpful for computing the values of the affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/I}(i)$.

Proposition 6.3.10. *Let* $I \subseteq K\langle X\rangle \setminus \{0\}$ *be an ideal, let* σ *be a length compatible admissible ordering on* $\langle X\rangle$, *and let* $G \subseteq K\langle X\rangle \setminus \{0\}$ *be a* σ*-Gröbner basis of* I. *Moreover, let* $B \subseteq \langle X\rangle$ *be the set of all words which are not a multiple of any word in the set* $\mathrm{LT}_\sigma\{G\}$. *Then we have* $\mathrm{HF}^a_{K\langle X\rangle/I}(i) = |B_{\le i}|$.

Proof. By Lemma 6.3.7 the residue classes of the words in B form a K-basis $K\langle X\rangle/I$. In the same way as the proof of [44], Proposition 5.6.3.a, we can show that the residue classes of the words in $B_{\le i}$ form a basis of K-vector space $\mathcal{F}_i/(\mathcal{F}_i \cap I)$. Then the claim follows. □

Assume that we are given a finite Gröbner basis G of I with respect to a length compatible admissible ordering. Using the result of the above proposition, we present the following algorithm for computing the values of the affine Hilbert function of $K\langle X\rangle/I$.

Corollary 6.3.11. *Let* $I \subseteq K\langle X\rangle \setminus \{0\}$ *be an ideal, let* σ *be a length compatible admissible ordering on* $\langle X\rangle$, *and let* $G \subseteq K\langle X\rangle \setminus \{0\}$ *be a finite* σ*-Gröbner basis of* I.

Moreover, let $n \in \mathbb{N}$. Consider the following sequence of instructions.

1) *Let $d = 0, B = \{1\}$ and $\mathrm{HF}^a(d) = 1$.*

2) *If $d = n$, then return the sequence $\mathrm{HF}^a(0), \mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(n)$.*

3) *Replace B by the set $\{w \cdot x \mid w \in B, x \in X\}$, and then delete from B all words $w \in B$ such that w is a multiple of some word in $\mathcal{F}_{d+1} \cap \mathrm{LT}_\sigma\{G\}$.*

4) *If $B = \emptyset$, then return the sequence $\mathrm{HF}^a(0), \mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(d), \mathrm{HF}^a(d+1), \ldots,$ $\mathrm{HF}^a(n)$ where $\mathrm{HF}^a(d{+}1) = \cdots = \mathrm{HF}^a(n) = \mathrm{HF}^a(d)$. Otherwise, set $\mathrm{HF}^a(d{+}1) = \mathrm{HF}^a(d) + |B|$, increase d by one. Then start again with step 2).*

This is an algorithm computing the sequence $\mathrm{HF}^a(0), \mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(n)$ which are the values of the affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/I}$.

Proof. Observe that the sequence of instructions constructs words in $\mathcal{O}_\sigma(I)$ length by length and the number d is strictly increasing until $d = n$ or $B = \emptyset$. The claim is an immediate consequence of Proposition 6.3.10. □

Remark 6.3.12. Let us make some observations about the preceding algorithm.

a) The algorithm enumerates sets of representatives of the basis elements of $K\langle X\rangle/I$ length by length. If the algorithm returns a result in step 4), then no new basis elements can be found and $\mathrm{HF}^a(d)$ becomes eventually stable. Consequently, the K-dimension $\dim_K(K\langle X\rangle/I)$ is finite. In this case by setting n large enough the algorithm computes K-dimension of $K\langle X\rangle/I$, i.e. we have $\dim_K(K\langle X\rangle/I) = \mathrm{HF}^a(n)$. Note that it is not very efficient to check the finiteness of $\dim_K(K\langle X\rangle/I)$ in this way. In the second part of this section we shall introduce Ufnarovski's finiteness criteria (see Theorem 6.3.27) to check the finiteness of $\dim_K(K\langle X\rangle/I)$. Moreover, the algorithm also computes the values of the Hilbert function $\mathrm{HF}_{K\langle X\rangle/I}$. Indeed, in step 4) we have $\mathrm{HF}(d+1) = |B|$.

b) The major operation in the algorithm is string matching. From the point of view of implementation, we would like to require that G is the reduced σ-Gröbner basis of I since the set $\mathrm{LT}_\sigma\{G\}$ becomes the minimal system of generators of $\mathrm{LT}_\sigma\{I\}$ and we can reduce a lot of string matching operations in step 3). However, to get the reduced Göbner basis we have to operate interreduction on the system of generators of I, which is known to be quite costly. An economic solution is to interreduce the set $\mathrm{LT}_\sigma\{G\}$ and obtain a small enough system of generators of $\mathrm{LT}_\sigma\{I\}$. This strategy is applied in the ApCoCoA package *gbmr*.

c) In practice the ideal I may not have a finite σ-Gröbner basis. In this case we shall combine the computation of the affine Hilbert function with the enumerating procedure of Gröbner basis computations.

   c.1) If the ideal I is generated by a set of homogeneous polynomials with respect to an $\mathbb{N}$-grading, then by applying the Homogeneous Buchberger Procedure (see Theorem 4.3.16) we compute truncated Gröbner bases of I degree by degree. Step 3) of the algorithm in Corollary 6.3.11 indicates that in order to compute $\mathrm{HF}^a_{K\langle X\rangle/I}(d)$ it is only necessary to compute d-truncated σ-Gröbner basis $G_{\le d}$ of I.

   c.2) If the ideal I is non-graded and has no finite Gröbner bases, then by applying the Buchberger Procedure (see Theorem 4.1.14) with the normal selection strategy we compute partial Gröbner bases of I to some degree. Then using the algorithm as in Corollary 6.3.11 we compute "pseudo" values of affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/I}$, which estimate the real values.

