Computation of free non-commutative Gröbner Bases over Z with Singular:Letterplace

Viktor Levandovskyy, Tobias Metzlaff, Karim Abou Zeid

Computation of Free Non-commutative Gröbner Bases over $\mathbb{Z}$ with Singular:Letterplace

Viktor Levandovskyy
Lehrstuhl D für Mathematik, RWTH Aachen University
Aachen, Germany
Viktor.Levandovskyy@math.rwth-aachen.de

Tobias Metzlaff
AROMATH, INRIA Méditerranée
Université Côte d'Azur
Sophia Antipolis, France
tobias.metzlaff@inria.fr

Karim Abou Zeid
Lehrstuhl D für Mathematik, RWTH Aachen University
Aachen, Germany
karim.abou.zeid@rwth-aachen.de

ABSTRACT

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 formation of critical pairs has to be reengineered, together with 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 accompany our presentation.

CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**; **Special-purpose algebraic systems**.

KEYWORDS

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

ACM Reference Format:
Viktor Levandovskyy, Tobias Metzlaff, and Karim Abou Zeid. 2020. Computation of Free Non-commutative Gröbner Bases over $\mathbb{Z}$ with Singular:Letterplace. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '20), July 20–23, 2020, Kalamata, Greece.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3373207.3404052

ISSAC '20, July 20–23, 2020, Kalamata, Greece

ACM ISBN 978-1-4503-7100-1/20/07…$15.00
https://doi.org/10.1145/3373207.3404052

INTRODUCTION

In the recent years a somewhat strange attitude has established itself around Gröbner bases: non-commutative generalizations of various concepts, related to algorithms and, in particular, Gröbner bases, are often met with sceptical expressions like "as expected", "straightforward", "more or less clear" and so on. This is not true in general for generalizations to various flavours of non-commutativity require deep analysis of procedures (algorithms) based on very good knowledge of properties of rings and modules over them. Characteristically, in this paper we demonstrate in e.g. Example 2.4 and 2.5 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: the same set $\{2x, 3y\}$ delivers a finite strong Gröbner basis $\{3x, 3y, yx, xy\}$ over $\mathbb{Z}\langle x, y\rangle$ and an infinite Gröbner basis over $\mathbb{Z}\langle x, y, z_1, \ldots, z_m\rangle$ for any $m \geq 1$, containing e.g. $xz_i^k y, yz_i^k x$ for any natural k.

In his recent articles and in the book [21] 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. The theory of non-commutative Gröbner bases was developed by many prominent scientists since the Diamond Lemma of G. Bergman [4]. Especially L. Pritchard [23] 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 [10]. In our attempts we balance the generality with the performance; based on Singular, we utilize its' long and successful 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. [7–9, 19]. 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. In the system Felix by Apel et al. [2], such computations were experimentally available, though not documented. In his paper [1], 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* [11–13, 17], 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 fix 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 choice of pairs, which we will discuss in the third chapter. This is followed up by computational examples 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.

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 [8, 9, 19, 20], are divisibility conditions of type $\mathrm{lm}(f) \mid \mathrm{lm}(g)$.

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 shortly "$\mathcal{B}$ 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 $\mathcal{B}^e = \{u \otimes v \mid u, v \in \mathcal{B}\}$. 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*.

[1] This concept can be extended to principal ideal rings. It was done in [7] for the commutative case with so-called annihilator polynomials.

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* $\mathrm{lc}(f) \in \mathcal{R} \setminus \{0\}$, 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* $\mathrm{L}(\mathcal{G}) = \langle \mathrm{lt}(f) \mid f \in \mathcal{G} \setminus \{0\}\rangle$.

Naturally, the notions of coefficient, monomial and term carry over to an element $h \in \mathcal{P}^e$ by considering $h1 \in \mathcal{P}$.

