Signature Gröbner bases in free algebras over rings

Clemens Hofstadler*
clemens.hofstadler@mathematik.uni-kassel.de
Institute of Mathematics, University of Kassel
Kassel, Germany

Thibaut Verron†
thibaut.verron@jku.at
Institute for Algebra, Johannes Kepler University
Linz, Austria

ABSTRACT

We generalize signature Gröbner bases, previously studied in the free algebra over a field or polynomial rings over a ring, to ideals in the *mixed algebra* $R[x_1, \dots, x_k]\langle y_1, \dots, y_n\rangle$ where R is a principal ideal domain. We give an algorithm for computing them, combining elements from the theory of commutative and noncommutative (signature) Gröbner bases, and prove its correctness.

Applications include extensions of the free algebra with commutative variables, e.g., for homogenization purposes or for performing ideal theoretic operations such as intersections, and computations over $\mathbb{Z}$ as universal proofs over fields of arbitrary characteristic.

By extending the signature cover criterion to our setting, our algorithm also lifts some technical restrictions from previous noncommutative signature-based algorithms, now allowing e.g., elimination orderings. We provide a prototype implementation for the case when R is a field, and show that our algorithm for the mixed algebra is more efficient than classical approaches using existing algorithms.

CCS CONCEPTS

• **Computing methodologies** → **Algebraic algorithms**.

KEYWORDS

Signature Gröbner bases, noncommutative polynomials, mixed commutative variables, coefficients in rings, principal ideal domains

ACM Reference Format:
Clemens Hofstadler and Thibaut Verron. 2023. Signature Gröbner bases in free algebras over rings. In *International Symposium on Symbolic and Algebraic Computation 2023 (ISSAC 2023), July 24–27, 2023, Tromsø, Norway.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3597066.3597071

1 INTRODUCTION

Gröbner bases are an essential tool in computational algebra. They are best known in algebras of commutative polynomials over fields [3], but have also been extended to various settings, including polynomials over rings [24, 30, 33, 43], modules [34], skew polynomial rings [13], and noncommutative polynomials in the free algebra over fields [36] or over rings [4, 5, 28, 32, 37, 39, 40, 44]. In this last setting, Gröbner bases have proven to be a key tool in reducing and proving operator identities [6, 18, 19, 45, 46].

In parallel to those generalizations, the last 20 years have seen the development of a new paradigm for computing Gröbner bases, with the concept of signatures [8, 11, 27]. This approach, which improves upon the idea of tracing syzygies presented in the earlier work [35], has had a significant impact on the field, leading to advances also in other algorithmic tools such as staggered linear bases [16, 17], initially introduced in [15].

Beyond their original purpose of optimizing the algorithms, it was more recently observed that the data of signatures also has direct applications. For instance, they have been used in computational geometry [9], and they allow to perform a number of operations on the syzygy module of a family of polynomials, without the additional cost of module Gröbner bases computations [14]. In particular, the data of a Gröbner basis with its signatures makes it possible to easily get a *proof* that an element lies in an ideal, by reconstructing a representation in terms of the original generators [22]. This potential has led to signature Gröbner bases being generalized beyond commutative polynomials over fields, for instance to polynomials over rings [10, 12], to solvable noncommutative algebras [47], and recently to the free algebra [21].

In this paper, we consider two generalizations of signature Gröbner bases in the free algebra at once. First, we consider the case of noncommutative polynomials with some commutative variables, namely elements in $R[X]\langle Y\rangle = R[x_1, \dots, x_k]\langle y_1, \dots, y_n\rangle$. Such objects arise, for example, when introducing auxiliary variables such as homogenization variables or parameters (e.g., when computing the intersection of ideals or the homogeneous part of an ideal). The naive approach, consisting of adding the commutator relations to the input polynomials, is inefficient with signatures, because the information of these relations is not propagated to the signatures.

In addition, we relax the conditions on the base ring, no longer requiring it to be a field, but only a principal ideal domain (PID). This, in particular, allows computations over $\mathbb{Z}$, which can be considered universal as they remain valid in arbitrary characteristic. Furthermore, $R[X]\langle Y\rangle$ provides a natural setting for studying many finitely presented structures, such as Iwahori-Hecke algebras [23, 28] or (discrete) Heisenberg groups [31].

In the noncommutative case, a difficulty is that most ideals do not admit a finite Gröbner basis, and even among those that do, most do not admit a finite Gröbner basis of the module of syzygies. In [21], the authors proposed an algorithm taking advantage of the data encoded within signatures, and of the structure of the syzygy module, to define and compute signature Gröbner bases which may be finite. This is the combined effect of two properties of noncommutative polynomials: the definition of S-polynomials [1] implicitly includes Buchberger's coprime criterion, which ensures that one can only form finitely many S-polynomials with any given

*C. Hofstadler was supported by the Austrian Science Fund (FWF) grant P 32301.
†T. Verron was supported by the Austrian Science Fund (FWF) grant P 34872.

ISSAC 2023, July 24–27, 2023, Tromsø, Norway

ACM ISBN 979-8-4007-0039-2/23/07…$15.00
https://doi.org/10.1145/3597066.3597071

pair of polynomials; and the signature F5 criterion makes it possible to identify a large number of structural syzygies.

In the case without signatures, when attempting to generalize Gröbner bases, it is frequent that, for structural reasons, Buchberger's criterion can no longer eliminate all but finitely many S-polynomials. This was already observed for classical noncommutative Gröbner bases over rings [28, 32], and also carries over to the generalizations at hand: Buchberger's criterion requires also the coefficients to be coprime, and the subsequently weakened criterion cannot ensure that only finitely many S-polynomials remain. In addition, when working with Gröbner bases over PIDs, one needs to compute so-called G-polynomials for each pair of polynomials, and there will typically be infinitely many such G-polynomials.

In this paper, we describe an algorithm for computing signature Gröbner bases for polynomials in the mixed algebra $R[X]\langle Y\rangle$. The algorithms and data structures combine elements from [32] for the combinations and reductions, [21] for managing signatures in the free algebra, and [12] for managing signatures with coefficients in a PID. With the limitations exposed above, one cannot hope that the algorithm terminates, but we show that it correctly enumerates a signature Gröbner basis, as well as a basis of the module of syzygies. The proof combines elements from the theory of signatures over the free algebra and of signatures over PIDs in the commutative case.

A feature of the algorithm is that it relies on the signature cover criterion [12, 14] instead of requiring that every element reduces to 0. As in the commutative case, this allows to decouple the selection strategy used for selecting S- and G-polynomials from the order on the signatures. As a consequence, the algorithm does not have to process S- and G-polynomials by increasing signature. This is particularly important in the noncommutative case, where all algorithms require that the selection strategy is so-called fair. This is a strong requirement excluding for instance elimination orderings. As such, the new algorithm with the selection strategy decoupled from the signature order is the first algorithm that allows to enumerate a signature Gröbner basis in the free algebra for any monomial order.

2 THE MIXED ALGEBRA

Let R be a commutative principal ideal domain (PID) with 1. We assume that R is computable, in the sense that all arithmetic operations, including gcd-computations and the computation of Bézout coefficients, can be performed effectively. Classical examples of such rings are the integers $\mathbb{Z}$ or the univariate polynomial ring $K[x]$ over a field K, with the extended Euclidean algorithm.

We denote by $A = R[X]\langle Y\rangle$ the *mixed algebra* of polynomials in commutative (or central) variables $x_1, \dots, x_k$ and noncommutative variables $y_1, \dots, y_n$. Formally, this algebra is the quotient $R\langle X, Y\rangle/(x_i y_j - y_j x_i, x_i x_j - x_j x_i \mid \forall i, j)$. Note that, in this algebra, $x_i f = f x_i$ for all $f \in R[X]\langle Y\rangle$, but in general $y_i f \neq f y_i$.

A (mixed) monomial in A is a product vw with $v = x_1^{\alpha_1} \cdots x_k^{\alpha_k}$ a (commutative) monomial in X and $w = y_{i_1} y_{i_2} \cdots y_{i_l}$ a (noncommutative) word in Y. We denote by $[X]$ the set of all commutative monomials in X and by $\langle Y\rangle$ the set of all noncommutative words in Y. A term in A is the product of a nonzero coefficient in R and a mixed monomial in A. We denote by $M(A)$ the set of all mixed monomials of A, and by $T(A)$ the set of all terms of A.

Divisibility of mixed monomials and terms in A is defined componentwise: given $c, d \in R$, $u, v \in [X]$ and $a, b \in \langle Y\rangle$, cua divides dvb if and only if c divides d, u divides v, and a is a subword of b.

A monomial ordering $\leq$ is a total ordering on $M(A)$ which is compatible with multiplication, that is, $m \leq m'$ implies $amb \leq am'b$ for all $a, b, m, m' \in M(A)$, and is such that every non-empty set has a minimal element (well-ordering). A monomial ordering naturally defines a partial ordering on $T(A)$, called a term ordering. For ease of notations, we extend the definition of monomial and term to contain 0, which is assumed to be smaller than all other elements.

Given a family $(f_1, \dots, f_r) \in A^r$ of polynomials in A, we let $I = (f_1, \dots, f_r)$ be the (two-sided) ideal generated by $f_1, \dots, f_r$. Furthermore, we consider the free A-bimodule $\Sigma = (A \otimes_{R[X]} A)^r$, see also [7, Sec. 0.11]. We denote its canonical basis by $\varepsilon_1, \dots, \varepsilon_r$, and we equip it with an A-bimodule homomorphism $\overline{\cdot} : \varepsilon_i \mapsto f_i$. A *labeled polynomial* is a pair $(f, \alpha) \in I \times \Sigma$ with $f = \overline{\alpha}$, denoted $f^{[\alpha]}$. The *labeled module* generated by $f_1, \dots, f_r$ is the set of all labeled polynomials and denoted by $I^{[\Sigma]}$. It is isomorphic to Σ as an A-bimodule.

