Algebraic proof methods for identities of matrices and operators: improvements of Hartwig’s triple reverse order law

Dragana S. Cvetković-Ilić¹, Clemens Hofstadler², Jamal Hossein Poor², Jovana Milošević¹, Clemens G. Raab², and Georg Regensburger²

¹Department of Mathematics, Faculty of Sciences and Mathematics, University of Niš, Serbia
²Institute for Algebra, Johannes Kepler University Linz, Austria

Abstract

When improving results about generalized inverses, the aim often is to do this in the most general setting possible by eliminating superfluous assumptions and by simplifying some of the conditions in statements. In this paper, we use Hartwig’s well-known triple reverse order law as an example for showing how this can be done using a recent framework for algebraic proofs and the software package OperatorGB. Our improvements of Hartwig’s result are proven in rings with involution and we discuss computer-assisted proofs that show these results in other settings based on the framework and a single computation with noncommutative polynomials.

Keywords: matrices and linear operators, algebraic operator identities, generalized inverses, reverse order law, automated proofs, noncommutative polynomials, quiver representations

MSC 2020: 15A09, 68V15, 03B35 (Primary); 16B50, 16G20 (Secondary)

1 Introduction

Introducing generalized inverses and developing tools working with them in the case when ordinary inverses do not exist, resulted in a lot of progress in several branches of mathematics and many other fields outside of mathematics (mechanics, robotics, control theory, automation, etc.). The importance and usefulness of this area of research is demonstrated by various open problems that have been solved using the theory of generalized inverses and by many published results. However, a lot of recently published results for generalized inverses and their applications were proved only under restrictive assumptions which limit their applications to certain very particular cases. One reason for that is that, in contrast to the setting of matrices, generalized inverses are not defined for each element of more general settings considered (algebras of operators, C*-algebras, rings, . . . ). In order to benefit from the rich theory of generalized inverses and many
already developed useful techniques, researchers usually impose existence of generalized inverses when proving statements. This leads to many results with redundant instances of assuming regularity of certain elements which makes them less applicable.

The basic example for unnecessary regularity assumptions is the matrix equation $AXB = C$, which was one of the first applications of the later called Moore-Penrose inverse that was introduced by Moore and Penrose independently. Its solvability and the general solution were considered by Penrose in 1955 [1] in the same paper in which he introduced the four Penrose equations. Since this result is almost algebraic, it was very easy to generalize it for example to the case of operator equations $AXB = C$ but under the additional assumptions of the closedness of the ranges of the bounded linear operators $A$ and $B$ (that is equivalent with the existence of their Moore-Penrose inverses for operators on Hilbert spaces). Solvability of this equation in the general case was only considered several years ago, see [2], but many other problems, such as, for example, the existence of a positive solution of that same equation, are still open in the general case. In fact, there are a lot of problems like this where we have an answer only in some particular cases. So, in the recent years a lot of effort has been made to widen the range of applicability of these results by considering more general cases of the problems without imposing any additional assumptions. This paper is exactly one such important step in generalizing Hartwig’s triple reverse order law.

In this paper, we present several significant improvements of Hartwig’s triple reverse order law motivated by using the software package OperatorGB [3], which is based on [4, 5]. The aim is to prove statements in an abstract setting in such a way that analogous statements in various concrete settings (e.g. for matrices, linear bounded operators, $C^*$-algebras, . . . ) can easily be proven in a rigorous way, but without inspecting every step of the proof of the abstract statement. To this end, we employ a recent framework that allows to produce rigorous proofs for several different concrete settings by translating a single statement about abstract noncommutative polynomials. This framework was developed in [4] and the software package OperatorGB provides extensive computer support for doing the computations needed. In particular, the software provides explicit certificates of identities, which can be checked independently. Moreover, the software can also be used to explore variations of given statements. That is what initiated the improvements of Hartwig’s triple reverse order law presented in this paper. Based on the results obtained by this software we give a hand proof in the setting of rings which hopefully provides motivation for further research with the same idea. In addition, we explain how computer-assisted proofs of all these improvements can be done and we provide a MATHEMATICA notebook containing all these automated proofs at http://gregensburger.com/softw/OperatorGB. These improvements are the first new results that are obtained by applying the framework and software. From this website also a MATHEMATICA as well as a SAGEMATH version of the OperatorGB package can be obtained.

The main setting that we consider in this paper is a ring $R$ with a unit $1 \neq 0$ and an involution $a \mapsto a^*$ satisfying

$$(a^*)^* = a, \quad (a + b)^* = a^* + b^*, \quad (ab)^* = b^*a^*. \quad (1)$$

**Definition 1.1.** We say that $a \in R$ is Moore-Penrose invertible (or MP-invertible), if there exists $b \in R$ such that the following hold:

$$aba = a, \quad bab = b, \quad (ab)^* = ab, \quad (ba)^* = ba.$$
An element $b$ that satisfies (1) is called a Moore-Penrose inverse of $a$. 

It is well known that the Moore-Penrose inverse is unique when it exists. We denote the Moore-Penrose inverse of $a$ by $a^\dagger$. We point out some properties of the Moore-Penrose inverse that follow from the definition. Clearly, $a$ is MP-invertible if and only if $a^*$ is MP-invertible; in this case $(a^*)^\dagger = (a^\dagger)^*$.

If $a$ is MP-invertible, then so are $a^*a$ and $aa^*$, with

$$(a^*a)^\dagger = a^\dagger(a^\dagger)^\dagger, \quad (aa^*)^\dagger = (a^\dagger)a^\dagger.$$ 

Definition 1.2. An element $a \in \mathcal{R}$ is left $*$-cancellable if, for all $z \in \mathcal{R}$, $a^*az = 0$ implies $az = 0$, it is right $*$-cancellable if, for all $z \in \mathcal{R}$, $zaa^* = 0$ implies $za = 0$, and $*$-cancellable if it is both left and right cancellable.

We observe that $a$ is left $*$-cancellable if and only if $a^*$ is right $*$-cancellable. In a $C^*$-algebra, every element is $*$-cancellable: If $a^*az = 0$, then $(az)^*az = 0$ which implies $az = 0$; similarly $zaa^* = 0$ implies $za = 0$.