The following corollary describes more precisely what we mean by saying "pseudo" values of affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/I}$ in Remark 6.3.12.c.2.

Corollary 6.3.13. *Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, let σ be a length compatible admissible ordering on $\langle X\rangle$, and let $G_p \subseteq K\langle X\rangle \setminus \{0\}$ be a partial σ-Gröbner basis of I. Moreover, let $d \in \mathbb{N}$, and let $\mathrm{HF}^a_p(d)$ be the result of the algorithm in Corollary 6.3.11. Then we have $\mathrm{HF}^a(d) \le \mathrm{HF}^a_p(d)$. In particular, $\dim_K(K\langle X\rangle/\langle G_p\rangle) < \infty$ implies $\dim_K(K\langle X\rangle/I) < \infty$.*

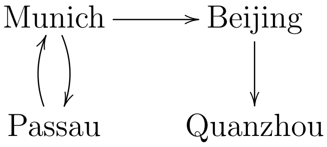
Proof. Clearly G_p is contained in a σ-Gröbner basis, say G, of I. Therefore we have $\mathcal{F}_d \cap \mathrm{LT}_\sigma\{G_p\} \subseteq \mathcal{F}_d \cap \mathrm{LT}_\sigma\{G\}$. The claim follows from Proposition 6.3.10. □

Given a Gröbner basis G of I with respect to a length compatible ordering, a less risky and more efficient method to check the finiteness of $\dim_K(K\langle X\rangle/I)$ is to use the Ufnarovski graph, whose initial intention was to check the finiteness of $\dim_K(K\langle X\rangle/I)$ and to compute the growth of $K\langle X\rangle/I$ (see [60, 69, 70, 71]). In the second part of this section we shall introduce the original idea of V. Ufnarovski [69] and explore it further. We develop an algorithm to compute Hilbert series by combining the computation of the values of the affine Hilbert function with Ufnarovski's technique. For our purpose we shall first borrow some notions from graph theory. We refer to [24, 39] as standard textbooks for more information on graph theory.

Definition 6.3.14. A **directed graph** G is a pair (V, E) of disjoint sets where $E \subseteq V \times V$ is a set of ordered pairs. An element $v \in V$ is called a **vertex**. An element $(v, v') \in E$ is called an **edge** from v to v'. An edge $(v, v) \in E$ is called a **loop**.

The advantage of graphs is that they have natural visual representations.

Example 6.3.15. Consider the graph $G = (V, E)$ with $V = \{$Munich, Passau, Beijing, Quanzhou$\}$ and $E = \{$(Passau,Munich), (Munich,Passau), (Munich,Beijing), (Beijing,Quanzhou)$\}$. We illustrate G as follows.



Definition 6.3.16. Let $G = (V, E)$ be a graph.

a) A **path** in G is a sequence of pairwise distinct vertices $v_0, v_1, \ldots, v_k \in V$ such that $(v_i, v_{i+1}) \in E$ for all $i \in \{0, \ldots, i-1\}$. The **length** of a path is the number of edges on the path.

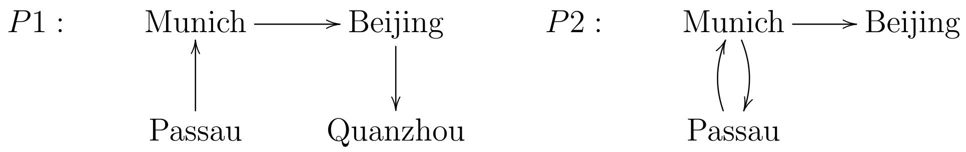
b) A **cycle** in G is a sequence of vertices $v_0, v_1, \ldots, v_k \in V$ such that $v_0, v_1, \ldots, v_{k-1}$ is a path and $v_0 = v_k$.

c) A **route** in G is a sequence of vertices $v_0, v_1, \ldots, v_k \in V$ such that $(v_i, v_{i+1}) \in E$ for all $i \in \{0, \ldots, k-1\}$. The **length** of a route is the number of edges on the route.

Using this definition, an edge is a path as well as a route of length 1, and a loop is a cycle as well as a route of length 1. For our purposes we shall also consider each vertex $v \in V$ as a route from v to v with length 0.

Example 6.3.17. (continued) Consider the graph as in Example 6.3.15. Let P_1 be the sequence Passau, Munich, Beijing, Quanzhou. Then P_1 is a path of length 3 from Passau to Quanzhou. Now let P_2 be the sequence Munich, Passau, Munich, Beijing.

Then P_2 is a route of length 3 from Munich to Beijing and contains a cycle of length 2.



Note that there are two standard ways to represent a graph: as a collection of adjacency lists or as an adjacency matrix (see [19], Chapter 22). The latter is an essential tool for our computations.

