Dimension Computations in Non-Commutative Associative Algebras

by

Grischa Studzinski

Diploma thesis in mathematics
submitted to
Fakultät für Mathematik, Informatik und Naturwissenschaften der
Rheinisch-Westfälischen Technischen Hochschule Aachen

May 9, 2010

produced at
Lehrstuhl D für Mathematik
Prof. Dr. Eva Zerz

Introduction

Any finitely generated associative algebra can be presented as a factor of the free associative algebra. Therefore computations in the free algebra have many applications in different areas of mathematics, like cryptography, ring theory, homological algebra, representation theory of monoids, groups and algebras, algebraic system and control theory, quantum algebras, in mathematical and theoretical physics.

The aim of this diploma thesis is to study factors of the free algebra with focus on the $\mathbb{K}$-dimension. In particular, we want to answer the question whether a factor algebra, given by a two-sided ideal, is finite dimensional or not. Here the approach to answer this question is to gather information which hopefully solves the question by studying the Gröbner basis.
Therefore one needs to construct a Gröbner basis explicitly from a given set of generators for an ideal. In theory this question was studied since the early years of computer algebra: Mora ([Mor86, Mor89, Mor94]), E. Green ([Gre93, Gre00]), Ufnarovskij ([Ufn90, Ufn98]) and Cojocaru et al. ([CPU99]) presented different facets of what we call today non-commutative Gröbner basis theory. In particular Mora discussed free non-commutative algebras and their quotient rings endowed also with negative (non-well-)orderings and further extended his theory (with Apel, [Ape00]). Other important contributions were made by Apel and Lassner ([AL88]) and especially Apel in [Ape00].

In the last years there has been more progress in theoretical, implementational and practical directions. Notably, the interest in free associative algebras grew stronger, as indicated by e. g. the book of D. Green ([Gre03]), where the author considers also negative (non-well-)orderings for certain non-commutative cases with a very different motivation and meaning, compared to the theory of Mora ([Mor89]) and Apel ([Ape00]) and with the commutative case as in Greuel et al. ([GP02]). Evans and Wensley investigated in [EW07] involutive bases in non-commutative algebras.

With the recent work of La Scala and Levandovskyy [LL09] a new way to compute Gröbner bases was born, where non-commutative Gröbner bases of graded ideals in free algebras are computed via the *Letterplace correspondence*. The most important point for practical computer algebra is that the computations take place in a commutative ring, where the data structures as well as many fundamental algorithms have been deeply studied and enhanced in the past 40 years.

So another task is to translate the setup of computing the $\mathbb{K}$-dimension for factor algebras into the realm of Letterplace. Here we found some interesting aspects, as well as new structures, as for example the $\mathbb{K}$-*shift-basis* (see 2.59).

Along the way there were many interesting applications and some theoretical development, like the mistletoes (see 2.43), which are a completely new way to store bases for factor algebras compactly, the concept of fake dimension (see 2.13) and the usage of the Ufnarovskij graph to determine the finiteness of the factor algebra by a given truncated Gröbner basis (see 2.19), which found their way into this thesis.

The mistletoes resemble the concept of border bases (cf. [KK06]). However, the connection to border bases is still to be investigated deeper. The algorithms to compute mistletoes and the $\mathbb{K}$-dimension have been analyzed for their algorithmic complexity(2.55,2.58).

The usage of the Ufnarovskij graph allows one to detect early the finiteness of a $\mathbb{K}$-basis, if applied in an adaptive algorithm for the computation of a Gröbner basis, what implies the finiteness of a Gröbner basis in this situation.
Adaptive computation of a Gröbner basis -either in the classical or in the Letterplace setting- is examined and realistic bounds for a single adaptive step are established (1.53,1.54,).

One of my personal goals for this thesis is to give an easy-to-understand introduction to non-commutative calculus in the free algebra, especially to non-commutative Gröbner bases, since although well studied, most work dealing with such general structures as the free associative algebra has not an introductive character.
Moreover, this work is a starting point for applications of non-commutative methods relying on Gröbner bases in free associative algebras and we are planing to expand our methods to other fields, like Gröbner basis cryptosystems and computations in non-commutative modules (see for example [AK05] and [BK07]).

Alongside the theoretical development we implemented the procedures in the computer algebra system Singular.
Singular [GPS09] has been developed since more than 20 years under the direction of Prof. Greuel, Prof. Pfister and Dr. Schönemann in Kaiserslautern, Germany. Singular is a specialized computer algebra system for supporting research in commutative algebra, algebraic geometry and singularity theory. Since 2005, there is a subsystem Singular:Plural [GLS06], which provides Gröbner bases-related functionality for a class of non-commutative *GR*-algebras [Lev05]. Special data structures, developed and implemented for polynomials, together with carefully designed and implemented algorithms, contribute to the widespread acceptance of Singular as one of the fastest computer algebra systems in the world.
The recently developed *Letterplace paradigm* allows the computation of Gröbner

bases in the free associative algebra and the corresponding algorithms have been implemented in the computer algebra system Singular.

I would like to thank many people for their support.
First of all there is my supervisor Dr. Viktor Levandovskyy, who gave me the opportunity for this work and a lot of help, who encouraged me on my way and of course for lots of interesting discussions during this work. Also I would like to thank my dear colleague Daniel Andres, who always was a great help and the one I could turn to with any questions, without annoying our supervisors.
Of course my sincere thanks go to my correctors, Prof. Dr. Eva Zerz and Prof. Dr. Martin Kreuzer, for the time they spent to review my thesis and for their useful suggestions.
Moreover, I would like to thank Prof. Dr. Roberto La Scala, Prof. Dr. Alexander Tiskin, Prof. Dr. Gunther Malle and Dr. Jürgen Müller, for their contributions by sharing their knowledge with me.

Aachen, May 9, 2010
Grischa Studzinski

Contents

1 Non-Commutative Gröbner Bases

The goal of this section is to introduce Gröbner bases of ideals of the free algebra $\mathbb{K}\langle\mathbf{X}\rangle$. Most of this chapter is basic knowledge and well studied (see for example [Ufn98], [Coh07], [GP02]). However, this knowledge is needed for a proper understanding of most computations in non-commutative algebras, and of great relevance for factor algebras.

1.1 Notations and Orders

Throughout this chapter let $\mathbb{K}$ be a field and $\mathbf{X}$ be the free monoid on n generators, denoted by $x_1, \ldots, x_n$.
We define the free algebra as the monoid ring

$$\mathbb{K}\langle\mathbf{X}\rangle := \{\sum_{i\in\mathbb{I}} \alpha_i m_i \mid \alpha_i \in \mathbb{K}, m_i \in \mathbf{X}, \quad \mathbb{I} \text{ an arbitrary index set,} \\ \text{only finitely many } \alpha_i \neq 0\}$$

and call the elements of $\mathbb{K}\langle\mathbf{X}\rangle$ *polynomials* and the elements of $\mathbf{X}$ embedded in $\mathbb{K}\langle\mathbf{X}\rangle$ together with the identity 1 *monomials*.
A subset $\mathbf{I} \subseteq \mathbb{K}\langle\mathbf{X}\rangle$ is called (two-sided) *ideal* of $\mathbb{K}\langle\mathbf{X}\rangle$, written $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$, if

1. $0 \in \mathbf{I}$
2. $r, s \in \mathbf{I} \quad \Rightarrow \quad r + s \in \mathbf{I}$
3. $r \in \mathbb{K}\langle\mathbf{X}\rangle, s \in \mathbf{I} \quad \Rightarrow \quad rs \in \mathbf{I},\ sr \in \mathbf{I}$

An ideal $\mathbf{I}$ is called *proper*, if $\mathbf{I} \neq \mathbb{K}\langle\mathbf{X}\rangle$ and $\mathbf{I} \neq \langle 0\rangle$.
A set $G \subset \mathbf{I}$ is called *generating set*, written $\mathbf{I} = \langle G\rangle$, if $\forall s \in \mathbf{I}\ \exists g_i \in G, r_i, l_i \in \mathbb{K}\langle\mathbf{X}\rangle : \quad s = \sum\limits_i \sum\limits_j l_{i,j} g_i r_{i,j}$. If there exists a finite generating set, $\mathbf{I}$ is called *finitely generated*. Since $\mathbb{K}$ is a field there is no loss of generality to assume that all polynomials of a given generating set are monic.

1.1 Definition. An *(strict total) ordering* $<$ is a total, transitive and asymmetric relation on $\mathbf{X}$, that is

- If $a < b$ then $\neg(a > b)$ *(asymmetry)*;
- If $a < b$ and $b < c$ then $a < c$ *(transitivity)*;
- Either $a < b$ or $b < a \quad \forall a, b \in \mathbf{X}, a \neq b$ *(totality)*.

1.2 Definition. A total ordering $<$ on $\mathbf{X}$ is called a

- *well ordering*, if every non-empty subset of $\mathbf{X}$ has a least element with respect to $<$. In particular, $1 < x \quad \forall x \in \mathbf{X}$.
- *reduction ordering*, if for all $m_1, m_2, l, r \in \mathbf{X}$ with $m_1 < m_2$ we have $lm_1r < lm_2r$.
- *monomial ordering*, if it is a well ordering and a reduction ordering.

Note that for a reduction ordering we have if $m, n \in \mathbf{X}$ are such that n *divides* m, that is, if there exists $l, r \in \mathbf{X}$ with $m = lnr$, denoted by $n \mid m$, then we have $n < m$, because for $1 < l, r \in \mathbf{X}$ we have $n = 1n < ln = ln1 < lnr = m$.
With a given ordering we can write each polynomial $f \in \mathbb{K}\langle \mathbf{X} \rangle$ uniquely as $f = \sum_{i=1}^{k} c_i m_i$, such that $c_i \in \mathbb{K}$ and $m_i \in \mathbf{X}$ with $m_1 < \cdots < m_k$. In this work we will always assume that $<$ is a monomial ordering (for existence see 1.4).

1.3 Definition. Given an ordering $<$, we define the *leading monomial* of a polynomial $f = \sum_{i=1}^{k} c_i m_i \neq 0$ as the maximum (with respect to $<$) of the set $\{m_i \mid c_i \neq 0\}$. and denote it by $\mathfrak{lm}(f)$. Also we call the coefficient of $\mathfrak{lm}(f)$ the *leading coefficient*, denoted by $\mathfrak{lc}(f)$ and we define the *leading term* of f as $\mathfrak{lt}(f) = \mathfrak{lc}(f) \cdot \mathfrak{lm}(f)$.
Finally we will denote with $\mathfrak{L}(\langle \mathbf{I} \rangle)$ the *leading ideal* of an ideal $\mathbf{I}$, which is the ideal generated by the leading monomials of $\mathbf{I}$.

1.4 Example. Without loss of generality, we can always assume that $x_1 < x_2 < \ldots < x_n$. Then we have the following two examples of monomial orderings:

- Let $\mu, \nu \in \mathbf{X}$, such that $\mu = x_{j_1} x_{j_2} \cdots x_{j_k}$, $\nu = x_{l_1} x_{l_2} \cdots x_{l_{\tilde{k}}}$. Then we have:

$$\mu <_{\text{lex}} \nu \quad \Longleftrightarrow \quad \exists 1 \leq i \leq \min\{k, \tilde{k}\} : \ x_{j_w} = x_{l_w} \ \forall w < i \ \wedge \ x_{j_i} < x_{l_i}$$

This is called the *(left) lexicographical ordering*.

- Take μ, ν as before. We define:

$$\mu <_{\text{gradlex}} \nu \quad \Longleftrightarrow \quad \begin{array}{ll} k < \tilde{k} & \text{or} \\ k = \tilde{k} \text{ and } \mu <_{\text{lex}} \nu. & \end{array}$$

This is called the *graded* or *degree lexicographical ordering.*

1.5 Definition. For a given ordering $<$ we define the *multidegree* of a monomial $m = x_{i_1}^{k_1} \cdots x_{i_j}^{k_j}$ as the k-tuple $(k_1, \ldots, k_j)$ and the *total degree* as $\sum\limits_{r=1}^{j} k_r$.
The (total) degree of a polynomial f is defined as the (total) degree of its leading monomial. We denote the total degree of f by $\deg_t(f)$ and the multidegree by $\deg(f)$.

1.2 Gröbner Bases and Normal Forms

1.6 Definition. Let $\mathbf{G} \subset \mathbb{K}\langle\mathbf{X}\rangle \setminus \{0\}$ and $\langle\mathbf{G}\rangle =: \mathbf{I}$. A *normal form* of $f \in \mathbb{K}\langle\mathbf{X}\rangle$ with respect to $\mathbf{G}$ is an element $g \in \mathbb{K}\langle\mathbf{X}\rangle$ such that $f - g \in \mathbf{I}$ and either $g = 0$ or $\mathfrak{lm}(g_i) \nmid \mathfrak{lm}(g)\ \forall g_i \in \mathbf{G}$. We denote a normal form of f with respect to $\mathbf{G}$ by $\mathfrak{NF}(f, \mathbf{G})$.
A subset $\mathbf{G} \subset \mathbf{I}$ is called a *Gröbner basis of $\mathbf{I}$* if the leading monomial of an arbitrary element in $\mathbf{I}$ is a multiple of the leading monomial of an element in $\mathbf{G}$. Equivalently, $\mathbf{G}$ is a Gröbner basis if $\langle\{\mathfrak{lm}(g) \mid g \in \mathbf{G}\}\rangle = \mathfrak{L}(\mathbf{I})$.

1.7 Remark. Note that a Gröbner basis always exists, since we can take $\mathbf{G} = \mathbf{I} \setminus \{0\}$. This is due to the fact that we do not demand our Gröbner basis to be finite. In fact there are some ideals, which do not posses a finite Gröbner basis, cf. 1.38. One can easily see the relevance of Gröbner bases: If $\mathbf{G}$ is a Gröbner basis of $\mathbf{I}$ then a normal form for $f \in \mathbf{I}$ is given by 0 and this is the only choice we have. However, neither the normal form nor the Gröbner basis are unique in general.

1.8 Example.

- If $\mathbf{G}$ is a Gröbner basis of an ideal $\mathbf{I}$ and $\mathbf{G} \neq \mathbf{I}$, then $\tilde{\mathbf{G}} := \mathbf{G} \cup \{g\},\ g \in \mathbf{I} \setminus \mathbf{G}$ is again a Gröbner basis.
- Take $B := \{x_2\} \subset \langle x_2 \rangle \trianglelefteq \mathbb{K}[x_1, x_2]$ with the degree lexicographical ordering with respect to $x_1 > x_2$ and consider $f = x_1$. Then $g_1 = x_1$ and $g_2 = x_1 - x_2$ are both normal forms of f with respect to B. Note that B is already a Gröbner basis for $\langle x_2 \rangle$.

Note that g_2 has terms which are contained in $\mathfrak{L}(\mathbf{I})$, which is the reason why we have two different normal forms.

1.9 Definition. A normal form $g = \sum\limits_{i=0}^{k} a_i t_i, \quad a_i \in \mathbb{K},\ t_i \in \mathbf{X}$ of $f \in \mathbb{K}\langle\mathbf{X}\rangle$ with respect to $\mathbf{G}$ is called *reduced*, if g is monic, that is, its leading coefficient is 1, and if $\mathfrak{lm}(g_w) \nmid t_i \quad \forall i = 0, \ldots, k,\ g_w \in \mathbf{G}$. We often speak about *the* normal form.

Before we solve our uniqueness problem, let us see the general idea on constructing normal forms.

1.10 Definition. Let $\{g_i \mid i \in \mathbb{J}, \mathbb{J}$ an arbitrary index set$\} = \mathbf{G} \subset \mathbb{K}\langle\mathbf{X}\rangle$ and $\langle\mathbf{G}\rangle =: \mathbf{I}$.

- Let $\tilde{\tau}_i :\ \mathbf{X} \ \rightarrow\ \mathbb{K}\langle\mathbf{X}\rangle$:
  $$x \mapsto \begin{cases} A(\mathfrak{lm}(g_i) - \mathfrak{lc}(g_i)^{-1} g_i)B, & \text{if } x = A\mathfrak{lm}(g_i)B \text{ for some } A, B \in \mathbf{X} \\ x & \text{otherwise} \end{cases}$$
  and let $\tau_i : \mathbb{K}\langle\mathbf{X}\rangle \ \rightarrow\ \mathbb{K}\langle\mathbf{X}\rangle$ be the $\mathbb{K}$-linear continuation of $\tilde{\tau}$. One calls τ_i a *reduction* with g_i.

- Let $f \in \mathbb{K}\langle \mathbf{X} \rangle$. One says that τ_i acts *trivially* on f, if the coefficient of $A\mathfrak{lm}(g_i)B$ is zero in f for all $A, B \in \mathbf{X}$. f is called *irreducible*, if all reductions act trivially on f.
  In other words $\tau_i(f) = f \; \forall i \in \mathbf{J}$.

1.11 Algorithm.

Input: An ideal $\mathbf{I} \trianglelefteq \mathbb{K}\langle \mathbf{X} \rangle$ with a given generating set $\mathbf{G} = \{g_i \mid i \in \mathbf{J}\}$, $f \in \mathbb{K}\langle \mathbf{X} \rangle$

Output: g, a reduced normal form of f w.r.t. $\mathbf{G}$

```
Set $g = f$.
while $\tau_i$ acts non-trivially on $g$ for some $i \in \mathbf{J}$ do
    $g = \tau_i(g)$;
end while;

return $g$;
```

1.12 Remark. By Definition 1.9, it is still not clear that the normal form is unique and in fact it is not. This is due to the fact that $\mathbf{G}$ is an arbitrary generating set and the construction of the normal form given in 1.11 depends on the choice of the reductor.

Furthermore it is not guaranteed that Algorithm 1.11 will terminate. We have to make further assumptions.

1.13 Definition.

- A finite sequence of reductions $\tau_{i_1}, \dots, \tau_{i_m}$ is said to be *final* on $f \in \mathbb{K}\langle \mathbf{X} \rangle$, if $\tau_{i_m} \circ \dots \circ \tau_{i_1}(f)$ is irreducible.

- An element $f \in \mathbb{K}\langle \mathbf{X} \rangle$ is called *reduction-finite*, if for any sequence $\{t_{i_j}\}_{j=1}^{\infty}$ of reductions there exists $m \in \mathbb{N}$, such that τ_{i_k} acts trivially on $\tau_{i_m} \circ \dots \circ \tau_{i_1}(f)$ for every $k > m$.

- An element $f \in \mathbb{K}\langle \mathbf{X} \rangle$ is called *reduction-unique*, if it is reduction-finite and if its images under all final sequences are the same.

1.14 Example. It is a good idea to see what happens in the commutative case, since it is a natural special case.

So assume $R = \mathbb{K}[x_1, \dots, x_n]$. All the definitions from above can be imported to R (in fact this is true for any sub- or factor algebra of $\mathbb{K}\langle \mathbf{X} \rangle$, see for example [GP02]).

Due to Hilbert's basis theorem R is Noetherian, that is, every ascending chain of ideals becomes stationary. Since for every $f \in R$ we have $\deg(\tau(f)) \leq \deg(f)$ for any reduction τ.

So for any given sequence of reductions $\{\tau_i\}_{i=1}^{\infty}$ with respect to $\mathbf{G}$ we have an ascending chain of ideals $\langle f + \mathbf{G} \rangle \trianglelefteq \langle \tau_1(f) + \mathbf{G} \rangle \trianglelefteq \langle \tau_2 \circ \tau_1(f) + \mathbf{G} \rangle \trianglelefteq \dots$, which

becomes stationary, that is there exists $m \in \mathbb{N}$, such that $\langle \tau_{i_{\tilde{m}}} \circ \cdots \circ \tau_{i_1}(f) + \mathbf{G} \rangle = \langle \tau_{i_m} \circ \cdots \circ \tau_{i_1}(f) + \mathbf{G} \rangle \quad \forall \tilde{m} \geq m$. So any $f \in R$ is reduction-finite.
Furthermore f is reduction-unique, if and only if $\mathbf{G}$ is a Gröbner basis. This is due to the fact that every remainder after division with $\mathbf{G}$ equals zero.

1.15 Lemma. Let $f \in \mathbb{K}\langle \mathbf{X} \rangle$ be reduction-finite. Then Algorithm 1.11 returns a reduced normal form $\tilde{f}$ of f after finitely many steps.
If f is even reduction-unique, then its normal form does not depend on the choices we have to make during the computation.

Proof: The termination of the algorithm is obvious. We have to show that $\tilde{f}$ is in fact a normal form of f.
Therefore we have to show that $f - \tau(f) \in \mathbf{I}$ for any reduction τ, because then $f - \tilde{f} \in \mathbf{I} = \langle \mathbf{G} \rangle$. Because of the definition of τ it is sufficient to prove the statement for monomials, so assume f is a monomial. If $\tau(f) = f$ there is nothing to prove, so assume otherwise, that is $f = A\mathfrak{lm}(g)B$ for some $A, B \in \mathbf{X}$, $g \in \mathbf{G}$. Since $\mathbb{K}$ is a field we may assume g is monic, as stated before. Therefore we have: $f - \tau(f) = A\mathfrak{lm}(g)B - \tau(A\mathfrak{lm}(g)B) = A\mathfrak{lm}(g)B - A(\mathfrak{lm}(g) - g)B = A(\mathfrak{lm}(g) - \mathfrak{lm}(g) + g)B = AgB \in \langle g \rangle \subset \mathbf{I}$.
Assume $\tilde{f}$ is not a reduced normal form, that is there exists $g \in \mathbf{G}$, such that $\mathfrak{lm}(g) \mid t$ for some monomial t occurring non-trivially in $\tilde{f}$. But then $t = A\mathfrak{lm}(g)B$ for some $A, B \in \mathbf{X}$ and the reduction τ_g acts non-trivially on $\tilde{f}$, which is a contradiction.
The last statement is clear by definition of reduction-uniqueness. q.e.d.

Now we have the potential to compute normal forms, but it is somehow vague, since we have to make many choices and cannot be sure about the uniqueness. Therefore we want to find a special Gröbner basis, such that the choices we have to make are minimal. First we note that a Gröbner basis is a special generating set.

1.16 Lemma. Let $\mathbf{G}$ be a Gröbner basis of a given ideal $\mathbf{I}$. Then $\mathbf{I} = \langle \mathbf{G} \rangle$.

Proof: Since $\mathbf{G} \subset \mathbf{I}$ we have $\langle \mathbf{G} \rangle \subset \mathbf{I}$, so take $f \in \mathbf{I} \setminus \langle \mathbf{G} \rangle$ with minimal degree, that is $f := \min\limits_{\deg(\tilde{f})} \{\tilde{f} \in \mathbf{I} \setminus \langle \mathbf{G} \rangle\}$ (the minimum exits because we assume that $<$ is a monomial ordering) and say without loss of generality that f is monic. By the definition of a Gröbner basis there exists $g \in \mathbf{G}$ such that $\mathfrak{lm}(g) \mid \mathfrak{lm}(f)$, say $\mathfrak{lm}(f) = A\mathfrak{lm}(g)B$ for some $A, B \in \mathbf{X}$. Then $\tilde{f} = f - AgB \in \mathbf{I}$ and $\deg(\tilde{f}) < \deg(f)$, so by minimality $\tilde{f} \in \langle \mathbf{G} \rangle$. But then $f = AgB + \tilde{f} = AgB + \sum\limits_{p \in P \subset \langle \mathbf{G} \rangle} a_p p b_p \in \langle \mathbf{G} \rangle$, which is a contradiction. q.e.d.

1.17 Definition. Let $\mathbf{G} \subset \mathbb{K}\langle\mathbf{X}\rangle$ and $\langle\mathbf{G}\rangle =: \mathbf{I}$.

- $\mathbf{G}$ is called *simplified* or *minimal* , if $\mathfrak{lm}(g) \notin \mathfrak{L}(\mathbf{G} \setminus \{g\}) \quad \forall g \in \mathbf{G}$.
- $\mathbf{G}$ is called *reduced* Gröbner basis, if $\mathbf{G}$ is simplified, a Gröbner basis and for every $g \in \mathbf{G}$ we have:
  1. g is monic.
  2. $g - \mathfrak{lm}(g)$ is in reduced normal form with respect to $\mathbf{I}$.

1.18 Remark. Note that we build the normal form with respect to $\mathbf{I}$. This is only a technical issue: in fact it would be absolutely equivalent, if we had demanded a normal form with respect to $\mathbf{G}$, since a Gröbner basis is a generating set and if a monomial is divisible by some leading monomial of a polynomial contained in $\mathbf{I}$, then it is divisible by a leading monomial of an element of the Gröbner basis. However, with this formulation the reduction of $g - \mathfrak{lm}(g)$ does not depend on the choice of the Gröbner basis.

1.19 Theorem. Fix an ordering $\leq$. For any ideal $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ consisting only of reduction-finite elements there exists a unique reduced Gröbner basis.

Proof:

- **Existence:**
  Let $\mathbf{F}$ be an arbitrary Gröbner basis. Without loss of generality we assume that all elements of $\mathbf{F}$ are monic. If $\mathbf{F}$ is not simplified, there exists $f \in \mathbf{F}$, such that $\mathfrak{lm}(f) \in \mathfrak{L}(\mathbf{F} \setminus \{f\})$, that is, $\mathbf{F} \setminus \{f\}$ is still a Gröbner basis. By iterating this step we find a simplified Gröbner basis after a countable number of steps.
  Assume now $\mathbf{F}$ is a monic, simplified Gröbner basis and take $f \in \mathbf{F}$. If $f - \mathfrak{lm}(f)$ is in reduced normal form we are finished. Otherwise we use Algorithm 1.11 to get an element $\tilde{f}$, which is the reduced normal form of $f - \mathfrak{lm}(f)$. (Note that the algorithm terminates, because $\mathbf{I}$ consists only of reduction-finite elements). Replace f by $g := \mathfrak{lm}(f) + \tilde{f}$ and call the new set $\tilde{\mathbf{G}}$. Then $\tilde{\mathbf{G}}$ is a simplified Gröbner basis, since $\mathfrak{lm}(g) = \mathfrak{lm}(f)$. If we do this iteratively we get a reduced Gröbner basis $\mathbf{G}$ after a countable number of steps.