If $b \in \mathcal{R}$ satisfies $\{i, \ldots, j\}$ of the Penrose equations from (1) we say that $b$ is a $\{i, \ldots, j\}$-inverse of $a$. The set of all $\{i, \ldots, j\}$-inverses of $a$ is denoted by $a\{i, \ldots, j\}$. Evidently $a\{1,2,3,4\} = \{a^\dagger\}$. We say that an element $a \in \mathcal{R}$ is regular if $a\{1\} \neq \emptyset$. In general, in $C^*$-algebras we have that the regularity property is equivalent with MP-invertibility. In particular, in an algebra of bounded linear operators the regularity of an arbitrary operator $A$ is equivalent to the closedness of the range of $A$ while in a ring with involution MP-invertibility of $m$ is equivalent to the right $*$-cancellability of $m$ and group invertibility of $mm^*$ (see Theorem 8.25 from [6] or Theorem 5.3 from [7]).

Definition 1.3. An element $a \in \mathcal{R}$ is EP if $a\mathcal{R} = a^*\mathcal{R}$.

In the following subsection, we give a self-contained informal overview of the framework for algebraic proofs and of the software package $\text{OperatorGB}$. In Section 2, we first discuss Hartwig’s triple reverse order law and related results from the literature. Then, we give hand proofs of several improvements of it in rings with involution. After that, in Section 2.1, we discuss how these results can be proven with the help of the computer in such a way that the framework yields rigorous proofs for these statements also in the context of matrices and operators. Formal definitions and statements about the framework for algebraic proofs, which is used by the software $\text{OperatorGB}$, are summarized in the appendix.

1.1 Introduction to the framework for algebraic proofs

The advantage of the framework presented below is that a single computation in an abstract setting proves analogous statements in various concrete settings (e.g. for matrices, linear bounded operators, $C^*$-algebras, . . .) without having to inspect every step of the abstract computation. Just like in any ring, computations with noncommutative polynomials allow any two elements to be added or multiplied. Therefore, it is not clear a priori that a given proof of a statement in a ring is valid also for rectangular matrices or
operators with domains and codomains. Using the framework for algebraic proofs, the following steps have to be carried out once in a suitable ring of noncommutative polynomials. Then, to rigorously prove a statement for various concrete settings, based on Theorem A.1, it suffices to check that the polynomials corresponding to the assumptions and claims are compatible with different domains and codomains of operators.

1. Express all assumptions and claimed properties as identities in terms of operators.

2. Take the differences of the left and right hand sides of these identities and replace the individual operators uniformly by noncommutative indeterminates in order to convert the identities into polynomials.

3. Find a concrete representation of the polynomials corresponding to the claim as a two-sided linear combination of polynomials corresponding to the assumptions, where coefficients are polynomials.

Representations of polynomials as mentioned in the last step are called cofactor representations and serve as certificates for ideal membership that can be checked independently of how they were found. However, finding them is a hard problem, since for noncommutative polynomials ideal membership is undecidable in general, see e.g. [8]. In practice, cofactor representations often can be found by computing a (partial) Gröbner basis, see [5] and references therein. Already in the pioneering work [9, 10] Gröbner bases have been used to simplify matrix identities in linear systems theory. Proving operator identities using Gröbner basis computations and related questions are also addressed in [11].

The software package OperatorGB provides the command Certify, which not only tries to compute cofactor representations but also does the compatibility checks of assumptions and claims. Inspecting the explicit cofactor representations found by the software can also give hints how assumptions could be relaxed by dropping the assumptions that do not appear in the cofactor representations. More generally, the software makes it easy to experiment with different sets of assumptions for proving a desired claim. Improvements of Hartwig’s triple reverse order law found by such experiments were the basis for the results presented in the next section. For details on how our framework and software are used to find and prove these results, see Section 2.1.

Next, we illustrate the approach with a simple statement about inner inverses of matrices, for details of the framework see the appendix. In [12, Thm. 2.3], Werner proved among other things the following statement about inner inverses of complex matrices. If \( A \) and \( B \) are complex matrices such that \( AB \) exists, then \( \mathcal{N}(A) \subseteq \mathcal{R}(B) \) implies that \( B\{1\}A\{1\} \subseteq (AB)\{1\} \). As a first step, we have to phrase all properties stated in the assumptions and in the claim in terms of identities of matrices, which results in the following statement. For any complex matrices \( A^{-}, B^{-} \) with

\[
AA^{-}A = A \quad \text{and} \quad BB^{-}B = B,
\]

we have that

\[
BB^{-}(I - A^{-}A) = I - A^{-}A
\]

implies

\[
ABB^{-}A^{-}AB = AB.
\]

The formats of these matrices can be visualized by the following diagram.
Secondly, we represent these identities by noncommutative polynomials in the indeterminates \{a, a^-, b, b^-, i\}. This is done by uniformly replacing each matrix (including the identity matrix) by an indeterminate and forming the difference of the left and right hand side of each identity.

\begin{align*}
f_1 &= aa^- - a \\
f_2 &= bb^- b - b \\
f_3 &= bb^- (i - a^- a) - i + a^- a \\
f &= ab^- a^- ab - ab \tag{5}
\end{align*}

Moreover, for correctly handling the identity matrix, we also need to represent its algebraic identities in terms of polynomials.

\begin{align*}
f_4 &= ai - a \\
f_5 &= ia^- - a^- \\
f_6 &= ib - b \\
f_7 &= b^- i - b^- \\
f_8 &= i^2 - i \tag{6}
\end{align*}

Finally, either by hand or with the help of software, we can express the polynomial \(f\) representing the claim in terms of the polynomials \(f_1, \ldots, f_8\) representing the assumptions.

\begin{align*}
f &= f_1 b + a f_2 - a f_3 b + (ab^- - a) f_6 \tag{8}
\end{align*}

By Theorem A.1, it follows from (8) that (4) holds for any matrices \(A, B\) with inner inverses \(A^-, B^-\) satisfying (3), see Lemma A.2 in the appendix. Moreover, based on the theorem, the cofactor representation (8) also proves the analogous statement for bounded linear operators \(A, B\) between Hilbert spaces \(U, V, W\) as in the following diagram.

As mentioned above, explicit cofactor representations not only certify ideal membership, but can also give hints how assumptions could be relaxed. In particular, they also allow to analyze which assumptions can be relaxed for proving a given identity of operators. For example, (8) does not involve \(f_4, f_5, f_7, f_8\), so in \(BB^- (I - A^- A) = I - A^- A\) we could replace the identity matrix \(I\) by any other matrix \(J\) satisfying \(JB = B\). Trivially, any cofactor representation with polynomials having only integer coefficients, as in (8) above, also holds in any ring, and hence proves an analogous statement for rings.