Definition 6.3.18. Let $G = (V, E)$ be a graph with the set of vertices $V = \{v_1, \dots, v_n\}$. An **adjacency matrix** B of G is a matrix of $\mathrm{Mat}_{n\times n}(\mathbb{N})$ whose the $(i, j)^{\text{th}}$ element b_{ij} is defined by

$$b_{ij} = \begin{cases} 1, & \text{if } (v_i, v_j) \in E, \\ 0, & \text{if } (v_i, v_j) \notin E. \end{cases}$$

Given an adjacency matrix B of a graph G, the following lemma enables us to compute the number of routes of specified length between any two vertices in G.

Lemma 6.3.19. *Let $G = (V, E)$ be a graph with the set of vertices $V = \{v_1, \dots, v_n\}$ and an adjacency matrix $B \in \mathrm{Mat}_{n\times n}(\mathbb{N})$. For $m \in \mathbb{N}$, the $(i, j)^{\text{th}}$ element $b_{ij}^{(m)}$ of the matrix B^m is the number of routes of length m from v_i to v_j for all $i, j \in \{1, \dots, n\}$.*

Proof. We prove the claim by induction on m. For $m = 0$ the adjacency matrix $B^{(0)} = I_n$ is the identity matrix of $\mathrm{Mat}_{n\times n}(\mathbb{N})$ since routes of length 0 are vertices. For $m = 1$ the claim holds since routes of length 1 are edges. Note that the $(i, j)^{\text{th}}$ element $b_{ij}^{(m)}$ of the matrix B^m is equal to $\sum_{k=1}^{n} b_{ik}^{(m-1)} b_{kj}^{(1)}$. By the induction hypothesis, $b_{ik}^{(m-1)}$ is the number of routes of length $m - 1$ from v_i to v_k and $b_{kj}^{(1)}$ is the number of routes of length 1 from v_k to v_j. Thus $b_{ik}^{(m-1)} b_{kj}^{(1)}$ is the number of routes of length m from v_i to v_j passing through v_k. Hence the number of routes of length m from v_i to v_j is $\sum_{k=1}^{n} b_{ik}^{(m-1)} b_{kj}^{(1)}$. □

Example 6.3.20. (continued) Consider the graph as in Example 6.3.15. An adjacency matrix B of the graph G is as follows.

$$\begin{array}{l} \\ \text{Munich} \\ \text{Passau} \\ \text{Beijing} \\ \text{Quanzhou} \end{array} \begin{array}{c} \begin{array}{cccc} \text{Munich} & \text{Passau} & \text{Beijing} & \text{Quanzhou} \end{array} \\ \left(\begin{array}{cccc} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) \end{array} = B$$

Moreover, for an integer $m \geq 2$ we have

$$B^m = \begin{pmatrix} (m+1) \bmod 2 & m \bmod 2 & m \bmod 2 & (m+1) \bmod 2 \\ m \bmod 2 & (m+1) \bmod 2 & (m+1) \bmod 2 & m \bmod 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

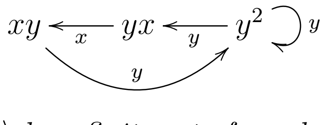
With ingredients introduced above, we are ready to define the Ufnarovski graph and investigate Ufnarovski's technique further.

Definition 6.3.21. Let $S \subset \langle X\rangle$ be a finite set of words, and let $k = \max\{\text{len}(w) \mid w \in S\} - 1$. The **Ufnarovski graph** U_S of S is a graph with the pair (V, E) satisfying the following conditions.

a) The vertices set V consists of all words $w \in \langle X\rangle$ of length k such that w is a normal word modulo $\langle S\rangle$.

b) For all $w, w' \in V$, there exists an edge $(w, w') \in E$ if and only if there exist $x_i, x_j \in X$ such that $wx_i = x_j w'$ and such that wx_i is a normal word modulo $\langle S\rangle$. In this case we denote the edge (w, w') by x_i.

Example 6.3.22. Consider $X = \{x, y\}$ and $S = \{x^2, xyx\}$. Then we have $k = 2$, $V = \{xy, yx, y^2\}$, and the following Ufnarovski graph U_S.

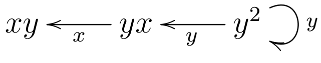


Lemma 6.3.23. *Let $S \subset \langle X\rangle$ be a finite set of words, let $k = \max\{\text{len}(w) \mid w \in S\} - 1$, and let U_S be the Ufnarovski graph of S. Then for all $m \in \mathbb{N}$ there is a one-to-one correspondence between the routes of length m in U_S and the normal words of length $m + k$ modulo $\langle S\rangle$.*

Proof. See [69], Theorem 3. □

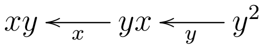
Example 6.3.24. (continued) Consider Example 6.3.22 again. Each vertex in $V = \{xy, yx, y^2\}$ is a route of length 0 and corresponding to a normal word of length 2. There are four edges (xy, y^2), (yx, xy), (y^2, yx), (y^2, y^2) which are routes of length 1 and corresponding to the normal words xy^2, yxy, y^2x, y^3 of length 3, respectively. Observe that the loop (y^2, y^2) generates infinite many normal words $\{y^{2+n} \mid n \in \mathbb{N}\}$, and the cycle xy, y^2, yx, xy generates infinite many normal words $\{xy(y^2x)^n, yx(xy^2)^n, y^2(yxy)^n \mid n \in \mathbb{N}\}$.

We add the word xy^2 to S, i.e. $S = \{x^2, xyx, xy^2\}$. Then we have $k = 2, V = \{xy, yx, y^2\}$, and the following Ufnarovski graph.