Definition 1.1. 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 in the first two cases $|t_1| < |v|$ and $|t_2| < |u|$. In the third, respectively fourth case, 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 $\mathrm{lcm}(u, v) = \emptyset$.

If $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$ for $f, g \in \mathcal{P}$, then $\mathrm{lm}(g) \preceq \mathrm{lm}(f)$ holds.

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 we will recall subsequently, and for any $f \in \mathcal{I} \setminus \{0\}$ the existence of an element $g \in \mathcal{G}$, such that $\mathrm{lt}(g)$ divides $\mathrm{lt}(f)$.

Definition 2.1. Let $f, g \in \mathcal{P} \setminus \{0\}$, $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ be a countable set and $\mathcal{I} \subseteq \mathcal{P}$ be an ideal. Fix a monomial well-ordering $\preceq$.

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 $m \in \mathbb{N}$, $g_i \in \mathcal{G}$, $h_i \in \mathcal{P}^e$ 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 $i \neq j$ where $h_i \neq 0$.

$\mathcal{G}$ 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 $\mathrm{lt}(f')$.

Those lm-reductions are the key to obtain a remainder after division through a set $\mathcal{G}$ (usually a generating set) and 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, i.e. the remainder of the division, is then known as a *normal form*.

The following strong normal form algorithm uses lm-reductions and can be compared to the normal form algorithms in algebras over fields (cf. [14]).

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 $||b|| <_{\mathrm{E}} ||\,\mathrm{lc}(h)||$
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

A normal form of the zero-polynomial is always unique and zero. Termination and correctness are analogous to the classical proofs.

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 reduction.

We confirm, that the proof of the following theorem carries over verbatim from the commutative case in [19].

Theorem 2.2. *Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and $\{0\} \neq \mathcal{I} \subseteq \mathcal{P}$. Then the following statements with respect to $\mathcal{G}$ and $\preceq$, 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 non-strong Gröbner bases in [23].

Such 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. However, this does not suffice, when leading coefficients are non-invertible.

Definition 2.3. Let $f, g \in \mathcal{P} \setminus \{0\}$. There exist $\tau_f, \tau_g \in \mathcal{B}^e$, 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 sign and so are a_f, a_g. Then a *S-polynomial* of f and g is defined as

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

It is known from the commutative case over rings (e.g. [19]), that it does not suffice to take such S-polynomials to obtain a strong Gröbner basis. Let $\mathcal{I} = \langle f = 3x, g = 2y\rangle$. Then every S-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.

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

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

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

Example 2.4. 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

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

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

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

is also a G-polynomial of f, g for every $w \in \mathcal{B}$ 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 $\mathrm{gpoly}(f, g)$ divides $\mathrm{gpoly}'(f, g)$. Furthermore, in the field case this is also irrelevant, because we do not need G-polynomials.

Example 2.5. A similar problem occurs with S-polynomials. Let $f = 2xy + x$, $g = 3yz + z$. Then $\mathrm{spoly}(f, g) = 3fz - 2xg = xz$ is an S-polynomial of f and g. However, so are all polynomials

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

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

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

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

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

is an S-polynomial of f with itself which does not reduce any further and we need $\mathrm{lm}(f)w\,\mathrm{lm}(f) \in \mathrm{cm}(\mathrm{lm}(f), \mathrm{lm}(f))$, although it is clearly not contained in $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(f))$. So even principal ideals do not have finite strong Gröbner bases in general! Such behavior of S-polynomials does not occur for non-commutative polynomials over fields.

Also, note that we do not consider any further extensions of the leading monomials, meaning that the S- and G-polynomial corresponding to $t \in \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ or $\mathrm{lm}(f)w\,\mathrm{lm}(g)$ make any further (trivial) overlap relations τt or $\tau(\mathrm{lm}(f)w\,\mathrm{lm}(g))$ for $\tau \in \mathcal{B}^e$ redundant. Therefore, in the definition of $\mathrm{lcm}(x, y)$ we attached importance to 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 $\mathrm{cm}(\mathrm{lm}(f), \mathrm{lm}(g))$ contains too many elements that are redundant whereas the set $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ 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 2.6. Let $f, g \in \mathcal{P} \setminus \{0\}$ and $a_f, a_g, b_f, b_g \in \mathcal{R}$ as in 2.3. We distinguish the following two cases.