As discussed before, to apply the proof framework directly, one has to translate all properties of the operators involved into identities. In the context of generalized inverses, such properties are often conditions on ranges and kernels of some basic operators. If a projection (idempotent) on these spaces can be expressed in terms of basic operators, the translation to identities is immediate, as illustrated in the example above. Inclusion of ranges \(\mathcal{R}(A) \subseteq \mathcal{R}(B)\) can be translated in many situations to the existence of a factorization \(A = BC\) for some operator \(C\). In Hilbert or Banach spaces, this is the well-known factorization property in Douglas’ lemma. For proving the existence of such a linear operator \(C\) without any additional properties, one just needs operators defined on a vector space over an arbitrary field. This principle will play a prominent role in Section 2.1.
2 Improvements of Hartwig’s triple reverse order law

The “reverse order law” problem was originally posed by Greville [13] as early as in the 1960’s, who first considered it in the case of the Moore-Penrose inverse of the product of two matrices. Namely, for given matrices $A, B$ such that $AB$ is defined the following was proved:

$$(AB)^\dagger = B^\dagger A^\dagger ⇔ \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B), \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*).$$  \hspace{1cm} (9)

This was followed by further research on this subject branching in several directions:

- for products of more than two matrices,
- for different classes of generalized inverses ($\{1\}, \{1, 3\}, \{1, 2, 3\}$, etc.), and
- in different settings (operator algebras, $C^*$-algebras, rings, etc.).

For more information on this subject please see [14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32].

One of the first to be inspired by Greville’s result (9) was Hartwig [33], who studied the reverse order law for the Moore-Penrose inverse of the product of three matrices. Indeed, he considered necessary and sufficient conditions such that

$$(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$$ \hspace{1cm} (10)

holds.

Theorem 2.1. [33] Let $A, B, C$ be complex matrices such that $ABC$ is defined and let $P = A^\dagger ABCC^\dagger$, $Q = CC^\dagger B^\dagger A^\dagger$. The following conditions are equivalent:

(i) $(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$;
(ii) $Q \in P\{1, 2\}$ and both of $A^*APQ$ and $QPCC^*$ are Hermitian;
(iii) $Q \in P\{1, 2\}$ and both of $A^*APQ$ and $QPCC^*$ are EP;
(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ and $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$;
(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ and $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

This inspired many authors to continue research in these directions and it was precisely Hartwig’s result that motivated further consideration of the reverse order law for MP-inverses in the case of three elements in certain other settings such as in the algebra of bonded linear operators and in $C^*$-algebras, which was done in [34] and [35], respectively. In both papers, results analogous to Hartwig’s paper were obtained, but with the additional conditions of regularity of all three elements and their products. Here, we mention a result presented in [35] for the case of $C^*$-algebras in order to give a clear picture of the conditions assumed and the equivalences obtained (in the case of bounded linear operators between Hilbert spaces the theorem looks identically).
Theorem 2.2. [35] Let $A$ be a complex unital $C^*$-algebra and let $a, b, c \in A$ be such that $a, b, c$ and $abc$ are regular. Let $p = a^\dagger abc^\dagger$ and $q = cc^\dagger b^\dagger a^\dagger a$. Then, the following conditions are equivalent:

(i) $(abc)^\dagger = c^\dagger b^\dagger a^\dagger$;

(ii) $q \in p\{1, 2\}$ and both of $a^*apq$ and $qpcc^*$ are Hermitian;

(iii) $q \in p\{1, 2\}$ and both of $a^*apq$ and $qpcc^*$ are EP;

(iv) $q \in p\{1\}$, $a^*apA = q^*A$ and $cc^*p^*A = qA$;

(v) $pq = (pq)^2$, $a^*apA = q^*A$ and $cc^*p^*A = qA$.

The main results presented here represent an important improvement of Hartwig’s result in several senses:

- We consider the problem in rings with involution, which is a more abstract setting than what was considered in the literature so far. Together with the framework and the discussion in Section 2.1 this generalizes all the results previously mentioned.

- We relax conditions (iv) and (v) in the original result of Hartwig (Theorem 2.1), by replacing the respective equalities of ranges assumed in both of these conditions with appropriate inclusions of ranges. For example, we show in Theorems 2.3 and 2.4 that certain combinations of inclusions (there are four of them in total), along with the assumption that the element $pq$ is idempotent, imply (10), while the other two combinations do not guarantee the claimed conclusion (see Example 2.5). As for the analogous results for algebras of operators and $C^*$-algebras (see [34] and [35]), we improve them in a similar way by replacing equalities with appropriate inclusions.

- Compared to the results for algebras of operators and $C^*$-algebras in general (see [34] and [35]), we significantly reduce the set of starting assumptions upon which these results are based by dropping certain regularity conditions. Namely, if one is interested in the validity of (10), it is possible to omit the requirement that the product $abc$ is MP-invertible, since this follows directly from some of the assumptions (iv) or (v). In the case of rings, MP-invertibility of the product $abc$ can be replaced with the weaker condition of right $*$-cancellability of $abc$. See Theorems 2.3 and 2.6 and similarly Theorem 2.4.

- Also, it is possible to generalize the result by showing that $b^\dagger$ can be replaced by an arbitrary element $\tilde{b}$ as well as that $a^\dagger$ and $c^\dagger$ can be replaced with arbitrary $a^{(1, 2, 3)}$ and $c^{(1, 2, 4)}$, respectively (see Theorem 2.7). In this way, the assumption of MP-invertibility of the element $b$ is dropped and the MP-invertibility of the elements $a$ and $c$ is replaced with the existence of $a^{(1, 2, 3)}$ and $c^{(1, 2, 4)}$. This, although the last two are equivalent conditions in operator algebras and $C^*$-algebras, improves the results significantly in rings with involution since there the existence of a $\{1, 2, 3\}$-inverse of an element is equivalent with the existence of its $\{1, 3\}$-inverse and the latter is a much weaker condition than MP-invertibility (as witnessed by the ring $M_2(\mathbb{C})$ with taking transposes as the involution).
Recall that $\mathcal{R}$ denotes a ring with a unit $1 \neq 0$ and with an involution.

