Algebraic Automated Theorem Proving

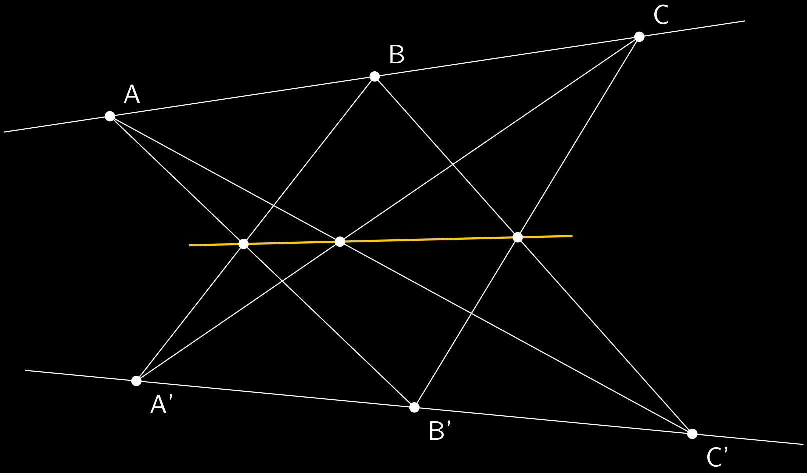
Clemens Hofstadler
Institute for Symbolic Artificial Intelligence, JKU Linz, Austria

Effective Algebra Days, Limoges, 7 November 2025

based on joint work with P. Krug, C.G. Raab, G. Regensburger, and T. Verron

JKU
JOHANNES KEPLER
UNIVERSITY LINZ

FWF
Der Wissenschaftsfonds.


C
B
A
A'
B'
C'

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

HANDBOOK OF LINEAR ALGEBRA

SECOND EDITION

$$\begin{bmatrix} 2 & 2 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 6 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$

Edited by

Leslie Hogben

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

5.7 Pseudo-Inverse

Definitions:

A **Moore–Penrose pseudo-inverse** of a matrix $A \in \mathbb{C}^{m\times n}$ is a matrix $A^\dagger \in \mathbb{C}^{n\times m}$ that satisfies the following four **Penrose** conditions:

$$AA^\dagger A = A; \quad A^\dagger AA^\dagger = A^\dagger; \quad (AA^\dagger)^* = AA^\dagger; \quad (A^\dagger A)^* = A^\dagger A.$$

Facts:

All the following facts except those with a specific reference can be found in [Gra83, pp. 105–141] or [RM71, pp. 44–67].

1. Every $A \in \mathbb{C}^{m\times n}$ has a unique pseudo-inverse $A^\dagger$.
2. If $A \in \mathbb{R}^{m\times n}$, then $A^\dagger$ is real.
3. If $A \in \mathbb{C}^{m\times n}$ of rank r has a full rank decomposition $A = BC$, where $B \in \mathbb{C}^{m\times r}$ and $C \in \mathbb{C}^{r\times n}$, then $A^\dagger$ can be evaluated using $A^\dagger = C^*(B^*AC^*)^{-1}B^*$.
4. [LH95, p. 38] If $A \in \mathbb{C}^{m\times n}$ of rank $r \le \min\{m,n\}$ has an SVD $A = U\Sigma V^*$, then its pseudo-inverse is $A^\dagger = V\Sigma^\dagger U^*$, where

$$\Sigma^\dagger = \mathrm{diag}(1/\sigma_1, \dots, 1/\sigma_r, 0, \dots, 0) \in \mathbb{R}^{n\times m}.$$

5. [Hig96, p. 412] The pseudo-inverse $A^\dagger$ of $A \in F^{m\times n}$ ($F = \mathbb{C}$ or $\mathbb{R}$) solves the minimization problem

$$\min_{X\in F^{n\times m}} \|AX - I_m\|_F^2.$$

6. $\mathbf{0}_{mn}^\dagger = \mathbf{0}_{nm}$ and $J_{mn}^\dagger = \frac{1}{mn}J_{nm}$, where $\mathbf{0}_{mn} \in \mathbb{C}^{m\times n}$ is the all 0s matrix and $J_{mn} \in \mathbb{C}^{m\times n}$ is the all 1s matrix.
7. If $\mathbf{x} \ne \mathbf{0}$, $\mathbf{y} \ne \mathbf{0}$, then $(\mathbf{x}\mathbf{y}^*)^\dagger = \dfrac{\mathbf{y}\mathbf{x}^*}{\|\mathbf{x}\|^2\|\mathbf{y}\|^2}$.
8. If $\mathbf{x} \ne \mathbf{0}$, then $\mathbf{x}^\dagger = \dfrac{\mathbf{x}^*}{\|\mathbf{x}\|^2}$.
9. Let α be a scalar. Denote

$$\alpha^\dagger = \begin{cases} \alpha^{-1}, & \text{if } \alpha \ne 0, \\ 0, & \text{if } \alpha = 0. \end{cases}$$

Then

(a) $(\alpha A)^\dagger = \alpha^\dagger A^\dagger$.

(b) $(\mathrm{diag}(\beta_1, \beta_2, \cdots, \beta_n))^\dagger = \mathrm{diag}(\beta_1^\dagger, \beta_2^\dagger, \cdots, \beta_n^\dagger)$.

10. $(A^\dagger)^* = (A^*)^\dagger; \quad (A^\dagger)^\dagger = A$.
11. If A is a nonsingular square matrix, then $A^\dagger = A^{-1}$.
12. If U has orthonormal columns or orthonormal rows, then $U^\dagger = U^*$.
13. If $A = A^*$ and $A = A^2$, then $A^\dagger = A$.
14. $A^\dagger = A^*$ if and only if A^*A is idempotent.
15. If A is normal and k is a positive integer, then $AA^\dagger = A^\dagger A$ and $(A^k)^\dagger = (A^\dagger)^k$.
16. If $U \in \mathbb{C}^{m\times n}$ is of rank n and satisfies $U^\dagger = U^*$, then U has orthonormal columns.
17. If $U \in \mathbb{C}^{m\times m}$ and $V \in \mathbb{C}^{n\times n}$ are unitary matrices, then $(UAV)^\dagger = V^*A^\dagger U^*$.
18. $A^\dagger = (A^*A)^\dagger A^* = A^*(AA^*)^\dagger$. In particular,

(a) if $A \in \mathbb{C}^{m\times n}$ $(m \ge n)$ has full rank n, then $A^\dagger = (A^*A)^{-1}A^*$;

(b) if $A \in \mathbb{C}^{m\times n}$ $(m \le n)$ has full rank m, then $A^\dagger = A^*(AA^*)^{-1}$.

19. Let $A \in \mathbb{C}^{m\times n}$. Then

(a) $A^\dagger A$, $AA^\dagger$, $I_n - A^\dagger A$, and $I_m - AA^\dagger$ are orthogonal projections.

(b) $\mathrm{rank}(A) = \mathrm{rank}(A^\dagger) = \mathrm{rank}(AA^\dagger) = \mathrm{rank}(A^\dagger A)$.

(c) $\mathrm{rank}(I_n - A^\dagger A) = n - \mathrm{rank}(A)$.

(d) $\mathrm{rank}(I_m - AA^\dagger) = m - \mathrm{rank}(A)$.

20. $AA^\dagger = \mathrm{Proj}_{\mathrm{range}(A)}$; $A^\dagger A = \mathrm{Proj}_{\mathrm{range}(A^\dagger)}$.
21. Suppose that $A \in F^{m\times n}$, where $F = \mathbb{C}$ or $\mathbb{R}$. Then

(a) $\mathrm{range}(A) = \mathrm{range}(AA^*) = \mathrm{range}(AA^\dagger)$.

(b) $\mathrm{range}(A^\dagger) = \mathrm{range}(\mathrm{A}^*) = \mathrm{range}(A^*A) = \mathrm{range}(A^\dagger A)$.

(c) $\ker(A) = \ker(\mathrm{A}^*\mathrm{A}) = \ker(A^\dagger A)$.

(d) $\ker(A^\dagger) = \ker(\mathrm{A}^*) = \ker(AA^*) = \ker(AA^\dagger)$.

(e) $\mathrm{range}(A^\dagger A) \oplus \ker(A^\dagger A) = F^n$.

(f) $\mathrm{range}(AA^\dagger) \oplus \ker(AA^\dagger) = F^m$.

22. If $A = A_1 + A_2 + \cdots + A_k$, $A_i^*A_j = 0$, and $A_iA_j^* = 0$, for all $i, j = 1, \cdots, k$, $i \ne j$, then $A^\dagger = A_1^\dagger + A_2^\dagger + \cdots + A_k^\dagger$.
23. If A is an $m\times r$ matrix of rank r and B is an $r\times n$ matrix of rank r, then $(AB)^\dagger = B^\dagger A^\dagger$.
24. $(A^*A)^\dagger = A^\dagger(A^*)^\dagger$; $(AA^*)^\dagger = (A^*)^\dagger A^\dagger$.
25. [Gre66] Each one of the following conditions is necessary and sufficient for $(AB)^\dagger = B^\dagger A^\dagger$:

(a) $\mathrm{range}(BB^*A^*) \subseteq \mathrm{range}(A^*)$ and $\mathrm{range}(A^*AB) \subseteq \mathrm{range}(B)$.

(b) $A^\dagger ABB^*$ and $A^*ABB^\dagger$ are both Hermitian matrices.

(c) $A^\dagger ABB^*A^* = BB^*A^*$ and $BB^\dagger A^*AB = A^*AB$.

(d) $A^\dagger ABB^*A^*ABB^\dagger = BB^*A^*A$.

(e) $A^\dagger AB = B(AB)^\dagger AB$ and $BB^\dagger A^* = A^*AB(AB)^\dagger$.

26. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$, where $\otimes$ denotes the Kronecker product.
27. $A^\dagger = \lim_{\alpha\to 0} A^*(\alpha I + AA^*)^{-1} = \lim_{\alpha\to 0}(\alpha I + A^*A)^{-1}A^*$.
28. $A^\dagger = \sum_{j=1}^{\infty} A^*(I + AA^*)^{-j} = \sum_{j=1}^{\infty}(I + A^*A)^{-j}A^*$.
29. (Continuity of pseudo-inverse) Suppose that $A \in F^{m\times n}$ and $E \in F^{m\times n}$, where $F = \mathbb{C}$ or $\mathbb{R}$. Then $\lim_{E\to 0}(A + E)^\dagger = A^\dagger$ if and only if there is $\epsilon > 0$ such that $\mathrm{rank}(A+E) = \mathrm{rank(A)}$ when $\|E\|_2 \le \epsilon$.
30. Let $A \in \mathbb{C}^{m\times n}$ be of rank r where $0 < r < \min\{m,n\}$. Suppose that A can be partitioned as

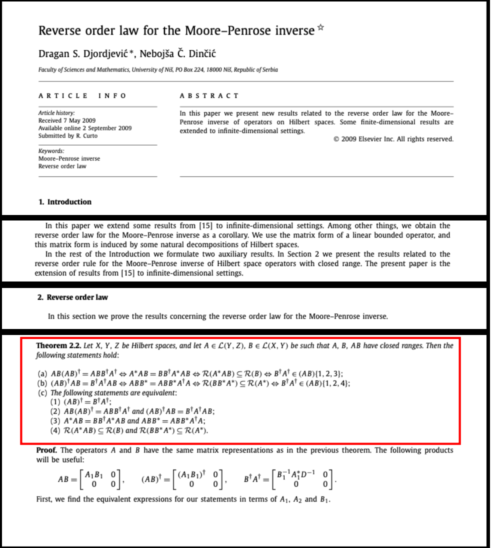
$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

where $A_{11} \in \mathbb{C}^{r\times r}$ and $\mathrm{rank}(A_{11}) = r$. Then

$$A^\dagger = \begin{bmatrix} A_{11}^*XA_{11}^* & A_{11}^*XA_{21}^* \\ A_{12}^*XA_{11}^* & A_{12}^*XA_{21}^* \end{bmatrix},$$

where

$$X = (A_{11}A_{11}^* + A_{12}A_{12}^*)^{-1}A_{11}(A_{11}^*A_{11} + A_{21}^*A_{21})^{-1}.$$



Reverse order law for the Moore–Penrose inverse ☆

Dragan S. Djordjević *, Nebojša Č. Dinčić

Faculty of Sciences and Mathematics, University of Niš, PO Box 224, 18000 Niš, Republic of Serbia

ARTICLE INFO

Article history:
Received 7 May 2009
Available online 2 September 2009
Submitted by R. Curto

Keywords:
Moore–Penrose inverse
Reverse order law

ABSTRACT

In this paper we present new results related to the reverse order law for the Moore–Penrose inverse of operators on Hilbert spaces. Some finite-dimensional results are extended to infinite-dimensional settings.