- **Uniqueness:**
  Let $\mathbf{G}, \tilde{\mathbf{G}}$ be two reduced Gröbner bases. Take $\tilde{g} \in \tilde{\mathbf{G}} \setminus \mathbf{G}$. Since $\mathbf{G}$ is a Gröbner basis of $\mathbf{I}$ we have $\mathfrak{lm}(\tilde{g}) \in \mathfrak{L}(\langle\mathbf{G}\rangle)$ and $\tilde{g} = \sum\limits_f a_f f b_f$ for some $f \in \langle\mathbf{G}\rangle$. Assume $\mathfrak{lm}(\tilde{g}) \notin \{\mathfrak{lm}(g) \mid g \in \mathbf{G}\}$. Then there exists $g \in \mathbf{G}$, such that $\mathfrak{lm}(g) \mid \mathfrak{lm}(\tilde{g})$. But because $\tilde{\mathbf{G}}$ is a Gröbner basis as well there exists $\tilde{\tilde{g}} \in \tilde{\mathbf{G}}$, such that $\mathfrak{lm}(\tilde{\tilde{g}}) \mid \mathfrak{lm}(f)$, which implies that $\mathfrak{lm}(\tilde{\tilde{g}}) \mid \mathfrak{lm}(\tilde{g})$, and therefore, since $\tilde{G}$ is reduced, we have $\mathfrak{lm}(\tilde{\tilde{g}}) = \mathfrak{lm}(f) = \mathfrak{lm}(\tilde{g})$. Repeating

this step for an $g \in \mathbf{G} \setminus \tilde{\mathbf{G}}$ we get $\{\mathfrak{lm}(\tilde{g}) \mid \tilde{g} \in \tilde{\mathbf{G}}\} = \{\mathfrak{lm}(g) \mid g \in \mathbf{G}\}$. Take $\tilde{g} \in \tilde{\mathbf{G}}, g \in \mathbf{G}$, such that $\mathfrak{lm}(g) = \mathfrak{lm}(\tilde{g})$. Because $\tilde{g} - g \in \mathbf{I}$ there exists $f \in \mathbf{G}$, such that $\mathfrak{lm}(f) \mid \mathfrak{lm}(\tilde{g} - g)$. Because of $\deg(\tilde{g} - g) < \deg(g)$ we have $f \neq g$ and there exists $\tilde{g} \neq \tilde{f} \in \tilde{\mathbf{G}}$, such that $\mathfrak{lm}(\tilde{f}) = \mathfrak{lm}(f)$. Since $\mathfrak{lm}(f)$ does not divide any term of g, $\mathfrak{lm}(\tilde{g} - g)$ must be a term occurring in $\tilde{g}$, say $\tilde{t}$. But then $\mathfrak{lm}(\tilde{f}) = \mathfrak{lm}(f) \mid \tilde{t}$, a contradiction to the assumption that $\tilde{\mathbf{G}}$ is reduced. q.e.d.

1.20 Corollary. Let $\mathbf{G}$ be a simplified Gröbner basis of $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ consisting only of reduction-finite elements. Then all elements of $\{g - \mathfrak{lm}(g) \mid g \in \mathbf{G}\}$ are already reduction-unique.

Proof: This is a immediate consequence of Theorem 1.19. q.e.d.

1.21 Remark. The question arises, whether all elements of $\mathbb{K}\langle\mathbf{X}\rangle$ are reduction-unique with respect to a given reduced Gröbner basis, which would imply the existence of a unique normal form. The answer is yes, but to prove this we need some further knowledge.

1.3 The Gröbner Basis Algorithm

For this section we will always assume that our ideal $\mathbf{I}$ is finitely generated, due to the fact that we want to do some computations, which would be quite difficult if we start with an infinite generating set. Nevertheless this assumption is not necessary. Note that even with a finite generating set we may get a Gröbner basis which is infinite (see 1.38).
Again we may assume that all polynomials in a generating set are monic.

1.22 Definition. Let $\mathbf{G} = \{g_1, \ldots, g_\omega\} \subset \mathbb{K}\langle\mathbf{X}\rangle$.
We call a polynomial f *weak* with respect to $\mathbf{G}$, if $f = \sum_{k=1}^{\omega} \sum_j c_{k,j} l_{k,j} g_k r_{k,j}$, where $c_{k,j} \in \mathbb{K}$ and $l_{k,j}, r_{k,j} \in \mathbf{X}$ such that $l_{k,j}\mathfrak{lm}(g_k) r_{k,j} \leq \mathfrak{lm}(f) \; \forall k = 1, \ldots, \omega$.
Let $\mathbf{H} \subset \mathbb{K}\langle\mathbf{X}\rangle$. A polynomial f is called *reducible* from $\mathbf{H}$ with respect to $\mathbf{G}$, if weakness with respect to $\mathbf{G}$ of all elements of $\mathbf{H}$ implies weakness of f with respect to $\mathbf{G}$.

Note that weakness is a special form of generating f with elements of $\mathbf{G}$. Since it is allowed to use the same generator more than one time it should be allowed for weakness as well. For example the polynomial $p := xy + yx + xyx \in \langle y \rangle$ should be weak with respect to $\{y\}$.
If one wants to avoid the twin-sum in the definition of weakness one can consider the enveloping algebra $\mathbb{K}\langle\mathbf{X}\rangle \otimes \mathbb{K}\langle\mathbf{X}\rangle^{op}$, where $\mathbb{K}\langle\mathbf{X}\rangle^{op}$ denotes the *opposite* algebra, that is, $\mathbb{K}\langle\mathbf{X}\rangle$ endowed with the multiplication $a * b = b \cdot a \; \forall a, b \in \mathbb{K}\langle\mathbf{X}\rangle$.

Then $\mathbb{K}\langle\mathbf{X}\rangle$ is a $\mathbb{K}\langle\mathbf{X}\rangle \otimes \mathbb{K}\langle\mathbf{X}\rangle^{op}$ module and the action of $\mathbb{K}\langle\mathbf{X}\rangle \otimes \mathbb{K}\langle\mathbf{X}\rangle^{op}$ on $\mathbb{K}\langle\mathbf{X}\rangle$ is given by:

$$\mathbb{K}\langle\mathbf{X}\rangle \otimes \mathbb{K}\langle\mathbf{X}\rangle^{op} \times \mathbb{K}\langle\mathbf{X}\rangle \;\rightarrow\; \mathbb{K}\langle\mathbf{X}\rangle : \;(l \otimes r, p) \mapsto l \cdot p \cdot r$$

1.23 Definition. Let $\mathbf{G} = \{g_i \mid 1 \leq i \leq \omega\}$ be a set of monic polynomials. An *obstruction* of $\mathbf{G}$ is a six-tuple $(l, i, r; \lambda, j, \rho)$ with $1 \leq i, j \leq \omega$ and $l, r, \lambda, \rho \in \mathbf{X}$ such that $\mathfrak{lm}(g_i) \leq \mathfrak{lm}(g_j)$ and $l\mathfrak{lm}(g_i)r = \lambda\mathfrak{lm}(g_j)\rho$.
For any given obstruction we define the corresponding *S-polynomial* as
$s(l, i, r; \lambda, j, \rho) = lg_ir - \lambda g_j\rho$.
A set $\mathbf{D}$ of polynomials is called *basic* for $\mathbf{G}$ if every S-polynomial of $\mathbf{G}$ is reducible from $\mathbf{D}$ with respect to $\mathbf{G}$.

1.24 Motivation. Starting with a generating set for $\mathbf{I}$ the set of all non-weak S-polynomials will be a Gröbner basis.
This seems to be an easy way to compute a Gröbner basis, since one only has to compute all S-polynomials and check if they are weak or not. This procedure has the disadvantage that it would take forever, literally, since the set of all obstructions is infinite. So our medium-term issue is to discard most of these obstructions.

1.25 Lemma. Let $\mathbf{G} = \{g_i \mid 1 \leq i \leq \omega\}$ be a set of monic polynomials and $(l, i, r; \lambda, j, \rho)$ a *weak obstruction*, that is, the corresponding S-polynomial is weak with respect to $\mathbf{G}$. Then all obstructions $(\tilde{l}, i, \tilde{r}; \tilde{\lambda}, j, \tilde{\rho})$ with $\tilde{l} = w_1 l$, $\tilde{r} = rw_2$, $\tilde{\lambda} = w_1\lambda$ and $\tilde{\rho} = \rho w_2$, where w_1, w_2 are arbitrary monomials, are also weak.

Proof: Set $s := s(l, i, r; \lambda, j, \rho)$ and $\tilde{s} := s(\tilde{l}, i, \tilde{r}; \tilde{\lambda}, j, \tilde{\rho})$. Because the obstruction is weak we can write $s = lg_ir - \lambda g_j\rho = \sum\limits_{k=1}^{\omega}\sum\limits_{l} c_{k,l}l_{k,l}g_kr_{k,l}$ with $c_{k,l} \in \mathbb{K}, l_{k,l}, r_{k,l} \in \mathbf{X}$, $l_{k,l}\mathfrak{lm}(g_k)r_{k,l} \leq \mathfrak{lm}(s)\ \forall k = 1, \ldots, \omega$. Now we have $\tilde{s} = \tilde{l}g_i\tilde{r} - \tilde{\lambda}g_j\tilde{\rho} = w_1(lg_ir - \lambda g_j\rho)w_2 = w_1sw_2 = w_1(\sum\limits_{k=1}^{\omega}\sum\limits_{l} c_{k,l}l_{k,l}g_kr_{k,l})w_2 = \sum\limits_{k=1}^{\omega}\sum\limits_{l} c_{k,l}\tilde{l}_{k,l}g_k\tilde{r}_{k,l}$ with
$\tilde{l}_{k,l} = w_1l_{k,l}$ and $\tilde{r}_{k,l} = r_{k,l}w_2$.
Furthermore we see that $\tilde{l}_{k,l}\mathfrak{lm}(g_k)\tilde{r}_{k,l} \leq w_1\mathfrak{lm}(s)w_2 = \mathfrak{lm}(\tilde{s})$, which shows that $\tilde{s}$ is weak with respect to $\mathbf{G}$. q.e.d.

So *multiples* of obstructions need not be considered. However the set we have to consider is still infinite. But the lemma helps us to prove our claim in 1.24.

1.26 Theorem. For a set $\mathbf{G}$ of polynomials generating an ideal $\mathbf{I}$ of $\mathbb{K}\langle\mathbf{X}\rangle$, the following statements are equivalent:

(i) $\mathbf{G}$ is a Gröbner basis.

(ii) The reduced normal form of each polynomial in $\mathbf{I}$ is equal to 0.

(iii) Each S-polynomial of $\mathbf{G}$ is weak with respect to $\mathbf{G}$.

(iv) The empty set is a basic set for $\mathbf{G}$.

Proof:
$(i) \Longrightarrow (ii)$: Induction with respect to the monomial ordering $<$:
The normal form of 0 equals 0. Take $0 \neq f \in \mathbf{I}$ and assume f is monic. Since $\mathbf{G}$ is a Gröbner basis there exists $g \in \mathbf{G}$ such that $\mathfrak{lm}(g) \mid \mathfrak{lm}(f)$, that is, $\exists l, r \in \mathbf{X}: \ l\mathfrak{lm}(g)r = \mathfrak{lm}(f)$. Because of $f, g \in \mathbf{I}$ we have $\tilde{f} := f - lgr \in \mathbf{I}$ and $\deg(\tilde{f}) < \deg(f)$. By the induction hypothesis, the normal form of $\tilde{f}$ equals zero and we obtain that the normal form of f equals zero as well.
$(ii) \Longrightarrow (iii)$: Suppose $s = s(l, i, r; \lambda, j, \rho)$. By assumption the normal form of s with respect to $\mathbf{G}$ equals 0, so s is weak by the definition of weakness.
$(iii) \Longleftrightarrow (iv)$: Clear by definition.
$(iii) \Longrightarrow (i)$: Suppose $f \in \mathbf{I}$, but $\mathfrak{lm}(f) \notin \langle \{\mathfrak{lm}(g) \mid g \in \mathbf{G}\}\rangle$ and $\mathfrak{lm}(f)$ is minimal with respect to $<$. Now there are at least two polynomials $g_i, g_j \in \mathbf{G}$, $g_i \neq g_j$, such that $f = \sum\limits_l c_{i,l} l_{i,l} g_i r_{i,l} + \sum\limits_l c_{j,l} l_{j,l} g_j r_{j,l} + \sum\limits_{g_k \in \mathbf{G}, g_k \neq g_i, g_j} \sum\limits_l c_{k,l} l_{k,l} g_k r_{k,l}$, $c_{k,l} \in \mathbb{K}$, $l_{k,l}, r_{k,l} \in \mathbf{X} \ \forall k$ and $t := \mathfrak{lm}(\sum\limits_l l_{i,l} g_i r_{i,l}) = \mathfrak{lm}(\sum\limits_l l_{j,l} g_j r_{j,l}) > \mathfrak{lm}(f)$.
Now by assumption $s := s(\mathfrak{lm}(l_{i,l}), i, \mathfrak{lm}(r_{i,l}); \mathfrak{lm}(l_{j,l}), j, \mathfrak{lm}(r_{j,l}))$ is weak and $s = \sum\limits_{k \in \mathbb{J}} \sum\limits_l a_{k,l} g_k b_{k,l}$, where $\mathbb{J}$ is an arbitrary set of indices and $g_k \in \mathbf{G}$, such that all leading terms of g_k are smaller than t. Then $f = \sum\limits_l \mathfrak{lc}(l_{i,l} r_{i,l}) \mathfrak{lc}(l_{j,l} r_{j,l})^{-1} l_{j,l} g_j r_{j,l} + \sum\limits_l \mathfrak{lc}(l_{i,l} r_{i,l}) \sum\limits_{k \in \mathbb{J}} a_{k,l} g_k b_{k,l} + \sum\limits_{h \neq i,j} \sum\limits_l l_{h,l} g_h r_{h,l}$ is an expression of f with fewer summands with leading term equal to t. If we do this iteratively until we have only one term equal to t left, we reach a contradiction and we can conclude that $\mathbf{G}$ is a Gröbner basis. q.e.d.

Note that the generating set is not taken to be finite. If we do not enumerate the polynomials in a generating set $\mathbf{G}$, we often write $(l, g, r; \lambda, p, \rho)$ for the obstruction of $g, p \in \mathbf{G}$.
Now we focus on finding a finite set of obstructions, from which we can construct a Gröbner basis. Therefore we introduce the concept of overlap.

1.27 Definition. We say two monomials $t_1, t_2 \in \mathbf{X}$ have *overlap* $b \in \mathbf{X}$ or *overlap at* $b \in \boldsymbol{X}$ if there are $a, c \in \mathbf{X}$ such that $t_1 = ab$ and $t_2 = bc$ or $t_1 = ba$ and $t_2 = cb$ or $t_1 = b$ and $t_2 = abc$. If 1 is the only overlap between t_1 and t_2 we say the monomials have *no overlap*. Equivalently the monomials are called *coprime*
An obstruction $(l, i, r; \lambda, j, \rho)$ is said to have *no overlap* if there exists $w \in \mathbf{X}$ such that $l\mathfrak{lm}(g_i)r = l\mathfrak{lm}(g_i)w\mathfrak{lm}(g_j)\rho$ or $l\mathfrak{lm}(g_i)r = \lambda\mathfrak{lm}(g_j)w\mathfrak{lm}(g_i)r$.

1.28 Example. Suppose $g_1, g_2 \in \mathbb{K}\langle x_1, x_2, x_3\rangle$ with $\mathfrak{lm}(g_1) = x_1x_2$ and $\mathfrak{lm}(g_2) = x_2x_3$. Then the only overlap between these monomials is x_2. It is easy to see, that the obstruction $(1, 1, x_2^\alpha x_3; x_1x_2^\alpha, 2, 1)$ has no overlap (take $w = x_2^{\alpha-1}$).

The more important question arises: Is the converse true?

1.29 Lemma (Product Criterion)**.** Let $g_1, g_2 \in \mathbb{K}\langle\mathbf{X}\rangle$ be such that $l_1 := \mathfrak{lm}(g_1)$ and $l_2 := \mathfrak{lm}(g_2)$ have no overlap. Then every obstruction $(l, g_1, r; \lambda, g_2, \rho)$ with $l, r, \lambda, \rho \in \mathbf{X}$ has no overlap.

Proof: Since l_1 and l_2 have no overlap $\mathfrak{lm}(lg_1r) = \mathfrak{lm}(\lambda g_2 \rho)$ implies that either ll_1 and λ or l_1r and ρ have overlap l_1.
Assume the first case is true. Then r and l_2 overlap at l_2, say $r = l_2\overline{r}$. Then $\overline{r} = \rho$ and therefore $ll_1r = ll_1l_2\overline{r} = ll_1l_2\rho$ which shows that $(l, g_1, r; \lambda, g_2, \rho)$ has no overlap.
Now if l_1r and ρ overlap at l_1 then l and λl_2 have overlap l_2 and $l = \overline{l}l_2 = \lambda l_2$. Hence we get $ll_1r = \lambda l_2 l_1 r$ and again we obtain that $(l, g_1, r; \lambda, g_2, \rho)$ has no overlap. q.e.d.

1.30 Theorem. Let $\mathbf{G} = \{g_i \mid i = 1, \ldots, \omega\} \subset \mathbb{K}\langle\mathbf{X}\rangle$. Every obstruction without overlap is reducible from an S-polynomial with overlap with respect to $\mathbf{G}$.

Proof: Let $b = (l, i, r; \lambda, j, \rho)$ be an obstruction without overlap and denote by s its S-polynomial. Since $l\mathfrak{lm}(g_i)r = \lambda\mathfrak{lm}(g_j)\rho$ we have either $r = w\mathfrak{lm}(g_j)\rho$ or $l = \lambda\mathfrak{lm}(g_i)w$.
If the former is valid then we also have $\lambda = l\mathfrak{lm}(g_i)w$ and by Lemma 1.25 $b = (l, i, w\mathfrak{lm}(g_j)\rho; l\mathfrak{lm}(g_i)w, j, \rho)$ is reducible from $(1, i, w\mathfrak{lm}(g_j); \mathfrak{lm}(g_i)w, j, 1)$. Therefore we assume $l = \rho = 1$.
Write $g_i = \sum_h c_h t_h,\ g_j = \sum_p d_p u_p$ with $t_h, u_p \in \mathbf{X},\ c_h, d_p \in \mathbb{K} \setminus \{0\}$, such that $t_h > t_{h+1}$ and $u_p > u_{p+1}$. Now $s = g_i r - \lambda g_j = g_i w\mathfrak{lm}(g_j) - \mathfrak{lm}(g_i)wg_j = g_i w(g_j - \sum_{p,p\neq 1} d_p u_p) - (g_i - \sum_{h,h\neq 1} c_h t_h)wg_j = \sum_{h,h\neq 1} c_h t_h w g_j - \sum_{p,p\neq 1} d_p g_i w u_p$. Assume $c_2t_2wu_1 = d_2t_1wu_2$, that is the leading terms $t_2w\mathfrak{lm}(g_j)$ and $\mathfrak{lm}(g_i)wu_2$ of the two summations cancel each other. Since $t_2 < t_1$ and $u_2 < u_1$ this only occurs if $c_2 = d_2$ and there are $v_1, v_2 \in \mathbf{X}$, such that $t_1 = t_2v_1$ and $u_1 = v_2u_2$ with $v_1w = wv_2$. If w is a left divisor of v_1, say $v_1 = wv_1'$, then $v_2 = v_2'w$, which implies that $v_1' = v_2'$ and therefore $(1, i, w\mathfrak{lm}(g_j); \mathfrak{lm}(g_i)w, j, 1)$ is reducible from $(1, i, v_1'\mathfrak{lm}(g_j); \mathfrak{lm}(g_i)v_1', j, 1)$ by Lemma 1.25. If w is not a left divisor of v_1, then w has a selfoverlap, that is, $w = v_1w' = w'v_2$. and again we apply Lemma 1.25. So we may assume $w = 1$ that is, $b = (1, i, \mathfrak{lm}(g_j); \mathfrak{lm}(g_i), j, 1)$. We find

$$\begin{aligned} s = g_i\mathfrak{lm}(g_j) - \mathfrak{lm}(g_i)g_j &= lm(g_i)\mathfrak{lm}(g_j) + \sum_{h,h\neq 1} c_h t_h \mathfrak{lm}(g_j) - lm(g_i)\mathfrak{lm}(g_j) \\ - \sum_{p,p\neq 1} \mathfrak{lm}(g_i) d_p u_p &= \sum_{h,h\neq 1} c_h t_h (g_j - \sum_{p,p\neq 1} d_p u_p) - \sum_{p,p\neq 1} (g_i - \sum_{h,h\neq 1} c_h t_h) d_p u_p \\ &= (\sum_{h,h\neq 1} c_h t_h) g_j - g_i (\sum_{p,p\neq 1} d_p u_p) \in \langle g_i, g_j \rangle, \end{aligned}$$

so s is weak with respect to $\mathbf{G}$, which implies that it is reducible from $\mathbf{G}$. q.e.d.

The theorem states: If an S-polynomial $s(l, g_i, r; \lambda, g_j, \rho)$ is not weak with respect to $\mathbf{G}$, then the leading monomials of the two polynomials g_i and g_j have an overlap. This will help us to find a finite basic set.

1.31 Lemma. Let $\mathbf{G} = \{g_i \mid i = 1, \ldots, \omega\} \subset \mathbb{K}\langle\mathbf{X}\rangle$. There is a finite basic set $\mathbf{D}$ of S-polynomials of $\mathbf{G}$, such that every S-polynomial of $\mathbf{G}$ in $\mathbf{D}$ corresponds to an obstruction $(l, i, r; \lambda, j, \rho)$ with overlap and with either one of the two parameters $\{l, \lambda\}$ and one of $\{r, \rho\}$ equal to 1 or $\lambda = \rho = 1$.

Proof: We write $s = s(l, i, r; \lambda, j, \rho)$, $\mathfrak{lm}(g_i) = m_1 \ldots m_p$ and $\mathfrak{lm}(g_j) = n_1 \ldots n_q$ with $m_k, n_{\tilde{k}} \in \mathbf{X}$ of degree 1, $k = 1, \ldots, p; \tilde{k} = 1, \ldots, q$ (this means that each m_k and $n_{\tilde{k}}$ corresponds to an $x_i, i = 1, \ldots, n$). Now if s is not weak, then it must have some overlap. In particular, $\mathfrak{lm}(g_i)$ and $\mathfrak{lm}(g_j)$ must overlap. This can occur in three ways:

$$\begin{aligned} m_1 \cdots m_h &= n_{q-h+1} \cdots n_q, && 1 \leq h < p, \\ n_1 \cdots n_h &= m_{p-h+1} \cdots m_p, && 1 \leq h < p, \\ m_1 \cdots m_p &= n_{h+1} \cdots n_{h+p}, && 1 \leq h < q - p. \end{aligned}$$

In particular, for every two polynomials the number of possible overlaps is finite. We show that $\mathbf{D}$ needs to contain at most one S-polynomial for every overlap, which completes the proof. Assume $\mathfrak{lm}(g_i)$ and $\mathfrak{lm}(g_j)$ have nontrivial overlap. To satisfy the equation $l\mathfrak{lm}(g_i)r = \lambda\mathfrak{lm}(g_j)\rho$, the factors that are not in the overlap have to be in λ or ρ respectively in l or r (cf. proof of Lemma 1.29). So for every obstruction corresponding to some overlap the monomials $l\mathfrak{lm}(g_i)r$ and $\lambda\mathfrak{lm}(g_j)\rho$ have to be equal to $\tilde{l}w\tilde{r}$ and $\tilde{\lambda}w\tilde{\rho}$, respectively, with w equal to

$$\begin{aligned} w &= n_1 \cdots n_{q-h}\mathfrak{lm}(g_i) &&= \mathfrak{lm}(g_j)m_{h+1} \cdots m_p, \\ w &= \mathfrak{lm}(g_i)n_{h+1} \cdots n_q &&= m_1 \cdots m_{p-h}\mathfrak{lm}(g_j), \\ w &= n_1 \cdots n_h\mathfrak{lm}(g_i)n_{h+p+1} \cdots n_q &&= \mathfrak{lm}(g_j), \end{aligned}$$

in the respective cases. Now by Lemma 1.25 these obstructions are weak except when $\tilde{l} = \tilde{r} = \tilde{\lambda} = \tilde{\rho} = 1$. So for every possible overlap there exists a single S-polynomial such that all other obstructions are reducible from it with respect to $\{g_i, g_j\}$; in the respective cases, the corresponding obstructions are

$$\begin{gathered} (n_1 \cdots n_{q-h}, i, 1; 1, j, m_{h+1} \cdots m_p), \\ (1, i, n_{h+1} \cdots n_q; m_1 \cdots m_{p-h}, j, 1), \\ (n_1 \cdots n_h, i, n_{h+p+1} \cdots n_q; 1, j, 1). \end{gathered}$$

This means that s need only to be in $\mathbf{D}$ if at least one of the two parameters l and λ and one of the two parameters r and ρ are equal to 1. q.e.d.

We refer to the S-polynomials of g and $\tilde{g}$, we have to consider, as $S(g, \tilde{g})$.

We distinguish between three kinds of obstructions:

1.32 Definition. Let $s = (l, i, r; \lambda, j, \rho)$ be an obstruction of the set $\mathbf{G} = \{g_i \mid 1 \leq i \leq \omega\}$ of monic polynomials in $\mathbb{K}\langle\mathbf{X}\rangle$.

- If $l = 1$, then we call s a *right obstruction*.
- If $l \neq 1$ and $r = 1$, then we call s a *left obstruction*.
- If s is not a right nor a left obstruction and $\lambda = \rho = 1$, then we call s a *central obstruction*.

1.33 Corollary. Let $\mathbf{G}$ be a set of polynomials in $\mathbb{K}\langle\mathbf{X}\rangle$ and let $\mathbf{D}$ be the set of all non-zero normal forms of S-polynomials with respect to $\mathbf{G}$ corresponding to all left, right and central obstructions of $\mathbf{G}$. Then $\mathbf{D}$ is a basic set for $\mathbf{G}$.

Proof: This is exactly the statement of 1.31. q.e.d.

In Definition 1.32 the restriction to a finite set $\mathbf{G}$ is not necessary, since an obstruction includes only two polynomials. However, as stated before, for "real-life" computations finiteness is required and so we will assume for the rest of this section that $\mathbf{G} = \{g_i \mid 1 \leq i \leq \omega\}$.

