Computing Free Non-commutative Groebner Bases over Z with Singular:Letterplace

Viktor Levandovskyy, Tobias Metzlaff, Karim Abou Zeid

Computing Free Non-commutative Gröbner Bases over $\mathbb{Z}$ with SINGULAR:LETTERPLACE

Viktor Levandovskyy

Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen University, Aachen, Germany

Tobias Metzlaff

AROMATH, INRIA Méditerranée, Université Côte d'Azur, Sophia Antipolis, France

Karim Abou Zeid

Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen University, Aachen, Germany

Abstract

With this paper we present an extension of our recent ISSAC paper about computations of Gröbner(-Shirshov) bases over free associative algebras $\mathbb{Z}\langle X\rangle$. We present all the needed proofs in details, add a part on the direct treatment of the ring $\mathbb{Z}/m\mathbb{Z}$ as well as new examples and applications to e.g. Iwahori-Hecke algebras. The extension of Gröbner bases concept from polynomial algebras over fields to polynomial rings over rings allows to tackle numerous applications, both of theoretical and of practical importance. Gröbner and Gröbner-Shirshov bases can be defined for various non-commutative and even non-associative algebraic structures. We study the case of associative rings and aim at free algebras over principal ideal rings. We concentrate ourselves on the case of commutative coefficient rings without zero divisors (i.e. a domain). Even working over $\mathbb{Z}$ allows one to do computations, which can be treated as universal for fields of arbitrary characteristic. By using the systematic approach, we revisit the theory and present the algorithms in the implementable form. We show drastic differences in the behavior of Gröbner bases between free algebras and algebras, close to commutative. Even the process of the formation of critical pairs has to be reengineered, together with the implementing the criteria for their quick discarding. We present an implementation of algorithms in the SINGULAR subsystem called LETTERPLACE, which internally uses Letterplace techniques (and Letterplace Gröbner bases), due to La Scala and Levandovskyy. Interesting examples and applications accompany our presentation.

Keywords: Non-commutative algebra; Coefficients in rings; Gröbner bases; Algorithms

Email addresses: Viktor.Levandovskyy@math.rwth-aachen.de (Viktor Levandovskyy), tobias.metzlaff@inria.fr (Tobias Metzlaff), karim.abou.zeid@rwth-aachen.de (Karim Abou Zeid)

URL: http://www.math.rwth-aachen.de/~Viktor.Levandovskyy/ (Viktor Levandovskyy)

Introduction

We present an extension of our recent ISSAC paper (Levandovskyy et al., 2020b) on the computations of Gröbner(-Shirshov) bases over free associative algebras like $\mathbb{Z}\langle X\rangle$. In the extended version we have added and proved new results for non-commutative Gröbner bases over rings with zero-divisors using factorization and lifting techniques. The proof of Lemma 10 received substantial enhancements, since it is essential for the correctness of our algorithm. We added details to the proof of Lemma 20 and showed the corresponding Lemma 21. New examples and applications are introduced in Example 25 and Example 26. Older examples are revisited and enhanced.

By 2010's the techniques, based on Gröbner bases were well-established in the sciences and applications and widely known. A number of generalizations of them to various settings have been proposed and discussed. However, especially when it came to non-commutative and non-associative cases, generalizations of, in particular, Gröbner bases, were often met with sceptical expressions like "as expected", "straightforward", "more or less clear" and so on. This is not true in general since generalizations to various flavours of non-commutativity require deep analysis of procedures (and in case of provided termination, algorithms) based on intricate knowledge of properties of rings and modules over them. Characteristically, in this paper we demonstrate in e.g. Example 6 and 7 how *intrinsically different* Gröbner bases over $\mathbb{Z}\langle X\rangle$ are even when compared with Gröbner bases over $\mathbb{Q}\langle X\rangle$, not taking the commutative case into account. An example can illustrate this better than a thousand words:

Example 1. *Consider the set $F = \{2x, 3y\}$. While taken over $\mathbb{Z}\langle x, y\rangle$, it has a finite strong Gröbner basis $\{2x, 3y, yx, xy\}$. On the other hand, considered over $\mathbb{Z}\langle x, y, z_1, \ldots, z_m\rangle$ for any $m \geq 1$, F has an infinite Gröbner basis, which contains e.g. $xz_i^k y$ and $yz_i^k x$ for any natural k.*

In his recent articles and in the book (Mora, 2016) Teo Mora has presented "a manual for creating your own Gröbner bases theory" over *effective* associative rings. This development is hard to underestimate, for it presents a unifying theoretical framework for handling very general rings. In particular, we can address the Holy Grail of computational algebra, that is the unified algorithmic treatment of finitely presented modules over the rings like

$$R = (\mathbb{Z}\langle Y\rangle/J)\langle X\rangle/I$$

where Y and X are finite sets of variables, J is a two-sided ideal from the free ring $\mathbb{Z}\langle Y\rangle$ and I is a two-sided ideal from the associative ring $(\mathbb{Z}\langle Y\rangle/J)\langle X\rangle$. The extension of $(\mathbb{Z}\langle Y\rangle/J)$ with X and I can be iterated. In order to compute within such a ring, it turns out to be enough to have two-sided Gröbner bases over $\mathbb{Z}\langle Z\rangle$ for a finite set of variables Z, with respect to – among other – block elimination orderings. Then, indeed, the concrete computation, still valid over R will take place in $\mathbb{Z}\langle Y \cup X\rangle/(I + J)$. Further on, over the factor-algebra R one needs left and right Gröbner bases for ideals and submodules of free bimodules. We provide these components over fields and over rings $\mathbb{Z}$.

The theory of non-commutative Gröbner bases was developed by many prominent scientists since the Diamond Lemma of G. Bergman (Bergman, 1977). Especially L. Pritchard (Pritchard, 1996) proved versions of the PBW Theorem and advanced the theory of bimodules, also over rings. On the other hand, procedures and even algorithms related to Gröbner bases in such frameworks are still very complicated. Therefore, when aiming at implementation, one faces the classical dilemma: generality versus performance. Perhaps the most general implementation

which exists is the JAS system by H. Kredel (Kredel, 2020, 2015). In our designs we balance the generality with the performance; based on SINGULAR, we utilize its' long, successful and widely recognized experience with data structures and algorithms in commutative algebra. Notably, the recent years have seen the in-depth development of Gröbner bases in commutative algebras with coefficients in principal ideal rings (O. Wienand, G. Pfister, A. Frühbis-Krüger, A. Popescu, C. Eder, T. Hofmann and others), see e.g. (Eder and Hofmann, 2019; Eder et al., 2016, 2021; Lichtblau, 2012). This required massive changes in the structure of algorithms; ideally, one has one code for several instances of Gröbner bases with specialization to individual cases. In particular, the very generation of critical pairs and the criteria for discarding them without much effort were intensively studied. These developments were additional motivation for us in the task of attacking Gröbner bases in free algebras over commutative principal ideal rings, with $\mathbb{Z}$ at the first place. Currently, to the best of our knowledge, no computer algebra system is able to do such computations. Also, a number of highly interesting applications wait to be solved: in studying representation theory of a finitely presented algebra (i.e. the one, given by generators and relations), computations over $\mathbb{Z}$ remain valid after specification to *any* characteristic and thus encode a universal information, see for example Example 25. In the system FELIX by Apel et al. (Apel and Klaus, 1991), such computations were experimentally available, though not documented. In his paper (Apel, 2000), Apel demonstrates Gröbner bases of several nontrivial examples over $\mathbb{Z}\langle X\rangle$, the correctness of which we can easily confirm now.

Our secret weapon is the *Letterplace technology* (La Scala and Levandovskyy, 2009, 2013; Levandovskyy et al., 2013; La Scala, 2014), which allows the usage of commutative data structures at the lowest level of algorithms. We speak, however, in theory, the language of free algebras over rings, since this is mutually bijective with the language of Letterplace.

This paper is organized as follows: In the first chapter we establish the notations which are necessary when dealing with polynomial rings. Subsequently, in the second chapter we generalize the notion of Gröbner bases for our setup, present a theoretical version of Buchberger's algorithm and give examples to visualize significant differences compared to the field case or the commutative case. Implementation of Buchberger's algorithm depends on and benefits from the gentle handling of critical pairs, which we will discuss in the third chapter. This is followed up by computational examples, applications and discussion on the implementational aspects.

1. Preliminaries

All rings are assumed to be associative and unital, but not necessarily commutative. We want to discuss non-commutative Gröbner bases over the integers $\mathbb{Z}$. Equivalently one can take any commutative Euclidean domain or principal ideal domain[1] $\mathcal{R}$.

We work towards an implementation and therefore we are interested in *algorithms*, which *terminate* after a finite number of steps. Since $\mathbb{Z}\langle X\rangle$ is not Noetherian, there exist finite generating sets whose Gröbner bases are infinite with respect to any monomial well-ordering. Therefore, our typical computation is executed subject to the *length bound* (where length is meant literally, applied to *words* from the free monoid $\langle X\rangle$), specified in the input, and therefore terminates per assumption. Thus, we talk about *algorithms* in this sense.

[1] This concept can be extended to principal ideal rings. It was done in (Eder and Hofmann, 2019) for the commutative case with so-called annihilator polynomials.

Our main goal is to obtain an algorithm to construct a Gröbner basis over such a ring, finding or adjusting criteria for critical pairs and setting up an effective method to implement Buchberger's algorithm in the computer algebra system Singular. The problem of applying the statements of commutative Gröbner basis over Euclidean domains and principal ideal rings, such as in (Eder et al., 2021, 2016; Lichtblau, 2012; Markwig et al., 2015), are divisibility conditions of leading monomials.

Let $X = \{x_1, \ldots, x_n\}$ denote the finite alphabet with n letters. We set $\mathcal{P} = \mathcal{R}\langle X\rangle$, the free $\mathcal{R}$-algebra of X, where all words on X form a basis $\mathcal{B} = \langle X\rangle$ of $\mathcal{P}$ as a free $\mathcal{R}$-module. From now on we say "$\mathcal{B}$ is an $\mathcal{R}$-basis". Moreover, let $\mathcal{P}^e = \mathcal{P} \otimes_{\mathcal{R}} \mathcal{P}^{\mathrm{opp}}$ be the free enveloping $\mathcal{R}$-algebra with basis $\mathcal{B}^e = \{u \otimes v \,|\, u, v \in \mathcal{B}\}$. The natural action $\mathcal{P}^e \times \mathcal{P} \to \mathcal{P}$, $(u \otimes v, t) \mapsto (u \otimes v)t := utv$ makes a bimodule $\mathcal{P}$ into a left $\mathcal{P}^e$-module. We call the elements of $\mathcal{B}$ **monomials**.

Let $\preceq$ be a monomial well-ordering on $\mathcal{B}$. With respect to $\preceq$, a polynomial $f \in \mathcal{P} \setminus \{0\}$ has a **leading coefficient** $\mathrm{lc}(f) \in \mathcal{R}$, a **leading monomial** $\mathrm{lm}(f) \in \mathcal{B}$ and a **leading term** $\mathrm{lt}(f) = \mathrm{lc}(f)\,\mathrm{lm}(f) \neq 0$. We denote by $|w|$ the length of the word $w \in \mathcal{B}$. An ordering $\preceq$ is called **length-compatible**, if $u \preceq v$ implies $|u| \leq |v|$. Every subset $\mathcal{G} \subseteq \mathcal{P}$ yields a two-sided ideal, the **ideal of leading terms** $\mathrm{L}(\mathcal{G}) = \langle \mathrm{lt}(f) \,|\, f \in \mathcal{G} \setminus \{0\}\rangle$.

Naturally, the notions of coefficient, monomial and term carry over to an element $h \in \mathcal{P}^e$ by considering $h \cdot 1 \in \mathcal{P}$.