1. Introduction

In this paper we extend some results from [15] to infinite-dimensional settings. Among other things, we obtain the reverse order law for the Moore–Penrose inverse as a corollary. We use the matrix form of a linear bounded operator, and this matrix form is induced by some natural decompositions of Hilbert spaces.

In the rest of the Introduction we formulate two auxiliary results. In Section 2 we present the results related to the reverse order rule for the Moore–Penrose inverse of Hilbert space operators with closed range. The present paper is the extension of results from [15] to infinite-dimensional settings.

2. Reverse order law

In this section we prove the results concerning the reverse order law for the Moore–Penrose inverse.

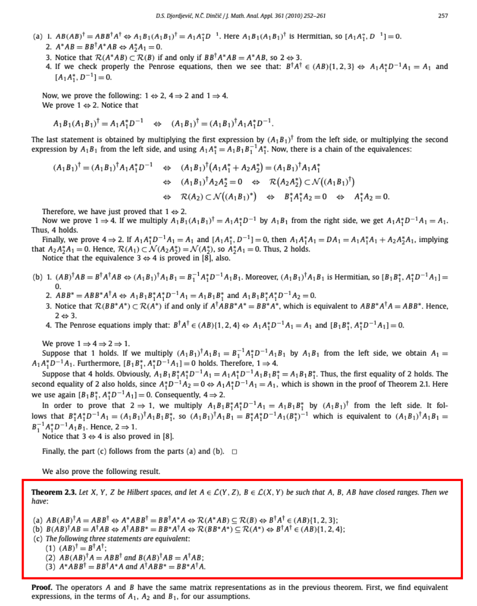
Theorem 2.2. *Let X, Y, Z be Hilbert spaces, and let $A \in \mathcal{L}(Y, Z)$, $B \in \mathcal{L}(X, Y)$ be such that A, B, AB have closed ranges. Then the following statements hold:*

(a) $AB(AB)^\dagger = ABB^\dagger A^\dagger \Leftrightarrow A^*AB = BB^\dagger A^*AB \Leftrightarrow \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,3\}$;
(b) $(AB)^\dagger AB = B^\dagger A^\dagger AB \Leftrightarrow ABB^* = ABB^*A^\dagger A \Leftrightarrow \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,4\}$;
(c) *The following statements are equivalent:*
  (1) $(AB)^\dagger = B^\dagger A^\dagger$;
  (2) $AB(AB)^\dagger = ABB^\dagger A^\dagger$ *and* $(AB)^\dagger AB = B^\dagger A^\dagger AB$;
  (3) $A^*AB = BB^\dagger A^*AB$ *and* $ABB^* = ABB^*A^\dagger A$;
  (4) $\mathcal{R}(A^*AB) \subseteq \mathcal{R}(B)$ *and* $\mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*)$.

Proof. The operators A and B have the same matrix representations as in the previous theorem. The following products will be useful:

$$AB = \begin{bmatrix} A_1B_1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad (AB)^\dagger = \begin{bmatrix} (A_1B_1)^\dagger & 0 \\ 0 & 0 \end{bmatrix}, \qquad B^\dagger A^\dagger = \begin{bmatrix} B_1^{-1}A_1^*D^{-1} & 0 \\ 0 & 0 \end{bmatrix}.$$

First, we find the equivalent expressions for our statements in terms of A_1, A_2 and B_1.



(a) 1. $AB(AB)^\dagger = ABB^\dagger A^\dagger \Leftrightarrow A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{\;1}$. Here $A_1B_1(A_1B_1)^\dagger$ is Hermitian, so $[A_1A_1^*, D^{\;1}] = 0$.
2. $A^*AB = BB^\dagger A^*AB \Leftrightarrow A_2^*A_1 = 0$.
3. Notice that $\mathcal{R}(A^*AB) \subset \mathcal{R}(B)$ if and only if $BB^\dagger A^*AB = A^*AB$, so $2 \Leftrightarrow 3$.
4. If we check properly the Penrose equations, then we see that: $B^\dagger A^\dagger \in (AB)\{1,2,3\} \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$ and $[A_1A_1^*, D^{-1}] = 0$.

Now, we prove the following: $1 \Leftrightarrow 2$, $4 \Rightarrow 2$ and $1 \Rightarrow 4$.
We prove $1 \Leftrightarrow 2$. Notice that

$$A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{-1} \quad \Leftrightarrow \quad (A_1B_1)^\dagger = (A_1B_1)^\dagger A_1A_1^*D^{-1}.$$

The last statement is obtained by multiplying the first expression by $(A_1B_1)^\dagger$ from the left side, or multiplying the second expression by A_1B_1 from the left side, and using $A_1A_1^* = A_1B_1B_1^{-1}A_1^*$. Now, there is a chain of the equivalences:

$$\begin{aligned} (A_1B_1)^\dagger = (A_1B_1)^\dagger A_1A_1^*D^{-1} \quad &\Leftrightarrow \quad (A_1B_1)^\dagger\big(A_1A_1^* + A_2A_2^*\big) = (A_1B_1)^\dagger A_1A_1^* \\ &\Leftrightarrow \quad (A_1B_1)^\dagger A_2A_2^* = 0 \quad \Leftrightarrow \quad \mathcal{R}\big(A_2A_2^*\big) \subset \mathcal{N}\big((A_1B_1)^\dagger\big) \\ &\Leftrightarrow \quad \mathcal{R}(A_2) \subset \mathcal{N}\big((A_1B_1)^*\big) \quad \Leftrightarrow \quad B_1^*A_1^*A_2 = 0 \quad \Leftrightarrow \quad A_1^*A_2 = 0. \end{aligned}$$

Therefore, we have just proved that $1 \Leftrightarrow 2$.

Now we prove $1 \Rightarrow 4$. If we multiply $A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{-1}$ by A_1B_1 from the right side, we get $A_1A_1^*D^{-1}A_1 = A_1$. Thus, 4 holds.

Finally, we prove $4 \Rightarrow 2$. If $A_1A_1^*D^{-1}A_1 = A_1$ and $[A_1A_1^*, D^{-1}] = 0$, then $A_1A_1^*A_1 = DA_1 = A_1A_1^*A_1 + A_2A_2^*A_1$, implying that $A_2A_2^*A_1 = 0$. Hence, $\mathcal{R}(A_1) \subset \mathcal{N}(A_2A_2^*) = \mathcal{N}(A_2^*)$, so $A_2^*A_1 = 0$. Thus, 2 holds.

Notice that the equivalence $3 \Leftrightarrow 4$ is proved in [8], also.

(b) 1. $(AB)^\dagger AB = B^\dagger A^\dagger AB \Leftrightarrow (A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$. Moreover, $(A_1B_1)^\dagger A_1B_1$ is Hermitian, so $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$.
2. $ABB^* = ABB^*A^\dagger A \Leftrightarrow A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1B_1B_1^*$ and $A_1B_1B_1^*A_1^*D^{-1}A_2 = 0$.
3. Notice that $\mathcal{R}(BB^*A^*) \subset \mathcal{R}(A^*)$ if and only if $A^\dagger ABB^*A^* = BB^*A^*$, which is equivalent to $ABB^*A^\dagger A = ABB^*$. Hence, $2 \Leftrightarrow 3$.
4. The Penrose equations imply that: $B^\dagger A^\dagger \in (AB)\{1,2,4\} \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$ and $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$.

We prove $1 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1$.

Suppose that 1 holds. If we multiply $(A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$ by A_1B_1 from the left side, we obtain $A_1 = A_1A_1^*D^{-1}A_1$. Furthermore, $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$ holds. Therefore, $1 \Rightarrow 4$.

Suppose that 4 holds. Obviously, $A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1A_1^*D^{-1}A_1B_1B_1^* = A_1B_1B_1^*$. Thus, the first equality of 2 holds. The second equality of 2 also holds, since $A_1^*D^{-1}A_2 = 0 \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$, which is shown in the proof of Theorem 2.1. Here we use again $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$. Consequently, $4 \Rightarrow 2$.

In order to prove that $2 \Rightarrow 1$, we multiply $A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1B_1B_1^*$ by $(A_1B_1)^\dagger$ from the left side. It follows that $B_1^*A_1^*D^{-1}A_1 = (A_1B_1)^\dagger A_1B_1B_1^*$, so $(A_1B_1)^\dagger A_1B_1 = B_1^*A_1^*D^{-1}A_1(B_1^*)^{-1}$ which is equivalent to $(A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$. Hence, $2 \Rightarrow 1$.

Notice that $3 \Leftrightarrow 4$ is also proved in [8].

Finally, the part (c) follows from the parts (a) and (b). □

We also prove the following result.

Theorem 2.3. *Let X, Y, Z be Hilbert spaces, and let $A \in \mathcal{L}(Y, Z)$, $B \in \mathcal{L}(X, Y)$ be such that A, B, AB have closed ranges. Then we have:*

(a) $AB(AB)^\dagger A = ABB^\dagger \Leftrightarrow A^*ABB^\dagger = BB^\dagger A^*A \Leftrightarrow \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,3\}$;
(b) $B(AB)^\dagger AB = A^\dagger AB \Leftrightarrow A^\dagger ABB^* = BB^*A^\dagger A \Leftrightarrow \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,4\}$;
(c) *The following three statements are equivalent:*
  (1) $(AB)^\dagger = B^\dagger A^\dagger$;
  (2) $AB(AB)^\dagger A = ABB^\dagger$ *and* $B(AB)^\dagger AB = A^\dagger AB$;
  (3) $A^*ABB^\dagger = BB^\dagger A^*A$ *and* $A^\dagger ABB^* = BB^*A^\dagger A$.

Proof. The operators A and B have the same matrix representations as in the previous theorem. First, we find equivalent expressions, in the terms of A_1, A_2 and B_1, for our assumptions.

$$\begin{tikzcd}
& \ker(a) \arrow[r] \arrow[d] & \ker(b) \arrow[r] \arrow[d] & \ker(c) \arrow[d] \arrow[dddll, rounded corners] & \\
& A \arrow[r, "f"'] \arrow[d, "a"] & B \arrow[r, "g"'] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"'] \arrow[d] & B' \arrow[r, "g'"'] \arrow[d] & C' \arrow[d] & \\
& \operatorname{coker}(a) \arrow[r] & \operatorname{coker}(b) \arrow[r] & \operatorname{coker}(c) &
\end{tikzcd}$$

"The Moore-Penrose inverse is unique"

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$ABA = A, \qquad BAB = B, \qquad B^*A^* = AB, \qquad A^*B^* = BA$$

"The Moore-Penrose inverse is unique"

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$ABA = A, \qquad BAB = B, \qquad B^*A^* = AB, \qquad A^*B^* = BA$$

Claim If B and C satisfy these identities, then $B = C$.

"The Moore-Penrose inverse is unique"

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$ABA = A, \qquad BAB = B, \qquad B^*A^* = AB, \qquad A^*B^* = BA$$

Claim If B and C satisfy these identities, then $B = C$.

Proof $$B = BAB = BACAB = \dots = C$$

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$ABA = A, \qquad BAB = B, \qquad B^*A^* = AB, \qquad A^*B^* = BA$$

Claim If B and C satisfy these identities, then $B = C$.

