Computing Elements of Certain Form in Ideals to Prove Properties of Operators

Clemens Hofstadler · Clemens G. Raab · Georg Regensburger

Abstract Proving statements about linear operators expressed in terms of identities often leads to finding elements of certain form in noncommutative polynomial ideals. We illustrate this by examples coming from actual operator statements and discuss relevant algorithmic methods for finding such polynomials based on noncommutative Gröbner bases. In particular, we present algorithms for computing the intersection of a two-sided ideal with a one-sided ideal as well as for computing homogeneous polynomials in two-sided ideals and monomials in one-sided ideals. All methods presented in this work are implemented in the MATHEMATICA package `OperatorGB`.

Contents

C. Hofstadler (✉) · C. G. Raab
Institute for Algebra, Johannes Kepler University Linz, Altenberger Straße 69, 4040 Linz, Austria
e-mail: clemens.hofstadler@jku.at

C. G. Raab
e-mail: clemensr@algebra.uni-linz.ac.at

G. Regensburger
Institute of Mathematics, University of Kassel, Heinrich-Plett-Straße 40, 34132 Kassel, Germany
e-mail: regensburger@mathematik.uni-kassel.de

Ⓑ Birkhäuser

1 Introduction

The main motivation for the work presented here is to automatize proofs of statements about matrices and linear operators. Many properties of matrices and linear operators can be expressed in terms of identities. Algebraically, these identities can be modeled as free noncommutative polynomials whose indeterminates represent the basic operators involved. From the polynomials corresponding to known or assumed identities of these operators a (two-sided) ideal is generated. The most basic instance of a computational problem that can be used for proving a statement about linear operators consists in identifying a given polynomial as a member of a given ideal. More generally, proving a statement about linear operators translates into finding polynomials of a certain form in the given ideal. In this paper, we discuss well-known and present novel algorithmic methods based on noncommutative Gröbner basis computations to do this and illustrate them by examples.

Gröbner bases of ideals arising from matrix identities have already been used in the pioneering work [7,8]. Recently, proving operator identities using Gröbner basis computations and related questions were also addressed in [20]. However, not every computation with noncommutative polynomials can be translated into a computation with operators, since addition and composition of operators are restricted by their domains and codomains. In [18], a general algebraic framework was developed that provides conditions on the generators of the ideal and the given polynomial to ensure that ideal membership of that polynomial is equivalent to the existence of a valid computation with actual operators proving the corresponding identity. More precisely, in this way a single computation with polynomials verifying ideal membership proves the statement about operators in an abstract setting in such a way that analogous statements in various concrete settings (e.g. for matrices, linear bounded operators, C^*-algebras, …) follow immediately in a rigorous way. To encode domains and codomains of operators, the framework uses a quiver, where vertices correspond to spaces, edges correspond to basic operators mapping between those spaces, and the labels of edges are indeterminates in a noncommutative polynomial ring. The central notion is then given by polynomials that are *compatible with the quiver*, i.e., only consist of monomials that are labels of paths between the same pair of vertices in the quiver.

Sometimes identities arising from the properties of operators contain undetermined operators. One class of such properties are conditions on ranges and kernels, like the inclusion of ranges $\mathcal{R}(A) \subseteq \mathcal{R}(B)$ of operators A, B. For linear operators over a field, such a range inclusion can be translated into the existence of a factorisation $A = BX$ for some operator X. In our setting, if we want to prove such a range inclusion, we have to find an element in the ideal generated by the assumptions that represents an identity of the form $A = BX$. More generally, solving operator equations explicitly leads to searching for elements of a particular form in a given ideal. This problem also arises when we want to use properties like injectivity or surjectivity of some operators in proofs. For example, to apply injectivity of an operator A, we have to search for elements representing an identity of the form $AB = AC$ to conclude that $B = C$. Also other properties can be described by the cancellability of certain left or right factors.

To motivate our work and illustrate our methods, we look at two concrete examples that deal with the solvability of operator equations. First, we consider the following characterisation of the solvability of the operator equation $AXB = C$ in Hilbert spaces from Proposition 3.3 in [1]. In the following, $P^\dagger$ denotes the Moore-Penrose inverse of a bounded linear operator P and P^* denotes the adjoint operator.

Theorem 1.1 *Let $A\colon \mathcal{H}_4 \to \mathcal{H}_2$, $B\colon \mathcal{H}_1 \to \mathcal{H}_3$, $C\colon \mathcal{H}_1 \to \mathcal{H}_2$ be bounded linear operators on complex Hilbert spaces. There exists a bounded linear operator $X\colon \mathcal{H}_3 \to \mathcal{H}_4$ such that $AXB = C$ if and only if $\mathcal{R}(C) \subseteq \mathcal{R}(A)$ and $\mathcal{R}((A^\dagger C)^*) \subseteq \mathcal{R}(B^*)$.*

We discuss how to prove the sufficiency of the range inclusions in Theorem 1.1 by a computation with polynomials. First, all properties appearing in the statement have to be phrased in terms of identities. For our assumptions, the postulated range inclusions can be translated into the existence of operators Y, Z such that $C = AY$ and $(A^\dagger C)^* = B^*Z$. The existence of the Moore-Penrose inverse $A^\dagger$ is encoded in terms of identities by adding the four defining equations of $A^\dagger$ to our assumptions. These identities, the two identities for the range inclusions, and the respective adjoint statements can be translated into a set F of 10 noncommutative polynomials with integer coefficients in 12 indeterminates. The quiver encoding the domains and codomains of the operators involved con-

sists of 4 vertices and 12 edges. It is depicted in Fig. 1. Then, finding a solution X of $AXB = C$ corresponds to finding a compatible polynomial $axb - c \in (F)$, where a, b, c are known but x is an unknown polynomial, in the ideal generated by F. In Sect. 3, we discuss how this can be done using ideal intersections. In particular, we discuss well-known ideal intersection techniques [16,17] and we present a new algorithm to compute generators of the intersection of an ideal with a one-sided ideal, which will allow us to solve this problem. We also characterize when an ideal has a finite right generating set.

However, not all properties of operators ultimately lead to statements about polynomials that can be solved by ideal intersections. One example of such a property is determining whether a given operator is positive. Recall that a linear operator P is called positive if there exists another linear operator Q such that P factors as $P = Q^*Q$. A concrete statement where one has to determine the positivity of a given operator is the following part of Theorem 4.3 in [1].

Theorem 1.2 *Let $A \colon \mathcal{H}_3 \to \mathcal{H}_2$, $B \colon \mathcal{H}_1 \to \mathcal{H}_3$, $C \colon \mathcal{H}_1 \to \mathcal{H}_2$ be bounded linear operators on complex Hilbert spaces such that $\mathcal{R}(B) \subseteq \mathcal{R}(A^*)$. If there exists a bounded, positive linear operator $X \colon \mathcal{H}_3 \to \mathcal{H}_3$ such that $AXB = C$, then $B^*A^\dagger C$ is positive.*

Proving this statement by a computation with polynomials ultimately leads to the following problem. Given the ideal (F) generated by the assumptions F of the theorem, find a polynomial of the form $p - q^*q \in (F)$, where p is known but the polynomial q, and therefore also q^*, are unknown. Here, q^* denotes the image of q under the involutive antiautomorphism $*$ that sends each variable x_i to an adjoint variable x_i^* and each x_i^* back to x_i. Ideal intersections are not useful here since the second term q^*q is completely unknown. To nevertheless solve this problem if q is a noncommutative monomial, we have generalized a method to compute monomials in a commutative ideal [13,19]. In Sect. 4, we present this new algorithm, that allows to compute homogeneous polynomials in noncommutative ideals, and discuss how it can be used to prove Theorem 1.2. Additionally, in Sect. 5 we show how a simple adaptation of this procedure allows to find monomials in one-sided ideals.

As a consequence of the undecidability of the word problem, also ideal membership in rings of noncommutative polynomials is undecidable. This is, among other things, also reflected in the fact that not all finitely generated ideals in such rings have a finite Gröbner basis. Nevertheless, an analog of Buchberger's algorithm can be used to enumerate a (possibly infinite) Gröbner basis [15]. Since all the methods presented in this work rely on noncommutative Gröbner basis computations, they are in fact not terminating algorithms but rather enumeration procedures. In practice, however, these tools still often allow to verify ideal membership for concrete polynomials. More generally, for finding polynomials of a certain form in an ideal, we first specify a certain subideal (e.g. by ideal intersections), which has to contain all polynomials of the desired form. Then, we enumerate generators of this subideal and search for a polynomial of the desired form. Note that, in general, there is no guarantee that we can find such a polynomial among the generators of the subideal. However, in practice, this was the case in almost all algebraic proofs of operator statements we considered so far.

All the procedures presented here are implemented in the MATHEMATICA software package `OperatorGB` [10], which also provides support for proving properties of matrices and operators along these lines using the framework mentioned above. The package is available at https://clemenshofstadler.com/software/ along with a notebook and PDF file containing detailed proofs of the examples discussed in this paper.

Finally, we note that the methods presented in this work are not exhaustive. There exist other procedures that also allow to compute elements of certain form in noncommutative polynomial ideals. For example, certain problems can also be solved by computing the intersection of a (two-sided) ideal with a subalgebra of the ring of noncommutative polynomials [17]. Furthermore, the problems that Theorems 1.1 and 1.2 lead to, could also be considered as factorisation problems in a suitable quotient of the ring of noncommutative polynomials. In [2], it was shown that this quotient is a finite factorisation domain if it admits a finite dimensional filtration and a terminating algorithm was given that allows to compute all such factorisations in the affirmative case. Unfortunately, however, for the problems arising from statements about operators, we usually do not have access to such a finite dimensional filtration (in fact, most of the time we do not even know whether it exists) as this would require a description of a complete Gröbner basis.

To keep the presentation self-contained, we briefly recall the most important notions about noncommutative polynomials and the algebraic proof framework from [18] in the following section.

2 Preliminaries and Notation

We denote by $\langle X \rangle$ the free monoid over $X = \{x_1, \ldots, x_n\}$ and we let $K\langle X \rangle$ be the free algebra generated by X over a field K. When speaking about an algebra over K, or a K-algebra for short, we always mean an (associative) K-algebra with unit element. We consider the elements in $K\langle X \rangle$ as *noncommutative polynomials* with coefficients in K and monomials in $\langle X \rangle$. In $K\langle X \rangle$, indeterminates still commute with coefficients but not with each other.