Definition 2.
*Let $u, v \in \mathcal{B}$. We say, that u and v have an **overlap**, if there exist monomials $t_1, t_2 \in \mathcal{B}$, such that at least one of the four cases*

$$(1)\ ut_1 = t_2v \qquad (2)\ t_1u = vt_2 \qquad (3)\ t_1ut_2 = v \qquad (4)\ u = t_1vt_2$$

*holds. Additionally, we say, that u and v have a **non-trivial overlap**, if* (3) *or* (4) *holds, or if in* (1) *or* (2) *we have $|t_1| < |v|$ and $|t_2| < |u|$. In* (3)*, respectively* (4)*, we say, that u **divides** v, respectively v **divides** u. The set of all elements, which are divisible by both u and v, is denoted by $\mathrm{cm}(u, v)$ (*cm:* common multiple). The set of all minimal, non-trivial elements, which are divisible by both u and v, is denoted by $\mathrm{lcm}(u, v)$ (*lcm:* least ...), i.e. $t \in \mathrm{lcm}(u, v)$, if and only if there exist $\tau_u, \tau_v \in \mathcal{B}^e$, such that $t = \tau_u u = \tau_v v$, representing non-trivial overlaps of u and v, and if $t, \tilde{t} \in \mathrm{lcm}(u, v)$ with $\tilde{t} = \tau t$ for some $\tau \in \mathcal{B}^e$, then $t = \tilde{t}$ and $\tau = 1 \otimes 1$. If there are only trivial overlaps, then $\mathrm{lcm}(u, v) = \emptyset$. Moreover, if $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$ for $f, g \in \mathcal{P}$, then $\mathrm{lm}(g) \preceq \mathrm{lm}(f)$.*

2. Non-commutative Gröbner Bases

A **Gröbner basis** $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ is a generating set for a two-sided ideal $\mathcal{I} \subseteq \mathcal{P}$ with the property $\mathrm{L}(\mathcal{I}) \subseteq \mathrm{L}(\mathcal{G})$. In the field case, this guarantees the existence of a so-called Gröbner representation, which will be recalled subsequently, and for any $f \in \mathcal{I} \setminus \{0\}$ it also guarantees the existence of an element $g \in \mathcal{G}$, such that $\mathrm{lt}(g)$ divides $\mathrm{lt}(f)$.

Definition 3.
Let $f, g \in \mathcal{P} \setminus \{0\}$, $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ a countable set and $\mathcal{I} \subseteq \mathcal{P}$ an ideal. Fix a monomial well-ordering $\preceq$ on $\mathcal{B}$.

*We say, that g **lm-reduces** f, if $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$ with $\mathrm{lm}(f) = \tau\,\mathrm{lm}(g)$ for some $\tau \in \mathcal{B}^e$ and there are $a, b \in \mathcal{R}$, $a \neq 0$ and $|b| < |\mathrm{lc}(f)|$ (in the Euclidean norm), such that $\mathrm{lc}(f) = a\ \mathrm{lc}(g) + b$. Then the **lm-reduction** of f by g is given by $f - a\tau g$.*

*We say, that f has a **strong Gröbner representation** w.r.t. $\mathcal{G}$, if $f = \sum_{i=1}^{m} h_i g_i$ with $m \in \mathbb{N}$, $g_i \in \mathcal{G}$, $h_i \in \mathcal{P}^e \setminus \{0\}$ and there exists a unique $1 \leq j \leq m$, such that $\mathrm{lm}(f) = \mathrm{lm}(h_j g_j)$ and $\mathrm{lm}(f) \succ \mathrm{lm}(h_i g_i)$ for all $i \neq j$.*

*$\mathcal{G}$ is called a **strong Gröbner basis** for $\mathcal{I}$, if $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$ and for all $f' \in \mathcal{I} \setminus \{0\}$ there exists $g' \in \mathcal{G}$, such that $\mathrm{lt}(g')$ divides $\mathrm{lt}(f')$.*

Such lm-reductions are the key to obtain a remainder after division through a finite generating set $\mathcal{G}$ for an ideal and they are used in Buchberger's algorithm to construct a Gröbner basis from $\mathcal{G}$. In this sense, the idea of a Gröbner basis is to deliver a unique remainder when dividing through it. Since we operate in a polynomial ring of multiple variables, the expression "reduction" is more justified than "division" to describe a chain of lm-reductions. The outcome of such a reduction, or the "remainder of the division", is then known as a **normal form**.

The following normal form algorithm uses lm-reductions and can be compared to the normal form algorithms, which is used for algebras over fields in (Levandovskyy, 2005).

NormalForm

---

input: $f \in \mathcal{P} \setminus \{0\}$, $\mathcal{G} \subseteq \mathcal{G}$ finite and partially ordered
output: normal form of f w.r.t. $\mathcal{G}$
01: $h = f$
02: **while** $h \neq 0$ **and** $\mathcal{G}_h = \{g \in \mathcal{G} \mid g \text{ lm-reduces } h\} \neq \emptyset$ **do**
03: choose $g \in \mathcal{G}_h$
04: choose $a, b \in \mathcal{R}$ with:
$a \neq 0$, $\mathrm{lc}(h) = a\,\mathrm{lc}(g) + b$ and $|b| < |\mathrm{lc}(h)|$
05: choose $\tau \in \mathcal{B}^e$ with $\mathrm{lm}(h) = \tau\,\mathrm{lm}(g)$
06: $h = h - a\tau g$, the lm-reduction of h by g
07: **end while**
08: **return** h

Every normal form of the zero-polynomial is zero. Termination and correctness are analogous to the proof in (Levandovskyy, 2005).

The output of the algorithm is in general not unique, but depends on the choice of elements $g \in \mathcal{G}_h$ which are used for the reduction.

We confirm, that the proof of the following theorem carries over verbatim from the commutative case in (Lichtblau, 2012).

Theorem 4. *((Lichtblau, 2012), Theorem 9)*
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and $\{0\} \neq \mathcal{I} \subseteq \mathcal{P}$ an ideal. Then the following statements with respect to $\mathcal{G}$ and a fixed monomial well-ordering $\preceq$ are equivalent:

1. *$\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$.*
2. *Every $f \in \mathcal{I} \setminus \{0\}$ has a strong Gröbner representation.*
3. *Every $f \in \mathcal{P} \setminus \{0\}$ has a unique normal form after reduction.*

An earlier non-commutative version was also proven by Pritchard for "weak" Gröbner bases in (Pritchard, 1996).

A strong Gröbner basis can be computed with Buchberger's algorithm using syzygy-relations between leading terms of generating polynomials. In the field case, the computation is done with S-polynomials. It is known from the commutative case over rings (Lichtblau, 2012), that it does not suffice to take so called "syzygy-polynomials" as in Definition 5 to obtain a strong Gröbner basis. To see this, let $\mathcal{I} = \langle f = 3x,\ g = 2y\rangle$. Then every syzygy-polynomial of f and g is zero, but clearly $xy = fy - xg \in \mathcal{I}$ has a leading term which is neither divisible by $\mathrm{lt}(f)$ nor $\mathrm{lt}(g)$. Thus, $\{f,\ g\}$ is not a strong Gröbner basis for $\mathcal{I}$. The problematic polynomial xy is constructed by looking at the greatest common divisor of the leading coefficients of f and g.

Definition 5.
*Let $f,\ g \in \mathcal{P} \setminus \{0\}$. Choose $\tau_f,\ \tau_g \in \mathcal{B}^e$, such that $\tau_f \,\mathrm{lm}(f) = \tau_g \,\mathrm{lm}(g) \in \mathrm{cm}(\mathrm{lm}(f),\ \mathrm{lm}(g))$. Furthermore, let $a = \mathrm{lcm}(\mathrm{lc}(f),\ \mathrm{lc}(f))$ and $a_f,\ a_g \in \mathcal{R}$, such that $a = a_f \,\mathrm{lc}(f) = a_g \,\mathrm{lc}(g)$. In a Euclidean domain, the least common multiple is uniquely determined up to a unit and so are $a_f,\ a_g$. Then an **S-polynomial** of f and g is defined as*

$$spoly(f,\ g) := a_f \tau_f f - a_g \tau_g g.$$

*Furthermore, let $b = gcd(\mathrm{lc}(f),\ \mathrm{lc}(f))$ and $b_f,\ b_f \in \mathcal{R}$, such that $b = b_f \,\mathrm{lc}(f) + b_g \,\mathrm{lc}(g)$ (the Bézout identity for the leading coefficients). As above, b is unique in a Euclidean domain as a greatest common divisor, although the Bézout coefficients $b_f,\ b_g$ may not be, but depend on the implementation of a Euclidean algorithm. A **G-polynomial** of f and g is defined as*

$$gpoly(f,\ g) := b_f \tau_f f + b_g \tau_g g.$$

So far everything seems to work out as in the commutative case. We consider some examples to see, that this assumption is wrong.

Example 6.
Let $f = 2xy,\ g = 3yz \in \mathbb{Z}\langle x,\ y,\ z\rangle$. Usually we would compute an S-polynomial $3fz - 2xg = 0$ and a G-polynomial

$$gpoly(f,\ g) := (-1) \cdot 2xy \cdot z + 1 \cdot x \cdot 3yz = xyz$$

and add them to $\{f,\ g\}$ to obtain a strong Gröbner basis for $\mathcal{I} = \langle f,\ g\rangle \subseteq \mathcal{P}$. But for every $w \in \mathcal{B}$

$$gpoly'(f,\ g) := (-1) \cdot 2xy \cdot w \cdot yz + 1 \cdot xy \cdot w \cdot 3yz = xywyz$$

is also a G-polynomial of $f,\ g$ and must be added to the basis. In other words there is no finite Gröbner basis for $\mathcal{I}$ and we have to be satisfied with computing up to a fixed maximal leading monomial or word length. Note that in the case of gpoly we computed a G-polynomial in the canonical way by looking for a non-trivial overlap of xy and yz. In the case of gpoly$'$ we ignored this overlap. In the commutative case this is irrelevant, because gpoly$(f,\ g)$ divides gpoly$'(f,\ g)$. Furthermore, in the field case this is also irrelevant, because we do not need G-polynomials.

Similar problems occur for S-polynomials.

Example 7.
Let $f = 2xy + x,\ g = 3yz + z$. Then $spoly(f,\ g) = 3fz - 2xg = xz$ is an S-polynomial of f and g. However, so are all polynomials

$$spoly'(f,\ g) := 3fwyz - 2xywg = 3xwyz - 2xywz$$

for any monomial $w \in \mathcal{B}$. Now we can reduce $spoly'(f, g)$ to

$$(spoly'(f, g) - xwg) + fwz = -2xywz + fwz = xwz$$

which is not reducible any further. Therefore, we have to add $spoly'(f, g)$ to the basis. And even this is not enough. For $f = 2xy + x$ we see that

$$spoly''(f, f) := fwxy - xywf = xwxy - xywx \neq 0$$

is an S-polynomial of f with itself which does not reduce any further and we need $\operatorname{lm}(f)w\operatorname{lm}(f) \in \operatorname{CM}(\operatorname{lm}(f), \operatorname{lm}(f))$, although it is clearly not contained in $\operatorname{LCM}(\operatorname{lm}(f), \operatorname{lm}(f))$.

Thus, in general **even principal ideals do not have finite strong Gröbner bases***! Such behavior of S-polynomials does not occur for non-commutative polynomials over fields.*

Note, that we do not consider any further extensions of the leading monomials, meaning that the S- and G-polynomial corresponding to $t \in \operatorname{LCM}(\operatorname{lm}(f), \operatorname{lm}(g))$ or $\operatorname{lm}(f)w\operatorname{lm}(g)$ make any further (trivial) overlap relations τt or $\tau(\operatorname{lm}(f)w\operatorname{lm}(g))$ for $\tau \in \mathcal{B}^e$ redundant. Therefore, in the definition of $\operatorname{LCM}(x, y)$ we stress the importance of the minimality.

The previous example shows, that we have to consider all possible S- and G-polynomials, but those are infinitely many. Moreover, the set $\operatorname{CM}(\operatorname{lm}(f), \operatorname{lm}(g))$ contains too many elements that are redundant whereas the set $\operatorname{LCM}(\operatorname{lm}(f), \operatorname{lm}(g))$ is too small. The following definition is made to classify two types of S- and G-polynomials, namely those corresponding to non-trivial overlap relations and those corresponding to trivial ones.

Definition 8.
Let $f, g \in \mathcal{P} \setminus \{0\}$ and $a_f, a_g, b_f, b_g \in \mathcal{R}$ as in Definition 5. We distinguish between the following two cases.