If $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$ have a non-trivial overlap, then there exist $t \in \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ and $\tau_f, \tau_g \in \mathcal{B}^e$, such that $t = \tau_f \,\mathrm{lm}(f) = \tau_g \,\mathrm{lm}(g)$. 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 $|t_f| < |\mathrm{lm}(g)|$, $|t_g|, |t'_g| < |\mathrm{lm}(f)|$. We define a *first type S-polynomial* of f and g w.r.t. t as

$$\mathrm{spoly}_1^t(f, g) := a_f \tau_f f - a_g \tau_g g$$

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

$$\mathrm{gpoly}_1^t(f, g) := b_f \tau_f f + b_g \tau_g g.$$

If such τ_f, τ_g do not exist then 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 results from $\mathcal{P}$ not being a unique (but merely a finite) factorization domain.

For any $w \in \mathcal{B}$ we define the *second type S-polynomial* of f and g w.r.t. w by

$$\mathrm{spoly}_2^w(f, g) := a_f f w \,\mathrm{lm}(g) - a_g \,\mathrm{lm}(f) w g$$

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

$$\mathrm{gpoly}_2^w(f, g) := b_f f w \,\mathrm{lm}(g) + b_g \,\mathrm{lm}(f) w g.$$

Remark 2.7. 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 2.4 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 2.8 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.