For a monomial $m = x_{i_1} \ldots x_{i_k} \in \langle X \rangle$, the quantity k is called the *length* of m and denoted by $|m|$. A *multiple* of m is any monomial m' of the form $m' = amb$ with $a, b \in \langle X \rangle$. If $a = 1$, then m' is called a *right multiple* of m. If m' is a multiple of m, then m is said to *divide* m'. Furthermore, m is called *(right) reducible* modulo $M \subseteq \langle X \rangle$ if m is a (right) multiple of some monomial in M, otherwise it is called *(right) irreducible* modulo M. We fix a monomial ordering $\preceq$ on $\langle X \rangle$, i.e., $\preceq$ is a well-ordering on $\langle X \rangle$ such that $m \preceq m'$ implies $amb \preceq am'b$ for all $a, b, m, m' \in \langle X \rangle$.

For a given set of polynomials $F \subseteq K\langle X \rangle$, we denote by (F) and $(F)_\rho$ the (two-sided) ideal, respectively the right ideal, generated by F. When working with one-sided ideals, we restrict ourselves to right ideals, since the situation for left ideals is completely symmetric and all theorems about right ideals also hold, mutatis mutandis, for left ideals. In order to help with the distinction between two-sided ideals and right ideals, we denote the former by capital letters, e.g. $I, J, \ldots$, and the latter by capital letters with an additional subscript ρ, e.g. $I_\rho, J_\rho, \ldots$.

Furthermore, we let $\text{lm}(F) = \{\text{lm}(f) \mid 0 \neq f \in F\}$, where $\text{lm}(f)$ denotes the leading monomial of f w.r.t. $\preceq$. The set F is called *(right) reduced* if every element in F is monic and if, for all $f \in F$, all monomials appearing in f are (right) irreducible modulo $\text{lm}(F \setminus \{f\})$. We note that a finite set F can always be transformed into a finite (right) reduced set F' such that $(F) = (F')$ (resp. s.t. $(F)_\rho = (F')_\rho$). See for example [21] on how this can be done.

Given an ideal $I \subseteq K\langle X \rangle$, we say that $G \subseteq K\langle X \rangle$ is a *(two-sided) Gröbner basis* of I if $(G) = I$ and $(\text{lm}(G)) = (\text{lm}(I))$. For a right ideal $I_\rho \subseteq K\langle X \rangle$, a right generating set $G \subseteq K\langle X \rangle$ is called a *right Gröbner basis* of I_ρ if $(\text{lm}(G))_\rho = (\text{lm}(I_\rho))_\rho$. If G is (right) reduced, it is called the *reduced (right) Gröbner basis*. We note that the reduced (right) Gröbner basis of an ideal (resp. a right ideal) is unique. Furthermore, the reduced right Gröbner basis of a right ideal I_ρ can be computed by right reducing any generating set of I_ρ. The following lemma expresses this fact and implies that every finitely generated right ideal has a finite Gröbner basis; no matter the chosen monomial ordering.

Lemma 2.1 *Let $I_\rho \subseteq K\langle X \rangle$ be a right ideal with right generating set $G \subseteq K\langle X \rangle$. If G is right reduced, then G is the reduced right Gröbner basis of I_ρ.*

Proof See [21, Proposition 4.4.4]. □

All the techniques presented in this work rely on the elimination property of noncommutative Gröbner bases [3]. If we let $I \subseteq K\langle X \rangle$ be an ideal and $Y \subseteq X$, then, analogous to the commutative case, the elimination property of noncommutative Gröbner bases allows to easily obtain a Gröbner basis of the elimination ideal $I \cap K\langle X \setminus Y \rangle$ from a suitable Gröbner basis of I. A Gröbner basis is suitable to do this, if it is computed w.r.t. a special monomial ordering, called an *elimination ordering*. Such an ordering is defined as follows. A monomial ordering is called an *elimination ordering* for $Y \subseteq X$ if $\text{lm}(f) \in \langle X \setminus Y \rangle$ implies $f \in K\langle X \setminus Y \rangle$ for all $f \in K\langle X \rangle$. The following theorem states the elimination property of noncommutative Gröbner bases.

Theorem 2.2 *Let $I \subseteq K\langle X \rangle$ be an ideal and $Y \subseteq X$. Furthermore, let G be a Gröbner basis of I computed w.r.t. an elimination ordering for Y. Then, $G \cap K\langle X \setminus Y \rangle$ is a Gröbner basis of the elimination ideal $I \cap K\langle X \setminus Y \rangle$.*

Proof See [3, Theorem 3.2]. □

We note that Theorem 2.2 also applies in the same way to right ideals. For further information on Gröbner bases in the free algebra, see for example [10,15,16,21], and also [12] for an overview on available software and further references.

To end this section, we recall some of the notions related to the framework developed in [18] that are also relevant for the work presented here. For a short, more formal summary see also the appendix in [5]. In order to translate identities of linear operators into noncommutative polynomials, each basic operator is replaced uniformly by a unique noncommutative indeterminate from some set X and the difference of the left and right hand side of each identity is formed. In this process, all information about the different domains and codomains of the operators is lost. In order to preserve this information, it is encoded in a *labelled quiver* Q. This is a directed multigraph where edges are labelled by the indeterminates in X. More precisely, the domains and codomains of the basic operators correspond to the vertices of Q and an edge with label $x \in X$ is drawn from a vertex v to a vertex w if and only if the operator that has been replaced by x maps from the space represented by v to the space represented by w. With this, a concatenation of paths in Q corresponds to a multiplication of monomials in $\langle X \rangle$. Then, a polynomial in $K\langle X \rangle$ is called *compatible* with Q if all its monomials correspond to paths in Q which all have the same start and end. Informally speaking, a polynomial is compatible with Q if and only if it can be translated into a valid operator in the setting encoded by Q. The main result of [18] then says the following. If the polynomials $F \subseteq K\langle X \rangle$ representing the assumptions of a statement about operators as well as the polynomial $f \in K\langle X \rangle$ corresponding to the claimed property are all compatible with the quiver Q encoding the domains and codomains, then the ideal membership $f \in (F)$ is equivalent to the correctness of the statement about operators.

3 Ideal Intersections

In the introduction, we have already indicated that ideal intersections provide a useful tool for finding elements of certain forms in an ideal $I \subseteq K\langle X \rangle$. For example, they allow us to systematically search for elements of the form $lar \in I$, where $a \in K\langle X \rangle$ is known but $l, r \in K\langle X \rangle$ are unknown. This can be done by intersecting I with the ideal (a). Moreover, we cannot only find polynomials where only a certain factor in the middle is known but also elements where, for example, only a specific prefix is given. More precisely, intersecting the ideal I with the right ideal $(a)_\rho$ allows to compute elements of the form $ar \in I$.

To support the proof of Theorem 1.1 by computing ideal intersections, we can use the following approach. To find a suitable polynomial $axb - c \in (F)$ in the ideal generated by the assumptions F of the statement, we intersect (F) with the right ideal $(a, c)_\rho$ and enumerate generators of this intersection. Among these generators, we then search for a polynomial of the form $ar - c$ with the additional requirement that the free part r has to end with the variable b. If we can find such a polynomial and show that it is compatible with the quiver Q encoding the domains and codomains of the statement, then this proves Theorem 1.1. This approach is carried out successfully in the example at the end of this section.

In this section, we discuss how generating sets of several different kinds of ideal intersections can be computed. Recall that $I, J, \ldots$ denote two-sided ideals while $I_\rho, J_\rho, \ldots$ denote right ideals.

In the case of commutative polynomials, two ideals $I, J \subseteq K[X]$ can be intersected by computing the elimination ideal $tI + (1 - t)J \cap K[X]$, where t denotes a new tag variable. It is well-known that the same also works for intersecting one-sided ideals in the free algebra (see e.g. [16, Remark 48.8.6]).

Theorem 3.1 *Let* $I_\rho = (f_1, \ldots, f_r)_\rho, J_\rho = (g_1, \ldots, g_s)_\rho \subseteq K\langle X \rangle$ *be two finitely generated right ideals. Consider the right ideal*

$$H_\rho = \big(tf_i, (1 - t)g_j \mid 1 \leq i \leq r, 1 \leq j \leq s\big)_\rho.$$

Then, $I_\rho \cap J_\rho = H_\rho \cap K\langle X \rangle$.

Consequently, making use of the elimination property of noncommutative Gröbner bases, a right Gröbner basis of $I_\rho \cap J_\rho$ can be computed by removing all polynomial involving the variable t from a right Gröbner basis of H_ρ

that is computed w.r.t. an elimination ordering for $\{t\}$. Lemma 2.1 ensures that the Gröbner basis computed in this way is always finite.

In [17], it was shown that the elimination property of noncommutative Gröbner bases also allows to compute the intersection of two-sided ideals provided that we introduce the commutator relations $tx_k - x_k t$, for all $k = 1, \ldots, n$, between the new tag variable t and the elements of X.

Theorem 3.2 *Let $I = (f_1, \ldots, f_r)$, $J = (g_1, \ldots, g_s) \subseteq K\langle X \rangle$ be two finitely generated ideals. Consider the ideal*

$$H = \left(tf_i, (1-t)g_j, tx_k - x_k t \mid 1 \leq i \leq r, 1 \leq j \leq s, 1 \leq k \leq n \right).$$

Then, $I \cap J = H \cap K\langle X \rangle$.

Proof See [17, Theorem 2]. □

Hence, as for right ideals, a Gröbner basis of the intersection can be computed by computing a Gröbner basis of H w.r.t. an elimination ordering for $\{t\}$ and by intersecting this Gröbner basis with $K\langle X \rangle$. However, in contrast to the previous case, we cannot expect this Gröbner basis to be finite in general.

Next, we consider the third and for our application most relevant type of ideal intersection—the intersection of a two-sided ideal $I \subseteq K\langle X \rangle$ with a right ideal $J_\rho \subseteq K\langle X \rangle$. The basic idea to compute the intersection $I \cap J_\rho$ is to consider I as a right ideal and to intersect two right ideals. As Theorem 3.1 provides an algorithmic way to compute the intersection of two right ideals, it remains to discuss how to obtain a right generating set of an ideal I. The following proposition is a spezialisation of a result in [6] for path algebras and tells us how the reduced two-sided Gröbner basis of an ideal I can be used to obtain a right Gröbner basis of I. In particular, this provides a way to obtain a right generating set of a two-sided ideal. We recall that a monomial $p \in \langle X \rangle$ is called a *proper prefix* of a monomial $m \in \langle X \rangle$ if $m = pq$ with $1 \neq q \in \langle X \rangle$.