If $\operatorname{lm}(f)$ and $\operatorname{lm}(g)$ have a non-trivial overlap, then there exist $t \in \operatorname{LCM}(\operatorname{lm}(f), \operatorname{lm}(g))$ and $\tau_f, \tau_g \in \mathcal{B}^e$, such that $t = \tau_f \operatorname{lm}(f) = \tau_g \operatorname{lm}(g)$. Furthermore, we assume that $\tau_f = 1 \otimes t_f$, $\tau_g = t_g \otimes 1$ or $\tau_f = 1 \otimes 1$, $\tau_g = t_g \otimes t'_g$ for $t_f, t_g, t'_g \in \mathcal{B}$ with $|t_f| < |\operatorname{lm}(g)|$, $|t_g|, |t'_g| < |\operatorname{lm}(f)|$. We define a ***first type S-polynomial*** *of f and g w.r.t. t to be*

$$spoly_1^t(f, g) := a_f \tau_f f - a_g \tau_g g$$

and a ***first type G-polynomial*** *of f and g w.r.t. t to be*

$$gpoly_1^t(f, g) := b_f \tau_f f + b_g \tau_g g.$$

If such τ_f, τ_g do not exist, we set the first type S- and G-polynomials both to zero. Since two monomials may have several non-trivial overlaps, these τ_f, τ_g are not unique. More precisely, this follows from the fact that $\mathcal{P}$ is not a unique, but a **finite factorization domain** *(Bell et al., 2016). For any $w \in \mathcal{B}$ we define the* ***second type S-polynomial*** *of f and g w.r.t. w to be*

$$spoly_2^w(f, g) := a_f fw\operatorname{lm}(g) - a_g \operatorname{lm}(f)wg$$

and the ***second type G-polynomial*** *of f and g w.r.t. w to be*

$$gpoly_2^w(f, g) := b_f fw\operatorname{lm}(g) + b_g \operatorname{lm}(f)wg.$$

Remark 9.
Clearly, it only makes sense to consider first type S- and G-polynomials if there is a non-trivial overlap of the leading monomials. However, as Example 6 shows, we always need to consider second type S- and G-polynomials. For any $w \in \mathcal{B}$ *we have* $\mathrm{lm}(f)w\,\mathrm{lm}(g) \in \mathrm{CM}(\mathrm{lm}(f), \mathrm{lm}(g))$ *and* $\mathrm{lm}(g)w\,\mathrm{lm}(f) \in \mathrm{CM}(\mathrm{lm}(f), \mathrm{lm}(g))$*, which are distinct in general. Therefore, we need to consider both* $\mathrm{spoly}_2^w(f, g)$ *and* $\mathrm{spoly}_2^w(g, f)$ *and the same holds for second type G-polynomials. Also, note that the set of first type S- and G-polynomials is finite, because our monomial ordering is a well-ordering, whereas the set of second type S- and G-polynomials is infinite. Therefore, we need to fix an upper bound for the length of monomials which may be involved.*

It is important to point out, that the elements τ_f, τ_g *are not uniquely determined. Take for example* $f = 2xyx + y$, $g = 3x + 1$. *Then* $t := xyx = \mathrm{lm}(f) = xy\,\mathrm{lm}(g) \in \mathrm{LCM}(\mathrm{lm}(f), \mathrm{lm}(f))$*, but also* $t = \mathrm{lm}(g)yx$ *and thus* $\mathrm{spoly}_1^t(f, g) = -3f + 2gyx = 2yx - 3y$ *and* $(\mathrm{spoly}_1^t)'(f, g) = -3f + 2xyg = 2xy - 3y$ *are both first type S-polynomials with different leading monomials.*

A finite set $\mathcal{G} \subseteq \mathcal{P}$ is called **length-bounded strong Gröbner basis** for an ideal $\mathcal{I}$, if there is a Gröbner basis $\mathcal{G}'$ for $\mathcal{I}$, such that $\mathcal{G} \subseteq \mathcal{G}'$ contains precisely the elements of $\mathcal{G}'$ of length smaller or equal to d for some $d \in \mathbb{N}$.

The following algorithm uses Buchberger's criterion 10 as a characterization for strong Gröbner bases, which we will prove subsequently. It computes S- and G-polynomials up to a fixed degree and reduces them with the algorithm NormalForm in order to obtain a length-bounded strong Gröbner basis for an input ideal given by a finite generating set.

BuchbergerAlgorithm

---

input: $\mathcal{I} = \langle f_1, \ldots, f_k \rangle \subseteq \mathcal{R}\langle X \rangle$, $d \in \mathbb{N}$, NormalForm
output: length-bounded strong Gröbner basis $\mathcal{G}$ for $\mathcal{I}$
01: $\mathcal{G} = \{f_1, \ldots, f_k\}$
02: $\mathcal{L} = \{\mathrm{spoly}_1^t(f_i, f_j), \mathrm{gpoly}_1^t(f_i, f_j) \mid \forall\, t\,^*, i, j\}$
03: $\mathcal{L} = \mathcal{L} \cup \{\mathrm{spoly}_2^w(f_i, f_j), \mathrm{gpoly}_2^w(f_i, f_j) \mid \forall\, w\,^{**}, i, j\}$
04: **while** $\mathcal{L} \neq \emptyset$ **do**
05: choose $h \in \mathcal{L}$
06: $\mathcal{L} = \mathcal{L} \setminus \{h\}$
07: $h = \mathrm{NormalForm}(h, \mathcal{G})$
08: **if** $h \neq 0$ **then**
09: $\mathcal{G} = \mathcal{G} \cup \{h\}$
10: **for** $g \in \mathcal{G}$ **do**
11: $\mathcal{L} = \mathcal{L} \cup \{\mathrm{spoly}_1^t(g, h), \mathrm{gpoly}_1^t(g, h) \mid \forall\, t\,^*\}$
$\mathcal{L} = \mathcal{L} \cup \{\mathrm{spoly}_1^t(h, g), \mathrm{gpoly}_1^t(h, g) \mid \forall\, t\,^*\}$
$\mathcal{L} = \mathcal{L} \cup \{\mathrm{spoly}_2^w(g, h), \mathrm{gpoly}_2^w(g, h) \mid \forall\, w\,^{**}\}$
$\mathcal{L} = \mathcal{L} \cup \{\mathrm{spoly}_2^w(h, g), \mathrm{gpoly}_2^w(h, g) \mid \forall\, w\,^{**}\}$
12: **end do**
13: **end if**
14: **end while**
15: **return** $\mathcal{G}$

---

* $t \in \mathrm{LCM}(\bullet, \bullet)$, such that $|t| < d$
** $w \in \mathcal{B}$, such that $|\,\mathrm{lm}(\bullet)| + |w| + |\,\mathrm{lm}(\bullet)| < d$

For the algorithm to terminate we need the set $\mathcal{L}$ to eventually become empty. This happens, if and only if after finitely many steps every S- and G-polynomial based on any combination of leading terms has normal form zero w.r.t $\mathcal{G}$, i.e. there exists a chain of lm-reductions, such that the current S- or G-polynomial reduces to zero. However, lm-reductions only use polynomials of smaller or equal length and all of these are being computed. Therefore, the algorithm terminates.

For the correctness of the algorithm we still need a version of Buchberger's criterion. More precisely, we want $\mathcal{G}$ to be a Gröbner basis for $\mathcal{I}$, if and only if for every pair $f, g \in \mathcal{G}$ all their S- and G-polynomials reduce to zero. Moreover, we only want to consider first and second type S- and G-polynomials, i.e. only use $t \in \text{CM}(\text{lm}(f), \text{lm}(g))$, such that one of the following four cases

$$\begin{aligned} &(1)\ t = \text{lm}(f)t'_f = t_g \,\text{lm}(g) \qquad (2)\ t = \text{lm}(f) = t_g \,\text{lm}(g)t'_g \\ &(3)\ t = t_f \,\text{lm}(f) = \text{lm}(g)t'_g \qquad (4)\ t = t_f \,\text{lm}(f)t'_f = \text{lm}(g) \end{aligned}$$

holds for $t_f, t'_f, t_g, t'_g \in \mathcal{B}$. This excludes all cases where t is not minimal, i.e. $t = \tau t'$ for $\tau \in \mathcal{B}^e$ and t' satisfying one of the above four cases. Pritchard has proven in (Pritchard, 1996), that for a generating set of the left syzygy module (which is not finitely generated in general) we may use only minimal syzygies.

Lemma 10. *((Lichtblau, 2012), Theorem* 10*)*
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$. Then $\mathcal{G}$ is a strong Gröbner basis for $\langle \mathcal{G} \rangle$, if and only if for every pair $f, g \in \mathcal{G}$ their first and second type S- and G-polynomials reduce to zero w.r.t. $\mathcal{G}$.

Proof. The idea of the proof goes back to (Lichtblau, 2012); we only need to show the "if" part. Let $0 \neq f \in \langle \mathcal{G} \rangle =: \mathcal{I}$ with $f = \sum_i h_i g_i$ for some $h_i \in \mathcal{P}^e$. We set $t := \max(\text{lm}(h_i g_i))$ and $M := \{i \in \mathbb{N} \mid \text{lm}(h_i g_i) = t\}$. Clearly $\text{lm}(f) \preceq t$ and we may assume that there is no other representation of f where t is smaller. Without loss of generality let $M = \{1, \ldots, m\}$. Moreover, since the Euclidean norm induces a well ordering, we can choose a representation where $\sum_{i=1}^{m} |\,\text{lc}(h_i)\,\text{lc}(g_i)|$ is minimal w.r.t. t. If M contains exactly one element, then $t = \text{lm}(f)$ and we have a strong standard representation of f w.r.t. $\mathcal{G}$. Suppose otherwise that $\text{card}(M) > 1$. Then $t \succeq \text{lm}(f)$. Note that $t = \text{lm}(h_i g_i) = \text{lm}(h_i)\,\text{lm}(g_i)$ for $i \leq m$. Then there exist monomials $t_1, t'_1, t_2, t'_2 \in X$, such that $t = t_1 \,\text{lm}(g_1)t'_1 = t_2 \,\text{lm}(g_2)t'_2$. This induces an overlap relation of the leading monomials, because then there exist $s_1, s'_1, s_2, s'_2 \in X$, such that

- $T := \text{lm}(g_1)s'_1 = s_2 \,\text{lm}(g_2)$,
- $T := \text{lm}(g_1) = s_2 \,\text{lm}(g_2)s'_2$,
- $T := s_1 \,\text{lm}(g_1) = \text{lm}(g_2)s'_2$ or
- $T := s_1 \,\text{lm}(g_1)s'_1 = \text{lm}(g_2)$

and $t = \tau T$ for some monomial $\tau \in \mathcal{P}^e$. Moreover, let τ_1, τ_2 result from s_1, s'_1, s_2, s'_2, such that $\tau_1 T = \text{lm}(g_1)$, $\tau_2 T = \text{lm}(g_2)$. Furthermore, let

$$a_1 := \frac{\text{lcm}(\text{lc}(g_1), \text{lc}(g_2))}{\text{lc}(g_1)}, \; a_2 := \frac{\text{lcm}(\text{lc}(g_1), \text{lc}(g_2))}{\text{lc}(g_2)}$$

$d := \gcd(\text{lc}(g_1), \text{lc}(g_2)) = b_1 \,\text{lc}(g_1) + b_2 \,\text{lc}(g_2) \in \mathcal{R}$, the Bézout identity for the leading coefficients. Now if T corresponds to a non-trivial overlap, then we can compute $\text{spoly}_1^T(g_1, g_2)$, $\text{gpoly}_1^T(g_1, g_2)$ or $\text{spoly}_1^T(g_2, g_1)$, $\text{spoly}_1^T(g_2, g_1)$. Otherwise, there exists a $w \in \mathcal{B}$, such that