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: G = {f_1, ..., f_k}
02: L = {spoly_1^t(f_i, f_j), gpoly_1^t(f_i, f_j) | ∀ t *, i, j}
03: L = L ∪ {spoly_2^w(f_i, f_j), gpoly_2^w(f_i, f_j) | ∀ w **, i, j}
04: while L ≠ ∅ do
05:     choose h ∈ L
06:     L = L \ {h}
07:     h = NormalForm(h, G)
08:     if h ≠ 0 then
09:         G = G ∪ {h}
10:         for g ∈ G do
11:             L = L ∪ {spoly_1^t(g, h), gpoly_1^t(g, h) | ∀ t *}
                L = L ∪ {spoly_1^t(h, g), gpoly_1^t(h, g) | ∀ t *}
                L = L ∪ {spoly_2^w(g, h), gpoly_2^w(g, h) | ∀ w ***}
                L = L ∪ {spoly_2^w(h, g), gpoly_2^w(h, g) | ∀ w ***}
12:         end do
13:     end if
14: end while
15: return G
```

* $t \in \mathrm{lcm}$, such that $|t| < d$
** $w \in \mathcal{B}$, such that $|\mathrm{lm}(f_i)| + |w| + |\mathrm{lm}(f_j)| < d$
*** $w \in \mathcal{B}$, such that $|\mathrm{lm}(h)| + |w| + |\mathrm{lm}(g)| < d$

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 $t \in \mathrm{cm}(\mathrm{lm}(f), \mathrm{lm}(g))$, such that one of the following four cases

(1) $t = \mathrm{lm}(f) t'_f = t_g \,\mathrm{lm}(g)$ (2) $t = \mathrm{lm}(f) = t_g \,\mathrm{lm}(g) t'_g$
(3) $t = t_f \,\mathrm{lm}(f) = \mathrm{lm}(g) t'_g$ (4) $t = t_f \,\mathrm{lm}(f) t'_f = \mathrm{lm}(g)$

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 [23], that for a generating set of the left syzygy module (which is not finitely generated in general) we may use only minimal syzygies.

Lemma 2.8. *Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$. Then $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I} := \langle \mathcal{G} \rangle$, 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 [19]; we only need to show the "if" part. Let $f \in \mathcal{I} \setminus \{0\}$ with $f = \sum_i h_i g_i$ for some $h_i \in \mathcal{P}^e$. We set $t := \max(\mathrm{lm}(h_i g_i))$ and $M := \{i \in \mathbb{N} \mid \mathrm{lm}(h_i g_i) =$

$t\}$. Clearly $\mathrm{lm}(f) \preceq t$ and we may assume that there is no other representation of f where t is smaller. Without loss of generality let $M = \{1, \ldots, m\}$. Showing, that M contains exactly one element, proves the lemma and can be done by contradiction as follows. We omit the technical details. The setup allows to choose a representation of f, where the coefficient sum $\sum_{i=1}^{m} |\mathrm{lc}(h_i)\,\mathrm{lc}(g_i)|$ is minimal for fixed t. If M contains more than one element, one can consider the first two polynomials in $\mathcal{G}$ (those shall be g_1 and g_2), that occur in the representation of f with $T = \tau_1\,\mathrm{lm}(g_1) = \tau_2\,\mathrm{lm}(g_2)$. Here, $\tau_1,\ \tau_2 \in \mathcal{B}^e$ and T results from one the above four cases (1), ..., (4). By analyzing $\mathrm{spoly}(g_1,\ g_2)$ and $\mathrm{gpoly}(g_1,\ g_2)$ and using the intrinsic properties of the Euclidean domain $\mathcal{R}$, we obtain a representation $h_1g_1 + h_2g_2 = \sum_j h'_j g_j$, which has a smaller coefficient sum than our original representation. This is in contradiction with the choice. □

It is possible to define monic[2] and reduced Gröbner bases [18, 22] 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) $\mathrm{lt}(\mathrm{tail}(g)) \notin \mathrm{L}(\mathcal{G})$ 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 a counterexample in [23].

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 2.9. *Suppose, that $\mathcal{G} \subset R\langle X\rangle$ is a result of a Gröbner basis computation up to a length bound $d \in \mathbb{N}$, and thus finite. $\mathcal{G}$ is a strong Gröbner basis of the ideal it generates, if and only if a Gröbner basis computation up to a length bound $2d-1$ does not change $L(\mathcal{G})$.*