**Theorem 2.3.** Let $a, b, c \in \mathcal{R}$ be such that $a, c$ are MP-invertible. Let $p = a^\dagger abc^\dagger$ and $q = cc^\dagger b a^\dagger$, for $b \in \mathcal{R}$. Then, the following conditions are equivalent:

(i) $abc$ is Moore-Penrose invertible and $(abc)^\dagger = c^\dagger ba^\dagger$;

(iv) $q \in p\{1\}$, $a^* a p \supseteq q^* \mathcal{R}$ and $c c^* p^* \mathcal{R} \subseteq q \mathcal{R}$;

(v) $abc$ is right $\ast$-cancellable, $pq = (pq)^2$, $a^* a p \supseteq q^* \mathcal{R}$ and $c c^* p^* \mathcal{R} \subseteq q \mathcal{R}$;

(vi) $q \in p\{2\}$, $a^* a p \supseteq q^* \mathcal{R}$ and $c c^* p^* \mathcal{R} \subseteq q \mathcal{R}$.

**Proof.** Let $m = abc$ and $\tilde{m} = c^\dagger ba^\dagger$. Evidently, $pq$ is idempotent if and only if $m\tilde{m}$ is idempotent. Also, we have that the following equivalences hold:

$$a^* a p \supseteq q^* \mathcal{R} \iff m \mathcal{R} \supseteq (\tilde{m})^* \mathcal{R} \iff \mathcal{R} m^* \supseteq \mathcal{R} \tilde{m} \iff \tilde{m} \in \mathcal{R} m^*;$$

$$c c^* p^* \mathcal{R} \subseteq q^* \mathcal{R} \iff m^* \mathcal{R} \subseteq \mathcal{R} \tilde{m} \iff m^* \in \mathcal{R} \tilde{m};$$

(i) $\Rightarrow$ (v): If $m^\dagger = \tilde{m}$, then clearly $m\tilde{m}$ is idempotent. Also,

$$\tilde{m} = m^\dagger = m^\dagger m m^\dagger = m^\dagger (m^\dagger) m^* \in \mathcal{R} m^*, $$

$$m^* = (m m^\dagger m)^* = m^\dagger m m^* = \tilde{m} m m^*, \in \mathcal{R} \tilde{m}.$$  

(v) $\Rightarrow$ (i): If (v) holds, then there exist $u, v \in \mathcal{R}$ such that $\tilde{m} = um^*$ and $m^* = \tilde{m}v$. Now, multiplying $m\tilde{m} = (m\tilde{m})^2$ by $v$ from the right side, we get $m m^* = m\tilde{m} m m^*$ i.e. $(1 - m\tilde{m}) m m^* = 0$, which gives $(1 - m\tilde{m}) m = 0$ by right $\ast$-cancellability of $m$. So, $\tilde{m}$ is an inner inverse of $m$. Further, we have that

$$m = v^* (\tilde{m})^* = v^* (m\tilde{m})^* = m(\tilde{m})^*, $$

which implies that $m\tilde{m}$ is Hermitian and further

$$\tilde{m} = \tilde{m}(m\tilde{m})^* = \tilde{m} m \tilde{m}.$$  

Also,

$$m = v^* (\tilde{m})^* = v^* (m\tilde{m})^* = m(\tilde{m})^*,$$

which implies that $\tilde{m} m$ is Hermitian.

(iv), (vi) $\Rightarrow$ (v): This is evident.

(i) $\Rightarrow$ (iv): The property $q \in p\{1\}$ follows directly from the fact that $\tilde{m}$ is an inner inverse of $m$. The rest of the proof follows as in the part (i) $\Rightarrow$ (v).

(i) $\Rightarrow$ (vi): The property $q \in p\{2\}$ follows from the fact that $\tilde{m}$ is an outer inverse of $m$. The rest of the proof follows as in the part (i) $\Rightarrow$ (v). □

It is interesting to mention that if we take the reverse inclusion from (ii) of Theorem 2.3 (notice that in Hartwig’s result we have equality!) and replace in the statement of the theorem the assumption of right $\ast$-cancellability of $abc$ with the assumption of left $\ast$-cancellability of $c^\dagger ba^\dagger$, we get the following analogous result.
**Theorem 2.4.** Let \( a, b, c, \overline{b} \in \mathcal{R} \) be such that \( a, c \) are MP-invertible. Let \( p = a^\dagger abcc^\dagger \) and \( q = cc^\dagger ba^\dagger a \). Then, the following conditions are equivalent:

1. \( abc \) is Moore-Penrose invertible and \( (abc)^\dagger = c^\dagger ba^\dagger \);
2. \( q \in p\{1\} \), \( a^\ast apR \subseteq q^\ast R \) and \( cc^\ast p^\ast R \supseteq qR \);
3. \( c^\dagger ba^\dagger \) is left \( \ast \)-cancellable, \( pq = (pq)^2 \), \( a^\ast apR \subseteq q^\ast R \) and \( cc^\ast p^\ast R \supseteq qR \);
4. \( q \in p\{2\} \), \( a^\ast apR \subseteq q^\ast R \) and \( cc^\ast p^\ast R \supseteq qR \).

The following example illustrates the fact that the remaining two combinations of inclusions in the original result of Hartwig (Theorem 2.1 (v)) do not necessarily imply (10).

**Example 2.5.** Let

\[
A = \begin{bmatrix}
-3 & 2 & 2 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}, \quad B = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
1 & 0 & 0
\end{bmatrix}, \quad C = \frac{1}{3} \begin{bmatrix}
1 & 1 & 1 \\
1 & 1 & 1 \\
1 & 1 & 1
\end{bmatrix}.
\]

Then

\[
A^\dagger = \frac{1}{17} \begin{bmatrix}
-3 & 0 & 0 \\
2 & 0 & 0 \\
2 & 0 & 0
\end{bmatrix}, \quad B^\dagger = \begin{bmatrix}
0 & 0 & 1 \\
-1 & 1 & 1 \\
1 & 0 & -1
\end{bmatrix}, \quad C^\dagger = C.
\]

If we define \( P \) and \( Q \) as in Theorem 2.1, we get that \( PQ = 0 \) is idempotent and \( \mathcal{R}(A^\ast AP) \subseteq \mathcal{R}(Q^\ast) \) and \( \mathcal{R}(CC^\ast P^\ast) \subseteq \mathcal{R}(Q) \) but \( (ABC)^\dagger \neq C^\dagger B^\dagger A^\dagger \).

