Signature Gröbner bases, bases of syzygies and cofactor reconstruction in the free algebra

Clemens Hofstadler, Thibaut Verron

Institute for Algebra, Johannes Kepler University Linz, Austria

Abstract

Signature-based algorithms have become a standard approach for computing Gröbner bases in commutative polynomial rings. However, so far, it was not clear how to extend this concept to the setting of noncommutative polynomials in the free algebra. In this paper, we present a signature-based algorithm for computing Gröbner bases in precisely this setting. The algorithm is an adaptation of Buchberger's algorithm including signatures. We prove that our algorithm correctly enumerates a signature Gröbner basis as well as a Gröbner basis of the syzygy module, and that it terminates whenever the ideal admits a finite signature Gröbner basis. Additionally, we adapt well-known signature-based criteria eliminating redundant reductions, such as the syzygy criterion, the F5 criterion and the singular criterion, to the case of noncommutative polynomials. We also generalize reconstruction methods from the commutative setting that allow to recover, from partial information about signatures, the coordinates of elements of a Gröbner basis in terms of the input polynomials, as well as a basis of the syzygy module of the generators. We have written a toy implementation of all the algorithms in the Mathematica package `OperatorGB` and we compare our signature-based algorithm to the classical Buchberger algorithm for noncommutative polynomials.

Keywords: Noncommutative polynomials, Signature Gröbner bases, Syzygy module, Cofactor reconstruction

1. Introduction

Gröbner bases have become a fundamental and multi-purpose tool in computational algebra. They were initially introduced [Buc65] to answer questions about ideals of multivariate (commutative) polynomials, and they were subsequently generalized to several noncommutative settings, including Weyl polynomials [Gal85] encoding, for example, differential equations, and noncommutative polynomials in the free algebra [Mor85], which can model matrix identities and, more generally, identities of linear operators. In the latter setting, Gröbner bases and the associated reduction machinery are notably useful for simplifying and proving operator identities [HW94, HSW98, HRR19, CHRR20, SL20, RRHP21].

Email addresses: `clemens.hofstadler@jku.at` (Clemens Hofstadler), `thibaut.verron@jku.at` (Thibaut Verron)

The main theoretical results needed to adapt the concept of Gröbner bases to the free algebra are due to Bergman [Ber78], who used the abstract concept of reduction systems to generalize the ideas from the commutative setting. This development was independent of the commutative theory. Around the same time, also Bokut' [Bok76] proved statements that are essentially equivalent to the ones by Bergman. Bokut' attributes his results to Shirshov, who had published similar results in the context of Lie algebras [Shi62]. The first explicit algorithm for computing noncommutative Gröbner bases was proposed by Mora [Mor85] a few years later, who adapted Buchberger's algorithm to the free algebra. Later, Mora also managed to unify the theory of Gröbner bases for commutative and noncommutative polynomial rings via a generalization of the Gaussian elimination algorithm [Mor94]. Recently, also the F4 algorithm [Fau99] has been adapted to this setting [Xiu12]. However, contrary to the commutative or the Weyl case, not all ideals in the free algebra admit a finite Gröbner basis. Instead, the algorithms always enumerate a Gröbner basis, with termination if and only if a finite Gröbner basis exists w.r.t. the chosen monomial order.

In the case of commutative polynomials, the latest generation of Gröbner basis algorithms are the so-called signature-based algorithms, heralded by the F5 algorithm [Fau02]. This class of algorithms was the subject of extensive research in the past 20 years, a survey of which can be found in [EF17]. Those algorithms compute, in addition to a Gröbner basis, some information on how the polynomials in that basis were computed. Using this information, the algorithms are able to identify relations between the computed polynomials, and use them to predict and avoid reductions to zero and redundant computations. This yields a significant performance improvement.

Additionally, it was observed recently [SW11, GVW15] that the data of signatures is enough to reconstruct the cofactors of the Gröbner basis, that is, the coordinates of the elements of the basis in terms of the input polynomials. Similarly, one can also compute a basis of the syzygy module of the generators. Alternatively, those operations can be realised using the classical theory and algorithms for Gröbner bases of modules (one can see [BW93, Ch. 10] for a textbook exposition with references, or [AL94, Ch. 3]), but signatures allow to reduce the cost of those computations to that of a Gröbner basis of an ideal. Algorithms for computing Gröbner bases with signatures have also been developed in the case of Weyl algebras [SWMZ12], with the same application to the computation of coordinates of Gröbner basis elements, and of syzygies.

The problem of computing the cofactors of a Gröbner basis is also central when working with noncommutative polynomials. In particular, when proving operator identities, this information allows to construct a proof certificate for a given identity, which can be checked easily and independently of how it was obtained, see for example [Hof20]. Like in the commutative case, the classical theory and algorithms for computing Gröbner bases in modules can also be used to obtain such information [BK06, Mor16], but those algorithms are significantly more expensive than a mere Gröbner basis computation. Furthermore, for most ideals in the free algebra, the module of syzygies is not finitely generated and does not admit a finite Gröbner basis, which makes those algorithms in fact only enumeration procedures.

In this paper, we show how to define and compute signature Gröbner bases for noncommutative polynomials in the free algebra, and we show how to use them to reconstruct the module representation of elements of the ideal, and a basis of the syzygy module of the generators. We also generalize some classical signature-based criteria such as the syzygy criterion, the F5 criterion and the singular criterion, in order to use signatures to accelerate the algorithms.

A difficulty specific to the case of noncommutative polynomials is that some ideals may not have a finite signature Gröbner basis, even if the ideal has a finite Gröbner basis. This is unavoidable, but we prove that the algorithm nonetheless correctly enumerates a signature Gröbner basis.

Additionally, as already mentioned, the module of syzygies of the generators usually does not admit a finite Gröbner basis. More precisely, the initial module of the set of so-called "trivial syzygies" (sometimes called Koszul syzygies, or principal syzygies) is typically not finitely generated. On the other hand, a strength of signature-based algorithms is precisely that they make it possible to identify those trivial syzygies, and in particular this set of trivial syzygies admits a finite and effective representation in terms of a signature Gröbner basis. In classical cases, avoiding those trivial syzygies is the crux of the F5 criterion, and in the noncommutative case, it allows the algorithm to enumerate a basis of the syzygy module by only considering the non-trivial syzygies.

If our algorithm terminates, it computes a finite signature Gröbner basis, and in particular, a finite Gröbner basis and a finite and effective description of the module of syzygies of the input polynomials. We conjecture that conversely, the existence of a finite Gröbner basis of the ideal and of a finite description of the module of syzygies of the generators, implies the existence of a finite signature Gröbner basis.

We also provide a toy implementation[1] of the algorithms presented in this paper in the Mathematica package `OperatorGB` [HRR19, Hof20]. Additionally, we show experimentally that the use of signatures allows to drastically reduce the number of S-polynomials considered and reduced to zero. For an overview on other available software packages in the realm of noncommutative Gröbner bases, see [LSZ20] and references therein.

2. Preliminaries

For the convenience of the reader, we recall the most important aspects of the theory of Gröbner bases in the free algebra and of Gröbner bases of submodules of the free bimodule in this section. Additionally, we introduce the notion of *signatures* in this noncommutative setting as a straightforward generalization of signatures from the commutative case.

We fix a finite set of indeterminates $X = \{x_1, \dots, x_n\}$ and denote by $\langle X \rangle$ the free monoid over X containing all *words* (or *monomials*) of the form $w = x_{i_1} \dots x_{i_k}$ including the *empty word* 1. The quantity k is called the *length* of w. Furthermore, for a field K, we let

$$K\langle X \rangle = \left\{ \sum_{w \in \langle X \rangle} c_w w \mid c_w \in K \text{ such that only finitely many } c_w \neq 0 \right\}$$

be the *free algebra* generated by X over K. We consider the elements in $K\langle X \rangle$ as noncommutative polynomials with coefficients in K and indeterminates in X, where indeterminates commute with coefficients but not with each other.

For a given set of polynomials $F \subseteq K\langle X \rangle$, we denote by (F) the *(two-sided) ideal* generated by F, that is

$$(F) = \left\{ \sum_{i=1}^{d} a_i f_i b_i \mid f_i \in F,\ a_i, b_i \in K\langle X \rangle,\ d \in \mathbb{N} \right\}.$$

[1] Available at `https://clemenshofstadler.com/software/`

The set F is called a *set of generators* of (F). An ideal $I \subseteq K\langle X\rangle$ is said to be *finitely generated* if there exists a finite set of generators $F \subseteq K\langle X\rangle$ such that $I = (F)$. We agree upon the convention to write $(f_1, \ldots, f_r)$ instead of $(\{f_1, \ldots, f_r\})$ if the elements of $F = \{f_1, \ldots, f_r\}$ are given explicitly.

Remark 1. If $|X| > 1$, the free algebra $K\langle X\rangle$ is not Noetherian, i.e. there exist ideals in $K\langle X\rangle$ which are not finitely generated. One prominent example is the ideal $(xy^ix \mid i \in \mathbb{N}) \subseteq K\langle x, y\rangle$, which has no finite set of generators.

Definition 2. A *monomial ordering* on $\langle X\rangle$ is a well-ordering $\preceq$ that is compatible with the multiplication in $\langle X\rangle$, that is, $w \preceq w'$ implies $awb \preceq aw'b$ for all $a, b, w, w' \in \langle X\rangle$.

An example of a monomial ordering on $\langle X\rangle$ is the degree lexicographic ordering $\preceq_{deglex}$, where two words $w, w' \in \langle X\rangle$ are first compared by their length and ties are broken by comparing the variables in w and w' from left to right using the lexicographic ordering $x_1 \prec_{lex} \cdots \prec_{lex} x_n$.

In what follows, we fix a monomial ordering $\preceq$ on $\langle X\rangle$. Then, every non-zero $f \in K\langle X\rangle$ has a unique representation of the form $f = c_1w_1 + \cdots + c_dw_d$ with $c_1, \ldots, c_d \in K \setminus \{0\}$ and $w_1, \ldots, w_d \in \langle X\rangle$ such that $w_1 \succ \cdots \succ w_d$.

Definition 3. Let $f = c_1w_1+\cdots+c_dw_d \in K\langle X\rangle\setminus\{0\}$ with $c_1, \ldots, c_k \in K\setminus\{0\}$ and $w_1, \ldots, w_k \in \langle X\rangle$ such that $w_1 \succ \cdots \succ w_k$. Then, w_1 is called the *leading monomial* of f, denoted by $\text{lm}(f)$. The coefficient c_i of w_i is denoted by $\text{coeff}(f, w_i)$ for $i = 1, \ldots, r$. We call c_1 the *leading coefficient* of f, abbreviated as $\text{lc}(f)$. Furthermore, the *leading term* $\text{lt}(f)$ of f is $\text{lt}(f) = \text{lc}(f) \cdot \text{lm}(f)$. Finally, the set $\{w_1, \ldots, w_k\}$ is called the *support* of f and denoted by $\text{supp}(f)$.

Remark 4. Note that the leading monomial/coefficient/term of the zero polynomial remain undefined.

In the following, we briefly recall the most important results about Gröbner bases in $K\langle X\rangle$. For a more extensive treatment of this subject, we refer to the recent surveys [Xiu12, Mor16, Hof20]. The main concept needed to discuss and compute noncommutative Gröbner bases is polynomial reduction.

Definition 5. Let $f, f', g \in K\langle X\rangle$ with $g \neq 0$. We say that f *reduces* to f' by g if there exist $a, b \in \langle X\rangle$ such that $a\,\text{lm}(g)b \in \text{supp}(f)$ and

$$f' = f - \frac{\text{coeff}(f, a\,\text{lm}(g)b)}{\text{lc}(g)} \cdot agb.$$

In this case, we write $f \to_g f'$.

Based on this concept, for a set $G \subseteq K\langle X\rangle$, we define a reduction relation $\to_G \subseteq K\langle X\rangle \times K\langle X\rangle$ by $f \to_G f'$ if there exists $g \in G$ such that $f \to_g f'$. We denote by $\overset{*}{\to}_G$ the reflexive, transitive closure of $\to_G$. Using this reduction relation, we can now define Gröbner bases in $K\langle X\rangle$.

Definition 6. Let $I \subseteq K\langle X\rangle$ be an ideal and $G \subseteq I$ such that $(G) = I$. Then, G is a *Gröbner basis* of I if $f \overset{*}{\to}_G 0$ for all $f \in I$.

We note that not all finitely generated ideals in $K\langle X\rangle$ have a finite Gröbner basis. One example is the principal ideal $(xyx-xy) \subseteq K\langle x, y\rangle$, which, regardless of the chosen monomial ordering, has no finite Gröbner basis. Even though ideal membership is undecidable in the free algebra, a noncommutative analog of Buchberger's algorithm can be used to enumerate a (possibly infinite) Gröbner basis.

We also need the notion of Gröbner bases of sub-bimodules of a free $K\langle X\rangle$-bimodule. Hence, we shall briefly recall this concept in the following. For further details on this topic, we refer to [Xiu12, Mor16]. We note that when speaking about a (sub)module, we always mean a (sub-)bimodule.

For $r \in \mathbb{N}$, we denote by $\mathcal{F}_r = (K\langle X\rangle \otimes K\langle X\rangle)^r$ the *free $K\langle X\rangle$-bimodule* of rank r with the canonical basis $\varepsilon_1, \ldots, \varepsilon_r$, where $\varepsilon_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$ with $1 \otimes 1$ appearing in the i-th position for $i = 1, \ldots, r$. Furthermore, we let $\mathbb{M}(\mathcal{F}_r) = \{a\varepsilon_i b \mid a, b \in \langle X\rangle, 1 \leq i \leq r\}$ be the set of *module monomials* in $\mathcal{F}_r$. This set forms a K-vector space basis of $\mathcal{F}_r$.

Definition 7. A *module ordering* on $\mathbb{M}(\mathcal{F}_r)$ is a well-ordering $\preceq_{\mathbb{M}}$ that is compatible with the scalar multiplication, that is, $\mu \preceq_{\mathbb{M}} \mu'$ implies $a\mu b \preceq_{\mathbb{M}} a\mu' b$ for all $\mu, \mu' \in \mathbb{M}(\mathcal{F}_r)$ and $a, b \in \langle X\rangle$.

Given a monomial ordering $\preceq$, an example of a module ordering is the term-over-position ordering $\preceq_{\mathbf{top}}$, where $a_1\varepsilon_{i_1}b_1 \preceq_{\mathbf{top}} a_2\varepsilon_{i_2}b_2$ for two module monomials $a_1\varepsilon_{i_1}b_1, a_2\varepsilon_{i_2}b_2 \in \mathbb{M}(\mathcal{F}_r)$ if one of the following conditions holds:

1. $a_1b_1 \prec a_2b_2$;
2. $a_1b_1 = a_2b_2$ and $a_1 \prec a_2$;
3. $a_1b_1 = a_2b_2$ and $a_1 = a_2$ and $i_1 \leq i_2$.

In the following, we fix a module ordering $\preceq_{\mathbb{M}}$ on $\mathbb{M}(\mathcal{F}_r)$. Then, using the K-vector space basis $\mathbb{M}(\mathcal{F}_r)$, every non-zero $\alpha \in \mathcal{F}_r$ can be uniquely written as $\alpha = c_1\mu_1 + \cdots + c_d\mu_d$ with $c_1, \ldots, c_d \in K \setminus \{0\}$ and $\mu_1, \ldots, \mu_d \in \mathbb{M}(\mathcal{F}_r)$ such that $\mu_1 \succ_{\mathbb{M}} \cdots \succ_{\mathbb{M}} \mu_d$.

Definition 8. Let $\alpha = c_1\mu_1 + \cdots + c_d\mu_d$ with $c_1, \ldots, c_d \in K \setminus \{0\}$ and $\mu_1, \ldots, \mu_d \in \mathbb{M}(\mathcal{F}_r)$ such that $\mu_1 \succ_{\mathbb{M}} \cdots \succ_{\mathbb{M}} \mu_d$. Then, μ_1 is called the *signature* of α, denoted by $\mathfrak{s}(\alpha)$. Analogously to the case of polynomials, we also define the *signature coefficient* $\mathfrak{sc}(\alpha)$ of α to be the coefficient appearing in front of $\mathfrak{s}(\alpha)$, that is $\mathfrak{sc}(\alpha) = c_1$. Furthermore, the *signature term* $\mathfrak{st}(\alpha)$ of α is $\mathfrak{st}(\alpha) = \mathfrak{sc}(\alpha) \cdot \mathfrak{s}(\alpha)$.

As for polynomials, the signature (coefficient/term) of the zero element in $\mathcal{F}_r$ remains undefined. By a slight abuse of notation, for a set $F \subseteq \mathcal{F}_r$, we denote by $\mathfrak{s}(F)$ the set of signatures of all non-zero $\alpha \in F$, i.e. $\mathfrak{s}(F) = \{\mathfrak{s}(\alpha) \mid 0 \neq \alpha \in F\}$.