Proof $$B = BAB = BACAB = \ldots = C$$

An algebraic point of view

$$L = R \quad \Longleftrightarrow \quad L - R = 0$$

"The Moore-Penrose inverse is unique"

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$ABA = A, \qquad BAB = B, \qquad B^*A^* = AB, \qquad A^*B^* = BA$$

Claim If B and C satisfy these identities, then $B = C$.

Proof $$B \;=\; BAB \;=\; BACAB \;=\; \dots \;=\; C$$

An algebraic point of view

$$L = R \quad \iff \quad L - R$$

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$ABA - A, \qquad BAB - B, \qquad B^*A^* - AB, \qquad A^*B^* - BA$$

Claim If B and C satisfy these identities, then $B = C$.

Proof $$B = BAB = BACAB = \ldots = C$$

An algebraic point of view

$$L = R \quad \Longleftrightarrow \quad L - R$$

Noncommutative polynomials

Noncom. polynomial $f = c_1 \cdot w_1 + \cdots + c_d \cdot w_d$

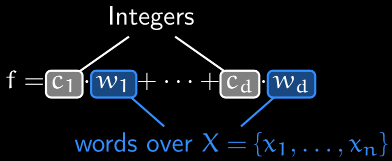
Noncommutative polynomials

Integers

Noncom. polynomial $f = \boxed{c_1} \cdot w_1 + \cdots + \boxed{c_d} \cdot w_d$

Noncommutative polynomials

Noncom. polynomial



Integers

$$f = \boxed{c_1} \cdot \boxed{w_1} + \cdots + \boxed{c_d} \cdot \boxed{w_d}$$

words over $X = \{x_1, \ldots, x_n\}$

Noncommutative polynomials

Integers

Noncom. polynomial $$f = \boxed{c_1} \cdot \boxed{w_1} + \cdots + \boxed{c_d} \cdot \boxed{w_d}$$

words over $X = \{x_1, \ldots, x_n\}$

Example $2xy + yx - 2xzx + 4$

Noncommutative polynomials

Integers

free algebra

Noncom. polynomial $f = \boxed{c_1} \cdot \boxed{w_1} + \cdots + \boxed{c_d} \cdot \boxed{w_d} \in \boxed{\mathbb{Z}\langle X \rangle}$

words over $X = \{x_1, \ldots, x_n\}$

Example $2xy + yx - 2xzx + 4 \in \mathbb{Z}\langle x, y, z \rangle$

Noncommutative polynomials

Integers

free algebra

Noncom. polynomial $\quad f = \boxed{c_1} \cdot \boxed{w_1} + \cdots + \boxed{c_d} \cdot \boxed{w_d} \quad \in \boxed{\mathbb{Z}\langle X \rangle}$

words over $X = \{x_1, \ldots, x_n\}$

Example $\quad 2xy + yx - 2xzx + 4 \;\in\; \mathbb{Z}\langle x, y, z \rangle$

Arithmetic operations

$$\begin{aligned} \text{Addition} \quad &= \quad \text{like in the commutative case} \\ (xy - z) + (yx + 2z) \quad &= \quad xy + yx + z \\[1em] \text{Multiplication} \quad &= \quad \text{concatenation of words} \\ (xy - z) \cdot (yx + 2z) \quad &= \quad xyyx + 2xyz - zyx - 2zz \end{aligned}$$

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$ABA - A, \qquad BAB - B, \qquad B^*A^* - AB, \qquad A^*B^* - BA$$

Claim If B and C satisfy these identities, then $B = C$.

Proof

$$B = BAB = BACAB = \ldots = C$$

An algebraic point of view

$$L = R \quad \Longleftrightarrow \quad L - R$$

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$aba \; - a\,, \qquad bab \; - b, \qquad b^*a^* \; - ab\,, \qquad a^*b^* \; - ba$$

Claim If B and C satisfy these identities, then $B = C$.

Proof

$$B = BAB = BACAB = \ldots = C$$

An algebraic point of view

$$L = R \quad \Longleftrightarrow \quad l - r \in \mathbb{Z}\langle \mathbf{X} \rangle$$

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$aba - a, \qquad bab - b, \qquad b^*a^* - ab, \qquad a^*b^* - ba$$

Claim If B and C satisfy these identities, then $B = C$.

Proof $$B = BAB = BACAB = \ldots = C$$

An algebraic point of view

$$L = R \quad \Longleftrightarrow \quad l - r \in \mathbb{Z}\langle \mathbf{X} \rangle$$

$$B = \ldots = C \quad \Longleftrightarrow \quad ?$$

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X\rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I,\, p, q \in \mathbb{Z}\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

The smallest ideal containing $f_1, \ldots, f_r$ is denoted by $I = (f_1, \ldots, f_r)$.

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X \rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I,\, p, q \in \mathbb{Z}\langle X \rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

The smallest ideal containing $\underbrace{\boxed{f_1, \dots, f_r}}_{\text{“axioms”}}$ is denoted by $I = (f_1, \dots, f_r)$.

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X\rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I, p, q \in \mathbb{Z}\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

"deduction rules"

The smallest ideal containing $\underbrace{\boxed{f_1, \ldots, f_r}}_{\text{“axioms”}}$ is denoted by $I = (f_1, \ldots, f_r)$.

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X\rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I,\, p, q \in \mathbb{Z}\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

"deduction rules"

The smallest ideal containing $\underbrace{\boxed{f_1, \dots, f_r}}_{\text{“axioms”}}$ is denoted by $\underbrace{\boxed{I = (f_1, \dots, f_r)}}_{\text{“theory”}}$.

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X\rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I,\, p, q \in \mathbb{Z}\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

"deduction rules"

The smallest ideal containing $\underbrace{f_1, \dots, f_r}_{\text{“axioms”}}$ is denoted by $\underbrace{I = (f_1, \dots, f_r)}_{\text{“theory”}}$.

$$f \text{ is consequence of } f_1, \dots, f_r \iff f \in (f_1, \dots, f_r)$$

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X \rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I,\, p, q \in \mathbb{Z}\langle X \rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

“deduction rules”

The smallest ideal containing $\underbrace{\boxed{f_1, \dots, f_r}}_{\text{“axioms”}}$ is denoted by $\underbrace{\boxed{I = (f_1, \dots, f_r)}}_{\text{“theory”}}$.

$$f \text{ is consequence of } f_1, \dots, f_r \quad\Longleftrightarrow\quad f \in (f_1, \dots, f_r)$$

Ideal membership problem $f \overset{?}{\in} (f_1, \dots, f_r)$ is only semi-decidable.

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X\rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I,\, p, q \in \mathbb{Z}\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

"deduction rules"

The smallest ideal containing $\underbrace{f_1, \ldots, f_r}_{\text{"axioms"}}$ is denoted by $\underbrace{I = (f_1, \ldots, f_r)}_{\text{"theory"}}$.

$$f \text{ is consequence of } f_1, \ldots, f_r \quad\Longleftrightarrow\quad f \in (f_1, \ldots, f_r)$$

Ideal membership problem $f \overset{?}{\in} (f_1, \ldots, f_r)$ is only semi-decidable.

- $f \in (f_1, \ldots, f_r)$ can always be verified in finite time
- in this case, we can compute $p_i, q_i \in \mathbb{Z}\langle X\rangle :\; f = \sum_i p_i \cdot f_i \cdot q_i$

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X\rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f + g \in I$
2. $f \in I, p, q \in \mathbb{Z}\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$

“deduction rules”

The smallest ideal containing $\underbrace{\boxed{f_1, \ldots, f_r}}_{\text{“axioms”}}$ is denoted by $\underbrace{\boxed{I = (f_1, \ldots, f_r)}}_{\text{“theory”}}$.

$$f \text{ is consequence of } f_1, \ldots, f_r \quad\Longleftrightarrow\quad f \in (f_1, \ldots, f_r)$$

Ideal membership problem $f \overset{?}{\in} (f_1, \ldots, f_r)$ is only semi-decidable.

- $f \in (f_1, \ldots, f_r)$ can always be verified in finite time
- in this case, we can compute $p_i, q_i \in \mathbb{Z}\langle X\rangle$: $\boxed{f = \sum_i p_i \cdot f_i \cdot q_i}$

“proof/certificate”

Consequences

Definition A nonempty set $I \subseteq \mathbb{Z}\langle X\rangle$ is a (two-sided) ideal if

1. $f, g \in I \;\Rightarrow\; f+g \in I$
2. $f \in I,\, p, q \in \mathbb{Z}\langle X\rangle \;\Rightarrow\; p\cdot f\cdot q \in I$

“deduction rules”

The smallest ideal containing $\underbrace{\boxed{f_1,\dots,f_r}}_{\text{“axioms”}}$ is denoted by $\underbrace{\boxed{I=(f_1,\dots,f_r)}}_{\text{“theory”}}$.

$$f \text{ is consequence of } f_1,\dots,f_r \iff f\in(f_1,\dots,f_r)$$

Ideal membership problem $f \overset{?}{\in} (f_1,\dots,f_r)$ is only semi-decidable.

- $f \in (f_1,\dots,f_r)$ can always be verified in finite time
- in this case, we can compute $p_i, q_i \in \mathbb{Z}\langle X\rangle$: $\boxed{f=\sum_i p_i\cdot f_i\cdot q_i}$ “proof/certificate”
- if $f \notin (f_1,\dots,f_r)$, we might run into an infinite computation

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$aba \; - a\,, \qquad bab \; - b, \qquad b^*a^* \; - ab\,, \qquad a^*b^* \; - ba$$

Claim If B and C satisfy these identities, then $B = C$.

Proof $$B = BAB = BACAB = \ldots = C$$

An algebraic point of view

$$L = R \quad \iff \quad l - r \in \mathbb{Z}\langle \mathbf{X} \rangle$$
$$B = \ldots = C \quad \iff \quad ?$$

"The Moore-Penrose inverse is unique"

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$aba \;-a\,, \qquad bab \;-b, \qquad b^*a^* \;-ab\,, \qquad a^*b^* \;-ba$$

Claim If B and C satisfy these identities, then $B = C$.

Proof $$B = BAB = BACAB = \ldots = C$$

An algebraic point of view

$$L = R \quad\Longleftrightarrow\quad l - r \in \mathbb{Z}\langle \mathbf{X} \rangle$$

$$B = \ldots = C \quad\Longleftrightarrow\quad b - c \in (f_1, \ldots, f_{12})$$

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$aba - a, \qquad bab - b, \qquad b^*a^* - ab, \qquad a^*b^* - ba$$

Claim If B and C satisfy these identities, then $B = C$.

Proof Using our software package operator_gb...

```
sage: from operator_gb import *
sage: assumptions = [a*b*a - a,...]
sage: certify(assumptions, b - c)
```

"The Moore-Penrose inverse is unique"

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$aba - a, \qquad bab - b, \qquad b^*a^* - ab, \qquad a^*b^* - ba$$

Claim If B and C satisfy these identities, then $B = C$.

Proof Using our software package operator_gb...

```
 sage: from operator_gb import *
 sage: assumptions = [a*b*a - a,...]
 sage: certify(assumptions, b - c)
b - c = (-c + c*a*c) + b*c_adj*(-a_adj + a_adj*b_adj*a_adj)
        - b*a*c*(-a*b + b_adj*a_adj) - b*(-a + a*c*a)*b
        + b*(-a*c + c_adj*a_adj) - b*(-a*c + c_adj*a_adj)*b_adj*a_adj
        - (-b + b*a*b) + (-c*a + a_adj*c_adj)*b*a*c
        - (-a_adj + a_adj*c_adj*a_adj)*b_adj*c + c*(-a + a*b*a)*c
        - (-b*a + a_adj*b_adj)*c + a_adj*c_adj*(-b*a + a_adj*b_adj)*c
```

“The Moore-Penrose inverse is unique”

Def.: A matrix B is Moore-Penrose inverse of a matrix A if

$$aba - a\,, \qquad bab - b\,, \qquad b^*a^* - ab\,, \qquad a^*b^* - ba$$

Claim If B and C satisfy these identities, then $B = C$.