$T = \operatorname{lm}(g_1)w\operatorname{lm}(g_2)$ or $T = \operatorname{lm}(g_2)w\operatorname{lm}(g_1)$. In this case we are interested in $\operatorname{spoly}_2^w(g_1, g_2)$, $\operatorname{gpoly}_2^w(g_1, g_2)$ or $\operatorname{spoly}_2^w(g_2, g_1)$, $\operatorname{gpoly}_2^w(g_2, g_1)$. By definition

$$\begin{aligned} & \operatorname{spoly}(g_1, g_2) := a_1\tau_1 g_1 - a_2\tau_2 g_2 \\ \text{and} \quad & \operatorname{gpoly}(g_1, g_2) := b_1\tau_1 g_1 + b_2\tau_2 g_2 \end{aligned}$$

are first or second type S- and G-polynomials and $\operatorname{lm}(h_1) = \tau\tau_1$, $\operatorname{lm}(h_2) = \tau\tau_2$. Choose $a, b \in \mathcal{R} \setminus \{0\}$, such that $\operatorname{lc}(h_1)\operatorname{lc}(g_1) + \operatorname{lc}(h_2)\operatorname{lc}(g_2) = ad$ and $\operatorname{lc}(h_1) = ab_1 + ba_1$, $\operatorname{lc}(h_2) = ab_2 - ba_2$. Then, since $|a_1 \operatorname{lc}(g_1) + a_2 \operatorname{lc}(g_2)| > 0$ and by the triangle inequality, we have

$$\begin{aligned} & |\operatorname{lc}(h_1)\operatorname{lc}(g_1)| + |\operatorname{lc}(h_2)\operatorname{lc}(g_2)| \\ =& |(ab_1 + ba_1)\operatorname{lc}(g_1)| + |(ab_2 - ba_2)\operatorname{lc}(g_2)| \\ \geq& |ab_1 \operatorname{lc}(g_1)| + |ba_1 \operatorname{lc}(g_1)| + |ab_2 \operatorname{lc}(g_2)| + |ba_2 \operatorname{lc}(g_2)| \\ >& |ab_1 \operatorname{lc}(g_1)| + |ab_2 \operatorname{lc}(g_2)| \geq |ab_1 \operatorname{lc}(g_1) + ab_2 \operatorname{lc}(g_2)| = |ad|, \end{aligned}$$

thus $|ad| < |\operatorname{lc}(h_1)\operatorname{lc}(g_1)| + |\operatorname{lc}(h_2)\operatorname{lc}(g_2)|$. Furthermore, we have

$$\begin{aligned} h_1 g_1 + h_2 g_2 =& (\operatorname{lc}(h_1)\operatorname{lm}(h_1)\operatorname{tail}(h_1))g_1 + (\operatorname{lc}(h_2)\operatorname{lm}(h_2)\operatorname{tail}(h_2))g_2 \\ =& (ab_1 + ba_1)\tau\tau_1 g_1 + \operatorname{tail}(h_1)g_1 + (ab_2 - ba_2)\tau\tau_2 g_2 + \operatorname{tail}(h_2)g_1 \\ =& a\tau(b_1\tau_1 g_1 + b_2\tau_2 g_2) + b\tau(a_1\tau_1 g_1 - a_2\tau_2 g_2) + \operatorname{tail}(h_1)g_1 + \operatorname{tail}(h_2)g_1 \\ =& a\tau \operatorname{gpoly}(g_1, g_2) + b\tau\operatorname{spoly}(g_1, g_2) + \operatorname{tail}(h_1)g_1 + \operatorname{tail}(h_2)g_1. \end{aligned}$$

Since the S- and the G-polynomial are of first or second type they reduce to zero w.r.t. $\mathcal{G}$. Hence we can write $h_1 g_1 + h_2 g_2 = \sum_j h'_j g_j$ for $h'_j \in \mathcal{P}^e$ and define $M' := \{j \in \mathbb{N} \mid \operatorname{lm}(h'_j g_j) = t\}$. Since $\operatorname{lm}(\tau\operatorname{spoly}(g_1, g_2)) \prec t$, $\operatorname{lm}(\operatorname{tail}(h_1)g_1) \prec t$ and $\operatorname{lm}(\operatorname{tail}(h_2)g_1) \prec t$ we have

$$\begin{aligned} & \sum_{j \in M'} |\operatorname{lc}(h'_j)\operatorname{lc}(g_j)| \\ =& \sum_{j \in M'} |\operatorname{lc}(h'_j g_j)| \\ =& |\operatorname{lc}(d\tau \operatorname{gpoly}(g_1, g_2))| \\ =& |ad| \\ <& |\operatorname{lc}(h_1)\operatorname{lc}(g_1)| + |\operatorname{lc}(h_2)\operatorname{lc}(g_2)|, \end{aligned}$$

which contradicts our assumption that the leading coefficient of our original representation are minimal. Therefore, M contains exactly one element and thus we have a strong Gröbner representation of f w.r.t. $\mathcal{G}$, i.e. $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$. □

It is possible to define monic (that is, with leading coefficients being 1) and reduced Gröbner bases (Li, 2012; Pauer, 2007) in our setup. Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$. It is called a **reduced Gröbner basis**, if

1. every $g \in \mathcal{G}$ has leading coefficient with signum 1,
2. $\mathrm{L}(\mathcal{G} \setminus \{g\}) \subsetneq \mathrm{L}(\mathcal{G})$ for every $g \in \mathcal{G}$ and
3. $\operatorname{lt}(\operatorname{tail}(g)) \notin \mathrm{L}(\mathcal{G})$ for every $g \in \mathcal{G}$.

The first condition states, that in the case of $\mathcal{R} = \mathbb{Z}$ every element of a reduced Gröbner basis has leading coefficient in $\mathbb{Z}_+$. The second condition is sometimes referred to as "simplicity" and means that the leading ideal becomes strictly smaller when removing an element, thus no element is useless. The third condition, "tail-reduced", is required in the classical field case with commutative polynomials to ensure that a reduced Gröbner basis is unique. However, this does not suffice in our setup: for instance, Pritchard gave the following counterexample in (Pritchard, 1996).

Let $f = 2y^2$, $g = 3x^2 + y^2$ and $\mathcal{I} = \langle f, g\rangle$. Then $\{f, g\}$ is a Gröbner basis for $\mathcal{I}$ with respect to any ordering $x \succ y$ and satisfies the above three conditions. On the other hand, this is also true for $\{f, g'\}$ where $g' = g - f = 3x^2 - y^2$, so we have two different reduced Gröbner bases for $\mathcal{I}$. In the field case the polynomial g is not tail-reduced. This example can be used in both the commutative and non-commutative case.

When implementing a version of Buchberger's algorithm, one should always aim to have a reduced Gröbner basis as an output. In fact this is more practical, because removing elements, which are not simplified or tail reduced speeds up the computation, since we do not need to consider them in critical pairs.

Lemma 11.
Let $\mathcal{G} \subset \mathcal{P} \setminus \{0\}$ be finite and contain only polynomials up to degree $d \in \mathbb{N}$. Assume moreover, that no new polynomials are added to $\mathcal{G}$, while computing a length-bounded Gröbner basis up to degree $3d - 1$ with the BuchbergerAlgorithm.
Then $\mathcal{G}$ is a strong Gröbner basis for $\langle\mathcal{G}\rangle$.

Proof. Suppose, that continuing the procedure beyond degree $3d$ would yield a new polynomial $p \in \langle\mathcal{G}\rangle$ from a pair f, g with leading monomial $\mathrm{lm}(f)w\,\mathrm{lm}(g)$ for some $w \in \mathcal{B}$, such that $|\mathrm{lm}(f)| = |\mathrm{lm}(g)| = |w| = d$. Then $\mathrm{lm}(f)w'\,\mathrm{lm}(g)$ can not yield a new leading monomial for every subword w' of w with length up to $d-1$. Hence we may assume, that $\mathrm{lm}(f)$, $\mathrm{lm}(g)$ are coprime and f, g, w satisfy the conditions of Buchberger's product criterion in the non-commutative ring case. We will prove this criterion in Lemma 16. Therefore p must reduce to zero, a contradiction. □

In the non-commutative case over fields the bound is $2d - 1$. Here we gain an extra d, because we have to consider S- and G-polynomials of the second kind corresponding to w. As we will see, the product criterion does not generalize simply from the field case. Generic examples show, that the bound $3d - 1$ is sharp.

3. Coefficient Rings with Zero-divisors

When the ring of coefficients is not a domain like $\mathbb{Z}$, but a Euclidean **ring** like $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ for some non-zero $m \in \mathbb{Z}$, which is neither a unit nor a prime, then we can make use of factorizations of m. Recall, that a factorization of m, say $m = ab$ for some coprime $a, b \in \mathbb{Z}$, implies, that $xy \neq m$ for $a \nmid x \mid a$, $b \nmid y \mid b$. Suppose, that $cx = a$, $dy = b$ and $xy = m$. Then $m = ab = cxdy = cdm$ and so $m(1 - cd) = 0$, which implies $1 = cd$, because $\mathbb{Z}$ is a domain. But then c is a unit, which contradicts $a \nmid x$.

This was easy to see, but it also means, that we have to choose our coefficients wisely, when using lifting methods. For $a, b \in \mathbb{Z}$ coprime, we consider the canonical projections

$$\begin{aligned} \pi &: \quad \mathbb{Z}\langle X\rangle \quad\quad\quad\quad\quad\quad\quad\quad \to \mathbb{Z}_m\langle X\rangle, \\ \pi_a &: \quad \mathbb{Z}_m\langle X\rangle \cong (a\mathbb{Z} + b\mathbb{Z})/m\mathbb{Z}\langle X\rangle \to \mathbb{Z}_a\langle X\rangle \\ \text{and} \quad \pi_b &: \quad \mathbb{Z}_m\langle X\rangle \cong (a\mathbb{Z} + b\mathbb{Z})/m\mathbb{Z}\langle X\rangle \to \mathbb{Z}_b\langle X\rangle. \end{aligned}$$

For an ideal $\mathcal{J}$ of $\mathbb{Z}_m\langle X\rangle =: \mathcal{P}_m$, we assume, that there exist countable sets $\mathcal{G}_a = \{g_{a,i}\}_i$, $\mathcal{G}_b = \{g_{b,j}\}_j \subseteq \mathcal{P}_m$, such that $\pi_a(\mathcal{G}_a)$ is a strong Gröbner basis for $\pi_a(\mathcal{J})$ and $\pi_b(\mathcal{G}_b)$ is a strong Gröbner basis for $\pi_b(\mathcal{J})$. Additionally, let $\pi(a) \in \mathcal{G}_a$, $\pi(b) \in \mathcal{G}_b$, $\pi(a) \nmid \mathrm{lc}(g_{a,i}) \mid \pi(a)$ for $g_{a,i} \neq \pi(a)$ and $\pi(b) \nmid \mathrm{lc}(g_{b,j}) \mid \pi(b)$ for $g_{b,j} \neq \pi(b)$. This implies, that each leading coefficient is a non-trivial zero divisor in the respective quotient ring. For every pair $(i,\ j)$ of indices there exist monomials $\tau_{i,j},\ \tau_{j,i} \in \mathcal{B}^e$, such that $\tau_{i,j}\,\mathrm{lm}(g_{a,i}) = \tau_{j,i}\,\mathrm{lm}(g_{b,j})$ and four following cases occur

- $\tau_{i,j} = 1 \otimes x',\ \tau_{j,i} = y \otimes 1$,
- $\tau_{i,j} = x \otimes 1,\ \tau_{j,i} = 1 \otimes y'$,
- $\tau_{i,j} = 1 \otimes 1,\ \tau_{j,i} = y \otimes y'$ or
- $\tau_{i,j} = x \otimes x',\ \tau_{j,i} = 1 \otimes 1$

for suitable monomials $x,\ x',\ y,\ y' \in \mathcal{B}^e$. These are precisely the overlap relations corresponding to first and second type S- and G-polynomials. We define

$$f_{i,j} := \pi(ar)\,\mathrm{lc}(g_{a,i})\tau_{j,i}g_{b,j} + \pi(bs)\,\mathrm{lc}(g_{b,j})\tau_{i,j}g_{a,i}.$$

Theorem 12.
Let $m = ab \in \mathbb{Z}$ with a, b coprime such that $ar + bs = 1$ for some $r,\ s \in \mathbb{Z}$. Furthermore, let $\mathcal{J}$ be an ideal of $\mathcal{P}_m$ accompanied by the sets $\mathcal{G}_a$ and $\mathcal{G}_b$ defined as above.
Then $\mathcal{G} := \{f_{i,j} \mid \tau_{i,j}\,\mathrm{lm}(g_{a,i}) = \tau_{j,i}\,\mathrm{lm}(g_{b,j})\}$ is a strong Gröbner basis for $\mathcal{J}$.