Proposition 3.3 *Let $I \subseteq K\langle X \rangle$ be an ideal and let G be its reduced Gröbner basis. Then, the set*

$$\rho(I) := \{mg \mid m \in \langle X \rangle, g \in G, p \text{ is irreducible modulo } \mathrm{lm}(G) \text{ for any proper prefix } p \text{ of } \mathrm{lm}(mg)\}$$

is a right Gröbner basis of I. Furthermore, $\mathrm{lm}(f)$ is right irreducible modulo $\mathrm{lm}(\rho(I) \setminus \{f\})$ for all $f \in \rho(I)$.

Proof Follows from [6, Proposition 7.1] since $K\langle X \rangle$ can be viewed as a path algebra with only one vertex. □

Remark 3.4 Equivalently, we can also write $\rho(I)$ as

$$\rho(I) = \{mg \mid m \in B_I, g \in G, p \in B_I \text{ for any proper prefix } p \text{ of } \mathrm{lm}(mg)\}, \tag{1}$$

where G is the reduced Gröbner basis of I and $B_I = \langle X \rangle \setminus \mathrm{lm}(I)$ is the set of all monomials which are irreducible modulo $\mathrm{lm}(I)$. Note that the equivalence classes of the monomials in B_I form a K-vector space basis of $K\langle X \rangle / I$.

It follows from the uniqueness of the reduced Gröbner basis, that, for a fixed monomial ordering, the set $\rho(I)$ only depends on I. In the following, we discuss under which conditions a two-sided ideal I is finitely generated as a right ideal. The following result tells us that this is the case if and only if the set $\rho(I)$ is finite.

Proposition 3.5 *Let $I \subseteq K\langle X \rangle$ be an ideal. Then, the following are equivalent.*

1. *I is finitely generated as a right ideal.*
2. *I has a finite right Gröbner basis.*
3. *The set $\rho(I)$ is finite.*

Proof The implications (3) $\Rightarrow$ (2) $\Rightarrow$ (1) are clear. Furthermore, the implication (1) $\Rightarrow$ (2) follows immediately from Lemma 2.1 and the fact that a finite set of polynomials can always be transformed into a finite right reduced set. For the implication (2) $\Rightarrow$ (3), assume that I has a finite right Gröbner basis, say $G = \{g_1, \ldots, g_m\} \subseteq K\langle X\rangle$, and assume that $\rho(I)$ is infinite. Since $\rho(I)$ is a right Gröbner basis of I, there exist $g'_1, \ldots, g'_m \in \rho(I)$ and $b_1, \ldots, b_m \in \langle X\rangle$ such that $\mathrm{lm}(g_i) = \mathrm{lm}(g'_i)b_i$ for all $i = 1, \ldots, m$. Now, let $g \in \rho(I) \setminus \{g'_1, \ldots, g'_m\}$ be arbitrary but fixed. We note that such an element exists since $\rho(I)$ is infinite. Then, there exist $1 \le i \le m$ and $b \in \langle X\rangle$ such that $\mathrm{lm}(g) = \mathrm{lm}(g_i)b = \mathrm{lm}(g'_i)b_ib$. Since $g \ne g'_i$, this is a contradiction to the assertion of Proposition 3.3 that $\mathrm{lm}(f)$ is right irreducible modulo $\mathrm{lm}(\rho(I) \setminus \{f\})$ for all $f \in \rho(I)$. $\qquad\square$

The set $\rho(I)$ depends on the monomial ordering w.r.t. which the reduced Gröbner basis of I is computed. However, Lemma 2.1 and Proposition 3.5 imply that the finiteness of $\rho(I)$ is independent of the monomial ordering.

We will now investigate under which conditions the set $\rho(I)$ is finite. Clearly, if the reduced Gröbner basis G of I is infinite, then so must be $\rho(I)$, or equivalently, the finiteness of $\rho(I)$ implies the finiteness of G. The converse, however, is not universally true. The finiteness of G alone is only sufficient to guarantee that also $\rho(I)$ is finite if I is the trivial ideal $I = \{0\}$. In this case, $G = \emptyset = \rho(I)$. We will see that in all other cases, we need the additional requirement that also B_I is finite. To this end, we recall that an ideal $I \subseteq K\langle X\rangle$ is called *zero-dimensional* if the quotient algebra $K\langle X\rangle/I$ is finite dimensional as a K-vector space, or equivalently, if the set B_I is finite. It is well-known that any zero-dimensional ideal has a finite Gröbner basis w.r.t. any monomial ordering (see e.g. 5.1 in [14]).

Lemma 3.6 *Let $I \subseteq K\langle X\rangle$ be a zero-dimensional ideal. Then, the reduced Gröbner basis of I is finite.*

In fact, this condition is also sufficient for an ideal to have a finite right Gröbner basis.

Lemma 3.7 *Let $I \subseteq K\langle X\rangle$ be a zero-dimensional ideal. Then, the set $\rho(I)$ is finite.*

Proof It follows from Lemma 3.6 that the reduced Gröbner basis of I is finite. Then, the finiteness of $\rho(I)$ follows directly from the representation (1) and the fact that B_I is finite. $\qquad\square$

Surprisingly, for a non-trivial ideal I, the property of I being zero-dimensional is also a necessary condition for it to have a finite right Gröbner basis. This fact is captured in the following lemma.

Lemma 3.8 *Let $I \subseteq K\langle X\rangle$ be a non-trivial ideal. If I has a finite right Gröbner basis, then I is zero-dimensional.*

Proof Let G be a finite right Gröbner basis of I and denote $N = \max\{|\mathrm{lm}(g)| \mid g \in G\}$. Let $m \in \langle X\rangle$ such that $|m| \ge N$ and choose $g \in G$ arbitrary. Then, $mg \in I$ and therefore, since G is a right Gröbner basis, there exists $g' \in G$ such that $m\,\mathrm{lm}(g)$ is a right multiple of $\mathrm{lm}(g')$. By the way m was chosen, m in fact has to be a right multiple of $\mathrm{lm}(g')$. Consequently, $m \notin B_I$. Since m was arbitrary of length at least N, this shows that B_I can contain only finitely many elements. Hence, I is zero-dimensional. $\qquad\square$

Combining Proposition 3.5 with Lemmas 3.7 and 3.8, we get the following theorem.

Theorem 3.9 *Let $I \subseteq K\langle X\rangle$ be an ideal. Then, the following are equivalent.*

1. *I is finitely generated as a right ideal.*
2. *I has a finite right Gröbner basis.*
3. *The set $\rho(I)$ is finite.*
4. *$I = \{0\}$ or I is zero-dimensional.*

However, the condition of I being zero-dimensional is very strong and in practice usually not fulfilled. Typically, the reduced Gröbner basis of I is not even finite. In such cases, there is no chance to obtain a finite right generating set. Consequently, we have to content ourselves with finite approximations of $\rho(I)$ and can therefore only work with a right subideal $I'_\rho \subsetneq I$. A priori, it is usually not clear how to choose such a finite approximation. For the

operator statements we looked at so far, we simply selected all elements in $\rho(I)$ up to a certain degree bound. Thus far, this has worked very well, allowing us to find the correct polynomials.

Moreover, in case of our applications, we can choose the subideal I'_ρ so that it still contains all polynomials that are of interest to us and such that I'_ρ is more likely to have a finite right generating set. This follows from the fact that for proving statements about operators, we are only interested in polynomials in I that are compatible with a certain quiver Q. Hence, if the objective is to find polynomials in I that are compatible with a given quiver Q, then $\rho(I)$ can be replaced by

$$\rho_Q(I) := \{f \in \rho(I) \mid f \text{ compatible with } Q\}.$$

The following corollary from [18, Theorem 16] ensures under very mild assumptions on the generators of I that, when working with $\rho_Q(I)$ instead of $\rho(I)$, we can still form all compatible polynomials in I.

Corollary 3.10 *Let Q be a labelled quiver and let $f_1, \ldots, f_r, f \in K\langle X \rangle$ be compatible with Q. Furthermore, let $I = (f_1, \ldots, f_r)$. Then,*

$$f \in I \iff f \in \left(\rho_Q(I)\right)_\rho.$$

Typically, the set $\rho_Q(I)$ is a lot smaller than $\rho(I)$. To illustrate this point, we finish the proof of Theorem 1.1.

Remark 3.11 It has been observed that the noncommutative version of Buchberger's algorithm preserves compatibility of polynomials with a quiver [4,7,20]. This means that, if all polynomials that are given as input to this algorithm are compatible with a quiver, then so are all polynomials in the output. We note that this behavior carries over to one-sided ideal intersections. More precisely, if all generators of two right ideals I_ρ and J_ρ are compatible with a quiver, then so are all polynomials in a Gröbner basis of $I_\rho \cap J_\rho$ when Buchberger's algorithm is used in combination with Theorem 3.1. In case of two-sided ideal intersections, however, this is no longer true. A Gröbner basis of the intersection $I \cap J$ of two ideals I and J with compatible generators computed with Buchberger's algorithm might contain incompatible polynomials. The reason for this is the introduction of the commutator relations $tx_k - x_kt$ during the computation of $I \cap J$.

Example Recall that we had translated the assumptions of Theorem 1.1 into a set F of 10 noncommutative polynomials with integer coefficients in 12 indeterminates. More precisely, the set F consists of the following elements:

$$aa^\dagger a - a, \qquad a^*(a^\dagger)^*a^* - a^*, \qquad (a^\dagger)^*a^* - aa^\dagger,$$
$$a^\dagger aa^\dagger - a^\dagger, \qquad (a^\dagger)^*a^*(a^\dagger)^* - (a^\dagger)^*, \qquad a^*(a^\dagger)^* - a^\dagger a,$$
$$c - ay, \qquad c^* - y^*a^*, \qquad c^*(a^\dagger)^* - b^*z, \qquad a^\dagger c - z^*b,$$

where the first two lines correspond to the existence of the Moore-Penrose inverse $A^\dagger$ (plus the respective adjoint statements) and the last line corresponds to the range inclusions $\mathcal{R}(C) \subseteq \mathcal{R}(A)$ and $\mathcal{R}((A^\dagger C)^*) \subseteq \mathcal{R}(B^*)$ (plus the respective adjoint statements). The quiver encoding the domains and codomains of the operators involved is depicted in Fig. 1.