An element $\alpha \in \Sigma$ with $\overline{\alpha} = 0$ is called a *syzygy of* $I^{[\Sigma]}$. The set of all syzygies of $I^{[\Sigma]}$, denoted by $\mathrm{Syz}(I^{[\Sigma]})$, forms an A-bimodule.

A (module) monomial in Σ is a product $ua\varepsilon_i b$ where $u \in [X]$ and $a, b \in \langle Y\rangle$. A term in Σ is the product of a nonzero coefficient and a monomial. The set of all monomials (resp. terms) in Σ is denoted by $M(\Sigma)$ (resp. $T(\Sigma)$). Every $\alpha \in \Sigma$ has a unique representation $\alpha = \sum_{i=1}^{d} c_i u_i a_i \varepsilon_{j_i} b_i$ with nonzero $c_i \in R$ and pairwise different $u_i a_i \varepsilon_{j_i} b_i \in M(\Sigma)$.

A module ordering is a total ordering on $M(\Sigma)$ which is compatible with multiplication and a well-ordering. A module ordering is called *fair* if for any monomial μ, the set of all monomials that are smaller than μ is finite. Given a monomial ordering $\leq$ on A and a module ordering $\preceq$ on Σ, the orders are said to be compatible if for all $u, v \in [X]$, $a, b \in \langle Y\rangle$, $i \in \{1, \dots, r\}$ we have $ua < vb$ iff $ua\varepsilon_i \prec vb\varepsilon_i$ iff $u\varepsilon_i a \prec v\varepsilon_i b$.

As for polynomials, we extend module orderings to partial orderings on terms. More precisely, for $\mu, \sigma \in M(\Sigma)$ and $c, d \neq 0 \in R$, we write $c\mu \simeq d\sigma$ if $\mu = \sigma$, and $c\mu \preceq d\sigma$ if $\mu \prec \sigma$ or $c\mu \simeq d\sigma$.

Given a monomial ordering, the leading term $\mathrm{lt}(f)$ of $f \in A$ is the largest term appearing in the support of f. The leading monomial $\mathrm{lm}(f)$ and the leading coefficient $\mathrm{lc}(f)$ are the corresponding monomial and coefficient, respectively. Given a module ordering, the signature $\mathrm{sig}(\alpha)$ of a module element α is the largest term appearing in the support of α. Note that signatures include coefficients and that they are compatible with scalar multiplication, i.e., $\mathrm{sig}(t\alpha t') = t\,\mathrm{sig}(\alpha)t'$ for $t, t' \in T(A)$.

3 SIGNATURE GRÖBNER BASES

We fix $(f_1, \dots, f_r) \in A^r$ and let $I^{[\Sigma]}$ be the labeled module generated by $f_1, \dots, f_r$. As in other settings, signature Gröbner bases in A are characterised by the fact that all elements in $I^{[\Sigma]}$ are reducible in a way that does not increase the signature. Such reductions are called sig-*reductions* and are defined below. In the setting of coefficient rings several notions of reductions exist (weak, strong, and also modular reductions by the coefficients). In this work, we focus on strong reductions requiring divisibility of the leading coefficients.

Definition 3.1. *Let* $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$. *A combination* $h^{[\gamma]} = f^{[\alpha]} - tg^{[\beta]}b$ *with* $t \in T(A)$, $b \in \langle Y\rangle$ *is a* (top) sig-reduction *if*

$\mathrm{lt}(tgb) = \mathrm{lt}(f) > \mathrm{lt}(h)$ *and* $\mathrm{sig}(t\beta b) \preceq \mathrm{sig}(\alpha)$. *The* sig*-reduction is* regular *if* $\mathrm{sig}(t\beta b) \prec \mathrm{sig}(\alpha)$, *and* singular *if* $\mathrm{sig}(t\beta b) = \mathrm{sig}(\alpha)$. *If such a combination exists,* $f^{[\alpha]}$ *is called* (regular/singular) sig-reducible *by* $g^{[\beta]}$.

As usual, an element $f^{[\alpha]}$ is (regular/singular) sig-reducible by a set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ if there exists $g^{[\beta]} \in G^{[\Sigma]}$ such that $f^{[\alpha]}$ is (regular/singular) sig-reducible by $g^{[\beta]}$. If the result of a sig-reduction of $f^{[\alpha]}$ is $0^{[\gamma]}$, then we say that $f^{[\alpha]}$ sig*-reduces to* 0. We extend these definitions also to sequences of sig-reductions.

Note that sig-reductions do not increase the signature, that is, $\mathrm{sig}(\gamma) \preceq \mathrm{sig}(\alpha)$, with equality for regular sig-reductions and strict inequality for singular sig-reductions. There are also sig-reductions which are neither regular nor singular; in this case $\mathrm{sig}(\gamma) \simeq \mathrm{sig}(\alpha)$.

We extend the definition of (strong) signature Gröbner bases from the commutative case [12, Def. 2.5] in a straightforward way.

Definition 3.2. *A set* $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ *is a* (strong) signature Gröbner basis of $I^{[\Sigma]}$ (up to signature $\sigma \in T(\Sigma)$) *if all* $f \in I^{[\Sigma]}$ *with* $f \neq 0$ *(and* $\mathrm{sig}(\alpha) \prec \sigma$*) are* sig*-reducible by* $G^{[\Sigma]}$.

By disregarding the module labelling from Definition 3.2, one recovers the definition of classical Gröbner bases in A [32]. The polynomial parts of a signature Gröbner basis of $I^{[\Sigma]}$ form a Gröbner basis of $I = (f_1, \ldots, f_r)$.

Signature Gröbner bases were introduced with the goal of using signatures of (known) syzygies to predict reductions to zero, and thereby, speed up Gröbner basis computations. Later, it was observed that signature-based algorithms also allow to compute, as a byproduct, a Gröbner basis of the syzygy module as defined below.

Definition 3.3. *An element* $\alpha \in \Sigma$ *is* (top) reducible *by a set* $H \subseteq \Sigma$ *if there exist* $\gamma \in H$, $t \in T(A)$, $b \in \langle Y \rangle$ *such that* $\mathrm{sig}(\alpha) = \mathrm{sig}(t\gamma b)$.

A set of syzygies $H \subseteq \mathrm{Syz}(I^{[\Sigma]})$ *is a* syzygy basis of $I^{[\Sigma]}$ (up to signature $\sigma \in T(\Sigma)$) *if every nonzero syzygy* $\alpha \in \mathrm{Syz}(I^{[\Sigma]})$ *(with* $\mathrm{sig}(\alpha) \prec \sigma$*) is reducible by* H.

4 AMBIGUITIES

In order to define S- (and G-)polynomials in our setting, we first adapt the notion of *ambiguities* from [1] to our setting. Ambiguities characterise situations where one term can be reduced in two different ways, and the aim of a (signature) Gröbner basis computation is to resolve ambiguities by forming S- (and G-)polynomials. We first recall the definition of ambiguities for noncommutative words, and then subsequently extend them to mixed monomials and to labeled polynomials.

Definition 4.1. *Let* $p, q \in \langle Y \rangle$. *If there exist* $a, b \in \langle Y \rangle \setminus \{1\}$ *with* $|a| < |q|$ *and* $|b| < |p|$ *such that* $ap = qb$, *resp.* $pa = bq$, *then we call the tuple* $(a \otimes 1, 1 \otimes b, p, q)$, *resp.* $(1 \otimes a, b \otimes 1, p, q)$, *an* overlap ambiguity *of* p *and* q.

If there exist $a, b \in \langle Y \rangle$ *such that* $p = aqb$, *resp.* $apb = q$, *then we call the tuple* $(1 \otimes 1, a \otimes b, p, q)$, *resp.* $(a \otimes b, 1 \otimes 1, p, q)$, *an* inclusion ambiguity *of* p *and* q.

Finally, for every $m \in \langle Y \rangle$, *we call the tuples* $(1 \otimes mq, pm \otimes 1, p, q)$ *and* $(qm \otimes 1, 1 \otimes mp, p, q)$ external ambiguities *of* p *and* q.

Remark 4.2. *Note that two words* p, q *can only have finitely many overlap and inclusion ambiguities, but they always have infinitely many external ambiguities.*

Definition 4.3. *Let* $up, vq \in M(A)$ *and* $(a \otimes b, c \otimes d, p, q)$ *be an ambiguity of* p *and* q. *An* ambiguity *of* up *and* vq *is given by* $(u'a \otimes b, v'c \otimes d, up, vq)$, *where* $u' = \mathrm{lcm}(u, v)/u$ *and* $v' = \mathrm{lcm}(u, v)/v$.

For $f, g \in A \setminus \{0\}$, *an* ambiguity *of* f *and* g *is* $(a \otimes b, c \otimes d, f, g)$ *where* $(a \otimes b, c \otimes d, \mathrm{lm}(f), \mathrm{lm}(g))$ *is an ambiguity of* $\mathrm{lm}(f)$ *and* $\mathrm{lm}(g)$. *We denote by* $\mathrm{amb}(f, g)$ *the set of all ambiguities of* f *and* g. *When clear by the context, we shall simply write* $(a \otimes b, c \otimes d) \in \mathrm{amb}(f, g)$.