Definition 9. Let $M \subseteq \mathcal{F}_r$ be a $K\langle X\rangle$-submodule. A subset $G \subseteq M \setminus \{0\}$ is called a *Gröbner basis* of M if

$$\mathfrak{s}(M) = \{a\,\mathfrak{s}(\gamma)b \mid a, b \in \langle X\rangle, \gamma \in G\}.$$

Remark 10. Gröbner bases of submodules could also be defined using a notion of reduction. However, the definition given above shall prove more useful to us here.

3. Signature Gröbner bases

The aim of this section is to introduce the notion of *signature Gröbner bases* of ideals in the free algebra. As for commutative polynomials, this is done via a restricted kind of polynomial reduction, called $\mathfrak{s}$-*reduction*. Moreover, we also define and characterize noncommutative *minimal* signature Gröbner bases. We note that all notions introduced here are straightforward generalization of the same notions for commutative polynomials.

For the rest of this paper, we fix a set of generators $\{f_1, \ldots, f_r\} \subseteq K\langle X\rangle$ of an ideal $I = (f_1, \ldots, f_r)$ as well as a monomial ordering $\preceq$ on $\langle X\rangle$ and a module ordering $\preceq_{\mathbb{M}}$ on $\mathbb{M}(\mathcal{F}_r)$. We additionally require the following two conditions:

1. $\preceq$ and $\preceq_{\mathbb{M}}$ have to be *compatible* in the sense that

$$a \prec b \iff a\varepsilon_i \prec_{\mathbb{M}} b\varepsilon_i \iff \varepsilon_i a \prec_{\mathbb{M}} \varepsilon_i b$$

for all $a, b \in \langle X \rangle$ and $i = 1, \ldots, r$.

2. $\preceq_{\mathbb{M}}$ has to be *fair*, meaning that the set $\{\mu' \in \mathbb{M}(\mathcal{F}_r) \mid \mu' \prec_{\mathbb{M}} \mu\}$ has to be finite for all $\mu \in \mathbb{M}(\mathcal{F}_r)$.

The second condition excludes position-over-term orderings but, for example, the module ordering $\preceq_{\mathbf{top}}$ is fair when the underlying monomial ordering is $\preceq_{deglex}$. In that case, the combination $\preceq_{deglex}$ and $\preceq_{\mathbf{top}}$ is also compatible. From now on, we shall denote both orders, $\preceq_{\mathbb{M}}$ as well as $\preceq$, by the symbol $\preceq$. It will be clear from the context which ordering is meant, as we will denote elements from $\mathcal{F}_r$ by Greek letters and elements from $K\langle X \rangle$ by Roman letters. We note that all results that follow from here on depend (implicitly) on $\preceq$ and are to be understood w.r.t. our fixed monomial and module ordering.

Elements in the free $K\langle X \rangle$-bimodule $\mathcal{F}_r$ encode elements of the ideal I via the $K\langle X \rangle$-module homomorphism

$$\overline{\cdot} : \mathcal{F}_r \to K\langle X \rangle, \quad \alpha = \sum_i c_i a_i \varepsilon_{j_i} b_i \mapsto \overline{\alpha} := \sum_i c_i a_i f_{j_i} b_i,$$

with $a_i, b_i \in \langle X \rangle$ and $j_i \in \{1, \ldots, r\}$.

We adapt the notation from [SW11] and denote by $f^{[\alpha]}$ a pair $(f, \alpha) \in K\langle X \rangle \times \mathcal{F}_r$ with $f = \overline{\alpha}$. We refer to $f^{[\alpha]}$ as a *signature polynomial*. By the definition of $\overline{\cdot}$, we always have $f^{[\alpha]} \in I \times \mathcal{F}_r$. Consequently, we denote by

$$I^{[\Sigma]} := \{f^{[\alpha]} \mid f = \overline{\alpha}\} \subseteq I \times \mathcal{F}_r$$

the set of all signature polynomials.

Remark 11. We note that different sets of generators of the same ideal $I \subseteq K\langle X \rangle$ lead to different sets $I^{[\Sigma]}$. Hence, to be precise, we should only speak of the the set of signature polynomials $I^{[\Sigma]}$ *w.r.t. the generators* $f_1, \ldots, f_r$. However, whenever the generators $f_1, \ldots, f_r$ are clear from the context, we might omit this part and only speak of $I^{[\Sigma]}$. We recall that we have fixed a set of generators $\{f_1, \ldots, f_r\}$ of the ideal $I = (f_1, \ldots, f_r)$. Hence, all further results are to be understood w.r.t. this set of generators.

Computations in $I^{[\Sigma]}$ can be defined naturally. In particular, for $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$, $c \in K$ and $a, b \in \langle X \rangle$ we have

- $f^{[\alpha]} + g^{[\beta]} = (f + g)^{[\alpha+\beta]}$, and
- $caf^{[\alpha]}b = (cafb)^{[ca\alpha b]}$.

With these operations the set $I^{[\Sigma]}$ becomes a $K\langle X \rangle$-bimodule. Furthermore, we set $f^{[\alpha]} = g^{[\beta]}$ if and only if $f = g$ and $\alpha = \beta$. We also extend the notions of leading monomial/coefficient/term and signature (coefficient/term) to signature polynomials in a straightforward way.

We call an element $\sigma \in \mathcal{F}_r$ a *syzygy* if $\overline{\sigma} = 0$. The set of all syzygies of $f_1, \ldots, f_r$ is denoted by $\mathrm{Syz}(f_1, \ldots, f_r)$ and forms a $K\langle X \rangle$-submodule of $\mathcal{F}_r$. For all signature polynomials $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ and any monomial $m \in \langle X \rangle$ we obtain with $\sigma = \alpha m g - f m \beta$ a so-called *trivial syzygy* between $f^{[\alpha]}$ and $g^{[\beta]}$.

In order to discuss signature Gröbner bases, we need to adapt the notion of polynomial reduction to signature polynomials. This leads to the following definition of $\mathfrak{s}$-*reduction*.

Definition 12. Let $f^{[\alpha]}, f'^{[\alpha']}, g^{[\gamma]} \in I^{[\Sigma]}$ with $\alpha, g \neq 0$. We say that $f^{[\alpha]}$ $\mathfrak{s}$-*reduces* to $f'^{[\alpha']}$ by $g^{[\gamma]}$ if there exist $a, b \in \langle X \rangle$ such that

- $a\,\mathrm{lm}(g)b \in \mathrm{supp}(f)$,
- $\mathfrak{s}(a\gamma b) \preceq \mathfrak{s}(\alpha)$, and
- $f'^{[\alpha']} = f^{[\alpha]} - \frac{\mathrm{coeff}(f, a\,\mathrm{lm}(g)b)}{\mathrm{lc}(g)} a g^{[\gamma]} b$.

In this case, we write $f^{[\alpha]} \rightarrow_{g^{[\gamma]}} f'^{[\alpha']}$.

Remark 13. In terms of polynomials, the first condition means that we can do usual polynomial reduction. This implies that either $f' = 0$ or $\mathrm{lm}(f') \preceq \mathrm{lm}(f)$. The second condition ensures that this inequality also transfers over to $\mathcal{F}_r$, i.e. that either $\alpha' = 0$ or $\mathfrak{s}(\alpha') \preceq \mathfrak{s}(\alpha)$.

A set of signature polynomials $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ induces a reduction relation $\rightarrow_{G^{[\Sigma]}} \subseteq I^{[\Sigma]} \times I^{[\Sigma]}$ by defining $f^{[\alpha]} \rightarrow_{G^{[\Sigma]}} f'^{[\alpha']}$ if there exists $g^{[\gamma]} \in G^{[\Sigma]}$ such that $f^{[\alpha]} \rightarrow_{g^{[\gamma]}} f'^{[\alpha']}$. Furthermore, as in the case of polynomials, we denote by $\overset{*}{\rightarrow}_{G^{[\Sigma]}}$ the reflexive, transitive closure of $\rightarrow_{G^{[\Sigma]}}$. The following lemma follows immediately from the definition.

Lemma 14. *If $f^{[\alpha]} \overset{*}{\rightarrow}_{G^{[\Sigma]}} f'^{[\alpha']}$, then $f \overset{*}{\rightarrow}_G f'$, where $G = \{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$.*

If $\mathrm{lm}(f') \prec \mathrm{lm}(f)$, then the $\mathfrak{s}$-reduction is called a *top* $\mathfrak{s}$-*reduction*. Otherwise it is called a *tail* $\mathfrak{s}$-*reduction*. Similarly, if $\mathfrak{s}(\alpha') \prec \mathfrak{s}(\alpha)$, then the $\mathfrak{s}$-reduction is called a *singular* $\mathfrak{s}$-*reduction*. Otherwise it is called a *regular* $\mathfrak{s}$-*reduction*. If $f^{[\alpha]}$ $\mathfrak{s}$-reduces to some $f'^{[\alpha']}$ with $f' = 0$, or in other words if α' is a syzygy, we say that $f^{[\alpha]}$ $\mathfrak{s}$-*reduces to zero*.

We capture some useful facts about $\mathfrak{s}$-reduction that will be needed later. This first corollary is an immediate consequence of the definition of regular $\mathfrak{s}$-reduction.

Corollary 15. *Regular $\mathfrak{s}$-reductions do not change the signature of a signature polynomial.*

Lemma 16. *Let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ and let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ be both top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$ with $\mathfrak{s}(\alpha) \preceq \mathfrak{s}(\alpha + \beta)$ and $\mathfrak{s}(\beta) \preceq \mathfrak{s}(\alpha + \beta)$. Then, $f^{[\alpha]} + g^{[\beta]}$ is also top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$ or* $\mathrm{lt}(f) + \mathrm{lt}(g) = 0$.

Proof. Assume that $\mathrm{lt}(f) + \mathrm{lt}(g) \neq 0$. Then, $\mathrm{lm}(f+g) = \max_{\preceq}\{\mathrm{lm}(f), \mathrm{lm}(g)\}$. W.l.o.g. assume that $\mathrm{lm}(f) \succeq \mathrm{lm}(g)$, so that $\mathrm{lm}(f+g) = \mathrm{lm}(f)$. Since $f^{[\alpha]}$ is top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$ and $\mathfrak{s}(\alpha) \preceq \mathfrak{s}(\alpha+\beta)$, the signature polynomial $f^{[\alpha]} + g^{[\beta]}$ is also top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$. In fact, the same element $g^{[\gamma]} \in G^{[\Sigma]}$ can be used to top $\mathfrak{s}$-reduce both, $f^{[\alpha]}$ as well as $f^{[\alpha]} + g^{[\beta]}$. □

The outcome of classical polynomial reduction depends on more than just the leading term of the polynomial that is reduced. Polynomials which share the same leading term can still reduce to different elements. In case of regular $\mathfrak{s}$-reductions, certain assumptions on the set of reducers $G^{[\Sigma]}$ imply that all signature polynomials with the same signature term yield the same regular $\mathfrak{s}$-reduced result. This fact is captured in the following lemma.

Lemma 17. *Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ be such that $\mathfrak{st}(\alpha) = \mathfrak{st}(\beta)$. Furthermore, assume that all $u^{[\mu]} \in I^{[\Sigma]}$ with $\mathfrak{s}(\mu) \prec \mathfrak{s}(\alpha)$ $\mathfrak{s}$-reduce to zero by $G^{[\Sigma]}$. Then, the following hold.*

- *If $f^{[\alpha]}$ and $g^{[\beta]}$ are regular $\mathfrak{s}$-reduced, then $f = g$.*
- *If $f^{[\alpha]}$ and $g^{[\beta]}$ are regular top $\mathfrak{s}$-reduced, then* $\mathrm{lt}(f) = \mathrm{lt}(g)$.

Proof. We first prove that $f = g$ if $f^{[\alpha]}$ and $g^{[\beta]}$ are regular $\mathfrak{s}$-reduced. Consider $u^{[\mu]} = f^{[\alpha]} - g^{[\beta]}$ and assume, for contradiction, that $u \neq 0$. Then, since $\mathfrak{st}(\alpha) = \mathfrak{st}(\beta)$, we have that $\mathfrak{s}(\mu) \prec \mathfrak{s}(\alpha)$. Hence, by assumption, $u^{[\mu]}$ $\mathfrak{s}$-reduces to zero. In particular, this means that there exists $g^{[\gamma]} \in G^{[\Sigma]}$ with $\mathfrak{s}(\gamma) \preceq \mathfrak{s}(\mu)$ such that $g^{[\gamma]}$ top $\mathfrak{s}$-reduces $u^{[\mu]}$. W.l.o.g. we may assume that $\mathrm{lm}(u)$ comes from a term in $f^{[\alpha]}$. Then, this term in $f^{[\alpha]}$ can be regular $\mathfrak{s}$-reduced by $g^{[\gamma]}$ since $\mathfrak{s}(\gamma) \preceq \mathfrak{s}(\mu) \prec \mathfrak{s}(\alpha)$. This is a contradiction to $f^{[\alpha]}$ being regular $\mathfrak{s}$-reduced.

The proof of the second statement is similar: consider $u^{[\mu]} = f^{[\alpha]} - g^{[\beta]}$ and assume, for contradiction, that $\mathrm{lm}(u) = \max_{\preceq}\{\mathrm{lm}(f), \mathrm{lm}(g)\}$. W.l.o.g. we may assume that $\mathrm{lm}(u) = \mathrm{lm}(f)$. The rest of the proof is identical: $\mathfrak{s}(\mu) \prec \mathfrak{s}(\alpha)$ so $u^{[\mu]}$ $\mathfrak{s}$-reduces to zero, and in particular it is top $\mathfrak{s}$-reducible. This is a contradiction to $f^{[\alpha]}$ being regular top $\mathfrak{s}$-reduced □

Using the notion of $\mathfrak{s}$-reduction, we can now define a *signature Gröbner basis* of the module $I^{[\Sigma]}$.

Definition 18. A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a *signature Gröbner basis of* $I^{[\Sigma]}$ *up to signature* $\sigma \in \mathbb{M}(\mathcal{F}_r)$ if all $f^{[\alpha]} \in I^{[\Sigma]}$ with $\mathfrak{s}(\alpha) \prec \sigma$ $\mathfrak{s}$-reduce to zero by $G^{[\Sigma]}$. Furthermore, $G^{[\Sigma]}$ is a *signature Gröbner basis of* $I^{[\Sigma]}$ if all $f^{[\alpha]} \in I^{[\Sigma]}$ $\mathfrak{s}$-reduce to zero by $G^{[\Sigma]}$.

Remark 19. Since different sets of generators of the ideal I lead to different modules $I^{[\Sigma]}$, they also lead to different signature Gröbner bases (see also Example 27). Consequently, we should only speak of a signature Gröbner basis of $I^{[\Sigma]}$ (up to signature σ) *w.r.t. the generators* $f_1, \dots, f_r$. However, as in the case of $I^{[\Sigma]}$, if the generators $f_1, \dots, f_r$ are clear from the context, we omit this part and only speak of "a signature Gröbner basis $G^{[\Sigma]}$ (of $I^{[\Sigma]}$) (up to signature σ)".

It follows directly from the definition that a signature Gröbner basis of $I^{[\Sigma]}$ is by no means unique. In fact, if $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then so is $G^{[\Sigma]} \cup \{f^{[\alpha]}\}$ for every $f^{[\alpha]} \in I^{[\Sigma]}$. Furthermore, the set $I^{[\Sigma]}$ is always a signature Gröbner basis of $I^{[\Sigma]}$. Thus, we can immediately deduce the following corollary.

Corollary 20. *For every finite set of generators of an ideal* $I \subseteq K\langle X\rangle$*, the module* $I^{[\Sigma]}$ *has a (possibly infinite) signature Gröbner basis.*

We also provide the following equivalent characterization of signature Gröbner basis, which will turn out to be useful later.

Lemma 21. *A set* $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ *is a signature Gröbner basis of* $I^{[\Sigma]}$ *if and only if every* $f^{[\alpha]} \in I^{[\Sigma]}$ *is top* $\mathfrak{s}$*-reducible by* $G^{[\Sigma]}$.

Proof. The "only if"-direction of this statement is clear. For the "if"-direction, let $G^{[\Sigma]}$ be such that every $f^{[\alpha]} \in I^{[\Sigma]}$ is top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$ and assume that there exists a signature polynomial which does not $\mathfrak{s}$-reduce to zero. Let $f^{[\alpha]}$ be such an element with minimal leading monomial. Then, by assumption we can top $\mathfrak{s}$-reduce $f^{[\alpha]}$ to some $f'^{[\alpha']}$ with either $f' = 0$ or $\mathrm{lm}(f') \prec \mathrm{lm}(f)$. We note that $f' = 0$ is a contradiction to the assumption that $f^{[\alpha]}$ does not $\mathfrak{s}$-reduce to zero. On the other hand, if $\mathrm{lm}(f') \prec \mathrm{lm}(f)$, then $f'^{[\alpha']}$ can be $\mathfrak{s}$-reduced to zero by $G^{[\Sigma]}$ since $\mathrm{lm}(f)$ was chosen to be minimal, but this is again a contradiction to $f^{[\alpha]}$ not being $\mathfrak{s}$-reducible to zero. □

The following proposition relates signature Gröbner bases to Gröbner bases and is an immediate consequence of Lemma 14.