Proof. By the second isomorphism theorem we have

$$\begin{aligned} &\mathbb{Z}_m/\overline{a}\mathbb{Z}_m = \mathbb{Z}_m/(\pi(a)\mathbb{Z}_m) \cong \mathbb{Z}_a \\ \text{and}\quad &\mathbb{Z}_m/\overline{b}\mathbb{Z}_m = \mathbb{Z}_m/(\pi(b)\mathbb{Z}_m) \cong \mathbb{Z}_b. \end{aligned}$$

From this and the forthcoming Theorem 13.1 it follows that $\mathcal{G}_a \cup \{\overline{a}\} = \mathcal{G}_a$, $\mathcal{G}_b \cup \{\overline{b}\} = \mathcal{G}_b$ are strong Gröbner basis of $\mathcal{I} + \overline{a}\mathcal{P}_m$, $\mathcal{I} + \overline{b}\mathcal{P}_m$ respectively. Then, again using the isomorphism theorem, all conditions of Theorem 13.2 are satisfied and it follows, that $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$. □

Note, that the $\tau_{i,j}$, $\tau_{j,i}$ are not uniquely determined since all overlap relations of the leading monomials have to be considered. The above lemma improves our algorithm for computing Gröbner bases over principal ideal rings. It remains to show, that the Theorems 10 and 12 from (Eder and Hofmann, 2019), formulated in the commutative case also hold in the non-commutative one.

Theorem 13. *((Eder and Hofmann, 2019), Theorems* 10 *and* 12*)*
1. *Let $m \in \mathbb{Z} \setminus \{0\}$ and $\mathcal{I}$ an ideal of $\mathcal{P}$. Let $\mathcal{G} \subseteq \mathcal{P}$, such that $\pi(\mathcal{G})$ is a strong Gröbner basis of $\pi(\mathcal{I})$. Additionally, we assume that $m \nmid \mathrm{lc}(g) \mid m$ for every $g \in \mathcal{G}$, i.e. $\pi(\mathrm{lc}(g))$ is a non-trivial zero divisor in $\mathbb{Z}_m$. Then $\mathcal{G} \cup \{m\}$ is a strong Gröbner basis for $\mathcal{I} + m\mathcal{P}$.*

2. *Let $\mathcal{J}$ be an ideal of $\mathcal{P}_m$ and a, b, r, $s \in \mathbb{Z}_m$, such that $ab = 0$ and a, b coprime with $ar + bs = 1$. Let $\mathcal{G}_a$, $\mathcal{G}_b$ be Gröbner bases for $\mathcal{J} + a\mathcal{P}_m$ and $\mathcal{J} + b\mathcal{P}_m$ respectively, such*

that for every $g_{a,i} \in \mathcal{G}_a \setminus \mathbb{Z}_m$ *we have* $a \nmid \operatorname{lc}(g_{a,i}) \mid a$. *Assume, that the same holds for* $\mathcal{G}_b$. *For* $g_{a,i} \in \mathcal{G}_a$ *and* $g_{b,j} \in \mathcal{G}_b$ *we define*

$$f_{i,j} := \pi(ar)\operatorname{lc}(g_{a,i})\tau_{j,i}g_{b,j} + \pi(bs)\operatorname{lc}(g_{b,j})\tau_{i,j}g_{a,i}$$

and assume that $\operatorname{lc}(g_{a,i})\operatorname{lc}(g_{b,j}) \neq 0$ *for all* i, j.
Then $\mathcal{G} := \{f_{i,j}\}_{i,j}$ *is a strong Gröbner basis for* $\mathcal{J}$.

Proof. 1. Clearly $\mathcal{G} \cup \{m\}$ is a subset of $\mathcal{I} + m\mathcal{P}$. Let $f \in \mathcal{I}$. If $\pi(f) = 0$, then $m \mid \operatorname{lt}(f)$. So we may assume $\pi(f) \neq 0$ and $m \nmid \operatorname{lc}(f)$. Then $\operatorname{lm}(\pi(f)) = \operatorname{lm}(f)$ and there exists $g \in \mathcal{G}$ such that $\operatorname{lt}(\pi(g)) \mid \operatorname{lt}(\pi(f))$, because $\pi(\mathcal{G})$ is a Gröbner basis and we can find a term $h \in \mathcal{P}^e$ with $\pi(h)\operatorname{lt}(\pi(g)) = \operatorname{lt}(\pi(f))$. Thus $\operatorname{lm}(h)\operatorname{lm}(g) = \operatorname{lm}(f)$ and $\pi(h\operatorname{lt}(g) - \operatorname{lt}(f)) = 0$. Thus, we have $h\operatorname{lt}(g) - \operatorname{lt}(f) = c\operatorname{lm}(f)$ for some $c \in m\mathbb{Z}$ and hence $\operatorname{lt}(g) \mid \operatorname{lt}(f)$, because $\operatorname{lc}(g) \mid m$ by our additional assumption and $\operatorname{lm}(g) \mid \operatorname{lm}(f)$. In other words $\mathcal{G} \cup \{m\}$ is a strong Gröbner basis for $\mathcal{I} + m\mathcal{P}$.

2. By our assumptions we have $\mathcal{J} = ar\mathcal{J} + bs\mathcal{J} = ar(\mathcal{J} + b\mathcal{P}_m) + bs(\mathcal{J} + a\mathcal{P}_m) = ar\langle\mathcal{G}_b\rangle + bs\langle\mathcal{G}_a\rangle$. Since a and b are coprime and $\operatorname{lc}(g_{a,i}) \mid a$, $\operatorname{lc}(g_{b,j}) \mid b$, we see that $\operatorname{lc}(g_{a,i})$ and $\operatorname{lc}(g_{b,j})$ are coprime as well. Furthermore, we have $\operatorname{lc}(g_{a,i})\operatorname{lc}(g_{b,j})\mathbb{Z}_m = \operatorname{lc}(g_{a,i})\mathbb{Z}_m \cap \operatorname{lc}(g_{b,j})\mathbb{Z}_m \supsetneq a\mathbb{Z}_m \cap b\mathbb{Z}_m = \{0\}$ and thus $\operatorname{lt}(f_{i,j}) = \operatorname{lc}(g_{a,i})\operatorname{lc}(g_{b,j})\tau_{j,i}\operatorname{lm}(g_{b,j})$. Now let $f \in \mathcal{J} \subseteq (\mathcal{J} + a\mathcal{P}_m) \cap (\mathcal{J} + b\mathcal{P}_m)$. Then there exist $g_{a,i} \in \mathcal{G}_a$ and $g_{b,j} \in \mathcal{G}_b$, such that $\operatorname{lt}(g_{a,i}) \mid \operatorname{lt}(f)$ and $\operatorname{lt}(g_{b,j}) \mid \operatorname{lt}(f)$. Especially $\tau_{i,j}\operatorname{lm}(g_{a,i}) \mid \operatorname{lm}(f)$ and $\operatorname{lcm}(\operatorname{lc}(g_{a,i}), \operatorname{lc}(g_{b,j})) \mid \operatorname{lc}(f)$. Finally, $\operatorname{lt}(f_{i,j}) \mid \operatorname{lt}(f)$ and $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{J}$. □

4. Forming and Discarding Critical Pairs

To improve the procedure BuchbergerAlgorithm, we need criteria to determine which pairs of polynomials of the input set yield S- and G-polynomials, which reduce to zero. In the following we will recall the criteria for discarding critical pairs known from the commutative case and analyze, which of them can be applied in the case $\mathcal{R}\langle X\rangle$.

Remark 14.
Consider the case $t := \operatorname{lm}(f)$ *is divisible by (or even equal to)* $\operatorname{lm}(g)$. *Then* $\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$ *contains exactly one element, namely* t, *because it is the only minimal element that is divisible by both leading monomials. Therefore,* $\operatorname{spoly}_1^t(f, g)$ *and* $\operatorname{gpoly}_1^t(f, g)$ *are the only first type S- and G-polynomials. However, these are not uniquely determined, we might have more overlap relations of* $\operatorname{lm}(f)$, $\operatorname{lm}(g)$, *as we have seen in the previous example of Remark 9, and we still need second type S-polynomials.*

The following Lemma justifies why G-polynomials are redundant over fields.

Lemma 15. *(Buchberger's criterion (Eder et al., 2021; Lichtblau, 2012))*
Let $f, g \in \mathcal{P} \setminus \{0\}$. *If* $\operatorname{lc}(f) \mid \operatorname{lc}(g)$ *in* $\mathcal{R}$, *then every G-polynomial of* f *and* g *is redundant.*

Proof. By the hypothesis we have $b = \operatorname{lcm}(\operatorname{lc}(f), \operatorname{lc}(g)) = \operatorname{lc}(f)$. Let $r \in \mathcal{R}$, such that $r\operatorname{lc}(f) = \operatorname{lc}(g)$. Then $\operatorname{lc}(f) = (nr + 1)\operatorname{lc}(f) - n\operatorname{lc}(g)$ yields any possible Bézout identity for b, where $n \in \mathbb{Z}$. Thus, with $t = \tau_f\operatorname{lm}(f) = \tau_g\operatorname{lm}(g)$, every G-polynomial of f and g has shape $\operatorname{gpoly}(f, g) = (nr + 1)\tau_f f - n\tau_g g = \operatorname{lc}(f)t + n(r\tau_f\operatorname{tail}(f) - \tau_g\operatorname{tail}(g)) + \tau_f\operatorname{tail}(f)$. Subtracting $\tau_f f$, we can reduce this to $n(r\tau_f\operatorname{tail}(f) - \tau_g\operatorname{tail}(g))$. Note that $r\tau_f\operatorname{tail}(f) - \tau_g\operatorname{tail}(g)$ is an S-polynomial of f and g. Hence, every G-polynomial of f and g reduces to zero, after we compute their S-polynomials. □

For $f \in \mathcal{P} \setminus \{0\}$, we iteratively define $\mathrm{tail}^0(f) := f$ and $\mathrm{tail}^i(f) := \mathrm{tail}(\mathrm{tail}^{i-1}(f))$ for $i \geq 1$.

Lemma 16. *(Buchberger's product criterion (Eder et al., 2021; Lichtblau, 2012))*
Let $f, g \in \mathcal{P} \setminus \{0\}$ and $w \in \mathcal{B}$, such that

1. $\mathrm{lc}(f)$ *and* $\mathrm{lc}(g)$ *are coprime over* $\mathcal{R}$,
2. $\mathrm{lm}(f)$ *and* $\mathrm{lm}(g)$ *only have trivial overlaps and*
3. *for all* $i, j \geq 1$ *the inequality* $\mathrm{lm}(\mathrm{tail}^i(f))w\,\mathrm{lm}(g) \neq \mathrm{lm}(f)w\,\mathrm{lm}(\mathrm{tail}^j(g))$ *takes place.*

Then $s := spoly_2^w(f, g)$ *reduces to zero w.r.t.* $\{f, g\}$.

Proof. Under the assumptions (1) and (2) we have $s = fw\,\mathrm{lt}(g) - \mathrm{lt}(f)wg = fw(g - \mathrm{tail}(g)) - (f - \mathrm{tail}(f))wg = \mathrm{tail}(f)wg - fw\,\mathrm{tail}(g)$. Note that $\mathrm{tail}(f)wg$ reduces to zero w.r.t. g and $fw\,\mathrm{tail}(g)$ reduces to zero w.r.t. f.

By (3) we can assume without loss of generality that $\mathrm{lt}(s) = \mathrm{lt}(\mathrm{tail}(f))w\,\mathrm{lt}(g)$. Then s reduces to $s' := s - \mathrm{lt}(\mathrm{tail}(f))wg$ and $\mathrm{lm}(s') \prec \mathrm{lm}(s)$. Again by (3) there is no cancellation of leading terms and, since $\prec$ is a well ordering, we iteratively see that s reduces to zero. □

Remark 17.
The commutative version of Buchberger's product criterion in (Eder et al., 2021; Lichtblau, 2012) states, that the S-polynomial reduces to zero, if the leading terms are coprime over $\mathbb{Z}[X]$.