Each vertex in $V = \{xy, yx, y^2\}$ is a route of length 0 and corresponding to a normal word of length 2. There are three edges (yx, xy), (y^2, yx), (y^2, y^2) which are routes of length 1 and corresponding to the normal words yxy, y^2x, y^3 of length 3, respectively. The loop (y^2, y^2) involves infinite many normal words $\{y^{2+n}, y^{2+n}x, y^{2+n}xy \mid n \in \mathbb{N}\}$.

Furthermore, we add the word y^3 to S, i.e. $S = \{x^2, xyx, xy^2, y^3\}$. Then we have $k = 2, V = \{xy, yx, y^2\}$, and the following Ufnarovski graph.



Each vertex in $V = \{xy, yx, y^2\}$ is a route of length 0 and corresponding to a normal word of length 2. There are two edges (yx, xy), (y^2, yx) which are routes of length 1 and corresponding to the normal words yxy, y^2x of length 3, respectively. There is one route y^2, yx, xy of length 2 with the corresponding normal words y^2xy of length 4. The maximal length of the routes in the graph is 2.

Using the Ufnarovski graph, we can check the finiteness of the K-dimension of the K-algebra $K\langle X\rangle/I$ as well as its growth.

Theorem 6.3.25. (Ufnarovski's Finiteness Criteria) *Let $I \subseteq K\langle X\rangle \setminus \{0\}$ be an ideal, let σ be a length compatible admissible ordering on $\langle X\rangle$, let $G \subseteq K\langle X\rangle \setminus \{0\}$ be a finite σ-Gröbner basis of I, and let U be the Ufnarovski graph of $\mathrm{LT}_\sigma\{G\}$. Then we have $\dim_K(K\langle X\rangle/I) < \infty$ if and only if U has no cycle. Moreover, the growth of $K\langle X\rangle/I$ is exponential if and only if U has two intersecting cycles. Otherwise, the growth of $K\langle X\rangle/I$ is polynomial of degree d, where d is the maximal number of distinct cycles that can be included in a single route in U.*

Proof. This follows from Lemma 6.3.7 and [69], Theorem 2. □

Inspired by Lemma 6.3.23, we develop another approach to compute the values of the affine Hilbert function of $K\langle X\rangle/I$.

Assumption 6.3.26. *In the rest of this section, we let σ be a length compatible admissible ordering on $\langle X\rangle$. We shall assume that the ideal I has a finite σ-Gröbner basis G. Moreover, let U be the Ufnarovski graph of $\mathrm{LT}_\sigma\{G\}$, let $k = \max\{\mathrm{len}(w) \mid w \in \mathrm{LT}_\sigma\{G\}\} - 1$, let $V = \{w_1, \ldots, w_n\}$ be the set of all vertices in U, and let $B \in \mathrm{Mat}_{n\times n}(\mathbb{N})$ be an adjacency matrix of U.*

By Lemma 6.3.19 the $(i,j)^{\text{th}}$ element $b_{ij}^{(m)}$ of the matrix B^m is the number of routes of length m from w_i to w_j for all $m \in \mathbb{N}$. By Lemma 6.3.23 we have

$$\mathrm{HF}(k+m) = \sum_{i,j} b_{ij}^{(m)}$$

for all $m \in \mathbb{N}$. Therefore the values of the affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/I}$ can be formulated as follows.

Theorem 6.3.27. *Under Assumption 6.3.26, we let $s \in \mathbb{N}$ such that $s > k$. Consider the following sequence of instructions.*

1) *Compute the sequence $\mathrm{HF}^a(0), \mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(k)$ using Corollary 6.3.11. Let $d = k$.*

2) *If $s = d$, then return the sequence $\mathrm{HF}^a(0), \mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(s)$.*

3) *If $B^{d+1-k} = 0$, then return the sequence $\mathrm{HF}^a(0), \mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(d), \mathrm{HF}^a(d+1), \ldots, \mathrm{HF}^a(s)$ where $\mathrm{HF}^a(d+1) = \cdots = \mathrm{HF}^a(s) = \mathrm{HF}^a(d)$. If $B^{d+1-k} \neq 0$, set $\mathrm{HF}^a(d+1) = \mathrm{HF}^a(d) + \sum_{i,j} b_{ij}^{(d+1-k)}$, increase d by one, and continue with step 2).*

This is an algorithm computing the sequence $\mathrm{HF}^a(0), \mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(s)$ which are the values of the affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/I}$.

Proof. Observe that $\sum_{i,j} b_{ij}^{(d+1-k)}$ is the number of the normal words of length $d+1$. The claim follows from Lemmas 6.3.19 and 6.3.23. □

Remark 6.3.28. The algorithm as in Theorem 6.3.27 is superior to the algorithm as in Corollary 6.3.11 in twofold.

a) Firstly, Corollary 6.3.11 has to compute all the values of the affine Hilbert function $\mathrm{HF}^a(0)$, $\mathrm{HF}^a(1), \ldots, \mathrm{HF}^a(d), \mathrm{HF}^a(d+1), \ldots$ sequentially; while for $d > k$ Theorem 6.3.27 can compute the individual value of the affine Hilbert function $\mathrm{HF}^a(d)$ using the formula $\mathrm{HF}^a(d) = \mathrm{HF}^a(k) + \sum_{i,j} \hat{b}_{ij}$ where $\hat{b}_{ij}$ is the $(i,j)^{\text{th}}$ element of the matrix $\hat{B} = \sum_{t=1}^{d-k} B^t$. In particular, we have $\mathrm{HF}_{K\langle X\rangle/I}(d) = \sum_{i,j} b_{ij}^{(d-k)}$ where $b_{ij}^{(d-k)}$ is the $(i,j)^{\text{th}}$ element of the matrix B^{d-k}.

b) Secondly, the fundamental computations in Corollary 6.3.11 are symbolic computations, i.e. string matching; while for $d > k$ the computations in Theorem 6.3.27, i.e. B^{d-k} and $\sum_{t=1}^{d-k} B^t$, are numeric computations which are generally much faster than symbolic computations.