If matrices \( A, B, C \) are defined as \( C^\dagger, B^\dagger \) and \( A^\dagger \), respectively, as given above, we conclude that also the second pair of inclusions \( \mathcal{R}(Q^\ast) \subseteq \mathcal{R}(A^\ast AP) \) and \( \mathcal{R}(Q) \subseteq \mathcal{R}(CC^\ast P^\ast) \) together with the assumption that the matrix \( PQ \) is idempotent fails to imply (10).

On the other hand, the above mentioned pairs of inclusions imply (10) with some assumptions on \( p \) and \( q \).

**Theorem 2.6.** Let \( a, b, c \in \mathcal{R} \) be such that \( a, c \) are MP-invertible. Let \( p = a^\dagger abcc^\dagger \) and \( q = cc^\dagger ba^\dagger a, \overline{b} \in \mathcal{R} \). Then, the following conditions are equivalent:

1. \( abc \) is Moore-Penrose invertible and \( (abc)^\dagger = c^\dagger ba^\dagger \);
2. \( q \in p\{1\} \), \( a^\ast apR \supseteq q^\ast R \) and \( cc^\ast p^\ast R \supseteq qR \);
3. \( q \in p\{2\} \), \( a^\ast apR \subseteq q^\ast R \) and \( cc^\ast p^\ast R \subseteq qR \).

In addition to the previously mentioned results, we can show that MP-invertibility of the elements \( a \) and \( c \) can be replaced with the existence of \( a^{(1,2,3)} \) and \( c^{(1,2,4)} \).

**Theorem 2.7.** Let \( a, b, c, \overline{b} \in \mathcal{R} \) be such that there exist \( a^{(1,3)} \) and \( c^{(1,4)} \) and such that \( abc \) is right \( \ast \)-cancellable. Let \( a^{(1,2,3)}, c^{(1,2,4)} \) be given such that \( c^{(1,2,4)}ba^{(1,2,3)} \) is left \( \ast \)-cancellable and let \( p = a^{(1,2,3)}abcc^{(1,2,4)} \) and \( q = cc^{(1,2,4)}ba^{(1,2,3)}a \). Then, the following conditions are equivalent:
Theorem 2.9. Let $A, B, C$ be complex matrices such that $ABC$ is defined and let $P = A^\dagger ABCC^\dagger$, $Q = CC^\dagger B^\dagger A^\dagger A$. The following conditions are equivalent:

(i) $(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$;

(ii) $Q \in P\{1, 2\}$ and both of $A^*AP$ and $QPCC^*$ are Hermitian;

(iii) $Q \in P\{1, 2\}$ and both of $A^*AP$ and $QPCC^*$ are EP;

(iv) $Q \in P\{1, 2\}$ and both of $A^*AP$ and $QPCC^*$ are Hermitian;

(v) $p = (pq)^2$, $A^*apR \supseteq q^*R$ and $cc^*p^*R \subseteq qR$;

(vi) $pq = (pq)^2$, $A^*apR \subseteq q^*R$ and $cc^*p^*R \supseteq qR$.

Notice that, if in Theorem 2.7 we replace $a^{(1,2,3)}$ and $c^{(1,2,4)}$ with $a^{(1,3)}$ and $c^{(1,4)}$, respectively, the assertion of the theorem does not hold anymore, which will be shown in the next example:

Example 2.8. Let $B = C = \tilde{B} = I$ and take any matrix $A$ such that $A\{1, 3, 4\} \neq \{A^\dagger\}$ (such $A$ can be any projection different from the identity). If we take $A^{(1,3)} = A^{(1,3,4)} \neq A^\dagger$ we get that the conditions (ii) – (v) are all satisfied while (i) from Theorem 2.7 is not satisfied.

Finally, by the discussion above we end this section with the improved version of Hartwig’s original result for matrices.


2.1 Computer-assisted algebraic proofs

In the following, we discuss different aspects and use cases of the proof framework outlined in Section 1.1. We use Hartwig’s result and its improvements presented above to exemplify this. Algebraically, the central point of the proof is membership of the polynomial representing the claimed identity in the ideal generated by the polynomials representing the assumed identities, c.f. the third step listed in the introduction. Below, we also describe how certain assumptions, which are not identities of matrices or operators themselves, can sometimes still be used within the framework.

First, we focus on the implication \((v) \Rightarrow (i)\) in Theorem 2.1: if \(PQPQ = PQ\), \(\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)\), and \(\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)\), then \(M^\dagger = C^\dagger B^\dagger A^\dagger\).

Based on Douglas’ lemma, we first translate the range conditions to identities of operators. The four inclusions of ranges are equivalent to the following identities for some operators \(U_1, U_2, V_1, V_2\).

\[
A^*AP = Q^*V_1 \quad A^*APV_2 = Q^* \quad CC^*P^* = QU_1 \quad CC^*P^*U_2 = Q \quad (11)
\]

For each Moore-Penrose inverse \(A^\dagger, B^\dagger, C^\dagger, M^\dagger\), we have the four defining identities.

Translating these identities into polynomials, we introduce an indeterminate for each basic operator. Moreover, for each indeterminate, we introduce another indeterminate representing the adjoint of the corresponding operator. In total, this amounts to 22 indeterminates. Similarly, each identity of operators is translated into two polynomials, one for the identity itself and one for its adjoint. Thereby, we obtain a set \(F\) of 34 noncommutative polynomials with integer coefficients representing the assumptions. The claim corresponds to the polynomial \(f = m^\dagger - c^\dagger b^\dagger a^\dagger\).

Then, we use our software to show that \(f\) lies in the ideal generated by the polynomials of \(F\). The cofactor representation certifying this ideal membership was computed in less than 45 seconds and has 157 terms. The diagram induced by generic domains and codomains of operators has 4 vertices and one edge for each indeterminate. By construction, the polynomial \(f\) and the elements of \(F\) are compatible with domains and codomains. By Theorem A.1, this now rigorously proves that \(M^\dagger = C^\dagger B^\dagger A^\dagger\) holds under the conditions given in \((v)\). Note that this proof only relies on the defining identities of Moore-Penrose inverses and does not use any additional properties or lemmas. Consequently, the implication \((v) \Rightarrow (i)\) is in fact proven for any setting in which it can be formulated, since the polynomials in the cofactor representation obtained have only integer coefficients.