We define analogously ambiguities of labeled polynomials by considering their polynomial parts.

Note that if $(m_1 \otimes n_1, m_2 \otimes n_2, f, g)$ is an ambiguity of f and g, then $\mathrm{lm}(m_1 f n_1) = \mathrm{lm}(m_2 g n_2)$.

Before defining S- and G-polynomials with module labelling, we introduce some useful terminology for ambiguities of labeled polynomials. In the following, for a pair of nonzero $f, g \in A$, let $\mathrm{lcmlc}(f, g)$ be the least common multiple of $\mathrm{lc}(f)$ and $\mathrm{lc}(g)$.

Definition 4.4. *Let* $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ *be such that* $f, g \neq 0$ *and let* $a = (m_1 \otimes n_1, m_2 \otimes n_2, f^{[\alpha]}, g^{[\beta]}) \in \mathrm{amb}(f^{[\alpha]}, g^{[\beta]})$. *The* leading monomial *of* a *is* $\mathrm{LM}(a) := \mathrm{lm}(m_1 f n_1) = \mathrm{lm}(m_2 g n_2)$ *and, with* $c_f = \frac{\mathrm{lcmlc}(f,g)}{\mathrm{lc}(f)}$, $c_g = \frac{\mathrm{lcmlc}(f,g)}{\mathrm{lc}(g)}$, *the* signature *of* a *is*

$$\mathrm{SIG}(a) := \max\left(\mathrm{sig}(c_f m_1 \alpha n_1), -\mathrm{sig}(c_g m_2 \beta n_2)\right),$$

choosing the first in case of tie. The ambiguity a *is called* regular *if* $\mathrm{sig}(m_1 \alpha n_1) \neq \mathrm{sig}(m_2 \beta n_2)$ *and* singular *if* $\mathrm{sig}(c_f m_1 \alpha n_1) = \mathrm{sig}(c_g m_2 \beta n_2)$.

Remark 4.5. *Recall that the ordering on the signatures is only partial, and thus, it can happen that an ambiguity* a *is neither regular nor singular.*

The following lemma asserts that any situation where multiples of two labeled polynomials share a common leading monomial but differ in their signatures, can be characterised by a regular ambiguity of the two elements.

Lemma 4.6. *Let* $g_1^{[\beta_1]}, g_2^{[\beta_2]} \in I^{[\Sigma]}$ *be such that* $g_1, g_2 \neq 0$ *and let* $t_i \in T(A), b_i \in \langle Y \rangle$, $i = 1, 2$, *such that*

$$\mathrm{lm}(t_1 g_1 b_1) = \mathrm{lm}(t_2 g_2 b_2) \quad \text{and} \quad \mathrm{sig}(t_1 \beta_1 b_1) \succ \mathrm{sig}(t_2 \beta_2 b_2).$$

Then there exists a regular ambiguity $a \in \mathrm{amb}(g_1^{[\beta_1]}, g_2^{[\beta_2]})$, $t_3 \in T(A), b_3 \in \langle Y \rangle$ *such that* $t_3 \mathrm{LM}(a) b_3 = \mathrm{lm}(t_i g_i b_i)$ *and* $t_3 \mathrm{SIG}(a) b_3 \simeq \mathrm{sig}(t_1 \beta_1 b_1)$, *with equality of signatures if* $\mathrm{lc}(t_1 g_1 b_1) = \mathrm{lc}(t_2 g_2 b_2)$.

Proof. Write $t_i = c_i u_i a_i$ and $\mathrm{lm}(g_i) = v_i w_i$ with $c_i \in R, u_i, v_i \in [X], a_i, w_i \in \langle Y \rangle$. Then, by assumption $u_1 v_1 = u_2 v_2$ and $a_1 w_1 b_1 = a_2 w_2 b_2 =: W$. If, in W, either of w_1 and w_2 is completely contained in the other, then there exists an inclusion ambiguity of w_1 and w_2 characterising this situation, otherwise one of them starts earlier in W and the other finishes later, in which case there is an overlap or external ambiguity of w_1 and w_2 characterising this situation. Hence, in any case, there exists an ambiguity $(p_1 \otimes q_1, p_2 \otimes q_2)$ of w_1 and w_2 such that $p_1 w_1 q_1 = p_2 w_2 q_2$ is a subword of W, i.e., there exist $l, r \in \langle Y \rangle$ such that $l p_1 w_1 q_1 r = l p_2 w_2 q_2 r = W$. By definition $a = (v_1' p_1 \otimes q_1, v_2' p_2 \otimes q_2)$, with $v_i' = \mathrm{lcm}(v_1, v_2)/v_i$, is an ambiguity in $\mathrm{amb}(g_1^{[\beta_1]}, g_2^{[\beta_2]})$. We claim that a satisfies the conditions of the lemma with $t_3 = m_3 l \in T(A)$, where $m_3 = u_1 v_1 / \mathrm{lcm}(v_1, v_2) = u_2 v_2 / \mathrm{lcm}(v_1, v_2)$, and $b_3 = r$. The condition on the leading monomials is clear by construction. For the claim concerning the signa-

tures, we note that $m_3 v_i' = u_i$ and by choice of l, r we have $lp_i = a_i$ and $q_i r = b_i$. Thus, for $i = 1, 2$,

$$\begin{aligned}\operatorname{sig}(t_3 v_i' p_i \beta_i q_i b_3) &= \operatorname{sig}(m_3 v_i' l p_i \beta_i q_i r) \\ &= \operatorname{sig}(u_i a_i \beta_i b_i) \simeq \operatorname{sig}(t_i \beta_i b_i),\end{aligned}$$

showing that a is regular since $\operatorname{sig}(t_1\beta_1 b_1) \succ \operatorname{sig}(t_2\beta_2 b_2)$ and that $t_3 \operatorname{SIG}(a) b_3 = \operatorname{sig}(t_3 v_1' p_1 \beta_1 q_1 b_3) \simeq \operatorname{sig}(t_1\beta_1 b_1)$.

For the final part, assume that also $\operatorname{lc}(t_1 g_1 b_1) = \operatorname{lc}(t_2 g_2 b_2)$, i.e., $c_1 \operatorname{lc}(g_1) = c_2 \operatorname{lc}(g_2)$. Then, multiplying t_3 by $c_1 \operatorname{lc}(g_1)/\operatorname{lcmlc}(g_1, g_2)$ yields the claimed equality of signatures. □

We extend the definition of S-polynomials to our setting.

Definition 4.7. *Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ be such that $f, g \neq 0$ and let $a = (m_1 \otimes n_1, m_2 \otimes n_2) \in \operatorname{amb}(f^{[\alpha]}, g^{[\beta]})$. The* S-polynomial *of a is*

$$\text{S-Pol}(a) \coloneqq \frac{\operatorname{lcmlc}(f,g)}{\operatorname{lc}(f)} m_1 f^{[\alpha]} n_1 - \frac{\operatorname{lcmlc}(f,g)}{\operatorname{lc}(g)} m_2 g^{[\beta]} n_2.$$

As usual, S-polynomials are defined so that leading terms cancel, i.e., if $h^{[\gamma]} = \text{S-Pol}(a)$, then $\operatorname{lm}(h) \prec \operatorname{LM}(a)$. Furthermore, $\operatorname{sig}(\gamma) \preceq \operatorname{SIG}(a)$, with equality if and only if the ambiguity is regular and strict inequality if and only if the ambiguity is singular.

In the setting of coefficient rings, we also need G-polynomials, which do not aim at canceling leading terms but at obtaining minimal leading coefficients.

Definition 4.8. *Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ be such that $f, g \neq 0$ and let $a = (m_1 \otimes n_1, m_2 \otimes n_2) \in \operatorname{amb}(f^{[\alpha]}, g^{[\beta]})$. Furthermore, let $c, d \in R$ be Bézout coefficients of $\operatorname{lc}(f)$ and $\operatorname{lc}(g)$, i.e., $c\operatorname{lc}(f) + d\operatorname{lc}(g) = \gcd(\operatorname{lc}(f), \operatorname{lc}(g))$. The* G-polynomial *of a w.r.t. c, d is*

$$\text{G-Pol}_{c,d}(a) \coloneqq c m_1 f^{[\alpha]} n_1 + d m_2 g^{[\beta]} n_2.$$

While the coefficients c, d in the definition of G-polynomials are not unique, the leading term is. More precisely, the leading monomial of $\text{G-Pol}_{c,d}(a)$ is $\operatorname{LM}(a)$ and the leading coefficient is $\gcd(\operatorname{lc}(f), \operatorname{lc}(g))$. The signature of the G-polynomial, however, depends on the choice of c, d. A crucial observation [12, Prop. 2.14] is that these coefficients can be chosen so that G-polynomials are *never* singular, i.e., so that the signatures of the two summands do not cancel each other.

Lemma 4.9. *Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ and let $a \in \operatorname{amb}(f^{[\alpha]}, g^{[\beta]})$. There exist $c, d \in R$ such that $\operatorname{sig}(\text{G-Pol}_{c,d}(a)) \simeq \operatorname{SIG}(a)$.*

Proof. The proof of [12, Prop. 2.14] only relies on properties of the leading coefficients and carries over directly to our setting. □

We only consider Bézout coefficients as in Lemma 4.9, and refer to the corresponding G-polynomial as *the* G-polynomial of a, denoted by $\text{G-Pol}(a)$. Note that if $h^{[\gamma]} = \text{G-Pol}(a)$, then $\operatorname{sig}(\gamma) \simeq \operatorname{SIG}(a)$ and $\operatorname{lm}(h) = \operatorname{LM}(a)$.