Now we are going to formulate the Hilbert series of the K-algebra $K\langle X\rangle/I$. Note that the adjacency matrix $B \in \mathrm{Mat}_{n\times n}(\mathbb{N})$ has a unique minimal polynomial $\mu_B(x)$ in $\mathbb{Q}[x]$, i.e. $\mu_B(x)$ is the monic polynomial of least degree such that $\mu_B(B) = 0$. Assume that $\mu_B(x) = x^s - \sum_{i=0}^{s-1} c_i x^i$ with $c_i \in \mathbb{Q}$ for $i = 0, 1, \ldots, s-1$.

Theorem 6.3.29. *Under Assumption 6.3.26 and using the same notation as above, we have*

$$\mathrm{HS}_{K\langle X\rangle/I}(z) = \frac{\sum_{j=0}^{k+s-1} (\mathrm{HF}_{K\langle X\rangle/I}(j) - \sum_{i=1}^{s} c_{s-i}\mathrm{HF}_{K\langle X\rangle/I}(j-i))z^j}{z^s \mu_B(\frac{1}{z})}.$$

Proof. From $\mu_B(B) = 0$, we get $B^s = \sum_{i=0}^{s-1} c_i B^i$. Multiplying both sides by B^j with $j \in \mathbb{N}$, we obtain $B^{s+j} = \sum_{i=0}^{s-1} c_i B^{i+j}$. Since $\mathrm{HF}(k+d) = \sum_{ij} b_{ij}^{(d)}$ for all $d \in \mathbb{N}$, we have the recurrence relation of the Hilbert function

$$\mathrm{HF}(k+s+j) = \sum_{i=0}^{s-1} c_i \mathrm{HF}(k+i+j) \text{ for all } j \geq 0.$$

We multiply both sides of the equation by z^{k+s+j} and sum over all $j \in \mathbb{N}$. By simplifying the summand we obtain the Hilbert series $\mathrm{HS}_{K\langle X\rangle/I}(z)$ as claimed. □

Example 6.3.30. (continued) Consider Example 6.3.22 again. Recall that we have $X = \{x, y\}$ and $S = \{x^2, xyx\}$. Consider the K-algebra $K\langle X\rangle/\langle S\rangle$. Clearly the set S is a Gröbner basis of the ideal $\langle S\rangle \subset K\langle X\rangle$. From Example 6.3.22, we have $k = 2$, $V = \{xy, yx, y^2\}$, and an adjacency matrix

$$\begin{array}{c|ccc} & xy & yx & y^2 \\ \hline xy & 0 & 0 & 1 \\ yx & 1 & 0 & 0 \\ y^2 & 0 & 1 & 1 \end{array} = B.$$

The minimal polynomial of B is $\mu_B(x) = x^3 - x^2 - 1$. Moreover, we have $\mathrm{HF}(0) = 1$, $\mathrm{HF}(1) = 2, \mathrm{HF}(2) = 3$ using Corollary 6.3.11, and $\mathrm{HF}(3) = 4, \mathrm{HF}(4) = 6$ using Theorem 6.3.27. Then by Theorem 6.3.29 we have $\mathrm{HS}(z) = \frac{1+z+z^2}{1-z-z^3}$. Equivalently, we have $\mathrm{HS}(z) = (1 + z + z^2)\sum_{i=0}^{\infty}(z + z^3)^i$. Clearly the affine Hilbert function $\mathrm{HF}^a_{K\langle X\rangle/\langle S\rangle}$ is strictly increasing. Moreover, by Example 6.3.22 and Theorem 6.3.25 the growth of $K\langle X\rangle/\langle S\rangle$ is exponential.

As in Example 6.3.24, we add the word xy^2 to S, i.e. $S = \{x^2, xyx, xy^2\}$. Then we have $k = 2, V = \{xy, yx, y^2\}$, and an adjacency matrix

$$\begin{array}{c} \\ xy \\ yx \\ y^2 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} xy & yx & y^2 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \end{array} = B.$$

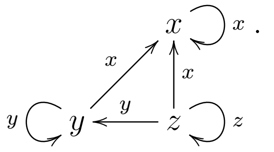
The minimal polynomial of B is $\mu_B(x) = x^3 - x^2$. Moreover, we have $\mathrm{HF}(0) = 1$, $\mathrm{HF}(1) = 2, \mathrm{HF}(2) = 3, \mathrm{HF}(3) = 3$, and $\mathrm{HF}(4) = 3$. Then by Theorem 6.3.29 we have $\mathrm{HS}(z) = \frac{1+z+z^2}{1-z}$. Equivalently, we have $\mathrm{HS}(z) = 1 + 2z + \sum_{i=2}^{\infty} 3z^i$. Therefore $\mathrm{HF}^a(i) = 3i$ for $i \geq 1$. Hence the growth of $K\langle X\rangle/\langle S\rangle$ is linear.