Using the software, it is easy to experiment with relaxing the assumptions and check if a cofactor representation of \(f\) in terms of a subset of \(F\) still can be found. For instance, it turns out that the first and last identity in (11) can be dropped. This corresponds to relaxing the range conditions in \((v)\) to \(\mathcal{R}(A^*AP) \supseteq \mathcal{R}(Q^*)\) and \(\mathcal{R}(CC^*P^*) \subseteq \mathcal{R}(Q)\). Additionally, we could also observe that the cofactor representation of \(f\) contains no polynomial associated to any of the four defining equations of \(B^\dagger\). This shows that \(B^\dagger\) can in fact be replaced by an arbitrary operator \(\tilde{B}\) that does not have to be related to \(B\) in any way.

It is also possible to prove the implication \((i) \Rightarrow (v)\) using our framework and software. To this end, first explicit expressions for \(U_1, U_2, V_1, V_2\) in terms of the other basic operators have to be found. By inspecting the proof of Theorem 2.3 one can see that these can be
chosen as
\[
U_1 = BCC^* B^* A^*(A^\dagger)^*, \quad U_2 = (B^\dagger)^*(C^\dagger)^* C^\dagger B^\dagger A^\dagger A, \\
V_1 = B^* A^* A BCC^\dagger, \quad V_2 = B^\dagger A^\dagger (A^\dagger)^* (B^\dagger)^* (C^\dagger)^* C^*.
\] (12)

Then, using the defining equations of \(A^\dagger, B^\dagger, C^\dagger, M^\dagger\), the identity \(M^\dagger = C^\dagger B^\dagger A^\dagger\) and their adjoint statements as assumptions, the software finds cofactor representations of the polynomial corresponding to \(PQ PQ\) as well as of the polynomials associated to the four identities in (11), where \(U_1, U_2, V_1, V_2\) have been replaced by the expressions in (12). We note that these cofactor representations only contain polynomials with integer coefficients. Hence, based on Theorem A.1, this proves the implication \((i) \Rightarrow (v)\) for any setting in which it can be formulated.

It is also possible to incorporate properties of operators into this framework that cannot be expressed in terms of identities but only in form of quasi-identities. In general, quasi-identities are implications where a conjunction of identities implies another identity. One example of such a property is \(*\)-cancellability. To use these properties to prove a claimed identity, first a suitable polynomial in the ideal representing the assumptions has to be found that corresponds to an operator identity to which such a property is applicable. Finding such a suitable polynomial is usually a non-trivial task and often has to be done by hand. For the automated proofs of some of the results presented here, for example, we obtained the required expressions by inspecting the corresponding hand proofs, which were done partly before the automated proofs. Once such a polynomial has been found, the corresponding quasi-identity can be applied to obtain a new polynomial that corresponds to a shorter identity and that is typically not contained in the ideal that is generated by the polynomials representing the assumptions. By including this new polynomial into the set of polynomials representing the assumptions, we can enlarge the ideal of all consequences of the assumptions and proceed to prove the ideal membership of the polynomial corresponding to the claimed identity in this larger ideal.

To prove a quasi-identity, the left-hand side of the implication has to be included in the assumptions and the right-hand side becomes the claimed identity. When translating these operator identities into polynomials it is important to introduce new indeterminates that do not satisfy any additional identities for all universally quantified operators in the quasi-identity. Then, to prove the quasi-identity, it only remains to prove the ideal membership of the polynomial associated to the claim in the ideal generated by the polynomials representing the assumptions.

Based on the discussion and the observations made above, it is no surprise that the software can also be used to prove all the improved results of Hartwig’s triple reverse order law presented in this work. In the following, we explain how this can be done using the equivalence \((i) \Leftrightarrow (v)\) of Theorem 2.3.

For the implication \((v) \Rightarrow (i)\), we translate the assumptions \(pq = (pq)^2, a^*apR \supseteq q^*R, cc^*p^*R \subseteq q^*R\) and their adjoint statements into polynomials. Note that in order to translate the set inclusions we can use factorizations analogous to (11). In contrast to the original statement of Hartwig, where the MP-invertibility of \(ABC\) is already given, we now have to prove that \(m = abc\) is MP-invertible and that \(m^\dagger = c^\dagger b^\dagger a^\dagger\). Hence, the claim is that \(\tilde{m} = c^\dagger b^\dagger a^\dagger\) satisfies the four defining equations of \(m^\dagger\). However, trying to show the ideal membership of the corresponding polynomials in the ideal generated by the polynomials representing the assumptions fails. This is because these polynomials do not contain any
information about the right ∗-cancellability of m. To use this property, we have to find a polynomial in the ideal generated by the polynomials associated to our assumptions that corresponds to an identity to which this property is applicable. In the hand proof of this implication, the right ∗-cancellability is applied to \((1 - \tilde{m}m)m^* = 0\). Using the software, we can show that the polynomial corresponding to this identity is indeed contained in the ideal generated by the polynomials representing the assumptions. Hence, as in the hand proof, we can apply the right ∗-cancellability of m to \((1 - \tilde{m}m)m^* = 0\) to obtain \((1 - \tilde{m}m)m = 0\). After including the polynomial associated to this new identity in the set of translated assumptions, the software manages to verify the ideal membership of all polynomials corresponding to the claimed identities fully automatically, and thereby, proves the claimed statement.

The proof of \((i) \Rightarrow (v)\) of Theorem 2.3 using the software essentially proceeds along the same lines as the proof discussed above concerning the same implication in Hartwig’s theorem. The only difference is that now also the right ∗-cancellability of m has to be shown. To this end, we include the identity \(zmm^* = 0\) in the assumptions and prove \(zm = 0\) with an arbitrary ring element z. When translating these identities into polynomials, z has to be replaced by a new indeterminate that does not satisfy any additional identities. The software then proves the ideal membership of the polynomial associated to the claimed identity in the ideal generated by the polynomials representing the assumptions fully automatically.

**Remark 2.10.** We note that in a similar fashion to the implications discussed above, also all other implications of Theorem 2.3 and all other results presented in this work, including Theorems 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, and 2.9, can be proven using the framework. The relevant computations with noncommutative polynomials were done using OperatorGB and are available at [http://gregensburger.com/softw/OperatorGB](http://gregensburger.com/softw/OperatorGB) along with a file containing all the certificates of ideal membership. Since all cofactor representations obtained have only polynomials with integer coefficients, by applying Theorem A.1, the corresponding theorems hold for any setting in which they can be formulated like rings with involution, (rectangular) matrices over such rings, and linear bounded operators between Hilbert spaces.