The overlaps given in 1.32 are also called *ambiguities*, since Bergman used this term in his famous work [Ber78]. Because one of the goals of this work is to translate the Diamond Lemma into a modern language we will stick to the term overlap. But before we come to this matter we introduce an algorithm that computes a reduced Gröbner basis.

1.34 Definition. Let $\mathbf{I}$ be a two-sided ideal of $\mathbb{K}\langle\mathbf{X}\rangle$ and let $\mathbf{G}$, $\mathbf{D}$ be subsets of $\mathbb{K}\langle\mathbf{X}\rangle$. We say that ($\mathbf{G}$,$\mathbf{D}$) is a *partial Gröbner pair* for $\mathbf{I}$ if the following properties are satisfied:

1. All polynomials in $\mathbf{G} \cup \mathbf{D}$ are monic.
2. $\mathbf{G}$ is a generating set of $\mathbf{I}$.
3. Every element of $\mathbf{D}$ belongs to $\mathbf{I}$ and it is in normal form with respect to the polynomials in $\mathbf{G}$.
4. The set $\mathbf{D}$ is basic for $\mathbf{G}$.
5. For every $f \in \mathbf{G}$ the normal form with respect to $\mathbf{G} \cup \mathbf{D}$ of the normal form with respect to $\mathbf{G} \setminus \{f\}$ equals zero.

1.35 Remark. Let $\mathbf{I}$ be a two-sided ideal in $\mathbb{K}\langle\mathbf{X}\rangle$ and let ($\mathbf{G}$,$\mathbf{D}$) be a partial Gröbner pair for $\mathbf{I}$. If $\mathbf{D}$ is the empty set, then $\mathbf{G}$ is a Gröbner basis.

Since $\mathbb{K}\langle\mathbf{X}\rangle$ is not Noetherian, for example the ideal $\langle x_1 x_2^n x_1 \mid n \in \mathbb{N}\rangle$ can not be finitely generated, our algorithm may not terminate in all cases. However, we will see later that we can use this algorithm to get some important results after finitely many steps.

1.36 Algorithm.

Input: a (finite) generating set $\mathbf{G}$ for $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$

Output: a reduced Gröbner basis for $\mathbf{I}$

Compute all non-zero normal forms of S-polynomials with respect to $\mathbf{G}$ corresponding to all left, right and central obstructions of $\mathbf{G}$ and call the resulting set $\mathbf{D}$. Then ($\mathbf{G}$,$\mathbf{D}$) is a partial Gröbner pair. Construct a new partial Gröbner pair $(\tilde{\mathbf{G}}, \tilde{\mathbf{D}})$ as follows:

1. Take $f \in \mathbf{D}$ and set $\tilde{\mathbf{G}} = \{g_1, \dots, g_\omega, g_{\omega+1} := f\}$.

2. Compute the left, right and central obstructions of $\tilde{\mathbf{G}}$ of the form $(l, i, r; \lambda, \omega+1, \rho)$ and $(l, \omega+1, r; \lambda, j, \rho)$ for certain $i, j \in \{1, \dots, \omega\}$ and $l, r, \lambda, \rho \in \mathbf{X}$ and put the non-zero normal forms of their S-polynomials with respect to $\mathbf{G} \cup \mathbf{D}$ in $\mathbf{D}$, such that $\mathbf{D}$ becomes a basic set for $\tilde{\mathbf{G}}$. Call this new basic set $\tilde{\mathbf{D}}$.

3. For each $i \in \{1, \dots, \omega\}$ compute the normal form g_i' with respect to $\tilde{\mathbf{G}} \setminus \{g_i\}$ of g_i. If $g_i' = 0$ remove g_i from $\tilde{\mathbf{G}}$. Otherwise, if g_i' is distinct from g_i,

   a) replace g_i by g_i';

   b) compute the left, right and central obstructions of the new $\tilde{\mathbf{G}}$ involving g_i';

   c) if the normal form with respect to $\tilde{\mathbf{G}} \cup \tilde{\mathbf{D}}$ of an S-polynomial of such an obstruction is non-zero then add its normal form to $\tilde{\mathbf{D}}$.

4. Replace each $d \in \tilde{\mathbf{D}}$ by its normal form with respect to $(\tilde{\mathbf{G}} \cup \tilde{\mathbf{D}}) \setminus \{d\}$.

1.37 Theorem. In the situation of 1.36, the ideal generated by the leading monomials of $\mathbf{G}$ is strictly contained in the ideal generated by the leading monomials of $\tilde{\mathbf{G}}$. If $\tilde{\mathbf{D}} = \emptyset$ then $\tilde{\mathbf{G}}$ is a Gröbner basis for $\mathbf{I}$ (and the routine stops).

Proof: First we have to show that $(\tilde{\mathbf{G}}, \tilde{\mathbf{D}})$ is a partial Gröbner pair, which means we have to verify condition one to five of Definition 1.34.
Since all polynomials in $\tilde{\mathbf{G}}$ and $\tilde{\mathbf{D}}$ are normal forms, they are monic, we get condition 1.
If $g_i \in \tilde{\mathbf{G}}$ adjusted as in step 4 of the algorithm, then the ideal generated by $\{g_i'\} \cup (\mathbf{G} \setminus \{g_i\})$ coincides with $\mathbf{I}$, so we get condition 2.
Clearly all elements of $\tilde{\mathbf{D}}$ belong to $\mathbf{I}$ and are in normal form with respect to $\tilde{\mathbf{G}}$ and this is condition 3.
Because of 1.33, $\tilde{\mathbf{D}}$ is a basic set for $\mathbf{G}$ and hence condition 4.
For every element $g \in \tilde{\mathbf{G}} \setminus \mathbf{G}$, the normal forms of the newly computed central obstructions of $\mathbf{G}$ involving g take care of condition 5.
That $\mathfrak{L}(\mathbf{G}) \subset \mathfrak{L}(\tilde{\mathbf{G}})$ is valid follows immediately from the construction we have made.
The final assertion is a consequence of Remark 1.35. q.e.d.

1.38 Example. For all examples we take the lexicographical ordering with $x_1 > x_2 > \ldots > x_n$ or $x > y > z$ respectively.

- Take $\mathbb{K}\langle x, y\rangle$ and $\mathbf{G}_1 = \{xyx + y^2\}$.
  There is only one obstruction to consider, since the only central obstruction are the trivial ones and every left obstruction is equal to a right obstruction, namely $(xy, 1, 1; 1, 1, yx) = xy^3 - y^3x$. $\Longrightarrow \mathbf{D}_1 = \{xy^3 - y^3x\}$.
  Now $\mathbf{G}_2 = \{xyx + y^2, xy^3 - y^3x\}$, since $xy^3 - y^3x$ is in normal form with respect to g_1.
  Because our new g_2 only has trivial obstruction with itself, there is only one new obstruction: $(1, 1, y^3; xy, 2, 1) = y^5 + xy^4x$, which has normal form 0 with respect to $\mathbf{G}_2$, so $\mathbf{G}_2$ is a Gröbner basis for $\mathbf{I} = \langle \mathbf{G}_1\rangle$.

- Take $\mathbf{G} = \{x_ix_j - x_jx_i \mid 1 \leq i < j \leq n\} \subset \mathbb{K}\langle \mathbf{X}\rangle$. We claim that $\mathbf{G}$ is already a Gröbner basis.
  The only non-trivial overlaps are given by the polynomials $x_ix_j - x_jx_i$ and $x_jx_w - x_wx_j$, where $1 \leq i < j < w \leq n$. The S-polynomial can be computed by $(x_ix_j - x_jx_i)x_w - x_i(x_jx_w - x_wx_j) = x_ix_wx_j - x_jx_ix_w$ which reduces to zero, using the leading monomials of $x_ix_w - x_wx_i$, $x_jx_w - x_wx_j$ and $x_ix_j - x_jx_i \in \mathbf{G}$.
  Note that $\mathbf{G}$ generates the *commutator ideal*, so we have $\mathbb{K}[x_1, \ldots, n] = \mathbb{K}\langle \mathbf{X}\rangle / \langle \mathbf{G}\rangle$.

- Let us consider the generating set $B = \{yzxy - xyzx, zxyz - xyzx, zxyz - yzxy\} \subseteq \mathbb{K}\langle x, y, z\rangle$, which consists of *braid relations* (cf. [Gar07]). Then the unique reduced Gröbner basis is given by $G = \{yzxy - zxyz, xyzx - zxyz, xzxyz - zxyzy, yz^nxyz - zxyz^2x^{n-1}, xz^nxyz - zxyzyx^{n-1} \mid n \in \mathbb{N}\}$. Obviously, none of the elements of G is redundant.
  To see that G is in fact a Gröbner basis one has to consider all pairs (g_i, g_j) of elements of G and check if all possible obstructions of (g_i, g_j) vanish to zero. We demonstrate this for $w_1 := yz^nxyz - zxyz^2x^{n-1}$ and $w_2 := yz^mxyz - zxyz^2x^{m-1}$ for arbitrary $n, m \in \mathbb{N}$. We only have to worry about the right overlap, since n and m are arbitrary elements in $\mathbb{N}$ (so we can exchange their places for the left overlap). Now w_1 and w_2 overlap at yz and we have:

$$\begin{aligned}
&(yz^nxyz - zxyz^2x^{n-1})\cdot z^{m-1}xyz - yz^nx\cdot(yz^mxyz - zxyz^2x^{m-1})\\
&= \qquad\qquad -zxyz^2x^{n-1}z^{m-1}xyz + yz^nxzxyz^2x^{m-1}\\
&\xrightarrow{xzxyz-zxyzy} \qquad yz^{n+1}xyzyzx^{m-1} - zxyz^2x^{n-1}z^{m-1}xyz\\
&\xrightarrow{yz^{n+1}xyz-zxyz^2x^n} \qquad zxyz^2x^nyzx^{m-1} - zxyz^2x^{n-1}z^{m-1}xyz\\
&\xrightarrow{xyzx-zxyz} \qquad zxyz^2x^{n-1}zxyzx^{m-2} - zxyz^2x^{n-1}z^{m-1}xyz\\
&\xrightarrow{xyzx-zxyz} \qquad zxyz^2x^{n-1}z^2xyzx^{m-3} - zxyz^2x^{n-1}z^{m-1}xyz\\
&\xrightarrow{xz^2xyz-zxyzyx} \qquad zxyz^2x^{n-2}zxyzyx^{m-2} - zxyz^2x^{n-1}z^{m-1}xyz\\
&\xrightarrow{xzxyz-zxyzy} \qquad zxyz^2x^{n-3}zxyzy^2x^{m-2} - zxyz^2x^{n-1}z^{m-1}xyz\\
&\xrightarrow{xz^{m-1}xyz-zxyzyx^{m-2}} \qquad zxyz^2x^{n-3}zxyzy^2x^{m-2} - zxyz^2x^{n-2}zxyzyx^{m-2}\\
&\xrightarrow{xzxyz-zxyzy} \qquad 0.
\end{aligned}$$

1.4 The Diamond Lemma

We now state our version of the Diamond Lemma, which will give us a uniquely determined normal form in certain situations. We will see that the assumptions we have to make are mostly for ensuring the existence of a reduced Gröbner basis.

1.39 Definition. An ordering $<$ is said to fulfill the *descending chain condition* if every descending chain of monomials (with respect to $<$) becomes stationary. Equivalently one says that $<$ is *Artinian* or *well-founded*.

Note that if $<$ fulfills the descending chain condition every element of $\mathbb{K}\langle\mathbf{X}\rangle$ is reduction-finite. Recall that we always assume we have a monomial ordering, in particular, we have a well-ordering, which implies that the ordering is Artinian.

1.40 Lemma. For a given subset $\mathbf{G} \subset \mathbb{K}\langle\mathbf{X}\rangle$ we have:

(i) The set of reduction-unique elements of $\mathbb{K}\langle\mathbf{X}\rangle$ (w.r.t. $\mathbf{G}$) forms a $\mathbb{K}$-subspace of $\mathbb{K}\langle\mathbf{X}\rangle$ and we have an $\mathbb{K}$-linear map $r_{\mathbf{G}}$ from this subspace into $\mathbb{K}\langle\mathbf{X}\rangle_{irr}$, the set of all irreducible elements of $\mathbb{K}\langle\mathbf{X}\rangle$.

(ii) Suppose $a, b, c \in \mathbb{K}\langle\mathbf{X}\rangle$ are such that for all monomials A, B, C occurring with non-zero coefficient in a, b, c, respectively, the product ABC is reduction-unique. (In particular this implies that abc is reduction-unique.) Let r be any finite composition of reductions. Then $ar(b)c$ is reduction-unique, and $r_{\mathbf{G}}(ar(b)c) = r_{\mathbf{G}}(abc)$.

Proof:

(i) Define $r_{\mathbf{G}}$ as the linear continuation of the map, that maps any given reduction-unique element to its uniquely determined reduced normal form. Let $a, b \in \mathbb{K}\langle\mathbf{X}\rangle$ be reduction-unique and take $k \in \mathbb{K}$. Then $ka + b$ is reduction-finite, since reductions are linear maps and a and b are reduction-finite.

Let r be a composition of reductions, such that r is finite on $ka + b$. Since a is reduction-unique there exists a composition with reduction r', such that $r'r(a) = r_{\mathbf{G}}(a)$ and similar there is r'', such that $r''r'r(b) = r_{\mathbf{G}}(b)$. Because $r(ka + b)$ is irreducible, we have $r(ka + b) = r''r'r(ka + b) = k \cdot r''r'r(a) + r''r'r(b) = kr_{\mathbf{G}}(a) + r_{\mathbf{G}}(b)$ and our claim follows.

(ii) By (i) it suffices to prove the claim for $a, b, c \in \mathbf{X}$ and a single reduction r. But then we have $ar(b)c = r(abc)$ and hence it is reduction-unique if and only if abc is, with the same reduced normal form. q.e.d.

Again the only challenge we meet is given by monomials involving an overlap: Assume we have three monomials A, B, C and consider AB and BC, such that these monomials have overlap B. Recall that reductions were defined for monomials. Therefore there might exist a reduction for AB and a different one for BC (assume $A \neq 1 \neq C$), say τ and σ. Then $\tau(ABC) \neq \sigma(ABC)$ and we have two different ways to reduce ABC.

1.41 Definition. Assume $A, B, C \in \mathbf{X}$. Consider AB and BC and let τ be a reduction on AB and σ be an reduction on BC. The overlap is called *resolvable* if there exist two compositions of reductions r and r', such that $r(\tau(ABC)) = r'(\sigma(ABC))$.
This is also known as the *diamond condition.*

1.42 Remark. The name *diamond condition* is taken from the field of graph theory, where the Diamond Lemma was stated first. It refers to the fact that for every two different edges τ, σ starting from the same vertex v there will be paths r and r' such that $r \circ \tau(v) = r' \circ \sigma(v)$, thus the paths forming a diamond as illustrated in Figure 1.1. But since graphs will be our matter in the next chapter we stick to the formulation within terms of the free algebra.

1.43 Definition. Assume $\mathbf{G} \subset \mathbb{K}\langle\mathbf{X}\rangle$. The set of all reductions defined by $\mathbf{G}$ (cf. 1.10) is called *reduction system.*
We refer to the overlaps occurring in the leading monomials of $\mathbf{G}$ as the *overlap of the reduction system* $\boldsymbol{G}$.

This is merely a renaming. The intention is rather obvious: With a given Gröbner basis $\mathbf{G}$ we want to reduce all polynomials to a normal form, therefore we may call $\mathbf{G}$ reduction system. The Diamond Lemma gives us now a condition for

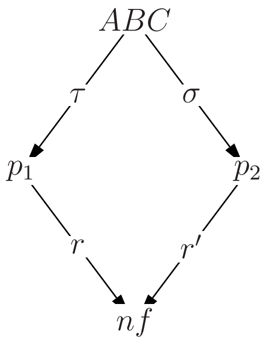


Figure 1.1: The Diamond Graph

uniqueness of the reduced normal form, namely the diamond condition. Recall that we have defined the normal form with respect to an arbitrary subset of $\mathbb{K}\langle\mathbf{X}\rangle$.

However in general the term reduction system depends on the chosen ordering: If we have two different orderings $<$ and $\prec$ on $\mathbb{K}\langle\mathbf{X}\rangle$ the leading monomials of $\mathbf{G}$ with respect to $<$ may be different from the ones with respect to $\prec$ and hence we have different reductions. Luckily, the Diamond Lemma states that if the overlaps are resolvable with respect to one Artinian ordering they are resolvable with respect to any Artinian ordering.

1.44 Theorem (Diamond Lemma)**.**

Let $\mathbf{G}$ be a reduction system and $<$ an Artinian ordering. Then the following conditions are equivalent:

(i) All overlaps of $\mathbf{G}$ are resolvable.

(ii) All overlaps of $\mathbf{G}$ are resolvable with respect to $<$.

(iii) All elements of $\mathbb{K}\langle\mathbf{X}\rangle$ are reduction-unique under $\mathbf{G}$.

Proof: Since the implications "(iii) $\Rightarrow$ (i) $\Rightarrow$ (ii)" are obvious we only have to prove "(ii) $\Rightarrow$ (iii)".

So assume (ii). Because the reduction-unique elements form an ideal of $\mathbb{K}\langle\mathbf{X}\rangle$ we only have to prove our claim for monomials $D \in \mathbf{X}$. This is done by induction over the degree of D (with respect to $<$).

For $\deg(D) = 0$ there is nothing to show, so assume all monomials with degree less than that of D are reduction-unique, that is $\mathbb{K}\langle\mathbf{X}\rangle_{<D} := \{f \in \mathbb{K}\langle\mathbf{X}\rangle \mid \deg(f) < \deg(D)\} \subseteq \mathfrak{Im}(r_{\mathbf{G}})$. Let r, r' be two reductions acting non-trivially on D. We want to show $r_{\mathbf{G}}(r(D)) = r_{\mathbf{G}}(r'(D))$.

- Assume $D = LABCM$, $r = r_{AB}$ and $r' = r_{BC}$, which corresponds to the case that the monomials we use to reduce D have a "right overlap". Then we have $r(D) - r'(D) = L(f_{AB}C - Af_{BC})M$, where f_m is the image of the monomial m under the corresponding reduction. By condition (ii) we have $f_{AB}C - Af_{BC} \in \mathbf{I}_{ABC}$, where $\mathbf{I}_E$, $E \in \mathbf{X}$, denotes the ideal of $\mathbb{K}\langle\mathbf{X}\rangle$ spanned by all elements FpH, $F, H \in \mathbf{X}$, $p \in \mathbb{K}\langle\mathbf{X}\rangle$, such that $F\mathfrak{lm}(p)H < E$. Therefore we have $L(f_{AB}C - Af_{BC})M \in \mathbf{I}_D$. By assumption $\mathbf{I}_D$ is annihilated by $r_{\mathbf{G}}$, so we have $r_{\mathbf{G}}(r(D)-r'(D)) = r_{\mathbf{G}}(r(D))-r_{\mathbf{G}}(r'(D)) = 0$ as required.

- The case $D = LABCM$, $r = r_B$ and $r' = r_{ABC}$ is completely analogous.

- Finally, let $D = LABCM$, $r = r_A$ and $r' = r_C$, where $A \neq C$ are disjoint words, that is, the monomials have no overlap at all. By Lemma 1.40 (ii) we know that $r_{\mathbf{G}}(Lf_ABCM) = r_{\mathbf{G}}(LABf_CM)$, which completes the proof. q.e.d.

1.45 Corollary. Let $\mathbf{G}$ be a reduced Gröbner basis and $<$ an Artinian ordering. Then for every element of $\mathbb{K}\langle\mathbf{X}\rangle$ there exists a unique reduced normal form with respect to $\mathbf{G}$.

Proof: Let $g_1, g_2 \in \mathbf{G}$ such that $m_1 := \mathfrak{lm}(g_1) = AB$, $m_2 := \mathfrak{lm}(g_2) = BC$ for some monomials $A < B < C \in \mathbf{X}$, that is, g_1 and g_2 have an overlap (due to the fact that $\mathbf{G}$ is reduced this is the only overlap that can occur). Then we have $Ag_2 - g_1C := g_3 \in \mathbf{G}$ or $g_3 = 0$. Denote by τ_i the reduction with g_i.

- Assume $g_3 = 0$. Then we have $\tau_1(ABC) - \tau_2(ABC) = m_1C - g_1C - Am_2 + Ag_2 = \underbrace{m_1C}_{=ABC} - \underbrace{Am_2}_{=ABC} + \underbrace{Ag_2 - g_1C}_{=0} = 0$. So the overlap is resolvable.

- Assume $g_3 \in \mathbf{G}$. Again we get $\tau_1(ABC) - \tau_2(ABC) = m_1C - g_1C - Am_2 + Ag_2 = \underbrace{Ag_2 - g_1C}_{=g_3}$ which can be reduced to zero by g_3, showing that this overlap is resolvable.

Now 1.44 is applicable and our claim is proven. q.e.d.

1.46 Remark. So we got the uniqueness of the reduced normal form. Note that with an Artinian ordering, we will always have a reduced normal form and may apply Algorithm 1.11 to compute it. However, even with this setup our reduced Gröbner basis may be infinite and Algorithm 1.11 has to check infinitely many reductions, even though only finitely many of them act non-trivially. So termination is not guaranteed, not to mention that “after finitely many steps” does not imply “computable in an acceptable amount of time”. Some tricks to deal with this are presented in the next section.

1.5 Truncated Gröbner Bases

Our goal for this section is to see how much information we can gather out of a part of a Gröbner basis. For this we first have to define what a *part of a Gröbner basis* is.

1.47 Definition. Let $\mathbf{G}$ be a set of polynomials such that $\deg_t(g) \leq q \ \forall g \in \mathbf{G}$ and some $q \in \mathbb{N}$. In Algorithm 1.36 discard every obstruction with an S-polynomial of total degree greater than q. If the algorithm returns the set $\mathbf{G}_q$, we call $\mathbf{G}_q$ a *truncated Gröbner basis of degree q*.
Let $\mathbf{B}$ be a Gröbner basis for $\mathbf{G}$ and $\tilde{\mathbf{G}} \subset \mathbf{G}$. We call $\tilde{\mathbf{G}}$ a *partial Gröbner basis*, if it is already a Gröbner basis for the ideal $\tilde{\mathbf{I}} := \langle \tilde{\mathbf{G}} \rangle$.

Since 1.36 always computes a reduced Gröbner basis, a truncated Gröbner basis will always be reduced. Note that a truncated Gröbner basis does not necessarily need to be a subset of our reduced Gröbner basis. But since the algebra $\mathbb{K}\langle\mathbf{X}\rangle$ has only finitely many variables there are only finitely many monomials of total degree $\leq q$ (up to scaling), so the "truncated" version of the algorithm will terminate.
It is clear, that $\langle \mathbf{G}_q \rangle = \langle \mathbf{G} \rangle$, since Algorithm 1.36 does not change the generated ideal. So we may use $\mathbf{G}_q$ to get to know more about the Gröbner basis we want to compute.

1.48 Lemma. Let $B \subseteq \mathbb{K}\langle\mathbf{X}\rangle$ and $\mathbf{G}_q$ be a truncated Gröbner basis of degree q of $\langle B \rangle$. If $\max\{\deg_t(g) \mid g \in \mathbf{G}_q\} \leq \frac{q}{2}$ then G_q is a Gröbner basis of the ideal generated by B.

Proof: Define $m := \max\{\deg_t(g) \mid g \in \mathbf{G}_q\}$. Since $\langle B \rangle = \langle \mathbf{G}_q \rangle$ we only need to show: Every S-polynomial of obstructions of polynomials in G_q is of degree at most $2m-1$, which implies the claim.
Take $g_m \in \mathbf{G}_q$ such that $\deg_t(g_m) = m$. Take an arbitrary $g_i \in G_q$, such that $(l, i, r; \lambda, m, \rho)$ is a left, right or central obstruction.
Note that $\deg_t(g_i) \leq \deg_t(g_m) \quad \forall g_i \in B$, so all obstructions we need to consider are of the form $(l, i, r; \lambda, m, \rho)$.
Because of 1.30 we may assume that $\mathfrak{lm}(g_i)$ and $\mathfrak{lm}(g_m)$ have overlap $b \neq 1$.

1. Assume $\mathfrak{lm}(g_i) = ab$ and $\mathfrak{lm}(g_m) = bc$ with $\deg_t(b) \geq 1$.
   Clearly $(1, i, c; a, m, 1)$ is an obstruction and the induced S-polynomial is of degree at most $2m-1$, since b is not a constant.
   Let $(1, i, r; \lambda, m, \rho)$ be a right obstruction. Since $\mathfrak{lm}(g_i r) = \mathfrak{lm}(\lambda g_m \rho) \Leftrightarrow ab\mathfrak{lm}(r) = \mathfrak{lm}(\lambda)bc\mathfrak{lm}(\rho)$ we get $\mathfrak{lm}(\lambda) = a$ and $\mathfrak{lm}(r)$ and $c\mathfrak{lm}(\rho)$ have overlap c. So $s(1, i, r; \lambda, m, \rho) = g_i c\tilde{r} - a g_m \tilde{\rho}$ for some $\tilde{r}, \tilde{\rho} \in \mathbb{K}\langle\mathbf{X}\rangle$, which is weak with respect to $\mathbf{G}_q \cup \{s(1, i, c; a, m, 1)\}$ by the definition of weakness.
   Now let $(l, i, 1; \lambda, m, \rho)$ be a left obstruction.
   As before we get $s(l, i, 1; \lambda, m, \rho) = \tilde{l} g_i c - \tilde{\lambda} a g_m$, which is weak with respect to $\mathbf{G}_q \cup \{s(1, i, c; a, m, 1)\}$.
   By assumption there will not be any central obstruction.

2. The case $g_i = ba$ and $g_m = cb$ is completely analogous to part 1.

3. Because the degree of g_m is maximal, the last case we have to study is $g_m = ag_ib$. But this would imply that g_m is weak with respect to $\mathbf{G}_q \setminus \{g_m\}$ which is a contradiction to the assumption that $\mathbf{G}_q$ is a truncated Gröbner basis. q.e.d.

1.49 Corollary. If $\mathbf{G}_q$ is a truncated Gröbner basis, then $\mathbf{H} := \{p \in \mathbf{G}_q \mid \deg_t(p) \leq \lfloor \frac{q}{2} \rfloor\}$ is a partial Gröbner basis for $\langle \mathbf{G}_q \rangle$.

Proof: Clear by 1.48. q.e.d.