The following lemma captures the significance of G-polynomials for our computations. It states that if a leading term can be written as a sum of two other leading terms, then it is divisible by the leading term of a G-polynomial.

Lemma 4.10. *Let $f^{[\alpha]}, g_1^{[\beta_1]}, g_2^{[\beta_2]} \in I^{[\Sigma]}$ be such that $f, g_1, g_2 \neq 0$ and such that there exist $t_i \in T(A), b_i \in \langle Y \rangle$, $i = 1, 2$, with*

$$\operatorname{lt}(f) = \operatorname{lt}(t_1 g_1 b_1) + \operatorname{lt}(t_2 g_2 b_2) \quad \text{and} \quad \operatorname{sig}(t_1\beta_1 b_1) \succ \operatorname{sig}(t_2\beta_2 b_2).$$

Then there exist $g_3^{[\beta_3]} = \text{G-Pol}(a)$ for some $a \in \operatorname{amb}(g_1^{[\beta_1]}, g_2^{[\beta_2]})$ and $t_3 \in T(A), b_3 \in \langle Y \rangle$ such that $\operatorname{lt}(t_3 g_3 b_3) = \operatorname{lt}(f)$ and $\operatorname{sig}(t_3\beta_3 b_3) \simeq \operatorname{sig}(t_1\beta_1 b_1)$.

Proof. Note that $\operatorname{lm}(t_1 g_1 b_1) = \operatorname{lm}(t_2 g_2 b_2)$. Thus, the result follows from Lemma 4.6, 4.9, and the properties of G-polynomials. □

Definition 4.11. *A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is* complete *if the G-polynomials of all ambiguities of $G^{[\Sigma]}$ are* sig*-reducible by $G^{[\Sigma]}$.*

A set can be completed by adding G-polynomials to it. The following definition extends the idea of G-polynomials to syzygies. To this end, we define the least common multiple of two module monomials as follows. Let $\sigma_i = u_i a_i \varepsilon_j b_i \in M(\Sigma)$, $i = 1, 2$. If $a_{k'}$ is a suffix of a_k and $b_{l'}$ is a prefix of b_l, where $\{k, k'\} = \{l, l'\} = \{1, 2\}$, then $\operatorname{lcm}(\sigma_1, \sigma_2) \coloneqq \operatorname{lcm}(u_1, u_2) a_k \varepsilon_j b_l$.

Definition 4.12. *Let $\gamma_1, \gamma_2 \in \operatorname{Syz}(I^{[\Sigma]})$ be such that $\operatorname{sig}(\gamma_i) = c_i \sigma_i$ with $c_i \in R$, $\sigma_i \in M(\Sigma)$. Assume that $\operatorname{lcm}(\sigma_1, \sigma_2)$ is defined and let $m_i \in M(A)$, $b_i \in \langle Y \rangle$ be such that $\operatorname{lcm}(\sigma_1, \sigma_2) = m_i \sigma_i b_i$. Also, let c, d be Bézout coefficients of $\gcd(c_1, c_2)$. The* sig-Combination *of γ_1 and γ_2 is* $\text{sig-Comb}(\gamma_1, \gamma_2) \coloneqq c m_1 \gamma_1 b_1 + d m_2 \gamma_2 b_2$.

A set $H \subseteq \operatorname{Syz}(I^{[\Sigma]})$ is sig-complete *if any sig-Combination of elements in H is reducible by H.*

To end this section, we introduce a concept needed later.

Definition 4.13. *Let $f^{[\alpha]} \in I^{[\Sigma]}$ and $G^{[\Sigma]} \subseteq I^{[\Sigma]}$. We say that $f^{[\alpha]}$ is* super reducible *by $G^{[\Sigma]}$ if there exist $g^{[\beta]} \in G^{[\Sigma]}$ and $t \in T(A), b \in \langle Y \rangle$ such that $\operatorname{sig}(\alpha) = \operatorname{sig}(t\beta b)$ and $\operatorname{lm}(f) = \operatorname{lm}(tgb)$.*

Note that super reducibility need not imply sig-reducibility as the former only requires equality of the leading monomials, without considering the leading coefficients. However, if a set of reducers is complete, a super reducible element is also sig-reducible. This the result of Proposition 4.14, which is an adaptation of [12, Prop. 2.19].

Proposition 4.14. *Let $f^{[\alpha]} \in I^{[\Sigma]}$ and $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be complete and a signature Gröbner basis up to signature $\operatorname{sig}(\alpha)$. If $f^{[\alpha]}$ is super reducible by $G^{[\Sigma]}$, then it is also* sig*-reducible by $G^{[\Sigma]}$.*

Proof. We essentially follow the proof of [12, Prop. 2.19]. Super reducibility implies the existence of $g_1^{[\beta_1]} \in G^{[\Sigma]}$ and $t_1 \in T(A)$, $b_1 \in \langle Y \rangle$ such that $\operatorname{sig}(\alpha) = \operatorname{sig}(t_1\beta_1 b_1)$ and $\operatorname{lm}(f) = \operatorname{lm}(t_1 g_1 b_1)$. If, in fact, $\operatorname{lt}(f) = \operatorname{lt}(t_1 g_1 b_1)$, then $f^{[\alpha]}$ is sig-reducible by $g_1^{[\beta_1]}$. Otherwise, with $h^{[\gamma]} = f^{[\alpha]} - t_1 g_1^{[\beta_1]} b_1$, we have $\operatorname{lm}(h) = \operatorname{lm}(f)$ and $\operatorname{sig}(\gamma) \prec \operatorname{sig}(\alpha)$. By assumption, $h^{[\gamma]}$ is sig-reducible by $G^{[\Sigma]}$. Let $g_2^{[\beta_2]}$ be such a reducer with $t_2 \in T(A)$, $b_2 \in \langle Y \rangle$ such that $\operatorname{sig}(\gamma) \succeq \operatorname{sig}(t_2\beta_2 b_2)$ and $\operatorname{lt}(h) = \operatorname{lt}(t_2 g_2 b_2)$. Consequently, we have $\operatorname{lt}(f) = \operatorname{lt}(t_1 g_1 b_1) + \operatorname{lt}(t_2 g_2 b_2)$ and $\operatorname{sig}(\alpha) \succ \operatorname{sig}(\gamma) \succeq \operatorname{sig}(t_2\beta_2 b_2)$. By Lemma 4.10 there exists $g_3^{[\beta_3]} = \text{G-Pol}(a)$ for some $a \in \operatorname{amb}(g_1^{[\beta_1]}, g_2^{[\beta_2]})$ and $t_3 \in T(A), b_3 \in \langle Y \rangle$ such that $\operatorname{lt}(t_3 g_3 b_3) = \operatorname{lt}(f)$ and $\operatorname{sig}(t_3\beta_3 b_3) \simeq \operatorname{sig}(t_1 g_1 b_1) = \operatorname{sig}(\alpha)$. Since $G^{[\Sigma]}$ is complete, $g_3^{[\beta_3]}$ is sig-reducible by $G^{[\Sigma]}$, and any reducer of $g_3^{[\beta_3]}$ can be used to sig-reduce $f^{[\alpha]}$. □

5 COVER CRITERION

In this section, we adapt the cover criterion [12, 14] to our setting, yielding an effective characterisation of signature Gröbner bases.

Definition 5.1. *Let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ and $H \subseteq \mathrm{Syz}(I^{[\Sigma]})$. Furthermore, let $g_1^{[\beta_1]}, g_2^{[\beta_2]} \in I^{[\Sigma]}$. An ambiguity $a \in \mathrm{amb}(g_1^{[\beta_1]}, g_2^{[\beta_2]})$ is* covered *by $(G^{[\Sigma]}, H)$ if there exist $g^{[\beta]} \in G^{[\Sigma]}$, $\gamma \in H$ and $t, t' \in T(A)$, $b, b' \in \langle Y \rangle$ such that the following conditions hold:*

- $\mathrm{SIG}(a) = \mathrm{sig}(t\beta b) + \mathrm{sig}(t'\gamma b')$;
- $\mathrm{lm}(tgb) < \mathrm{LM}(a)$;

Remark 5.2. *In Definition 5.1, either of t and t' can also be 0. If $t = 0$, then $\mathrm{lm}(tgb) = 0$ and the second condition is trivially fulfilled.*

Our version of the cover criterion differs in one main point from the classical one [14, Thm. 2.4] for (commutative) polynomials over coefficient fields: We need to consider linear combinations to form the signature. This requirement comes from the fact that we deal with coefficient rings and is also necessary in the commutative case, see [12, Def. 2.20].

We can prove a characterisation of noncommutative signature Gröbner bases and syzygy bases using the cover criterion. The following theorem is an adaptation of [12, Thm. 3.1].

Theorem 5.3. *Let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ and $H \subseteq \mathrm{Syz}(I^{[\Sigma]})$ be such that the following conditions hold:*

(1) for all $g^{[\beta]} \in G^{[\Sigma]} : g \neq 0$;
(2) $G^{[\Sigma]}$ is complete and H is sig-complete;
(3) all $\sigma \in T(A)$ are reducible by $H \cup \{\beta \mid g^{[\beta]} \in G^{[\Sigma]}\}$;
(4) all regular ambiguities of $G^{[\Sigma]}$ are covered by $(G^{[\Sigma]}, H)$;

Then $G^{[\Sigma]}$ is a signature Gröbner basis and H is a syzygy basis of $I^{[\Sigma]}$.