Furthermore, we also add the word y^3 to S, i.e. $S = \{x^2, xyx, xy^2, y^3\}$. Then we have $k = 2, V = \{xy, yx, y^2\}$, and an adjacency matrix

$$\begin{array}{c} \\ xy \\ yx \\ y^2 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} xy & yx & y^2 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array} = B.$$

The minimal polynomial of B is $\mu_B(x) = x^3$. Moreover, we have $\mathrm{HF}(0) = 1, \mathrm{HF}(1) = 2$, $\mathrm{HF}(2) = 3, \mathrm{HF}(3) = 2$, and $\mathrm{HF}(4) = 1$. Then by Theorem 6.3.29 we have $\mathrm{HS}(z) = 1 + 2z + 3z^2 + 2z^3 + z^4$. Therefore $\mathrm{HF}^a(i) = 9$ for $i \geq 4$. Hence $\dim_K(K\langle X\rangle/\langle S\rangle) = 9$.

Example 6.3.31. Consider the free monoid ring $K\langle x, y, z\rangle$ and the ideal I generated by the set $G = \{xy - yx, xz - zx, yz - zy\}$. Let $\sigma = \texttt{LLex}$ on $\langle X\rangle$ such that $x >_\sigma y >_\sigma z$. It is easy to verify that G is a σ-Gröbner basis of I. Consider the K-algebra $K\langle x, y, z\rangle/I$. Note that $K\langle x, y, z\rangle/I \cong K[x, y, z]$. We have $\mathrm{LT}_\sigma\{G\} = \{xy,\ xz,\ yz\}$, $k = 1, V = \{x, y, z\}$, and the following Ufnarovski graph U.



By Theorem 6.3.25 the growth of $K\langle x, y, z\rangle/I$ is polynomial of degree 3. An adjacency matrix of U is

$$\begin{array}{c|ccc} & x & y & z \\ \hline x & 1 & 0 & 0 \\ y & 1 & 1 & 0 \\ z & 1 & 1 & 1 \end{array} = B.$$

The minimal polynomial of B is $\mu_B(x) = (x-1)^3$. Moreover, we have $\mathrm{HF}(0) = 1$, $\mathrm{HF}(1) = 3, \mathrm{HF}(2) = 6$ using Corollary 6.3.11, and $\mathrm{HF}(3) = 10, \mathrm{HF}(4) = 15$ using Theorem 6.3.27. Then by Theorem 6.3.29 we have $\mathrm{HS}(z) = (1-z)^{-3} = \sum_{i=0}^{\infty} \binom{2+i}{2} z^i$. Therefore $\mathrm{HF}^a(i) = \sum_{j=0}^{i} \binom{2+j}{2} = \binom{i+3}{3}$.

Remark 6.3.32. Finally, we shall make some remarks about Theorem 6.3.29. Let $\mu_B(x) = x^s - \sum_{i=0}^{s-1} c_i x^i \in \mathbb{Q}[x]$ be the minimal polynomial of the adjacency matrix B. As seen in the proof of the theorem, for all $j \in \mathbb{N}$ the recurrence relation $\mathrm{HF}(k+j+s) = c_0\mathrm{HF}(k+j) + c_1\mathrm{HF}(k+j+1) + \cdots + c_{s-1}\mathrm{HF}(k+j+s-1)$ holds. We can use this recurrence relation instead of the multiplication of the adjacency matrix B to compute the values of the Hilbert function $\mathrm{HF}(i)$ where $i \geq k+s$. As a result, we can improve the algorithm in Theorem 6.3.27 using the recurrence relation. Moreover, using sufficiently effective techniques from combinatorial theory (see for instance [32], Chapter 7), we can obtain the formula for the Hilbert function $\mathrm{HF}(i)$ by expanding the Hilbert series $\mathrm{HS}(z)$ into a power series and reading off the coefficient of z^i. Further, as seen in the previous examples, we might also obtain the formula for the affine Hilbert function $\mathrm{HF}^a(i)$.

Bibliography

[1] P. Ackermann and M. Kreuzer, Gröbner basis cryptosystems, Applicable Algebra in Engineering, Communication and Computing (2006), 17, 173-194.

[2] ApCoCoA team, ApCoCoA: Applied Computations in Commutative Algebra, available at http://www.apcocoa.org.

[3] M.A. Borges-Trenard, M. Borges-Quintana and T. Mora, Computing Gröbner bases by FGLM techniques in a non-commutative setting, Journal of Symbolic Computation (2000), 30, 429-449.

[4] A. Bigatti, M. Caboara and L. Robbiano, Computing inhomogeneous Gröbner bases, Journal of Symbolic Computation (2011), 46, 498-510.

[5] G.M. Bergman, The diamond lemma in ring theory, Advanced Mathematics (1978), 29, 178-218.

[6] G.M. Bergman, A note on the growth functions of algebras and semigroups, mimeographed notes, University of California, Berkeley, USA, 1978.

[7] W. Borho and H. Kraft, Über die Gelfand-Kirillov Dimension, Mathematische Annalen (1976), 220(1), 1-24.

[8] H. Bluhm and M. Kreuzer, Gröbner basis techniques in the computation of two-sided syzygies, Contemporary Mathematics (2006), 421, 45-64.