The existence of a solution X of $AXB = C$ corresponds to finding a compatible polynomial $axb - c \in (F)$, where a, b, c are known but x is unknown. Using one-sided ideal intersection as discussed in this section, we can now find such a polynomial. To this end, we intersect $I = (F)$ with the right ideal $(a, c)_\rho$. Working over $K = \mathbb{Q}$ with a degree lexicographic ordering, the reduced Gröbner basis of I consists of 17 polynomials. In this example, $\rho(I)$ as well as $\rho_Q(I)$ seem to be infinite. However, it turns out that it suffices to consider the finite approximation $\rho_Q^{(5)}(I) \subseteq \rho_Q(I)$ of compatible polynomials of degree at most 5 to find a suitable polynomial in the intersection. We note that $|\rho_Q^{(5)}(I)| = 263$ while computing all elements in $\rho(I)$ up to degree 5 would yield 3485 elements.
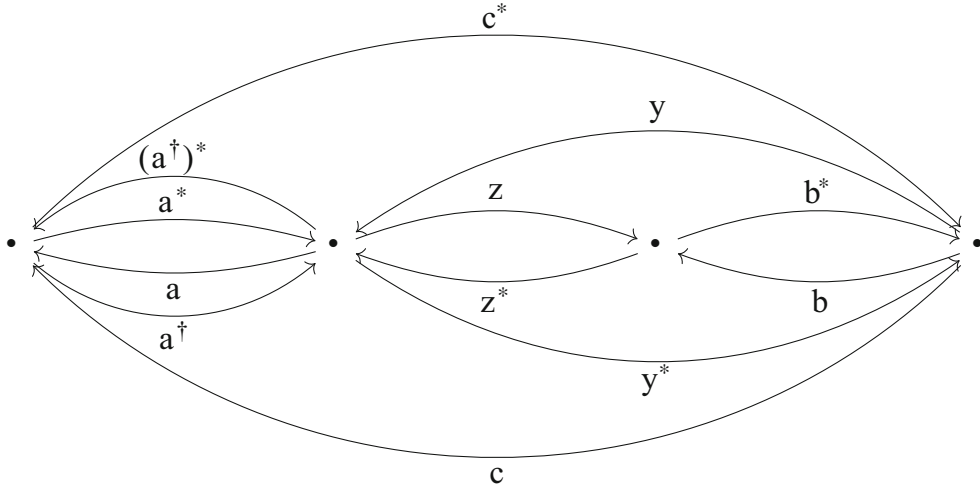
Fig. 1 Quiver encoding the domains and codomains of the operators of Theorem 1.1

Then, the reduced Gröbner basis of $(\rho_Q^{(5)}(I))_\rho \cap (a, c)_\rho$ contains the compatible polynomial $az^*b - c$, which proves Theorem 1.1 and shows that Z^* is a solution of $AXB = C$.

To end this section, we mention another example of applying the methods described above. In a recent application of the algebraic proof framework, we investigated automated proofs of the triple reverse order law for Moore-Penrose inverses [5]. All parts of these proofs that can be reduced to verifying ideal membership of an explicitly given polynomial could be automatized back then. The only step that does not lead to such a problem is the proof of certain range inclusions $\mathcal{R}(A) \subseteq \mathcal{R}(B)$. As explained in the introduction, this leads to the problem of finding a polynomial of the form $a - bx$, where a, b are known but x is an unknown polynomial, in the ideal (F) generated by the assumptions F of the statement. Back then, a polynomial of this form had to be found by hand. Using the methods presented in this section, this step can now be supported by computing the intersection of the two-sided ideal (F) with the right ideal generated by a and b. For further information, we refer to the MATHEMATICA notebook accompanying this paper.

4 Homogeneous Part

The previous section has shown that ideal intersections can provide a useful tool for computing elements of special form in an ideal. However, ideal intersections require to explicitly know a factor in every summand of the element. In some situations we do not have this explicit knowledge. This is for example the case when searching for polynomials in an ideal $I \subseteq K\langle X, X^*\rangle$ of the form $p - q^*q \in I$, where p is known but q, and therefore also q^*, are unknown. Recall that q^* is the image of q under the involutive antiautomorphism * on $K\langle X, X^*\rangle$ that maps each $x_i \in X$ to $x_i^* \in X^*$ and each x_i^* back to x_i. As already mentioned in the introduction, such a task corresponds to determining the positivity of the linear operator represented by the polynomial p. If q is a monomial, a polynomial of the desired form can be found by computing the *homogeneous part* of the ideal I.

So, in this section, we describe how the homogeneous part of an ideal can be computed. Our result is a generalisation of [13], which describes how the set of all monomials contained in a commutative ideal can be computed. We note that a variant of the approach described in [13] can also be found in [19, Algorithm 4.4.2].

First, we recall that an *M-grading* of a ring R by a monoid $(M, +)$ is given by a decomposition $R = \bigoplus_{\alpha \in M} R_\alpha$ of R into a direct sum of abelian groups R_α such that $R_\alpha R_\beta \subseteq R_{\alpha+\beta}$ for all $\alpha, \beta \in M$. Given an M-grading of R, an element $r \in R$ is called *homogeneous* if $r \in R_\alpha$ for some $\alpha \in M$. If $r \neq 0$, then α is called the *degree* of r, denoted by $\deg(r) = \alpha$. Every nonzero $r \in R$ can be written uniquely as $r = r_{\alpha_1} + \cdots + r_{\alpha_d}$ with $\alpha_j \in M$

and $0 \neq r_{\alpha_j} \in R_{\alpha_j}$ for all $j = 1, \ldots, d$. The elements r_{α_j} are referred to as the *homogeneous components* of r. An ideal $I \subseteq R$ is called *homogeneous* if I is generated by homogeneous elements. We note that there are also other equivalent characterisations of a homogeneous ideal. The following one will be relevant for the proof of Theorem 4.4. An ideal $I \subseteq R$ is homogeneous if and only if, with every nonzero element $r \in I$, also all homogeneous components of r lie in I.

A matrix $A \in \mathbb{R}^{n \times k}$ with rows $a_1, \ldots, a_n \in \mathbb{R}^k$ specifies a grading of the free algebra $K\langle X \rangle$ by the monoid $(\mathbb{R}^k, +)$. The grading is given by the monoid homomorphism $\deg_A : \langle X \rangle \to \mathbb{R}^k$ defined on the basis X to be $\deg_A(x_i) = a_i$, for $i = 1, \ldots, n$. This map decomposes $K\langle X \rangle$ into a direct sum of the abelian subgroups

$$K\langle X \rangle_\alpha = \left\{ \sum_{m \in \langle X \rangle} c_m m \mid c_m \in K, \deg_A(m) = \alpha \text{ if } c_m \neq 0 \right\},$$

for $\alpha \in \mathbb{R}^k$. Given a grading $\deg_A$ of $K\langle X \rangle$ and an ideal $I \subseteq K\langle X \rangle$, we can now ask what are the polynomials in I that are homogeneous w.r.t. $\deg_A$. More precisely, we want to consider the ideal generated by all these polynomials. Analogous to the commutative case (see e.g. [11, Tutorial 50]), we call this ideal the *homogeneous part* of I w.r.t. $\deg_A$.

Definition 4.1 Let $I \subseteq K\langle X \rangle$ be an ideal and let $A \in \mathbb{R}^{n \times k}$. We denote by $\hom_A(I) := (f \in I \mid f$ is homogeneous w.r.t. $\deg_A)$ the *homogeneous part* of I w.r.t. $\deg_A$.

The next lemma follows directly from the definition above.

Lemma 4.2 *Let $I \subseteq K\langle X \rangle$ be an ideal and let $A \in \mathbb{R}^{n \times k}$. Then, $\hom_A(I)$ is the largest homogeneous ideal w.r.t. $\deg_A$ contained in I.*

In the following, we describe how a Gröbner basis of $\hom_A(I)$ can be computed. In our approach, we have to restrict ourselves to the case that A has only integer entries, that is, $A \in \mathbb{Z}^{n \times k}$. Note that this is equivalent to having $A \in \mathbb{Q}^{n \times k}$ as, for any nonzero $c \in \mathbb{Q}$, the matrix cA induces the same decomposition of $K\langle X \rangle$ as A.

For the following, some notation is needed. First, for two sets Y and Z, we denote by $[Y, Z] := \{yz - zy \mid y \in Y, z \in Z\}$ the set of commutator relations between Y and Z. Then, with two new sets of indeterminates $T = \{t_1, \ldots, t_k\}$ and $T^{-1} = \{t_1^{-1}, \ldots, t_k^{-1}\}$, we let $J \subseteq K\langle X, T, T^{-1} \rangle$ be the ideal generated by

$$[X \cup T \cup T^{-1}, T \cup T^{-1}] \cup \{1 - t_j t_j^{-1} \mid j = 1, \ldots, k\}.$$

Furthermore, we let $\mathcal{A} = K\langle X, T, T^{-1} \rangle / J$. We denote the equivalence class of an element $f \in K\langle X, T, T^{-1} \rangle$ in $\mathcal{A}$ by $\overline{f}$. Note that, in $\mathcal{A}$, the elements $\overline{t}_j$ and $\overline{t_j^{-1}}$ commute with each other and with everything else. Furthermore, they are also invertible. Consequently, we can think of the equivalence classes of monomials in the variables $T \cup T^{-1}$ as commutative monomials. Hence, there is a bijection τ between exponent vectors and suitable representatives of these equivalence classes. More precisely, for $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{Z}^k$ we define

$$\tau(\alpha) := s_1^{|\alpha_1|} \ldots s_k^{|\alpha_k|} \in \langle T, T^{-1} \rangle, \quad \text{where } s_j = \begin{cases} t_j & \text{if } \alpha_j \geq 0 \\ t_j^{-1} & \text{otherwise} \end{cases}.$$

Example For $\alpha = (3, -2, 0, 1) \in \mathbb{Z}^4$, we have $\tau(\alpha) = t_1^3 (t_2^{-1})^2 t_4$.

So, the map τ turns a vector of integers into a monomial in $\langle T, T^{-1} \rangle$. The following lemma captures an important property of this map in $\mathcal{A}$. It follows from the fact that the equivalence classes $\overline{t}_j$ commute with each other and with their designated inverses.

Lemma 4.3 *Let $\alpha, \beta \in \mathbb{Z}^k$. Then, $\overline{\tau(\alpha + \beta)} = \overline{\tau(\alpha)} \cdot \overline{\tau(\beta)}$.*

For a fixed matrix $A \in \mathbb{Z}^{n \times k}$, we can use the map τ to define the K-algebra homomorphism

$$\varphi_A : K\langle X \rangle \to K\langle X, T, T^{-1} \rangle, \quad x_i \mapsto x_i \tau(a_i),$$

where a_i denotes the i-th row of A. Furthermore, we let $\overline{\varphi}_A : K\langle X \rangle \to \mathcal{A}$ be the composition of φ_A with the canonical epimorphism that sends each element in $K\langle X, T, T^{-1} \rangle$ to its equivalence class. Applying $\overline{\varphi}_A$ to a polynomial f maps each monomial m appearing in f to $\overline{mm_t}$, where $m_t = \tau(\deg_A(m)) \in \langle T, T^{-1} \rangle$ is a monomial in the variables $T \cup T^{-1}$ encoding $\deg_A(m)$. Finally, for an ideal $I \subseteq K\langle X \rangle$ with generating set $F \subseteq K\langle X \rangle$, we consider the *extension* of I along the homomorphism $\overline{\varphi}_A$, which we denote by

$$I^{\overline{\varphi}_A} := (\overline{\varphi}_A(f) \mid f \in F) \subseteq \mathcal{A}.$$

Note that this definition is independent of the generating set F. Then, we can state the main result of this section.