Condition (3)*, or rather its negation, describes a very specific relation between the terms of f and g. There is only a finite amount of $w \in \mathcal{B}$, that satisfy such relation and are at the same time considered in* BuchbergerAlgorithm*, because we only compute up to a certain length.*

The version over fields for this criterion is much simpler, because then we only consider w to be the empty word which clearly satisfies (3)*. Moreover,* (1) *is redundant and Buchberger's product criterion states that an S-polynomial reduces to zero when the leading monomials have only trivial overlap relations.*

We consider further situations, in which we might find applications for criteria.

Example 18.
If $\mathrm{lm}(f)$ *and* $\mathrm{lm}(g)$ *have no non-trivial overlap and the leading coefficients are not coprime, i.e.* $\mathrm{lcm}(\mathrm{lc}(f), \mathrm{lc}(g)) \neq 1$*, then we can make no* a priori *statement about reduction. This only applies to second type S- and G-polynomials. Take for example* $f = 4xy + x$, $g = 6zy + z \in \mathbb{Z}\langle X\rangle = \mathbb{Z}\langle x, y, z\rangle$ *in the degree left lexicographical ordering with* $x \succ y \succ z$*. Then both*

$$spoly_2^1(f, g) = 3fzy - 2xyg = 3xzy - 2xyz$$
$$\text{and} \quad gpoly_2^1(f, g) = (-1)fzy + 1xyg = 2xyzy + xyz - xzy$$

do not reduce any further. Thus, they must be added to the Gröbner basis just as any other second type S- and G-polynomial. Finally, the Gröbner basis of $\langle 4xy + x, 6zy + z\rangle$ with respect to classical monomial orderings seem to be infinite, containing several infinite parametrizable series like $\{zy^izy - zy^{i+1}z : i \geq 0\}$.

When the leading coefficients are not coprime, no statement for S- and G-polynomials of the first type can be made. For example, in the case of $f = 4xy + y$, $g = 6yz + y$ we have $spoly_1^{xyz}(f, g) = 3fz - 2xg = 3yz - 2xy$ and $gpoly_1^{xyz}(f, g) = (-1)fz + 1xg = 2xyz - yz + xy$ which do not reduce any further.

The Gröbner basis of $\langle 4xy+y, 6yz+y\rangle$ with respect to classical monomial orderings seem to be infinite as the one above. This time we see infinite parametrizable series like $\{yz^iy - y^2z^i : i \geq 0\}$.

Remark 19.
In the commutative case, according to (Eder et al., 2021), a pair $\{f, g\}$ *with* $\operatorname{lm}(f) = \operatorname{lm}(g)$ *can be replaced by the new pair* $\{spoly(f, g), gpoly(f, g)\}$. *Now set* $\operatorname{lm}(f) = \operatorname{lm}(g) =: t$, *then in the definition of S- and G-polynomials of the first type we have* $\tau_f = \tau_g = 1 \otimes 1$ *and therefore* $spoly_1^t(f, g) = a_f f - a_g g$ *and* $gpoly_1^t(f, g) = b_f f + b_g g$. *This yields a linear equation*

$$\begin{pmatrix} spoly_1^t(f, g) \\ gpoly_1^t(f, g) \end{pmatrix} = \begin{pmatrix} a_f & -a_g \\ b_f & b_g \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix},$$

where the defining matrix has determinant $a_f b_g + a_g b_f = 1$, *thus it is invertible over* $\mathcal{R}$! *Hence, we can recover* f *and* g *back from their S- and G- polynomials and replace them. The importance of this statement was discussed for the commutative case in (Eder et al., 2021) and its effectiveness translates equivalently to the non-commutative one.*

The following two lemmata are chain criteria, which are based on the idea to have two critical pairs and derive a third one from them under certain conditions. The commutative versions for both criteria were proven in (Eder et al., 2021).

Lemma 20. *(Buchberger's S-chain criterion (Eder et al., 2021; Lichtblau, 2012))*
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ *and* $f, g, h \in \mathcal{G}$. *For* $p, q \in \{f, g, h\}$ *let* $\operatorname{LCM}(\operatorname{lm}(p), \operatorname{lm}(q)) \neq \emptyset$ *and fix* $T_{pq} \in \operatorname{LCM}(\operatorname{lm}(p), \operatorname{lm}(q))$ *and choose* $\tau_{pq} \in \mathcal{B}^e$ *with* $\tau_{pq} \operatorname{lm}(p) = T_{pq}$. *There exist* $\tau_{qp} \in \mathcal{B}^e$, *such that* $\tau_{qp} \operatorname{lm}(q) = T_{pq}$. *Assume* $T_{pq} = T_{qp}$ *and let*

1. $T_{hg} = T_{gh}$ *be divisible by both* T_{hf} *and* T_{gf} *with* $\delta_{gf} T_{hf} = T_{hg}$ *and* $\delta_{hf} T_{gf} = T_{gh}$ *for some* $\delta_{gf}, \delta_{hf} \in \mathcal{B}^e$,
2. $\operatorname{lc}(f) \mid \operatorname{lcm}(\operatorname{lc}(g), \operatorname{lc}(h))$ *over* $\mathcal{R}$ *and*
3. $spoly_1^{T_{fg}}(f, g)$ *and* $spoly_1^{T_{fh}}(f, h)$ *both have strong Gröbner representations w.r.t.* $\mathcal{G}$.

Then $spoly_1^{T_{gh}}(f, g)$ *has a strong Gröbner representation w.r.t.* $\mathcal{G}$.

Proof. Let $c_{pq} := \dfrac{\operatorname{lcm}(\operatorname{lc}(p), \operatorname{lc}(q))}{\operatorname{lc}(p)}$ for $p, q \in \{f, g, h\}$. Then one can check, that

$$\begin{aligned} &\frac{c_{hg}}{c_{hf}} \delta_{gf} \operatorname{spoly}_1^{T_{fh}}(f, h) - \frac{c_{gh}}{c_{gf}} \delta_{hf} \operatorname{spoly}_1^{T_{fg}}(f, g) \\ =&c_{gh} \delta_{hf} \tau_{gf} g - c_{hg} \delta_{gf} \tau_{hf} h + \left(\frac{c_{hg} c_{fh}}{c_{hf}} \delta_{gf} \tau_{fh} - \frac{c_{gh} c_{fg}}{c_{gf}} \delta_{hf} \tau_{fg} \right) f. \end{aligned}$$

Using relations for the monomial expressions τ_{pq}, T_{pq}, δ_{pq} and the coefficients c_{pq}, we see that the first term on the right hand side is equal to $\operatorname{spoly}_1^{T_{gh}}(g, h)$ and we obtain

$$\operatorname{spoly}_1^{T_{gh}}(g, h) = \frac{c_{hg}}{c_{hf}} \delta_{gf} \operatorname{spoly}_1^{T_{fh}}(f, h) - \frac{c_{gh}}{c_{gf}} \delta_{hf} \operatorname{spoly}_1^{T_{fg}}(f, g),$$

which shows that $\operatorname{spoly}_1^{T_{gh}}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$. This works analogously for second type S-polynomials $\operatorname{spoly}_2^{w}(g, h)$ or $\operatorname{spoly}_2^{\tilde{w}}(h, g)$, if we choose w or $\tilde{w}$, such that either $\operatorname{lm}(g) w \operatorname{lm}(h) = T_{gh}$ or $\operatorname{lm}(h) \tilde{w} \operatorname{lm}(g) = T_{hg}$. □

We give a similar criterion for G-polynomials.

Lemma 21. *(Buchberger's G-chain criterion, cf. (Eder et al., 2021; Lichtblau, 2012))*
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and $f, g, h \in \mathcal{G}$. We keep the notations T_{pq} and τ_{pq} from Lemma 20. Let

1. *$T_{hg} = T_{gh}$ be divisible by both T_{hf} and T_{gf} with $\delta_{gf} T_{hf} = T_{hg}$ and $\delta_{hf} T_{gf} = T_{gh}$ for some $\delta_{gf}, \delta_{hf} \in \mathcal{B}^e$ and*
2. *$\operatorname{lc}(f) \mid gcd(\operatorname{lc}(g), \operatorname{lc}(g))$ with $d := \dfrac{gcd(\operatorname{lc}(g), \operatorname{lc}(g))}{\operatorname{lc}(f)}$.*

Then $\operatorname{gpoly}_1^{T_{gh}}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$.

Proof. First we observe, that

$$\begin{aligned}
&\operatorname{gpoly}_1^{T_{gh}}(g, h) = \operatorname{gcd}(\operatorname{lc}(g), \operatorname{lc}(h)) T_{gh} + b_g \tau_{gh} \operatorname{tail}(g) + b_h \tau_{hg} \operatorname{tail}(h),\\
&\operatorname{spoly}_1^{T_{fg}}(f, g) = \frac{\operatorname{lc}(g)}{\operatorname{lc}(f)} \tau_{fg} f - \tau_{gf} g = \frac{\operatorname{lc}(g)}{\operatorname{lc}(f)} \tau_{fg} \operatorname{tail}(f) - \tau_{gf} \operatorname{tail}(g)\\
\text{and}\quad &\operatorname{spoly}_1^{T_{fh}}(f, h) = \frac{\operatorname{lc}(h)}{\operatorname{lc}(f)} \tau_{fh} f - \tau_{hf} h = \frac{\operatorname{lc}(h)}{\operatorname{lc}(f)} \tau_{fh} \operatorname{tail}(f) - \tau_{hf} \operatorname{tail}(h).
\end{aligned}$$

Since T_{fh} divides T_{gh}, there exists a $w \in \mathcal{B}^e$ with $w \operatorname{lm}(f) = T_{gh}$ and

$$w \operatorname{lm}(f) = T_{gh} = \delta_{gf} T_{fh} = \delta_{gf} T_{fh} \operatorname{lm}(f).$$

Hence, $w = \delta_{gf} \tau_{fh}$ and analogously $w = \delta_{hf} \tau_{fg}$. Moreover, $dw \operatorname{lc}(f) \operatorname{lm}(f) = \operatorname{gcd}(\operatorname{lc}(g), \operatorname{lc}(h)) T_{gh}$ and finally we obtain

$$\begin{aligned}
&\operatorname{gpoly}_1^{T_{gh}} - dwf + b_g \delta_{hf} \operatorname{spoly}_1^{T_{fg}} + b_h \delta_{gf} \operatorname{spoly}_1^{T_{fh}}\\
&= \operatorname{gcd}(\operatorname{lc}(g), \operatorname{lc}(h)) T_{gh} - (\operatorname{gcd}(\operatorname{lc}(g), \operatorname{lc}(h)) T_{gh} + dw \operatorname{tail}(f))\\
&\quad + b_g \tau_{gh} \operatorname{tail}(g) + b_g \delta_{hf} \left(\frac{\operatorname{lc}(g)}{\operatorname{lc}(f)} \tau_{fg} \operatorname{tail}(f) - \tau_{gf} \operatorname{tail}(g) \right)\\
&\quad + b_h \tau_{hg} \operatorname{tail}(h) + b_h \delta_{gf} \left(\frac{\operatorname{lc}(h)}{\operatorname{lc}(f)} \tau_{fh} \operatorname{tail}(f) - \tau_{hf} \operatorname{tail}(h) \right)\\
&= b_g \tau_{gh} \operatorname{tail}(g) + b_h \tau_{hg} \operatorname{tail}(h) - dw \operatorname{tail}(f) + b_g \frac{\operatorname{lc}(g)}{\operatorname{lc}(f)} \delta_{hf} \tau_{fg} \operatorname{tail}(f)\\
&\quad - b_g \underbrace{\delta_{hf} \tau_{gf}}_{=\tau_{gh}} \operatorname{tail}(g) + b_h \frac{\operatorname{lc}(h)}{\operatorname{lc}(f)} \underbrace{\delta_{gf} \tau_{fh}}_{=\delta_{hf} \tau_{fg}} \operatorname{tail}(f) - b_h \underbrace{\delta_{gf} \tau_{hf}}_{=\tau_{hg}} \operatorname{tail}(h)\\
&= \left(\frac{b_g \operatorname{lc}(g) + \operatorname{lc}(h)}{\operatorname{lc}(f)} \delta_{hf} \tau_{fg} - dw \right) \operatorname{tail}(f) = d(\delta_{hf} \tau_{fg} - w) \operatorname{tail}(f) = 0.
\end{aligned}$$

Finally, we can write $\operatorname{gpoly}_1^{T_{gh}}$ as

$$\operatorname{gpoly}_1^{T_{gh}} = dwf - b_g \delta_{hf} \operatorname{spoly}_1^{T_{fg}} - b_h \delta_{gf} \operatorname{spoly}_1^{T_{fh}},$$

which is a strong Gröbner representation. □

We conclude, that the well-known criteria for S- and G-polynomials from the commutative case can also be applied in the non-commutative case with modifications, if we distinguish between first and second type S- and G-polynomials. Computations show how hard these requirements are to be satisfied compared to the commutative case by specifically counting the number of applications of product and chain criteria.