Proof. The proof is an adaption of that of [14, Thm. 2.4]. Assume, for contradiction, that there exists $f^{[\alpha]} \in I^{[\Sigma]}$ such that either $f \neq 0$ and $f^{[\alpha]}$ is not sig-reducible by $G^{[\Sigma]}$ or $f = 0$ and α is not reducible by H. Pick such $f^{[\alpha]}$ with minimal signature. Note that this implies that $G^{[\Sigma]}$ is, by definition, a signature Gröbner basis up to signature $\mathrm{sig}(\alpha)$.

Let $g_1^{[\beta_1]} \in G^{[\Sigma]}, \gamma_1 \in H$ and $t_1, t_1' \in T(A), b_1, b_1' \in \langle Y \rangle$ such that

$$\mathrm{sig}(\alpha) = \mathrm{sig}(t_1\beta_1 b_1) + \mathrm{sig}(t_1'\gamma_1 b_1'). \tag{1}$$

By assumption, such a decomposition exists (in fact, with either $t_1 = 0$ or $t_1' = 0$ but we do not require this for (1)). We select these elements so that $\mathrm{lm}(t_1 g_1 b_1)$ is minimal and claim that $t_1 g_1^{[\beta_1]} b_1$ is not regular sig-reducible by $G^{[\Sigma]}$.

To prove this, suppose that $t_1 g_1^{[\beta_1]} b_1$ is regular sig-reducible by $g_2^{[\beta_2]}$, i.e., there exist $t_2 \in T(A), b_2 \in \langle Y \rangle$ such that $\mathrm{lt}(t_1 g_1 b_1) = \mathrm{lt}(t_2 g_2 b_2)$ and $\mathrm{sig}(t_1\beta_1 b_1) \succ \mathrm{sig}(t_2\beta_2 b_2)$. Then Lemma 4.6 implies the existence of a regular ambiguity $a \in \mathrm{amb}(g_1^{[\beta_1]}, g_2^{[\beta_2]})$ and $t_3 \in T(A), b_3 \in \langle Y \rangle$ such that

$$t_3 \mathrm{LM}(a) b_3 = \mathrm{lm}(t_i g_i b_i) \;\;\&\;\; t_3 \mathrm{SIG}(a) b_3 = \mathrm{sig}(t_1\beta_1 b_1). \tag{2}$$

By assumption a is covered by $(G^{[\Sigma]}, H)$, i.e., there exist $g^{[\beta]} \in G^{[\Sigma]}, \gamma \in H$ and $t, t' \in T(A), b, b' \in \langle Y \rangle$ such that $\mathrm{lm}(tgb) < \mathrm{LM}(a)$ and $\mathrm{SIG}(a) = \mathrm{sig}(t\beta b) + \mathrm{sig}(t'\gamma b')$. With (1) and (2), this yields

$$\mathrm{sig}(\alpha) = \mathrm{sig}(t_3 t\beta b b_3) + \mathrm{sig}(t_3 t'\gamma b' b_3) + \mathrm{sig}(t_1'\gamma_1 b_1')$$

and $\mathrm{lm}(t_3 tgbb_3) < \mathrm{lm}(t_1 g_1 b_1)$. Let $\delta = \text{sig-Comb}(\gamma_1, \gamma) \in H$, which is well-defined. Since, by definition, $\mathrm{sig}(\delta)$ divides the sum $\mathrm{sig}(t_3 t'\gamma b' b_3) + \mathrm{sig}(t_1'\gamma_1 b_1')$, the pair $(g^{[\beta]}, \delta)$ yields a decomposition of $\mathrm{sig}(\alpha)$ with smaller leading monomial than $\mathrm{lm}(t_1 g_1 b_1)$; a contradiction to the minimality of $\mathrm{lm}(t_1 g_1 b_1)$.

Thus, $t_1 g_1^{[\beta_1]} b_1$ is not regular sig-reducible. Now, we distinguish between two cases depending on whether $f = 0$ or not.

If $f \neq 0$, then $\mathrm{lm}(f) \neq \mathrm{lm}(t_1 g_1 b_1)$ because otherwise $f^{[\alpha]} - t_1' 0^{[\gamma_1]} b_1'$ would be super reducible by $g_1^{[\beta_1]}$, and thus, by Proposition 4.14, sig-reducible by $G^{[\Sigma]}$. But then also $f^{[\alpha]}$ would be sig-reducible – a contradiction.

Let $f_1^{[\alpha_1]} = f^{[\alpha]} - t_1 g_1^{[\beta_1]} b_1 - t_1' 0^{[\gamma_1]} b_1'$. Then $\mathrm{sig}(\alpha_1) \prec \mathrm{sig}(\alpha)$ and $\mathrm{lt}(f_1) = \max(\mathrm{lt}(f), \mathrm{lt}(t_1 g_1 b_1)) \neq 0$. By minimality of $\mathrm{sig}(\alpha)$, $f_1^{[\alpha_1]}$ is sig-reducible by $G^{[\Sigma]}$. But this implies that $f^{[\alpha]}$ or $t_1 g_1^{[\beta_1]} b_1$ is regular sig-reducible by $G^{[\Sigma]}$, which is a contradiction.

If $f = 0$ and $f_1^{[\alpha_1]}$ is like before, then $\mathrm{lt}(f_1) = \mathrm{lt}(t_1 g_1 b_1)$. Now, if $f_1 \neq 0$, then $f_1^{[\alpha_1]}$ being sig-reducible implies that $t_1 g_1^{[\beta_1]} b_1$ is regular sig-reducible by $G^{[\Sigma]}$, which is a contradiction. Thus $f_1 = t_1 g_1 b_1 = 0$, and by assumption on $G^{[\Sigma]}$, we can conclude $t_1 = 0$, showing that α is reducible by $\gamma_1 \in H$. □

6 ALGORITHM

6.1 Description

Algorithm 1: Signature Gröbner basis

Input: $(f_1, \ldots, f_r) \in A^r$ generating a labeled module $I^{[\Sigma]}$
Output:
- $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ a signature Gröbner basis of $I^{[\Sigma]}$
- $H \subseteq \mathrm{Syz}(I^{[\Sigma]})$ a syzygy basis of $I^{[\Sigma]}$

$G^{[\Sigma]} \leftarrow \emptyset$; $H \leftarrow \emptyset$; $P \leftarrow \{(f_1^{[\varepsilon_1]}, \mathtt{N}), \ldots, (f_r^{[\varepsilon_r]}, \mathtt{N})\}$;
while $P \neq \emptyset$ **:**
  select and remove $(p^{[\pi]}, \mathtt{type})$ from P ;
  if type is not $\mathrm{S}(a)$ or a is not covered by $(G^{[\Sigma]}, H)$ **:**
    $p'^{[\pi']} \leftarrow$ result of regular sig-reducing $p^{[\pi]}$ by $G^{[\Sigma]}$;
    if $p' = 0$ **:**
      $H \leftarrow H \cup \{\pi'\}$, and make H sig-complete ;
    else:
      $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{p'^{[\pi']}\}$;
      for $g^{[\beta]} \in G^{[\Sigma]}$ and $a \in \mathrm{amb}(p'^{[\pi']}, g^{[\beta]})$ **:**
        add $(\text{S-Pol}(a), \mathrm{S}(a))$ to P if a is regular;
        add $(\text{G-Pol}(a)), \mathrm{G}(a))$ to P;
      end
end
return $G^{[\Sigma]}, H$

Equipped with Theorem 5.3, we can describe an algorithm for enumerating signature Gröbner bases and syzygy bases in A. This algorithm combines key elements of Kandri-Rody and Kapur's algorithm [24] for Gröbner bases over $\mathbb{Z}$ with signatures [12] and the general algorithm for computing signature Gröbner bases in free algebras over fields [21]. The difference between the free algebra and the mixed algebra is not apparent in the algorithm, but the computation of ambiguities, S- and G-polynomials and the reductions are using the definitions from the mixed algebra.

The algorithm runs on a loop, processing polynomials from a queue. At each step, it selects a polynomial, and if not redundant, reduces it and forms new polynomials from it, adding them to the queue. The algorithm ensures that, for every ambiguity of $G^{[\Sigma]}$, an element is eventually added which covers it.

As in the classical case, S- and G-polynomials are added for different purposes: S-polynomials create new leading monomials, and G-polynomials create new leading coefficients for existing leading monomials. The cover criterion concerns the existence of leading monomials in the basis, and can be used to skip over S-polynomials which correspond to an ambiguity that is already covered. The situation is different for G-polynomials: even if the corresponding ambiguity is covered, it is necessary to process and add the G-polynomial to complete the set $G^{[\Sigma]}$.

This requires keeping track of the construction of each labeled polynomial in the algorithm. For this purpose, the main queue P contains pairs $(p^{[\pi]}, \texttt{type})$, where `type` is either the symbol N indicating that p is one of the input polynomials, or the symbol $\mathrm{S}(a)$, resp. $\mathrm{G}(a)$, indicating that $p^{[\pi]}$ is the S-polynomial, resp. the G-polynomial, of the ambiguity a.

As is classically done when presenting signature-based algorithms, the definitions, properties and the algorithm are stated using labeled polynomials, carrying their entire module representation. However, all those properties only require considering the signature of the module representation, and the true strength is that the algorithms need only maintain pairs $(f, \mathrm{sig}(\alpha))$ instead of labeled polynomials $f^{[\alpha]}$. In that case, the output only contains the signatures of the computed polynomials and syzygies, but the full module representations can be recovered *a posteriori*. We refer to [14, 21] for details on that reconstruction step.