Proof Using our software package operator_gb...

```
 sage: from operator_gb import *
 sage: assumptions = [a*b*a - a,...]
 sage: certify(assumptions, b - c)
b - c = (-c + c*a*c) + b*c_adj*(-a_adj + a_adj*b_adj*a_adj)
        - b*a*c*(-a*b + b_adj*a_adj) - b*(-a + a*c*a)*b
        + b*(-a*c + c_adj*a_adj) - b*(-a*c + c_adj*a_adj)*b_adj*a_adj
        - (-b + b*a*b) + (-c*a + a_adj*c_adj)*b*a*c
        - (-a_adj + a_adj*c_adj*a_adj)*b_adj*c + c*(-a + a*b*a)*c
        - (-b*a + a_adj*b_adj)*c + a_adj*c_adj*(-b*a + a_adj*b_adj)*c
```

Observation Proof only relies on basic linearity properties

⇒ Statement proven for matrices, (un)bounded operators, morphisms,...

Operator statements

Operators

- $0, A, B, C, \ldots$
- $S + T, \;\; S \cdot T, \;\; f(T_1, \ldots, T_n)$

Operator statements

Operators

$*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes,\ \dots$

- $0, A, B, C, \dots$
- $S + T,\ \ S \cdot T,\ \ \boxed{f}(T_1, \dots, T_n)$

Operator statements

Operators

$*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes,\ \ldots$

- $0, A, B, C, \ldots$
- $S + T,\ \ S \cdot T,\ \ \boxed{f}(T_1, \ldots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity

Operator statements

Operators

- $0, A, B, C, \ldots$
- $S + T,\ \ S \cdot T,\ \ \overset{*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes,\ \ldots}{\boxed{f}}(T_1, \ldots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity
4. [*] we also allow partial operations

Operator statements

Operators

$*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes,\ \ldots$

- $0, A, B, C, \ldots$
- $S + T,\ \ S \cdot T,\ \ \boxed{f}(T_1, \ldots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity
4.* we also allow partial operations

Operator statements

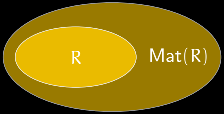
Operators

$*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes,\ \ldots$

- $0, A, B, C, \ldots$
- $S + T,\ \ S \cdot T,\ \boxed{f}(T_1, \ldots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity
4. [*] we also allow partial operations



Operator statements

Operators

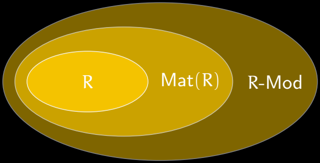
$*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes, \dots$

- $0, A, B, C, \dots$
- $S + T,\ \ S \cdot T,\ \ \boxed{f}(T_1, \dots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity

4.* we also allow partial operations



Operator statements

Operators

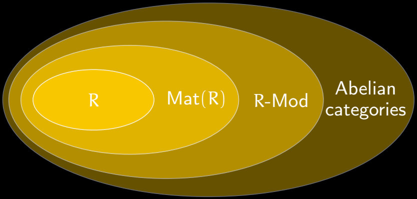
- $0, A, B, C, \dots$

$*, \ \cdot^{\mathsf{T}}, \ \|\cdot\|, \ \otimes, \dots$

- $S + T, \ \ S \cdot T, \ \ \boxed{f}(T_1, \dots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity
4. [*] we also allow partial operations



Operator statements

Operators

$*, \cdot^{\mathsf{T}}, \|\cdot\|, \otimes, \dots$

- $0, A, B, C, \dots$
- $S + T, \;\; S \cdot T, \;\; \boxed{f}(T_1, \dots, T_n)$

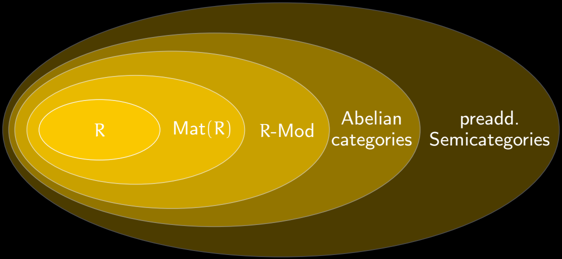
Linearity

1. $+$ forms an abelian group

2. $\cdot$ is associative

3. distributivity

4.* we also allow partial operations



Operator statements

Operators

$*, \ \cdot^{\mathsf{T}}, \ \|\cdot\|, \ \otimes, \ldots$

- $0, A, B, C, \ldots$
- $S + T, \ \ S \cdot T, \ \ \boxed{f}(T_1, \ldots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity
4. [*] we also allow partial operations

Operator statements

$$S = T, \quad \neg\,\varphi, \quad (\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \Rightarrow \psi), \quad \exists X : \varphi, \quad \forall X : \varphi$$

Operator statements

Operators

$^*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes,\ \dots$

- $0, A, B, C, \dots$
- $S + T,\ \ S \cdot T,\ \ \boxed{f}(T_1, \dots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity
4.* we also allow partial operations

Operator statements

$$S = T, \quad \neg\,\varphi, \quad (\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \Rightarrow \psi), \quad \exists X : \varphi, \quad \forall X : \varphi$$

Def. An operator statement is universally true if it follows from linearity.

Operator statements

Operators

$^*,\ \cdot^{\mathsf{T}},\ \|\cdot\|,\ \otimes,\ \ldots$

- $0, A, B, C, \ldots$
- $S + T,\ \ S \cdot T,\ \ \boxed{f}(T_1, \ldots, T_n)$

Linearity

1. $+$ forms an abelian group
2. $\cdot$ is associative
3. distributivity

4.* we also allow partial operations

Operator statements

$$S = T, \quad \neg\,\varphi, \quad (\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \Rightarrow \psi), \quad \exists X : \varphi, \quad \forall X : \varphi$$

Def. An operator statement is universally true if it follows from linearity.

Fact: Determining universal truth is not decidable

Best we can hope for: semi-decision procedure

Semi decision procedure

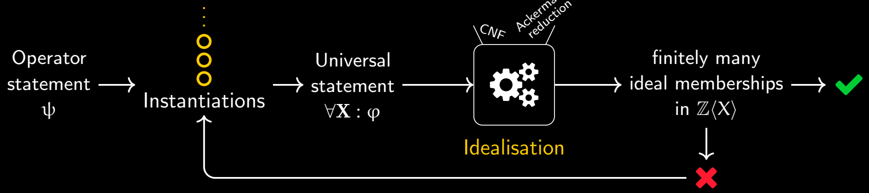
Quasi-identities

(Helton, Stankus, Wavrik '98, Schmitz, Levandovskyy '20, Raab, Regensburger, Hossein Poor '21)

$$\bigwedge_{i=1}^{m} P_i = Q_i \;\Rightarrow\; S = T \qquad \text{iff} \qquad s - t \in (p_1 - q_1, \ldots, p_m - q_m)$$

Semi decision procedure

General operator statements



Operator statement ψ → Instantiations → Universal statement $\forall \mathbf{X} : \varphi$ → Idealisation → finitely many ideal memberships in $\mathbb{Z}\langle X \rangle$ → ✓

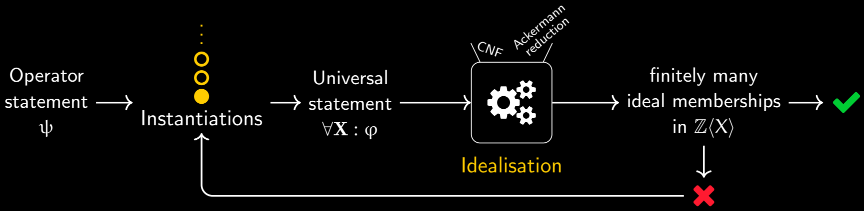
CNF

Ackermann reduction

✗

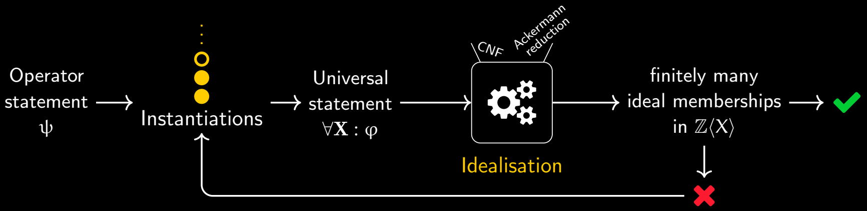
Semi decision procedure

General operator statements


Operator statement ψ
Instantiations
Universal statement $\forall \mathbf{X} : \varphi$
CNF
Ackermann reduction
Idealisation
finitely many ideal memberships in $\mathbb{Z}\langle X \rangle$
✓
✗

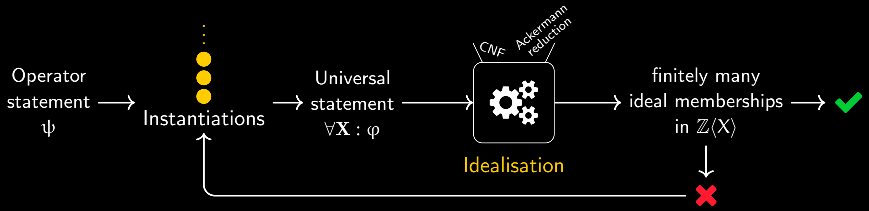
Semi decision procedure

General operator statements


Operator statement ψ
Instantiations
Universal statement $\forall \mathbf{X} : \varphi$
CNF
Ackermann reduction
Idealisation
finitely many ideal memberships in $\mathbb{Z}\langle X \rangle$
✓
✗

Semi decision procedure

General operator statements



Operator statement ψ → Instantiations → Universal statement $\forall \mathbf{X} : \varphi$ → Idealisation → finitely many ideal memberships in $\mathbb{Z}\langle X\rangle$ → ✓

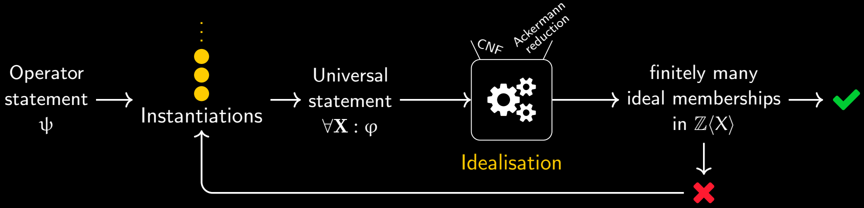
CNF

Ackermann reduction

✗ → Instantiations

Semi decision procedure

General operator statements



Operator statement ψ

Instantiations

Universal statement $\forall \mathbf{X} : \varphi$

CNF

Ackermann reduction

Idealisation

finitely many ideal memberships in $\mathbb{Z}\langle X\rangle$

✓

✗

Theorem (H., Raab, Regensburger '22)

An operator statement is universally true iff this procedure terminates and returns ✓.

5.7 Pseudo-Inverse

Definitions:

A **Moore–Penrose pseudo-inverse** of a matrix $A \in \mathbb{C}^{m\times n}$ is a matrix $A^\dagger \in \mathbb{C}^{n\times m}$ that satisfies the following four **Penrose** conditions:

$$AA^\dagger A = A; \quad A^\dagger AA^\dagger = A^\dagger; \quad (AA^\dagger)^* = AA^\dagger; \quad (A^\dagger A)^* = A^\dagger A.$$

Facts:

All the following facts except those with a specific reference can be found in [Gra83, pp. 105–141] or [RM71, pp. 44–67].

✓ 1. Every $A \in \mathbb{C}^{m\times n}$ has a unique pseudo-inverse $A^\dagger$.

✓ 2. If $A \in \mathbb{R}^{m\times n}$, then $A^\dagger$ is real.

✓ 3. If $A \in \mathbb{C}^{m\times n}$ of rank r has a full rank decomposition $A = BC$, where $B \in \mathbb{C}^{m\times r}$ and $C \in \mathbb{C}^{r\times n}$, then $A^\dagger$ can be evaluated using $A^\dagger = C^*(B^*AC^*)^{-1}B^*$.