Provided there exists a finite Gröbner basis, this leads to a way to compute the whole Gröbner basis starting with a truncated one, by iteratively increasing the degree bound.

1.50 Algorithm.

Input: A (finite) truncated Gröbner basis $\mathbf{G}_q$ for $\mathbf{I} = \langle \mathbf{G}_q \rangle$

Output: A reduced Gröbner basis for $\mathbf{I}$

```
($\star$) $p := \max\{\deg_t(g) \mid g \in \mathbf{G}_q\}$
Apply the truncated version of Algorithm 1.36 to $\mathbf{G}_q$ with degree bound $2p-1$
and call the result $\mathbf{G}_{2p-1}$
if $p = \max\{\deg_t(g) \mid g \in \mathbf{G}_{2p-1}\}$ then
  return $\mathbf{G}_{2p-1}$
  else: go to ($\star$)
end if
```

1.51 Remark. It is obvious that 1.50 terminates, if there exists a finite Gröbner basis, and that it will return this Gröbner basis of $\mathbf{I}$.
The proof of Lemma 1.48 states that if we construct an S-polynomial we will lose at least one degree to the overlap, since it is not trivial. This illustration shows us that our lemma includes only the worst case. In fact most of the time we will not have to double our q for the truncated Gröbner basis, as the following lemma states:

1.52 Lemma. Let $B \subseteq \mathbb{K}\langle \mathbf{X} \rangle$ and $\mathbf{G}_q$ be a truncated Gröbner basis of degree q of B. Take $g_1 \in \mathbf{G}_q$ of degree m, and $g_2 \in \mathbf{G}_q$ of maximal degree, say o, such that g_2 has a non-trivial and non-central overlap with g_1. Define $l := lcm(\mathfrak{lm}(g_1), \mathfrak{lm}(g_2))$, where lcm denotes the least common multiple, that is $lcm(\mathfrak{lm}(g_1), \mathfrak{lm}(g_2)) := \max\limits_{\deg_t(b)} \{b \in \mathbf{X} \mid \mathfrak{lm}(g_1) \text{ and } \mathfrak{lm}(g_2) \text{ have overlap } b\}$ and set $p := \deg_t(l)$. Then $m + 1 \leq p \leq m + o - 1$.

Proof: Assume $\mathfrak{lm}(g_1) = ab$ and $\mathfrak{lm}(g_2) = bc$ for some $a, b, c \in \mathbf{X}$, which corresponds to a right obstruction. Since the overlap is non-trivial, none of the monomials a, b, c equal one, so they are all of positive degree. Therefore $l = abc$ is of degree $p = \deg_t(abc) = \deg_t(g_1) + \deg_t(c) \geq m + 1$ on the one hand and on the other $p = \deg_t(abc) = \deg_t(ab) + \deg_t(c) \leq \deg_t(ab) + \deg_t(bc) = m + o$. By relabeling g_1 and g_2 we get the case of a left obstruction as above. q.e.d.

1.53 Proposition. Let $B \subseteq \mathbb{K}\langle \mathbf{X} \rangle$ and $\mathbf{G}_q$ be a truncated Gröbner basis of degree q of B. Take $g_1 \in \mathbf{G}_q$ of degree m, and $g_2 \in \mathbf{G}_q$ of maximal total degree, say o, such that g_2 has any non-trivial overlap with g_1. The overlap may have total degree p.
If we can write $g_1 = \mathfrak{lm}(g_1) + \tilde{g_1}, \quad \deg_t(\tilde{g_1}) = \tilde{m} \leq m$ and $g_2 = \mathfrak{lm}(g_2) + \tilde{g_2}, \quad \deg_t(\tilde{g_2}) = \tilde{o} \leq o$, then the total degree of the normal form of any S-polynomial of $\mathbf{G}_q$ is at most m', where $m' = \max\{\tilde{m}(o-p), \tilde{o}(m-p)\}$.

Proof: The only two obstructions we need to consider are $(1, 2, c; a, 1, 1)$ and $(c, 2, 1; 1, 1, a)$, as seen in the proof of Lemma 1.48. In the first case, we have

$$\deg_t(c) = \deg_t(g_1) - \deg_t(b) = m - p, \quad \deg_t(a) = \deg_t(g_2) - \deg_t(b) = o - p.$$

Since the leading terms of g_1 and g_2 cancel each other, we have

$$\deg_t((1, 2, c; a, 1, 1)) \leq \max\{\tilde{m}(o-p), \tilde{o}(m-p)\}.$$

For the second case we get analogously:

$$\deg_t((c, 2, 1; 1, 1, a)) \leq \max\{\tilde{m}(o-p), \tilde{o}(m-p)\}.$$

q.e.d.

The bound given in Proposition 1.53 is again not strict: It determines the highest total degree p of all S-polynomials. Therefore, we have to compute a Gröbner basis at least up to degree p. But if all S-polynomials of total degree p reducing to zero the degree bound needed is in fact lower.
However, 1.53 can be used to enhance Algorithm 1.50 in an obvious way:

1.54 Algorithm.
Input: A truncated Gröbner basis $\mathbf{G}_q$ for $\mathbf{I} = \langle \mathbf{G}_q \rangle$
Output: A reduced Gröbner basis for $\mathbf{I}$

```
(⋆) Set:
        $p := \max\{ \deg_t(m) \mid m = \mathfrak{lm}(S(g, \tilde{g})), (g, \tilde{g}) \in \mathbf{G}_q \times \mathbf{G}_q,$
                $g$ and $\tilde{g}$ have non trivial overlap$\}$

    for $g \in \{\tilde{g} \in \mathbf{G}_q \mid \deg_t(\tilde{g}) = p\}$ do

        $p_g := \max\{p + d_{\tilde{g}} - p_{g,\tilde{g}} \mid d_{\tilde{g}} = \deg_t(\tilde{g}),$
                $p_{g,\tilde{g}} = \min\{o \mid g$ and $\tilde{g}$ have overlap of total degree $o\},$
                $\tilde{g} \in \mathbf{G}_q\}$
```

```
end for
Set $p = \max\{p_g \mid g \in \{\tilde{g} \in \mathbf{G}_q \mid \deg_t(\tilde{g}) = p\}\}$
if $p \leq q$ then
   return $\mathbf{G}_q$
   else: Apply the truncated version of Algorithm 1.36 to $\mathbf{G}_q$ with degree
   bound $p$ and call the result $\mathbf{G}_p$
   if $\mathbf{G}_p = \mathbf{G}_q$ then
      return $\mathbf{G}_p$
      else: Set $\mathbf{G}_q = \mathbf{G}_p$ and go to $(\star)$
   end if
end if
```

1.55 Remark. Algorithm 1.54 will be of great use in the setup of the Letterplace analogon. Here one always has a degree bound, at least in practice (cf. [LL09]). So one always computes a truncated Gröbner basis. Therefore, the adaptive algorithm is the only way to get to a complete Gröbner basis.
It is in no way clear, whether this algorithm will terminate. In fact the question for termination is the question for finiteness of the Gröbner basis. In general, if the Gröbner basis is infinite, we do not have any possibility to determine that, whereas if the Gröbner basis is finite the Algorithm 1.54 will terminate.
However, there are some situations, when we can decide whether the Gröbner basis will be finite or not, as we will see in 2.40.

1.6 The Letterplace Approach

It is a well known fact that there exists a one to one correspondence between all ideals $\mathbf{J} \trianglelefteq \mathbb{K}[\mathbf{X}]$ and some ideals $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$. So the question arises, if there is an ideal $\mathbf{J}$ in some commutative ring $\mathbb{K}[\mathbf{Y}]$ for each $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$, such that we can construct a one to one correspondence between those ideals and especially their Gröbner bases.
Roberto La Scala and Viktor Levandovskyy introduced the *Letterplace ring* (cf. [LL09]), which provides a commutative analogon of the free algebra. The basic idea, going back to Richard Feynman and Gian-Carlo Rota, is pleasingly simple: one enumerates the variables occurring in a monomial by their position in the monomial. Then one may commute the variables.
In this section we will mainly follow [LL09].

1.56 Definition. We call $\mathbf{X}$ and $\mathbf{P} \subseteq \mathbb{N}_0$ respectively the *set of letters and places*. We write for the elements of the product set $\mathbf{X} \times \mathbf{P}$: $x_i(j) := (x_i, j)$. Furthermore we denote by $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ the polynomial ring in the commuting variables $x_i(j)$ and by $[\mathbf{X}|\mathbf{P}]$ the set of all monomials in $\mathbb{K}[\mathbf{X}|\mathbf{P}]$.
Let $\mu = (\mu_k)_{k\in\mathbb{N}}, \nu = (\nu_k)_{k\in\mathbb{N}}$ be two sequences of non-negative integers with finite support. We can consider (μ, ν) as a multidegree for the monomials

$m = x_{i_1}(j_1)\dots x_{i_r}(j_r) \in [\mathbf{X}|\mathbf{P}]$. Precisely, we define $\mu_k = \sharp\{\alpha \mid x_{i_\alpha} = x_k\}$, $\nu_k = \sharp\{\beta \mid j_\beta = k\}$.

1.57 Remark. If we define $\mathbb{K}[\mathbf{X}|\mathbf{P}]_{\mu,\nu}$ to be the homogeneous component of degree (μ,ν) we have $\mathbb{K}[\mathbf{X}|\mathbf{P}] = \bigoplus_{\mu,\nu} \mathbb{K}[\mathbf{X}|\mathbf{P}]_{\mu,\nu}$, so $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ is a multigraded algebra. By putting $\mathbb{K}[\mathbf{X}|\mathbf{P}]_{*,\nu} = \bigoplus_{\mu} \mathbb{K}[\mathbf{X}|\mathbf{P}]_{\mu,\nu}$ and $\mathbb{K}[\mathbf{X}|\mathbf{P}]_{\mu,*} = \bigoplus_{\nu} \mathbb{K}[\mathbf{X}|\mathbf{P}]_{\mu,\nu}$ we obtain that $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ is also multigraded with respect to letter or place multidegrees only.

1.58 Example. We just want to see a simple example to visualize the Letterplace analogon. So take $xyx \in \mathbb{K}\langle x,y\rangle$. Now introducing places we see that xyx corresponds to $x(0)y(1)x(2) = x(2)x(0)y(1) = y(1)x(2)x(0)$ and each of the three Letterplace monomials has only xyx as inverse image.
Unfortunately, there are some elements we have no use for, because they do not correspond to any monomial in $\mathbb{K}\langle x,y\rangle$, for example $x(3)y(6)y(9)$ and $x(0)y(0)$.

So we try to get rid of those elements.

1.59 Remark. The monoid $\mathbb{N}$ has a natural faithful action on the graded algebra $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ given by $s \cdot x_i(j) = x_i(j+s)\ \ \forall s \in \mathbb{N}$.

1.60 Definition. For each monomial $m = x_{i_1}(j_1)\cdots x_{i_r}(j_r) \in [\mathbf{X}|\mathbf{P}]$ we define by $sh(m) = \min\{j_1,\dots,j_r\}$ the *shift of* m.
For each $s, r \in \mathbb{N}$ we denote by $s \cdot 1^r$ the place-multidegree $\nu = (\nu_k)_{k\in\mathbb{N}}$ such that

$$\nu_k = \begin{cases} 1, & \text{if } s \le k \le s+r-1. \\ 0, & \text{otherwise.} \end{cases}$$

For $s = 0$ we write simply 1^r.
Define $V = \bigoplus_{n\in\mathbb{N}} \mathbb{K}[\mathbf{X}|\mathbf{P}]_{*,1^r}$, which is a subspace of $\mathbb{K}[\mathbf{X}|\mathbf{P}]^{(0)}$, the subspace of $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ generated by all monomials with shift 0.

1.61 Lemma. $\iota : \mathbb{K}\langle\mathbf{X}\rangle \to V : \ x_{i_1}\cdots x_{i_r} \mapsto x_{i_1}(0)\cdots x_{i_r}(r-1)$ is an isomorphism of vector spaces, which preserves letter-multidegrees and hence total degrees of monomials.

Proof: By the definition of ι it is obvious that ι is a $\mathbb{K}$-linear map. Moreover, we have $\iota^{-1} : V \to \mathbb{K}\langle\mathbf{X}\rangle : \ x_{i_1}(0)\cdots x_{i_r}(r-1) \mapsto x_{i_1}\cdots x_{i_r}$ and hence ι is bijective. Since ι is $\mathbb{K}$-linear we only have to show that ι preserves letter-multidegrees of monomials, which is clear by definition of ι. q.e.d.

So the vector space V is a good candidate for a commutative correspondence of the free algebra. Let us see what happens to an ideal in $\mathbb{K}\langle\mathbf{X}\rangle$.

1.62 Definition. Let $\mathbf{J}$ be an ideal of $\mathbb{K}[\mathbf{X}|\mathbf{P}]$. Then $\mathbf{J}$ is called

- *place-multigraded*, if $\mathbf{J} = \sum_{\nu} \mathbf{J}_{*,\nu}$, where $\mathbf{J}_{*,\nu} = \mathbf{J} \cap \mathbb{K}[\mathbf{X}|\mathbf{P}]_{*,\nu}$.

- *shift-decomposable*, if $\mathbf{J} = \sum_s \mathbf{J}^{(s)}$, where $\mathbf{J}^{(s)} = \mathbf{J} \cap \mathbb{K}[\mathbf{X}|\mathbf{P}]^{(s)}$.

Clearly a place-multigraded ideal is also graded and shift-decomposable.

1.63 Lemma. Let $\mathbf{J} \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$ be an ideal. Then $\mathbf{J}$ is shift-decomposable if and only if $\mathbf{J}$ is generated by $\bigcup_{s\in\mathbb{N}} \mathbf{J}^{(s)}$.

Proof: The necessary condition is obvious. Assume now that $\mathbf{J} = \langle\{mf \mid m \in [\mathbf{X}|\mathbf{P}], f \in \mathbf{J}^{(s)}, s \in \mathbb{N}\}\rangle$. Then, for $t = \min\{sh(m), s\}$ we have $mf \in \mathbf{J}^{(t)}$ and hence $\mathbf{J} = \sum_s \mathbf{J}^{(s)}$. q.e.d.

1.64 Definition. Let $\mathbf{J}$ be a shift-decomposable ideal of $\mathbb{K}[\mathbf{X}|\mathbf{P}]$. We say that $\mathbf{J}$ is *shift-invariant* if $s \cdot \mathbf{J}^{(t)} = \mathbf{J}^{(s+t)}$ for all $s, t \in \mathbb{N}$.

Note that $\mathbf{J}$ is shift-invariant if and only if $s \cdot \mathbf{J}^{(0)} = \mathbf{J}^{(s)}$.

1.65 Lemma. Let $\mathbf{J} \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$ be an ideal. Then $\mathbf{J}$ is shift-invariant if and only if $\mathbf{J} = \sum_{s\in\mathbb{N}} s \cdot \mathbf{J}^{(0)}$.

Proof: Clearly we have the necessary condition. Assume now $\mathbf{J} = \sum_s s \cdot \mathbf{J}^{(0)}$. We have $s \cdot \mathbf{J}^{(0)} \subset \mathbf{J}$ and $s \cdot \mathbf{J}^{(0)} \subset s \cdot \mathbb{K}[\mathbf{X}|\mathbf{P}]^{(0)} = \mathbb{K}[\mathbf{X}|\mathbf{P}]^{(s)}$ and hence $s \cdot \mathbf{J}^{(0)} \subset \mathbf{J}^{(s)}$. Let $f \in \mathbf{J}^{(s)}$. Since $\mathbf{J} = \sum_{t\in\mathbb{N}} t \cdot \mathbf{J}^{(0)}$ we have necessarily $f \in s \cdot \mathbf{J}^{(0)}$. We conclude that $s \cdot \mathbf{J}^{(0)} = \mathbf{J}^{(s)}$ and therefore $\mathbf{J} = \sum_{s\in\mathbb{N}} \mathbf{J}^{(s)}$. q.e.d.

1.66 Theorem. Let $\mathbf{J}$ be an ideal of $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ an put $\mathbf{I} = \iota^{-1}(\mathbf{J} \cap V) \subset \mathbb{K}\langle\mathbf{X}\rangle$.

- If $\mathbf{J}$ is a shift-invariant ideal, then $\mathbf{I}$ is a left ideal of $\mathbb{K}\langle\mathbf{X}\rangle$.
- If $\mathbf{J}$ is a place-multigraded ideal, then $\mathbf{I}$ is a graded right ideal.

Proof: Assume $\mathbf{J}$ is shift-invariant and let $f \in \mathbf{I}, w \in \mathbf{X}$. Denote $g = \iota(f) \in \mathbf{J} \cap V$ and $m = \iota(w)$. If $\deg_t(w) = s$, we have $\iota(wf) = m(s \cdot g) \in \mathbf{J} \cap V$ and therefore $wf \in \mathbf{I}$.
Suppose now that $\mathbf{J}$ is place-multigraded and hence graded. Since V is a graded subspace, it follows that $\mathbf{J} \cap V = \sum_d (\mathbf{J}_d \cap V)$ and then, setting $\mathbf{I}_d = \iota^{-1}(\mathbf{J}_d \cap V)$ we obtain $\mathbf{I} = \sum_d \mathbf{I}_d$. Let $f \in \mathbf{I}_d$, that is $\iota(f) = g \in \mathbf{J}_d \cap V$. For all $w \in \mathbf{X}$ we have that $\iota(fw) = g(d \cdot m) \in \mathbf{J} \cap V$, that is $fw \in \mathbf{I}$. q.e.d.

1.67 Theorem. Let $\mathbf{I}$ be a left ideal of $\mathbb{K}\langle\mathbf{X}\rangle$ and put $\mathbf{I}' = \iota(\mathbf{I})$. Define $\mathbf{J} = \langle \bigcup_{s\in\mathbb{N}} s \cdot \mathbf{I}' \rangle \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$. Then $\mathbf{J}$ is a shift-invariant ideal. Moreover, if $\mathbf{I}$ is graded then $\mathbf{J}$ is place-multigraded.

Proof: From $s \cdot \mathbf{I}' \subset \mathbf{J}^{(s)}$ it follows that $\mathbf{J}$ is generated by $\bigcup\limits_{s\in\mathbb{N}} \mathbf{J}^{(s)}$, that is $\mathbf{J}$ is shift-decomposable. By definition one has $\mathbf{J} = \langle\{m(t\cdot f) \mid m \in [\mathbf{X}|\mathbf{P}], t \in \mathbb{N}, f \in \mathbf{I}'\}\rangle$. Then the vector space $\mathbf{J}^{(s)}$ is spanned by the elements $m(t \cdot f)$ such that $\min\{sh(m), t\} = s$. In particular, $\mathbf{J}^{(0)}$ is spanned by the elements $m(t \cdot f)$ where $\min\{sh(m), t\} = 0$. By acting with s, we obtain that $s\cdot\mathbf{J}^{(0)}$ is spanned by elements of the form $s \cdot (m(t \cdot f)) = (s \cdot m)((s + t) \cdot f)$, where $m \in [\mathbf{X}|\mathbf{P}], t \in \mathbb{N}, f \in \mathbf{I}'$, such that $\min\{sh(m), t\} = 0$ and therefore $\min\{sh(s \cdot m), s + t\} = s$. Since $s \cdot \mathbb{K}[\mathbf{X}|\mathbf{P}]^{(0)} = \mathbb{K}[\mathbf{X}|\mathbf{P}]^{(s)}$ we conclude that $s \cdot \mathbf{J}^{(0)} = \mathbf{J}^{(s)}$.
Assume now that $\mathbf{I}$ is a graded ideal. Any element $f \in \mathbf{I}$ can be written as $f = \sum\limits_d f_d$, where $f_d \in \mathbf{I}\cap\mathbb{K}\langle\mathbf{X}\rangle_d$. Put $g = \iota(f_d)$ and $g_d = \iota(f_d)$. Then $g_d \in \mathbf{I}'\cap V_d$. For any $s \in \mathbb{N}$ one has that $s \cdot g = \sum\limits_d s \cdot g_d$, where $s \cdot g_d \in \cdot(\mathbf{I}' \cap V_d) \subset \mathbf{J}$. Note that all polynomials $s \cdot g_d$ are homogeneous with respect to place-multigrading. We conclude that $\mathbf{J}$ is generated by homogeneous elements and hence it is a place-multigraded ideal. q.e.d.

1.68 Definition.

- Let $\mathbf{I} \subset \mathbb{K}\langle\mathbf{X}\rangle$ be a graded two-sided ideal. We denote by $\tilde{\iota}(\mathbf{I})$ the shift-invariant place-multigraded ideal $\mathbf{J} \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$ generated by $\bigcup\limits_{s\in\mathbb{N}} s \cdot \iota(\mathbf{I})$, and call $\mathbf{J}$ the *Letterplace analogon of the ideal* $\boldsymbol{I}$.
- For a shift-invariant place-multigraded ideal $\mathbf{J} \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$ we denote by $\tilde{\iota}^{-1}(\mathbf{J})$ the graded two-sided ideal $\mathbf{I} = \iota^{-1}(\mathbf{J} \cap V) \subset \mathbb{K}\langle\mathbf{X}\rangle$.
- A graded ideal $\mathbf{J} \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$ is called a *Letterplace ideal* if $\mathbf{J}$ is generated by $\bigcup\limits_{s,d\in\mathbb{N}} s \cdot (\mathbf{J}_d \cap V)$. In this case, $\mathbf{J}$ is shift-invariant and place-multigraded.

1.69 Remark. The map $\iota : \mathbb{K}\langle\mathbf{X}\rangle \to V$ induces a one-to-one correspondence $\tilde{\iota}$ between graded two-sided ideals $\mathbf{I}$ of the free associative algebra $\mathbb{K}\langle\mathbf{X}\rangle$ and the Letterplace ideals $\mathbf{J}$ of the polynomial ring $\mathbb{K}[\mathbf{X}|\mathbf{P}]$.

So now we have finally found the correspondence for an ideal in $\mathbb{K}\langle\mathbf{X}\rangle$. We are now interested in generating sets and especially Gröbner bases. If we find a correspondence we may find a Gröbner basis for a given ideal as follows: Starting with a generating set for $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ we switch to the corresponding "Letterplace generating set", compute a "Letterplace Gröbner basis" with commutative methods and use then the correspondence again to get our desired Gröbner basis. In this work we will only see the correspondence and accept the fact, that the Letterplace ring is a polynomial ring, so that commutative Gröbner theory may be applied to it.

1.70 Definition. Let $\mathbf{J}$ be a Letterplace ideal of $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ and $H \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$. We say that H is a *Letterplace basis* of $\mathbf{J}$ if $H \subset \bigcup\limits_{d\in\mathbb{N}} \mathbf{J}_d\cap V$ and $\bigcup\limits_{s\in\mathbb{N}} s\cdot H$ is a generating set of the ideal $\mathbf{J}$.

1.71 Theorem. Let $\mathbf{I}$ be a graded two-sided ideal of $\mathbb{K}\langle\mathbf{X}\rangle$ and put $\mathbf{J} = \tilde{\iota}(\mathbf{I})$. Moreover, let $G \subset \bigcup_{d\in\mathbb{N}} \mathbf{I}_d$ and define $H = \iota(G) \subset \bigcup_{d\in\mathbb{N}} \mathbf{J}_d \cap V$. Then G is a generating set of $\mathbf{I}$ as a two-sided ideal if and only if H is a Letterplace basis of $\mathbf{J}$.

Proof: Assume $\bigcup_{s\in\mathbb{N}} s \cdot H$ is a basis of $\mathbf{J}$, that is, $\mathbf{J} = \langle m(s \cdot h) \mid m \in [\mathbf{X}|\mathbf{P}], s \in \mathbb{N}, h \in H\rangle$. Since $\mathbf{J}$ is place-multigraded, one has that $\mathbf{J} \cap V = \langle m(s \cdot h) \in V \mid m \in [\mathbf{X}|\mathbf{P}], s \in \mathbb{N}, h \in H\rangle$. If $d = \deg_t(h)$ then $m(s \cdot h) = m_1(s \cdot h)((s + d) \cdot m_2)$, where $m_1, m_2 \in [\mathbf{X}|\mathbf{P}] \cap V$. By applying ι^{-1} we obtain that $\mathbf{I} = \langle w_1 g w_2 \mid w_1, w_2 \in \mathbf{X}, g \in G\rangle$, that is G is a generating set of $\mathbf{I}$ as a two-sided ideal.
Assume now G generates $\mathbf{I}$. By reversing the above argument, one has that $\mathbf{J} \cap V \subset U := \langle m(s \cdot h) \mid m \in [\mathbf{X}|\mathbf{P}], s \in \mathbb{N}, h \in H\rangle \subset \mathbf{J}$. From $s \cdot (m(t \cdot h)) = (s \cdot m)((s + t) \cdot h)$ $\forall s, t \in \mathbb{N}$, it follows that $s \cdot (\mathbf{J} \cap V) \subset U$ for any s. We conclude that $\mathbf{J} = U$, because $\mathbf{J}$ is generated by $\bigcup_{s\in\mathbb{N}} s \cdot (\mathbf{J} \cap V)$. This implies the claim. q.e.d.

So the correspondence for generating sets is rather simple. For the correspondence of Gröbner bases, we have to do a little more work.

1.72 Definition. Let $\mathbf{J}$ be an ideal of $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ and $H \subset \mathbf{J}$. Then H is called a (Gröbner) *shift-basis of* $\mathbf{J}$ if $\bigcup_{s\in\mathbb{N}} s \cdot H$ is a (Gröbner) basis of $\mathbf{J}$.

1.73 Remark.

1. If $\mathbf{J}$ has a shift-basis, then $s \cdot \mathbf{J} \subset \mathbf{J}$ $\forall s \in \mathbb{N}$.

2. If $\mathbf{J}$ is a Letterplace ideal, then any Letterplace basis of $\mathbf{J}$ is a shift-basis, but not generally a Gröbner shift-basis.

3. Let $\mathbf{J} \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$ be an ideal and $H \subset \mathbf{J}$. Then H is a Gröbner shift-basis of $\mathbf{J}$ if and only if $\mathfrak{lm}(H)$ is a shift-basis of $\mathfrak{L}(\mathbf{J})$, the ideal generated by the leading monomials of all elements of $\mathbf{J}$.

1.74 Lemma. Let $\mathbf{J} \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]$ be a shift-invariant ideal. Then $\mathbf{J}^{(0)}$ is a Gröbner shift-basis of the ideal $\mathbf{J}$.