Theorem 4.4 *Let $I \subseteq K\langle X \rangle$ be an ideal and let $A \in \mathbb{Z}^{n \times k}$. Furthermore, let $I^{\overline{\varphi}_A}$ be the extension of I along $\overline{\varphi}_A$. Then,*

$$\hom_A(I) = I^{\overline{\varphi}_A} \cap K\langle X \rangle := \bigcup_{\overline{f} \in I^{\overline{\varphi}_A}} \overline{f} \cap K\langle X \rangle.$$

Proof We note that it follows from the definition of $I^{\overline{\varphi}_A}$ that $f \in I$ implies $\overline{\varphi}_A(f) \in I^{\overline{\varphi}_A}$. Now, to prove the inclusion $\hom_A(I) \subseteq I^{\overline{\varphi}_A} \cap K\langle X \rangle$, let $f \in \hom_A(I)$. W.l.o.g. we can assume that f is homogeneous. Let $\alpha = \deg_A(f) \in \mathbb{Z}^k$. Note that since f is homogeneous, every term in f has degree α. Due to this fact, in $\mathcal{A}$, we have $\overline{\tau(\alpha)f} = \overline{\varphi}_A(f) \in I^{\overline{\varphi}_A}$. To see that this implies that also $\overline{f} \in I^{\overline{\varphi}_A}$, we use Lemma 4.3 and compute

$$\overline{f} = \overline{\tau(0)} \cdot \overline{f} = \overline{\tau(-\alpha)} \cdot \overline{\tau(\alpha)} \cdot \overline{f} = \overline{\tau(-\alpha)} \cdot \overline{\tau(\alpha)f} \in I^{\overline{\varphi}_A}.$$

For the other inclusion $I^{\overline{\varphi}_A} \cap K\langle X \rangle \subseteq \hom_A(I)$, we show that $I^{\overline{\varphi}_A} \cap K\langle X \rangle \subseteq I$ and that $I^{\overline{\varphi}_A} \cap K\langle X \rangle$ is a homogeneous ideal. Then, the claim follows from Lemma 4.2. For the first part, let $f \in I^{\overline{\varphi}_A} \cap K\langle X \rangle$. Then, f can be written as

$$f = \sum_{i=1}^d p_i \varphi_A(f_i) q_i + \sum_{i=1}^e u_i g_i v_i,$$

with $f_i \in I$, $g_i \in [X \cup T \cup T^{-1}, T \cup T^{-1}] \cup \{1 - t_j t_j^{-1} \mid j = 1, \ldots, k\}$ and $p_i, q_i, u_i, v_i \in K\langle X, T, T^{-1} \rangle$. Note that the left hand side of this identity does not depend on the indeterminates in T and T^{-1}. Hence, by setting $t_j = t_j^{-1} = 1$ for all $j = 1, \ldots, k$, we obtain $f = \sum_{i=1}^d \tilde{p}_i f_i \tilde{q}_i$ with $\tilde{p}_i, \tilde{q}_i \in K\langle X \rangle$. This shows that $f \in I$.

Finally, to show that $I^{\overline{\varphi}_A} \cap K\langle X \rangle$ is a homogeneous ideal, we extend the $\mathbb{Z}^k$-grading of $K\langle X \rangle$ defined by A to a $\mathbb{Z}^k$-grading of $K\langle X, T, T^{-1} \rangle$ by setting

$$\deg_A(x_i) = a_i, \quad \deg_A(t_j) = -e_j, \quad \deg_A(t_j^{-1}) = e_j,$$

for $i = 1, \ldots, n$, $j = 1, \ldots, k$, where e_j denotes the j-th unit vector of $\mathbb{Z}^k$. Then, the ideal J is homogeneous w.r.t. this grading. Consequently, this induces a well-defined grading on $\mathcal{A}$ w.r.t. which the ideal $I^{\overline{\varphi}_A}$ is homogeneous. To see that also the intersection $I^{\overline{\varphi}_A} \cap K\langle X \rangle$ is homogeneous, let $f \in I^{\overline{\varphi}_A} \cap K\langle X \rangle$. Since $I^{\overline{\varphi}_A}$ is homogeneous, the homogeneous components of $\overline{f}$ are in $I^{\overline{\varphi}_A}$. As the normal forms of these homogeneous components do not depend on T or T^{-1}, they are consequently also contained in $I^{\overline{\varphi}_A} \cap K\langle X \rangle$. This shows that the intersection is also a homogeneous ideal. □

To turn Theorem 4.4 into an effective procedure, we can make use of the fact that there is a bijection between ideals in $K\langle X, T, T^{-1}\rangle/J$ and superideals of J in $K\langle X, T, T^{-1}\rangle$. Using this, we can obtain a Gröbner basis of $\hom_A(I)$ as described in Procedure 1.

Procedure 1 Gröbner basis enumeration of $\hom_A(I)$

Input: a generating set $F \subseteq K\langle X\rangle$ of an ideal I, a degree matrix $A \in \mathbb{Z}^{n \times k}$
Output: $G \subseteq I$ a Gröbner basis of $\hom_A(I)$
1: $T \leftarrow \{t_1, \ldots, t_k\}$, $T^{-1} \leftarrow \{t_1^{-1}, \ldots, t_k^{-1}\}$
2: $J \leftarrow$ the ideal in $K\langle X, T, T^{-1}\rangle$ generated by
$\qquad [X \cup T \cup T^{-1}, T \cup T^{-1}] \cup \{1 - t_j t_j^{-1} \mid j = 1, \ldots, k\}$
3: $H \leftarrow (\varphi_A(f) \mid f \in F) \subseteq K\langle X, T, T^{-1}\rangle$
4: enumerate a Gröbner basis $\{g_0, g_1, \ldots\}$ of $H + J$ w.r.t. an elimination ordering for $T \cup T^{-1}$
5: $G \leftarrow \{g_i \mid i \in \mathbb{N}, g_i \in K\langle X\rangle\}$
6: **return** G

Remark 4.5 If $A \in \mathbb{N}^{n \times k}$, then the ideal J can be replaced by

$$J' = \left([X \cup T, T] \cup \{1 - t_j t_j^{-1} \mid j = 1, \ldots, k\} \right).$$

To end this section, we discuss how computing the homogeneous part of an ideal $I \subseteq K\langle X, X^*\rangle$ allows to find elements of the form $p - q^*q \in I$, where $p \in K\langle X, X^*\rangle$ is given and q is unknown. In case that q is a monomial, we can choose a grading of $K\langle X, X^*\rangle$ that makes elements of the form $p - q^*q$ homogeneous. Taking the matrix A such that $\deg_A(x_i) = e_i$ and $\deg_A(x_i^*) = -e_i$, where e_i denotes the i-th unit vector of $\mathbb{Z}^n$ for all $i = 1, \ldots, n$, yields $\deg_A(q^*q) = 0$ for all $q \in \langle X, X^*\rangle$. Now, if there exists an element of the form $p - q^*q \in I$ and if we introduce a new variable v with $\deg_A(v) = 0$ and set $I' = I + (v - p)$, then the homogeneous polynomial $v - q^*q$ of degree 0 lies in I'. By enumerating generators of $\hom_A(I')$ we can systematically search for this element. We note that we can increase our chances of finding a suitable element by computing a Gröbner basis of $\hom_A(I')$ w.r.t. an elimination ordering for $\{v\}$. Because then, provided that I contains an element of the form $p - q^*q$, this Gröbner basis must contain an element with leading monomial v. In the following, we apply this procedure to prove Theorem 1.2.

Example Recall that Theorem 1.2 states that if $\mathcal{R}(B) \subseteq \mathcal{R}(A^*)$ and if the operator equation $AXB = C$ has a positive solution X, then the operator $B^*A^\dagger C$ is positive as well. To prove this statement by a computation with polynomials, we have to translate all properties of the operators first into identities and then into noncommutative polynomials. For the assumptions, the existence of a positive solution X and the range inclusion translate into the identities $AY^*YB = C$ and $B = A^*Z$, respectively, with new operators Y, Z. Furthermore, the existence of the Moore-Penrose inverse $A^\dagger$ is encoded by the four defining identities of $A^\dagger$. Translating all these identities and the respective adjoint statements into noncommutative polynomials, gives a set $F \subseteq \mathbb{Q}\langle X, X^*\rangle$ of 10 polynomials with integer coefficients in 12 indeterminates. Proving Theorem 1.2 boils down to finding an operator Q such that $B^*A^\dagger C = Q^*Q$, or in terms of polynomials, to finding a compatible polynomial of the form $b^*a^\dagger c - q^*q \in (F)$, where $b^*, a^\dagger, c \in X \cup X^*$ are known but $q \in \mathbb{Q}\langle X, X^*\rangle$, and therefore also q^*, are unknown. We note that the quiver encoding the domains and codomains of the operators involved consists of 3 vertices and 12 edges representing the 12 indeterminates. We refer to the MATHEMATICA notebook accompanying this paper for a visualisation of the quiver and for further information on the computations.

Following the procedure outlined above, we consider the ideal $I' = (F) + (v - b^*a^\dagger c) \subseteq \mathbb{Q}\langle X, X^*, v\rangle$ and enumerate a Gröbner basis of the homogeneous part $\hom_A(I')$ w.r.t. the degree matrix $A \in \mathbb{Z}^{13 \times 6}$ such that $\deg_A(v) = 0$, $\deg_A(x_i) = e_i$, $\deg_A(x_i^*) = -e_i$ for all $x_i \in X$, $x_i^* \in X^*$. We do this computation w.r.t. an elimination ordering for $\{v\}$. To speed up the computation, we first compute the reduced Gröbner basis G of

I' and then use this generating set as input to enumerate a Gröbner basis of $\text{hom}_A(I')$. While $|G| = 25$, the Gröbner basis of $\text{hom}_A(I')$ seems to be infinite. However, after enumerating 273 generators of $\text{hom}_A(I')$, one can see that $v - b^* y^* yb = v - (yb)^* yb \in \text{hom}_A(I')$, which shows that $b^* a^\dagger c - (yb)^* yb \in (F)$. After verifying that this polynomial is compatible with our quiver, this reveals that $B^* A^\dagger C = (YB)^* YB$ is indeed positive, and consequently, proves Theorem 1.2.