Proposition 22. *Let* $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ *be a signature Gröbner basis of* $I^{[\Sigma]}$*. Then,* $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\} \subseteq K\langle X\rangle$ *is a Gröbner basis of* I.

Although a signature Gröbner basis $G^{[\Sigma]}$ of $I^{[\Sigma]}$ is not unique in general – not even for a fixed set of generators –, we can demand certain additional properties from $G^{[\Sigma]}$ in order to at least obtain a signature Gröbner basis which is as small as possible. We call such a signature Gröbner basis a *minimal signature Gröbner basis* of $I^{[\Sigma]}$.

Definition 23. Let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis of $I^{[\Sigma]}$ (up to some signature $\sigma \in \mathbb{M}(\mathcal{F}_r)$). Then, $G^{[\Sigma]}$ is called a *minimal signature Gröbner basis of $I^{[\Sigma]}$ (up to signature σ)* if no $g^{[\gamma]} \in G^{[\Sigma]}$ can be top $\mathbb{s}$-reduced by $G^{[\Sigma]} \setminus \{g^{[\gamma]}\}$.

A minimal signature Gröbner basis is minimal in the following sense.

Proposition 24. *Let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a minimal signature Gröbner basis and $H^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis of $I^{[\Sigma]}$. Then, for every $g^{[\gamma]} \in G^{[\Sigma]}$ there exists $h^{[\delta]} \in H^{[\Sigma]}$ such that*

$$\operatorname{lm}(g) = \operatorname{lm}(h) \quad \textit{and} \quad \mathbb{s}(\gamma) = \mathbb{s}(\delta).$$

Proof. Let $g^{[\gamma]} \in G^{[\Sigma]}$. Since $H^{[\Sigma]}$ is a signature Gröbner basis, $g^{[\gamma]}$ can be $\mathbb{s}$-reduced to zero by $H^{[\Sigma]}$. In particular, this means that $g^{[\gamma]}$ is top $\mathbb{s}$-reducible by $H^{[\Sigma]}$, that is, there exist $h^{[\delta]} \in H^{[\Sigma]}$ and $a, b \in \langle X \rangle$ such that

$$\operatorname{lm}(g) = \operatorname{lm}(ahb) \quad \text{and} \quad \mathbb{s}(\gamma) \geq \mathbb{s}(a\delta b).$$

Similarly, since $G^{[\Sigma]}$ is also a signature Gröbner basis, there exist $g'^{[\gamma']} \in G^{[\Sigma]}$ and $a', b' \in \langle X \rangle$ such that

$$\operatorname{lm}(h) = \operatorname{lm}(a'g'b') \quad \text{and} \quad \mathbb{s}(\delta) \geq \mathbb{s}(a'\gamma'b').$$

Combining these two statements yields

$$\operatorname{lm}(g) = \operatorname{lm}(ahb) = \operatorname{lm}(aa'g'b'b) \quad \text{and} \quad \mathbb{s}(\gamma) \geq \mathbb{s}(a\delta b) \geq \mathbb{s}(aa'\gamma'b'b).$$

Now, if $g^{[\gamma]} \neq g'^{[\gamma']}$, then $g'^{[\gamma']}$ could be used to top $\mathbb{s}$-reduce $g^{[\gamma]}$ but this is a contradiction to the fact that $G^{[\Sigma]}$ is a minimal Gröbner basis. So, $g^{[\gamma]} = g'^{[\gamma']}$, which implies that $a = a' = b = b' = 1$, and therefore,

$$\operatorname{lm}(g) = \operatorname{lm}(h) \quad \text{and} \quad \mathbb{s}(\gamma) = \mathbb{s}(\delta). \qquad \square$$

We note that, starting with a finite set of generators $\{f_1, \ldots, f_r\}$ of an ideal $I \subseteq K\langle X \rangle$, the module $I^{[\Sigma]}$ always has a minimal signature Gröbner basis, which is finite if and only if $I^{[\Sigma]}$ has a finite signature Gröbner basis w.r.t. the generators $f_1, \ldots, f_r$. This follows from the following proposition, which tells us that we can obtain a minimal signature Gröbner basis from a signature Gröbner basis by removing all elements that are top $\mathbb{s}$-reducible.

Proposition 25. *Let $G^{[\Sigma]} \in I^{[\Sigma]}$ be a signature Gröbner basis of $I^{[\Sigma]}$ such that there exists $g^{[\gamma]} \in G^{[\Sigma]}$ which is top $\mathbb{s}$-reducible by $G^{[\Sigma]} \setminus \{g^{[\gamma]}\}$. Then, $G^{[\Sigma]} \setminus \{g^{[\gamma]}\}$ is also a signature Gröbner basis of $I^{[\Sigma]}$.*

Proof. If $g^{[\gamma]}$ is top $\mathbb{s}$-reducible by $G^{[\Sigma]} \setminus \{g^{[\gamma]}\}$, then there exist $g'^{[\gamma']} \in G^{[\Sigma]} \setminus \{g^{[\gamma]}\}$ and $a, b \in \langle X \rangle$ such that

$$\operatorname{lm}(g) = \operatorname{lm}(ag'b) \quad \text{and} \quad \mathbb{s}(\gamma) \leq \mathbb{s}(a\gamma'b).$$

So, every element $f^{[\alpha]} \in I^{[\Sigma]}$ which is top $\mathbb{s}$-reducible by $g^{[\gamma]}$ is also top $\mathbb{s}$-reducible by $g'^{[\gamma']}$. Consequently, it follows from Lemma 21 that $G^{[\Sigma]} \setminus \{g^{[\gamma]}\}$ is also a signature Gröbner basis of $I^{[\Sigma]}$. $\square$

Corollary 26. *The module $I^{[\Sigma]}$ has a finite signature Gröbner basis if and only if $I^{[\Sigma]}$ has a finite minimal signature Gröbner basis. Furthermore, all minimal signature Gröbner bases of $I^{[\Sigma]}$ have the same cardinality.*

Proof. If $I^{[\Sigma]}$ has a finite signature Gröbner basis $G^{[\Sigma]}$, then, applying Proposition 25 repeatedly, $G^{[\Sigma]}$ contains a minimal signature Gröbner basis of $I^{[\Sigma]}$ as a subset. The converse is clear.

For the last statement, assume that $G_1^{[\Sigma]}$ and $G_2^{[\Sigma]}$ are minimal signature Gröbner bases of $I^{[\Sigma]}$. If they are both infinite, they have the same (countable) cardinality. Otherwise, assume that $G_1^{[\Sigma]}$ is finite. Define the sets R_1 and R_2 by

$$R_i = \{(\mathrm{lm}(g), \mathfrak{s}(\gamma)) \mid g^{[\gamma]} \in G_i^{[\Sigma]}\}.$$

By Proposition 24, $R_1 \subseteq R_2$ and $R_2 \subseteq R_1$, so $R_1 = R_2$. We claim that the cardinality of $G_1^{[\Sigma]}$ and $G_2^{[\Sigma]}$ is equal to that of R_1.

Indeed, assume that it is not the case. W.l.o.g. we can assume that $G_1^{[\Sigma]}$ is larger than R_1, so by the pidgeonhole principle, there exist $g^{[\gamma]}$ and $h^{[\delta]}$ in $G_1^{[\Sigma]}$, distinct, such that $\mathrm{lm}(g) = \mathrm{lm}(h)$ and $\mathfrak{s}(\gamma) = \mathfrak{s}(\delta)$. Then by definition, $h^{[\delta]}$ is top $\mathfrak{s}$-reducible by $g^{[\gamma]}$, which contradicts the minimality of $G_1^{[\Sigma]}$. □

However, we cannot expect $I^{[\Sigma]}$ to have a finite (minimal) signature Gröbner basis for any finitely generated ideal $I \subseteq K\langle X\rangle$, as there are finitely generated ideals that simply do not have a finite Gröbner basis, and consequently, also no finite signature Gröbner basis. Unfortunately, the condition that an ideal $I = (f_1, \dots, f_r)$ has a finite Gröbner basis is also not sufficient to ensure that $I^{[\Sigma]}$ has a finite signature Gröbner basis w.r.t. the generators $f_1, \dots, f_r$ as the following example shows.

Example 27. Let K be any field, $X = \{x, y\}$ and let

$$f_1 = xyx - xy, \qquad f_2 = yxy, \qquad f_3 = xyy - xxy \in K\langle X\rangle.$$

We consider the ideal $I = (f_1, f_2, f_3)$ and equip $K\langle X\rangle$ with $\preceq_{deglex}$ where we order the indeterminates as $x \prec_{lex} y$. Furthermore, we use $\preceq_{\mathbf{top}}$ as a module ordering. Then, it is not too hard to see that $G = \{f_1, f_2, f_3, f_4\}$, where $f_4 = xxy$, is a Gröbner basis of I. Moreover, we claim that the infinite set

$$G^{[\Sigma]} = \{f_1^{[\varepsilon_1]}, f_2^{[\varepsilon_2]}, f_3^{[\varepsilon_3]}, f_4^{[\alpha]}\} \cup \{g_n^{[\gamma_n]} \mid n \geq 0\},$$

with $g_n = yx^{n+2}y$ and certain $\alpha, \gamma_n \in \mathcal{F}_r$ such that $\mathfrak{s}(\alpha) = \varepsilon_1 y$ and $\mathfrak{s}(\gamma_n) = y\varepsilon_3 y^n$, is a minimal signature Gröbner basis of $I^{[\Sigma]}$ w.r.t. the generators f_1, f_2, f_3. This, according to Corollary 26 implies that $I^{[\Sigma]}$ does not have a finite signature Gröbner basis w.r.t. this set of generators.

To prove our claim, we note that $f_4^{[\alpha]}$ cannot be used to $\mathfrak{s}$-reduce $f_3^{[\varepsilon_3]}$ or $g_n^{[\gamma_n]}$ because these reductions would increase the respective signatures as $\mathfrak{s}(\alpha) \succ \varepsilon_3$ and $yx^n\,\mathfrak{s}(\alpha) \succ \mathfrak{s}(\gamma_n)$, respectively. Consequently, no element in $G^{[\Sigma]}$ can be top $\mathfrak{s}$-reduced by any other element in $G^{[\Sigma]}$. The final step, to show that $G^{[\Sigma]}$ is also a signature Gröbner basis, is done in Appendix A.

We finish this example here by noting that if we consider the set of generators $\{f_1, f_2, f_3, f_4\}$, then the finite set

$$\tilde{G}^{[\Sigma]} = \{f_1^{[\varepsilon_1]}, f_2^{[\varepsilon_2]}, f_3^{[\varepsilon_3]}, f_4^{[\varepsilon_4]}\} \cup \{yxxy^{[\gamma_0]}\}$$

with $\mathfrak{s}(\gamma_0) = y\varepsilon_3$ is a minimal signature Gröbner basis of $I^{[\Sigma]}$ w.r.t. f_1, f_2, f_3, f_4. As before, no element in $\tilde{G}^{[\Sigma]}$ can be top $\mathfrak{s}$-reduced by any other element. We show in Appendix A that also $\tilde{G}^{[\Sigma]}$

is a signature Gröbner basis. Here, we conclude with the following two insights. First of all, $I^{[\Sigma]}$ need not have a finite signature Gröbner basis w.r.t. to a specific set of generators, even if I has a finite Gröbner basis, and secondly, different choices of generators of I can lead to drastically different (minimal) signature Gröbner bases of $I^{[\Sigma]}$.

4. Computation of signature Gröbner bases

4.1. Regular S-polynomials

The objective of this section is to state an adaptation of the noncommutative version of Buchberger's algorithm to include signatures. To this end, we need to adapt the notion of S-polynomials to the case of signature polynomials. We first extend the notion of *ambiguities* from [Ber78] from polynomials to signature polynomials. Recall that we fixed a set of generators $\{f_1, \ldots, f_r\} \subseteq K\langle X\rangle$ of an ideal $I = (f_1, \ldots, f_r)$ as well as a monomial and a module ordering.

Definition 28. Let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ and let $f^{[\alpha]}, g^{[\beta]} \in G^{[\Sigma]}$ be such that $f, g \neq 0$. If $\mathrm{lm}(f) = AB$ and $\mathrm{lm}(g) = BC$ for some words $A, B, C \in \langle X\rangle \setminus \{1\}$, then we call the tuple

$$(ABC, A, C, f^{[\alpha]}, g^{[\beta]})$$

an *overlap ambiguity* of $G^{[\Sigma]}$. We define its *S-polynomial* $\mathrm{sp}(a)$ to be

$$\mathrm{sp}(a) := \frac{1}{\mathrm{lc}(f)} f^{[\alpha]} C - \frac{1}{\mathrm{lc}(g)} A g^{[\beta]}.$$

Similarly, if $f \neq g$, $\mathrm{lm}(f) = ABC$ and $\mathrm{lm}(g) = B$ for some words $A, B, C \in \langle X\rangle$, then we call the tuple

$$(ABC, A, C, f^{[\alpha]}, g^{[\beta]})$$

an *inclusion ambiguity* of $G^{[\Sigma]}$. We define its *S-polynomial* $\mathrm{sp}(a)$ to be

$$\mathrm{sp}(a) := \frac{1}{\mathrm{lc}(f)} f^{[\alpha]} - \frac{1}{\mathrm{lc}(g)} A g^{[\beta]} C.$$

We remark that two signature polynomials can have more than one ambiguity with each other. Furthermore, an element can also form overlap ambiguities with itself. Note that in the noncommutative case, we only form S-polynomials in the presence of an ambiguity, which effectively embeds Buchberger's coprime criterion in the definition. This ensures that two signature polynomials can only give rise to finitely many S-polynomials.

An ambiguity $a = (ABC, A, C, f^{[\alpha]}, g^{[\beta]})$ is called *singular* if

$$\mathfrak{s}(\alpha C) = \mathfrak{s}(A\beta)$$

in case that a is an overlap ambiguity, respectively if

$$\mathfrak{s}(\alpha) = \mathfrak{s}(A\beta C)$$

in case that a is an inclusion ambiguity. We call an S-polynomial *regular/singular*, if the respective ambiguity is regular/singular.

In the following, we collect some useful results about S-polynomials. We start by relating the signature of a regular S-polynomial to the signatures of the two input elements. This first corollary is an immediate consequence of the definition of a regular ambiguity.

Corollary 29. *Let $a = (ABC, A, C, f^{[\alpha]}, g^{[\beta]})$ be a regular ambiguity of a set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$. Then,*

$$\mathbb{s}(\mathrm{sp}(a)) \geq \max_{\leq}\{\mathbb{s}(\alpha), \mathbb{s}(\beta)\}.$$

Lemma 30. *Let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ and let $f^{[\alpha]} \in I^{[\Sigma]}$. Assume that $f^{[\alpha]}$ is not top $\mathbb{s}$-reducible by $G^{[\Sigma]}$. Then, any regular S-polynomial between $f^{[\alpha]}$ and any element in $G^{[\Sigma]}$ has signature strictly larger than $\mathbb{s}(\alpha)$.*

Proof. Let $a = (ABC, A, C, f_1^{[\alpha_1]}, f_2^{[\alpha_2]})$ be a regular ambiguity between $f^{[\alpha]}$ and some element $g^{[\gamma]} \in G^{[\Sigma]}$, i.e.

$$f_1^{[\alpha_1]} = f^{[\alpha]} \text{ and } f_2^{[\alpha_2]} = g^{[\gamma]} \qquad \text{or} \qquad f_1^{[\alpha_1]} = g^{[\gamma]} \text{ and } f_2^{[\alpha_2]} = f^{[\alpha]}.$$

According to Corollary 29, we have $\mathbb{s}(\mathrm{sp}(a)) \geq \mathbb{s}(\alpha)$. Assume for contradiction that $\mathbb{s}(\mathrm{sp}(a)) = \mathbb{s}(\alpha)$. Then, a cannot be an overlap ambiguity as otherwise

$$\mathbb{s}(\alpha) = \mathbb{s}(\mathrm{sp}(a)) = \max_{\leq}\{\mathbb{s}(\alpha_1 C), \mathbb{s}(A\alpha_2)\} > \max_{\leq}\{\mathbb{s}(\alpha_1), \mathbb{s}(\alpha_2)\} \geq \mathbb{s}(\alpha),$$

where the strict inequality follows from the fact that $A, C \neq 1$. So, a must be an inclusion ambiguity. Now, we distinguish between the cases whether $f_1^{[\alpha_1]} = f^{[\alpha]}$ or $f_2^{[\alpha_2]} = f^{[\alpha]}$. If $f_1^{[\alpha_1]} = f^{[\alpha]}$ and $\mathbb{s}(\mathrm{sp}(a)) = \mathbb{s}(\alpha)$, then $\mathrm{lm}(f) = \mathrm{lm}(AgC)$ and $\mathbb{s}(\alpha) \geq \mathbb{s}(A\gamma C)$. Consequently, $f^{[\alpha]}$ is top $\mathbb{s}$-reducible by $g^{[\gamma]}$, which is a contradiction. If $f_2^{[\alpha_2]} = f^{[\alpha]}$ and $\mathbb{s}(\mathrm{sp}(a)) = \mathbb{s}(\alpha)$, then

$$\mathbb{s}(\alpha) = \mathbb{s}(\mathrm{sp}(a)) = \max_{\leq}\{\mathbb{s}(\gamma), \mathbb{s}(A\alpha C)\} \geq \mathbb{s}(A\alpha C).$$

Therefore, we can conclude that $A = C = 1$. So, $\mathrm{lm}(f) = \mathrm{lm}(AgC) = \mathrm{lm}(g)$ and $\mathbb{s}(\alpha) \geq \mathbb{s}(\gamma)$, showing again that $f^{[\alpha]}$ is top $\mathbb{s}$-reducible by $g^{[\gamma]}$, which is a contradiction. □

4.2. *Characterization of signature Gröbner bases*

As in the commutative case, the design and the proof of correctness of the algorithm will rely on a signature variant of Buchberger's characterization of Gröbner bases, stating that if all *regular* S-polynomials $\mathbb{s}$-reduce to zero, then one has a signature Gröbner basis.