Proof. It suffices to prove the "if" part. Assume that $\mathcal{G}'$ is a result of a computation up to degree $2d-1$ and $\mathrm{L}(\mathcal{G}) = \mathrm{L}(\mathcal{G}')$. This means that all overlap relations of length $2d-1$, which are precisely the non-trivial overlap relations for polynomials of degree up to d, do not enlarge the leading ideal. In other words, all first kind S- and G-polynomials reduce to zero. Because $\mathcal{G}$ is finite and since for a Gröbner basis over fields or respectively for a "weak" (not strong) Gröbner basis over rings, we only need non-trivial overlap relations, this is the characterizing property of a Gröbner basis. □

[2] An element is *monic* if it's leading coefficient is 1

If we additionally assume that a Gröbner basis computation up to degree $2d$ does not change $\mathrm{L}(\mathcal{G})$, then this means that the trivial overlap relations $\mathrm{lm}(f)\,\mathrm{lm}(g)$, which are of length $\leq 2d$, do not add new polynomials to the basis. It remains to prove that this suffices for all trivial overlap relations $\mathrm{lm}(f)w\,\mathrm{lm}(g)$ with $w \in \mathcal{B}$ to be irrelevant. Moreover, we need to take the divisibility condition $\mathrm{lt}(g) \mid \mathrm{lt}(f)$ into account. As a consequence we could replace "Gröbner basis" with "strong Gröbner basis" in Lemma 2.9.

3 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 3.1. First we consider the case where $t := \mathrm{lm}(f)$ is divisible by (or even equals to) $\mathrm{lm}(g)$. Then $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ contains exactly one element, namely t, because it is the only minimal element that is divisible by both leading monomials. Therefore, $\mathrm{spoly}_1^t(f,\ g)$ and $\mathrm{gpoly}_1^t(f,\ g)$ are the only first type S- and G-polynomials. However, these are not uniquely determined, we might have more overlap relations of $\mathrm{lm}(f)$, $\mathrm{lm}(g)$, as we have seen in the previous example of Remark 2.7, and we still need second type S-polynomials.

The following Lemma has the obvious consequence that G-polynomials are redundant over fields.

Lemma 3.2. *(cf. [9, 19]) Let $f,\ g \in \mathcal{P} \setminus \{0\}$. If $\mathrm{lc}(f) \mid \mathrm{lc}(g)$ in $\mathcal{R}$, then every G-polynomial of f and g is redundant.*

Proof. By the hypothesis we have $b = \mathrm{lcm}(\mathrm{lc}(f), \mathrm{lc}(g)) = \mathrm{lc}(f)$. Let $r \in \mathcal{R}$, such that $r\,\mathrm{lc}(f) = \mathrm{lc}(g)$. Then $\mathrm{lc}(f) = (nr+1)\,\mathrm{lc}(f) - n\,\mathrm{lc}(g)$ yields any possible Bézout identity for b, where $n \in \mathbb{Z}$. Thus, with $t = \tau_f\,\mathrm{lm}(f) = \tau_g\,\mathrm{lm}(g)$, every G-polynomial of f and g has shape $\mathrm{gpoly}(f,\ g) = (nr+1)\tau_f f - n\tau_g g = \mathrm{lc}(f)t + n(r\tau_f\,\mathrm{tail}(f) - \tau_g\,\mathrm{tail}(g)) + \tau_f\,\mathrm{tail}(f)$. Subtracting $\tau_f f$, we can reduce this to $n(r\tau_f\,\mathrm{tail}(f) - \tau_g\,\mathrm{tail}(g))$. Note that $r\tau_f\,\mathrm{tail}(f) - \tau_g\,\mathrm{tail}(g)$ 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 define recursively $\mathrm{tail}^0(f) := f$ and $\mathrm{tail}^i(f) := \mathrm{tail}(\mathrm{tail}^{i-1}(f))$ for $i \geq 1$ when $\mathrm{tail}^{i-1}(f) \neq 0$.

Lemma 3.3. *(Buchberger's product criterion, cf. [9, 19]) 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 $i,\ j \geq 1$, w does not satisfy:
$$\mathrm{lm}(\mathrm{tail}^i(f))w\,\mathrm{lm}(g) = \mathrm{lm}(f)w\,\mathrm{lm}(\mathrm{tail}^j(g))\ .$$
Then $s := \mathrm{spoly}_2^w(f,\ g)$ 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 3.4. The commutative version of Buchberger's product (cf. [9, 19]) criterion states, that the S-polynomial reduces to zero, if the leading terms are coprime over $K[X]$.

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 situation where we might find applications for criteria.

Example 3.5. If $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$ do not 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 $\mathrm{spoly}_2^1(f, g) = 3fzy - 2xyg = 3xzy-2xyz$ and $\mathrm{gpoly}_2^1(f, g) = (-1)fzy+1xyg = 2xyzy+xyz-xzy$ both do not reduce any further and thus must be added to the Gröbner basis just as any other second type S- and G-polynomial.