Proof: Clearly $\mathbf{J}^{(0)}$ is a shift-basis of $\mathbf{J}$. Let $f \in \mathbf{J}^{(u)}/\{0\}, g \in \mathbf{J}^{(v)}/\{0\}, f \neq g$ and denote the S-polynomial $s(f, g,) = cmf - dng$, where $c, d \in \mathbb{K}$ and $m, n \in [\mathbf{X}|\mathbf{P}]$, such that $lcm(\mathfrak{lm}(f), \mathfrak{lm}(g)) = m\mathfrak{lm}(f) = n\mathfrak{lm}(g)$. We have to show that $s(f, g) \in \bigcup_s \mathbf{J}^{(s)}$. If $u = v$ this is trivial. Assume $u < v$. The variables of m come from the leading monomial of g which has shift v. Therefore cmf has shift u and no variable of the leading term of g has shift u. Then also dng is shift-uniform with shift u and the same clearly holds for $s(f, g) = cmf - dng$. q.e.d.

1.75 Remark. Before we can state the main theorem, we need a little clue: We assume our given ordering is *compatible* with ι, that is, if we fix the orderings $<$ on $\mathbb{K}\langle\mathbf{X}\rangle$ and $\prec$ on $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ then $v < w$ holds if and only if $\iota(v) \prec \iota(w)$ for any $v, w \in \mathbf{X}$. This is no restriction, since most choices of orderings are compatible with ι.

1.76 Theorem. Let $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ be a graded two-sided ideal and put $\mathbf{J} = \tilde{\iota}(\mathbf{I})$. Moreover, let H be a Gröbner Letterplace basis of $\mathbf{J}$ and put $G = \iota^{-1}(H \cap V) \subset \bigcup\limits_{d\in\mathbb{N}} \mathbf{I}_d$. Then G is a Gröbner basis of $\mathbf{I}$ as a two-sided ideal.

Proof: Let $f \in \mathbf{I}_d$ and put $f' = \iota(f)$. Then there is $m \in [\mathbf{X}|\mathbf{P}],\ s \in \mathbb{N},\ h \in H$ such that $\mathfrak{lm}(f') = m\mathfrak{lm}(s \cdot h) = m(s \cdot \mathfrak{lm}(h))$. From $f' \in \mathbf{J}_d \cap V$ and $\sqrt{\nu_h} = 1^n, n \in \mathbb{N}$, it follows that $\nu_h = 1^n$, that is $h \in H \cap V$. This implies that $\mathfrak{lm}(f') = m(s \cdot \mathfrak{lm}(h)) = m_1(s \cdot \mathfrak{lm}(h))((s+n) \cdot m_2)$, where $m_1, m_2 \in [\mathbf{X}|\mathbf{P}] \cap V$ and $s = \deg_t(m_1)$. Since the orderings are compatible with ι, we obtain that $\mathfrak{lm}(f) = w_1\mathfrak{lm}(g)w_2$, where $g = \iota^{-1} = (H), w_i = \iota^{-1}(m_i)$. q.e.d.

1.77 Remark. In 1.68 we demand that $\mathbf{I}$ is graded and that every element of $\mathbf{I}$ is homogeneous. However, this is not too restrictive. In fact, it is well-known that a Gröbner basis of any two-sided ideal $\mathbf{I}$ can be obtained via a Gröbner basis of a homogenized version of $\mathbf{I}$. Nevertheless, the work on a direct non-homogeneous version of the Letterplace Gröbner basis algorithm, that is, without homogenization, is in progress.
Since we will see at the beginning of the next chapter that we only need to study the lead ideal in ordering to find a $\mathbb{K}$-basis of the factor algebra this theory is all we need, because all elements of the lead ideal are monomials and therefore homogeneous.

2 Factor Algebras

For a given ideal $\mathbf{I}$ we can consider the *factor algebra* $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I} := \{f + \mathbf{I} \mid f \in \mathbb{K}\langle\mathbf{X}\rangle\}$, which is again a $\mathbb{K}$-algebra via $[f]\cdot[g] = [fg]$ and $[f]+[g] = [f+g] \quad f, g \in \mathbb{K}\langle\mathbf{X}\rangle$, where $[f] = f + \mathbf{I}$. We will drop the brackets, whenever it is possible.

2.1 Motivation. For a given factor algebra $A = \mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$, where $\mathbf{G}$ is a Gröbner basis for $\mathbf{I} = \langle\mathbf{G}\rangle$ one is interested in the following questions:

1. Is $\dim_{\mathbb{K}}(A) < \infty$?
2. If $\dim_{\mathbb{K}}(A) < \infty$, compute $\dim_{\mathbb{K}}(A)$.
3. If $\dim_{\mathbb{K}}(A) < \infty$, compute a $\mathbb{K}$-basis for A.
4. Compute the (partial) Hilbert series (see 2.28) of A.

Why is one interested in computing the $\mathbb{K}$-dimension of a factor algebra? Our main goal is to prepare the computation of the *Gel'fand-Kirillov dimension*:
Let A be a finitely generated $\mathbb{K}$-algebra. Then there exists a $\mathbb{K}$-subspace $V \subset A$ such that A is generated by V as a $\mathbb{K}$-algebra. V induces a *standard finite dimensional filtration* $\{A_i | i \in \mathbb{Z}\}$ on A by setting $A_i := \{0\}$ for $i < 0$, $A_0 := V^0 := \mathbb{K}$ and $A_i := \sum_{j=1}^{i} V^j$ for $i > 0$, where $V^j = \langle\{\prod_{k=1}^{j} v_k \mid v_k \in V\}\rangle$.
Then the *Gel'fand-Kirillov dimension* is defined as

$$GK\dim(A) = \limsup_{i\to\infty} \log_i(\dim_{\mathbb{K}}(A_i)).$$

2.1 A Basis for a Factor Algebra

Since $\mathbb{K}\langle\mathbf{X}\rangle$ is a $\mathbb{K}$-algebra, we can think of it as a $\mathbb{K}$-vector space which has basis $\mathbf{X}$. In this section we are interested in a $\mathbb{K}$-basis of $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ for a given ideal $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$. This basis will not be unique, since it depends on our choice of the representative of $[f] \in \mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$. So the first goal is to define a basis with some nice properties. The Diamond Lemma 1.44 gives us a first hint.

2.2 Theorem (Diamond Lemma)**.** Let $\mathbf{G}$ be a reduction system and $<$ an monomial ordering (in particular $<$ has the descending chain condition), such that all overlaps of $\mathbf{G}$ are resolvable with respect to $<$. Then the set of all irreducible monomials with respect to $\mathbf{G}$ is a basis of $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$ (we will speak of *the* (monomial) basis).

Proof: We will show that under the assumptions of 1.44 every element of $\mathbb{K}\langle\mathbf{X}\rangle$ is reduction-unique if and only if the set of all irreducible monomials forms a basis of $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$.
Note that the latter statement is equivalent to $\mathbb{K}\langle\mathbf{X}\rangle = \mathbb{K}\langle\mathbf{X}\rangle_{irr} \oplus \mathbf{I}$ as vector spaces, where $\mathbb{K}\langle\mathbf{X}\rangle_{irr}$ is the $\mathbb{K}$-subspace spanned by all irreducible monomials.
Assume all elements are reduction-unique. Then $r_{\mathbf{G}}$ (as in 1.40) is a projection onto $\mathbb{K}\langle\mathbf{X}\rangle_{irr}$. Obviously $\ker(r_{\mathbf{G}}) \subseteq \mathbf{I}$, since every element is altered by an element in $\mathbf{I}$. By 1.40 we have $r_{\mathbf{G}}(AgB) = r_{\mathbf{G}}(A\mathfrak{lm}(g)B) - r_{\mathbf{G}}(A(\mathfrak{lm}(g) - g)B) = 0 \quad \forall g \in \mathbf{G},\ A, B \in \mathbf{X}$. Therefore we have $\mathbf{I} \subseteq \ker(r_{\mathbf{G}})$. By the first isomorphism theorem, we have $\mathbb{K}\langle\mathbf{X}\rangle = \mathbb{K}\langle\mathbf{X}\rangle_{irr} \oplus \mathbf{I}$. Conversely assume $\mathbb{K}\langle\mathbf{X}\rangle = \mathbb{K}\langle\mathbf{X}\rangle_{irr} \oplus \mathbf{I}$ and let $a \in \mathbb{K}\langle\mathbf{X}\rangle$ be reducible to b and b' in $\mathbb{K}\langle\mathbf{X}\rangle_{irr}$. Then $b - b' \in \mathbb{K}\langle\mathbf{X}\rangle_{irr} \cap \mathbf{I} = \{0\}$, showing that a is reduction-unique. q.e.d.

2.3 Corollary.

1. The basis B for $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ as constructed in 2.2 is also a basis for $\mathbb{K}\langle\mathbf{X}\rangle/\mathfrak{L}(\mathbf{I})$.
2. $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathfrak{L}(\mathbf{I})) = \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I})$.

Proof:

1. The irreducible monomials with respect to $\mathbf{I}$ are precisely the irreducible monomials with respect to $\mathfrak{L}(\mathbf{I})$.
2. This is a direct consequence of item 1 and 2.2. q.e.d.

2.4 Remark. Note that the reduction induced by a monomial either acts trivially on a monomial or the monomial can be reduced to zero with this reduction. In order to find a basis for $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ we can now proceed as follows: Given a (reduced) Gröbner basis $\mathbf{G}$ for $\mathbf{I}$ we take only the leading monomials of $\mathbf{G}$, which generate $\mathfrak{L}(\mathbf{I})$. Then we compute a monomial basis for $\mathbb{K}\langle\mathbf{X}\rangle/\mathfrak{L}(\mathbf{I})$, which will be a basis for $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ as well. However, this only works for computing a basis (and similar computations, like determination of the $\mathbb{K}$-dimension). If one is interested in computations in the factor algebra, one has to consider the whole Gröbner basis. For an example take the multiplication of two elements $a, b \in \mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$. We then have $a \cdot b = r_{\mathbf{G}}(ab)$.

2.2 Graphs and Trees

For our work with the factor algebra, it is useful to consider graphs and build up some special kind of trees. Therefore we will do a short introduction to graph theory.

All of the following definitions are easily understandable and we refer to [Die05] for further information. However this is all we need to know to understand the next sections.

2.5 Definition. A **graph** G is a pair (V, E) of disjoint sets, where $E \subseteq \{\{e, e'\} \mid e, e' \in V\}$. We call $v \in V$ a **vertex** and $e \in E$ an **edge**.

The benefit we get from dealing with graphs is that they can be illustrated very easily, as the following example shows.

2.6 Example. Take $V = \{1, \ldots, 7\}$ with the edges
$E = \{\{1, 2\}, \{1, 5\}, \{2, 5\}, \{3, 4\}, \{5, 7\}\}$. Now if we draw a point for each vertex and a line between two vertices, whenever there is a edge between these vertices, we can illustrate the graph as in Figure 2.1.

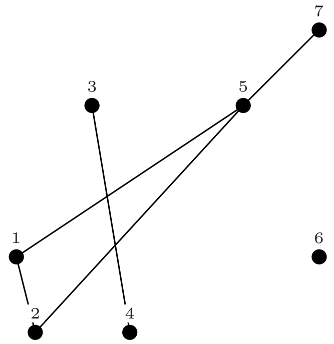


Figure 2.1: The Graph of Example 2.6

2.7 Definition. Let $G = (V, E)$ be a graph.

1. We call $\tilde{G} = (\tilde{V}, \tilde{E})$ a **subgraph** of G, if $\tilde{V} \subseteq V$ and $\tilde{E} \subseteq E$.
2. A **path** in G is a subgraph $P = (\tilde{V}, \tilde{E})$ of the form $\tilde{V} = \{x_0, x_1, \ldots, x_k\}$, $\tilde{E} = \{\{x_0, x_1\}, \{x_1, x_2\}, \{x_2, x_3\}, \ldots, \{x_{k-1}, x_k\}\}$, where $x_i \neq x_j \quad \forall 1 \leq i, j \leq k, i \neq j$. $x_1, \ldots, x_{k-1}$ are called the **inner points** of P, k is the **length** of P. x_0 is sometimes called the **starting-** and x_k the **endpoint** of P. A **cycle** is a path with $x_0 = x_k$.
3. A graph $G = (V, E)$ is called **directed**, if $E \subseteq V \times V$.

To distinguish a directed graph in the illustration one often draws arrows instead of lines, as pictured in Figure 2.2.

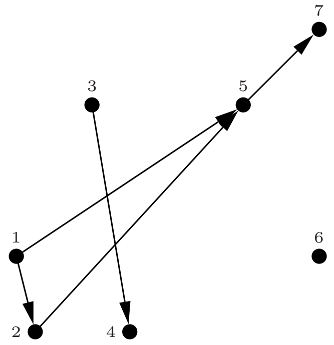


Figure 2.2: The directed Graph of Example 2.6

2.8 Definition.

- A graph is called **connected** if for every two vertices x, y there exists a path from x to y.
- A **forest** is a graph with no cycles.
- A **tree** is a connected forest.

2.3 The Dimension of Factor Algebras

Starting with a (reduced) Gröbner basis for a given ideal $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ our first goal is to get certain information about the dimension of the factor algebra only by the knowledge of the Gröbner basis. However, this is not as simple as in the commutative case, as the next example shows.

2.9 Lemma. $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}) < \infty \implies \forall i \exists n_i \in \mathbb{N}_0 : \; x_i^{n_i} \in \mathfrak{L}(\mathbf{I})$

Proof: Assume $x_i^k \notin \mathfrak{L}(\mathbf{I})$ $\forall k \in \mathbb{N}_0$. Then $\{x_i^j\}_{j=0}^{\infty}$ are linearly independent over $\mathbb{K}$ as elements of $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$, which proves the claim. q.e.d.

The converse is not true in general:

2.10 Example. Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{K}\langle x, y\rangle$ and $\mathbf{I} = \langle x^2, y^2\rangle$. Then $\{(xy)^n \mid n \in \mathbb{N}_0\}$ is an infinite set of linear independent elements in $\mathbb{K}\langle x, y\rangle/\mathbf{I}$ and therefore $\mathbb{K}\langle x, y\rangle/\mathbf{I}$ has infinite $\mathbb{K}$-dimension.

Therefore many characterizations, which are useful in the commutative case, are useless in the non-commutative case. But we can use our concept of partial Gröbner bases to test if the dimension of the factor algebra is finite.

2.11 Lemma. Assume we have a Gröbner basis $\mathbf{G}$ of the ideal $\mathbf{I}$ and a partial Gröbner basis $\mathbf{G}_p$. If $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_p\rangle) < \infty$, then also $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle) < \infty$.

Proof: Since $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_p\rangle) < \infty$, so is $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathfrak{L}(\mathbf{G}_p)\rangle)$. We show that $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathfrak{L}(\mathbf{G})\rangle) < \infty$, which implies the statement.
A $\mathbb{K}$-basis of the factor algebra consists of all monomials, which are not divisible by any of the monomials occurring as leading monomials in the corresponding Gröbner basis. Since $\mathbf{G}_p \subseteq \mathbf{G}$ we have also $\{\mathfrak{lm}(g_p) \mid g_p \in \mathbf{G}_p\} \subseteq \{\mathfrak{lm}(g) \mid g \in \mathbf{G}\}$. So the basis of $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathfrak{L}(\mathbf{G})\rangle$ will be contained in the basis of $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathfrak{L}(\mathbf{G}_p)\rangle$, which proves the claim. q.e.d.

2.12 Remark. This lemma will be not very useful in general, because for any partial Gröbner basis strictly contained in a Gröbner basis, the dimension might be infinite, but if we take the whole Gröbner basis $\mathbf{G}$, then $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$ may be finite anyway.
A much better way to come to a decision, whether the factor algebra is finite dimensional or not, is to use a truncated Gröbner basis $\mathbf{G}_t$, since $\mathbf{G}$ and $\mathbf{G}_t$ both generate the same ideal. So we expect the factor algebras $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{G}$ and $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{G}_t$ to have the same dimension.
Sadly our computations on a computer will not work due to the non-uniqueness of the normal form. So if we get a $\mathbb{K}$-basis for $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle$ then it will contain more elements than a basis for $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$, since it may contain two elements with different normal form, which are actually the same in $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$, so we get $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle) \geq \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle)$. Let us put this in mathematically correct terms:

2.13 Definition. Let $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ with truncated Gröbner basis $\mathbf{G}_t$. We call $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathfrak{L}(\mathbf{G}_t)\rangle)$, where $\mathfrak{L}(\mathbf{G}_t) := \{\mathfrak{lm}(g_t) \mid g_t \in \mathbf{G}_t\}$, the *fake dimension of* $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle$, and denote it by $\dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle)$.

2.14 Lemma. Let $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ with Gröbner basis $\mathbf{G}$ and truncated Gröbner basis $\mathbf{G}_t$. Then we have: $\langle\mathfrak{L}(\mathbf{G}_t)\rangle \subseteq \langle\mathfrak{L}(\mathbf{G})\rangle$.

Proof: Clear by definition of Gröbner basis. q.e.d.

2.15 Theorem. Let $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ with truncated Gröbner basis $\mathbf{G}_t$.
Then $\dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle) \geq \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/I)$.

Proof:
$$\dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle) = \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathfrak{L}(\mathbf{G}_t)\rangle) \overset{2.14}{\geq} \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathfrak{L}(\mathbf{G})\rangle)$$
$$= \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/I)$$
q.e.d.

So if we achieve finite fake dimension, we can conclude that our $\mathbb{K}$-dimension is finite, too. This can be used to upgrade Algorithm 1.54 in the following way: Before starting the Gröbner basis computation with the new degree bound, check if we already achieved finite fake dimension. Then the factor algebra will have finite $\mathbb{K}$-dimension as well and we can return this information.
Sometimes one knows the $\mathbb{K}$-dimension of the algebra, but needs to find a Gröbner basis. In these cases, the following statement will be of great use:

2.16 Theorem. Let $\mathbf{I} \trianglelefteq \mathbb{K}\langle\mathbf{X}\rangle$ with truncated Gröbner basis $\mathbf{G}_t$ of degree q. If $\dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle) = \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I})$, then $\mathbf{G}_t$ is a Gröbner basis for $\mathbf{I}$.

Proof: Assume we have $g_1, g_2 \in \mathbf{G}_t$, such that the leading monomials have an overlap and $\tilde{q} = \deg_t(\mathfrak{NF}(s(l, g_1, r; \lambda, g_2, \rho), \mathbf{G}_t)) > q$.
Now if $s := s(l, g_1, r; \lambda, g_2, \rho)$ is not weak with respect to $\mathbf{G}_t$, then there is no $g_t \in \mathbf{G}_t$, such that $\mathfrak{lm}(g_t) \mid \mathfrak{lm}(s)$.
This implies $\dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle) > \dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t \cup \{s\}\rangle)$. Now let $\tilde{\mathbf{G}}_t$ be a truncated Gröbner basis of degree $\tilde{q}$. It certainly contains a g_s, such that $\mathfrak{lm}(g_s) \mid \mathfrak{lm}(s)$, so without loss of generality we may assume $s \in \tilde{\mathbf{G}}_t$. But then we have $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}) = \dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}_t\rangle) > \dim_f(\mathbb{K}\langle\mathbf{X}\rangle/\langle\tilde{\mathbf{G}}_t\rangle)$, which is a contradiction to Theorem 2.15. q.e.d.

Our goal now is to state an algorithm which can decide whether a given factor algebra has finite $\mathbb{K}$-dimension. Recall 2.3, which tells us that we only need to consider the leading monomials of a given Gröbner basis, so we identify $\mathbf{G}$ with $\mathfrak{L}(\mathbf{G})$. We assume that our Gröbner basis is reduced, which means that no $\mathfrak{lm}(g)$, $g \in \mathbf{G}$, divides any monomial in $\mathbf{G} \setminus \{g\}$.
In terms of a monomial algebra one often speaks about *words* instead of monomials, the set $\mathbf{X}$ is called the *set of all words* over an *alphabet* of n *letters*, corresponding to the generators of $\mathbf{X}$. The total degree of a monomial is called the *length* of a word and will be denoted with $\mathfrak{lg}$. A word w is called **standard** or **normal** with respect to $\mathbf{G} \subset \mathbf{X}$, if it is not divided by one of the monomials in $\mathbf{G}$, denoted by $\mathbf{G} \nmid w$ (recall that this means $r_{\mathbf{G}}(w) = w$) or $\mathbf{G} \mid w$, if there is a monomial in $\mathbf{G}$ that divides w (which implies $r_{\mathbf{G}}(w) = 0$).
The difference here is that we allow words of infinite length, whereas the free monoid $\mathbf{X}$ consists only of monomials of finite total degree.

2.17 Remark. For a Gröbner basis $\mathbf{G}$ consisting of monomials the set of all non-zero standard words equals the set of non-zero normal forms of elements in $\mathbf{X}$. So the set of all standard words is a basis for $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$.

2.18 Lemma. A basis for $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$ is infinite if and only if it contains a standard word of infinite length.

Proof:
"$\Rightarrow$": Since our alphabet $\mathbf{X}$ is finite there are only finitely many words up to a given length.
"$\Leftarrow$": A word i of infinite length contains infinitely many subwords. Since i is a standard word, so are all of its subwords. q.e.d.

2.19 Definition. Given an alphabet $\mathbf{X}$ and a set of monomials $\mathbf{G}$, we can define the *Ufnarovskij graph* G_U. Its vertex set V consists of all standard words $w \in \mathbf{X}^{l_{\mathbf{G}}} = \{m \in \mathbf{X} \mid m = x_{i_1} \cdots x_{i_{l_{\mathbf{G}}}}\}$, where $l_{\mathbf{G}} := -1 + \max_{m \in \mathbf{G}} \mathfrak{lg}(m)$. For each $v, w \in V$ there is a directed edge (v, w) if and only if there exists $a, b \in \mathbf{X}$ such that $va = bw$ and $\mathbf{G} \nmid va$.

The graph is named after Victor Ufnarovskij, who introduced it in his work [Ufn89] and discussed it further in [Ufn90].

2.20 Remark.

1. There is a one-to-one correspondence between paths of length l in G_U and standard words of length $l + l_{\mathbf{G}}$. This implies that each infinite standard word corresponds to an infinite path in G_U, which must contain a cycle, because G_U has a finite vertex set due to the finiteness of $\mathbf{X}$ and $\mathbf{G}$. Therefore we have $\dim_{\mathbb{K}}(\mathbb{K}\langle \mathbf{X}\rangle/\langle \mathbf{G}\rangle) = \infty$ if and only if G_U contains a cycle.

2. If there exists an infinite word that is standard with respect to $\mathbf{G}$, then either it is cyclic or it gives rise to a cyclic infinite word that is also standard with respect to $\mathbf{G}$.

2.21 Lemma. If there exists an infinite word $w' \in \mathbf{X}$ that is standard with respect to $\mathbf{G}$, then there also exists a cyclic infinite word $w \in \mathbf{X}$ that is standard with respect to $\mathbf{G}$ such that

$$\forall r, s \geq 1 : \; w[1 \ldots s] \leq w[r \ldots r + s - 1], \tag{2.1}$$

where $w[p \ldots q]$ is the subword of w obtained by removing the first up to the $(p-1)$-th and the $(q+1)$-th up to the last letter.

Proof: We will use $u \trianglelefteq v$ to denote that u is a prefix of v, respectively $u \triangleleft v$, if it is a proper prefix. Further we denote with u^t the word consisting of the concatenation of t copies of the word u.
Let $w' \in \mathbf{X}$ be infinite and standard with respect to $\mathbf{G}$. Then w' gives rise to a cyclic infinite word $w'' = v'^{\infty}$, where $v' \in \mathbf{X}^p$ for some finite $p > 0$. Assume that v is the lexicographically smallest shift of v'. Then there is a $u \trianglelefteq v'$ such that $v'^{\infty} = uv^{\infty}$. Now define $w := v^{\infty}$ and the claim follows. q.e.d.

The lemma states that in order to find an infinite word, it suffices to use only words satisfying (2.1). So we will proceed as follows: For a given Gröbner basis $\mathbf{G}$ we build up the Ufnarovskij graph. If $\mathbb{K}\langle \mathbf{X}\rangle/\langle \mathbf{G}\rangle$ has infinite $\mathbb{K}$-dimension, the graph will contain a cycle; if it is finite, the graph will be a tree.
Note that the Ufnarovskij graph is only defined for finite Gröbner bases, since in an infinite one has no upper degree bound.
In the following algorithm we assume $x_1 < x_2 < \ldots < x_n$.

2.22 Algorithm.
Input: A Gröbner basis $\mathbf{G}$ of the ideal $\mathbf{I}$
Output: $\begin{cases} \text{true,} & \text{if the dimension of } \mathbb{K}\langle \mathbf{X}\rangle/\mathbf{I} \text{ is infinite,} \\ \text{false,} & \text{else.} \end{cases}$

```
  Start with $w = 1,\ V = \emptyset$.
  If $w$ is normal w. r. t. $\mathbf{G}$ then:
```

- If $\mathfrak{lg}(w) < l_{\mathbf{G}}$: Extend w to $v = w \cdot x_i$ for $i = 1, \dots, n$ and start again.
- If $\mathfrak{lg}(w) \geq l_{\mathbf{G}}$: Set $v = w[(k - l_{\mathbf{G}} + 1) \dots k]$
  - · If $v \in V$ **return** true
  - · If $v \notin V$ set $V' = V \cup \{v\}$ and start again with $v \cdot x_i$ and V' for $i = 1, \dots, n$.

If w is not normal w. r. t. $\mathbf{G}$ then return to the point of the last extension of w.
If all normal words have been checked **return** false.

Proof: There are two possibilities we have to consider:

- Assume $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$ has infinite dimension. The set V contains the vertices of the corresponding Ufnarovskij graph. Due to the one-to-one correspondence between paths and words we are moving along the edges of the graph by building up the word. Since the Ufnarovskij graph must contain a cycle, by assumption we will discover the same vertex twice. Because the Ufnarovskij graph has only finitely many edges, this will happen after finitely many steps and the algorithm will terminate.

- Now let $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$ be of finite $\mathbb{K}$-dimension. Then the Ufnarovskij graph contains no cycle, so we can never discover the same vertex twice. Because there are only finitely many normal words by assumption, the algorithm will terminate after finitely many steps and return "false". q.e.d.