6.2 Spooling the list of pairs & Correctness

For brevity, the presentation of the algorithm is simplified concerning the handling of the queue of pairs. Unlike in the commutative case or the free case over fields, in general the inserting from line 10 to 12 involves infinitely many elements. In order for the algorithm to correctly enumerate a signature Gröbner basis, it needs to process all possible S- and G-polynomials, so it cannot enter an infinite loop inside of the main loop (necessarily infinite).

Instead, the algorithm should be modified to add a spooling machinery ensuring that all pairs are processed. We detail a possible implementation of such a mechanism. The main idea is that the algorithm must ensure that P is finite at all times. The spooling mechanism ensures that by adding a finite number of pairs to P, then adding more whenever they have all been processed. The additional mechanism would then run in parallel for all sources of pairs, ensuring that the pairs are processed in a fair order.

More precisely, we assume that we know a way to enumerate ambiguities, that is, we are given two functions:

- `firstamb` taking as input two labeled polynomials $f^{[\alpha]}$ and $g^{[\beta]}$, and returning an ambiguity a_0 of them;
- `nextamb` taking as input an ambiguity a of two labeled polynomials $f^{[\alpha]}$ and $g^{[\beta]}$, and returning another ambiguity $n(a)$ of them;

with the property that $\{a_0, n(a_0), n(n(a_0)), \dots\} = \mathrm{amb}(f^{[\alpha]}, g^{[\beta]})$.

The algorithm would maintain an additional variable `spool`, which is a finite list of tuples formed of two labeled polynomials and an ambiguity between them. The lines 10 to 12 would be replaced by initialization in that list:

Algorithm 1a: Add the ambiguities to the spooling queue

```
12a for g^[β] ∈ G^[Σ] :
12b     a_0 ← firstamb(p'^[π'], g^[β]);
12c     add a_0 to spool;
12d end
```

The construction of the pairs would be done closer to their actual use, by adding the following lines at the very end of the main loop, just prior to selection of the next pair:

Algorithm 1b: Process ambiguities in the queue

```
16a for i ∈ {1, ..., #spool} :
16b     a ← spool[i];
16c     add (S-Pol(a), S(a)) to P if a is regular;
16d     add (G-Pol(a), G(a)) to P ;
16e     spool[i] ← nextamb(a);
16f end
```

This has the effect of adding finitely many new elements to P, namely at most 2 for each element of `spool`, and updating `spool` to generate new elements the next time the code is evaluated.

The main property that the machinery must satisfy is that it should correctly enumerate all ambiguities of pairs of polynomials. This property, called a fair selection strategy, was originally introduced for the computation of subalgebra bases [25, 42] and adopted for noncommutative bases in [38].

Definition 6.1. *Algorithm 1 is called* fair *if, given any ambiguity of elements in $G^{[\Sigma]}$, the corresponding S- and G-polynomials are eventually processed in the main loop or discarded.*

Proposition 6.2. *With the structure described above, and if insertion and selection in P are done first in, first out, the algorithm is fair.*

Proof. Let $g_i^{[\beta_i]}, g_j^{[\beta_j]} \in G^{[\Sigma]}$ and let a be an ambiguity between them. Since the function `nextamb` enumerates all ambiguities of $g_i^{[\beta_i]}$ and $g_j^{[\beta_j]}$, eventually the insertion mechanism reaches the ambiguity a, at which point the corresponding S- and G-polynomials are either inserted into P or discarded. If the S-polynomial is discarded, there is nothing to prove. If it is inserted, let N be the length of the list P after insertion. Since selection in P is done on a first in, first out basis, after N runs through the loop, the S-polynomial will be processed. The same applies to the G-polynomial. □

Theorem 6.3. *If Algorithm 1 is fair, then it correctly enumerates a signature Gröbner basis and a syzygy basis of $I^{[\Sigma]}$.*

Proof. We prove that the algorithm enforces the requirements of Theorem 5.3. First, by construction all elements added to $G^{[\Sigma]}$ have a nonzero polynomial part. The bases $G^{[\Sigma]}$ and H are complete and sig-complete respectively, because all G-polynomials and all sig-Combinations are added to them. All signatures ε_i are processed, and result in either an element in H or in $G^{[\Sigma]}$, depending on whether $f_i^{[\varepsilon_i]}$ regular sig-reduces to 0 or not. Finally, the algorithm ensures that all ambiguities it considers are covered: either the ambiguity a is already covered, or an element is added to either

$G^{[\Sigma]}$ or H with signature $\mathrm{sig}(a)$. Either way, this element covers the ambiguity a. Finally, since the algorithm is fair, it processes all ambiguities, covering all of them eventually. □

Remark 6.4. *If the used module ordering is fair and the selection strategy processes elements by increasing signatures, then, whenever the algorithm considers a labeled polynomial $p^{[\pi]}$, the sets $G^{[\Sigma]}$ and H are a signature Gröbner basis and a syzygy basis respectively up to signature* $\mathrm{sig}(\pi)$.

6.3 Elimination criteria

For simplicity, we presented the algorithm stripped to its main loop, with only the cover criterion necessary for the loop invariant. In this section, we list a few additional criteria which can be added to the algorithm to skip redundant ambiguities and polynomials. They all work similarly to their counterpart in the commutative case, ensuring that elements are covered (for S-polynomials) or sig-reducible (for G-polynomials). First, we focus on G-polynomials.

Corollary 6.5. *Let $g_1^{[\beta_1]}, g_2^{[\beta_2]} \in G^{[\Sigma]}$ and $a \in \mathrm{amb}(g_1^{[\beta_1]}, g_2^{[\beta_2]})$. If* G-Pol$(a)$ *is* sig*-reducible by $G^{[\Sigma]}$, then it can be discarded.*

Proof. Follows from Theorem 5.3 and Definition 4.11. □

The criterion allows to avoid all reductions of G-polynomials to zero, and, in fact, since we only consider top reductions, it avoids reductions of G-polynomials entirely. As a special case, we see that, if $\mathrm{lc}(g_1) \mid \mathrm{lc}(g_2)$, then all their G-polynomials can be discarded as they are all sig-reducible by $g_1^{[\beta_1]}$.

We now move to S-polynomials. Excluding covered ambiguities encapsulates a number of criteria, including the *Syzygy criterion* [e.g. 8, Lem. 6.1], stating that any regular ambiguity whose signature is reducible by the signature of a syzygy in H can be discarded, and the *Singular criterion* [e.g. 8, Lem. 6.2], which says that for each signature only one regular ambiguity (the one with minimal leading monomial) has to be considered. To make the cover criterion even stronger, we can exploit the fact that signatures of some syzygies, so-called *trivial syzygies*, can be predicted in advance without having to perform any reductions. In particular, for all $g_1^{[\beta_1]}, g_2^{[\beta_2]} \in I^{[\Sigma]}$ and $m \in M(A)$, we obtain a trivial syzygy $g_2 m\beta_1 - \beta_2 m g_1$. The aim of the F5 criterion is to detect these trivial syzygies.

Corollary 6.6 (F5 criterion). *Let a be a regular ambiguity of elements in $G^{[\Sigma]}$ such that there exist $g_1^{[\beta_1]}, g_2^{[\beta_2]} \in G^{[\Sigma]}$ and $m \in M(A)$ with*

- $\mathrm{sig}(g_2 m\beta_1) \neq \mathrm{sig}(\beta_2 m g_1)$, *and*
- $\mathrm{sig}(a)$ *is reducible by* $\max(\mathrm{sig}(g_2 m\beta_1), -\mathrm{sig}(\beta_2 m g_1))$.

Then a is covered by the trivial syzygy $g_2 m\beta_1 - \beta_2 m g_1$ and S-Pol(a) *can be discarded after adding this trivial syzygy to the set H.*

The F5 criterion as phrased above also includes Buchberger's coprime criterion for eliminating S-polynomials coming from elements with coprime leading terms, see [28, Lem. 22] for a noncommutative version without signatures. In particular, if $g_1^{[\beta_1]}, g_2^{[\beta_2]}$ are such that $\mathrm{lc}(g_1)$ and $\mathrm{lc}(g_2)$ as well as the commutative parts of $\mathrm{lm}(g_1)$ and $\mathrm{lm}(g_2)$ are coprime, then, for every regular external ambiguity of these elements, the S-polynomial can be discarded after adding a suitable trivial syzygy to H.

Unlike in the commutative case, it is not possible to simply add all trivial syzygies to H whenever a new element is added to the signature Gröbner basis, as there are infinitely many. However, in order to check the F5 criterion, only finitely many syzygies can apply, and we can construct them on demand. This renders the complexity of applying Corollary 6.6 essentially quadratic in the size of $G^{[\Sigma]}$. In Section 7.3, we show that, analogous to the commutative case, this cost can be reduced to linear for homogeneous polynomials under certain module orderings.

It was observed in [21] that for some labeled modules $I^{[\Sigma]}$, there exist a finite set of labeled polynomials $G^{[\Sigma]}$, and a finite set of syzygies H, such that $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, and $H \cup \{\text{trivial syzygies formed with elements of } G^{[\Sigma]}\}$ is a syzygy basis of $I^{[\Sigma]}$. If that is the case, Algorithm 1 will eventually have produced $G^{[\Sigma]}$ and H, and P will only contain an infinite set of elements with signature all reducible by a trivial signature.