A particularity of the noncommutative case is that we will need to handle trivial syzygies separately in the proof process. This is because the noncommutative definition of S-polynomials (Definition 28) effectively contains the restrictions granted by Buchberger's coprime criterion, eliminating some trivial syzygies. Without those restrictions, the algorithms (even without signatures) would rarely terminate, because the module of trivial syzygies is in general not finitely generated.

In order to prove the noncommutative characterization of signature Gröbner bases, we prove several lemmas. Leaving aside the provisions for trivial syzygies, we first prove Lemma 31, which states that given a regular linear combination of two signature polynomials eliminating their leading terms, one can find a regular S-polynomial whose signature divides the signature of that syzygy of the leading terms. This lemma is technical and useful for the rest of the proofs. It ensures that is suffices to consider regular S-polynomials.

Then, we prove Lemma 32, which states that given an S-polynomial $p^{[\pi]}$, one can find a multiple a regular S-polynomial with the same signature $\mathbb{s}(\pi)$ satisfying certain additional conditions concerning its $\mathbb{s}$-reducibility. This allows us to prove Lemma 33, which makes the same statement, but starting from any polynomial. This last lemma is a noncommutative analogue of Lemma 9 in [RS12, appendix]. Just like in the commutative case, it is the cornerstone of the proof of the final Theorem 34, which is the wanted characterization.

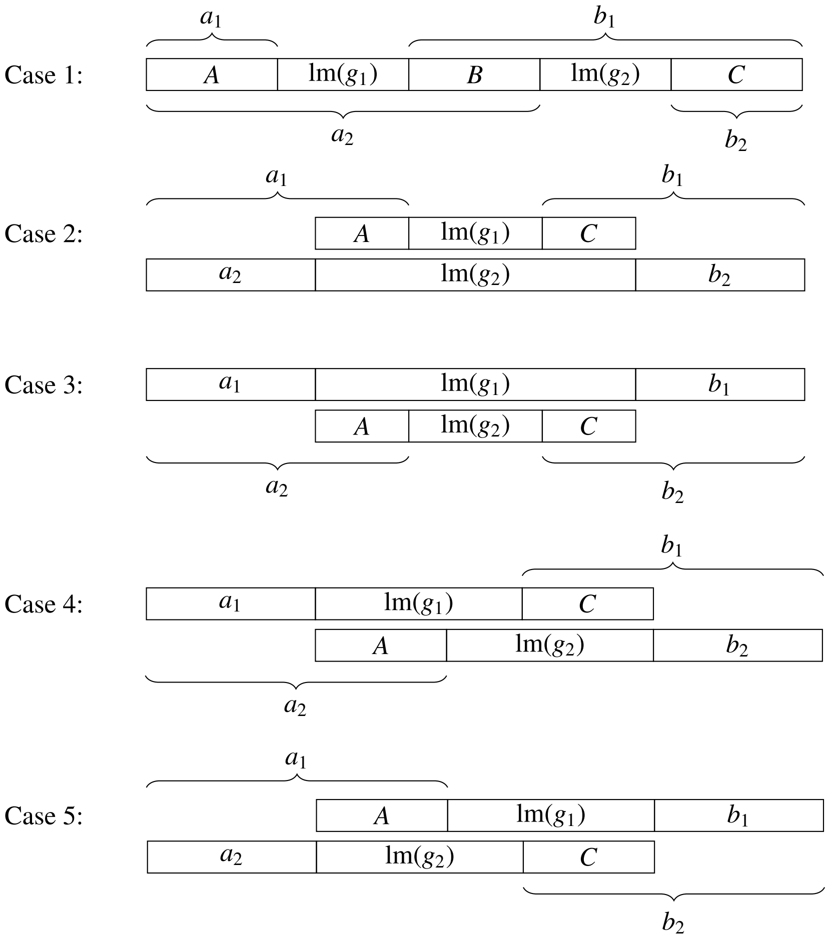

Figure 1: Relative position of $\mathrm{lm}(g_1)$ and $\mathrm{lm}(g_2)$ in the proof of Lemma 31

Lemma 31. *Let $g_1^{[\gamma_1]}, g_2^{[\gamma_2]} \in I^{[\Sigma]}$ and let $a_1, a_2, b_1, b_2 \in \langle X \rangle$ such that*

$$\mathrm{lm}(a_1 g_1 b_1) = \mathrm{lm}(a_2 g_2 b_2) \quad \text{and} \quad \mathfrak{s}(a_1 \gamma_1 b_1) \succ \mathfrak{s}(a_2 \gamma_2 b_2).$$

Then, there exist $p^{[\pi]} \in I^{[\Sigma]}$ and $a, b \in \langle X \rangle$ such that $\mathfrak{s}(a\pi b) = \mathfrak{s}(a_1 \gamma_1 b_1)$ and such that one of the following conditions holds:

1. *π is a trivial syzygy between $g_1^{[\gamma_1]}$ and $g_2^{[\gamma_2]}$;*
2. *$p^{[\pi]}$ is a regular S-polynomial of $g_1^{[\gamma_1]}$ and $g_2^{[\gamma_2]}$ with $p = 0$ or $\mathrm{lm}(apb) \prec \mathrm{lm}(a_1 g_1 b_1)$.*

Proof. We distinguish between different cases (see Figure 1), depending on the position of $\mathrm{lm}(g_1)$ and $\mathrm{lm}(g_2)$ relative to each other in $W = \mathrm{lm}(a_1 g_1 b_1) = \mathrm{lm}(a_2 g_2 b_2)$.

Case 1: $\mathrm{lm}(g_1)$ *is fully contained in* a_2 *or* b_2. In this case, $\mathrm{lm}(g_1)$ and $\mathrm{lm}(g_2)$ do not overlap in W. We only consider the case where $\mathrm{lm}(g_1)$ is contained in a_2, i.e. where $W = A\,\mathrm{lm}(g_1)B\,\mathrm{lm}(g_2)C$ for some $A, B, C \in \langle X\rangle$, and note that the other case works along the same lines. We let

$$0^{[\pi]} = g_1^{[\gamma_1]}Bg_2 - g_1Bg_2^{[\gamma_2]}.$$

Then π is a trivial syzygy between $g_1^{[\gamma_1]}$ and $g_2^{[\gamma_2]}$. To prove the assertion regarding the signatures, we note that $\mathbb{s}(\pi) = \mathbb{s}(\gamma_1 Bg_2) \succ \mathbb{s}(g_1B\gamma_2)$ as $A\,\mathbb{s}(g_1B\gamma_2)C = \mathbb{s}(Am_1B\gamma_2C) = \mathbb{s}(a_2\gamma_2b_2) \prec \mathbb{s}(a_1\gamma_1b_1) = \mathbb{s}(A\gamma_1Bm_2C) = A\,\mathbb{s}(\gamma_1Bg_2)C$. Hence, by setting $a = A$ and $b = C$, we obtain $\mathbb{s}(a\pi b) = \mathbb{s}(A\pi C) = \mathbb{s}(A\gamma_1Bg_2C) = \mathbb{s}(a_1\gamma_1b_1)$.

Case 2: $\mathrm{lm}(g_1)$ *is fully contained in* $\mathrm{lm}(g_2)$. In this case, there exists an inclusion ambiguity with S-polynomial

$$p^{[\pi]} = \frac{1}{\mathrm{lc}(g_2)}g_2^{[\gamma_2]} - \frac{1}{\mathrm{lc}(g_1)}Ag_1^{[\gamma_1]}C.$$

Since $a_2\,\mathbb{s}(\gamma_2)b_2 = \mathbb{s}(a_2\gamma_2b_2) \prec \mathbb{s}(a_1\gamma_1b_1) = a_2\,\mathbb{s}(A\gamma_1C)b_2$, we get that $\mathbb{s}(\pi) = \mathbb{s}(A\gamma_1C) \succ \mathbb{s}(\gamma_2)$. So, the S-polynomial is regular, and with $a = a_2$ and $b = b_2$ we have $\mathbb{s}(a\pi b) = \mathbb{s}(a_2A\gamma_1Cb_2) = \mathbb{s}(a_1\gamma_1b_1)$ and $\mathrm{lm}(apb) \prec \mathrm{lm}(ag_2b) = \mathrm{lm}(a_2g_2b_2) = \mathrm{lm}(a_1g_1b_1)$, in case $p \neq 0$.

Case 3: $\mathrm{lm}(g_2)$ *is fully contained in* $\mathrm{lm}(g_1)$. In this case, there exists an inclusion ambiguity with S-polynomial

$$p^{[\pi]} = \frac{1}{\mathrm{lc}(g_1)}g_1^{[\gamma_1]} - \frac{1}{\mathrm{lc}(g_2)}Ag_2^{[\gamma_2]}C$$

with $\mathbb{s}(\pi) = \mathbb{s}(\gamma_1) \succ \mathbb{s}(A\gamma_2C)$ as $a_1\,\mathbb{s}(A\gamma_2C)b_1 = \mathbb{s}(a_2\gamma_2b_2) \prec \mathbb{s}(a_1\gamma_1b_1) = a_1\,\mathbb{s}(\gamma_1)b_1$. So, the S-polynomial is regular, and with $a = a_1$ and $b = b_1$ we have $\mathbb{s}(a\pi b) = \mathbb{s}(a_1\gamma_1b_1)$ and $\mathrm{lm}(apb) \prec \mathrm{lm}(ag_1b) = \mathrm{lm}(a_1g_1b_1)$, in case $p \neq 0$.

Case 4: $\mathrm{lm}(g_1)$ *and* $\mathrm{lm}(g_2)$ *overlap but are not fully contained in one another and* $\mathrm{lm}(g_1)$ *begins before* $\mathrm{lm}(g_2)$. In this case, there exists an overlap ambiguity with S-polynomial

$$p^{[\pi]} = \frac{1}{\mathrm{lc}(g_1)}g_1^{[\gamma_1]}C - \frac{1}{\mathrm{lc}(g_2)}Ag_2^{[\gamma_2]}$$

with $\mathbb{s}(\pi) = \mathbb{s}(\gamma_1C) \succ \mathbb{s}(A\gamma_2)$ as $a_1\,\mathbb{s}(A\gamma_2)b_2 = \mathbb{s}(a_2\gamma_2b_2) \prec \mathbb{s}(a_1\gamma_1b_1) = a_1\,\mathbb{s}(\gamma_1C)b_2$. So, the S-polynomial is regular, and with $a = a_1$ and $b = b_2$ we have $\mathbb{s}(a\pi b) = \mathbb{s}(a_1\gamma_1Cb_2) = \mathbb{s}(a_1\gamma_1b_1)$ and $lm(apb) \prec \mathrm{lm}(ag_1Cb) = \mathrm{lm}(a_1g_1Cb_2) = \mathrm{lm}(a_1g_1b_1)$, in case $p \neq 0$.

Case 5: $\mathrm{lm}(g_1)$ *and* $\mathrm{lm}(g_2)$ *overlap but are not fully contained in one another and* $\mathrm{lm}(g_1)$ *begins after* $\mathrm{lm}(g_2)$. In this case, there exists an overlap ambiguity with S-polynomial

$$p^{[\pi]} = \frac{1}{\mathrm{lc}(g_2)}g_2^{[\gamma_2]}C - \frac{1}{\mathrm{lc}(g_1)}Ag_1^{[\gamma_1]}$$

with $\mathbb{s}(\pi) = \mathbb{s}(A\gamma_1) \succ \mathbb{s}(\gamma_2C)$ as $a_2\,\mathbb{s}(\gamma_2C)b_1 = \mathbb{s}(a_2\gamma_2b_2) \prec \mathbb{s}(a_1\gamma_1b_1) = a_2\,\mathbb{s}(A\gamma_1)b_1$. So, the S-polynomial is regular and with $a = a_2$ and $b = b_1$ we have $\mathbb{s}(a\pi b) = \mathbb{s}(a_2A\gamma_1b_1) = \mathbb{s}(a_1\gamma_1b_1)$ and $\mathrm{lm}(apb) \prec \mathrm{lm}(aAg_1b) = \mathrm{lm}(a_2Ag_1b_1) = \mathrm{lm}(a_1g_1b_1)$, in case $p \neq 0$. □

Lemma 32. *Let $p^{[\pi]} \in I^{[\Sigma]}$ be an S-polynomial of $G^{[\Sigma]}$. Furthermore, assume that there exist $a, b \in \langle X\rangle$ such that all $u^{[\mu]} \in I^{[\Sigma]}$ with $\mathbb{s}(\mu) \prec \mathbb{s}(a\pi b)$ $\mathbb{s}$-reduce to zero by $G^{[\Sigma]}$. Then, there exist $q^{[\rho]} \in I^{[\Sigma]}$ and $a', b' \in \langle X\rangle$ such that $\mathbb{s}(a'\rho b') = \mathbb{s}(a\pi b)$ and such that one of the following conditions holds.*

1. *ρ is a trivial syzygy between two elements in $G^{[\Sigma]}$,*
2. *$q^{[\rho]}$ is a regular S-polynomial of $G^{[\Sigma]}$ and $a'q'^{[\rho']}b'$ is not regular top $\mathfrak{s}$-reducible where $q'^{[\rho']}$ is the result of regular $\mathfrak{s}$-reducing $q^{[\rho]}$.*

Proof. Let $p'^{[\pi']}$ be the result of regular $\mathfrak{s}$-reducing $p^{[\pi]}$. We can assume that $ap'^{[\pi']}b$ is regular top $\mathfrak{s}$-reducible because otherwise we are done. This means that $ab \neq 1$, and therefore, that $\mathfrak{s}(\pi') = \mathfrak{s}(\pi) \prec a\,\mathfrak{s}(\pi)b = \mathfrak{s}(a\pi b)$. Hence, $p^{[\pi]}$, as well as $p'^{[\pi']}$, $\mathfrak{s}$-reduce to zero by $G^{[\Sigma]}$.

We are now going to construct $q^{[\rho]} \in I^{[\Sigma]}$ such that there exist $a', b' \in \langle X \rangle$ with $\mathfrak{s}(a'\rho b') = \mathfrak{s}(a\pi b)$ and

1. ρ is a trivial syzygy between two elements in $G^{[\Sigma]}$, or
2. $q^{[\rho]}$ is an S-polynomial with $q = 0$ or $\operatorname{lm}(a'qb') \prec \operatorname{lm}(apb)$.

If $q^{[\rho]}$ is a trivial syzygy or not regular top $\mathfrak{s}$-reducible, we are done. Otherwise we can repeat this process to construct a third signature polynomial with the same properties. This process must terminate at some point since $\prec$ is a well-ordering.