[9] H. Bluhm, Syzyienberechnung übner nicht-kommutativen Polynomringen, Diploma thesis, Fachbereich Mathematik, Universität Dortmund, Germany, 2005.

[10] M. Brichenstein, Slimgb: Gröbner bases with slim polynomials, Revista Matemática Complutense (2010), 23(2), 453-466.

[11] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal, Dissertation, Universität Inssbruck, Austria, 1965.

[12] B. Buchberger, A criterion for detecting unnecessary reductions in the construction of Groebner bases, in: Proceedings of the International Symposiumon on Symbolic and Algebraic Computation (EUROSAM '79), Edward W. Ng (Ed.), Springer-Verlag, London, UK, 1979, 3-21.

[13] B. Buchberger, Gröbner bases: an algorithmic method in polynomial ideal theory, in: Multidimensional Systems Theory-Progress, Directions and Open Problems in Multidimensional Systems, N.K. Bose (Ed.), Reidel Publishing Company, Dodrecht-Boston-Lancaster, 1985, 184-232.

[14] B. Buchberger, Applications of Gröbner bases in non-linear computational geometry, in: Trends in Computer Algebra, R. Janßen (ed.), Springer, Berlin, 296 (1988), 52-80.

[15] V.G. Bardakov and A.Y. Vesnin, A generalizeion of Fibonacci groups, Algebra and Logic (2003), 42, 73-91.

[16] T. Becker and V. Weispfenning, Gröbner Bases: A Computational Approach to Commutative Algebra, Springer-Verlag, 1992.

[17] M. Caboara, M. Kreuzer and L. Robbiano, Efficiently computing minimal sets of critical pairs, Journal of Symbolic Computation (2004), 38, 1169-1190.

[18] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra (2nd edition), Springer-Verlag, 2006.

[19] T.H. Cormen, C.E. Leiserson, R.L. Rivest and C. Stein, Introduction to Algorithms (2nd edition), The MIT Press, Cambridge, 2002.

[20] CoCoA: Computations in Commutative Algebra, available at http://cocoa.dima.unige.it.

[21] A.M. Cohen, Non-commutative polynomial computations, available at www.win.tue.nl/∼amc/pub/gbnpaangepast.pdf.

[22] , M. Dehn, Über unendliche diskontinuierliche Gruppen, Mathematische Annalen (1911), 71(1), 116-144.

[23] J. Dixmier, Enveloping Algebras, North-Holland Publishing Company, 1977.

[24] R. Diestel, Graph Theory (3rd edition), Graduate Texts in Mathematics 173, Springer-Verlag, Berlin, 2005.

[25] I.S. Duff, A.M. Erisman and J.K. Ried, Direct Methods for Sparse Matrices, Oxford Science Publications, 1986.

[26] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F4), Journal of Pure and Applied Algebra (1999), 139, 61-88.

[27] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC '02), T. Mora (Ed.), ACM, New York, USA, 2002, 75-83.

[28] J.-C. Faugère, P. Gianni, D. Lazard and T. Mora, Efficient computation of zero-dimensional Gröbner bases by change of ordering, Journal of Symbolic Computation (1993), 16, 329-344.

[29] B. Fine, M. Hahn, A. Hulpke, V. Rebel, G. Rosenberger and M. Scheer, All finite generalized tetrahedron groups, available at https://eldorado.tu-dortmund.de/handle/2003/25188.

[30] J.-C. Faugère and S. Lachartre, Parallel Gaussian elimination for Gröbner bases computations in finite fields, in: Proceedings of the 4th International Workshop on Parallel and Symbolic Computation (PASCO '10), 2010, 89-97.

[31] GAP: Groups, Algorithms, Programming, available at http://www.gap-system.org.

[32] R.L. Graham, D.E. Knuth and O. Patashnik, Concrete Mathematics: A Foundation for Computer Science (2nd edition), Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1994.

[33] R. Gebrauer and H.M. Möller, On an installation of Buchberger's algorithm, Journal Symbolic Computation (1988), 6, 275-286.

[34] A. Giovini, T. Mora, G. Niesi, L. Robbiano and C. Traverso, "One sugar cube, please" or selection strategies in the Buchberger algorithm, in: Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation (ISSAC '91), Stephen M. Watt (Ed.), ACM, New York, USA, 1991, 49-54.

[35] E.L. Green, T. Mora and V. Ufnarovski, The non-commutative Gröbner freaks, in: Symbolic rewriting techniques, M. Bronsetein, J. Grabmeier and V. Weispfenning (Eds.), Birkhäuser Verlag, Basel, Switzerland, 1998, 93-104.

[36] E.L. Green, Noncommutative Gröbner bases and projective resolutions, in: Proceedings of the Euroconference Computational Methods for Representations of Groups and Algebras, Michler, Schneider (Eds.), Essen, 1997, Progress in Mathematics, 173, Birkhäuser Verlag, Basel, 1999, 29-60.

[37] E.L. Green, Multiplicative bases, Gröbner bases, and right Gröbner bases, Journal of Symbolic Computation (2000), 29, 601-623.

[38] D.F. Holt, B. Eick and E.A. O'Brien, Handbook of Computational Group Theory, Chapman and Hall/CRC press, 2005.

[39] J.M. Harris, J.L. Hirst and M.J. Mossinghoff, Combinatorics and Graph Theory, Springer-Verlag, New York, 2000.