Algorithm 2.22 is formulated in the most easy way to understand the concept. However, there is the great disadvantage of this formulation: In the finite case we check every normal word, which could be quite many. However, if one already knows that a normal word of length $l_{\mathbf{G}}$ does not lead to a cycle, one can add it to $\mathbf{G}$, avoiding to check extensions of this word and thereby reducing the total number of words to check.

2.23 Example.

1. Take $\mathbf{A} = \{x, y\}, G = \{xxx, xyx, yxy\}$. We will start with $w_1 = x$, since $w_0 = 1$ is only needed for the formulation of the algorithm (since 1 is always a basis element). Let us assume $x > y$, so we extend every word with x first, then with y. Note that $l_{\mathbf{G}} = 2$, so our vertices will be all normal words of length 2. The candidates for those are underlined.
   The word $w_1 = x$ is normal, so set $V = \emptyset$. We extend it by x to $w_{11} = \underline{xx}$, which is still normal, so we set $V = \{xx\}$.
   With $w_{111} = x\underline{xx}$ we discover the first word which is not normal, so we do not need to extend it any further. Therefore we extend w_{11} now to $w_{112} = x\underline{xy}$, which is normal and we set $V = \{xx, xy\}$. Extending again with x leads to $w_{1121} = xx\underline{yx}$, which is of course not normal, so we extend to $w_{1122} = xx\underline{yy}$ and add it to V, that is $V = \{xx, xy, yy\}$. Extending twice

with x yields $w_{11221} = xxy\underline{yx}$ and $w_{112211} = xxyy\underline{xx}$. While the first one adds yx to V, the latter one implies xx is a new element for V. Since xx is already contained in V we have discovered a cycle and can conclude, that the dimension is not finite.
Of course one could conclude this outcome using Lemma 2.9.

2. Take $\mathbf{A} = \{x, y\}, G = \{xx, xyx, yy\}$. Again we have $l_{\mathbf{G}} = 2$ and we get, using the same notation as before, that w_1 is normal, while w_{11} is not. Extending w_1 to $w_{12} = \underline{xy}$, which is a normal word, leads us to $V = \{xy\}$. Then $w_{121} = xy\underline{x}$ and $w_{122} = xy\underline{y}$ are not normal and we can add xx and xy to the set G and starting again by resetting V.
Now $w_2 = y$ is a normal word, which can be extended to $w_{21} = \underline{yx}$, which is normal again, so we set $V = \{yx\}$. With our new added words, we conclude that $w_{211} = y\underline{xx}$ and $w_{212} = y\underline{xy}$ are not normal or at least we will not discover a cycle using these words.
So the last word we have to check is $w_{22} = y\underline{y}$, which is not normal. Since we have checked all normal words without discovering a cycle, we can conclude that the dimension is finite.

Since we have not seen an Ufnarovskij graph yet, let us draw the ones for the examples in 2.23.

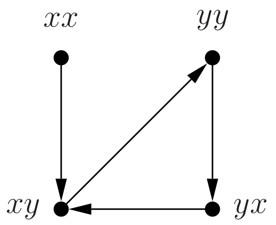


Figure 2.3: The Ufnarovskij graph for $\mathbf{G} = \{xxx, xyx, yxy\}$

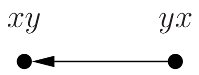


Figure 2.4: The Ufnarovskij graph for $\mathbf{G} = \{xx, yxy, yy\}$

2.24 Remark. There are many application for this algorithms. We like to highlight one special applications:
For a given finitely presented group G one is interested, if G is finite. Therefore, one can consider the group algebra $\mathbb{K}G$. So one can consider $\mathbb{K}G$ as an factor of the free algebra and can apply the methods presented above. For more information regarding this topic we refer to [KMRU05].

2.4 $\mathbb{K}$-Bases of Factor Algebras

We have now the possibility to check if a factor algebra given by a (reduced) Gröbner basis has finite $\mathbb{K}$-dimension or not. Once we know that a factor algebra is of finite dimension, one may want to compute a $\mathbb{K}$-basis. This is the goal of this section.
For obvious reasons we will always assume $\mathbf{I} \lhd \mathbb{K}\langle \mathbf{X} \rangle$.

2.25 Algorithm.
Input: A Gröbner basis $\mathbf{G}$ of the ideal $\mathbf{I} \lhd \mathbb{K}\langle \mathbf{X} \rangle$
Output: A $\mathbb{K}$-basis B of $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$

```
Set $\tilde{B} := \{1\}, B_{temp} := \emptyset, B := \{1\}$
while $\tilde{B} \neq \emptyset$ do
  for $j = 1$ to $|\tilde{B}|$ do
    for $i = 1$ to $n$ do
      if $\mathbf{G} \nmid \tilde{B}[j] \cdot x_i$ then
        $B = B \cup \{\tilde{B}[j] \cdot x_i\}$; $B_{temp} = B_{temp} \cup \{\tilde{B}[j] \cdot x_i\}$;
      end if
    end for
  end for
  $\tilde{B} = B_{temp}; B_{temp} = \emptyset$;
end while;
return $B$;
```

2.26 Theorem. If $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$ has finite dimension, then Algorithm 2.25 terminates and returns a $\mathbb{K}$-basis of the factor algebra.

Proof: Since $\mathbf{I} \neq \mathbb{K}\langle \mathbf{X} \rangle$ we have $1 \in B$. Assume we have found all basis elements up to degree $d \geq 1$. To construct all elements of degree $d+1$, we just have to consider those elements which do not contain any subwords s, such that $\deg_t(s) \leq d$ and $s \in G$. Those are of the form $p \cdot x_i,\ i = 1, \ldots, n,\ p \in \{q \in B \mid \deg_t(q) = d\}$. Now if all new monomials can be reduced to zero with respect to $\mathbf{G}$ there will not be any elements of degree $d + r,\ r \in \mathbb{N}$ and the algorithm stops. Since we have assumed that the dimension is finite, there will be a $m \in \mathbb{N}$, such that $m = \max\{\deg_t(p) \mid p \in B\}$, which implies that the algorithm will terminate. q.e.d.

Before we examine our achievements further let us consider an example.

2.27 Example.

1. Take $A := \mathbb{K}\langle x, y \rangle / \langle \mathbf{G} \rangle$ with $\mathbf{G} := \{x^2, y^2, xy\}$, which is clearly a Gröbner basis. The algorithm does the following steps:
   a) $\mathbf{G} \nmid x, y \implies B = \{1, x, y\};\ \tilde{B} = \{x, y\}$;
   b) i. $\mathbf{G} \mid x^2; \mathbf{G} \mid xy$;
      ii. $\mathbf{G} \nmid yx; \mathbf{G} \mid y^2 \implies B = \{1, x, y, yx\};\ \tilde{B} = \{yx\}$;

   c) $\mathbf{G} \mid yx^2; \mathbf{G} \mid yxy; \implies \tilde{B} = \emptyset$

   RETURN: $B = \{1, x, y, yx\}$;

2. We already know from 2.23 that the factor algebra by $\mathbf{G} = \{x^2, yxy, y^3\}$ has finite $\mathbb{K}$-dimension. So let us see a basis for that one:
   a) $\mathbf{G} \nmid x, y \implies B = \{1, x, y\};\ \tilde{B} = \{x, y\}$;
   b) $\mathbf{G} \mid x^2;\ \mathbf{G} \nmid xy;\ \mathbf{G} \nmid yx; \mathbf{G} \nmid y^2$
   $\implies B = \{1, x, y, yx, xy, y^2\};\ \tilde{B} = \{xy, yx, y^2\}$;
   c) $\mathbf{G} \nmid xyx;\ \mathbf{G} \nmid xy^2\mathbf{G} \mid yx^2;\ \mathbf{G} \mid yxy;\ \mathbf{G} \nmid y^2x;\ \mathbf{G} \mid y^3$
   $\implies B = \{1, x, y, xy, yx, y^2, xyx, xy^2, y^2x\};\ \tilde{B} = \{xyx, xy^2, y^2x\}$;
   d) $\mathbf{G} \mid xyx^2;\ \mathbf{G} \mid xyxy;\ \mathbf{G} \nmid xy^2x;\ \mathbf{G} \mid xy^3;\ \mathbf{G} \mid y^2x^2;\ \mathbf{G} \mid y^2xy$
   $\implies B = \{1, x, y, xy, yx, y^2, xyx, xy^2, y^2x, xy^2x\}; \tilde{B} = \{xy^2x\}$;
   e) $\mathbf{G} \mid xy^2x^2;\ \mathbf{G} \mid xy^2xy$;
   $\implies B = \{1, x, y, xy, yx, y^2, xyx, xy^2, y^2x, xy^2x\}; \tilde{B} = \emptyset$;

   RETURN: $B = \{1, x, y, xy, yx, y^2, xyx, xy^2, y^2x, xy^2x\}$;

2.28 Remark. Let us enlist some of the advantages of 2.25:

- It is very easy to implement a truncated version of this algorithm by just stopping at a given degree, even if $\tilde{B} \neq \emptyset$.

- One can easily compute finite number of terms of the *Hilbert series*, that is, the formal series $\sum_{i=1}^{\infty} \dim_{\mathbb{K}}(A_i) \cdot t^i$, where $A_i = \{p \in \mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I} \mid \deg_t(p) = i\}$ and t is a formal variable, if one just stores the number of new elements of degree i, that is, the elements of $\tilde{B}$, which form a basis of A_i. Of course the Hilbert series is by definition not finite, so it is impossible to compute it in practice. However, if we provide a degree bound or if the factor algebra is of finite $\mathbb{K}$-dimension one can compute at least a part of the series: One can compute the coefficients up to a given degree or, in the finite case, up to $k \in \mathbb{N}$, such that $\dim_{\mathbb{K}}(A_j) = 0\ \forall j > k$. In that cases the Hilbert series is a polynomial.

- Note that we only add new elements by right multiplication!

The last point leads to an interesting observation: Every normal word is uniquely determined by its path in the algorithm.

2.29 Definition. The *basis tree* of $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ is the directed graph with vertex set $V = \{m \in \mathbf{X} \mid \mathbf{G} \nmid m\}$ and there is an edge from m to m', if and only if $m' = m \cdot x_i$ for one $i \in \{1, \ldots, n\}$.

2.30 Remark. We would like to mention that in computer science structures like the basis tree are well-known and called *trie*. They are usually used to work with strings and are applied for example to auto-complete words. For more information we refer to [CR94].

2.31 Remark. We construct the basis tree by right multiplication with the variables. If one would construct the basis tree by left multiplication, the set of edges would be different, namely there is an edge from m to m', if and only if $m' = x_i \cdot m$ for one $i \in \{1, \ldots, n\}$. Thus we should distinguish between right basis trees and left basis trees. Since all the results for a right basis tree are valid for a left basis tree as well, we will only study right basis trees.

2.32 Example. Let us consider a small example for the difference between left and right basis trees:
Take $\mathbf{G} = \{y^2 - y, xyx - xxy, yx^2 - x^2y, yxy - yx, x^4 - \frac{3}{5}x^3 + \frac{1}{5}yx - \frac{1}{5}xy + \frac{2}{5}x^2 + \frac{1}{5}x\} \subset \mathbb{K}\langle x, y\rangle$. Then one checks easily that $\mathbf{G}$ is a Gröbner basis for $\mathbf{J} = \langle \mathbf{G} \rangle$. We get the following two different basis trees:

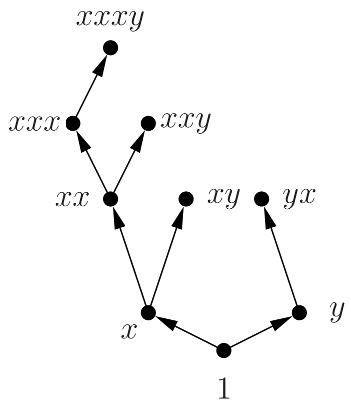


Figure 2.5: The right basis tree

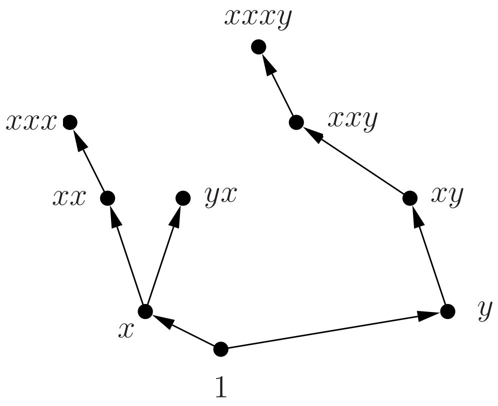


Figure 2.6: The left basis tree

2.33 Example.
Let us draw the basis trees for the examples above:

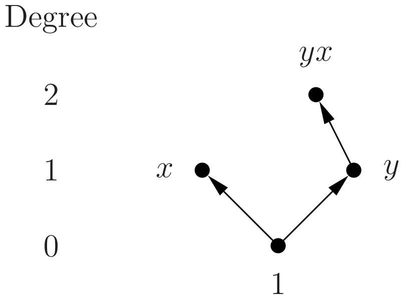


Figure 2.7: The basis tree for $\mathbf{G} = \{x^2, y^2, xy\}$, cf. Example 2.27.1

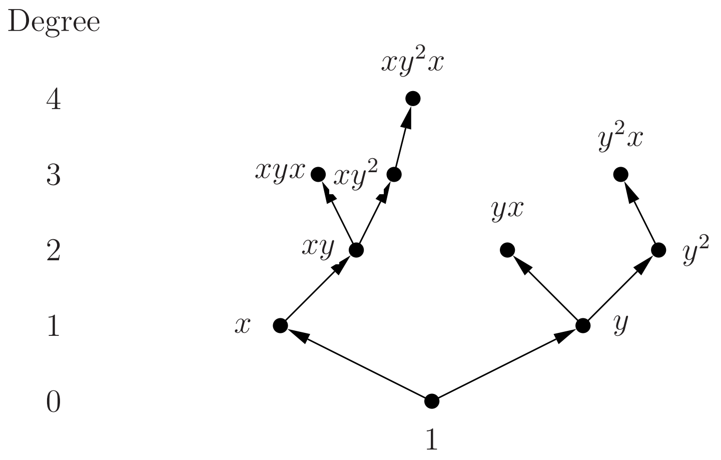


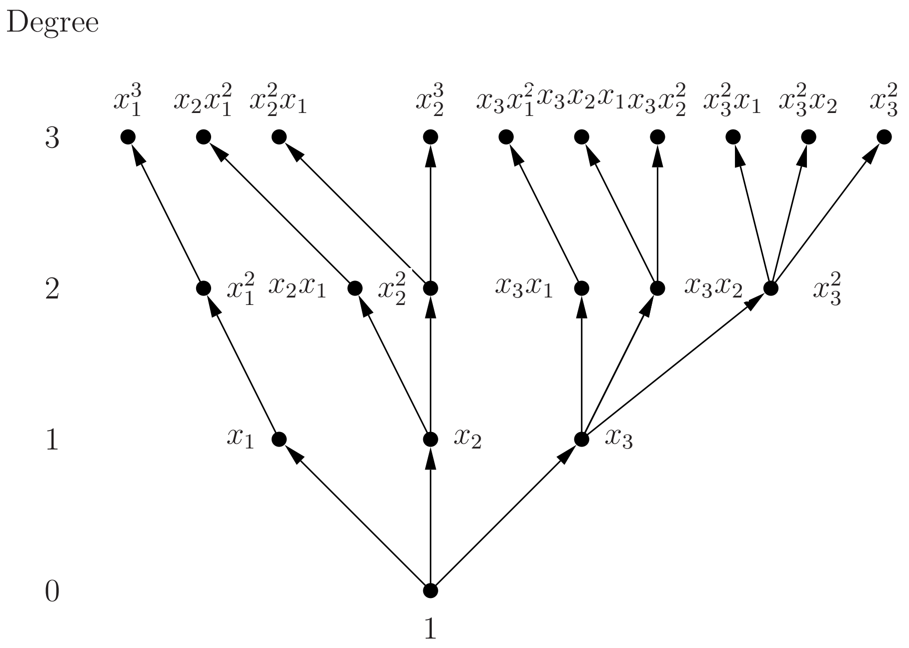
Figure 2.8: The basis tree for $\mathbf{G} = \{x^2, yxy, y^3\}$, cf. Example 2.27.2

2.34 Theorem. The basis tree for any reduced Gröbner basis is a tree, that is, every vertex is uniquely determined by its path.

Proof: Clear by construction of the basis in Algorithm 2.25. q.e.d.

2.35 Remark. Note that 2.34 has no analog in the commutative case. There, different ways may lead to the same basis element.
For example $1 \to x \to xy \to xyx$ and $1 \to y \to yx \to yxx$ are different paths, but due to commutativity, we have $xyx = yxx = x^2y$. So the non-commutative case is absolutely different, comparing with the commutative one, at least in this respect.

2.36 Example. As seen before $\mathbf{G} = \{x_ix_j - x_jx_i \mid 1 \leq i < j \leq n\} \subset \mathbb{K}\langle\mathbf{X}\rangle$ is a Gröbner basis. We want to see that we can construct the commutative polynomial ring P and still get a well defined basis tree. We will do this for $n = 3$ and up to degree 3. We assume that we have chosen the graded lexicographical ordering with $x_1 > x_2 > x_3$.
Then $\mathfrak{L}(\langle\mathbf{G}\rangle) = \langle\{x_1x_2, x_1x_3, x_2x_3\}\rangle$. Then the basis tree looks like this:



2.37 Remark. Recall that we always assume that our Gröbner basis is reduced. This leads to the following observation:

2.38 Lemma. Let $\mathbf{G}$ be a reduced Gröbner basis and take $g \in \mathbf{G}$ and say $\deg_t(g) = d$. Then $\mathfrak{lm}(g)[1, \ldots, d-1]$ is a normal word with respect to $\mathbf{G}$.

Proof: Obviously $\mathfrak{lm}(g) \nmid \mathfrak{lm}(g)[1, \ldots, d-1]$. Since $\mathbf{G}$ is reduced we have $\mathfrak{lm}(\tilde{g}) \nmid \mathfrak{lm}(g)\ \forall \tilde{g} \in \mathbf{G}$, which implies $\mathfrak{lm}(\tilde{g}) \nmid \mathfrak{lm}(g)[1, \ldots, d-1]\ \forall \tilde{g} \in \mathbf{G}$. q.e.d.

2.39 Theorem.
If $\mathbf{G}$ is a reduced Gröbner basis and $|\mathbf{G}| = \infty$, then $\dim_{\mathbb{K}}(\mathbb{K}\langle \mathbf{X} \rangle / \langle \mathbf{G} \rangle) = \infty$.

Proof: By Lemma 2.38 the set $B = \{\mathfrak{lm}(g)[1, \ldots, d-1] \mid g \in \mathbf{G}, \deg_t(g) = d, d \in \mathbb{N}\}$ contains only normal words with respect to $\mathbf{G}$, therefore we have $\dim_{\mathbb{K}}(\mathbb{K}\langle \mathbf{X} \rangle / \langle \mathbf{G} \rangle) \geq |B|$.
Since the number of letters is finite only finitely many leading monomials in $\mathbf{G}$ ill contain the same subword, which implies $|B| = \infty$. q.e.d.

2.40 Corollary. If $\dim_{\mathbb{K}}(\mathbb{K}\langle \mathbf{X} \rangle / \langle \mathbf{G} \rangle) < \infty$, then $|\mathbf{G}| < \infty$ as well.

Proof: This is the negation of Theorem 2.39. q.e.d.

2.41 Remark. This is a nice way to estimate the dimension and answer Question 1 in 2.1 in some cases. However, there is no general way to decide if an ideal will have an infinite Gröbner basis. Since the $\mathbb{K}$-dimension of a factor algebra depends not on the chosen ordering, if we find one infinite Gröbner basis we can apply Theorem 2.39. In some cases this is possible, as one can see in Example 1.38.

Again we want to point out the importance of an adaptive algorithm: As stated before one can check in each step of Algorithm 1.54 if one has achieved finite fake dimension. If so, one knows that the Gröbner basis will be finite and one can pursue the computation until the whole Gröbner basis is determined. So there is a great advantage in the combination of these procedures.

2.42 Remark. When we have constructed the basis tree for a given factor algebra, we expect to have all the information we want. However, Figure 2.6 shows that drawing the basis tree easily gets challenging. So we need a good way to store our information. This is the goal of the next section.

2.5 Mistletoes

We will still assume that $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ has finite $\mathbb{K}$-dimension.

2.43 Definition. For a given basis tree a vertex with no edges starting at it is called *mistletoe*.

We like to mention that in graph theory mistletoes are sometimes called *leaves*, but since the definition may differ, depending on the author, we stick to the term mistletoe, to emphasize the special value of these vertices.

2.44 Remark. In Romanian traditions, mistletoes are considered a source of good fortune. We will see that this is true, at least for the mistletoes growing on a basis tree.
Considering Example 2.32, we observe that for a left basis tree the mistletoes are different from those given by a right basis tree, but again all the results for right mistletoes are valid for the left mistletoes as well. Since mistletoes are elements of the vertex set of the basis tree, they are uniquely determined by the path that leads to them, as stated in 2.34.

2.45 Lemma. Every vertex v in a basis tree can be extended to a mistletoe, that is there is a path in the basis tree that starts in v and ends up in a mistletoe.

Proof: If v is a mistletoe there is nothing to prove, so assume the contrary. Then there is an edge starting in v and leading to $v' = v \cdot x_i$ for some $i \in \{1, \ldots, n\}$. If v' is a mistletoe we are finished again. If not there is an edge leading to an extension of v'. If we do this iteratively we reach a mistletoes, since we are strictly increasing the degree and we have assumed that basis tree has only a finite number of vertices. q.e.d.

2.46 Remark. Algorithm 2.25 can be used to compute the mistletoes, since they are basis elements. The modifications are quite simple: Assume we have $\tilde{B} \neq \emptyset$. If $\mathbf{G} \mid \tilde{B}[j] \cdot x_i \quad \forall i = 1, \ldots, n$ then $\tilde{B}[j]$ is a mistletoe and we store it. Otherwise we proceed as in 2.25.
We make the following observation:

2.47 Theorem. The set of all mistletoes of a $\mathbb{K}$-basis for $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ uniquely determines the whole $\mathbb{K}$-basis.

Proof: Since every vertex lies beneath a mistletoe and mistletoes are uniquely determined by their paths, we get every vertex by removing the last variables of mistletoe, that is, going backwards along the path. So out of the set of mistletoes we can construct every basis element, that is, we know the whole basis. q.e.d.

2.48 Remark. Note that we have different choices for a $\mathbb{K}$-basis, but if we have a reduced Gröbner basis, there is only one choice for a basis consisting only of monomials, namely the set of normal words. So when we say "uniquely determine", we mean the monomial basis, fixed by the chosen ordering, not the choice for a basis.
In general there will be vertices lying under more than one mistletoe. For example, let us consider 2.27 (2) again. One can see the mistletoes directly from Figure 2.6: $M = \{xyx, xy^2x, yx, y^2x\}$. Now the basis element xy lies under $m_1 = xyx$ and $m_2 = xy^2x$. In theory this is not a problem, because
$\{xyx, xy, x, 1, xy^2x, xy^2, xy, x, 1, yx, y, 1, y^2x, y^2, y, 1\} = \{xy^2x, xy^2, xyx, y^2x,$
$xy, yx, y^2, x, y, 1\}$ as sets. However, if we want to compute the basis or the dimension for a factor algebra given through mistletoes, this is a problem. Therefore it is necessary to compute the *intersection* of two mistletoes.

2.49 Definition. For two given mistletoes $m_1 \neq m_2$ we define the *intersection* of m_1 and m_2 as the largest common left subword, that is,

$$\iota(m_1, m_2) = m_1[1, \ldots, k] = m_2[1, \ldots, k],$$

where $k \geq 0$ is maximal and $k = 0$ corresponds to $\iota(m_1, m_2) = 1$.

2.50 Remark. Recall that we always assume that the ideal $\mathbf{I}$ is given via a Gröbner basis $\mathbf{G}$. For the computation of $\mathbf{G}$ we have to fix an ordering. However, we can rearrange the branches of the basis tree, that is, we order the mistletoes, without changing anything, since the set of mistletoes is invariant under permutation. This corresponds to the fact that we can draw the basis tree as we like: even if $x_2 > x_1$ we can draw the edges corresponding with multiplication with x_1 leftmost.

How can we use this to find the intersections?

2.51 Lemma. Let $M = \{m_1, \ldots, m_l\}$ be the set of mistletoes for $\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle$. Let us order them lexicographically, that is $m_1 \geq_{\text{lex}} m_2 \geq_{\text{lex}} \ldots \geq_{\text{lex}} m_l$. Then the set of all intersections is given by $\{\iota(m_i, m_{i+1}) \mid m_i \in M, i = 1, \ldots, l-1\}$.

Proof: We need to show: $\forall 1 \leq k \neq j \leq l \; \exists 1 \leq i \leq l : \quad \iota(m_k, m_j) = \iota(m_i, m_{i+1})$.
We may assume without loss of generality that $k < j$, since
$\iota(m_k, m_j) = \iota(m_j, m_k)$. If $j = k+1$ there is nothing to show, so assume otherwise,

that is, there are at least 3 mistletoes atop $\iota(m_k, m_j)$. We use induction on the number of mistletoes. Assume $j = k + 2$. If $\iota(m_k, m_{k+1}) \geq_{\text{lex}} \iota(m_{k+1}, m_j)$ then $\iota(\iota(m_k, m_{k+1}), m_j) = \iota(m_{k+1}, m_j)$, that is, $\iota(m_{k+1}, m_j)$ is the greatest common left subword of $\iota(m_k, m_{k+1})$ and m_j. Since the mistletoes are uniquely determined by their paths, it is also the greatest common left subword of m_k and m_j which implies $\iota(m_k, m_j) = \iota(m_{k+1}, m_j)$. If $\iota(m_k, m_{k+1}) \leq_{\text{lex}} \iota(m_{k+1}, m_j)$ the same argument can be applied and we get $\iota(m_k, m_j) = \iota(m_k, m_{k+1})$.
Now assume $j = k + n$ and the assumption is true for all $\iota(m_{\tilde{k}}, m_{\tilde{k}+n-1})$. Then there exists $\tilde{i}$, such that $\iota(m_k, m_{j-1}) = \iota(m_{\tilde{i}}, m_{\tilde{i}+1}) =: I$.
Then $I \geq_{\text{lex}} \iota(m_{j-1}, m_j)$ or $I \leq_{\text{lex}} \iota(m_{j-1}, m_j)$ and we get (arguing as above) either $\iota(m_k, m_j) = \iota(m_{j-1}, m_j)$ or $\iota(m_k, m_j) = I$. q.e.d.