We note that $p' \neq 0$ because otherwise $ap'^{[\pi']}b$ would not be regular top $\mathfrak{s}$-reducible. Then, since $p'^{[\pi']}$ is regular $\mathfrak{s}$-reduced but $\mathfrak{s}$-reduces to zero, $p'^{[\pi']}$ must be singular top $\mathfrak{s}$-reducible. Hence, there exist $g_1^{[\gamma_1]} \in G^{[\Sigma]}$ and $a_1, b_1 \in \langle X \rangle$ such that

$$\operatorname{lm}(a_1 g_1 b_1) = \operatorname{lm}(p') \quad \text{and} \quad \mathfrak{s}(a_1\gamma_1 b_1) = \mathfrak{s}(\pi') = \mathfrak{s}(\pi).$$

Furthermore, as $ap'^{[\pi']}b$ is regular top $\mathfrak{s}$-reducible, there exist $g_2^{[\gamma_2]} \in G^{[\Sigma]}$ and $a_2, b_2 \in \langle X \rangle$ such that

$$\operatorname{lm}(a_2 g_2 b_2) = \operatorname{lm}(ap'b) \quad \text{and} \quad \mathfrak{s}(a_2\gamma_2 b_2) \prec \mathfrak{s}(a\pi' b) = \mathfrak{s}(a\pi b).$$

To summarize, we have

$$\begin{aligned} \operatorname{lm}(aa_1 g_1 b_1 b) &= \operatorname{lm}(ap'b) = \operatorname{lm}(a_2 g_2 b_2) \prec \operatorname{lm}(apb), \\ \mathfrak{s}(aa_1\gamma_1 b_1 b) &= \mathfrak{s}(a\pi b) \succ \mathfrak{s}(a_2\gamma_2 b_2). \end{aligned}$$

Now, the existence of $a', b' \in \langle X \rangle$ and $q^{[\rho]}$ with the required properties follows from Lemma 31. □

Lemma 33. *Let $h^{[\delta]} \in I^{[\Sigma]}$ be top $\mathfrak{s}$-reduced by $G^{[\Sigma]}$. Assume that for all $i = 1, \dots, r$ with $\varepsilon_i \preceq \mathfrak{s}(\mu)$ there exists $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\mathfrak{s}(\gamma_i) = \varepsilon_i$. Furthermore, assume that all $u^{[\mu]} \in I^{[\Sigma]}$ with $\mathfrak{s}(\mu) \prec \mathfrak{s}(\delta)$ $\mathfrak{s}$-reduce to zero by $G^{[\Sigma]}$. Then, there exist $p^{[\pi]} \in I^{[\Sigma]}$ and $a, b \in \langle X \rangle$ such that $\mathfrak{s}(\delta) = \mathfrak{s}(a\pi b)$ and such that one of the following conditions holds.*

1. *π is a trivial syzygy between two elements in $G^{[\Sigma]}$,*
2. *$p^{[\pi]}$ is a regular S-polynomial of $G^{[\Sigma]}$ and $ap'^{[\pi']}b$ is not regular top $\mathfrak{s}$-reducible where $p'^{[\pi']}$ is the result of regular $\mathfrak{s}$-reducing $p^{[\pi]}$.*

Proof. The proof follows the same structure as that of [RS12, Lemma 9, appendix]: first, we combine leading terms to show that there exists $L^{[\lambda]} \in I^{[\Sigma]}$ with signature dividing that of δ, and then, starting from that element, we construct $p^{[\pi]}$ as wanted.

Considering leading terms. Let $\mathbb{s}(\delta) = a_1\varepsilon_i b_1$ for some $1 \leq i \leq r$ and $a_i, b_i \in \langle X\rangle$. By our assumption on $G^{[\Sigma]}$ there exists $g_1^{[\gamma_1]} \in G^{[\Sigma]}$ such that $\mathbb{s}(\gamma_1) = \varepsilon_i$. Let $\lambda = ca_1\gamma_1 b_1$ with $c = \frac{\mathbb{sc}(\delta)}{\mathbb{sc}(\gamma_1)}$ and observe that $\mathbb{st}(\lambda) = \mathbb{st}(\delta)$. Then, with $L = \overline{\lambda}$, the signature polynomial $h^{[\delta]} - L^{[\lambda]}$ has a strictly smaller signature than $h^{[\delta]}$, so it $\mathbb{s}$-reduces to zero by $G^{[\Sigma]}$ and in particular it is top $\mathbb{s}$-reducible. Clearly, also $L^{[\lambda]} = ca_1 g_1^{[\gamma_1]} b_1$ is top $\mathbb{s}$-reducible by $g_1^{[\gamma_1]}$. However, the sum $h^{[\delta]} = (h^{[\delta]} - L^{[\lambda]}) + L^{[\lambda]}$ is not top $\mathbb{s}$-reducible by assumption. So, Lemma 16 yields that

$$\mathrm{lt}(h - L) + \mathrm{lt}(L) = 0.$$

Constructing $p^{[\pi]}$. Since $h^{[\delta]} - L^{[\lambda]}$ $\mathbb{s}$-reduces to zero by $G^{[\Sigma]}$, there exists a $g_2^{[\gamma_2]} \in G^{[\Sigma]}$ and $a_2, b_2 \in \langle X\rangle$ such that

$$\mathrm{lm}(a_2 g_2 b_2) = \mathrm{lm}(h - L) \quad \text{and} \quad \mathbb{s}(a_2\gamma_2 b_2) \preceq \mathbb{s}(\delta - \lambda) \prec \mathbb{s}(\delta).$$

Hence, with $a_1, b_1, g_1^{[\gamma_1]}$ from above, we have

$$\begin{aligned} \mathrm{lm}(a_1 g_1 b_1) &= \mathrm{lm}(L) = \mathrm{lm}(h - L) = \mathrm{lm}(a_2 g_2 b_2), \\ \mathbb{s}(a_1\gamma_1 b_1) &= \mathbb{s}(\delta) \succ \mathbb{s}(\delta - \lambda) \succeq \mathbb{s}(a_2\gamma_2 b_2). \end{aligned}$$

Then, Lemma 31 and Lemma 32 yield the existence of $a, b \in \langle X\rangle$ and $p^{[\pi]}$ with the required properties. □

We can now finally state and prove the following theorem.

Theorem 34. *Let $\sigma \in \mathbb{M}(\mathcal{F}_r)$ be a module monomial and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be such that for all $\varepsilon_i \prec \sigma$ we have $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\mathbb{s}(\gamma_i) = \varepsilon_i$. Assume that all regular S-polynomials $p^{[\pi]}$ of $G^{[\Sigma]}$ with $\mathbb{s}(\pi) \prec \sigma$ regular $\mathbb{s}$-reduce to some $p'^{[\pi']}$ by $G^{[\Sigma]}$ such that π' is a syzygy or $p'^{[\pi']}$ is singular top $\mathbb{s}$-reducible. Then, $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ.*

Proof. Assume, for contradiction, that $G^{[\Sigma]}$ is not a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ. Then, there exists a signature polynomial $h^{[\delta]} \in I^{[\Sigma]}$ with $\mathbb{s}(\delta) \prec \sigma$ which does not $\mathbb{s}$-reduce to zero by $G^{[\Sigma]}$. W.l.o.g. we let $h^{[\delta]}$ be such that $\mathbb{s}(\delta)$ is minimal. Furthermore, we can also assume that $h^{[\delta]}$ is top $\mathbb{s}$-reduced. Then, according to Lemma 33, there exist $p^{[\pi]} \in I^{[\Sigma]}$ and $a, b \in \langle X\rangle$ such that $\mathbb{s}(a\pi b) = \mathbb{s}(\delta)$ and such that

1. π is a (trivial) syzygy (between two elements in $G^{[\Sigma]}$), or
2. $p^{[\pi]}$ is a regular S-polynomial of $G^{[\Sigma]}$ and $ap'^{[\pi']}b$ is not regular top $\mathbb{s}$-reducible where $p'^{[\pi']}$ is the result of regular $\mathbb{s}$-reducing $p^{[\pi]}$.

We distinguish between the two possible cases.

Case 1: π is a syzygy. Then the signature polynomial $\frac{\mathbb{sc}(\delta)}{\mathbb{sc}(\pi)}a0^{[\pi]}b$ is (regular) top $\mathbb{s}$-reduced. Hence, since also $h^{[\delta]}$ is regular top $\mathbb{s}$-reduced and $\mathbb{st}(\delta) = \mathbb{st}(\frac{\mathbb{sc}(\delta)}{\mathbb{sc}(\pi)}a\pi b)$, Lemma 17 yields that $h = \frac{\mathbb{sc}(\delta)}{\mathbb{sc}(\pi)}a0b = 0$. But this is a contradiction to the assumption that $h^{[\delta]}$ does not $\mathbb{s}$-reduce to zero.

Case 2: π is not a syzygy. Then $p^{[\pi]}$ is a regular S-polynomial of $G^{[\Sigma]}$ and $ap'^{[\pi']}b$ is not regular top $\mathbb{s}$-reducible where $p'^{[\pi']}$ is the result of regular $\mathbb{s}$-reducing $p^{[\pi]}$. By assumption, π' is a syzygy or $p'^{[\pi']}$ is singular top $\mathbb{s}$-reducible. In the first case, we can reuse the arguments from the above to obtain a contradiction. Hence, we can assume that $p' \neq 0$ and that $p'^{[\pi']}$ is singular top $\mathbb{s}$-reducible. Then, we note that $\frac{\mathbb{sc}(\delta)}{\mathbb{sc}(\pi')}ap'^{[\pi']}b$ is regular top $\mathbb{s}$-reduced since $ap'^{[\pi']}b$ is regular top $\mathbb{s}$-reduced. Since also $h^{[\delta]}$ is regular top $\mathbb{s}$-reduced and $\mathbb{st}(\delta) = \mathbb{st}(\frac{\mathbb{sc}(\delta)}{\mathbb{sc}(\pi')}ap'^{[\pi']}b)$, Lemma 17 yields that $\operatorname{lt}(h) = \operatorname{lt}(\frac{\mathbb{sc}(\delta)}{\mathbb{sc}(\pi')}ap'b)$. So, anything that top $\mathbb{s}$-reduces $ap'^{[\pi']}b$ also top $\mathbb{s}$-reduces $h^{[\delta]}$. We note that $ap'^{[\pi']}b$ is top $\mathbb{s}$-reducible as $p'^{[\pi']}$ is top $\mathbb{s}$-reducible. Thus, $h^{[\delta]}$ is top $\mathbb{s}$-reducible, which is a contradiction. □

4.3. *Effective description of the module of syzygies*

Similarly to Buchberger's classical characterization of Gröbner bases, Theorem 34 allows us to state a first, non-optimized version of a signature Gröbner basis algorithm for noncommutative polynomials, by ensuring that regular S-polynomials which are not trivial syzygies $\mathbb{s}$-reduce to zero.

The fact that we need to handle at least some trivial syzygies separately is a crucial difference to the commutative case: in the commutative case, Buchberger's coprime criterion and the F5 criterion allow to eliminate some (resp. all) trivial syzygies, but signature-based algorithms terminate even without the criteria.

By contrast, in the noncommutative case, the module of trivial syzygies is in general not finitely generated, which requires handling trivial syzygies separately. On the other hand, by handling trivial syzygies separately, we are able to obtain an effective description of the module of syzygies. More precisely, we state the following fact about syzygies.

Lemma 35. *Let $\mu \in \mathcal{F}_r$ be a syzygy and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis of $I^{[\Sigma]}$ up to some signature $\sigma \in \mathbb{M}(\mathcal{F}_r)$ with $\sigma \succ \mathbb{s}(\mu)$. Then, there exist $p^{[\pi]} \in I^{[\Sigma]}$ and $a, b \in \langle X\rangle$ such that $\mathbb{s}(a\pi b) = \mathbb{s}(\mu)$ and such that one of the following conditions holds.*

1. *π is a trivial syzygy between two elements in $G^{[\Sigma]}$,*
2. *$p^{[\pi]}$ is a regular S-polynomial of $G^{[\Sigma]}$ which regular $\mathbb{s}$-reduces to zero by $G^{[\Sigma]}$.*

Proof. Since $0^{[\mu]}$ is top $\mathbb{s}$-reduced by $G^{[\Sigma]}$, Lemma 33 yields the existence of $p^{[\pi]} \in I^{[\Sigma]}$ and $a, b \in \langle X\rangle$ such that $\mathbb{s}(\mu) = \mathbb{s}(a\pi b)$ and such that one of the following conditions holds.

1. π is a trivial syzygy between two elements in $G^{[\Sigma]}$,
2. $p^{[\pi]}$ is an S-polynomial of $G^{[\Sigma]}$ and $ap'^{[\pi']}b$ is not regular top $\mathbb{s}$-reducible where $p'^{[\pi']}$ is the result of regular $\mathbb{s}$-reducing $p^{[\pi]}$.

If π is a trivial syzygy, we are done. Otherwise, since neither $0^{[\mu]}$ nor $cap'^{[\pi']}b$, with $c = \frac{\mathbb{sc}(\mu)}{\mathbb{sc}(\pi')}$ are regular top $\mathbb{s}$-reducible and $\mathbb{st}(\mu) = \mathbb{st}(ca\pi'b)$, Lemma 17 yields that $0 = cap'b$, and consequently, also $p' = 0$. □

Lemma 35 allows us to describe more precisely the syzygy module $S = \operatorname{Syz}(f_1, \ldots, f_r)$. Consider the set H_{triv} of trivial trivial syzygies of $G^{[\Sigma]}$

$$H_{\text{triv}} = \left\{\gamma_1 m g_2 - g_1 m \gamma_2 \mid g_1^{[\gamma_1]}, g_2^{[\gamma_2]} \in G^{[\Sigma]}, m \in \langle X\rangle\right\}.$$

Note that the set of signatures of H_{triv} contains all the elements of the form

$$\max_{\preceq}\{\mathbb{s}(\gamma_1)m\operatorname{lm}(g_2), \operatorname{lm}(g_1)m\,\mathbb{s}(\gamma_2)\}, \tag{1}$$

for $g_1^{[\gamma_1]}, g_2^{[\gamma_2]} \in G^{[\Sigma]}$. It may happen that this set contains infinitely many module monomials which do not divide each other, and indeed this will be the case for all sufficiently non-trivial ideals. It implies that for such ideals, S does not admit a finite Gröbner basis.

However, Lemma 35 shows that a Gröbner basis of S is given by adding to H_{triv} all the syzygies found by regular $\mathfrak{s}$-reducing to zero all regular S-polynomials of $G^{[\Sigma]}$. Furthermore, if $G^{[\Sigma]}$ is finite, the set of signatures of syzygies in H_{triv} can be enumerated using the description (1), and altogether, we obtain an effective description of the syzygy module of $f_1, \dots, f_r$.

4.4. Algorithm

The algorithm, incorporating both the computation of the signature Gröbner basis and of the aforementioned description of the syzygy module of $f_1, \dots, f_r$, is given in Algorithm 1.

Algorithm 1 SigGB

Input: $I = (f_1, \dots, f_r) \subseteq K\langle X\rangle$

Output (if the algorithm terminates):

- $G^{[\Sigma]}$ a signature Gröbner basis of $I^{[\Sigma]}$
- H s.t. $H \cup \{\gamma m g' - g m \gamma' \mid g^{[\gamma]}, g'^{[\gamma']} \in G^{[\Sigma]},\ m \in \langle X\rangle\}$ is a Gröbner basis of $\mathrm{Syz}(f_1, \dots, f_r)$

```
$G^{[\Sigma]} \leftarrow \emptyset$
$H \leftarrow \emptyset$
$P \leftarrow \{f_1^{[\varepsilon_1]}, \dots, f_r^{[\varepsilon_r]}\}$
**while** $P \neq \emptyset$ **do**
    choose $p^{[\pi]} \in P$ s.t. $\mathfrak{s}(\pi) = \min_{\preceq}\{\mathfrak{s}(\pi') \mid p'^{[\pi']} \in P\}$
    $P \leftarrow P \setminus \{p^{[\pi]}\}$
    $p'^{[\pi']} \leftarrow$ result of regular $\mathfrak{s}$-reducing $p^{[\pi]}$ by $G^{[\Sigma]}$
    **if** $p' = 0$ **then**
        $H \leftarrow H \cup \{\pi'\}$
    **else if** $p'^{[\pi']}$ is not singular top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$ **then**
        $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{p'^{[\pi']}\}$
        $P \leftarrow P \cup \{$all regular S-polynomials between $p'^{[\pi']}$ and all $g^{[\gamma]} \in G^{[\Sigma]}\}$
**return** $G^{[\Sigma]}, H$
```

We note that we cannot expect Algorithm 1 to always terminate since, as already mentioned, there are polynomials in $K\langle X\rangle$ generating a module $I^{[\Sigma]}$ which does not have a finite signature Gröbner basis. However, the following theorem ensures that SigGB always correctly enumerates a signature Gröbner basis of the module $I^{[\Sigma]}$ defined by the input $I = (f_1, \dots, f_r)$, and a Gröbner basis of the syzygy module $\mathrm{Syz}(f_1, \dots, f_r)$.