5. Examples

We give examples for Gröbner bases that have been computed up to a certain length bound over the integers. These examples also show that although computing over $\mathbb{Z}$ delivers infinite results much more often than when computing over fields, non-commutative Gröbner bases over $\mathbb{Z}$ can be finite as well.

We start with the examples from (Apel, 2000) until Example 24. Let $\mathcal{P} = \mathbb{Z}\langle x, y, z\rangle$ with the degree left lexicographical ordering and $x \succ y \succ z$ (if not indicated otherwise).

Example 22.
We consider the ideal $\mathcal{I} = \langle f_1 = yx - 3xy - 3z,\ f_2 = zx - 2xz + y,\ f_3 = zy - yz - x\rangle \subset \mathcal{P}$. *We investigated it over* $\mathbb{Q}\langle x, y, z\rangle$ *in (Levandovskyy et al., 2020d) where we also comment in details on syntax and commands of* Singular:Letterplace.
At first, we analyze this ideal over the field $\mathbb{Q}$*:*

```
LIB "freegb.lib"; // initialization of free algebras
ring r = 0,(z,y,x),Dp; // degree left lex ord on z>y>x
ring R = freeAlgebra(r,7); // length bound is 7
ideal I = y*x - 3*x*y - 3*z, z*x - 2*x*z +y, z*y-y*z-x;
option(redSB); option(redTail); // for minimal reduced GB
option(intStrategy); // avoid divisions by coefficients
ideal J = twostd(I); // compute a two-sided GB of I
J; // prints generators of J
```

The output is a finite Gröbner basis

$$\left\{4xy + 3z,\ 3xz - y,\ 4yx - 3z,\ 2y^2 - 3x^2,\ 2yz + x, 3zx + y, 2zy - x,\ 3z^2 - 2x^2,\ 4x^3 + x\right\}.$$

As we see, original generators have decomposed. In order to compute their expressions in the Gröbner basis above, one can use the `lift` *command. In particular*

$$yx - 3xy - 3z = -\frac{3}{4}(4xy + 3z) + \frac{1}{4}(4yx - 3z).$$

Now, it seems from the form of leading monomials, that $\mathbb{Q}\langle x, y, z\rangle/J$ *is finite dimensional vector space. Let us check it:*

```
LIB "fpadim.lib"; // load the library for K-dimensions
lpMonomialBasis(7,0,J); // compute all monomials
// of length up to 7 in Q<x,y,z>/J
```

which results in $\left\{1, z, y, x, x^2\right\}$.

```
LIB "freegb.lib"; //initialization of free algebras
ring r = integer,(z,y,x),Dp; //degree left lex ord z>y>x
ring R = freeAlgebra(r,7); // length bound is 7
ideal I = y*x - 3*x*y - 3*z, z*x - 2*x*z +y, z*y-y*z-x;
option(redSB); // Groebner basis will be minimal
option(redTail); // Groebner basis will be tail-reduced
ideal J = twostd(I); // compute a two-sided GB of I
J; // print generators of J
```

The output has plenty of elements in each degree (which is the same as length because of the degree ordering), what hints at potentially infinite Gröbner basis (what we confirm below) and the elements, which can be subsequently constructed, are

$$\begin{aligned}
&\{f_1,\ f_2,\ f_3,\ 12xy + 9z,\ 9xz - 3y,\ 6y^2 - 9x^2,\ 6yz + 3x,\\
&3z^2 + 2y^2 - 5x^2,\ 6x^3 - 3yz,\ 4x^2y + 3xz,\ 3x^2z + 3xy + 3z,\\
&2xy^2 + 3x^3 + 3yz + 3x,\ 3xyz + 3y^2 - 3x^2,\ 2y^3 + x^2y + 3xz,\\
&2x^4 + y^2 - x^2,\ 2x^3y + 3y^2z + 3xy + 3z,\ x^2yz + xy^2 - x^3,\\
&xy^2z - y^3 + x^2y,\ x^5 - y^3z - xy^2 + x^3,\ y^3z^2 - x^4y,\\
&x^4z + x^3y + 2y^2z + x^2z + 3xy + 3z,\ xy^3z - y^4 + x^4 - y^2 + x^2,\\
&xy^4z - y^5 + x^2y^3,\ xy^5z - y^6 + x^4y^2 + y^4 + x^4 + 2y^2 - 2x^2\}
\end{aligned}$$

Indeed, we can show that $\mathcal{I}$ contains an element with the leading monomial xy^iz for all $i \geq 2$. Therefore this Gröbner basis is infinite, but can be presented in finite terms. Note, that the original generators have been preserved in a Gröbner basis, while over $\mathbb{Q}$ (see (Levandovskyy et al., 2020d)) they were decomposed. Also, over $\mathbb{Q}$ the input ideal has a finite Gröbner basis of degree at most 3.

Example 23.
Let $\mathcal{I} = \langle f_1 = yx - 3xy - z,\ f_2 = zx - xz + y,\ f_3 = zy - yz - x\rangle \subset \mathcal{P}$. Then $\mathcal{I}$ has a finite strong Gröbner basis, namely

$$\left\{f_1,\ f_2,\ f_3,\ 8xy + 2z,\ 4xz - 2y,\ 4yz + 2x, 2x^2 - 2y^2,\ 4y^2 - 2z^2,\ 2z^3 - 2xy\right\}.$$

As we can see, the leading coefficients of the Gröbner basis above might vanish, if we pass to the field of characteristic 2. Therefore the bimodule $M := \mathbb{Z}\langle x, y, z\rangle/I$ might have nontrivial 2-torsion, i.e. there is a nonzero submodule $T_2(M) := \{p \in M : \exists n \in \mathbb{N}_0\ 2^n \cdot p \in I\}$. By adopting the classical method of Caboara and Traverso for computing colon (or quotient) ideals to our situation, where we use the fact that the ground ring is central (i.e. commutes with all variables), we do the following:

```
LIB "freegb.lib"; //we will use position-over-term order
ring r = integer,(x,y,z),(c,dp);
ring R = freeAlgebra(r,7,2); // 2==number of components
ideal I = y*x - 3*x*y - z, z*x - x*z +y, z*y-y*z-x;
option(redSB); option(redTail);
ideal J = twostd(I);    module N;
N = 2*ncgen(1)*gen(1)+ncgen(2)*gen(2),J*ncgen(1)*gen(1);
module SN = twostd(N);   SN;
```

Above, `gen(i)` *stands for the i-th canonical basis vector (commuting with everything) and* `ncgen(i)` *- for the i-th canonical generator of the free bimodule, which commutes only with constants. The output, which is a list of vectors, looks as follows:*

```
...
SN[9]=[0,z*z*z*ncgen(2)-x*y*ncgen(2)]
SN[10]=[2*ncgen(1),ncgen(2)]
SN[11]=[z*y*ncgen(1)-y*z*ncgen(1)-x*ncgen(1)]
...
```

From this output we gather all vectors with 0 in the first component `ncgen(1)*gen(1)`*, and form an ideal, whose Gröbner basis is*

$$\left\{ zy - yz - x,\ zx - xz + y,\ yx + xy,\ 2yz + x, 2xz - y,\ 2y^2 - z^2,\ 4xy + z,\ x^2 - y^2,\ z^3 - xy \right\}.$$

Another colon computation does not change this ideal, therefore it is the saturation ideal of I at 2, denoted by $L = I : 2^\infty \subset \mathbb{Z}\langle x, y, z\rangle$. It is the presentation for the 2-torsion submodule $T_2(M) = \mathbb{Z}\langle x, y, z\rangle L/I$ and, moreover, $2 \cdot L \subset I \subset L$ holds.

Example 24.
In this example we have to run a Gröbner basis of $\langle f_1 = zy - yz + z^2,\ f_2 = zx + y^2,\ f_3 = yx - 3xy\rangle$ up to length bound 11*. We use degree right lexicographical ordering and obtain a finite Gröbner basis*

$$\begin{aligned}
&\{zy - yz + z^2,\ zx + y^2,\ yx - 3xy,\ 2y^3 + y^2z - 2yz^2 + 2z^3,\ y^2z^2 - 4yz^3 + 6z^4,\\
&y^4 + 27xy^2z - 54xyz^2 + 54xz^3,\ 54xy^2z - y^3z - 108xyz^2 + 108xz^3 + 62yz^3 - 124z^4,\\
&14z^5,\ 14yz^3 - 28z^4,\ 2yz^4 - 6z^5,\ 2xyz^3 - 4xz^4,\ xy^3z,\ 2z^6,\ 2xz^5\}.
\end{aligned}$$

As we can see from the leading terms, the corresponding module might have 2*- and* 7*-torsion submodules. There have been* 17068 *critical pairs created, and internal total length of intermediate elements was* 11*. The product criterion has been used* 196 *times, while the chain criterion was invoked* 36711 *times. Totally, up to* 2.9 *GB of memory was allocated.*

Comparing the data with increasing the length bound to the presumably unlucky 13, we had to create over 135300 *critical pairs, while the product criterion has been used* 1876 *and the chain criterion* 365367 *times. This illustrates the explosive behaviour of the number of critical pairs when dealing with rings as coefficients.*

In the contrast, the Gröbner basis computation of the same input over $\mathbb{Q}$ considered only 14 *critical pairs, went up to total degree* 6 *of intermediate elements, used no product criterion and* 9 *times the chain criterion with less than* 1 *MB of memory. The result is*

$$\begin{aligned}
&\{zy - yz + z^2,\ zx + y^2,\ yx - 3xy,\ 2y^3 + y^2z - 2yz^2 + 2z^3,\\
&y^2z^2 - 2z^4,\ xy^2z - 2xyz^2 + 2xz^3,\ yz^3 - 2z^4, z^5\}.
\end{aligned}$$

This demonstrates once again, how technically involved computations with free algebras over rings as coefficients are.