[40] T.W. Hungerford, Algebra, Graduate Texts in Mathematics 73, Springer-Verlag, New York, 1974.

[41] D.E. Knuth and P.B. Bendix, Simple word problems in universal algebra, in: Computational Problems in Abstract Algebra, J. Leech (Ed.), Oxford: Pergamon, 1970, 263-297.

[42] G.R. Krause and T.H. Lenagn, Growth of Algebras and Gelfand-Kirillov Dimension, Pitman Advanced Publishing Program, Boston, 1985.

[43] M. Kreuzer and L. Robbiano, Computational Commutative Algebra 1, Springer, Heidelberg 2000.

[44] M. Kreuzer and L. Robbiano, Computational Commutative Algebra 2, Springer, Heidelberg 2005.

[45] M. Kreuzer, Gröbner basis computations in monoid and group rings, Complexity and Group Bases Cryptography, Montreal, Sept. 2, 2010.

[46] S. Lang, Algebra, Addison-Wesley, Reading, MA 1993.

[47] V. Levandovskyy, Non-commutative Computer Algebra for Polynomial Algebras: Gröbner bases, applications and implementation, Dissertation, Universität Kaiserslautern, Germany, 2005.

[48] H. Li, Noncommutative Gröbner Bases and Filtered-graded Transfer, LNM, 1795, Springer-Verlag, Berlin, 2002.

[49] B. LaMacchia and A. Odlyzko, Solving large sparse linear systems over finite fields, in: Advances in Cryptology (CRYPTO '90), A.J. Menezes and S. Vanstone (Eds.), Springer-Verlag, 1991, 109-133.

[50] H. Li and C. Su, On (de)homogenized Gröbner bases, arXiv:0907.0526v2.

[51] Magma Computational Algebra System, URL http://magma.maths.usyd.edu.au/magma.

[52] K. Madlener and F. Otto, Some applications of prefix-rewriting in monoids, groups and rings, Reports on computer algebra, 22, Universität Kaiserlautern, Germany, 1998.

[53] F. Mora, Gröbner bases for non-commutative polynomial rings, in: Proceedings of the 3rd International Conference on Algebraic Algorithms and Error-Correcting Codes (AAECC-3), Jacques Calmet (Ed.), Springer-Verlag, London, UK, 1986, 353-362.

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

[55] T. Mora, An introduction to commutative and non-commutative Gröbner Bases, Journal of Theoretical Computer Science (1994), 134, 131-173.

[56] J.C. McConnell and J.C. Robson, Noncommutative Noetherian Rings, John Wiley and Sons Ltd., 1987.

[57] K. Madlener and B. Reinert, Computing Gröbner bases in monoid and group rings, in: Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation (ISSAC '93), M. Bronstein (Ed.), ACM, New York, 1993, 253-263.

[58] K. Madlener and 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 Verlag, Basel, 1998, 127-150.

[59] P. Narendran, C. Ó'Dúnlang and F. Otto, It is undecidable whether a finite special string-writing systems presents a group, Discrete Mathematics (1991), 98, 153-159.

[60] P. Nordbeck, On the finiteness of Gröbner bases computation in quotients of the free algebra, Applicable Algebra in Engineering, Communication and Computing (2001), 11, 157-180.

[61] C.H. Papadimitriou, Computational Complexity, Addison-Wesley Publishing Company, 1994.

[62] C. Pomerance and J.W. Smith, Reduction of huge, sparse matrices over finite fields via created catastrophes, Experimental Mathematics (1992), 1, 89-94.

[63] B. Reinert, On Gröbner Bases in Monoid and Group Rings, Dissertation, Universität Kaiserslautern, Germany, 1995.

[64] G. Rosenberger and M. Scheer, Classification of the finite generalized tetrahedron groups, Contemporary Mathematics (2002), 296, 207- 229.

[65] SINGULAR, available at http://www.singular.uni-kl.de.

[66] C. Sims, Computation with Finitely Presented Groups, Cambridge University Press, 1994.

[67] R. Scala and V. Levandovskyy, Letterplace ideals and non-commutative Gröbner bases, Journal of Symbolic Computation (2009), 44, 1374-1393.

[68] Symbolic Data, available at ftp://apcocoa.org/pub/symbolic_data.

[69] V.A. Ufnarovski, A growth criterion for graphs and algebras defined by words, Matematicheskie Zametki (1982), 31(3), 465-472.

[70] V.A. Ufnarovski, On the use of graphs for calculating the basis, growth and Hilbert series of associative algebras, Matematicheskii Sbornik (1989), 180(11),1548-1560.

[71] V.A. Ufnarovski, Combinatorial and asymptotic methods in algebra, Algebra VI, Encyclopedia of Mathematical Sciences, 57, Springer (1995), 5-196.

[72] V.A. Ufnarovski, On the cancellation rule in the homogenization, Computer Science Journal of Moldova (2008), 16, 133-145.

[73] R.B. Warfield, The Gelfand-Kirillov dimension of a tensor product, Mathematische Zeitschrift (1984), 185, 441-447.

[74] F. Winkler, Knuth-Bendix procedure and Buchberger algorithm: a synthesis, in: Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation (ISSAC '89), G.H. Gonnet (Ed.), ACM, New York, USA, 1989, 55-67.

[75] G. Williams, The aspherical Cavicchioli-Hegenbarth-Repovš generalized Fibonacci groups, Journal of Group Theory (2009), 12, 139-149.