Theorem 36. *Let $f_1, \dots, f_r \in K\langle X\rangle$, denote $G_0^{[\Sigma]} = H_0 = \emptyset$. Furthermore, let $G_n^{[\Sigma]}$ and H_n be the value of $G^{[\Sigma]}$ and H in Algorithm 1 after n iterations of the "*while*" loop given $f_1, \dots, f_r$ as input. Then, the following holds.*

1. *$G^{[\Sigma]} = \bigcup_{n \geq 0} G_n^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ w.r.t. the generators $f_1, \dots, f_r$;*
2. *Let $H_{\text{triv}} = \{\gamma m g' - g m \gamma' \mid g^{[\gamma]}, g'^{[\gamma']} \in G^{[\Sigma]}\}$. Then,*

$$H \cup H_{\text{triv}} = \bigcup_{n \geq 0} (H_n \cup \{\gamma m g' - g m \gamma' \mid g^{[\gamma]}, g'^{[\gamma']} \in G_n^{[\Sigma]}, m \in \langle X\rangle\})$$

is a Gröbner basis of $\mathrm{Syz}(f_1, \dots, f_r)$.

In this sense, Algorithm 1 enumerates a signature Gröbner basis of $I^{[\Sigma]}$ and a Gröbner basis of the syzygy module $\mathrm{Syz}(f_1, \ldots, f_r)$.

In order to prove this theorem, we first state the following useful lemma which ensures that Algorithm 1 cannot "get stuck" at a certain signature indefinitely.

Lemma 37. *During the execution of Algorithm 1, elements from P are processed in ascending order w.r.t. their signatures and every possible signature is eventually processed.*

Proof. For $n \geq 0$, we denote by $p_n^{[\pi_n]}$ the signature polynomial, which is chosen from the set P in the $(n+1)$-th iteration of the "*while*" loop of Algorithm 1. We note that it follows from Corollary 15, Corollary 29, and the fact that $p_n^{[\pi_n]}$ is always chosen to have minimal signature among all elements in P, that $\mathfrak{s}(\pi_n) \preceq \mathfrak{s}(\pi_{n+1})$ for all $n \geq 0$. If we can show that for every $n \geq 0$ there exists a $k > 0$ such that $\mathfrak{s}(\pi_n) \prec \mathfrak{s}(\pi_{n+k})$, then the fact that $\preceq$ is a fair ordering ensures that there is no element in P, which is postponed indefinitely, and consequently, that every possible signature is eventually processed. Hence, it remains to show that it is not possible to obtain infinitely many elements with the same signature. Assume for a contradiction that this is the case, i.e. that there exists an $N \geq 0$ such that $\mathfrak{s}(\pi_N) = \mathfrak{s}(\pi_{N+k})$ for all $k > 0$. We note that since the set P is finite at all times, such an infinite chain can only appear if at some point $n \geq N$ a signature polynomial $p_n^{[\pi_n]}$ is chosen from P and regular $\mathfrak{s}$-reduced to some $p'^{[\pi']}$ such that $p'^{[\pi']}$ causes the algorithm in line 12 to add a regular S-polynomial between $p'^{[\pi']}$ and some $g^{[\gamma]} \in G^{[\Sigma]}$ with signature $\mathfrak{s}(\pi')$ to P. In other words, a signature polynomial introduces a regular S-polynomial with the same signatures as itself. (In fact, this has to happen infinitely often but this is not relevant for the proof.) We note that the algorithm only gets to line 12 if $p'^{[\pi']}$ is not top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$. Then, Lemma 30 yields that all S-polynomials between $p'^{[\pi']}$ and any element from $G^{[\Sigma]}$ have signature strictly larger than $\mathfrak{s}(\pi')$, which ensures that such an infinite chain can not occur. □

Using this lemma, we can now proceed to prove Theorem 36.

Proof of Theorem 36. As in the proof of Lemma 37, for $n \geq 0$, we denote by $p_n^{[\pi_n]}$ the signature polynomial, which is chosen from the set P in the $(n+1)$-th iteration of the "*while*" loop of Algorithm 1.

$G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$. We claim that for every $n \geq 0$, the set $G_n^{[\Sigma]}$ is a signature Gröbner basis up to signature $\mathfrak{s}(\pi_n)$. Indeed, it follows from Lemma 37, that, when $p_n^{[\pi_n]}$ is chosen in line 5, all S-polynomials as well as all $f_i^{[\varepsilon_i]}$ with signature strictly smaller than $\mathfrak{s}(\pi_n)$ have already been processed. Therefore, Theorem 34 yields that $G_n^{[\Sigma]}$ is a signature Gröbner basis up to signature $\mathfrak{s}(\pi_n)$. Since every signature is eventually processed, the set $G^{[\Sigma]} = \bigcup_{n \geq 0} G_n^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$.

$H \cup H_{\mathrm{triv}}$ is a Gröbner basis of $\mathrm{Syz}(f_1, \ldots, f_r)$. Let $\mu \in S \setminus \{0\}$.We have to show that there exist $n \geq 0$ and $a, b \in \langle X \rangle$ such that $\mathfrak{s}(\mu) = a\,\mathfrak{s}(\alpha)b$ for some $\alpha \in H_n \cup \{\gamma m g' - g m \gamma' \mid g^{[\gamma]}, g'^{[\gamma']} \in G_n^{[\Sigma]}, m \in \langle X \rangle\}$. To this end, let n be such that $G_n^{[\Sigma]}$ is a signature Gröbner basis up to a signature $\sigma \succ \mathfrak{s}(\mu)$. Such an n must exist due to the previous discussion. Then, Lemma 35 yields the existence of $p^{[\pi]} \in I^{[\Sigma]}$ and $a, b \in \langle X \rangle$ such that $\mathfrak{s}(a\pi b) = \mathfrak{s}(\mu)$ and such that one of the following conditions holds.

1. π is a trivial syzygy between two elements in $G_n^{[\Sigma]}$,

2. $p^{[\pi]}$ is an S-polynomial of $G^{[\Sigma]}$ which regular $\mathfrak{s}$-reduces to zero by $G_n^{[\Sigma]}$.

Hence, either a module element with signature $\mathfrak{s}(\pi)$ has been added to H_n or there exist $g^{[\gamma]}$, $g'^{[\gamma']} \in G_n^{[\Sigma]}$ and $m \in \langle X \rangle$ such that $\mathfrak{s}(\pi) = \mathfrak{s}(\gamma m g' - g m \gamma')$. □

We make a few observations about Algorithm 1.

1. As already mentioned in Lemma 37, Algorithm 1 processes S-polynomials in ascending order w.r.t. their signature. Furthermore, the requirement that $\preceq$ is a fair module ordering ensures that no S-polynomial is postponed indefinitely. Both of these properties are crucial to ensure the correctness of the algorithm.
2. After every iteration of the "*while*" loop, the set $G^{[\Sigma]}$ is a signature Gröbner basis up to signature σ, where $\sigma \in \mathbb{M}(\mathcal{F}_r)$ is the minimal signature of all elements left in P.
3. Whenever an element $p'^{[\pi']}$ is added to $G^{[\Sigma]}$ in line 12, it is not top $\mathfrak{s}$-reducible by $G^{[\Sigma]}$. Also, no element $q'^{[\rho']}$, which is added to $G^{[\Sigma]}$ after $p'^{[\pi']}$, can be used to top $\mathfrak{s}$-reduce $p'^{[\pi']}$. To see this, we note that it follows from the first point above that $\mathfrak{s}(\pi') \preceq \mathfrak{s}(\rho')$. Now, if $\mathfrak{s}(\pi') \prec \mathfrak{s}(\rho')$, then $q'^{[\rho']}$ can obviously not be used to $\mathfrak{s}$-reduce $p'^{[\pi']}$. If $\mathfrak{s}(\pi') = \mathfrak{s}(\rho')$, then $q'^{[\rho']}$ can only be used to top $\mathfrak{s}$-reduce $p'^{[\pi']}$ if $\operatorname{lm}(q') = \operatorname{lm}(p')$. But this would imply that $q'^{[\rho']}$ is singular top $\mathfrak{s}$-reducible by $p'^{[\pi']}$, which would contradict the check in line 10.

The following corollary is an immediate consequence of the last observation.

Corollary 38. *Algorithm 1 enumerates a minimal signature Gröbner basis.*

Combining this corollary with Corollary 26, we see that Algorithm 1 terminates whenever $I^{[\Sigma]}$ admits a finite signature Gröbner basis w.r.t. the generators $f_1, \dots, f_r$.

Corollary 39. *Let $I = (f_1, \dots, f_r) \subseteq K\langle X \rangle$ be such that $I^{[\Sigma]}$ has a finite signature Gröbner basis w.r.t. the generators $f_1, \dots, f_r$. Then, Algorithm 1 terminates when given $f_1, \dots, f_r$ as input.*

Proof. Since $I^{[\Sigma]}$ has a finite signature Gröbner basis $G^{[\Sigma]}$ w.r.t. the generators $f_1, \dots, f_r$, by Corollary 38, the algorithm will eventually compute a minimal signature Gröbner basis $G^{[\Sigma]}$ of $I^{[\Sigma]}$, which must be finite as well by Corollary 26. At each run of the loop, only finitely many S-polynomials are added to P, so P has finite cardinality. Since $G^{[\Sigma]}$ is a signature Gröbner basis, all the remaining elements in P will regular $\mathfrak{s}$-reduce to 0 or be singular top $\mathfrak{s}$-reducible, so no new polynomials will be added to P and the algorithm will terminate. □

Note that if the algorithm terminates, or equivalently if $I^{[\Sigma]}$ admits a finite signature Gröbner basis, then it has finite output $G^{[\Sigma]}$ and H. This output is such that the polynomial part of elements of $G^{[\Sigma]}$ forms a (finite) Gröbner basis of the ideal I, and that $H \cup H_{\text{triv}}$ is a (usually infinite, but with a finite data representation) Gröbner basis of the module $\operatorname{Syz}(f_1, \dots, f_r)$.

We conjecture that also the converse holds.

Conjecture 40. *Let $f_1, \dots, f_r \in K\langle X \rangle$, and $I^{[\Sigma]}$ be the corresponding module. Assume that there exists a finite set $\tilde{G}^{[\Sigma]} \subseteq I^{[\Sigma]}$ of signature polynomials, with $f_1^{[\epsilon_1]}, \dots, f_r^{[\epsilon_r]} \in \tilde{G}^{[\Sigma]}$, and a finite subset $\tilde{H} \subseteq \operatorname{Syz}(f_1, \dots, f_r)$ such that:*

- *$\tilde{G} := \{g \mid g^{[\gamma]} \in \tilde{G}^{[\Sigma]}\}$ is a Gröbner basis of I;*
- *$\tilde{H} \cup \{\gamma m g' - g m \gamma' \mid g^{[\gamma]}, g'^{[\gamma']} \in \tilde{G}^{[\Sigma]}\}$ is a Gröbner basis of $\operatorname{Syz}(f_1, \dots, f_r)$.*

Let $G_n^{[\Sigma]} \subseteq I^{[\Sigma]}$ and $H_n \subseteq \mathrm{Syz}(f_1, \ldots, f_r)$ be intermediate values of $G^{[\Sigma]}$ and H, respectively, in Algorithm 1 such that

- *all elements of $\tilde{G}^{[\Sigma]}$ $\mathfrak{s}$-reduce to 0 modulo $G_n^{[\Sigma]}$;*
- *for all $\tilde{\sigma} \in \tilde{H}$, there exists $\sigma \in H_n$ such that $\mathfrak{s}(\sigma) = \mathfrak{s}(\tilde{\sigma})$.*

Then $G_n^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, and in particular $I^{[\Sigma]}$ has a finite signature Gröbner basis.

Note that $\tilde{G}^{[\Sigma]}$ need not be a signature Gröbner basis, but merely a set of signature polynomials which, without the signatures, forms a Gröbner basis. Put differently, the statement is equivalent to saying that I admits a finite Gröbner basis G, and that the module $\mathrm{Syz}(f_1, \ldots, f_r)$ has a Gröbner basis given by adding a finite set to the set of trivial syzygies of G (expressed in the module $\mathcal{F}_r$).

In the commutative case where all ideals have a finite signature Gröbner basis, the analogue of this conjecture would give a characterization of signature Gröbner bases in terms of a Gröbner basis of the ideal and of its module of syzygies. To the best of our knowledge, no such characterization is proved in the commutative case.

4.5. S-polynomial elimination

In the commutative case, it is well known that additional criteria can be used to detect $\mathfrak{s}$-reductions to zero. So far, we have already seen that we can immediately discard all singular S-polynomials. In this section, we adapt some other well-known techniques from the commutative case to our setting, namely the *syzygy criterion*, the *F5 criterion* and the *singular criterion*.

Proposition 41 (**Syzygy criterion**). *Let $p^{[\pi]} \in I^{[\Sigma]}$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis up to signature $\mathfrak{s}(\pi)$. If there exists a syzygy $\sigma \in \mathcal{F}_r$ and $a, b \in \langle X \rangle$ such that $\mathfrak{s}(\pi) = a\,\mathfrak{s}(\sigma)b$, then $p^{[\pi]}$ can be regular $\mathfrak{s}$-reduced to zero by $G^{[\Sigma]}$.*

Proof. Let $\sigma \in \mathcal{F}_r$ be a syzygy and $a, b \in \langle X \rangle$ such that $\mathfrak{s}(\pi) = a\,\mathfrak{s}(\sigma)b$. Now, consider

$$p^{[\tau]} = p^{[\pi]} - \frac{\mathfrak{sc}(\pi)}{\mathfrak{sc}(\sigma)} a 0^{[\sigma]} b.$$

Then, $\mathfrak{s}(\tau) \prec \mathfrak{s}(\pi)$. Since $G^{[\Sigma]}$ is a signature Gröbner basis up to signature $\mathfrak{s}(\pi)$, the signature polynomial $p^{[\tau]}$ $\mathfrak{s}$-reduces to zero by $G^{[\Sigma]}$. Thus, using the same reductions, we see that $p^{[\pi]}$ regular $\mathfrak{s}$-reduces to zero by $G^{[\Sigma]}$. □

Hence, we can immediately discard an S-polynomial $p^{[\pi]}$ during the computation of a signature Gröbner basis if its signature $\mathfrak{s}(\pi)$ is divisible by the signature of a syzygy. Clearly, we obtain syzygies whenever we $\mathfrak{s}$-reduce an S-polynomial to zero but there are also syzygies immediately known prior to any computations. Recall that for all signature polynomials $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ we have the trivial syzygies $\alpha m g - f m \beta$, for all monomials $m \in \langle X \rangle$. This means that for any set of generators $\{f_1, \ldots, f_r\} \subseteq K\langle X \rangle$ we immediately obtain the trivial syzygies

$$\varepsilon_i m f_j - f_i m \varepsilon_j,$$

for all $1 \leq i \leq j \leq r$ and all $m \in \langle X \rangle$, which we can use to eliminate S-polynomials. Additionally, whenever we add a new element $g^{[\gamma]}$ to $G^{[\Sigma]}$ during the executing of Algorithm 1, we get the new trivial syzygies

$$\gamma m g' - g m \gamma',$$

for all $g'^{[\gamma']} \in G^{[\Sigma]}$ and all $m \in \langle X \rangle$. Identifying those trivial syzygies lead to the *F5 criterion*.

Corollary 42 (**F5 criterion**). *Let $p^{[\pi]} \in I^{[\Sigma]}$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis up to signature $\mathfrak{s}(\pi)$. Assume that there exist $g^{[\gamma]}, g'^{[\gamma']} \in G^{[\Sigma]}$ and $a, b, m \in \langle X \rangle$ such that one of the following conditions holds.*

1. $\mathfrak{s}(\pi) = a\, \mathfrak{s}(\gamma) m \operatorname{lm}(g') b$ *and* $\mathfrak{s}(\gamma) m \operatorname{lm}(g') \succ \operatorname{lm}(g) m\, \mathfrak{s}(\gamma')$.
2. $\mathfrak{s}(\pi) = a \operatorname{lm}(g) m\, \mathfrak{s}(\gamma') b$ *and* $\operatorname{lm}(g) m\, \mathfrak{s}(\gamma') \succ \mathfrak{s}(\gamma) m \operatorname{lm}(g')$.

Then $p^{[\pi]}$ can be regular $\mathfrak{s}$-reduced to zero by $G^{[\Sigma]}$.

Remark 43. In the noncommutative case, it is not clear how to check the F5 criterion efficiently, as it requires *a priori* $\Theta(|G^{[\Sigma]}|^2)$ checks.

Lemma 17 provides another way to detect redundant S-polynomials.

Corollary 44 (**Singular criterion**). *Let $p^{[\pi]} \in I^{[\Sigma]}$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis up to signature $\mathfrak{s}(\pi)$. If there exists a regular $\mathfrak{s}$-reduced element $g^{[\gamma]} \in G^{[\Sigma]}$ such that $\mathfrak{s}(\gamma) = \mathfrak{s}(\pi)$, then $p^{[\pi]}$ $\mathfrak{s}$-reduces to zero.*

Proof. It follows immediately from Lemma 17 □

Using Algorithm 1, all elements that are added to $G^{[\Sigma]}$ are regular $\mathfrak{s}$-reduced. Hence, during the executing of Algorithm 1, an S-polynomial $p^{[\pi]}$ can be removed immediately if its signature already appears in $G^{[\Sigma]}$.