✓ 4. [LH95, p. 38] If $A \in \mathbb{C}^{m\times n}$ of rank $r \le \min\{m,n\}$ has an SVD $A = U\Sigma V^*$, then its pseudo-inverse is $A^\dagger = V\Sigma^\dagger U^*$, where

$$\Sigma^\dagger = \mathrm{diag}(1/\sigma_1, \dots, 1/\sigma_r, 0, \dots, 0) \in \mathbb{R}^{n\times m}.$$

✗ 5. [Hig96, p. 412] The pseudo-inverse $A^\dagger$ of $A \in F^{m\times n}$ ($F = \mathbb{C}$ or $\mathbb{R}$) solves the minimization problem

$$\min_{X\in F^{n\times m}} \|AX - I_m\|_F^2.$$

✓ 6. $\mathbf{0}_{mn}^\dagger = \mathbf{0}_{nm}$ and $J_{mn}^\dagger = \frac{1}{mn}J_{nm}$, where $\mathbf{0}_{mn} \in \mathbb{C}^{m\times n}$ is the all 0s matrix and $J_{mn} \in \mathbb{C}^{m\times n}$ is the all 1s matrix.

✓ 7. If $\mathbf{x} \ne \mathbf{0}$, $\mathbf{y} \ne \mathbf{0}$, then $(\mathbf{x}\mathbf{y}^*)^\dagger = \dfrac{\mathbf{y}\mathbf{x}^*}{\|\mathbf{x}\|^2\|\mathbf{y}\|^2}$.

✓ 8. If $\mathbf{x} \ne \mathbf{0}$, then $\mathbf{x}^\dagger = \dfrac{\mathbf{x}^*}{\|\mathbf{x}\|^2}$.

✓ 9. Let α be a scalar. Denote

$$\alpha^\dagger = \begin{cases} \alpha^{-1}, & \text{if } \alpha \ne 0, \\ 0, & \text{if } \alpha = 0. \end{cases}$$

Then

✓ (a) $(\alpha A)^\dagger = \alpha^\dagger A^\dagger$.

✗ (b) $(\mathrm{diag}(\beta_1, \beta_2, \cdots, \beta_n))^\dagger = \mathrm{diag}(\beta_1^\dagger, \beta_2^\dagger, \cdots, \beta_n^\dagger)$.

✓ 10. $(A^\dagger)^* = (A^*)^\dagger$; $(A^\dagger)^\dagger = A$.

✓ 11. If A is a nonsingular square matrix, then $A^\dagger = A^{-1}$.

✓ 12. If U has orthonormal columns or orthonormal rows, then $U^\dagger = U^*$.

✓ 13. If $A = A^*$ and $A = A^2$, then $A^\dagger = A$.

✓ 14. $A^\dagger = A^*$ if and only if A^*A is idempotent.

✓ 15. If A is normal and k is a positive integer, then $AA^\dagger = A^\dagger A$ and $(A^k)^\dagger = (A^\dagger)^k$.

✓ 16. If $U \in \mathbb{C}^{m\times n}$ is of rank n and satisfies $U^\dagger = U^*$, then U has orthonormal columns.

✓ 17. If $U \in \mathbb{C}^{m\times m}$ and $V \in \mathbb{C}^{n\times n}$ are unitary matrices, then $(UAV)^\dagger = V^*A^\dagger U^*$.

✓ 18. $A^\dagger = (A^*A)^\dagger A^* = A^*(AA^*)^\dagger$. In particular,

✓ (a) if $A \in \mathbb{C}^{m\times n}$ ($m \ge n$) has full rank n, then $A^\dagger = (A^*A)^{-1}A^*$;

✓ (b) if $A \in \mathbb{C}^{m\times n}$ ($m \le n$) has full rank m, then $A^\dagger = A^*(AA^*)^{-1}$.

✓ 19. Let $A \in \mathbb{C}^{m\times n}$. Then

✓ (a) $A^\dagger A$, $AA^\dagger$, $I_n - A^\dagger A$, and $I_m - AA^\dagger$ are orthogonal projections.

✗ (b) $\mathrm{rank}(A) = \mathrm{rank}(A^\dagger) = \mathrm{rank}(AA^\dagger) = \mathrm{rank}(A^\dagger A)$.

✗ (c) $\mathrm{rank}(I_n - A^\dagger A) = n - \mathrm{rank}(A)$.

✗ (d) $\mathrm{rank}(I_m - AA^\dagger) = m - \mathrm{rank}(A)$.

✓ 20. $AA^\dagger = \mathrm{Proj}_{\mathrm{range}(A)}$; $A^\dagger A = \mathrm{Proj}_{\mathrm{range}(A^\dagger)}$.

✓ 21. Suppose that $A \in F^{m\times n}$, where $F = \mathbb{C}$ or $\mathbb{R}$. Then

✓ (a) $\mathrm{range}(A) = \mathrm{range}(AA^*) = \mathrm{range}(AA^\dagger)$.

✓ (b) $\mathrm{range}(A^\dagger) = \mathrm{range}(A^*) = \mathrm{range}(A^*A) = \mathrm{range}(A^\dagger A)$.

✓ (c) $\ker(A) = \ker(A^*A) = \ker(A^\dagger A)$.

✓ (d) $\ker(A^\dagger) = \ker(A^*) = \ker(AA^*) = \ker(AA^\dagger)$.

✓ (e) $\mathrm{range}(A^\dagger A) \oplus \ker(A^\dagger A) = F^n$.

✓ (f) $\mathrm{range}(AA^\dagger) \oplus \ker(AA^\dagger) = F^m$.

✓ 22. If $A = A_1 + A_2 + \cdots + A_k$, $A_i^*A_j = 0$, and $A_iA_j^* = 0$, for all $i, j = 1, \cdots, k$, $i \ne j$, then $A^\dagger = A_1^\dagger + A_2^\dagger + \cdots + A_k^\dagger$.

✓ 23. If A is an $m\times r$ matrix of rank r and B is an $r\times n$ matrix of rank r, then $(AB)^\dagger = B^\dagger A^\dagger$.

✓ 24. $(A^*A)^\dagger = A^\dagger(A^*)^\dagger$; $(AA^*)^\dagger = (A^*)^\dagger A^\dagger$.

✓ 25. [Gre66] Each one of the following conditions is necessary and sufficient for $(AB)^\dagger = B^\dagger A^\dagger$:

✓ (a) $\mathrm{range}(BB^*A^*) \subseteq \mathrm{range}(A^*)$ and $\mathrm{range}(A^*AB) \subseteq \mathrm{range}(B)$.

✓ (b) $A^\dagger ABB^*$ and $A^*ABB^\dagger$ are both Hermitian matrices.

✓ (c) $A^\dagger ABB^*A^* = BB^*A^*$ and $BB^\dagger A^*AB = A^*AB$.

✓ (d) $A^\dagger ABB^*A^*ABB^\dagger = BB^*A^*A$.

✓ (e) $A^\dagger AB = B(AB)^\dagger AB$ and $BB^\dagger A^* = A^*AB(AB)^\dagger$.

✓ 26. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$, where $\otimes$ denotes the Kronecker product.

✗ 27. $A^\dagger = \lim_{\alpha\to 0} A^*(\alpha I + AA^*)^{-1} = \lim_{\alpha\to 0}(\alpha I + A^*A)^{-1}A^*$.

✗ 28. $A^\dagger = \sum_{j=1}^{\infty} A^*(I + AA^*)^{-j} = \sum_{j=1}^{\infty}(I + A^*A)^{-j}A^*$.

✗ 29. (Continuity of pseudo-inverse) Suppose that $A \in F^{m\times n}$ and $E \in F^{m\times n}$, where $F = \mathbb{C}$ or $\mathbb{R}$. Then $\lim_{E\to 0}(A+E)^\dagger = A^\dagger$ if and only if there is $\epsilon > 0$ such that $\mathrm{rank}(A+E) = \mathrm{rank(A)}$ when $\|E\|_2 \le \epsilon$.

✓ 30. Let $A \in \mathbb{C}^{m\times n}$ be of rank r where $0 < r < \min\{m,n\}$. Suppose that A can be partitioned as

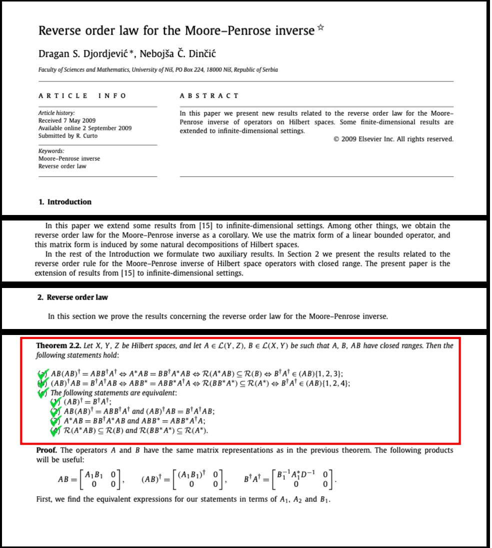
$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

where $A_{11} \in \mathbb{C}^{r\times r}$ and $\mathrm{rank}(A_{11}) = r$. Then

$$A^\dagger = \begin{bmatrix} A_{11}^*XA_{11}^* & A_{11}^*XA_{21}^* \\ A_{12}^*XA_{11}^* & A_{12}^*XA_{21}^* \end{bmatrix},$$

where

$$X = (A_{11}A_{11}^* + A_{12}A_{12}^*)^{-1}A_{11}(A_{11}^*A_{11} + A_{21}^*A_{21})^{-1}.$$



Reverse order law for the Moore–Penrose inverse ☆

Dragan S. Djordjević *, Nebojša Č. Dinčić

Faculty of Sciences and Mathematics, University of Niš, PO Box 224, 18000 Niš, Republic of Serbia

ARTICLE INFO

Article history:
Received 7 May 2009
Available online 2 September 2009
Submitted by R. Curto

Keywords:
Moore–Penrose inverse
Reverse order law

ABSTRACT

In this paper we present new results related to the reverse order law for the Moore–Penrose inverse of operators on Hilbert spaces. Some finite-dimensional results are extended to infinite-dimensional settings.

1. Introduction

In this paper we extend some results from [15] to infinite-dimensional settings. Among other things, we obtain the reverse order law for the Moore–Penrose inverse as a corollary. We use the matrix form of a linear bounded operator, and this matrix form is induced by some natural decompositions of Hilbert spaces.

In the rest of the Introduction we formulate two auxiliary results. In Section 2 we present the results related to the reverse order rule for the Moore–Penrose inverse of Hilbert space operators with closed range. The present paper is the extension of results from [15] to infinite-dimensional settings.

2. Reverse order law

In this section we prove the results concerning the reverse order law for the Moore–Penrose inverse.

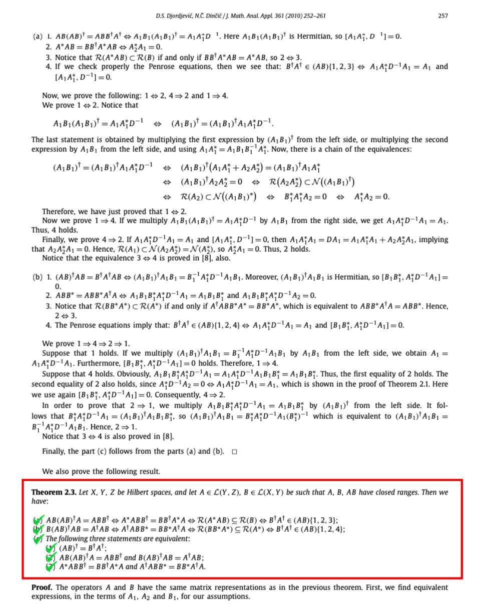
Theorem 2.2. *Let X, Y, Z be Hilbert spaces, and let $A \in \mathcal{L}(Y,Z)$, $B \in \mathcal{L}(X,Y)$ be such that A, B, AB have closed ranges. Then the following statements hold:*

✓ (a) $AB(AB)^\dagger = ABB^\dagger A^\dagger \Leftrightarrow A^*AB = BB^\dagger A^*AB \Leftrightarrow \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,3\}$;
✓ (b) $(AB)^\dagger AB = B^\dagger A^\dagger AB \Leftrightarrow ABB^* = ABB^*A^\dagger A \Leftrightarrow \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,4\}$;
✓ (c) *The following statements are equivalent:*
  ✓ (1) $(AB)^\dagger = B^\dagger A^\dagger$;
  ✓ (2) $AB(AB)^\dagger = ABB^\dagger A^\dagger$ *and* $(AB)^\dagger AB = B^\dagger A^\dagger AB$;
  ✓ (3) $A^*AB = BB^\dagger A^*AB$ *and* $ABB^* = ABB^*A^\dagger A$;
  ✓ (4) $\mathcal{R}(A^*AB) \subseteq \mathcal{R}(B)$ *and* $\mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*)$.