We will now state several algorithms which are working with mistletoes, starting with recovering the basis.

2.52 Algorithm.

```
Input: $M = \{m_1, \ldots, m_l\}$, the set of mistletoes for $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$, lexicographically ordered
Output: A monomial $\mathbb{K}$-basis $B$ of $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$.
  Set $B = \{1\}$.
  for $j = 1$ to $\mathfrak{lg}(m_1)$ do
    $B = B \cup \{m_1[1 \ldots j]\}$
  end for
  for $i = 1$ to $l$ do
    Set $k = \mathfrak{lg}(\iota(m_{i-1}, m_i)) + 1$
    for $j = k$ to $\mathfrak{lg}(m_j)$ do
      $B = B \cup \{m_i[k \ldots j]\}$
    end for
  end for
  return $B$
```

Proof: Clear by construction of the mistletoes and Lemma 2.51. q.e.d.

This algorithm ensures that we are always able to get our $\mathbb{K}$-basis. However, it is not necessary to construct the basis. If one only wants to know the dimension one can apply the following algorithm:

2.53 Algorithm.

```
Input: $M = \{m_1, \ldots, m_l\}$, the set of mistletoes for $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$, lexicographically ordered
Output: The $\mathbb{K}$-dimension of $\mathbb{K}\langle \mathbf{X} \rangle / \mathbf{I}$
  Set $k = \mathfrak{lg}(m_1) + 1$
  for $j = 1$ to $l - 1$ do
    $k = k + (\mathfrak{lg}(m_{j+1}) - \mathfrak{lg}(\iota(m_j, m_{j+1})))$
  end for
  return $k$
```

Proof: The mistletoe m_k stores $\mathfrak{lg}(m_k)$ basis elements, from which we already considered
$\mathfrak{lg}(\iota(m_{k-1}, m_k))$ ones. This proves $k = \dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I})$. If $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I})$ is finite, the termination is obvious, since we have a finite set of mistletoes of finite length. q.e.d.

Now if we can compute the $\mathbb{K}$-dimension, we are also able to compute the Hilbert series.

2.54 Algorithm.

Input: $M = \{m_1, \ldots, m_l\}$, the set of mistletoes for $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$, lexicographically ordered, $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}) < \infty$

Output: The coefficients of the Hilbert series of $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ as a vector of integers H

```
Set $H[0] = 1$
for $j = 1$ to $\mathfrak{lg}(m_1)$ do
    $H[j] = 1$
end for
for $i = 2$ to $l$ do
    Set $k = \mathfrak{lg}(\iota(m_{j-1}, m_j))$
    for $i = k$ to $\mathfrak{lg}(m_j)$ do
        $H[i] = H[i] + 1$
    end for
end for
return $H$
```

Proof: As before, m_k stores $\mathfrak{lg}(m_k)$ basis elements, from which we already considered $\mathfrak{lg}(\iota(m_{k-1}, m_k))$. Each of these elements has a different total degree, therefore increasing different coefficient of the Hilbert series by one. By setting $H[i] = c_i$, where c_i denotes the i^{th} coefficient of the Hilbert series, and increasing the corresponding entry in H we get the coefficients of the Hilbert series after finitely many steps, assuming that the Hilbert series is finite. q.e.d.

It would be nice if we could construct the Gröbner basis $\mathbf{G}$ for $\mathbf{I}$ from the mistletoes. This is not possible, since we are working with the leading monomials only. Thus two different Gröbner bases may give rise to the same set of mistletoes, respectively to the same $\mathbb{K}$-basis. So can we at least construct the leading monomials of $\mathbf{G}$?
The answer is again no. This is due to the fact that the greatest left subword of an element of $\mathbf{G}$ does not need to be a mistletoe. So in order to do arithmetic operations inside the factor algebra, we still need the Gröbner basis.

2.55 Remark. Although the next chapter focuses mainly at the implementation, one might be interested in the running time of the above algorithms. We take Algorithm 2.53 as an example. Now to use Lemma 2.51 we need to sort our

set of mistletoes, which will take $m\log(m)$ operations for a set consisting of m mistletoes. Then the comparison of the neighboring mistletoes will take $m-1$ operations and finally we have to add all of those mistletoes, which again takes $m-1$ operations. So we have an approximate runtime of $\mathcal{O}((m-1)^2 m\log(m)) \approx \mathcal{O}(m^3 log(m))$, which is rather bad.
We can try a different approach by just using combinatorial methods. However, this will give us only an upper bound for the dimension. But since this can be useful in certain situations we state the following algorithm.

2.56 Algorithm.

Input: $\{m_1, \ldots, m_m\}$, a set of mistletoes, n, the number of variables
Output: d_{est}, an integer

```
  Set $\tilde{m}$ as a mistletoe of minimal total degree $l_{min}$
  $g := \sum_{i=0}^{l_{min}} k_i$, where $k_i = \begin{cases} m, \text{ if } m < n^i \\ n^i, \text{else} \end{cases}$
  $d_{est} := g + \sum_{i=1}^{m} l_i - l_{min}$, where $l_i = \mathfrak{lg}(m_i)$.
  return $d_{est}$
```

While the termination of this algorithm is obvious due to the finiteness of m and n, we need to see that the returned result is of any use to us.

2.57 Lemma. With the setup of Algorithm 2.56 we have:

$$\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle G\rangle) \le d_{est}.$$

Moreover, equality holds, if $g = \sum_{i=0}^{l_{min}} n^i$ and $\mathfrak{lg}(\iota(m_i, m_j)) \le l_{min}\ \forall 1 \le i, j \le m$.

Proof:

- Let us first assume that $m > n^i\ \forall 1 \le i \le l_{min}$.
If there exists a non normal word of length l_{min}, then there exists a pair of mistletoes m_i, m_j, such that $\mathfrak{lg}(\iota(m_i, m_j)) > l_{min}$. So by assuming that those mistletoes have an intersection of length smaller than l_{min}, we have found a lower bound for the dimension and we can assume, that all words of length l_{min} are normal. Therefore $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle G\rangle) \le \sum_{i=0}^{l_{min}} n^i + \sum_{i=1}^{m}(\mathfrak{lg}(m_i) - l_k) - c \le \sum_{i=0}^{l_{min}} n^i + \sum_{i=1}^{m}(\mathfrak{lg}(m_i) - l_k)$, where c denotes the number of multiply counted words.

- Now assume that there exists k', such that $1 \le k' \le l_{min}$ and $m \le n^{k'}$.
Then there are at most m normal words of length k', so we may reduce our basis tree to this m branches of the basis tree and can argue further as above.

This proves $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle G\rangle) \leq d_{est}$.

Now in the special case, that $g = \sum\limits_{i=0}^{l_{min}} n^i$ and $\mathfrak{lg}(\iota(m_i, m_j)) \leq l_{min}\ \forall 1 \leq i, j \leq m$, one finds the equality by carefully studying the first case. q.e.d.

Let us count the number of operations made in Algorithm 2.56: To find a mistletoe of shortest total degree we have to do m operations, to compute g we have l_{min} operations and another m operations for the computation of d_{est} However, l_{min} does not depend on the number of mistletoes and is therefore a constant. This leaves us with a total runtime of $\mathcal{O}(m^2)$.

The question arises: How good is our estimation? We have already seen, that in some cases we even reach equality. The next lemma states an upper bound for our estimation.

2.58 Lemma. With the notations of Algorithm 2.56 we have:

$$d_{est} \leq 1 + \sum_{i=1}^{m} \mathfrak{lg}(m_j)$$

Proof:

- Assume $n^i \leq m\ \forall 1 \leq i \leq l_{min}$. Then we have:
  $d_{est} := \sum\limits_{i=0}^{l_{min}} k_i + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i) - l_{min} = \sum\limits_{i=0}^{l_{min}} n^i + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i) - l_k =$
  $\sum\limits_{i=1}^{n^l_{min}} l_{min} + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i) - l_k \leq \sum\limits_{i=1}^{m} l_{min} + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i) - l_{min} = \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i)$
- Assume $\exists 1 \leq k' \leq l_{min} :\ n^{k'} \geq m$. Then we have:
  $d_{est} := \sum\limits_{i=0}^{l_{min}} k_i + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i) - l_{min} = \sum\limits_{i=0}^{k'} n^i + \sum\limits_{i=k'+1}^{l_{min}} m + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i) - l_k \leq$
  $\sum\limits_{i=1}^{m} l_{min} + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i) - l_k = \sum\limits_{i=1}^{m} \mathfrak{lg}(m_i)$ q.e.d.

Note that $1 + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_j)$ is the "natural" bound for the $\mathbb{K}$-dimension. However, in most situations it is too big and there is only one situation, in which $\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\langle\mathbf{G}\rangle) = 1 + \sum\limits_{i=1}^{m} \mathfrak{lg}(m_j)$ holds, that is, every mistletoe is coprime with each other mistletoe.

2.6 Factor Algebras over Letterplace Rings

Our goal is now to construct a correspondence between a $\mathbb{K}$-basis of $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ and the Letterplace analogon $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$, where $\mathbf{J} = \iota(\mathbf{I})$, that is $\mathbf{J}$ is a Letterplace

ideal, especially $\mathbf{J}$ is shift-invariant. It is obvious, that most of the factor algebras $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$ will not have a finite $\mathbb{K}$-dimension, even if $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$ has finite $\mathbb{K}$-dimension, because with every element $p \in \mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$, $p \notin \mathbb{K}$, all shifts $s \cdot p$ will be in the algebra. These elements are linearly independent and the infiniteness of $\mathbf{P}$ implies the infiniteness of the $\mathbb{K}$-dimension.
Let us start with some basic definitions.

2.59 Definition. Let $B \subset \mathbb{K}\langle\mathbf{X}\rangle$. We call B a $\mathbb{K}$-*shift-basis* of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$, if $\bigcup\limits_{s\in\mathbb{N}} s \cdot B$ is a $\mathbb{K}$-basis of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$.

2.60 Lemma. A $\mathbb{K}$-shift-basis of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$ always exists.
Proof: Take a $\mathbb{K}$-basis of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$. Since $x_i(r)$ and $x_j(r+t)$ are linearly independent for all choices of $i, j, r, t \in \mathbb{N}$ it is already a $\mathbb{K}$-shift-basis. q.e.d.

Because the $\mathbb{K}$-basis will be infinite most times, the proof has only theoretical value. So our goal is to find a basis, which is as small as possible in some sense.

2.61 Definition. Let $B \subset \mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$. We call B a *minimal* $\mathbb{K}$-*shift-basis* of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$, if it is a $\mathbb{K}$-shift-basis and if for any $\mathbb{K}$-shift-basis $B' \subseteq B$ we have $B = B'$.

2.62 Lemma. Every $\mathbb{K}$-shift-basis B of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$ contains a minimal $\mathbb{K}$-shift-basis B' of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$.
Proof: Assume there exists an element $b \in B$, such that $b = s \cdot b'$ for some $s \in \mathbb{N}, b' \in B$. Then $b \in \bigcup\limits_{t\in\mathbb{N}} t \cdot (B/\{b\})$, so $B' := B/\{b\}$ is also a $\mathbb{K}$-shift-basis. So we can assume that we already have removed all such elements and call the set B' again. We show that B' is a minimal $\mathbb{K}$-shift-basis. Assume not, that is, there exists $B'' \subset B'$, such that B'' is again a $\mathbb{K}$-shift-basis. Take $b' \in B'/B''$. By assumption $b' \notin \bigcup\limits_{t\in\mathbb{N}} t \cdot B''$ and $b' \in \langle \bigcup\limits_{t\in\mathbb{N}} t \cdot B''\rangle$. But this would imply that $\bigcup\limits_{t\in\mathbb{N}} t \cdot B'$ is not linearly independent in contradiction to the assumption that B' is a $\mathbb{K}$-shift-basis. q.e.d.

2.63 Corollary. A minimal $\mathbb{K}$-shift-basis of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$ always exists.

Proof: By Lemma 2.60, there exists a $\mathbb{K}$-shift-basis, which contains a minimal $\mathbb{K}$-shift-basis. q.e.d.

2.64 Definition.

- Let B be a minimal $\mathbb{K}$-shift-basis of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$. Then $K := B \cap V$ is called a $\mathbb{K}$-*Letterplace-basis*.

- We call the number of elements in a $\mathbb{K}$-Letterplace-basis the *Letterplace-dimension of* $\mathbb{K}[\boldsymbol{X}|\boldsymbol{P}]/\boldsymbol{J}$, denoted by $\dim_{lp}(\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J})$.

2.65 Remark. Note that the Letterplace-dimension is well defined, since any two $\mathbb{K}$-Letterplace-bases have the same number of elements. The statement is obvious, since we can consider the vector space $\tilde{V} = V/(V \cap J)$. Then any $\mathbb{K}$-Letterplace-basis will be a $\mathbb{K}$-basis of $\tilde{V}$.

2.66 Theorem. Let $\mathbf{I} \subset \mathbb{K}\langle\mathbf{X}\rangle$ be an ideal and let $\mathbf{J} = \tilde{\iota}(\mathbf{I})$. Further let K be a $\mathbb{K}$-Letterplace-basis of $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$. Then $B := \iota^{-1}(K \cap V)$ is a $\mathbb{K}$-basis for $\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$.

Proof: Clearly all elements of B are linearly independent, so $B \subseteq B'$ for a $\mathbb{K}$-basis $B' \subset \mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}$. Assume there exists $b \in B' \setminus B$ and set $k := \iota(b)$. By assumption $k \notin K$, so we have $k = \sum\limits_{\tilde{k} \in K} a_{\tilde{k}}\tilde{k}$ for some $a_{\tilde{k}} \in \mathbb{K}$. It follows that $b = \iota^{-1}(k) = \iota^{-1}(\sum\limits_{\tilde{k} \in K} a_{\tilde{k}}\tilde{k}) = \sum\limits_{\tilde{k} \in K} a_{\tilde{k}}\iota^{-1}(\tilde{k}) = \sum\limits_{\tilde{b} \in B} a_{\tilde{k}}\tilde{b}$, which is a contradiction to the assumption that B' is a $\mathbb{K}$-basis. So we have $B = B'$, which proves the claim. q.e.d.

2.67 Corollary. Let $\mathbf{I} \subset \mathbb{K}\langle\mathbf{X}\rangle$ be an ideal and let $\mathbf{J} = \tilde{\iota}(\mathbf{I})$. Then

$$\dim_{\mathbb{K}}(\mathbb{K}\langle\mathbf{X}\rangle/\mathbf{I}) = \dim_{lp}(\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}).$$

Proof: This is a consequence of Theorem 2.66. q.e.d.

2.68 Remark. Note that for the correspondence we only need the vector space V. If we have constructed a factor algebra $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$ we face a special problem: The (commutative) multiplication in this algebra does not correspond to the multiplication in our original algebra. Take for example the elements $x(0)$ and $y(0)$. The standard multiplication in the Letterplace ring will satisfy $x(0) \cdot y(0) = x(0)y(0) = y(0)x(0)$, which is not an element of V. So it is necessary to introduce a new multiplication: For two monomials $p, q \in V$ with $\mathfrak{lg}(p) = s$ we define $p * q = p(s \cdot q) \in V$. However, our previous example shows that this multiplication is not commutative, $y(0) * x(0) = y(0)x(1) \neq x(0)y(1) = x(0) * y(0)$, so we do not get any benefits out of the Letterplace structure.
However, there is another approach to this matter.

2.69 Definition. Define $\tilde{V} = \bigoplus\limits_{\nu \in \{0,1\}^n} \mathbb{K}[\mathbf{X}|\mathbf{P}]_{*,\nu}$.

By its definition $\tilde{V}$ is only a vector space, not an algebra. To see this consider again $x(0), y(0) \in \tilde{V}$. Then $x(0)y(0) \notin \tilde{V}$. But there is a very simple solution to this problem, which Roberto La Scala suggested in a private communication:

2.70 Lemma. Define $\mathfrak{LS} = \langle\{x_i(k)x_j(k) \mid i, j = 1, \ldots, n, k \in \mathbb{N}\}\rangle$. Then $\tilde{V} \cong \mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathfrak{LS}$ as $\mathbb{K}$-vector spaces.

Proof: We show that for each $[0] \neq [m] \in \mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathfrak{LS}$, where m is a monomial, there is one $\tilde{m} \in [m]$, such that $\tilde{m} \in \tilde{V} \setminus \{0\}$. Assume $[m]$ is a counterexample

to this statement. Then each $\tilde{m} \in [m]$ contains a subword of the form $x_i(k)x_j(k)$ (since $\mathbb{K}[\mathbf{X}|\mathbf{P}]$ is a commutative ring, we can order the variables contained in a monomial by their places). So each monomial is contained in $\mathfrak{LG}$, that is, $[m] = [0]$, a contradiction to the assumption.
Now we define $\tilde{\beta} : [\mathbf{X}|\mathbf{P}]/\mathfrak{LG} \to \tilde{V} : \ [m] \mapsto \tilde{m}$, where $\tilde{m} \in [m]$ is a monomial contained in $\tilde{V}$.
That this map is well-defined follows immediately, since there is only one monomial in each residue class $[m]$ for all $m \notin \mathfrak{LG}$. Clearly each $m \in \tilde{V}$ can be mapped to $[m]$ by the natural epimorphism and each two different monomials $m, m' \in \tilde{V}$ are mapped to two different residue classes, so $\tilde{\beta}$ is a bijection.
Now define β as the linear continuation of $\tilde{\beta}$ and the claim follows. q.e.d.

2.71 Remark. Note that $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathfrak{LG}$ is a commutative $\mathbb{K}$-algebra and we can identify it with the vector space $\tilde{V}$. Now we have $x(0)y(0) = 0 = y(0)x(0)$, if we consider the example in 2.68. However, $x(0)y(1) \in \tilde{V}$ and since $y(1) \in \tilde{V}$ we find $x(0) \cdot y(1) = x(0)y(1)$, so we have to consider multiplication up to shift-operation. This is a well-known phenomenon, because the reduction process in the Letterplace Gröbner algorithm works with the same idea (and reduction in a factor algebra needs the same process, since for example $y(0)x(1)x(2)$ should be reduced to zero, if the Letterplace Gröbner basis contains $x(0)x(1)$). So instead of working with $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\mathbf{J}$ for some ideal $\mathbf{J}$ we add the generators of $\mathfrak{LG}$ and consider the algebra $\mathbb{K}[\mathbf{X}|\mathbf{P}]/\langle \mathbf{J}, \mathfrak{LG} \rangle$, which is much smaller. In fact, we only have to remove the monomials, which contain "holes" in the places, which are the only elements in $\tilde{V} \setminus V$. So this is one way to use the Letterplace structure for non-commutative computations.

3 Implementation

In this chapter we will focus on the implementations of the algorithms and see some examples.
All the algorithms are contained in the SINGULAR library `sickle.lib`. As mentioned before, the implementation of the Letterplace structure is discussed in [LL09], so we will not discuss this any further. However, the `freegb.lib` is needed to be called (see [Lev08]).
For an introduction to SINGULAR we refer to the online-manual [GPS09].

3.1 The Data Structure

Our main task is the following: For a given factor algebra $\mathbb{K}\langle \mathbf{X}\rangle/\mathbf{I}$, find a $\mathbb{K}$-basis. The Diamond Lemma 2.2 states that there is a basis consisting only of monomials, that is, a basis for $\mathbb{K}\langle \mathbf{X}\rangle/\mathfrak{L}(I)$, so we may assume $\mathbf{G} = \mathfrak{L}(\mathbf{G})$. Therefore we have fixed the ordering, since different orderings will give us different leading monomials. But since we have no further need for the ordering we can change the appearance of the monomials.

- **Variables and Words:**
  The variables are stored as integers: $x_1 \mapsto 1,\ x_2 \mapsto 2, \ldots,\ x_n \mapsto n$. A word corresponds to a vector of integers. Multiplication corresponds to concatenation.

3.1 Example. The free algebra $\mathbb{K}\langle x, y, z\rangle$ has three variables, therefore $x \mapsto 1,\ y \mapsto 2,\ z \mapsto 3$. Here are some examples for monomials and their integer vector representation:

- $xyzxyz \quad \mapsto \quad (1, 2, 3, 1, 2, 3)$
- $xxyyzz \quad \mapsto \quad (1, 1, 2, 2, 3, 3)$
- $xxyzyyx \quad \mapsto \quad (1, 1, 2, 3, 2, 2, 1)$

It is obvious that there is a one-to-one correspondence between monomials of length d and the integer vectors of length d, if the entries are bounded by the number of variables.

The user can choose to use the Letterplace polynomials or the integer vector representation to enter his data. There are also procedures to switch between

those two representations.
As a convention we write *iv*, whenever we refer to the integer vector presentation, and *lp*, whenever we refer to the letterplace presentation.

3.2 Main Procedures

Throughout this section let L be a `list` of integer vectors, G an `ideal` of Letterplace polynomials and the `integer` n the number of variables in the free algebra (all according to the definitions in SINGULAR, in particular the `ideal` is a way to store a set of polynomials).

3.2.1 Determine Finiteness of $\mathbb{K}$-Dimension

One can check the finiteness of the $\mathbb{K}$-dimension of the factor algebra by calling `ivDimCheck`(L, n).
The procedure returns 1, if the dimension is infinite and 0 otherwise. Optionally one can call `lpDimCheck`(G), if the data is an `ideal` of Letterplace polynomials. Here the number of variables is not needed, since the procedure can check the data of the basering.
Note that if L or G respectively do not correspond to a Gröbner basis, the algorithm will not work properly. However, if L or G correspond to a truncated Gröbner basis and the algorithm returns 0, then the dimension for the ideal $\mathbf{I} = \langle G \rangle$, respectively $\mathbf{I} = \langle L \rangle$ will also have finite $\mathbb{K}$-dimension. This is due to 2.15.

3.2.2 Harvesting the Mistletoes

Instead of computing the whole basis, we are only interested in the mistletoes, since they contain all the data we need to know about the whole $\mathbb{K}$-basis.
To obtain the mistletoes one calls `ivSickle`(L, n) or `lpSickle`(G) respectively. The procedure returns the mistletoes as a `list` of integer vectors or an `ideal` of Letterplace polynomials, ordered lexicographically with respect to $1 > 2 > \ldots > n$, respectively $x_1 > x_2 > \ldots > x_n$, starting with the highest degree.
If the $\mathbb{K}$-dimension is not finite, one may add an optional parameter d to declare a degree bound. The mistletoes of higher degree will be projected to the left subword of degree d.
Internally the algorithm will stop at degree d and treat the normal words of degree d as mistletoes.

3.2.3 Determine $\mathbb{K}$-Dimension

To compute the $\mathbb{K}$-dimension, one calls `ivKDim`(L, n) or `lpKDim`(G) respectively. A natural number of type `int` corresponding to the $\mathbb{K}$-dimension is returned.
Again, one may add an optional parameter d to specify a degree bound. Then the integer indicates the $\mathbb{K}$-dimension of the factor algebra up to degree d, which is finite for any $d \in \mathbb{N}$.

3.2.4 Computing the Coefficients of the Hilbert series

The procedures `ivHilbert`(L, n) and `lpHilbert`(G) return the coefficients of the Hilbert series of a factor algebra as a vector of integers, starting with the 0^{th} coefficient.
To guarantee finiteness one may add an optional parameter d as a degree bound. The procedure will return the first $d+1$ coefficients. If the factor algebra is known to be of finite $\mathbb{K}$-dimension the degree bound is not needed and the procedure will compute all non-trivial coefficients of the Hilbert polynomial.

Note that we always have a degree bound for a Letterplace ring. If one uses the Letterplace structure, this degree bound is used by the procedures, unless one specifies a smaller one.

3.2.5 Combined Procedures

One may combine any of the latter procedures. The input is always as described above.

- `lp/ivDHilbert`:
  Returns a `list` with first entry the $\mathbb{K}$-dimension and second entry the integer vector containing the coefficients of the Hilbert series.

- `lp/ivDHilbertSickle`:
  Returns a `list` with first entry the `ideal/list` of mistletoes, second the $\mathbb{K}$-dimension and third the integer vector containing the coefficients of the Hilbert series.

- `lp/ivSickleDim`:
  Returns a `list` with first entry the `ideal/list` of mistletoes and second the $\mathbb{K}$-dimension.

- `lp/ivSickleHil`:
  Returns a `list` with first entry the `ideal/list` of mistletoes and second the integer vector containing the coefficients of the Hilbert series.

Moreover the procedure `Sickle`(G, m, d, h), where G is an `ideal` of lp-polynomials, allows to access all functions: by setting the optional integers m (for mistletoes), d (for dimension) or h (for Hilbert series) to 1. If one simply calls `Sickle`(G) only the mistletoes are returned. Again a degree bound may be added.

3.3 Procedures Dealing with Mistletoes

As stated before it is much easier to work with mistletoes instead of the whole basis. So given a set M of type `list` for iv-vectors and of type `ideal` for lp-monomials respectively of mistletoes for some factor algebra $\mathbf{A}$, again in n variables, we have the following procedures:

3.3.1 Determine $\mathbb{K}$-Dimension

Calling `ivMis2Dim`(M) or `lpMis2Dim`(M) respectively, depending on the format the mistletoes are in, returns the $\mathbb{K}$-dimension of the factor algebra as an `integer`. The mistletoes have to be sorted lexicographically to do so (cf. 2.51).

3.3.2 Computing the Coefficients of the Hilbert series

Again there are the procedures `ivMis2Hil`(M) and `lpMis2Hil`(M), which need the mistletoes to be ordered lexicographically. Both variants return the coefficients of the Hilbert series as an integer vector, starting in degree 0.

Again we can combine the two procedures using `lp/ivMis2DH`. Each of these procedures returns a `list` with first entry the $\mathbb{K}$-dimension of type `int` and second entry the coefficients of the Hilbert series as an integer vector.

Note, that given a set of mistletoes we always have finite $\mathbb{K}$-dimension, because if the factor algebra is of infinite $\mathbb{K}$-dimension, the mistletoes are bounded by a fixed degree. Therefore no degree bound for these procedures is needed. If one is interested in the question of finiteness, one needs the leading monomials of the Gröbner basis to build up the Ufnarovskij graph.
If the factor algebra is known to be of finite dimension, but it is unclear, whether one has already all the mistletoes, the procedure `ivCheckMis`(M, G) respectively `lpCheckMis`(M, G), can be used to determine if the set of mistletoes is already complete. The procedure returns 1, if there are no further extensions possible and 0 otherwise. However, these procedures need the set G of leading monomials of the Gröbner basis.