We note that neither Algorithm 1 nor the criteria discussed in this section rely on all the information encoded in the full module representations of the polynomials. Keeping track of the full module representation, however, causes a significant overhead in terms of memory consumption and overall computation time. Consequently, we can optimize Algorithm 1 by only keeping track of the signatures of each polynomial.

We use the notation from [SW11] and denote by $f^{(\sigma)}$ a pair $(f, \sigma) \in K\langle X \rangle \times \mathcal{F}_r$ such that there exists $f^{[\alpha]} \in I^{[\Sigma]}$ with $\mathfrak{s}(\alpha) = \sigma$. We call such a pair a *signature-labeled polynomial*. We denote the set of all signature-labeled polynomials by $I^{(\Sigma)}$, i.e.

$$I^{(\Sigma)} = \{f^{(\sigma)} \mid \exists f^{[\alpha]} \in I^{[\Sigma]} : \mathfrak{s}(\alpha) = \sigma\}.$$

Additionally, we introduce the following concept which is defined analogously in [SW11].

Definition 45. Let $\mathcal{I}$ be an index set and let $\sigma \in \mathbb{M}(\mathcal{F}_r)$. We call a set $G^{(\Sigma)} = \{g_i^{(\sigma_i)} \mid i \in \mathcal{I}\} \subseteq I^{(\Sigma)}$ a *signature-labeled Gröbner basis of $I^{(\Sigma)}$ (up to signature σ)* if there exist $g_i^{[\gamma_i]} \in I^{[\Sigma]}$ such that $\mathfrak{s}(\gamma_i) = \sigma_i$ and such that $\{g_i^{[\gamma_i]} \mid i \in \mathcal{I}\}$ is a signature Gröbner basis of $I^{[\Sigma]}$ (up to signature σ). Furthermore, $G^{(\Sigma)}$ is called *minimal* if $G^{[\Sigma]}$ is minimal.

Hence, we can adapt Algorithm 1 to work only with signature-labeled polynomials instead of signature polynomials. In this way, instead of computing a signature Gröbner basis and a Gröbner basis of $\operatorname{Syz}(f_1, \ldots, f_r)$, we can only compute a signature-labeled Gröbner basis and a Gröbner basis of $\mathfrak{s}(\operatorname{Syz}(f_1, \ldots, f_r))$.

In the following section, we discuss how to recover the information that is lost when Algorithm 1 only works with signature-labeled polynomials. In particular, this means reconstructing a signature Gröbner basis from a signature-labeled Gröbner basis and reconstructing a Gröbner basis of $\operatorname{Syz}(f_1, \ldots, f_r)$ from one of $\mathfrak{s}(\operatorname{Syz}(f_1, \ldots, f_r))$.

4.6. From signature-labeled Gröbner bases to signature Gröbner bases

In this section, we adapt the reconstruction methods described in [GVW15] to recover module representations of elements of the ideal and of syzygies from signatures to our noncommutative setting. In particular, we assume that Algorithm 1 has been adapted to work with signature-labeled polynomials instead of signature polynomials. Then, we let $G^{(\Sigma)} \subseteq I^{(\Sigma)}$ and $H \subseteq \mathbb{M}(\mathcal{F}_r)$ be the output of this adapted version of the algorithm when given $f_1, \ldots, f_r \in K\langle X\rangle$ as input. We note that we do not necessarily require the algorithm to naturally terminate. We also allow the scenario where we artificially abort the computation after a certain number of iterations. In such cases, the set $G^{(\Sigma)}$ is only a minimal signature-labeled Gröbner basis up to a certain signature $\sigma \in \mathbb{M}(\mathcal{F}_r)$ and H together with the signatures of the trivial syzygies does not necessarily form a Gröbner basis of $\mathfrak{s}(\mathrm{Syz}(f_1, \ldots, f_r))$.

In this general setting, the goal of this section is twofold. First of all, starting from $G^{(\Sigma)}$ we want to reconstruct a signature Gröbner basis $G^{[\Sigma]}$ (up to signature σ). Secondly, for each element $\beta \in H$, we want to find a module element $\alpha \in \mathrm{Syz}(f_1, \ldots, f_r)$ such that $\mathfrak{s}(\alpha) = \beta$.

In situations where Algorithm 1 naturally terminates, i.e. when $G^{(\Sigma)}$ is a signature-labeled Gröbner basis and when H together with the signatures of the trivial syzygies forms a Gröbner basis of $\mathfrak{s}(\mathrm{Syz}(f_1, \ldots, f_r))$, both of these goals combined allow us to also recover a Gröbner basis of $\mathrm{Syz}(f_1, \ldots, f_r)$. The algorithms which we describe in this section are direct adaptation of the procedure outlined in [GVW15].

Our first goal can be achieved by the following algorithm. We note that no matter whether Algorithm 1 naturally terminates or whether we abort it, the sets $G^{(\Sigma)}$ and H are always finite.

Algorithm 2 SigLabeled2SigGB

```
Input: $G^{(\Sigma)}$ a finite minimal signature-labeled Gröbner basis (up to some signature $\sigma \in \mathbb{M}(\mathcal{F}_r)$)
Output: $G^{[\Sigma]}$ a finite minimal signature Gröbner basis (up to signature $\sigma$)
$G^{[\Sigma]} \leftarrow \emptyset$
$H^{(\Sigma)} \leftarrow G^{(\Sigma)}$                    ▷ make a copy so that we do not alter $G^{(\Sigma)}$
while $H^{(\Sigma)} \neq \emptyset$ do
    choose $f^{(\sigma)} \in H^{(\Sigma)}$ s.t. $\sigma = \min_{\preceq}\{\sigma' \mid f'^{(\sigma')} \in H^{(\Sigma)}\}$
    $H^{(\Sigma)} \leftarrow H^{(\Sigma)} \setminus \{f^{(\sigma)}\}$
    if there exist $a, b \in \langle X\rangle, g^{[\gamma]} \in G^{[\Sigma]}$ s.t. $\mathfrak{s}(a\gamma b) = \sigma$ then
        choose $a, b \in \langle X\rangle, g^{[\gamma]} \in G^{[\Sigma]}$ s.t. $\mathfrak{s}(a\gamma b) = \sigma$ and $\mathrm{lm}(agb)$ is minimal
    else
        choose $a, b \in \langle X\rangle$ and $1 \leq i \leq r$ s.t. $a\varepsilon_i b = \sigma$
        $g^{[\gamma]} \leftarrow f_i^{[\varepsilon_i]}$
    $g'^{[\gamma']} \leftarrow$ result of regular top $\mathfrak{s}$-reducing $ag^{[\gamma]}b$ by $G^{[\Sigma]}$
    $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{g'^{[\gamma']}\}$
return $G^{[\Sigma]}$
```

Proposition 46. *Algorithm 2 is correct.*

Proof. To prove the proposition, we show that the following loop invariant holds at the beginning of every iteration of the "*while*" loop:

$$\{(\mathrm{lm}(g), \sigma) \mid g^{(\sigma)} \in G^{(\Sigma)} \setminus H^{(\Sigma)}\} = \{(\mathrm{lm}(g), \mathfrak{s}(\gamma)) \mid g^{[\gamma]} \in G^{[\Sigma]}\}. \tag{2}$$

In other words, the signature polynomials in $G^{[\Sigma]}$ have the same leading monomials and signatures as the signature-labeled polynomials in $G^{(\Sigma)} \setminus H^{(\Sigma)}$. Once the algorithm terminates and $H^{(\Sigma)} = \emptyset$ this implies that $G^{[\Sigma]}$ is a minimal signature Gröbner basis.

Obviously this loop invariant holds in the very beginning when $H^{(\Sigma)} = G^{(\Sigma)}$. So, now assume that (2) holds at some point and let $f^{(\sigma)} \in H^{(\Sigma)}$ be the signature-labeled polynomial that is chosen in line 4 during the next iteration. Furthermore, let $\alpha \in \mathcal{F}_r$ be such that $f^{[\alpha]} \in I^{[\Sigma]}$ with $\mathfrak{s}(\alpha) = \sigma$. Obviously, the signature-polynomial $g'^{[\gamma']}$ is regular top $\mathfrak{s}$-reduced by $G^{[\Sigma]}$. Additionally, the minimality of $G^{(\Sigma)}$ together with the loop invariant implies that also $f^{[\alpha]}$ is regular top $\mathfrak{s}$-reduced by $G^{[\Sigma]}$, which in turn implies that so is $cf^{[\alpha]}$ with $c = \frac{\mathfrak{sc}(\gamma')}{\mathfrak{sc}(\alpha)}$. We note that it also follows from the loop invariant that $G^{[\Sigma]}$ is a signature Gröbner basis up to signature σ. Hence, Lemma 17 is applicable to $g'^{[\gamma']}$ and $cf^{[\alpha]}$. It yields that $\mathrm{lt}(g') = \mathrm{lt}(cf)$, and consequently, $\mathrm{lm}(g') = \mathrm{lm}(f)$. Since also $\mathfrak{s}(\gamma') = \mathfrak{s}(a\gamma b) = \sigma$, the loop invariant still holds after removing $f^{(\sigma)}$ from $H^{(\Sigma)}$ and adding $g'^{[\gamma']}$ to $G^{[\Sigma]}$. □

After recovering a signature Gröbner basis, we can proceed with the following algorithm to also recover the syzygies whose signatures are saved in H.

Algorithm 3 SyzygyRecovery

```
Input: $G^{(\Sigma)} \subseteq I^{(\Sigma)}$ and $H \subseteq \mathbb{M}(\mathcal{F}_r)$ as produced by Algorithm 1
Output: $\tilde{H} \subseteq \mathrm{Syz}(f_1, \dots, f_r)$ such that $\mathfrak{s}(\tilde{H}) = H$
1: $\tilde{H} \leftarrow \emptyset$
2: $G^{[\Sigma]} \leftarrow$ apply Algorithm 2 to $G^{(\Sigma)}$
3: for $\sigma \in H$ do
4:     choose $a, b \in \langle X \rangle, g^{[\gamma]} \in G^{[\Sigma]}$ s.t. $\mathfrak{s}(a\gamma b) = \sigma$ and $\mathrm{lm}(agb)$ is minimal.
5:     $0^{[\gamma']} \leftarrow$ result of regular $\mathfrak{s}$-reducing $ag^{[\gamma]}b$ by $G^{[\Sigma]}$
6:     $\tilde{H} \leftarrow \tilde{H} \cup \{\gamma'\}$
7: return $\tilde{H}$
```

Proposition 47. *Algorithm 3 is correct.*

Proof. To see the correctness of the algorithm, the only problematic lines are line 4 and 5. To this end, let $\sigma \in H$ be the module monomial that is chosen in line 3 during some iteration. By definition of H we get that σ is the signature of an S-polynomial of $G^{(\Sigma)}$ which regular $\mathfrak{s}$-reduces to zero. Hence, σ is a multiple of the signature of some element in $G^{(\Sigma)}$. Consequently, there exist $a, b \in \langle X \rangle$ and $g^{[\gamma]} \in G^{[\Sigma]}$ as required in line 4. It remains to show that $ag^{[\gamma]}b$ really regular $\mathfrak{s}$-reduces to zero by $G^{[\Sigma]}$. To this end, we note that it follows from the definition of $G^{(\Sigma)}$ and Proposition 46, that $G^{[\Sigma]}$ is a signature Gröbner basis up to signature $\sigma' = \max_{\preceq} \mathfrak{s}(H)$. Consequently, we can apply Proposition 41 to conclude that $ag^{[\gamma]}b$ indeed regular $\mathfrak{s}$-reduces to zero. □

Remark 48. The minimality condition in line 7 of Algorithm 2, respectively in line 4 of Algorithm 3, is not required for the correctness of these algorithms. It is included purely for efficiency reasons with the hope of having to do less $\mathfrak{s}$-reductions if $\mathrm{lm}(agb)$ is minimal.

To conclude this section, we note that if Algorithm 1 naturally terminates, a Gröbner basis of $\mathrm{Syz}(f_1, \dots, f_r)$ can be obtained as follows: First, apply Algorithm 2 to obtain a signature Gröbner basis of $I^{[\Sigma]}$. Next, use Algorithm 3 to get the set $\tilde{H}$ containing the recovered syzygies. Finally, a Gröbner basis of $\mathrm{Syz}(f_1, \dots, f_r)$ is given by $\tilde{H} \cup \{\gamma m g' - g m \gamma' \mid g^{[\gamma]}, g'^{[\gamma']} \in G^{[\Sigma]}, m \in \langle X \rangle\}$.

5. Experimental results and future work

In this section, we compare Algorithm 1 to the classical Buchberger algorithm. Since our focus is on the feasibility of signature-compatible computations and not on their efficiency, we give data about the number of S-polynomials computed and reduced as well as about the number of reductions to zero when computing (signature) Gröbner bases for certain benchmark examples. The following are taken from [LSL09].

Example	Generators of the ideal
`braid3`	$yxy - zyz, xyx - zxy, zxz - yzx, x^3 + y^3 + z^3 + xyz$
`lp1`	$z^4 + yxyx - xy^2x - 3zyxz, x^3yxy - xyx, zyx - xyz + zxz$
`lv2`	$xy + yz, x^2 + xy - yx - y^2$

As done in [LSL09], we only compute truncated (signature) Gröbner bases of these homogeneous ideals. The designated degree bounds are indicated by the number after the "`-`" in the name of each example in Table 1. So, for example `lp1-11` means that we compute a partial Gröbner basis of the example `lp1` up to degree 11. Additionally, we also consider two non-homogeneous ideals derived from finite generalized triangular groups taken from [RS02, Theorem 2.12] as done in [Xiu12]. Both of these ideals have finite (signature) Gröbner bases.

Example	Generators of the ideal
`tri1`	$x^3 - 1, y^2 - 1, (yxyxyx^2yx^2)^2 - 1$
`tri3`	$x^3 - 1, y^3 - 1, (yxyx^2)^2 - 1$

For all examples, we fix $\preceq_{deglex}$ as a monomial ordering where we order the indeterminates as $x \prec_{lex} y \prec_{lex} z$ and work over the coefficient field $\mathbb{Q}$. As a module ordering, $\preceq_{\mathbf{top}}$ is chosen.

The following table compares the number of S-polynomials computed and reduced and the number of reductions to zero that occur while computing (truncated) (signature) Gröbner bases for the examples stated above. Algorithm 1 including the criteria discussed in Section 4.5, denoted by `SigGB`, is compared to a vanilla Buchberger algorithm, denoted by `BB vanilla`, and to an optimized Buchberger algorithm including a noncommutative version of the chain criterion as described in [Hof20, Section 4.5.1], denoted by `BB optimized`. For each example, we list in the column "S-poly" the total number of S-polynomials that are computed and reduced during the execution of the respective algorithm. Additionally, we list the total number of reductions to zero in the column "red. to 0".

We note that all algorithms are part of the `OperatorGB` package[2] and that a Mathematica notebook containing all computations can be obtained from the same website as the package.

[2] Available at `https://clemenshofstadler.com/software/`

Example	`SigGB`		`BB vanilla`		`BB optimized`	
	S-poly	red. to 0	S-poly	red. to 0	S-poly	red. to 0
`braid3-10`	1053	40	1154	661	1121	634
`lp1-11`	155	0	205	130	198	125
`lv2-100`	201	0	9702	4990	9702	4990
`tri1`	335	164	9435	8897	3480	3288
`tri3`	252	136	2705	2573	1060	979

Table 1: Number of S-polynomials and reduction to zero during the computation of (truncated) (signature) Gröbner bases for several benchmark examples.

As can be seen, the signature-based algorithm considers less S-polynomials and needs less reductions to zero. In two of the examples, there are even no zero reductions at all. However, in terms of absolute computation time, `SigGB` cannot compete with the two other algorithms. This is mainly because of two reasons. First of all, when using the F5 criterion, the number of checks that have to be done for each S-polynomial increases quadratically with the size of the set $G^{[\Sigma]}$, which becomes computationally quite intense as $G^{[\Sigma]}$ grows. Additionally, the fact that we are restricted to regular $\mathfrak{s}$-reductions in Algorithm 1 requires an additionally check before each $\mathfrak{s}$-reduction. This cost also adds up for longer computations.

We will investigate whether it is possible to improve the performance of Algorithm 1 to obtain a competitive algorithm in practice. One step towards achieving this goal could be finding ways to also allow non-fair module orderings such as a position-over-term ordering. Additionally, future research will be focused on adapting the concepts developed in this paper to the noncommutative F4 algorithm.

We also plan to leverage the algorithms developed here to find short representations of ideal elements. This is particularly useful when proving operator identities, where such short representations correspond to short proofs of the statement about operators. In particular, the effective description of the syzygy module provided by a signature Gröbner basis might allow to compute the *shortest* proof of certain operator identities.