Proof. The operators A and B have the same matrix representations as in the previous theorem. The following products will be useful:

$$AB = \begin{bmatrix} A_1B_1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad (AB)^\dagger = \begin{bmatrix} (A_1B_1)^\dagger & 0 \\ 0 & 0 \end{bmatrix}, \qquad B^\dagger A^\dagger = \begin{bmatrix} B_1^{-1}A_1^*D^{-1} & 0 \\ 0 & 0 \end{bmatrix}.$$

First, we find the equivalent expressions for our statements in terms of A_1, A_2 and B_1.



(a) 1. $AB(AB)^\dagger = ABB^\dagger A^\dagger \Leftrightarrow A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{\ 1}$. Here $A_1B_1(A_1B_1)^\dagger$ is Hermitian, so $[A_1A_1^*, D^{\ 1}] = 0$.
2. $A^*AB = BB^\dagger A^*AB \Leftrightarrow A_2^*A_1 = 0$.
3. Notice that $\mathcal{R}(A^*AB) \subset \mathcal{R}(B)$ if and only if $BB^\dagger A^*AB = A^*AB$, so $2 \Leftrightarrow 3$.
4. If we check properly the Penrose equations, then we see that: $B^\dagger A^\dagger \in (AB)\{1,2,3\} \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$ and $[A_1A_1^*, D^{-1}] = 0$.

Now, we prove the following: $1 \Leftrightarrow 2$, $4 \Rightarrow 2$ and $1 \Rightarrow 4$.

We prove $1 \Leftrightarrow 2$. Notice that

$$A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{-1} \quad \Leftrightarrow \quad (A_1B_1)^\dagger = (A_1B_1)^\dagger A_1A_1^*D^{-1}.$$

The last statement is obtained by multiplying the first expression by $(A_1B_1)^\dagger$ from the left side, or multiplying the second expression by A_1B_1 from the left side, and using $A_1A_1^* = A_1B_1B_1^{-1}A_1^*$. Now, there is a chain of the equivalences:

$$\begin{aligned} (A_1B_1)^\dagger = (A_1B_1)^\dagger A_1A_1^*D^{-1} \quad &\Leftrightarrow \quad (A_1B_1)^\dagger\big(A_1A_1^* + A_2A_2^*\big) = (A_1B_1)^\dagger A_1A_1^* \\ &\Leftrightarrow \quad (A_1B_1)^\dagger A_2A_2^* = 0 \quad \Leftrightarrow \quad \mathcal{R}\big(A_2A_2^*\big) \subset \mathcal{N}\big((A_1B_1)^\dagger\big) \\ &\Leftrightarrow \quad \mathcal{R}(A_2) \subset \mathcal{N}\big((A_1B_1)^*\big) \quad \Leftrightarrow \quad B_1^*A_1^*A_2 = 0 \quad \Leftrightarrow \quad A_1^*A_2 = 0. \end{aligned}$$

Therefore, we have just proved that $1 \Leftrightarrow 2$.

Now we prove $1 \Rightarrow 4$. If we multiply $A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{-1}$ by A_1B_1 from the right side, we get $A_1A_1^*D^{-1}A_1 = A_1$. Thus, 4 holds.

Finally, we prove $4 \Rightarrow 2$. If $A_1A_1^*D^{-1}A_1 = A_1$ and $[A_1A_1^*, D^{-1}] = 0$, then $A_1A_1^*A_1 = DA_1 = A_1A_1^*A_1 + A_2A_2^*A_1$, implying that $A_2A_2^*A_1 = 0$. Hence, $\mathcal{R}(A_1) \subset \mathcal{N}(A_2A_2^*) = \mathcal{N}(A_2^*)$, so $A_2^*A_1 = 0$. Thus, 2 holds.

Notice that the equivalence $3 \Leftrightarrow 4$ is proved in [8], also.

(b) 1. $(AB)^\dagger AB = B^\dagger A^\dagger AB \Leftrightarrow (A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$. Moreover, $(A_1B_1)^\dagger A_1B_1$ is Hermitian, so $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$.
2. $ABB^* = ABB^*A^\dagger A \Leftrightarrow A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1B_1B_1^*$ and $A_1B_1B_1^*A_1^*D^{-1}A_2 = 0$.
3. Notice that $\mathcal{R}(BB^*A^*) \subset \mathcal{R}(A^*)$ if and only if $A^\dagger ABB^*A^* = BB^*A^*$, which is equivalent to $ABB^*A^\dagger A = ABB^*$. Hence, $2 \Leftrightarrow 3$.
4. The Penrose equations imply that: $B^\dagger A^\dagger \in (AB)\{1,2,4\} \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$ and $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$.

We prove $1 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1$.

Suppose that 1 holds. If we multiply $(A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$ by A_1B_1 from the left side, we obtain $A_1 = A_1A_1^*D^{-1}A_1$. Furthermore, $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$ holds. Therefore, $1 \Rightarrow 4$.

Suppose that 4 holds. Obviously, $A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1A_1^*D^{-1}A_1B_1B_1^* = A_1B_1B_1^*$. Thus, the first equality of 2 holds. The second equality of 2 also holds, since $A_1^*D^{-1}A_2 = 0 \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$, which is shown in the proof of Theorem 2.1. Here we use again $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$. Consequently, $4 \Rightarrow 2$.

In order to prove that $2 \Rightarrow 1$, we multiply $A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1B_1B_1^*$ by $(A_1B_1)^\dagger$ from the left side. It follows that $B_1^*A_1^*D^{-1}A_1 = (A_1B_1)^\dagger A_1B_1B_1^*$, so $(A_1B_1)^\dagger A_1B_1 = B_1^*A_1^*D^{-1}A_1(B_1^*)^{-1}$ which is equivalent to $(A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$. Hence, $2 \Rightarrow 1$.

Notice that $3 \Leftrightarrow 4$ is also proved in [8].

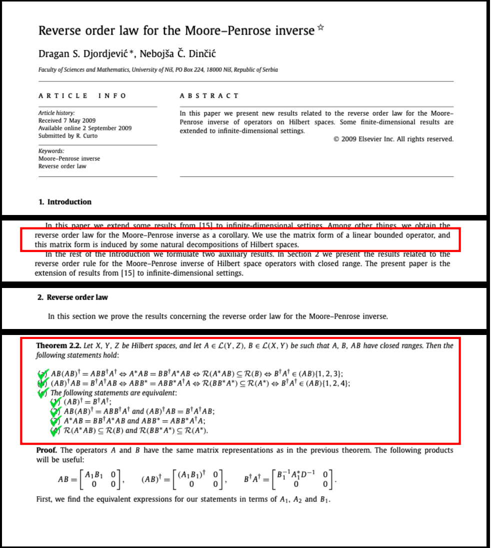
Finally, the part (c) follows from the parts (a) and (b). □

We also prove the following result.

Theorem 2.3. *Let X, Y, Z be Hilbert spaces, and let $A \in \mathcal{L}(Y,Z)$, $B \in \mathcal{L}(X,Y)$ be such that A, B, AB have closed ranges. Then we have:*

✓ (a) $AB(AB)^\dagger A = ABB^\dagger \Leftrightarrow A^*ABB^\dagger = BB^\dagger A^*A \Leftrightarrow \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,3\}$;
✓ (b) $B(AB)^\dagger AB = A^\dagger AB \Leftrightarrow A^\dagger ABB^* = BB^*A^\dagger A \Leftrightarrow \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,4\}$;
✓ (c) *The following three statements are equivalent:*
  ✓ (1) $(AB)^\dagger = B^\dagger A^\dagger$;
  ✓ (2) $AB(AB)^\dagger A = ABB^\dagger$ *and* $B(AB)^\dagger AB = A^\dagger AB$;
  ✓ (3) $A^*ABB^\dagger = BB^\dagger A^*A$ *and* $A^\dagger ABB^* = BB^*A^\dagger A$.

Proof. The operators A and B have the same matrix representations as in the previous theorem. First, we find equivalent expressions, in the terms of A_1, A_2 and B_1, for our assumptions.



Reverse order law for the Moore–Penrose inverse ☆

Dragan S. Djordjević *, Nebojša Č. Dinčić

Faculty of Sciences and Mathematics, University of Niš, PO Box 224, 18000 Niš, Republic of Serbia

ARTICLE INFO

Article history:
Received 7 May 2009
Available online 2 September 2009
Submitted by R. Curto

Keywords:
Moore–Penrose inverse
Reverse order law

ABSTRACT

In this paper we present new results related to the reverse order law for the Moore–Penrose inverse of operators on Hilbert spaces. Some finite-dimensional results are extended to infinite-dimensional settings.

1. Introduction

In this paper we extend some results from [15] to infinite-dimensional settings. Among other things, we obtain the reverse order law for the Moore–Penrose inverse as a corollary. We use the matrix form of a linear bounded operator, and this matrix form is induced by some natural decompositions of Hilbert spaces.

In the rest of the Introduction we formulate two auxiliary results. In Section 2 we present the results related to the reverse order rule for the Moore–Penrose inverse of Hilbert space operators with closed range. The present paper is the extension of results from [15] to infinite-dimensional settings.

2. Reverse order law

In this section we prove the results concerning the reverse order law for the Moore–Penrose inverse.

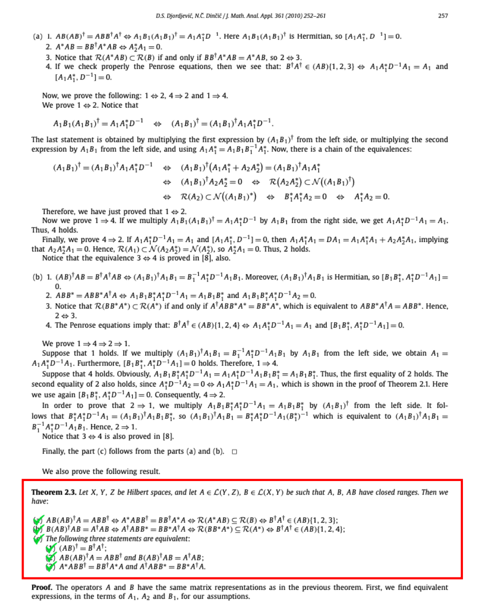
Theorem 2.2. *Let X, Y, Z be Hilbert spaces, and let $A \in \mathcal{L}(Y,Z)$, $B \in \mathcal{L}(X,Y)$ be such that A, B, AB have closed ranges. Then the following statements hold:*

✓ (a) $AB(AB)^\dagger = ABB^\dagger A^\dagger \Leftrightarrow A^*AB = BB^\dagger A^*AB \Leftrightarrow \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,3\}$;
✓ (b) $(AB)^\dagger AB = B^\dagger A^\dagger AB \Leftrightarrow ABB^* = ABB^*A^\dagger A \Leftrightarrow \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,4\}$;
✓ (c) *The following statements are equivalent:*
  ✓ (1) $(AB)^\dagger = B^\dagger A^\dagger$;
  ✓ (2) $AB(AB)^\dagger = ABB^\dagger A^\dagger$ *and* $(AB)^\dagger AB = B^\dagger A^\dagger AB$;
  ✓ (3) $A^*AB = BB^\dagger A^*AB$ *and* $ABB^* = ABB^*A^\dagger A$;
  ✓ (4) $\mathcal{R}(A^*AB) \subseteq \mathcal{R}(B)$ *and* $\mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*)$.