5 Monomial Part

Other elements in an ideal that are often of special interest are monomials. The goal of this section is to effectively describe the *monomial part* of a (right) ideal $I \subseteq K\langle X\rangle$, that is, the (right) ideal generated by all monomials contained in I. More precisely, we show how a simple adaptation of the technique described in the previous section allows to compute all monomials in a given right ideal. We note that the following definition is analogous to the commutative case (cf. the discussion before Algorithm 4.4.2 in [19]).

Definition 5.1 Let $I \subseteq K\langle X\rangle$ be an ideal. Then, we denote by $\text{mon}(I) := (m \in I \mid m \in \langle X\rangle)$ the *monomial part* of I. Analogously, for a right ideal $I_\rho \subseteq K\langle X\rangle$, we denote by $\text{mon}(I_\rho) := (m \in I \mid m \in \langle X\rangle)_\rho$ the *monomial part* of I_ρ.

This is clearly a monomial (right) ideal as defined below.

Definition 5.2 Let $I \subseteq K\langle X\rangle$ be a (right) ideal. Then, I is called a *monomial (right) ideal* if I has a (right) generating set consisting only of monomials.

Monomial ideals can also be characterized in a different way. To this end, we recall that the *support* of a polynomial $f \in K\langle X\rangle$, denoted by $\text{supp}(f)$, is the set consisting of all monomials that appear in f. Then, a (right) ideal $I \subseteq K\langle X\rangle$ is a monomial (right) ideal if and only if, with every element $f \in I$, also $\text{supp}(f) \subseteq I$. The next lemma follows directly from the definition above.

Lemma 5.3 *Let $I \subseteq K\langle X\rangle$ be a (right) ideal. Then,* $\text{mon}(I)$ *is the largest monomial (right) ideal contained in I.*

In the following, we describe how an adaptation of the technique from the previous section allows to compute a right Gröbner basis of $\text{mon}(I_\rho)$ for a given right ideal $I_\rho \subseteq K\langle X\rangle$. As for the homogeneous part of an ideal, we need some notation. First, we define the ideal

$$J = \left([X, T] \cup \{1 - t_j t_j^{-1} \mid j = 1, \ldots, n\} \right), \tag{2}$$

where $T = \{t_1, \ldots, t_n\}$ and $T^{-1} = \{t_1^{-1}, \ldots, t_n^{-1}\}$ are new indeterminates. Then, we consider the quotient algebra $\mathcal{B} = K\langle X, T, T^{-1}\rangle / J$. We again denote the equivalence classes of elements $f \in K\langle X, T, T^{-1}\rangle$ in $\mathcal{B}$ by $\overline{f}$. In $\mathcal{B}$, the $\overline{t}_j$ commute with all $\overline{x}_i$ but not with each other. The fact that the $\overline{t}_j$ do not commute with each other is the main and crucial difference compared to the previous section. Furthermore, each $\overline{t}_j$ can also be cancelled from the right.

Additionally, we define the K-algebra homomorphism

$$\varphi : K\langle X\rangle \to K\langle X, T, T^{-1}\rangle, \quad x_i \mapsto x_i t_i. \tag{3}$$

The map φ can be considered as a special case of the map φ_A defined in the previous section by setting $A = I_n$. As before, $\overline{\varphi}$ denotes the composition of φ with the canonical epimorphism. Applying $\overline{\varphi}$ to a polynomial f maps each monomial $m \in \text{supp}(f)$ to the equivalence class $\overline{mt_m}$, where t_m is a copy of m but in the variables $t_1, \ldots, t_n$.

Next, for a right ideal $I_\rho \subseteq K\langle X\rangle$ with right generating set F, we consider the extension of I_ρ along the homomorphism $\overline{\varphi}$, which we denote by

$$I_\rho^{\overline{\varphi}} := (\overline{\varphi}(f) \mid f \in F)_\rho \subseteq \mathcal{B}. \tag{4}$$

Note that, as in the previous section, this definition is independent of the generating set F. However, in contrast to before, $I_\rho^{\overline{\varphi}}$ is now a right ideal. The main result of this section is the following theorem.

Theorem 5.4 *Let $I_\rho \subseteq K\langle X \rangle$ be a right ideal. Furthermore, let $I_\rho^{\overline{\varphi}}$ be the extension of I_ρ along $\overline{\varphi}$. Then,*

$$\mathrm{mon}(I_\rho) = I_\rho^{\overline{\varphi}} \cap K\langle X \rangle := \bigcup_{\overline{f} \in I_\rho^{\overline{\varphi}}} \overline{f} \cap K\langle X \rangle.$$

Before we proceed to prove this theorem, we describe in Procedure 2 how a right Gröbner basis of $\mathrm{mon}(I_\rho)$ can be obtained.

Remark 5.5 Procedure 2 requires the computation of a right Gröbner basis of the right ideal $I_\rho^{\overline{\varphi}}$ in the quotient algebra $\mathcal{B} = K\langle X, T, T^{-1} \rangle / J$. As described in [9], this can be done effectively by introducing a new tag variable y and computing the Gröbner basis of a two-sided ideal containing J in the free algebra $K\langle X, T, T^{-1}, y \rangle$. This is what is done in line 3–5 of Procedure 2. We note that there are also other ways to compute a Gröbner basis of a one-sided ideal in a quotient algebra (see e.g. [21, Section 6.1.2]), however the approach described above has the advantage that it can be realized with a standard two-sided Gröbner basis implementation without any additional adaptations.

Procedure 2 Gröbner basis enumeration of $\mathrm{mon}(I_\rho)$

Input: a right generating set $F \subseteq K\langle X \rangle$ of a right ideal I_ρ
Output: $G \subseteq I_\rho$ a right Gröbner basis of $\mathrm{mon}(I_\rho)$
1: $T \leftarrow \{t_1, \ldots, t_n\}$, $T^{-1} \leftarrow \{t_1^{-1}, \ldots, t_n^{-1}\}$
2: $J \leftarrow$ the ideal in $K\langle X, T, T^{-1}, y \rangle$ generated by
        $[X, T] \cup \{1 - t_j t_j^{-1} \mid j = 1, \ldots, n\}$
3: $H \leftarrow (y \cdot \varphi(f) \mid f \in F) \subseteq K\langle X, T, T^{-1}, y \rangle$
4: enumerate a Gröbner basis $\{g_0, g_1, \ldots\}$ of $H + J$ w.r.t. an elimination ordering for $T \cup T^{-1}$
5: $G' \leftarrow \{g \mid yg = g_i \text{ for some } i \in \mathbb{N}\}$
6: $G \leftarrow G' \cap K\langle X \rangle$
7: **return** G

The proof of the commutative analog of Theorem 5.4 in [13] relies on the fact that a certain ideal is homogeneous w.r.t. a certain matrix grading and that an ideal can only be homogeneous w.r.t. this grading if it is a monomial ideal. Unfortunately, this argument does not immediately carry over to the case of noncommutative polynomials because no matter which matrix grading we choose, monomials that are permutations of each other will always have the same degree. For example, the right ideal $(x_1 x_2 - x_2 x_1)_\rho$ is homogeneous w.r.t. any matrix grading but it is clearly not a monomial ideal. In order to prove Theorem 5.4, we introduce the notion of a *separating pseudograding* for a subset $S \subseteq R$ of a ring R.

Definition 5.6 Let R be a ring and let $(N, \cdot)$ be a monoid. Furthermore, let $S \subseteq R$. We call a decomposition

$$R = \bigoplus_{\alpha \in N} S_\alpha,$$

of R into a direct sum of abelian groups a *separating (right) N-pseudograding* for S if the following conditions hold:

1. $S_1 S_\alpha \subseteq S_\alpha$ for all $\alpha \in N$;
2. $|S \cap S_\alpha| = 1$ for all $\alpha \in N$;

Intuitively speaking, a separating N-pseudograding for S allows us to separate the elements in S as they all have to lie in different subgroups S_α. As in the case of usual gradings, we omit the information about the monoid N in a separating N-pseudograding if N is clear from the context.

The following example shows that the multidegree yields a separating pseudograding for commutative monomials.

Example Let $R = K[X]$ be the usual polynomial ring in $X = \{x_1, \ldots, x_n\}$. Consider the monoid $(\mathbb{N}^n, +)$ and let $S = [X]$. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, we denote $x^\alpha := x_1^{\alpha_1} \ldots x_n^{\alpha_n} \in [X]$. The grading of R induced by the multidegree $\deg(x^\alpha) = \alpha$ is a separating $\mathbb{N}^n$-pseudograding for S. This follows from the fact that for all $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, the set S_α is given by $S_\alpha = \{cx^\alpha \mid c \in K \setminus \{0\}\}$.

For the following definition and proposition, we fix a ring R and a monoid $(N, \cdot)$. Given a separating $(N\text{-})$pseudograding for a set $S \subseteq R$, we can define *separable homogeneous* elements, or short *s-homogeneous* elements, and, based on this, *separable homogeneous* ideals, or short *s-homogeneous* ideals.

Definition 5.7 Let $S \subseteq R$ and let $R = \bigoplus_{\alpha \in N} S_\alpha$ be a separating pseudograding for S. An element $r \in R$ is called *separable homogeneous*, or short *s-homogeneous*, if $r \in S_\alpha$ for some $\alpha \in N$. If $r \neq 0$, then we call α the *s-degree* of r, denoted by $\mathrm{sdeg}(r) = \alpha$. An ideal $I \subseteq R$ is called *separable homogeneous*, or short *s-homogeneous*, if I is generated by s-homogeneous elements.

The following proposition is the crucial observation about separating pseudogradings. It is a weaker version of the property that, with an element r, a homogeneous ideal also contains all homogeneous components of r.