Also, for first type S- and G-polynomials no statement can be made when the leading coefficients are not coprime. For example in the case of $f = 4xy+y$, $g = 6yz+y$ we have $\mathrm{spoly}_1^{xyz}(f, g) = 3fz-2xg = 3yz-2xy$ and $\mathrm{gpoly}_1^{xyz}(f, g) = (-1)fz+1xg = 2xyz-yz+xy$ which do not reduce any further.

Remark 3.6. Recall that the pair $\{f, g\}$ can be replaced in the commutative case (cf. [9]) by $\{\mathrm{spoly}(f, g), \mathrm{gpoly}(f, g)\}$, if $t = \mathrm{lm}(f) = \mathrm{lm}(g)$ (cf. [9]). Now, if $\mathrm{lm}(f) = \mathrm{lm}(g)$ then in the definition of first type S- and G-polynomials we have $\tau_f = \tau_g = 1 \otimes 1$ and therefore $\mathrm{spoly}_1^t(f, g) = a_f f - a_g g$ and $\mathrm{gpoly}_1^t(f, g) = b_f f + b_g g$. This yields a linear equation

$$\begin{pmatrix} \mathrm{spoly}_1^t(f, g) \\ \mathrm{gpoly}_1^t(f, g) \end{pmatrix} = \begin{pmatrix} a_f & -a_g \\ b_f & b_g \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix},$$

where the defining matrix has determinant $a_f b_g + a_g b_f = 1$, and thus is invertible over $\mathcal{R}$. Hence, we can obtain f and g from their S- and G- polynomial and replace them. The importance of this statement was discussed for the commutative case in [9] and 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 [9].

Lemma 3.7. *(Buchberger's S-chain criterion, cf. [9, 19]) Let $\mathcal{G} \subseteq \mathcal{P}\setminus\{0\}$ and $f, g, h \in \mathcal{G}$. For $a, b \in \{f, g, h\}$ let $\mathrm{LCM}(\mathrm{lm}(a), \mathrm{lm}(b)) \neq \emptyset$ and fix $T_{ab} \in \mathrm{LCM}(\mathrm{lm}(a), \mathrm{lm}(b))$ and choose $\tau_{ab} \in \mathcal{B}^e$ with $\tau_{ab}\,\mathrm{lm}(a) = T_{ab}$. There exist $\tau_{ba} \in \mathcal{B}^e$, such that $\tau_{ba}\,\mathrm{lm}(b) = T_{ab}$. We assume that $T_{ab} = T_{ba}$. Furthermore, 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) $\mathrm{lc}(f) \mid \mathrm{lcm}(\mathrm{lc}(g), \mathrm{lc}(h))$ over $\mathcal{R}$ and
(3) $\mathrm{spoly}_1^{T_{fg}}(f, g)$ and $\mathrm{spoly}_1^{T_{fh}}(f, h)$ both have strong Gröbner representations w.r.t. $\mathcal{G}$.

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

Proof. Let $c_{ab} := \dfrac{\mathrm{lcm}(\mathrm{lc}(a), \mathrm{lc}(b))}{\mathrm{lc}(a)}$ for $a, b \in \{f, g, h\}$. Then one can check by hand, that

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

Using the relations for monomial expressions τ_{ab}, T_{ab}, δ_{ab} and coeffiecients c_{ab}, we see that the first term equals $\mathrm{spoly}_1^{T_{gh}}(g, h)$ and we obtain

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

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

We give a similar criterion for G-polynomials, which can be proven in a manner similar to 3.7.

Lemma 3.8. *(Buchberger's G-chain criterion, cf. [9, 19]) Let $\mathcal{G} \subseteq \mathcal{P}\setminus\{0\}$ and $f, g, h \in \mathcal{G}$. We retain the notations T_{ab} and τ_{ab} from the above. 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) $\mathrm{lc}(f) \mid \gcd(\mathrm{lc}(g), \mathrm{lc}(g))$ with $d := \dfrac{\gcd(\mathrm{lc}(g), \mathrm{lc}(g))}{\mathrm{lc}(f)}$.

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

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 can show how hard these requirements are to be fulfilled compared to the commutative case by specifically counting the number of applications of product and chain criteria.

4 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.

For the examples in this Section, which we take from [1], 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 4.1. 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 [16] (in the same issue of the proceedings), where we also comment in details on syntax and commands of Singular:Letterplace.