Proof. The operators A and B have the same matrix representations as in the previous theorem. The following products will be useful:

$$AB = \begin{bmatrix} A_1B_1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad (AB)^\dagger = \begin{bmatrix} (A_1B_1)^\dagger & 0 \\ 0 & 0 \end{bmatrix}, \qquad B^\dagger A^\dagger = \begin{bmatrix} B_1^{-1}A_1^*D^{-1} & 0 \\ 0 & 0 \end{bmatrix}.$$

First, we find the equivalent expressions for our statements in terms of A_1, A_2 and B_1.



(a) 1. $AB(AB)^\dagger = ABB^\dagger A^\dagger \Leftrightarrow A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{\;1}$. Here $A_1B_1(A_1B_1)^\dagger$ is Hermitian, so $[A_1A_1^*, D^{\;1}] = 0$.
2. $A^*AB = BB^\dagger A^*AB \Leftrightarrow A_2^*A_1 = 0$.
3. Notice that $\mathcal{R}(A^*AB) \subset \mathcal{R}(B)$ if and only if $BB^\dagger A^*AB = A^*AB$, so $2 \Leftrightarrow 3$.
4. If we check properly the Penrose equations, then we see that: $B^\dagger A^\dagger \in (AB)\{1,2,3\} \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$ and $[A_1A_1^*, D^{-1}] = 0$.

Now, we prove the following: $1 \Leftrightarrow 2$, $4 \Rightarrow 2$ and $1 \Rightarrow 4$.
We prove $1 \Leftrightarrow 2$. Notice that

$$A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{-1} \quad \Leftrightarrow \quad (A_1B_1)^\dagger = (A_1B_1)^\dagger A_1A_1^*D^{-1}.$$

The last statement is obtained by multiplying the first expression by $(A_1B_1)^\dagger$ from the left side, or multiplying the second expression by A_1B_1 from the left side, and using $A_1A_1^* = A_1B_1B_1^{-1}A_1^*$. Now, there is a chain of the equivalences:

$$\begin{aligned} (A_1B_1)^\dagger = (A_1B_1)^\dagger A_1A_1^*D^{-1} \quad &\Leftrightarrow \quad (A_1B_1)^\dagger\big(A_1A_1^* + A_2A_2^*\big) = (A_1B_1)^\dagger A_1A_1^* \\ &\Leftrightarrow \quad (A_1B_1)^\dagger A_2A_2^* = 0 \quad \Leftrightarrow \quad \mathcal{R}\big(A_2A_2^*\big) \subset \mathcal{N}\big((A_1B_1)^\dagger\big) \\ &\Leftrightarrow \quad \mathcal{R}(A_2) \subset \mathcal{N}\big((A_1B_1)^*\big) \quad \Leftrightarrow \quad B_1^*A_1^*A_2 = 0 \quad \Leftrightarrow \quad A_1^*A_2 = 0. \end{aligned}$$

Therefore, we have just proved that $1 \Leftrightarrow 2$.

Now we prove $1 \Rightarrow 4$. If we multiply $A_1B_1(A_1B_1)^\dagger = A_1A_1^*D^{-1}$ by A_1B_1 from the right side, we get $A_1A_1^*D^{-1}A_1 = A_1$. Thus, 4 holds.

Finally, we prove $4 \Rightarrow 2$. If $A_1A_1^*D^{-1}A_1 = A_1$ and $[A_1A_1^*, D^{-1}] = 0$, then $A_1A_1^*A_1 = DA_1 = A_1A_1^*A_1 + A_2A_2^*A_1$, implying that $A_2A_2^*A_1 = 0$. Hence, $\mathcal{R}(A_1) \subset \mathcal{N}(A_2A_2^*) = \mathcal{N}(A_2^*)$, so $A_2^*A_1 = 0$. Thus, 2 holds.

Notice that the equivalence $3 \Leftrightarrow 4$ is proved in [8], also.

(b) 1. $(AB)^\dagger AB = B^\dagger A^\dagger AB \Leftrightarrow (A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$. Moreover, $(A_1B_1)^\dagger A_1B_1$ is Hermitian, so $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$.
2. $ABB^* = ABB^*A^\dagger A \Leftrightarrow A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1B_1B_1^*$ and $A_1B_1B_1^*A_1^*D^{-1}A_2 = 0$.
3. Notice that $\mathcal{R}(BB^*A^*) \subset \mathcal{R}(A^*)$ if and only if $A^\dagger ABB^*A^* = BB^*A^*$, which is equivalent to $ABB^*A^\dagger A = ABB^*$. Hence, $2 \Leftrightarrow 3$.
4. The Penrose equations imply that: $B^\dagger A^\dagger \in (AB)\{1,2,4\} \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$ and $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$.

We prove $1 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1$.

Suppose that 1 holds. If we multiply $(A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$ by A_1B_1 from the left side, we obtain $A_1 = A_1A_1^*D^{-1}A_1$. Furthermore, $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$ holds. Therefore, $1 \Rightarrow 4$.

Suppose that 4 holds. Obviously, $A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1A_1^*D^{-1}A_1B_1B_1^* = A_1B_1B_1^*$. Thus, the first equality of 2 holds. The second equality of 2 also holds, since $A_1^*D^{-1}A_2 = 0 \Leftrightarrow A_1A_1^*D^{-1}A_1 = A_1$, which is shown in the proof of Theorem 2.1. Here we use again $[B_1B_1^*, A_1^*D^{-1}A_1] = 0$. Consequently, $4 \Rightarrow 2$.

In order to prove that $2 \Rightarrow 1$, we multiply $A_1B_1B_1^*A_1^*D^{-1}A_1 = A_1B_1B_1^*$ by $(A_1B_1)^\dagger$ from the left side. It follows that $B_1^*A_1^*D^{-1}A_1 = (A_1B_1)^\dagger A_1B_1B_1^*$, so $(A_1B_1)^\dagger A_1B_1 = B_1^*A_1^*D^{-1}A_1(B_1^*)^{-1}$ which is equivalent to $(A_1B_1)^\dagger A_1B_1 = B_1^{-1}A_1^*D^{-1}A_1B_1$. Hence, $2 \Rightarrow 1$.

Notice that $3 \Leftrightarrow 4$ is also proved in [8].

Finally, the part (c) follows from the parts (a) and (b). □

We also prove the following result.

Theorem 2.3. *Let X, Y, Z be Hilbert spaces, and let $A \in \mathcal{L}(Y,Z)$, $B \in \mathcal{L}(X,Y)$ be such that A, B, AB have closed ranges. Then we have:*

✓ (a) $AB(AB)^\dagger A = ABB^\dagger \Leftrightarrow A^*ABB^\dagger = BB^\dagger A^*A \Leftrightarrow \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,3\}$;
✓ (b) $B(AB)^\dagger AB = A^\dagger AB \Leftrightarrow A^\dagger ABB^* = BB^*A^\dagger A \Leftrightarrow \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,4\}$;
✓ (c) *The following three statements are equivalent:*
  ✓ (1) $(AB)^\dagger = B^\dagger A^\dagger$;
  ✓ (2) $AB(AB)^\dagger A = ABB^\dagger$ *and* $B(AB)^\dagger AB = A^\dagger AB$;
  ✓ (3) $A^*ABB^\dagger = BB^\dagger A^*A$ *and* $A^\dagger ABB^* = BB^*A^\dagger A$.

Proof. The operators A and B have the same matrix representations as in the previous theorem. First, we find equivalent expressions, in the terms of A_1, A_2 and B_1, for our assumptions.

Break time!!!

A common problem

Theorem A, B matrices such that AB exists.

$$B^\dagger(ABB^\dagger)^\dagger = (A^\dagger AB)^\dagger A^\dagger = B^\dagger A^\dagger \quad \Rightarrow \quad (AB)^\dagger = B^\dagger A^\dagger$$

A common problem

Theorem A, B matrices such that AB exists.

$$B^\dagger(ABB^\dagger)^\dagger \;=\; (A^\dagger AB)^\dagger A^\dagger \;=\; B^\dagger A^\dagger \quad\Rightarrow\quad (AB)^\dagger \;=\; B^\dagger A^\dagger$$

Correctness of this theorem translates into

$$(ab)^\dagger - b^\dagger a^\dagger \in (f_1, \ldots, f_{44})$$

A common problem

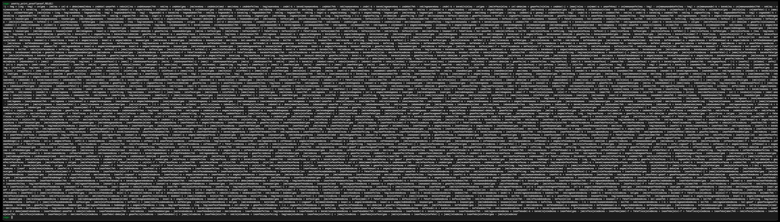
Theorem A, B matrices such that AB exists.

$$B^\dagger (ABB^\dagger)^\dagger = (A^\dagger AB)^\dagger A^\dagger = B^\dagger A^\dagger \quad \Rightarrow \quad (AB)^\dagger = B^\dagger A^\dagger$$

Correctness of this theorem translates into

$$(ab)^\dagger - b^\dagger a^\dagger \in (f_1, \ldots, f_{44})$$

Proof



```
sage: pretty_print_proof(proof,ROLB1)
```

A common problem

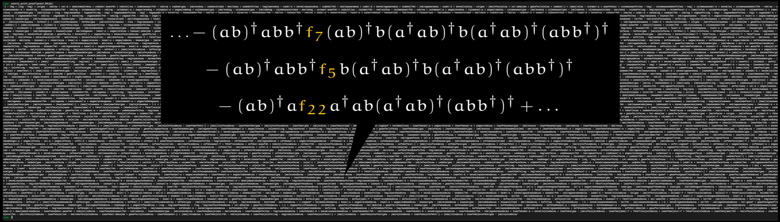
Theorem A, B matrices such that AB exists.

$$B^\dagger(ABB^\dagger)^\dagger \;=\; (A^\dagger AB)^\dagger A^\dagger \;=\; B^\dagger A^\dagger \quad\Rightarrow\quad (AB)^\dagger \;=\; B^\dagger A^\dagger$$

Correctness of this theorem translates into

$$(ab)^\dagger - b^\dagger a^\dagger \in (f_1, \dots, f_{44})$$

Proof



```
sage: pretty_print_proof(proof,RDLB1)
```

$$\dots - (ab)^\dagger abb^\dagger f_7 (ab)^\dagger b(a^\dagger ab)^\dagger b(a^\dagger ab)^\dagger (abb^\dagger)^\dagger$$

$$- (ab)^\dagger abb^\dagger f_5 b(a^\dagger ab)^\dagger b(a^\dagger ab)^\dagger (abb^\dagger)^\dagger$$

$$- (ab)^\dagger a f_{22} a^\dagger ab(a^\dagger ab)^\dagger (abb^\dagger)^\dagger + \dots$$

A common problem

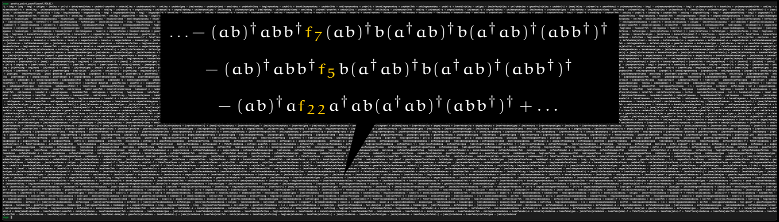
Theorem A, B matrices such that AB exists.

$$B^\dagger(ABB^\dagger)^\dagger = (A^\dagger AB)^\dagger A^\dagger = B^\dagger A^\dagger \quad \Rightarrow \quad (AB)^\dagger = B^\dagger A^\dagger$$