Proposition 5.8 *Let $S \subseteq R$ and $R = \bigoplus_{\alpha \in N} S_\alpha$ be a separating pseudograding for S. Furthermore, let $I_\rho \subseteq R$ be an s-homogeneous right ideal generated by s-homogeneous elements of s-degree 1. If $r = c_1 s_1 + \cdots + c_d s_d \in I_\rho$ with $s_1, \ldots, s_d \in S$ pairwise different and $c_1, \ldots, c_d \in S_1$, then $c_1 s_1, \ldots, c_d s_d \in I_\rho$.*

Proof W.l.o.g. we can assume that $c_i s_i \neq 0$ for all $i = 1, \ldots, d$. We note that it suffices to show that $c_1 s_1 \in I_\rho$, for then also $r - c_1 s_1 \in I_\rho$ and the statement follows by induction. We denote by $F \subseteq S_1$ a right generating set of I_ρ consisting of s-homogeneous elements of s-degree 1. Then, with $b_f \in R$ and $b_{f,\alpha} \in S_\alpha$ such that $b_f = \sum_{\alpha \in N} b_{f,\alpha}$, we can write r as

$$r = \sum_{f \in F} f b_f = \sum_{f \in F} f \sum_{\alpha \in N} b_{f,\alpha} = \sum_{f \in F} \sum_{\alpha \in N} f b_{f,\alpha}.$$

As all $f \in S_1$, it follows from the definition of a separating pseudograding that $f b_{f,\alpha} \in S_1 S_\alpha \subseteq S_\alpha$. Furthermore, by the definition of a separating pseudograding for S there exist pairwise different $\alpha_1, \ldots, \alpha_d \in N$ such that $S \cap S_{\alpha_i} = \{s_i\}$ for all $i = 1, \ldots, d$. Then, also $c_i s_i \in S_1 S_{\alpha_i} \subseteq S_{\alpha_i}$ for all $i = 1, \ldots, d$. Since the subgroups S_{α_i} have trivial intersection with each other, the nonzero elements $c_2 s_2, \ldots, c_d s_d$ cannot lie in S_{α_1}. Therefore, by comparing s-degrees, one can see that $c_1 s_1 = \sum_{f \in F} f b_{f,\alpha_1} \in I_\rho$. $\square$

Coming back to noncommutative polynomials, our next goal is to define a separating pseudograding for $\langle X \rangle$ in $K\langle X, T, T^{-1} \rangle$. To this end, we denote by $\mathcal{F}_n$ the free group of rank n generated by $g_1, \ldots, g_n$. This allows us to consider the two monoid homomorphisms

$$\lambda : \langle X, T, T^{-1} \rangle \to \mathcal{F}_n, \qquad x_i \mapsto g_i, \qquad t_i \mapsto 1, \qquad t_i^{-1} \mapsto 1,$$
$$\mu : \langle X, T, T^{-1} \rangle \to \mathcal{F}_n, \qquad x_i \mapsto 1, \qquad t_i \mapsto g_i, \qquad t_i^{-1} \mapsto g_i^{-1}.$$

Using λ and μ, we define the map sdeg : $\langle X, T, T^{-1} \rangle \to \mathcal{F}_n$ that sends each $m \in \langle X, T, T^{-1} \rangle$ to $\mathrm{sdeg}(m) := \mu(m)^{-1}\lambda(m) \in \mathcal{F}_n$.

Example Let $X = \{x_1, x_2\}$, $T = \{t_1, t_2\}$ and $T^{-1} = \{t_1^{-1}, t_2^{-1}\}$. Then, for $m = x_1 t_1 x_2 t_2 \in \langle X, T, T^{-1} \rangle$, we have $\mathrm{sdeg}(m) = (g_1 g_2)^{-1} g_1 g_2 = 1$. Analogously, taking $m' = t_1 t_2^{-1} x_1 t_1^{-1} x_2 \in \langle X, T, T^{-1} \rangle$, yields $\mathrm{sdeg}(m') = (g_1 g_2^{-1} g_1^{-1})^{-1} g_1 g_2 = g_1 g_2 g_2$.

The following lemma captures some important properties of the map sdeg.

Lemma 5.9 *Let $m, m' \in \langle X, T, T^{-1} \rangle$, $x_i \in X$, $t_j \in T$ and $t_j^{-1} \in T^{-1}$. Then, the following hold.*

1. $\mathrm{sdeg}(m x_i t_j m') = \mathrm{sdeg}(m t_j x_i m')$;
2. $\mathrm{sdeg}(m t_j t_j^{-1} m') = \mathrm{sdeg}(m m')$;
3. $\mathrm{sdeg}(m) = 1 \implies \mathrm{sdeg}(m m') = \mathrm{sdeg}(m')$;

Proof The properties 1 and 2 follow immediately from the definition. To prove the third property, we assume $\mathrm{sdeg}(m) = 1$. This yields

$$\mathrm{sdeg}(mm') = \mu(mm')^{-1}\lambda(mm') = \mu(m')^{-1}\mu(m)^{-1}\lambda(m)\lambda(m')$$
$$= \mu(m')^{-1}\mathrm{sdeg}(m)\lambda(m') = \mu(m')^{-1}\lambda(m') = \mathrm{sdeg}(m').$$

$\square$

The map sdeg allows us to decompose $K\langle X, T, T^{-1} \rangle$ into a direct sum of the abelian subgroups

$$K\langle X, T, T^{-1} \rangle_\alpha = \left\{ \sum_{m \in \langle X, T, T^{-1} \rangle} c_m m \mid c_m \in K, \mathrm{sdeg}(m) = \alpha \text{ if } c_m \neq 0 \right\},$$

for $\alpha \in \mathcal{F}_n$. In particular, the following proposition tells us that this decomposition forms a separating $\mathcal{F}_n$-pseudograding for $\langle X \rangle$, and hence, justifies the name sdeg.

Proposition 5.10 *The abelian subgroups $K\langle X, T, T^{-1} \rangle_\alpha$ with $\alpha \in \mathcal{F}_n$ as defined above form a separating $\mathcal{F}_n$-pseudograding for $\langle X \rangle$.*

Proof It is clear that the subgroups $K\langle X, T, T^{-1} \rangle_\alpha$ decompose $K\langle X, T, T^{-1} \rangle$ into a direct sum. Furthermore, the first condition of Definition 5.6 follows immediately from Lemma 5.9. Finally, we note that sdeg restricted to $\langle X \rangle$ is an isomorphism. Hence, $\mathrm{sdeg}(m) \neq \mathrm{sdeg}(m')$ for all $m \neq m' \in \langle X \rangle$. This implies the second property of a separating $\mathcal{F}_n$-pseudograding. $\square$

It follows from the first two properties in Lemma 5.9 that the map sdeg is invariant modulo the ideal J from (2). Hence, we can set $\mathrm{sdeg}(\overline{m}) = \mathrm{sdeg}(m)$ for all $m \in \langle X, T, T^{-1} \rangle$ and thereby extend sdeg to the quotient algebra $\mathcal{B}$. Consequently, the separating $\mathcal{F}_n$-pseudograding for $\langle X \rangle$ in $K\langle X, T, T^{-1} \rangle$ can be extended in a straightforward way to give a separating $\mathcal{F}_n$-pseudograding for $\langle \overline{X} \rangle = \{\overline{x} \mid x \in \langle X \rangle\}$ in $\mathcal{B}$.

Finally, we have all tools available to prove Theorem 5.4. We split this proof into two lemmas.

Lemma 5.11 *Let $I_\rho \subseteq K\langle X \rangle$ be a right ideal. Furthermore, let $I_\rho^{\overline{\varphi}}$ be the extension of I_ρ along $\overline{\varphi}$. Then,*

$$\mathrm{mon}(I_\rho) \subseteq I_\rho^{\overline{\varphi}} \cap K\langle X \rangle \subseteq I_\rho.$$

Proof We note that it follows from the definition of $I_\rho^{\overline{\varphi}}$ that $f \in I_\rho$ implies $\overline{\varphi}(f) \in I_\rho^{\overline{\varphi}}$. Now, to prove the first inclusion, $\mathrm{mon}(I_\rho) \subseteq I_\rho^{\overline{\varphi}} \cap K\langle X \rangle$, let $m = x_{i_1} \ldots x_{i_k} \in \mathrm{mon}(I_\rho)$. Then, we get $\overline{mt_{i_1} \ldots t_{i_k}} = \overline{\varphi}(m) \in I_\rho^{\overline{\varphi}}$, which implies

$$\overline{m} = \overline{m} \cdot \overline{t_{i_1} \ldots t_{i_k} t_{i_k}^{-1} \ldots t_{i_1}^{-1}} = \overline{mt_{i_1} \ldots t_{i_k}} \cdot \overline{t_{i_k}^{-1} \ldots t_{i_1}^{-1}} \in I_\rho^{\overline{\varphi}},$$

and consequently, $m \in I_\rho^{\overline{\varphi}} \cap K\langle X \rangle$.

For the second inclusion, $I_\rho^{\overline{\varphi}} \cap K\langle X \rangle \subseteq I_\rho$, let $f \in I_\rho^{\overline{\varphi}} \cap K\langle X \rangle$. Then, f can be written as

$$f = \sum_{i=1}^d \varphi(f_i) q_i + \sum_{i=1}^e g_i v_i$$

with $f_i \in I_\rho$, $g_i \in [X, T] \cup \{1 - t_j t_j^{-1} \mid j = 1, \ldots, n\}$ and $q_i, v_i \in K\langle X, T, T^{-1} \rangle$. Note that the left hand side of this identity does not depend on the indeterminates in T and T^{-1}. Hence, by setting $t_j = t_j^{-1} = 1$ for all $j = 1, \ldots, n$, we obtain $f = \sum_{i=1}^d f_i \tilde{q}_i \in I_\rho$ with $\tilde{q}_i \in K\langle X \rangle$. $\square$

Lemma 5.12 *Let $I_\rho \subseteq K\langle X \rangle$ be a right ideal. Furthermore, let $I_\rho^{\overline{\varphi}}$ be the extension of I_ρ along $\overline{\varphi}$. Then, $I_\rho^{\overline{\varphi}} \cap K\langle X \rangle$ is a monomial right ideal.*

Proof Let $f = c_1 m_1 + \cdots + c_d m_d \in I_\rho^{\overline{\varphi}} \cap K\langle X \rangle$ with nonzero $c_1, \ldots, c_d \in K$ and pairwise different $m_1, \ldots, m_d \in \langle X \rangle$. To show that $I_\rho^{\overline{\varphi}} \cap K\langle X \rangle$ is a monomial right ideal, we have to show that $m_1, \ldots, m_d \in I_\rho^{\overline{\varphi}} \cap K\langle X \rangle$, which is equivalent to $\overline{m}_1, \ldots, \overline{m}_d \in I_\rho^{\overline{\varphi}}$. To show this, we fix the $\mathcal{F}_n$-pseudograding for $\langle \overline{X} \rangle$ in $\mathcal{B}$ induced by the map sdeg and note that the image $\overline{\varphi}(g)$ of any nonzero $g \in K\langle X \rangle$ under the map $\overline{\varphi}$ defined in (3) is an s-homogeneous polynomial of s-degree 1. In particular, this means that $I_\rho^{\overline{\varphi}}$ is an s-homogeneous right ideal in $\mathcal{B}$ generated by s-homogeneous elements of s-degree 1. Since $\mathrm{sdeg}(\overline{c}_i) = 1$ and $\overline{m}_i \in \langle \overline{X} \rangle$ for all $i = 1, \ldots, d$, Proposition 5.8 is applicable and yields that $\overline{c_1 m_1}, \ldots, \overline{c_d m_d} \in I_\rho^{\overline{\varphi}}$. But then clearly also $\overline{m}_1, \ldots, \overline{m}_d \in I_\rho^{\overline{\varphi}}$. $\square$

The proof of Theorem 5.4 now follows from Lemmas 5.3, 5.11 and 5.12.