**Acknowledgements**

We thank Anja Korporal, Marko Petković, and Milan Tasić for discussions related to this paper in the course of the OeAD project SRB 05/2016. This work was supported by the Ministry of Science, Technology and Development, Republic of Serbia, and by the Austrian Science Fund (FWF): P 27229, P 31952, and P 32301.

**References**

[1] Roger Penrose, *A generalized inverse for matrices*, Proc. Cambridge Philos. Soc. 51, pp. 406–413, 1955.

[2] M. Laura Arias and M. Celeste Gonzalez, *Positive solutions to operator equations* \(AXB = C\), Linear Algebra Appl. 433, pp. 1194–1202, 2010.
[3] Clemens Hofstadler, Clemens G. Raab, and Georg Regensburger, *Certifying operator identities via noncommutative Gröbner bases*, ACM Commun. Comput. Algebra 53, pp. 49–52, 2019.

[4] Clemens G. Raab, Georg Regensburger, and Jamal Hossein Poor, *Formal proofs of operator identities by a single formal computation*, J. Pure Appl. Algebra, 2020. To appear. arXiv:1910.06165

[5] Clemens Hofstadler, *Certifying operator identities and ideal membership of noncommutative polynomials*, Master’s Thesis, Johannes Kepler University Linz, Austria, 2020.

[6] K. P. S. Bhaskara Rao, *The theory of generalized inverses over commutative rings*, Taylor and Francis, London, 2002.

[7] Jerry J. Koliha and Pedro Patricio, *Elements of rings with equal spectral idempotents*, J. Aust. Math. Soc. 72, pp. 137–152, 2002.

[8] Teo Mora, *An introduction to commutative and noncommutative Gröbner bases*, Theoret. Comput. Sci. 134, pp. 131–173, 1994.

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

[10] J. William Helton, Mark Stankus, and John J. Wavrik, *Computer simplification of formulas in linear systems theory*, IEEE Trans. Automat. Control 43, pp. 302–314, 1998.

[11] Leonard Schmitz and Viktor Levandovskyy, *Formally verifying proofs for algebraic identities of matrices*, in Intelligent Computer Mathematics, CICM 2020, LNCS vol. 12236, pp. 222–236, Springer, Cham, 2020.

[12] Hans J. Werner, *When is $B^{-A}$ a generalized inverse of $AB$?*, Linear Algebra Appl. 210, pp. 255–263, 1994.

[13] Thomas N. E. Greville, *Note on the generalized inverse of a matrix product*, SIAM Rev. 8, pp. 518–521, 1966.

[14] Adi Ben-Israel and Thomas N. E. Greville, *Generalized inverses: theory and applications*, 2nd Edition, Springer, New York, 2003.

[15] Dragana S. Cvetković-Ilić and Yimin Wei, *Algebraic properties of generalized inverses*, Springer, Singapore, 2017.

[16] Yongge Tian, *Reverse order laws for the weighted Moore-Penrose inverse of a triple matrix product with applications*, Int. Math. J. 3, pp. 107–117, 2003.

[17] Wenyu Sun and Yimin Wei, *Triple reverse-order law for weighted generalized inverses*, Appl. Math. Comput. 125, pp. 221–229, 2002.

[18] Dragana S. Cvetković-Ilić, *New conditions for the reverse order laws for $\{1,3\}$ and $\{1,4\}$-generalized inverses*, Electron. J. Linear Algebra 23, pp. 231–242, 2012.
[19] Xiaoji Liu, Shuxia Wu, and Dragana S. Cvetković-Ilić, *New results on reverse order law for \{1, 2, 3\}- and \{1, 2, 4\}-inverses of bounded operators*, Math. Comp. 82, pp. 1597–1607, 2013.

[20] Dragana S. Cvetković-Ilić and Jovana Nikolov, *Reverse order laws for \{1, 2, 3\}-generalized inverses*, Appl. Math. Comput. 234, pp. 114–117, 2014.

[21] Vladimir Pavlović and Dragana S. Cvetković-Ilić, *Applications of completions of operator matrices to reverse order law for \{1\}-inverses of operators on Hilbert spaces*, Linear Algebra Appl. 484, pp. 219–236, 2015.

[22] Dragana S. Cvetković-Ilić, *Reverse order laws for \{1, 3, 4\}-generalized inverses in C*-algebras*, Appl. Math. Lett. 24, pp. 210–213, 2011.

[23] Dragana S. Cvetković-Ilić and Vladimir Pavlović, *A comment on some recent results concerning the reverse order law for \{1, 3, 4\}-inverses*, Appl. Math. Comput. 217, pp. 105–109, 2010.

[24] Alvaro R. De Pierro and Musheng Wei, *Reverse order laws for reflexive generalized inverse of products of matrices*, Linear Algebra Appl. 277, pp. 299–311, 1998.

[25] Saichi Izumino, *The product of operators with closed range and an extension of the reverse order law*, Tohoku Math. J. (2) 34, pp. 43–52, 1982.

[26] Deqiang Liu and Hu Yang, *Further results on the reverse order law for \{1, 3\}-inverse and \{1, 4\}-inverse of a matrix product*, J. Inequal. Appl., Article ID 312767, 13 pages, 2010.

[27] Deqiang Liu and Hu Yang, *The reverse order law for \{1, 3, 4\}-inverse of the product of two matrices*, Appl. Math. Comput. 215, pp. 4293–4303, 2010.

[28] Xiaoji Liu, Julio Benítez, and Jin Zhong, *Some results on partial ordering and reverse order law of elements of C*-algebras*, J. Math. Anal. Appl. 370, pp. 295–301, 2010.

[29] Jovana N. Radenković, *Reverse order laws for generalized inverses of multiple operator products*, Linear Multilinear Algebra 64, pp. 1266–1282, 2016.

[30] Nobuo Shinozaki and Masaaki Sibuya, *Further results on the reverse order law*, Linear Algebra Appl. 27, pp. 9–16, 1979.

[31] Yoshio Takane, Yongge Tian, and Haruo Yanai, *On reverse-order laws for least-squares g-inverses and minimum norm g-inverses of a matrix product*, Aequationes Math. 73, pp. 56–70, 2007.

[32] Guorong Wang and Bing Zheng, *The reverse order law for the generalized inverse A_{TS}^{(2)}*, Appl. Math. Comput. 157, pp. 295–305, 2004.