A particular case is that where R is a field and there are no commutative variables, that is, when we are using Algorithm 1 in the free algebra over a field. In that setting, Buchberger's coprime criterion excludes all external ambiguities, which leads to two elements only having finitely many ambiguities, and the algorithm may terminate. The advantages of Algorithm 1 over that in [21] is the stronger cover criterion and the ability to use any module order (Section 7.1).

7 APPLICATIONS

7.1 Elimination orders

Write $X = X_1 \dot\cup X_2$ and $Y = Y_1 \dot\cup Y_2$. Recall that a monomial ordering $\leq$ on $M(A)$ is an *elimination ordering* for $X_1 \cup Y_1$ if $\mathrm{lm}(f) \in [X_2]\langle Y_2\rangle$ implies $f \in R[X_2]\langle Y_2\rangle$ for all $f \in A$. If G is a Gröbner basis of I for such an ordering, then $G \cap R[X_2]\langle Y_2\rangle = \{g \in G \mid g \in R[X_2]\langle Y_2\rangle\}$ is a Gröbner basis of $I \cap R[X_2]\langle Y_2\rangle$, see [2].

Those orders are thus very useful when simplifying expressions (or in particular solving systems), and signatures allow to prove that the simplified expression is correct. Unfortunately, in the case of the free algebra, any module ordering compatible with an elimination ordering cannot be fair. As such, even if $X = \emptyset$ and R is a field, the algorithm from [21] was not applicable. On the other hand, provided that ambiguities are processed in a fair order, Algorithm 1 correctly enumerates a signature Gröbner basis with respect to any order, including elimination orders.

7.2 Ideal arithmetic

The next application we mention concerns the use of Gröbner bases to perform ideal arithmetic operations. We recall [41] that, given two ideals $I, J \subseteq R[X]\langle Y\rangle$, a Gröbner basis of their intersection is obtained by eliminating a new commutative indeterminate t from $tI + (1-t)J \subseteq R[X,t]\langle Y\rangle$. Similarly, computing the homogeneous part of an ideal I, that is, computing a Gröbner basis of the subideal of I generated by all homogeneous polynomials in I, can be realised by a computation in $R[X,T,T^{-1}]\langle Y\rangle$, where T, T^{-1} are sets of new commutative and invertible indeterminates. We refer to [20, Sec. 4] for further details.

7.3 Homogenization

Recall that given a polynomial $f = \sum_{i=1}^{d} c_i w_i \in R[X]\langle Y\rangle$, its degree $\deg(f)$ is the maximum length of the monomials w_i appearing in f, i.e., $\deg(f) = \max_i |w_i|$. It is called homogeneous if all its

terms have the same length. The homogenized polynomial $f^h \in R[X,h]\langle Y\rangle$ is $f^h = \sum_{i=1}^{d} c_i h^{\deg(f)-|w_i|} w_i$, it is a homogeneous polynomial, and evaluating it at $h = 1$ yields back f. In that construction, the homogenization variable h commutes with all the variables.

If $R[X,h]\langle Y\rangle$ is ordered by a graded ordering and h is treated as smaller than all other variables, evaluating a (signature) Gröbner basis of $(f_1^h, \dots, f_r^h)$ at $h = 1$ yields a Gröbner basis of $(f_1, \dots, f_r)$.

It is frequently preferrable to work with homogeneous polynomials when computing Gröbner bases, in both the commutative and noncommutative case. Specifically in the context of signatures, they open the possibility to use more efficient orderings for the F5 criterion. More precisely, the fact that one does not know in advance which signature realizes the maximum in the second condition of Corollary 6.6 makes it expensive to use the criterion.

This can be partially remedied by considering module orders which make this comparison easy, such as the *position-over-term* (PoT) ordering, first comparing the index $\mathrm{ind}(\sigma) := i$ of a signature $\sigma = a\varepsilon_i b$ before comparing the terms a and b. However, to fully utilize the F5 criterion in this case, elements have to be processed by increasing signatures, which does not constitute a fair selection strategy in the noncommutative setting if PoT is used. An alternative can be to decouple the selection strategy from the module ordering, but then one cannot expect that all elements necessary to use the F5 criterion will be present in time for its use.

Another possibility, when dealing with homogeneous polynomials and a graded monomial ordering, is the *degree-over-position-over-term* (DoPoT) order. This order defines the degree of a signature $a\varepsilon_i b$ as $|a| + \deg(f_i) + |b|$. In the homogeneous case, given a labeled polynomial $f^{[\alpha]}$, $\deg(f) = \deg(\mathrm{sig}(\alpha))$. In the inhomogeneous case, it only holds that $\deg(f) \le \deg(\mathrm{sig}(\alpha))$. The DoPoT ordering first compares the degree of the signatures, then the index i, and finally the terms a and b. This ordering is fair, and can thus be used as a selection strategy in the algorithm, by always picking the element with smallest signature in the queue P in line 3. Moreover, this ordering makes it possible to verify the conditions of the F5 criterion easily, and the incremental calculation ensures that all the required signatures are available when applying the criterion.

Corollary 7.1 (F5 criterion optimised). *Assume that the generators $f_1, \dots, f_r$ of the labeled module $I^{[\Sigma]}$ are homogeneous and that DoPoT is used as a module ordering with a graded term ordering.*

Let $g^{[\beta]} \in G^{[\Sigma]}$. For all $m \in M(A)$ and $j > \mathrm{ind}(\beta)$, the module terms $\mathrm{lt}(g)m\varepsilon_j$ and $\varepsilon_j m\mathrm{lt}(g)$ are signatures of trivial syzygies.

If, additionally, elements in Algorithm 1 are processed by increasing signature and all ambiguities with signature divisible by a signature as above are discarded, then all ambiguities whose signature is divisible by the signature of a trivial syzygy $\sigma = g_2 m\beta_1 - \beta_2 m g_1$, with $\mathrm{ind}(\beta_1) \neq \mathrm{ind}(\beta_2)$, are discarded in this way.

Proof. They are the signature of the trivial syzygies $gm\varepsilon_j - \beta m f_j$ and $\varepsilon_j mg - f_j m\beta$ respectively, observing that both members of a trivial syzygy must have the same degree.

For the second part, the signature of the trivial syzygy σ is $\mathrm{sig}(g_2 m\beta_1)$ if $\mathrm{ind}(\beta_1) > \mathrm{ind}(\beta_2)$ and $-\mathrm{sig}(\beta_2 m g_1)$ otherwise. Both cases are handled similarly, so assume that we are in the first one. Then the signature of σ is a discarded signature, obtained from $g_2^{[\beta_2]}$. It remains to prove $\mathrm{sig}(\beta_2) \prec \mathrm{sig}(a)$, to ensure that $g_2^{[\beta_2]}$ was computed in time for discarding a. Since $\mathrm{sig}(a)$ is divisible by $\mathrm{sig}(\sigma) > \mathrm{sig}(\beta_2 m g_1)$, we have $\deg(\mathrm{sig}(a)) \ge \deg(\mathrm{sig}(\beta_2))$. With $\mathrm{ind}(\mathrm{sig}(a)) = \mathrm{ind}(\beta_1) > \mathrm{ind}(\beta_2)$, this yields $\mathrm{sig}(\beta_2) \prec \mathrm{sig}(a)$. □

8 EXPERIMENTAL RESULTS

We have written a prototype implementation[1] of Algorithm 1 in SageMath for the case when R is a field including the criteria for S-polynomial elimination discussed in Section 6.3 (G-polynomials are redundant over fields). We use it to compare the mixed algebra setting to other (more naive) approaches for computing noncommutative (signature) Gröbner bases involving some commutative variables. More precisely, we compare Algorithm 1 to the following two approaches: (1) classical Gröbner basis computations in the free algebra where commutator relations are added explicitly to the generators of an ideal; (2) signature Gröbner basis computations in the free algebra where commutator relations are added explicitly to the generators of an ideal but are given a trivial signature 0 so that sig-reductions by these relations are always possible.

For the classical Gröbner basis computations we use Singular:Letterplace [29] and for the naive signature-based computations we use our SageMath package `SignatureGB`[1]. In Table 1, we report on the number of polynomials reduced, the number of zero reductions and the size of the resulting (signature) Gröbner basis for the following benchmark examples.

- Example `ufn1h` is from [26] and described there. It concerns a homogeneous ideal in $\mathbb{Q}[h]\langle a,b,c,d\rangle$.
- Iwahori-Hecke algebras [23], from [28, Ex. 31]:
  `ih` $= (x^2 + hx - qx - hq, y^2 + hy - qy - hq, z^2 + hz - qz - hq, zx - xz, yxy - xyx, zyz - yzy, h^2 - qq^{-1}) \subseteq \mathbb{Q}[q, q^{-1}, h]\langle x,y,z\rangle$.
- Homogenization of the relations of the discrete Heisenberg group $\langle x,y,z \mid z = xyx^{-1}y^{-1}, xz = zx, yz = zy\rangle$:
  `heis` $= (h^3 z - xyx^{-1}y^{-1}, h^2 - zz^{-1}, h^2 - xx^{-1}, h^2 - x^{-1}x, h^2 - yy^{-1}, h^2 - y^{-1}y) \subseteq \mathbb{Q}[z, z^{-1}, h]\langle x, x^{-1}, y, y^{-1}\rangle$.