Example 25.
The important class of Iwahori-Hecke algebras (Humphreys, 1990) is associated to Coxeter

groups and are constructed by means of finite presentation over $\mathbb{Z}[q,q^{-1}]$ *where* q *will later be specialized, most frequently to the root of unity over a finite field. Consider the Iwahori-Hecke algebra of type* A_3*, then the presentation is as follows:*

$$\mathbb{Z}[q,q^{-1}]\langle x,y,z\rangle/\langle x^2+(1-q)x-q, y^2+(1-q)y-q, z^2+(1-q)z-q, zx-xz, yxy-xyx, zyz-yzy\rangle,$$

where we observe **braid** *relations between* x,y *and* y,z*. In order to treat the ground ring* $\mathbb{Z}[q,q^{-1}]$ *appropriately, we do the following:*

- *introduce two free variables* `q, iq` *with the latter standing for* q^{-1}*,*
- *use a block ordering for the variables, giving eliminating preference to the block* x,y,z*,*
- *to the ideal of relations above we insert new commutation relations (*`q, iq` *mutually commute with* `x,y,z`*) and reciprocity relations.*

```
LIB "freegb.lib";
ring r = integer,(x,y,z,iq,q),(a(1,1,1,0,0),Dp);
ring R = freeAlgebra(r,7);
ideal I = x^2 + (1-q)*x - q, y^2 + (1-q)*y - q, z^2 + (1-q)*z - q,
z*x - x*z, y*x*y - x*y*x, z*y*z - y*z*y,
bracket(q,x), bracket(q,y), bracket(q,z),
bracket(iq,x), bracket(iq,y), bracket(iq,z), q*iq -1, iq*q-1;
option(redSB); option(redTail);
ideal J = twostd(I);
```

The resulting Gröbner basis is finite, and has only one new generator $xyzx-yxyz$ *of degree* 4*. We also observe, that no integers, other than* ± 1*, appear among the coefficients from* $\mathbb{Z}$*. Now we specialize* q *to the primitive third root of unity.*

```
ideal L = J, q^2+q+1;
L = twostd(L);
```

In the output we see the relation $iq+q+1=0$*, which has been used to replace* `iq`*. Since except for the minimal polynomial* q^2+q+1 *and commutativity relations, no* q *appear as leading coefficients, we can proceed to the ground field* $\mathbb{K}:=\mathbb{Q}[q]/\langle q^2+q+1\rangle$*. One of the possibilities to do this is the localization at* $\mathbb{Z}\setminus\{0\}$*. Now, with the abilities of* Letterplace *over fields we easily establish, that specialized over* $\mathbb{K}$*, the Iwahori-Hecke algebra of type* A_3 *is finite-dimensional of dimension 24. Hence further computations with modules over this algebra can be carried on.*

Example 26.
Over $K[X]$*, an ideal is called* ***binomial****, if it is generated by polynomials of length at most two. A distinct property of binomial ideals, which is easy to prove, is that with respect to any monomial ordering, a binomial ideal possesses a Gröbner basis, consisting of binomials. This is not true over rings anymore, as, for instance, a Gröbner basis with respect to the degree reverse lexicographical ordering of* $\{2x-3y, xy-3x\}$ *is* $\{2x-3y, 3y^2-9y, xy+x-6y\}$*.*
In the setting of a free algebra, the binomiality of a Gröbner basis still holds over $K\langle X\rangle$*. As expected, it breaks over rings since in the very same example the commutativity relation* $yx-xy$ *is a binomial. Hence, a strong minimal Gröbner basis of* $\{2x-3y, xy-3x, yx-xy\}\subset\mathbb{Z}\langle x,y\rangle$ *is*

$$\left\{2x-3y, 3y^2-9y, xy+x-6y, yx+x-6y\right\},$$

which cannot be made binomial.

6. Implementation

We have created a powerful implementation called LETTERPLACE (Levandovskyy et al., 2020a,d,c) in the framework of SINGULAR (Decker et al., 2020). Its' extension to coefficient rings like $\mathbb{Z}$ addresses the following functions with the current release for ideals and subbimodules of a free bimodule with finite rank. We provide a vast family of orderings on monoids and modules including three kinds of orderings, which eliminate variables or free bimodule components.

- `twostd`: a two-sided Gröbner basis; when executed with respect to an elimination ordering, it allows to eliminate variables (Borges and Borges, 1998), and thus to compute kernels of ring morphisms and preimages of ideals under such morphisms;
- `reduce (NF)`: a normal form of a vector or a polynomial with respect to a two-sided Gröbner basis;
- `syz`: a generating set of a syzygy bimodule (Bluhm and Kreuzer, 2007) of an input;
- `modulo`: kernel of a bimodule homomorphism;
- `lift`: computation of a transformation matrix between a module and its submodule, in other words expressing generators of a submodule in terms of generators of a module;
- `liftstd`: computation of a two-sided Gröbner basis and a transformation matrix of a given ideal or subbimodule and, optionally, a syzygy bimodule.

Caveats: As every software, which is intensively used, our implementation has some artefacts, which we cannot overcome and therefore describe as caveats.

a) Computing with the options `redSB` and `redTail` enabled, sometimes the resulting Gröbner basis will not be minimal. This occurs only with rings as coefficients and cannot be changed at this time. Computing a Gröbner basis of the result one more time produces a minimal Gröbner basis.

b) A computation, involving Gröbner bases, might stop with the following error message:

```
? degree bound of Letterplace ring is 9, but at least
10 is needed for this multiplication
```

This is not a bug or an error. It indicates that internally a potentially non-Noetherian reduction has been invoked, what often happens for monomial orderings, which are not compatible with the length of monomials. We recommend to increase the length bound on the ring, and keep polynomials or vectors tail-reduced.

c) In Example 23 a built-in command `modulo` can be used instead of the construction of the module `SN` and gathering the vectors from the first component. However, because of the multiplication bound as in b), encountered internally, `modulo` is not coming to a result even after increasing the length bound to high values. Therefore in such cases the explicit construction, like the one of the module `SN` in Example 23 will lead to the result.

7. Conclusion and Future Work

Following Mora's "manual for creating own Gröbner basis theory" (Mora, 2016), we have considered the case of free non-commutative Gröbner bases for ideals and bimodules over $\mathbb{Z}\langle X\rangle$. We have derived novel information on the building critical pairs and on criteria to discard them when possible. Armed with this theoretical and algorithmic knowledge, we have created an implementation in a SINGULAR subsystem LETTERPLACE, which offers a rich functionality at a decent speed. We are not aware of yet other systems or packages, which can do such computations.

In this paper we have demonstrated several important applications of our algorithms and their implementation, in particular the determination of torsion submodules with respect to natural numbers, and operations with Iwahori-Hecke algebras.

A further extension of our implementation to the explicitly given $\mathbb{Z}/m\mathbb{Z}$ is planned, along the lines, discussesd in Section 3. Also, we plan to develop (in theory and in practice) one-sided Gröbner bases in factor algebras (over fields, LETTERPLACE already offers `rightStd` and more functions are under development). More functions for dealing with matrices and one-sided modules will make possible the usage of our implementation as a backend from the system HOMALG (Barakat et al., 2019). This system performs homological algebra computations within computable Abelian categories and uses other computer algebra systems as backends for concrete calculations with matrices over rings. Other existing systems like SAGEMATH (Stein et al., 2020) and OSCAR (The OSCAR Team, 2020) can use our implementation as backend, since they have a low-level communication with SINGULAR.

8. Acknowledgements

The authors are grateful to Hans Schönemann, Gerhard Pfister (Kaiserslautern), Anne Frühbis-Krüger (Oldenburg), Leonard Schmitz, Eva Zerz (RWTH Aachen) and Evelyne Hubert (INRIA Méditerranée) for fruitful discussions. The critics and suggestions of anonymous referees helped to enhance the exposition of the results.

The first and third authors (V. Levandovskyy and K. Abou Zeid) have been supported by Project II.6 of SFB-TRR 195 "Symbolic Tools in Mathematics and their Applications" of the German Research Foundation (DFG).

The work of the second author (T. Metzlaff) has been supported by European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Actions, grant agreement 813211 (POEMA).

References

Apel, J., 2000. Computational ideal theory in finitely generated extension rings. Theor. Comput. Sci. 244, 1–33.

Apel, J., Klaus, U., 1991. *FELIX* – an assistant for algebraists, in: Proc. ISSAC'91, ACM Press. pp. 382–389. See also http://felix.hgb-leipzig.de.

Barakat, M., Gutsche, S., Lange-Hegermann, M., 2019. homalg - a homological algebra meta-package for computable Abelian categories. https://homalg-project.github.io/homalg_project/homalg/.

Bell, J.P., Heinle, A., Levandovskyy, V., 2016. On noncommutative finite factorization domains. Trans. Amer. Math. Soc. 369, 2675–2695.

Bergman, G.M., 1977. The diamond lemma for ring theory. Adv. Math. 29, 178–218. doi:10.1016/0001-8708(78)90010-5.

Bluhm, H., Kreuzer, M., 2007. Computation of two-sided syzygies over non-commutative rings. Contemp. Math. , 45–64.

Borges, M.A., Borges, M., 1998. Gröbner bases property on elimination ideal in the noncommutative case, in: Buchberger, B., Winkler, F. (Eds.), Gröbner bases and applications, Cambridge University Press. pp. 323–337.
Decker, W., Greuel, G.M., Pfister, G., Schönemann, H., 2020. SINGULAR 4-1-3 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de.
Eder, C., Hofmann, T., 2019. Efficient Gröbner bases computation over principal ideal rings. Journal of Symbolic Computation 103, 1 – 13. doi:10.1016/j.jsc.2019.10.020.
Eder, C., Pfister, G., Popescu, A., 2016. New strategies for standard bases over $\mathbb{Z}$. https://arxiv.org/abs/1609.04257.
Eder, C., Pfister, G., Popescu, A., 2021. Standard bases over Euclidean domains. Journal of Symbolic Computation 102, 21 – 36. doi:10.1016/j.jsc.2019.10.007.
Humphreys, J.E., 1990. Reflection Groups and Coxeter Groups. Cambridge University Press.
Kredel, H., 2015. Parametric solvable polynomial rings and applications, in: Gerdt, V.P., Koepf, W., Seiler, W.M., Vorozhtsov, E.V. (Eds.), Proc. CASC'15, Springer Cham. pp. 275–291. URL: http://dx.doi.org/10.1007/978-3-319-24021-3_21.
Kredel, H., 2020. Java computer algebra system (jas). http://krum.rz.uni-mannheim.de/jas.
La Scala, R., 2014. Extended letterplace correspondence for nongraded noncommutative ideals and related algorithms. Int. J. Algebra Comput. 24, 1157–1182.
La Scala, R., Levandovskyy, V., 2009. Letterplace ideals and non-commutative Gröbner bases. Journal of Symbolic Computation 44, 1374–1393. doi:10.1016/j.jsc.2009.03.002.
La Scala, R., Levandovskyy, V., 2013. Skew polynomial rings, Gröbner bases and the letterplace embedding of the free associative algebra. Journal of Symbolic Computation 48, 110–131. URL: http://dx.doi.org/10.1016/j.jsc.2012.05.003.
Levandovskyy, V., 2005. Non–commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation. http://kluedo.ub.uni-kl.de/volltexte/2005/1883/.
Levandovskyy, V., Abou Zeid, K., Schönemann, H., 2020a. SINGULAR:LETTERPLACE — A SINGULAR 4-1 subsystem for non-commutative finitely presented algebras. http://www.singular.uni-kl.de.
Levandovskyy, V., Metzlaff, T., Abou Zeid, K., 2020b. Computations of free non-commutative Gröbner bases over $\mathbb{Z}$ with SINGULAR:LETTERPLACE, in: Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'20), ACM Press. pp. 312–319.
Levandovskyy, V., Schönemann, H., Abou Zeid, K., 2020c. LETTERPLACE — a subsystem of SINGULAR for computations with finitely presented associative algebras. Submitted.
Levandovskyy, V., Schönemann, H., Abou Zeid, K., 2020d. LETTERPLACE — a subsystem of SINGULAR for computations with free algebras via letterplace embedding, in: Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'20), ACM Press. pp. 305–311.
Levandovskyy, V., Studzinski, G., Schnitzler, B., 2013. Enhanced computations of Gröbner bases in free algebras as a new application of the Letterplace paradigm, in: Kauers, M. (Ed.), Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'13), ACM Press. pp. 259 – 266.
Li, H., 2012. Algebras defined by monic Gröbner bases over rings. International Mathematical Forum 7, 1427–1450.
Lichtblau, D., 2012. Effective computation of strong Gröbner bases over Euclidean domains. Illinois Journal of Mathematics 56, 177–194.
Markwig, T., Ren, Y., Wienand, O., 2015. Standard bases in mixed power series and polynomial rings over rings. Journal of Symbolic Computation 79. doi:10.1016/j.jsc.2016.08.009.
Mora, T., 2016. Solving Polynomial Equation Systems IV: Volume 4, Buchberger Theory and Beyond. 1st ed., Cambridge University Press.
Pauer, F., 2007. Gröbner bases with coefficients in rings. Journal of Symbolic Computation 42, 1003 – 1011. doi:10.1016/j.jsc.2007.06.006.
Pritchard, F.L., 1996. The ideal membership problem in non-commutative polynomial rings. J. Symb. Comput. 22, 27–48. doi:10.1006/jsco.1996.0040.
Stein, W., et al., 2020. Sage Mathematics Software. The Sage Development Team.
The OSCAR Team, 2020. The OSCAR project. https://oscar.computeralgebra.de.