Acknowledgements

The first author was supported by the Austrian Science Fund (FWF) grant P32301. The second author was supported by the Austrian Science Fund (FWF) grant P31571-N32. The authors thank Clemens G. Raab and Georg Regensburger for their careful reading and their valuable comments.

References

[AL94] William Adams and Philippe Loustaunau. An Introduction to Gröbner Bases. *Graduate Studies in Mathematics*, 1994.

[Ber78] George M. Bergman. The diamond lemma for ring theory. *Advances in Mathematics*, 29:178–218, 1978.

[BK06] Holger Bluhm and Martin Kreuzer. Gröbner Basis Techniques in the Computation of Two-Sided Syzygies. In *Combinatorial Group Theory, Discrete Groups, and Number Theory: A Conference in Honor of Gerhard Rosenberger, December 8-9, 2004, Fairfield University: AMS Special Session on Infinite Groups, October 8-9, 2005, Bard College*, volume 10, page 45. American Mathematical Soc., 2006.

[Bok76] L. A. Bokut'. Embeddings into simple associative algebras. *Algebra i Logika*, 15(2):117–142, 1976.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, University of Innsbruck, Austria, 1965.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[CHRR20] Cyrille Chenavier, Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger. Compatible rewriting of noncommutative polynomials for proving operator identities. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, pages 83–90, 2020.

[EF17] Christian Eder and Jean-Charles Faugère. A survey on signature-based algorithms for computing Gröbner bases. *Journal of Symbolic Computation*, 80:719–784, 2017.

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic). ACM, 2002.

[Gal85] André Galligo. Some algorithmic questions on ideals of differential operators. *Lecture Notes in Computer Science*, page 413–421, 1985.

[GVW15] Shuhong Gao, Frank Volny IV, and Mingsheng Wang. A new framework for computing Gröbner bases. *Mathematics of Computation*, 85(297):449–465, 2015.

[Hof20] Clemens Hofstadler. Certifying operator identities and ideal membership of noncommutative polynomials. Master's thesis, Johannes Kepler University Linz, Austria, 2020. Available at `https://epub.jku.at/obvulihs/content/titleinfo/5013051`.

[HRR19] Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger. Certifying operator identities via noncommutative Gröbner bases. *ACM Communications in Computer Algebra*, 53(2):49–52, 2019.

[HSW98] J. William Helton, Mark Stankus, and John J. Wavrik. Computer simplification of formulas in linear systems theory. *IEEE Transactions on Automatic Control*, 43(3):302–314, 1998.

[HW94] J. William Helton and John J. Wavrik. Rules for computer simplification of the formulas in operator model theory and linear systems. In *Nonselfadjoint operators and related topics*, pages 325–354. Springer, 1994.

[LSL09] Roberto La Scala and Viktor Levandovskyy. Letterplace ideals and non-commutative Gröbner bases. *Journal of Symbolic Computation*, 44(10):1374–1393, 2009.

[LSZ20] Viktor Levandovskyy, Hans Schönemann, and Karim Abou Zeid. Letterplace: a Subsystem of SINGULAR for Computations with Free Algebras via Letterplace Embedding. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, pages 305–311, 2020.

[Mor85] Ferdinando Mora. Gröbner bases for non-commutative polynomial rings. In *International Conference on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 353–362. Springer, 1985.

[Mor94] Teo Mora. An introduction to commutative and noncommutative Gröbner bases. *Theoretical Computer Science*, 134(1):131–173, 1994.

[Mor16] Teo Mora. *Solving Polynomial Equation Systems IV: Volume 4, Buchberger Theory and Beyond*, volume 158. Cambridge University Press, 2016.

[RRHP21] Clemens G. Raab, Georg Regensburger, and Jamal Hossein Poor. Formal proofs of operator identities by a single formal computation. *Journal of Pure and Applied Algebra*, 225(5):106564, 2021.

[RS02] Gerhard Rosenberger and Martin Scheer. Classification of the finite generalized tetrahedron groups. *Contemporary Mathematics*, 296:207–230, 2002.

[RS12] Bjarke Hammersholt Roune and Michael Stillman. Practical Gröbner basis computation. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 203–210, 2012. Full version including the appendix available at arXiv:1206.6940.

[Shi62] A. I. Shirshov. Some algorithmic problems for Lie algebras. *Sibirsk. Mat. Z.*, 3:292–296, 1962. (in Russian); English translation in SIGSAM Bull. 33(2):3–6 (1999).

[SL20] Leonard Schmitz and Viktor Levandovskyy. Formally verifying proofs for algebraic identities of matrices. In *International Conference on Intelligent Computer Mathematics*, pages 222–236. Springer, 2020.

[SW11] Yao Sun and Dingkang Wang. Solving detachability problem for the polynomial ring by signature-based Gröbner basis algorithms. *arXiv preprint arXiv:1108.1301*, 2011.

[SWMZ12] Yao Sun, Dingkang Wang, Xiaodong Ma, and Yang Zhang. A Signature-Based Algorithm for Computing Gröbner Bases in Solvable Polynomial Algebras. *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation - ISSAC '12*, 2012.

[Xiu12] Xingqiang Xiu. *Non-commutative Gröbner bases and applications*. PhD thesis, University of Passau, Germany, 2012. Available at `http://www.opus-bayern.de/uni-passau/volltexte/2012/2682/`.

Appendix A. Detailed example

Example 27 (continued). Recall that in Example 27 we considered the ideal $I = (f_1, f_2, f_3) \subseteq K\langle X\rangle$ with

$$f_1 = xyx - xy, \qquad f_2 = yxy, \qquad f_3 = xyy - xxy,$$

over an arbitrary field K in the variables $X = \{x, y\}$. Furthermore, we used $\preceq_{deglex}$ where we ordered the indeterminates as $x \prec_{lex} y$ and used $\preceq_{\mathbf{top}}$ as a module ordering. We claimed that the set

$$G^{[\Sigma]} = \{f_1^{[\varepsilon_1]}, f_2^{[\varepsilon_2]}, f_3^{[\varepsilon_3]}, f_4^{[\alpha]}\} \cup \{g_n^{[\gamma_n]} \mid n \geq 0\}.$$

with $f_4 = xxy$, $g_n = yx^{n+2}y$ and certain $\alpha, \gamma_n \in \mathcal{F}_r$ such that $\mathfrak{s}(\alpha) = \varepsilon_1 y$ and $\mathfrak{s}(\gamma_n) = y\varepsilon_3 y^n$, is a minimal signature Gröbner basis of $I^{[\Sigma]}$ w.r.t. the generators f_1, f_2, f_3. We postponed the verification that $G^{[\Sigma]}$ is indeed a signature Gröbner basis. We finish this proof here using Theorem 34. To this end, we compute all regular ambiguities of $G^{[\Sigma]}$ and regular $\mathfrak{s}$-reduce the respective S-polynomials. We have the following regular ambiguities a_{ij} between f_i and f_j:

$$\begin{aligned}
a_{11} &= (xyxyx, xy, yx, f_1^{[\varepsilon_1]}, f_1^{[\varepsilon_1]}), & a_{12} &= (xyxy, x, y, f_1^{[\varepsilon_1]}, f_2^{[\varepsilon_2]}),\\
a_{13} &= (xyxyy, xy, yy, f_1^{[\varepsilon_1]}, f_3^{[\varepsilon_3]}), & a_{14} &= (xyxxy, xy, xy, f_1^{[\varepsilon_1]}, f_4^{[\alpha]}),\\
a_{21} &= (yxyx, y, x, f_2^{[\varepsilon_2]}, f_1^{[\varepsilon_1]}), & a_{22} &= (yxyxy, yx, xy, f_2^{[\varepsilon_2]}, f_2^{[\varepsilon_2]}),\\
a_{23} &= (yxyy, y, y, f_2^{[\varepsilon_2]}, f_3^{[\varepsilon_3]}), & a_{32} &= (xyyxy, xy, xy, f_3^{[\varepsilon_3]}, f_2^{[\varepsilon_2]}),\\
a_{41} &= (xxyx, x, x, f_4^{[\alpha]}, f_1^{[\varepsilon_1]}), & a_{42} &= (xxyxy, xx, xy, f_4^{[\alpha]}, f_2^{[\varepsilon_2]}),\\
a_{43} &= (xxyy, x, y, f_4^{[\alpha]}, f_3^{[\varepsilon_3]}).
\end{aligned}$$

The corresponding S-polynomials are

$$\begin{aligned}
\mathrm{sp}(a_{11}) &= (-xyyx + xyxy)^{[\varepsilon_1 yx - xy\varepsilon_1]}, & \mathrm{sp}(a_{12}) &= -xyy^{[\varepsilon_1 y - x\varepsilon_2]},\\
\mathrm{sp}(a_{13}) &= (-xyyy + xyxxy)^{[\varepsilon_1 yy - xy\varepsilon_3]}, & \mathrm{sp}(a_{14}) &= -xyxy^{[\varepsilon_1 xy - xy\alpha]},\\
\mathrm{sp}(a_{21}) &= yxy^{[\varepsilon_2 x - y\varepsilon_1]}, & \mathrm{sp}(a_{22}) &= 0^{[\varepsilon_2 xy - yx\varepsilon_2]},\\
\mathrm{sp}(a_{23}) &= yxxy^{[\varepsilon_2 y - y\varepsilon_3]}, & \mathrm{sp}(a_{32}) &= -xxyxy^{[\varepsilon_3 xy - xy\varepsilon_2]},\\
\mathrm{sp}(a_{41}) &= xxy^{[\alpha x - x\varepsilon_1]}, & \mathrm{sp}(a_{42}) &= 0^{[\alpha xy - xx\varepsilon_2]},\\
\mathrm{sp}(a_{43}) &= xxxy^{[\alpha y - x\varepsilon_3]}.
\end{aligned}$$

In the following, we show that the non-zero S-polynomials can be regular $\mathfrak{s}$-reduced to zero or to a singular top $\mathfrak{s}$-reducible element. It is easy to check that by regular $\mathfrak{s}$-reducing the S-polynomials above, we obtain

$$\begin{aligned}
\mathrm{sp}(a_{11}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\alpha_{11}]}, & \mathrm{sp}(a_{12}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} -xxy^{[\alpha_{12}]}, & \mathrm{sp}(a_{13}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\alpha_{13}]},\\
\mathrm{sp}(a_{14}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\alpha_{14}]}, & \mathrm{sp}(a_{21}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\alpha_{21}]}, & \mathrm{sp}(a_{23}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} yxxy^{[\alpha_{23}]},\\
\mathrm{sp}(a_{32}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\alpha_{32}]}, & \mathrm{sp}(a_{41}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\alpha_{41}]}, & \mathrm{sp}(a_{43}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\alpha_{43}]},
\end{aligned}$$

for certain $\alpha_{ij} \in \mathcal{F}_r$. Note that $\mathfrak{s}(\alpha_{12}) = \mathfrak{s}(\mathrm{sp}(a_{12})) = \varepsilon_1 y$ and $\mathfrak{s}(\alpha_{23}) = \mathfrak{s}(\mathrm{sp}(a_{23})) = y\varepsilon_3$. Hence, $-xxy^{[\alpha_{12}]}$ and $yxxy^{[\alpha_{23}]}$ are singular top $\mathfrak{s}$-reducible by $f_4^{[\alpha]}$ and $g_0^{[\gamma_0]}$, respectively.

Additionally, we have the following regular ambiguities between f_i and g_n for all $n \geq 0$:

$$\begin{aligned}
\tilde{a}_{1n} &= (xyx^{n+2}y, x, x^{n+1}y, f_1^{[\varepsilon_1]}, g_n^{[\gamma_n]}), & \tilde{a}_{n1} &= (yx^{n+2}yx, yx^{n+1}, x, g_n^{[\gamma_n]}, f_1^{[\varepsilon_1]}),\\
\tilde{a}_{2n} &= (yxyx^{n+2}y, yx, x^{n+2}y, f_2^{[\varepsilon_2]}, g_n^{[\gamma_n]}), & \tilde{a}_{n2} &= (yx^{n+2}yxy, yx^{n+2}, xy, g_n^{[\gamma_n]}, f_2^{[\varepsilon_2]}),\\
\tilde{a}_{3n} &= (xyyx^{n+2}y, xy, x^{n+2}y, f_3^{[\varepsilon_3]}, g_n^{[\gamma_n]}), & \tilde{a}_{n3} &= (yx^{n+2}yy, yx^{n+1}, y, g_n^{[\gamma_n]}, f_3^{[\varepsilon_3]}),\\
\tilde{a}_{4n} &= (xxyx^{n+2}y, xx, x^{n+2}y, f_4^{[\alpha]}, g_n^{[\gamma_n]}), & \tilde{a}_{n4} &= (yx^{n+2}y, yx^{n}, 1, g_n^{[\gamma_n]}, f_4^{[\alpha]}).
\end{aligned}$$

The respective S-polynomials are

$$\begin{aligned}
\operatorname{sp}(\tilde{a}_{1n}) &= -xyx^{n+1}y^{[\varepsilon_1 x^{n+1}y - x\gamma_n]}, & \operatorname{sp}(\tilde{a}_{n1}) &= yx^{n+2}y^{[\gamma_n x - yx^{n+1}\varepsilon_1]},\\
\operatorname{sp}(\tilde{a}_{2n}) &= 0^{[\varepsilon_2 x^{n+2}y - yx\gamma_n]}, & \operatorname{sp}(\tilde{a}_{n2}) &= 0^{[\gamma_n xy - yx^{n+2}\varepsilon_2]},\\
\operatorname{sp}(\tilde{a}_{3n}) &= -xxyx^{n+2}y^{[\varepsilon_3 x^{n+2}y - xy\gamma_n]}, & \operatorname{sp}(\tilde{a}_{n3}) &= yx^{n+3}y^{[\gamma_n y - yx^{n+1}\varepsilon_3]},\\
\operatorname{sp}(\tilde{a}_{4n}) &= 0^{[\alpha x^{n+2}y - xx\gamma_n]}, & \operatorname{sp}(\tilde{a}_{n4}) &= 0^{[\gamma_n - yx^{n}\alpha]},
\end{aligned}$$

which regular $\mathfrak{s}$-reduce to

$$\begin{aligned}
\operatorname{sp}(\tilde{a}_{1n}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\tilde{\alpha}_{1n}]}, & \operatorname{sp}(\tilde{a}_{n1}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\tilde{\alpha}_{n1}]},\\
\operatorname{sp}(\tilde{a}_{3n}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} 0^{[\tilde{\alpha}_{3n}]}, & \operatorname{sp}(\tilde{a}_{n3}) &\overset{*}{\rightarrow}_{G^{[\Sigma]}} \operatorname{sp}(\tilde{a}_{n3}) = yx^{n+3}y^{[\gamma_n y - yx^{n+1}\varepsilon_3]},
\end{aligned}$$

for certain $\tilde{\alpha}_{ij} \in \mathcal{F}_r$. Note that $\mathfrak{s}(\operatorname{sp}(\tilde{a}_{n3})) = \gamma_n y = y\varepsilon_3 y^{n+1}$. Hence, $yx^{n+3}y^{[\gamma_n y - yx^{n+1}\varepsilon_3]}$ is singular top $\mathfrak{s}$-reducible by $g_{n+1}^{[\gamma_{n+1}]}$.

Finally, we also have the following regular ambiguity between all g_i and g_j for $i, j \geq 0$:

$$a'_{ij} = (yx^{i+2}yx^{j+2}y, yx^{i+2}, x^{j+2}y, g_i^{[\gamma_i]}, g_j^{[\gamma_j]}).$$

The respective S-polyomial is $\operatorname{sp}(a'_{ij}) = 0^{[\gamma_i x^{j+2}y - yx^{i+2}\gamma_j]}$.

So, all S-polynomials of $G^{[\Sigma]}$ regular $\mathfrak{s}$-reduce to zero or to a singular top $\mathfrak{s}$-reducible element. Hence, Theorem 34 yields that $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ w.r.t. the generators f_1, f_2, f_3.

Furthermore, we also claimed that the set

$$\tilde{G}^{[\Sigma]} = \{f_1^{[\varepsilon_1]}, f_2^{[\varepsilon_2]}, f_3^{[\varepsilon_3]}, f_4^{[\varepsilon_4]}\} \cup \{yxxy^{[\gamma_0]}\}$$

with $\mathfrak{s}(\gamma_0) = y\varepsilon_3$ is a minimal signature Gröbner basis of $I^{[\Sigma]}$ w.r.t. the generators f_1, f_2, f_3, f_4. To see why this is the case, we note that with f_4 now being a basis element, it has the signature ε_4 instead of $\varepsilon_1 y$. Consequently, $f_4^{[\varepsilon_4]}$ can now be used to regular $\mathfrak{s}$-reduce the S-polynomial $\operatorname{sp}(\tilde{a}_{03}) = yxxxy^{[y\varepsilon_3 y - yx\varepsilon_3]}$ to zero. Therefore, $\tilde{G}^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ w.r.t. the generators f_1, f_2, f_3, f_4.