For each of these homogeneous ideals, we compute truncated (signature) Gröbner bases up to a fixed degree. The used degree bounds are indicated by the number after the "–" in the names of the examples in Table 1. For all examples, a degree-lexicographic monomial ordering is used, in combination with DoPoT for the signature-based computations.

As Table 1 shows, Algorithm 1 has to perform a lot less reductions and yields a lot smaller outputs. The main reason for this behaviour is that in the classical approaches the commutator relations become oriented reduction rules, which makes them less flexible. This causes a lot of computations that are avoided in the mixed algebra. Additionally, the naive signature-based computation suffers from the fact that the commutator relations are only "visible" on the polynomial level but not on the signature level. Hence, the elimination criteria cannot be exploited fully because they miss this crucial information. In contrast to this, in the mixed algebra setting, the information about the commutative variables is also directly propagated to the signatures.

Acknowledgement. We thank the reviewers for their careful reading and their remarks.

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

Example	classical Gröbner basis			naive signature basis			Algorithm 1		
	reductions	red. to 0	size	reductions	red. to 0	size	reductions	red. to 0	size
ufn1h-7	877	737	140	1784	401	1343	168	73	95
ufn1h-8	1447	1243	204	4594	922	3556	270	120	150
ih-7	759	658	101	1690	158	1363	31	7	24
ih-8	1059	937	122	3635	289	2857	35	8	27
heis-8	1167	823	344	18 418	755	17 431	22	4	18
heis-9	4002	2947	1055	63 734	2476	60 510	48	14	34

Table 1

REFERENCES

[1] George M. Bergman. 1978. The diamond lemma for ring theory. *Adv. in Math.* 29, 2 (1978), 178–218.

[2] Miguel Angel Borges and Mijail Borges. 1998. Gröbner Bases Property on Elimination Ideal in the Noncommutative Case. In *Gröbner Bases and Applications*. Cambridge University Press, 323–337.

[3] Bruno Buchberger. 1965. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph. D. Dissertation. University of Innsbruck, Austria.

[4] Michela Ceria and Teo Mora. 2017. Buchberger-Weispfenning theory for effective associative rings. *J. Symb. Comput.* 83 (2017), 112–146.

[5] Michela Ceria and Teo Mora. 2017. Buchberger–Zacharias Theory of multivariate Ore extensions. *J. Pure Appl. Algebra* 221, 12 (2017), 2974–3026.

[6] Cyrille Chenavier, Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger. 2020. Compatible rewriting of noncommutative polynomials for proving operator identities. In *Proceedings of ISSAC 2020*. 83–90.

[7] Paul M. Cohn. 1985. *Free rings and their relations* (2nd ed.). Academic Press.

[8] Christian Eder and Jean-Charles Faugère. 2017. A Survey on Signature-based Algorithms for Computing Gröbner Bases. *J. Symbolic Comput.* 80 (2017), 719–784.

[9] Christian Eder, Pierre Lairez, Rafael Mohr, and Mohab Safey El Din. 2023. A signature-based algorithm for computing the nondegenerate locus of a polynomial system. *J. Symbolic Comput.* 119 (2023), 1–21.

[10] Christian Eder, Gerhard Pfister, and Adrian Popescu. 2017. On signature-based Gröbner bases over Euclidean rings. In *Proceedings of ISSAC 2017*. 141–148.

[11] Jean-Charles Faugère. 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of ISSAC 2002*. 75–83.

[12] Maria Francis and Thibaut Verron. 2021. On two signature variants of Buchberger's algorithm over principal ideal domains. In *Proceedings of ISSAC 2021*. 139–146.

[13] André Galligo. 1985. Some algorithmic questions on ideals of differential operators. *Lecture Notes in Comput. Sci.* (1985), 413–421.

[14] Shuhong Gao, Frank Volny IV, and Mingsheng Wang. 2015. A new framework for computing Gröbner bases. *Math. Comput.* 85, 297 (2015), 449–465.

[15] Rüdiger Gebauer and H. Michael Möller. 1986. Buchberger's algorithm and staggered linear bases. In *Proceedings of the Symposium on Symbolic and Algebraic Manipulation, SYMSAC 1986*. 218–221.

[16] Amir Hashemi and Masoumeh Javanbakht. 2020. On the construction of staggered linear bases. *J. Algebra Appl.* 20, 08 (2020), 2150132.

[17] Amir Hashemi and H. Michael Möller. 2023. A new algorithm for computing staggered linear bases. *J. Symb. Comput.* 117 (2023), 1–14.

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

[19] Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger. 2019. Certifying operator identities via noncommutative Gröbner bases. *ACM Commun. Comput. Algebra* 53, 2 (2019), 49–52.

[20] Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger. 2022. Computing elements of certain form in ideals to prove properties of operators. *Math. Comput. Sci.* 16, 2-3 (2022), 17.

[21] Clemens Hofstadler and Thibaut Verron. 2022. Signature Gröbner bases, bases of syzygies and cofactor reconstruction in the free algebra. *J. Symbolic Comput.* 113 (2022), 211–241.

[22] Clemens Hofstadler and Thibaut Verron. 2023. Short proofs of ideal membership. *arXiv preprints* arXiv:2302.02832 (2023).

[23] James E. Humphreys. 1990. *Reflection groups and Coxeter groups*. Cambridge Stud. Adv. Math., Vol. 29. Cambridge University Press, Cambridge. xii+204 pages.

[24] Äbdelilah Kandri-Rody and Deepak Kapur. 1988. Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain. *J. Symbolic Comput.* 6, 1 (1988), 37–57.

[25] Deepak Kapur and Klaus Madlener. 1989. A Completion Procedure for Computing a Canonical Basis for a k-Subalgebra. In *Computers and Mathematics*. Springer US, 1–11.

[26] Roberto La Scala and Viktor Levandovskyy. 2009. Letterplace ideals and noncommutative Gröbner bases. *J. Symbolic Comput.* 44, 10 (2009), 1374–1393.

[27] Pierre Lairez. 2022. Axioms for a theory of signature bases. *arXiv preprints* arXiv:2210.13788 (2022).

[28] Viktor Levandovskyy, Tobias Metzlaff, and Karim Abou Zeid. 2023. Computing free non-commutative Gröbner bases over $\mathbb{Z}$ with Singular:Letterplace. *J. Symbolic Comput.* 115 (2023), 201–222.

[29] Viktor Levandovskyy, Hans Schönemann, and Karim Abou Zeid. 2020. Letterplace—a Subsystem of Singular for Computations with Free Algebras via Letterplace Embedding. In *Proceedings of ISSAC 2020*. 305–311.

[30] Daniel Lichtblau. 2012. Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.* 56, 1 (2012), 177–194.

[31] Douglas Lind and Klaus Schmidt. 2015. A survey of algebraic actions of the discrete Heisenberg group. *Russ. Math. Surveys* 70, 4 (2015), 657.

[32] Alexander A. Mikhalev and Andrej A. Zolotykh. 1998. Standard Gröbner-Shirshov bases of free algebras over rings. I. Free associative algebras. *Internat. J. Algebra Comput.* 8, 6 (1998), 689–726.

[33] H. Michael Möller. 1988. On the Construction of Gröbner Bases using Syzygies. *J. Symbolic Comput* 6, 2-3 (1988), 345–359.

[34] H. Michale Möller and Ferdinando Mora. 1986. New Constructive Methods in Classical Ideal Theory. *J. Algebra* 100, 1 (1986), 138 –178.

[35] H. Michael Möller, Teo Mora, and Carlo Traverso. 1992. Gröbner Bases Computation Using Syzygies. In *Proceedings of ISSAC 1992*. 320–328.

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

[37] Ferdinando Mora. 2015. De Nugis Groebnerialium 4: Zacharias, Spears, Möller. In *Proceedings of ISSAC 2015*. 283–290.

[38] Teo Mora. 1994. An Introduction to Commutative and Noncommutative Gröbner Bases. *Theor. Comput. Sci.* 134, 1 (1994), 131–173.

[39] Teo Mora. 2016. *Solving Polynomial Equation Systems IV*. Cambridge University Press.

[40] Bertrand Nguefack and Emmanuel Pola. 2020. Effective Buchberger-Zacharias-Weispfenning theory of skew polynomial extensions of subbilateral coherent rings. *J. Symb. Comput.* 99 (2020), 50–107.

[41] Patrik Nordbeck. 1998. On some Basic Applications of Gröbner Bases in Noncommutative Polynomial Rings. In *Gröbner Bases and Applications*. Cambridge University Press, 463–472.

[42] François Ollivier. 1991. Canonical Bases: Relations with Standard Bases, Finiteness Conditions and Application to Tame Automorphisms. In *Effective Methods in Algebraic Geometry*. Birkhäuser Boston, 379–400.

[43] Luquan Pan. 1989. On the D-bases of Polynomial Ideals over Principal Ideal Domains. *J. Symbolic Comput.* 7, 1 (1989), 55–69.

[44] F. Leon Pritchard. 1996. The Ideal Membership Problem in Non-Commutative Polynomial Rings. *J. Symb. Comput.* 22, 1 (1996), 27–48.

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

[46] Leonard Schmitz and Viktor Levandovskyy. 2020. Formally Verifying Proofs for Algebraic Identities of Matrices. In *International Conference on Intelligent Computer Mathematics*. Springer, 222–236.

[47] Yao Sun, Dingkang Wang, Xiaodong Ma, and Yang Zhang. 2012. A Signature-Based Algorithm for Computing Gröbner Bases in Solvable Polynomial Algebras. In *Proceedings of ISSAC 2012*. 351–358.