```
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); option(redTail); // for minimal reduced GB
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

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

Indeed, we can show that $\forall i \geq 2$ I contains an element with the leading monomial xy^iz. 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 [16]) they were decomposed. Also, over $\mathbb{Q}$ the input ideal has a finite Gröbner basis of degree at most 3.

Example 4.2. 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

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

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)`, which results into an ideal, whose Gröbner basis is

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

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 4.3. 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, in order to prove with the Lemma 2.9 that we have computed a finite Gröbner basis. We use degree right lexicographical ordering and obtain $\{f_1,\ f_2,\ f_3,\ 2y^3 + y^2z - 2yz^2 + 2z^3\}\cup$

$$\{y^2z^2 - 4yz^3 + 6z^4,\ y^4 + 27xy^2z - 54xyz^2 + 54xz^3,$$
$$54xy^2z - y^3z - 108xyz^2 + 108xz^3 + 62yz^3 - 124z^4,\ 14z^5,$$
$$14yz^3 - 28z^4,\ 2yz^4 - 6z^5,\ 2xyz^3 - 4xz^4,\ xy^3z,\ 2z^6,\ 2xz^5\}.$$

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 degree 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.

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, used no product criterion and 9 times the chain criterion with less than 1 MB of memory. The result is $\{f_1,\ f_2,\ f_3\} \cup \{z^5, yz^3 - 2z^4\}\cup$

$$\{2y^3 + y^2z - 2yz^2 + 2z^3, y^2z^2 - 2z^4, xy^2z - 2xyz^2 + 2xz^3\}.$$

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

5 IMPLEMENTATION

We have created a powerful implementation called Letterplace [15] in the framework of Singular. Its' extension to coefficient rings like $\mathbb{Z}$ addresses the following functions with the current release for ideals and subbimodules of a free bimodule of a finite rank. We provide a vast family of monomial and module orderings including three kinds of orderings eliminating variables or free bimodule components.

`twostd`: a two-sided Gröbner basis; run with respect to an elimination ordering, it allows to eliminate variables [6], and thus to compute kernels of ring morphisms and preimages of ideals under such;

`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 [5] 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.

6 CONCLUSION AND FUTURE WORK

Following Mora's "manual for creating own Gröbner basis theory" [21], 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.

A further adaptation of our implementation to the explicitly given $\mathbb{Z}/m\mathbb{Z}$ is planned, as well as the development (also a theoretical) of one-sided Gröbner bases in factor algebras (over fields, Letterplace already offers `rightstd`). More functions for dealing with matrices will make possible the usage of our implementation as a backend from the system HomAlg [3]. 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. Also big systems like SageMath and OSCAR can use our implementation as backend.

7 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) for fruitful discussions.