Remark 5.13 We make some remarks on Theorem 5.4.

1. Theorem 5.4 can also be adapted to work with left ideals. In this case, the ideal J, w.r.t. which the quotient is taken, has to be changed to

$$J' = \left([X, T] \cup \{1 - t_j^{-1} t_j \mid j = 1, \ldots, n\} \right).$$

   Then, in the quotient $K\langle X, T, T^{-1} \rangle / J'$ each $\overline{t}_j$ can be cancelled from the left instead of from the right. To then prove the theorem for left ideals, Definition 5.6 and the map sdeg have to be adapted accordingly as well.
2. Unfortunately, this approach does not generalize to two-sided ideals, as witnessed by the following example.

Example In this example, we show that the approach described in this section does not generalize to two-sided ideals in a straightforward way. To this end, we consider the ideal $I = (x_1 - x_2) \subseteq K\langle x_1, x_2 \rangle$ over an arbitrary field K. It is not hard to see that $\mathrm{mon}(I) = \{0\}$. However, if we consider the two-sided ideal $I^{\overline{\varphi}} = (\overline{\varphi}(x_1 - x_2)) = (x_1 t_1 - x_2 t_2) \subseteq \mathcal{B}$, then $x_1 x_2 - x_2 x_1 \in I^{\overline{\varphi}} \cap K\langle x_1, x_2 \rangle$ as the following computation shows:

$$\left(\overline{x_1 t_1 - x_2 t_2}\right)\overline{x_2 t_1}^{-1} - \overline{x_2}\left(\overline{x_1 t_1 - x_2 t_2}\right)\overline{t_1}^{-1}$$
$$= \left(\overline{x_1 x_2} - \overline{x_2 x_2 t_2 t_1^{-1}}\right) - \left(\overline{x_2 x_1} - \overline{x_2 x_2 t_2 t_1^{-1}}\right)$$
$$= \overline{x_1 x_2 - x_2 x_1} \in I^{\overline{\varphi}}.$$

To compute a generating set of $\mathrm{mon}(I)$ in case of a two-sided ideal $I \subseteq K\langle X \rangle$, we were so far only able to prove the following rather restrictive result. In what follows, we fix a monomial ordering $\preceq$ on $\langle X \rangle$. Recall that the *tail* of $f \in K\langle X \rangle$ is $\mathrm{tail}(f) = f - \mathrm{lc}(f)\,\mathrm{lm}(f)$, where $\mathrm{lc}(f)$ denotes the leading coefficient of f (w.r.t. $\preceq$).

Proposition 5.14 *Let X, Y be two disjoint sets of indeterminates and let $I \subseteq K\langle X, Y \rangle$ be an ideal. Furthermore, let $G \subseteq K\langle X, Y \rangle$ be a Gröbner basis of I such that $\mathrm{lm}(g) \in \langle X \rangle$ and $\mathrm{tail}(g) \in K\langle Y \rangle$ for all $g \in G$. Then $G \cap \langle X \rangle$ is a Gröbner basis of $\mathrm{mon}(I)$.*

To prove this proposition, we recall the concept of polynomial (top) reduction in $K\langle X \rangle$. For $f, f', g \in K\langle X \rangle$ with $f, g \neq 0$, we write $f \to_g f'$ if there exist $a, b \in \langle X \rangle$ such that $\mathrm{lm}(f) = a\,\mathrm{lm}(g)b$ and $f' = f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)}agb$. It is well-known that a generating set $G \subseteq K\langle X \rangle$ of an ideal $I \subseteq K\langle X \rangle$ is a Gröbner basis of I if for every $f \in I$, there exist $g_1, \ldots, g_k \in G$ and $f_0, \ldots, f_k \in K\langle X \rangle$ such that $f_0 = f$, $f_k = 0$ and $f_{i-1} \to_{g_i} f_i$ for all $i = 1, \ldots, k$. Additionally, we also need the following result about Gröbner bases of monomial ideals, which follows immediately from our definition of a Gröbner basis.

Lemma 5.15 *Let $M \subseteq \langle X \rangle$ be a set of monomials generating an ideal $(M) \subseteq K\langle X \rangle$. Then, M is a Gröbner basis of (M).*

Proof (Proof of Proposition 5.14) Denote $M = G \cap \langle X \rangle$. Due to Lemma 5.15, it suffices to show that $(M) = \mathrm{mon}(I)$. The inclusion $(M) \subseteq \mathrm{mon}(I)$ is trivial. For the other inclusion $\mathrm{mon}(I) \subseteq (M)$, let $m \in \mathrm{mon}(I)$ be a monomial. Since G is a Gröbner basis of I, there exist $g_1, \ldots, g_k \in G$ such that

$$m \to_{g_1} m_1 \to_{g_2} \cdots \to_{g_k} m_k = 0,$$

with $m_1, \ldots, m_k \in K\langle X, Y \rangle$. In particular, we have that $m_1 = -a\,\mathrm{tail}(g_1)b$ for some $a, b \in \langle X \rangle$. Since $\mathrm{lm}(g_2) \in \langle X \rangle$ but $\mathrm{tail}(g_1) \in K\langle Y \rangle$, the second reduction can only act on a or b but not on $\mathrm{tail}(g_1)$. W.l.o.g. assume that the reduction with g_2 acts on a. Then, $m_2 = a'\,\mathrm{tail}(g_2)a''\,\mathrm{tail}(g_1)b$. Analogously, since $\mathrm{lm}(g_3) \in \langle X \rangle$, the reduction with g_3 cannot act on $\mathrm{tail}(g_1)$ or $\mathrm{tail}(g_2)$ and as this also holds for all other reductions, m_k must be of the form

$$m_k = (-1)^k a_1\,\mathrm{tail}(g_{i_1})a_2\,\mathrm{tail}(g_{i_2})\ldots a_k\,\mathrm{tail}(g_{i_k})a_{k+1}$$

for some $a_1, \ldots, a_{k+1} \in \langle X \rangle$ and $\{i_1, \ldots, i_k\} = \{1, \ldots, k\}$. Note that all parts in any m_j that lie in $K\langle X \rangle$ are subwords of m. Furthermore, since the reductions with all g_i can act on these parts, we get that $\mathrm{lm}(g_i)$ divides m for all $i = 1, \ldots, k$. Hence, in particular, $\mathrm{lm}(g_k)$ divides m. To finish the proof, we show that g_k is in fact a monomial and therefore contained in M. To see this, we note that m_k can only be zero if one of the factors in this product is zero and since none of the a_j can be zero, we must have $\mathrm{tail}(g_i) = 0$ for some $1 \leq i \leq k$. In particular, we know that $m_{k-1} \neq 0$, and therefore, $\mathrm{tail}(g_k) = 0$. This means that g_k is a monomial, and so, $g_k \in M$, which implies that $m \in (M)$. $\square$

It remains open how to compute a generating set of $\mathrm{mon}(I)$ for an arbitrary (finitely generated) two-sided ideal $I \subseteq K\langle X \rangle$.

References

1. Arias, M.L., Gonzalez, M.C.: Positive solutions to operator equations $AXB = C$. Linear Algebra Appl. **433**, 1194–1202 (2010)
2. Bell, J., Heinle, A., Levandovskyy, V.: On noncommutative finite factorization domains. Trans. Am. Math. Soc. **369**, 2675–2695 (2017)
3. Borges, M.A., Borges, M.: Gröbner bases property on elimination ideal in the noncommutative case. In: Gröbner Bases and Applications, pp. 323–337. Cambridge University Press (1998)
4. Chenavier, C., Hofstadler, C., Raab, C.G., Regensburger, G.: Compatible rewriting of noncommutative polynomials for proving operator identities. In: Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, pp. 83–90 (2020)
5. Cvetković-Ilić, D.S., Hofstadler, C., Hossein Poor, J., Milošević, J., Raab, C.G., Regensburger, G.: Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law. Appl. Math. Comput. **409**, Article 126357, 10 pages (2021)
6. Green, E.L.: Multiplicative bases, Gröbner bases, and right Gröbner bases. J. Symb. Comput. **29**, 601–623 (2000)
7. Helton, J.W., Stankus, M., Wavrik, J.J.: Computer simplification of formulas in linear systems theory. IEEE Trans. Autom. Control **43**, 302–314 (1998)
8. Helton, J.W., Wavrik, J.J.: Rules for computer simplification of the formulas in operator model theory and linear systems. In: Nonselfadjoint Operators and Related Topics, pp. 325–354. Birkhäuser, Basel (1994)
9. Heyworth, A.: One-sided noncommutative Groebner bases with applications to computing Green's relations. J. Algebra **242**, 401–416 (2001)
10. Hofstadler, C.: Certifying operator identities and ideal membership of noncommutative polynomials, Master's thesis, Johannes Kepler University Linz (2020)
11. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 2. Springer, Berlin (2005)
12. Levandovskyy, V., Schönemann, H., Abou Zeid, K.: 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, pp. 305–311 (2020)
13. Miller, E.: Finding all monomials in a polynomial ideal. arXiv:1605.08791 (2016)
14. Mora, T.: Gröbner Bases and the Word Problem. University of Genova, Preprint (1987)
15. Mora, T.: An introduction to commutative and noncommutative Gröbner bases. Theor. Comput. Sci. **134**, 131–173 (1994)
16. Mora, T.: Solving Polynomial Equation Systems IV: Buchberger Theory and Beyond, vol. 4. Cambridge University Press, Cambridge (2016)
17. Nordbeck, P.: On some basic applications of Gröbner bases in non-commutative polynomial rings. In: Gröbner Bases and Applications, pp. 463–472. Cambridge University Press (1998)
18. Raab, C.G., Regensburger, G., Hossein Poor, J.: Formal proofs of operator identities by a single formal computation. J. Pure Appl. Algebra **225**, Article 106564, 20 pages (2021)
19. Saito, M., Sturmfels, B., Takayama, N.: Gröbner deformations of hypergeometric differential equations. Algorithms Comput. Math. **6** (2000)
20. Schmitz, L., Levandovskyy, V.: Formally verifying proofs for algebraic identities of matrices. In: CICM 2020, vol. 12236, pp. 222–236. LNCS (2020)
21. Xiu, X.: Non-commutative Gröbner Bases and Applications, PhD thesis, University of Passau, Germany (2012)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.