3.4 Other Procedures

There are more auxiliary procedures which can be called by the user to transform Letterplace polynomials into their integer vector correspondence and vice versa:

- `ivL2lpI`(L):
  Transforms a `list` of integer vectors L into an `ideal` of Letterplace monomials.

- `iv2lp`(I):
  Transforms an integer vector into the corresponding Letterplace monomial.

- `iv2lpList`(L):
  Transforms a `list` of integer matrices, each containing iv-monomials as rows, into an `ideal` of Letterplace monomials.

- `iv2lpMat`(M): Transforms an integer matrix, which corresponds to a set of integer vectors, into an `ideal` of Letterplace monomials. Note that these will all have the same total degree.

- `lp2iv`(p):
  Transforms the leading monomial of a Letterplace polynomial into the corresponding vector of integers.

- `lp2ivId`(G):
  Transforms an `ideal` G of Letterplace polynomials into the corresponding `list` of integer matrices. This is done by taking the leading monomials of G and storing all monomials of the same total degree in the one matrix.

Moreover, the procedure `ivSortMis` or `lpSortMis` respectively, can be used to sort the mistletoes lexicographically.

3.5 An Example in Singular

We like to give a quick example of the usage of Singular. Therefore we choose the example *braid*62 (see 3.6). The ideal is given by the generators $yxy-zyz, xyx-zxy, zxz-yzx, x^3-2y^3+3z^3-4xyz+5xz^2-6xy^2+7x^2z-8x^2y$.

```
LIB "sickle.lib"; // Loading the library
ring r = 0,(x,y,z),dp; // Define commutative ring
int d  = 6; // Degree bound
def R  = makeLetterplaceRing(d); // Define corresponding Lp ring
setring R; // Sets R as basering
// Defining the ideal by a set of generators:
```

```
ideal I = y(1)*x(2)*y(3) - z(1)*y(2)*z(3),
x(1)*y(2)*x(3) - z(1)*x(2)*y(3),
z(1)*x(2)*z(3) - y(1)*z(2)*x(3),
x(1)*x(2)*x(3) - 2*y(1)*y(2)*y(3) + 3*z(1)*z(2)*z(3)
- 4*x(1)*y(2)*z(3) + 5*x(1)*z(2)*z(3) - 6*x(1)*y(2)*y(3)
+ 7*x(1)*x(2)*z(3) - 8*x(1)*x(2)*y(3);
option(redSB);option(redTail); // To get a reduced Groebner basis
ideal J = system("freegb",I,d,3); // Computes a GB for I
ideal M = Sickle(J,1,0,0,d); // Compute mistletoes up to degree d
size(M); // This is the number of mistletoes,
         // which is too large to display here
==> 314
Sickle(J,0,1,0,d); // Compute the K-dimension up to degree 6
==> 541
Sickle(J,0,0,1,d); // Compute the Hilbert series up to degree 6
==> 1,3,9,23,57,135,313
```

3.6 Other Computer Algebra Systems

There are only a few computer algebra systems which provide a user with the possibility of performing computations in free associative algebras, and the functionality of modern computer algebra systems in such general structures is surprisingly limited. Namely, a typical system can compute only a Gröbner basis up to a given degree bound and solve the ideal membership problem via a normal form computation.
In the following we will enlist the most important computer algebra systems along with a short overview of their most important abilities:

- **MAGMA** [BCP97]
  With the system Magma it is possible to construct a free algebra and compute a Gröbner basis for a given two-sided ideal. There are two variants of the Gröbner basis algorithm, namely non-commutative Buchberger's algorithm and Alan Steel's generalization of Faugère's F4 algorithm to the case of free algebras. Moreover, a factor algebra can be constructed as the image of a homomorphism, that is, one can compute the image of an element under the natural epimorphism $\mathbb{K}\langle \mathbf{X}\rangle \to \mathbb{K}\langle \mathbf{X}\rangle/\mathbf{I}$. Furthermore it is possible to compute the dimension and a $\mathbb{K}$-basis of the factor algebra (in the case where the dimension is finite).
  One is restricted to the use of the graded lexicographical ordering, which, for example, does not allow to perform elimination procedures.

- **GAP** [Coh07, Kro03]
  The Gbnp package of Gap provides the user with the possibility to compute

Gröbner bases of non-commutative ideals and some variations of it, such as a weighted and truncated version. A tracing facility allows one to recover cofactors from a Gröbner presentation of a polynomial, belonging to an ideal (two-sided lift). In addition, there are algorithms for analyzing the quotient of a non-commutative polynomial algebra by a two-sided ideal, whose finite Gröbner basis has been determined. This includes an algorithm to check the finiteness of the $\mathbb{K}$-dimension. In the case of an affirmative result, one can compute a monomial $\mathbb{K}$-basis, the $\mathbb{K}$-dimension and the Hilbert series. For the latter computation, it is possible to specify a degree bound, so one can use it even in the infinite case via truncated computation.
Unfortunately, GBNP can only work with the `deglex` ordering, which, as in the case of MAGMA, cannot be used for elimination.

- **BERGMAN** [CU95]
  BERGMAN is a flexible tool to calculate Gröbner bases, Hilbert and Poincaré-Betti series, Anick resolutions and Betti numbers in non-commutative algebras and modules over them. By default, BERGMAN takes homogeneous polynomials as input only. However, recently it became possible to compute Gröbner bases of non-homogeneous ideals using homogenization and the so called "rabbit strategy", see [Ufn08] and [Nor98]. There are three orderings available: the `deglex` ordering and two orderings for elimination (cf. [BCU05]).

- **OPAL** [GHK97]
  OPAL is a stand-alone system for Gröbner bases in free and path algebras and is able to compute degree-bounded Gröbner bases, normal forms and a (bounded) $\mathbb{K}$-basis of a factor algebra. OPAL is not developed anymore.

- **FELIX** [AK91]
  FELIX provides generalizations of Buchberger's algorithm to free $\mathbb{K}$-algebras, polynomial rings and non-commutative G-algebras. Also, syzygy computations and basic ideal arithmetics are implemented. Also it provides the user with the possibility to compute products and quotients of ideals, sums and intersection of modules. FELIX is able to do elimination, compute syzygies and transformation matrices. FELIX is the only system which can compute over the (non-commutative) integer ring $\mathbb{Z}\langle\mathbf{X}\rangle$.
  Unfortunately, FELIX is not under development any longer.

For a comparison of our implementation MAGMA and GAP were available to us. However, there are lots of drawbacks to those programs, as will be explained in the next section.

3.7 Examples

Up to now, there is still no publicly available collection of standard benchmarks for non-commutative Gröbner bases in free and path algebras. In [LL09] Viktor Levandovskyy and Roberto La Scala stressed the importance of creating a unified set of examples, which will serve as benchmarks for systems, computing non-commutative Gröbner bases in free and path algebras. They created a large set of examples for computing Gröbner bases and used it to test their implementation of the Letterplace Gröbner basis algorithm. We intend to use these examples to test our implementation as well and to compare the timings of the computations with that of Magma and Gap.
However, there is a big drawback to this set of examples: While there always exists at least a truncated Gröbner basis $\mathbf{G}$ of each example, the factor algebra $\mathbb{K}\langle \mathbf{X}\rangle/\langle \mathbf{G}\rangle$ is not guaranteed to be of finite $\mathbb{K}$-dimension and in fact it turns out that for these examples it is not. While our implementation in Singular can handle infinite $\mathbb{K}$-dimension by adding a degree-bound (so we compute only part of the $\mathbb{K}$-basis), Magma is not able to do so, while Gap can compute a part of the Hilbert series (up to a given degree) and the function `BaseQA` can be used to compute a finite number of elements. But since it is not clear which part of the $\mathbb{K}$-basis is returned, because there is no explanation for this behavior in the online guide (cf. [CK09]), it is not meaningful to compare the two procedures. Note that this “bad” behavior of Gap makes its use complicated.
On the other hand, it is not reasonable to compare those programs in the finite case, because most of those cases are too small, meaning that the computation time is below one second (for all three systems) and therefore they are equally fast.

3.7.1 Explanation of the Examples

The following examples are all taken from [LL09].

3.2 Example. Consider the two-sided ideal $\mathbf{I}$, such that $\mathbb{K}\langle \mathbf{X}\rangle/\mathbf{I}$ is the universal enveloping algebra of the (relatively) free nilpotent Lie algebra L of class c. In other words, the ideal $\mathbf{I}$ is generated by all (left-normed) commutators $[x_{i_1}, \ldots, x_{i_c}]$ of length $c+1$, where the number of variables $x_i \in \mathbf{X}$ is the dimension n of the algebra L.
In particular, we study the case when $n = 5$ and $c = 3, 4$, as did Levandovskyy and La Scala (cf. [LL09] Example 5.1). We called these examples $3nil\_5dim$ and $4nil\_5dim$. We compute up to degree 6 and 7 for both these cases.

3.3 Example. In the theory of associative algebras, a fundamental role is played by the so-called T-ideals which are (multi)graded two-sided ideals $\mathbf{I}$ of the free associative algebra $\mathbb{K}\langle \mathbf{X}\rangle$ given by all polynomials which are zero when evaluated on elements of an algebra A. Then, A is said to be a polynomial identity algebra,

written PI-algebra, that is, $\mathbf{I}$ is different from zero. Usually the T-ideals are not finitely generated as ideals of $\mathbb{K}\langle\mathbf{X}\rangle$, and so one can give a finite set of generators just up to some degree d.
As an example for testing their implementation, Levandovskyy and La Scala considered the T-ideal $\mathbf{I}$ of the algebra of 2-by-2 upper triangular matrices. Then the ideal $\mathbf{I}$ is generated by polynomials $[x_i, x_j]w[x_k, x_l]$ where w is an arbitrary word (including 1) of $\mathbb{K}\langle\mathbf{X}\rangle$. For the test, they fixed the number of variables equal to 4 and degree bound to 7 and denoted this example as *2tri_4var* (cf. [LL09] Example 5.3) and so do we.

3.4 Example. The Cartan matrices for the algebras F_4 and E_6 are well-known and can be obtained explicitly with e.g. Gap. The generalized Cartan matrices for HA_1^1 and for $EHA_1^{1,2}$ (which is an instance of parametric extended HA_1^1 matrix) are the following:

$$HA_1^1 := \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -2 \\ 0 & -2 & 2 \end{pmatrix}; \qquad EHA_1^{1,2} := \begin{pmatrix} 2 & -2 & -3 \\ -2 & 2 & -1 \\ -2 & -5 & 2 \end{pmatrix}.$$

These examples have been called *ser_f4*, *ser_e6*, *ser_ha* and *ser_eha* respectively (cf. [LL09] Example 5.4).

3.5 Example. We consider also an example, communicated to Viktor Levandovskyy and Roberto La Scala by Victor Ufnarovskij and denoted as *ufn3*. This is a list of 125 binomials of degree 2 in 15 variables. Some of them represent anti-commutativity, $ab + ba$; the rest are of the form $ab + cd$, $ca + ab$, $de + fd$ and so on.

3.6 Example. Some examples were invented by Viktor Levandovskyy and Roberto La Scala for the purpose of a fast comparison with other systems. The generators can be found in Table 3.1.

Table 3.1:

Example	Generators of ideal
braid3_11	$yxy - zyz, xyx - zxy, zxz - yzx, x^4 + y^3 + z^3 + xyz$
braid4_11	$yxy - zyz, xyz - zxy, zxz - yzx, x^4 + y^3 + z^3 + xyz$
braid62	$yxy - zyz, xyz - zxy, zxz - yzx,$ $x^3 - 2y^3 + 3z^3 - 4xyz + 5xz^2 - 6xy^2 + 7x^2z - 8x^2y$
lp1_10	$z^4 + yxyx - xy^2x - 3zyxz, x^3 + yxy - xyx, zyx - xyz + zxz$
lv2_15	$xy + yz, x^2 + xxy - yx - y^2$

All tests were performed on a PC equipped with an Intel Core i7 Quadcore Processor (4 × 2933 MHz) with 12GB RAM running Linux. However, during the computation it was only possible to use 4GB RAM at most and only part of the capacity of the processor.

3.7.2 Timings

The running times in the tables below are given in the format

"hours:minutes:seconds:hundredth seconds".

We drop the hours, whenever they are not required.

As one can see in Table 3.2, the dimensions of each factor algebra are quite high, so we expect long computational time.
However, as one can see in Table 3.3, each computation with Singular is pretty fast, so we have mostly timings below one minute.

Example	Dimension	Time GB-Computation
2tri_4var7deg	6237	00:04.00
3nil_5dim_d6	8557	00:01.01
3nil_5dim_d7	28272	00:03.65
4nil_5dim_d6	13207	00:14.46
4nil_5dim_d7	51672	00:55.39
Braid3_11	31214	00:14.73
Braid4_11	32123	00:03.65
Braid62_6	541	00:00.02
Braid62_10	14149	01:36.04
lp1_10	39737	00:00.44
lv2d10	4083	00:00.07
serre_e6_d10	101803	00:00.32
serre_e6_d13	919083	00:08.65
serre_eha112_d10	44811	00:00.22
serre_eha112_d12	323704	00:07.70
serre_f4_d10	11912	00:00.10
serre_f4_d15	198930	00:04.76
serre_ha11_d10	4944	00:00.09
serre_ha11_d15	98412	00:27.28
ufn3_d6	5863	00:21.51
ufn3_d8	12882	01:05.19

Table 3.2: List of examples, their dimension and timings for Gröbner basis computation

Example	Time Hilb	Time Dimen	Time Sickle	Time DCheck
$2tri\_4var7deg$	00:39.08	00:39.28	00:45.02	00:00.33
$3nil\_5dim - d6$	00:28.47	00:28.89	00:37.02	00:00.04
$3nil\_5dim - d7$	01:45.44	01:44.16	02:12.38	00:00.26
$4nil\_5dim - d6$	01:55.28	01:55.76	02:12.18	00:00.42
$4nil\_5dim - d7$	11:05.87	11:10.12	12:04.26	00:00.39
$Braid3\_11$	03:08.62	03:08.32	03:41.83	00:00.87
$Braid4\_11$	02:08.74	02:08.29	02:45.12	00:00.32
$Braid62\_6$	00:00.33	00:00.34	00:00.69	00:00.02
$Braid62\_10$	00:00.72	00:00.68	00:11.36	00:00.03
$lp1\_10$	00:44.29	00:44.84	01:31.69	00:00.03
$lv2d10$	00:05.67	00:05.78	00:09.46	00:00.05
$serre\_e6\_d10$	02:51.63	02:53.38	04:34.33	00:00.02
$serre\_e6\_d13$	31:49.28	31:27.90	45:12.87	00:00.99
$serre\_eha112\_d10$	00:50.15	00:51.30	01:41.58	00:00.02
$serre\_eha112\_d12$	10:03.88	10:20.23	17:47.82	00:00.14
$serre\_f4\_d10$	00:13.54	00:13.90	00:23.69	00:00.07
$serre\_f4\_d15$	05:26.05	05:35.93	09:11.80	00:00.07
$serre\_ha11\_d10$	00:04.97	00:05.16	00:09.21	00:00.02
$serre\_ha11\_d15$	03:19.33	03:21.02	05:15.57	00:00.95
$ufn3\_d6$	01:28.56	01:27.57	01:31.27	00:00.98
$ufn3\_d8$	04:52.44	04:49.52	05:02.41	00:01.03

Table 3.3: Timings for all `sickle.lib` procedures

3.7.3 A Comparison to GAP

We now state the timings for the analogous procedures in Gap. The notation and the treatment is as before.

Example	Time Hilbert	Time FinCheck	Time GB-Computation
2tri_4var7deg	00:44.90	00:01.38	00:34.64
3nil_5dim_d6	0:04.97	0:00.86	00:04.08
3nil_5dim_d7	00:06.94	00:01.73	00:33.96
4nil_5dim_d6	00:04.07	00:01.92	00:27.56
4nil_5dim_d7	00:12.98	00:57.18	02:34.17
Braid3_11	00:06.70	00:05.19	03:34.19
Braid4_11	00:02.02	00:00.76	00:31.31
Braid62_6	00:01.12	00:00.66	00:01.10
Braid62_10	17:52.00	22:01.00	13:46:20.00
lp1_10	00:01.97	00:00.98	00:08.88
lv2d10	00:01.51	00:00.49	00:01.48
serre_e6_d10	00:01.07	00:00.21	00:12.11
serre_e6_d13	00:06.91	00:13.12	05:36.71
serre_eha112_d10	00:03.04	00:00.10	00:03.05
serre_eha112_d12	02:01.35	00:00.92	01:12.87
serre_f4_d10	00:02.43	00:01.63	00:02.44
serre_f4_d15	31:16.00	01:08.53	45:08.30
serre_ha11_d10	00:01.82	00:01.12	00:01.73
serre_ha11_d15	00:57.00	01:18.00	01:20:45.00
ufn3_d6			00:01.08 [1]
ufn3_d8			00:01.06 [1]

Table 3.4: Timings for corresponding Gap procedures

For a quick comparison between the systems, we have prepared Table 3.5.
Let us first consider the timings for the check of finiteness of the $\mathbb{K}$-dimension: As one can see, Singular is the faster system in all examples. This is due to the fact that the fincheck-procedure of Gap constructs a so-called search-tree (cf. [Kro03]) for all the monomials in the Gröbner basis. This seems to be very time-consuming for these large examples.
On the other hand, the timings for the (partial) Hilbert series seem to indicate that Gap is the faster system, even if we consider the total time, meaning the sum of the time for the Gröbner basis computation and the time for the computation

[1] The computation was terminated after the stated amount of time, because it reached the memory limit.

Example	**Hilbert**	**Time dimension check**
2tri_4var7deg	Singular	Singular
3nil_5dim_d6	Gap	Singular
3nil_5dim_d7	Gap	Singular
4nil_5dim_d6	Gap	Singular
4nil_5dim_d7	Gap	Singular
Braid3_11	Gap	Singular
Braid4_11	Gap	Singular
Braid62_6	Singular	Singular
Braid62_10	Singular	Singular
lp1_10	Gap	Singular
lv2d10	Gap	Singular
serre_e6_d10	Gap	Singular
serre_e6_d13	Gap	Singular
serre_eha112_d10	Gap	Singular
serre_eha112_d12	Gap	Singular
serre_f4_d10	Gap	Singular
serre_f4_d15	Singular	Singular
serre_ha11_d10	Gap	Singular
serre_ha11_d15	Gap	Singular
ufn3_d6	Singular	Singular
ufn3_d8	Singular	Singular

Table 3.5: Evaluation of the Tables

of the Hilbert series. However, if one considers the outcome of the computation the results of Gap are somehow suspicious, take for example *serre_e6_d13*, then Gap returns:

$$[1, 6, 26, 91, 281, 782, 2003, 4741, 10358, 20571, 35693, 47705, 19076, -174732]$$

as coefficients for the Hilbert series (starting with the coefficient of the smallest term). By definition of the Hilbert series, there should be only natural numbers, so $-174732 \notin \mathbb{N}$ should not be a coefficient. The algorithm implemented in Gap is using the so-called *graph of chains* and another series, which can be considered as the inverse of the Hilbert series (for more information on this procedure see [Kro03]). Since we have a truncated Gröbner basis as input, it is not clear if the procedure returns a meaningful result and in fact the examples *serre_e6_d13* shows that it does not work properly in this case, while our procedure returns the fake dimension for each graded component, as one would wish for.

In conclusion, our procedures implemented in Singular can cope in direct comparison to Gap and therefore with other computer algebra systems, and moreover, the procedures return meaningful results, even in the cases, in which the corresponding functions in Gap fail to do so.

Erklärung

Hiermit versichere ich, dass ich die Aufgabenstellung selbständig bearbeitet und keine außer den angegebenen Hilfsmitteln verwendet habe.

Aachen, May 9, 2010

Grischa Studzinski

Index

Bibliography

[AK91] J. Apel and U. Klaus. FELIX - ein Computeralgebrasystem für konstruktive Algebra, 1991.

[AK05] P. Ackermann and M. Kreuzer. Gröbner basis cryptosystems. *Journal of AAECC (Appl. Alg. in Eng. Comm. and Comp.)*, 2005.

[AL88] J. Apel and W. Lassner. An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *J. Symbolic Comput.*, 6(2-3):361–370, 1988. Computational aspects of commutative algebra.

[Ape00] Joachim Apel. Computational ideal theory in finitely generated extension rings. *Theoret. Comput. Sci.*, 244(1-2):1–33, 2000.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235 – 265, 1997.

[BCU05] J. Backelin, S. Cojocaru, and V. Ufnarosvkij. Mathematical computations using Bergman. Technical report, Lund University, 2005. `http://servus.math.su.se/bergman/`.

[Ber78] G. Bergman. The Diamond Lemma for ring theory. *Adv. Math.*, 29:178–218, 1978.

[BK07] H. Bluhm and M. Kreuzer. Computation of two-sided syzygies over non-commutative rings. *Contemp. Math. 421*, pages 45 – 64, 2007.

[CK09] A. M. Cohen and J. W. Knopper. GBNP Homepage, 2009. `http://dam02.win.tue.nl/products/gbnp/`.

[Coh07] A. M. Cohen. Non-commutative polynomial computations. `http://www.win.tue.nl/~amc/pub/grobner/gbnp.pdf`, 2007. TU Eindhoven. Technical Report.

[CPU99] S. Cojocaru, A. Podoplelov, and V. Ufnarovskij. Non-commutative Gröbner bases and Anick's resolution. In P. Dräxler, editor, *Computational methods for representations of groups and algebras. Proc. of the Euroconference in Essen, Germany, April 1997*, pages 29–60. Birkhäuser, 1999.

[CR94] Maxime Crochemore and Wojciech Rytter. *Text algorithms*. Oxford University Press, Inc., New York, NY, USA, 1994.

[CU95] S. Cojocaru and V. Ufnarovskij. Noncommutative Gröbner basis, Hilbert series, Anick's resolution and BERGMAN under MS-DOS. *Computer Science Journal of Moldova*, 3(1):24 – 39, 1995.

[Die05] R. Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 2005.

[EW07] G.A. Evans and C.D. Wensley. Complete involutive rewriting systems. *J. Symbolic Computation*, 42(11-12):1034–1051, 2007.

[Gar07] D. Garber. Braid group cryptography. *CoRR*, abs/0711.3941, 2007.

[GHK97] E. Green, L. Heath, and B. Keller. Opal: A system for computing noncommutative Gröbner bases. In *RTA '97: Proceedings of the 8th International Conference on Rewriting Techniques and Applications*, pages 331–334. Springer, 1997.

[GLS06] G.-M. Greuel, V. Levandovskyy, and H. Schönemann. PLURAL. A SINGULAR 3.0 subsystem for computations with non–commutative polynomial algebras. Centre for Computer Algebra, University of Kaiserslautern, 2006. `http://www.singular.uni-kl.de`.

[GP02] G.-M. Greuel and G. Pfister. *A* SINGULAR *introduction to commutative algebra*. Springer-Verlag, Berlin, 2002. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[GPS09] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3-1-0 — A computer algebra system for polynomial computations. 2009. `http://www.singular.uni-kl.de`.

[Gre93] E. Green. An introduction to noncommutative Gröbner bases. In K. Fischer, editor, *Computational algebra. Papers from the Mid-Atlantic Algebra Conference, May 1993*, pages 167–190. Dekker. Lect. Notes Pure Appl. Math. 151, 1993.

[Gre00] E. Green. Multiplicative Bases, Gröbner Bases, and Right Gröbner Bases. *J. Symbolic Computation*, 29(4/5), 2000.

[Gre03] D. J. Green. *Gröbner bases and the computation of group cohomology*. Lecture Notes in Mathematics 1828. Springer, 2003.

[KK06] A. Kehrein and M. Kreuzer. Computing border bases. *Journal of Pure and Applied Algebra*, 205(2):279–295, 5 2006.

[KMRU05] M. Kreuzer, A. Myasnikov, G. Rosenberger, and A. Ushakov. *Quotient tests and Gröbner bases*, 2005.

[Kro03] C. Krook. Dimensionality of quotient algebras. http://www.win.tue.nl/~amc/pub/grobner/dqa.ps, 2003. Technical Report.

[Lev05] V. Levandovskyy. *Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation*. PhD thesis, Universität Kaiserslautern, 2005. http://kluedo.ub.uni-kl.de/volltexte/2005/1883/.

[Lev08] V. Levandovskyy. A SINGULAR 3.1 library for computing two-sided Gröbner bases in free algebras via letterplace methods freegb.lib, 2008. http://www.singular.uni-kl.de.

[LL09] R. La Scala and V. Levandovskyy. Letterplace ideals and non-commutative Gröbner bases. *J. Symbolic Computation*, 44(10):1374–1393, 2009.

[Mor86] T. Mora. Gröbner bases for non-commutative polynomial rings. *Proc. AAECC 3 Lect. N. Comp. Sci*, 229:353–362, 1986.

[Mor89] T. Mora. Gröbner bases in non-commutative algebras. In *Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'88)*, pages 150–161. LNCS 358, 1989.

[Mor94] T. Mora. An introduction to commutative and non-commutative Gröbner bases. *Theor. Comp. Sci.*, 134:131–173, 1994.

[Nor98] P. Nordbeck. On some basic applications of Gröbner bases in non-commutative polynomial rings. In B. Buchberger and F. Winkler, editors, *Gröbner bases and applications*, pages 463–472. Cambridge University Press, 1998.

[Ufn89] V. Ufnarovskij. On the use of graphs for calculating the basis, growth and Hilbert series of associative algebras. (Russian). *Mat. Sb.*, 180:1548–1560, 1989. translation in Math. USSR-Sb., 68:417–428, 1991.

[Ufn90] V. Ufnarovskij. *Combinatorial and asymptotic methods in algebra.* Itogi Nauki i Tekhniki. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1990.

[Ufn98] V. Ufnarovskij. Introduction to noncommutative Gröbner bases theory. In B. Buchberger and F. Winkler, editors, *Gröbner bases and applications*, pages 259–280. Cambridge University Press, 1998.

[Ufn08] V. Ufnarovskij. On the cancellation rule in the homogenization. *Computer Science Journal of Moldova*, 16(1), 2008.