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

[1] J. Apel. 2000. Computational ideal theory in finitely generated extension rings. *Theor. Comput. Sci.* 244, 1-2 (2000), 1–33.
[2] J. Apel and U. Klaus. 1991. *FELIX* – an assistant for algebraists. In *Proc. ISSAC'91*. ACM Press, 382–389. See also http://felix.hgb-leipzig.de.
[3] Mohamed Barakat, Sebastian Gutsche, and Markus Lange-Hegermann. 2019. homalg - A homological algebra meta-package for computable Abelian categories. https://homalg-project.github.io/homalg_project/homalg/.
[4] George M. Bergman. 1977. The diamond lemma for ring theory. *Adv. Math.* 29 (1977), 178–218. https://doi.org/10.1016/0001-8708(78)90010-5
[5] Holger Bluhm and Martin Kreuzer. 2007. Computation of two-sided syzygies over non-commutative rings. *Contemp. Math.* 421 (2007), 45–64.
[6] M. A. Borges and M. Borges. 1998. Gröbner bases property on elimination ideal in the noncommutative case. In *Gröbner bases and applications*, B. Buchberger and F. Winkler (Eds.). Cambridge University Press, 323–337.
[7] Christian Eder and Tommy Hofmann. 2019. Efficient Gröbner Bases Computation over Principal Ideal Rings. https://arxiv.org/abs/1906.08543.
[8] Christian Eder, Gerhard Pfister, and Adrian Popescu. 2016. New Strategies for Standard Bases over Z. https://arxiv.org/abs/1609.04257.
[9] Christian Eder, Gerhard Pfister, and Adrian Popescu. 2018. Standard Bases over Euclidean Domains. https://arxiv.org/abs/1811.05736.
[10] Heinz Kredel. 2015. Parametric Solvable Polynomial Rings and Applications. In *Proc. CASC'15*, Vladimir P. Gerdt, Wolfram Koepf, Werner M. Seiler, and Evgenii V. Vorozhtsov (Eds.). Springer International Publishing, Cham, 275–291. https://doi.org/10.1007/978-3-319-24021-3_21
[11] Roberto La Scala. 2014. Extended letterplace correspondence for nongraded noncommutative ideals and related algorithms. *Int. J. Algebra Comput.* 24, 8 (2014), 1157–1182.
[12] Roberto La Scala and Viktor Levandovskyy. 2009. Letterplace ideals and noncommutative Gröbner bases. *Journal of Symbolic Computation* 44, 10 (2009), 1374–1393. https://doi.org/10.1016/j.jsc.2009.03.002
[13] Roberto La Scala and Viktor Levandovskyy. 2013. Skew polynomial rings, Gröbner bases and the letterplace embedding of the free associative algebra. *Journal of Symbolic Computation* 48, 1 (2013), 110–131. http://dx.doi.org/10.1016/j.jsc.2012.05.003
[14] Viktor Levandovskyy. 2005. Non–commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation. http://kluedo.ub.uni-kl.de/volltexte/2005/1883/.
[15] Viktor Levandovskyy, Karim Abou Zeid, and Hans Schönemann. 2020. Singular:Letterplace — A Singular 4-1-3 Subsystem for Non-commutative Finitely Presented Algebras. http://www.singular.uni-kl.de.
[16] Viktor Levandovskyy, Hans Schönemann, and Karim Abou Zeid. 2020. Letterplace — a Subsystem of Singular for computations with free algebras via Letterplace Embedding. In *Proc. ISSAC'20*. ACM Press. to appear.
[17] Viktor Levandovskyy, Grischa Studzinski, and Benjamin Schnitzler. 2013. Enhanced Computations of Gröbner Bases in Free Algebras as a New Application of the Letterplace Paradigm. In *Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'13)*, Manuel Kauers (Ed.). ACM Press, 259 – 266.
[18] Huishi Li. 2012. Algebras Defined by Monic Gröbner Bases over Rings. *International Mathematical Forum* 7 (2012), 1427–1450.
[19] Daniel Lichtblau. 2012. Effective computation of strong Gröbner bases over Euclidean domains. *Illinois Journal of Mathematics* 56 (2012), 177–194.
[20] Thomas Markwig, Yue Ren, and Oliver Wienand. 2015. Standard Bases in mixed Power Series and Polynomial Rings over Rings. *Journal of Symbolic Computation* 79 (09 2015). https://doi.org/10.1016/j.jsc.2016.08.009
[21] Teo Mora. 2016. *Solving Polynomial Equation Systems IV: Volume 4, Buchberger Theory and Beyond* (1st ed.). Cambridge University Press.
[22] Franz Pauer. 2007. Gröbner bases with coefficients in rings. *Journal of Symbolic Computation* 42 (2007), 1003 – 1011. https://doi.org/10.1016/j.jsc.2007.06.006
[23] F. Leon Pritchard. 1996. The ideal membership problem in non-commutative polynomial rings. *J. Symb. Comput.* 22, 1 (1996), 27–48. https://doi.org/10.1006/jsco.1996.0040