[33] Robert E. Hartwig, *The reverse order law revisited*, Linear Algebra Appl. 76, pp. 241–246, 1986.
A Formal summary of algebraic proof framework

Now, we give a more formal explanation of the framework developed in [4]. In the following, we fix a set $X$ and a commutative ring $R$ with unit element. We consider the ring $R\langle X \rangle$ of noncommutative polynomials with coefficients in $R$ and indeterminates in $X$, where indeterminates do not commute with each other but with coefficients.

Recall that a quiver is given by a tuple $(V, E, s, t)$ where $V$ is the set of vertices, $E$ is the set of edges, and $s, t : E \to V$ give the source $s(e)$ and target $t(e)$ of each edge $e \in E$. We consider labelled quivers where edges have labels in $X$, i.e. with a function $l : E \to X$ giving the labels of edges. In the following, we fix a labelled quiver $Q = (V, E, X, s, t, l)$ such that edges have unique labels, i.e. $l$ is injective. Based on the labels of edges, it is straightforward to label paths in $Q$ so that multiplication of labels as monomials corresponds to concatenation of paths. Likewise, the notion of source and target of edges can be naturally extended to paths.

A polynomial in $R\langle X \rangle$ such that all its monomials are labels of paths in $Q$ that have the same source and the same target is called compatible with $Q$. For vertices $v, w \in V$, we collect all compatible polynomials arising from paths with source $v$ and target $w$ in the set $R\langle X \rangle_{v,w}$, which is an $R$-module. Note that for the case $v = w$ there exists an empty path from $v$ to $w$, which has the constant monomial 1 as its label. By construction, the polynomials $f_1, \ldots, f_8, f$ defined in Section 1.1 are compatible with the following labelled quiver.

![Labelled quiver for Werner’s theorem](image)

Figure 1: Labelled quiver for Werner’s theorem

A representation of a quiver $(V, E, s, t)$ can be specified by a pair $(\mathcal{M}, \varphi)$ such that $\mathcal{M} = (\mathcal{M}_v)_{v \in V}$ is a family of $R$-modules and the map $\varphi$ assigns to each $e \in E$ an $R$-linear map $\varphi(e) : \mathcal{M}_{s(e)} \to \mathcal{M}_{t(e)}$. For example, with $R = \mathbb{Z}$ or $R = \mathbb{C}$, the two diagrams in Section 1.1 specify representations of the labelled quiver shown in Figure 1.

Now, for a given representation $(\mathcal{M}, \varphi)$ of $Q$, plugging in the $R$-linear maps $\varphi(e), e \in E$, for the indeterminates $l(e)$ of polynomials in $R\langle X \rangle$ can be formalized as follows. For every nonconstant monomial $m \in R\langle X \rangle_{v,w}$, there exists a nonempty path $e_n \ldots e_1$ in $Q$
with source $v$, target $w$, and label $m$, which allows to define the $R$-linear map $\varphi_{v,w}(m) := \varphi(e_n)\cdots\varphi(e_1)$ from $\mathcal{M}_v$ to $\mathcal{M}_w$. Note that, by definition of $\varphi$, the composition of the maps $\varphi(e_i)$ exists. Similarly, if $v = w$, we define $\varphi_{v,v}(1) := \text{id}_{\mathcal{M}_v}$. The map $\varphi_{v,w}$ extends $R$-linearly to all $f \in R\langle X \rangle_{v,w}$ and we call the $R$-linear map $\varphi_{v,w}(f)$ a realization of $f$ w.r.t. the representation $(\mathcal{M}, \varphi)$ of $Q$.

Altogether, one can prove the following main theorem about the framework. The formulation stated here is a consequence of Theorem 32 and 15 in [4].

**Theorem A.1.** Let $R$ be a commutative ring with unit element, let $F \subseteq R\langle X \rangle$ be a set of polynomials without a constant term, and let $f \in (F)$. Then, for all labelled quivers $Q$ with unique labels in $X$ such that $f$ and all polynomials in $F$ are compatible with $Q$ and for all representations $(\mathcal{M}, \varphi)$ of $Q$ such that the realizations of the polynomials in $F$ w.r.t. $(\mathcal{M}, \varphi)$ are zero, we have that also the realization of $f$ w.r.t. $(\mathcal{M}, \varphi)$ is zero.

All notions and results of this section naturally generalize to $R$-linear categories by considering objects and morphisms in such a category instead of $R$-modules and $R$-linear maps, respectively. For more details, see Section 5.2 in [4]. Based on a refined version of the framework using rewriting, it is possible to obtain a similar theorem where polynomials in $F$ are allowed to have a constant term, see Theorem 32 in [36].

Altogether, based on the theorem above, we obtain a rigorous proof of the following statement for matrices discussed in Section 1.1.

**Lemma A.2.** Let $A, B$ be matrices with entries in a commutative ring $R$ with unit element and let $A^{-}, B^{-}$ be inner inverses of $A$ resp. $B$. If $BB^{-}(I - A^{-}A) = I - A^{-}A$ holds, then $B^{-}A^{-}$ is an inner inverse of $AB$.

**Proof.** In the polynomial ring $R(a, a^{-}, b, b^{-}, i)$, the cofactor representation (8) shows that the polynomial $f$ given by (6) lies in the ideal $(F) \subseteq R\langle a, a^{-}, b, b^{-}, i \rangle$, where $F := \{f_1, \ldots, f_8\}$. The generators of the ideal as well as the polynomial $f$ are compatible with the labelled quiver shown in Figure 1. We fix the following representation of this quiver.

$$
\begin{array}{c}
R^m \\ A^{-} \\
R^n \\
A
\end{array} \quad \bigcap \quad 
\begin{array}{c}
B^{-} \\
R^k \\
B
\end{array}
$$

If $BB^{-}(I - A^{-}A) = I - A^{-}A$, then the realizations of all elements of $F$ are zero by assumption. Then, the realization of $f$ is zero by Theorem A.1, i.e.

$$ABB^{-}A^{-}AB - AB = 0.
$$

Note that the proof of this lemma relies on the purely algebraic fact that the polynomial $f$ representing the claim lies in the ideal $(F)$ representing the assumptions. By changing the representation of the quiver, Theorem A.1 gives rigorous proofs also of analogous lemmas for bounded linear operators between Hilbert spaces, for homomorphisms of $R$-modules, and for ring elements.