Correctness of this theorem translates into

$$(ab)^\dagger - b^\dagger a^\dagger \in (f_1, \ldots, f_{44})$$

Proof



```
sage: pretty_print_proof(proof,ROL81)
[illegible]
```

$$\ldots - (ab)^\dagger abb^\dagger f_7 (ab)^\dagger b(a^\dagger ab)^\dagger b(a^\dagger ab)^\dagger (abb^\dagger)^\dagger$$

$$- (ab)^\dagger abb^\dagger f_5 b(a^\dagger ab)^\dagger b(a^\dagger ab)^\dagger (abb^\dagger)^\dagger$$

$$- (ab)^\dagger a f_{22} a^\dagger ab(a^\dagger ab)^\dagger (abb^\dagger)^\dagger + \ldots$$

Another proof

$$\begin{aligned}
(ab)^\dagger - b^\dagger a^\dagger = {} & f_{21} - f_{10} + b^\dagger f_{14} - f_{12}(ab)^\dagger - b^\dagger(abb^\dagger)^\dagger f_{11} + b^\dagger(abb^\dagger)^\dagger f_{15} \\
& + (a^\dagger ab)^\dagger a^\dagger f_9 (ab)^\dagger - b^* f_{23}((ab)^\dagger)^*(ab)^\dagger - f_{21} ab(ab)^\dagger + f_{22} ab(ab)^\dagger \\
& - f_{39}(a^\dagger)^*((ab)^\dagger)^*(ab)^\dagger + b^\dagger(abb^\dagger)^\dagger((abb^\dagger)^\dagger)^*(b^\dagger)^* f_{31} - b^\dagger f_{14} d^* b^*(a^\dagger)^* \\
& + (a^\dagger ab)^\dagger a^\dagger ab f_{12}(ab)^\dagger - b^\dagger(abb^\dagger)^\dagger f_{15}((ab)^\dagger)^* b^*(a^\dagger)^* \\
& + f_{20} b^*(a^\dagger)^*((ab)^\dagger)^*(ab)^\dagger + (a^\dagger ab)^\dagger a^\dagger abb^* f_{23}((ab)^\dagger)^*(ab)^\dagger
\end{aligned}$$

A common problem

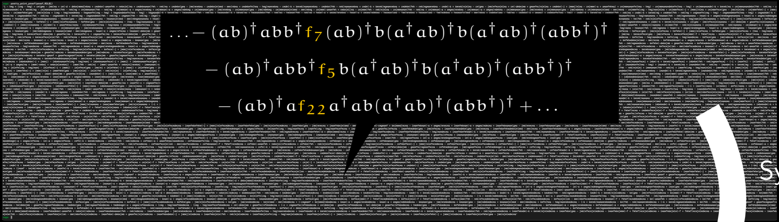
Theorem A, B matrices such that AB exists.

$$B^\dagger(ABB^\dagger)^\dagger = (A^\dagger AB)^\dagger A^\dagger = B^\dagger A^\dagger \quad \Rightarrow \quad (AB)^\dagger = B^\dagger A^\dagger$$

Correctness of this theorem translates into

$$(ab)^\dagger - b^\dagger a^\dagger \in (f_1, \ldots, f_{44})$$

Proof



```
sage: pretty_print_proof(proof,ROL81)
[illegible]
```

$$\ldots - (ab)^\dagger abb^\dagger f_7 (ab)^\dagger b(a^\dagger ab)^\dagger b(a^\dagger ab)^\dagger (abb^\dagger)^\dagger$$
$$- (ab)^\dagger abb^\dagger f_5 b(a^\dagger ab)^\dagger b(a^\dagger ab)^\dagger (abb^\dagger)^\dagger$$
$$- (ab)^\dagger a f_{22} a^\dagger ab(a^\dagger ab)^\dagger (abb^\dagger)^\dagger + \ldots$$

Syzygies
+
LP

Another proof

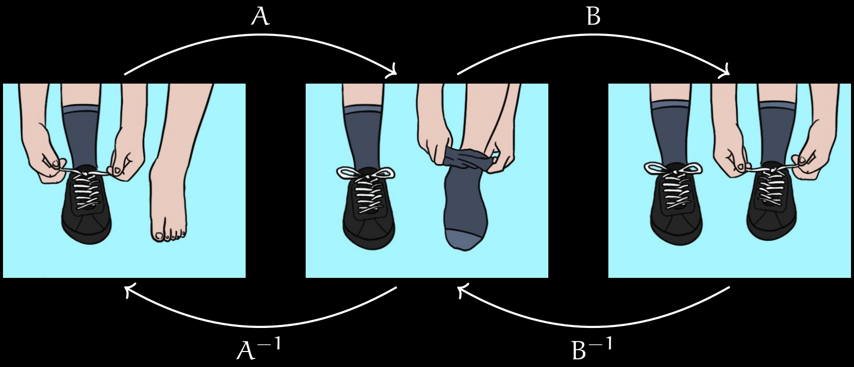
$$\begin{aligned}(ab)^\dagger - b^\dagger a^\dagger = {} & f_{21} - f_{10} + b^\dagger f_{14} - f_{12}(ab)^\dagger - b^\dagger(abb^\dagger)^\dagger f_{11} + b^\dagger(abb^\dagger)^\dagger f_{15} \\ & + (a^\dagger ab)^\dagger a^\dagger f_9 (ab)^\dagger - b^* f_{23}((ab)^\dagger)^*(ab)^\dagger - f_{21} ab(ab)^\dagger + f_{22} ab(ab)^\dagger \\ & - f_{39}(a^\dagger)^*((ab)^\dagger)^*(ab)^\dagger + b^\dagger(abb^\dagger)^\dagger((abb^\dagger)^\dagger)^*(b^\dagger)^* f_{31} - b^\dagger f_{14} d^* b^*(a^\dagger)^* \\ & + (a^\dagger ab)^\dagger a^\dagger ab f_{12}(ab)^\dagger - b^\dagger(abb^\dagger)^\dagger f_{15}((ab)^\dagger)^* b^*(a^\dagger)^* \\ & + f_{20} b^*(a^\dagger)^*((ab)^\dagger)^*(ab)^\dagger + (a^\dagger ab)^\dagger a^\dagger abb^* f_{23}((ab)^\dagger)^*(ab)^\dagger\end{aligned}$$

What about false statements?

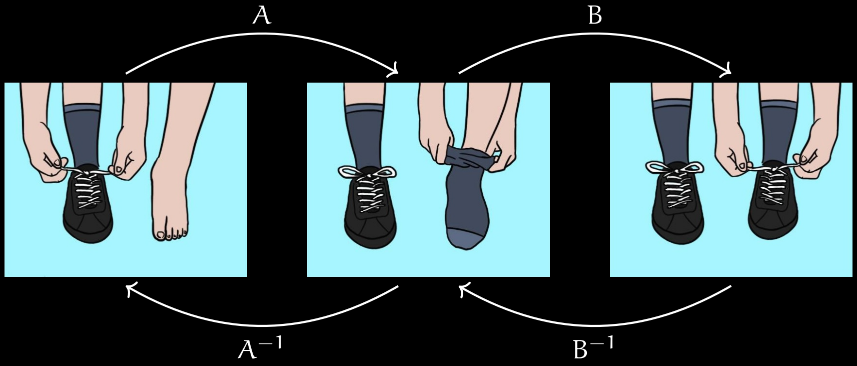
$$\forall A, B, X, Y \ : \ (AX = 1 \ \wedge \ BY = 1) \ \Rightarrow \ ABXY = 1$$

The Sock-Shoe-Principle

The Sock-Shoe-Principle



The Sock-Shoe-Principle



$$(AB)^{-1} = B^{-1}A^{-1}$$

What about false statements?

$$\forall A, B, X, Y \ : \ (AX = 1 \ \wedge \ BY = 1) \ \Rightarrow \ ABXY = 1$$

What about false statements?

$$\forall A, B, X, Y \ : \ (AX = 1 \ \wedge \ BY = 1) \ \Rightarrow \ ABXY = 1$$

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

What about false statements?

$$\forall A, B, X, Y \ : \ (AX = 1 \ \wedge \ BY = 1) \ \Rightarrow \ ABXY = 1$$

Plug in
and check

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

What about false statements?

$$\forall A, B, X, Y \;:\; (AX = 1 \;\wedge\; BY = 1) \;\Rightarrow\; ABXY = 1$$

$$\Downarrow \qquad ?$$

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

What about false statements?

$$\forall A, B, X, Y \; : \; (AX = 1 \;\wedge\; BY = 1) \;\Rightarrow\; ABXY = 1$$

Idea: make ansatz with matrices of fixed size

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \quad X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \quad Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$$

What about false statements?

$$\forall A, B, X, Y \;:\; (AX = 1 \;\wedge\; BY = 1) \;\Rightarrow\; ABXY = 1$$

Idea: make ansatz with matrices of fixed size

SAT solving + Hensel lifting

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \quad X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \quad Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$$

What about false statements?

$$\forall A, B, X, Y \; : \; (AX = 1 \;\wedge\; BY = 1) \;\Rightarrow\; ABXY = 1$$

Idea: make ansatz
with matrices
of fixed size

SAT solving
+
Hensel lifting

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

What about false statements?

$$\forall A, B, X, Y \ : \ (AX = 1 \ \wedge \ BY = 1) \ \Rightarrow \ ABXY = 1$$

Idea: make ansatz
with matrices
of fixed size

SAT solving
+
Hensel lifting

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

Does this always work? – No.

What about false statements?

$$\forall A, B, X, Y \ : \ (AX = 1 \ \wedge \ BY = 1) \ \Rightarrow \ ABXY = 1$$

Idea: make ansatz
with matrices
of fixed size

SAT solving
+
Hensel lifting

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

Does this always work? – No.

Will a better method always work? – No.

What about false statements?

$$\forall A, B, X, Y \ : \ (AX = 1 \ \wedge \ BY = 1) \ \Rightarrow \ ABXY = 1$$

Idea: make ansatz with matrices of fixed size

SAT solving + Hensel lifting

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$$

Does this always work? – No.

Will a better method always work? – No.

Does this work often enough? – Seems so.

Satisfiability of polynomial system

Given $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$

Compute a common root of $f_1, \ldots, f_r$ over $\mathbb{Q}$

Satisfiability of polynomial system

Given $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$

Compute a common root of $f_1, \dots, f_r$ over $\mathbb{Q}$

Idea Compute root over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^N} \longrightarrow \mathbb{Q}$$

Satisfiability of polynomial system

Given $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$

Compute a common root of $f_1, \dots, f_r$ over $\mathbb{Q}$

Idea Compute root over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^N} \longrightarrow \mathbb{Q}$$

Reading each x_i as a boolean variable, $\cdot$ as $\wedge$, and $+$ as XOR, the problem becomes a prop. formula. Use SAT solver to compute solution.

Satisfiability of polynomial system

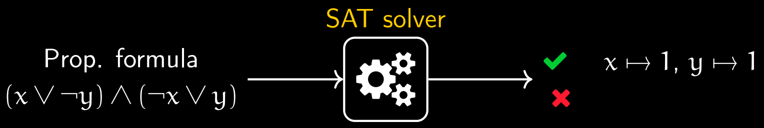
Given $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$

Compute a common root of $f_1, \dots, f_r$ over $\mathbb{Q}$

Idea Compute root over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^N} \longrightarrow \mathbb{Q}$$

Reading each x_i as a boolean variable, $\cdot$ as $\wedge$, and $+$ as XOR, the problem becomes a prop. formula. Use SAT solver to compute solution.



SAT solver

Prop. formula

$(x \vee \neg y) \wedge (\neg x \vee y)$

✓ $x \mapsto 1$, $y \mapsto 1$

✗

Satisfiability of polynomial system

Given $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$

Compute a common root of $f_1, \ldots, f_r$ over $\mathbb{Q}$

Idea Compute root over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^N} \longrightarrow \mathbb{Q}$$

Reading each x_i as a boolean variable, $\cdot$ as $\wedge$, and $+$ as XOR, the problem becomes a prop. formula. Use SAT solver to compute solution.

Given a root over $\mathbb{Z}_{2^n}$, we can lift it to a root over $\mathbb{Z}_{2^{n+1}}$ by linear algebra (Hensel lifting).

Satisfiability of polynomial system

Given $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$

Compute a common root of $f_1, \dots, f_r$ over $\mathbb{Q}$

Idea Compute root over

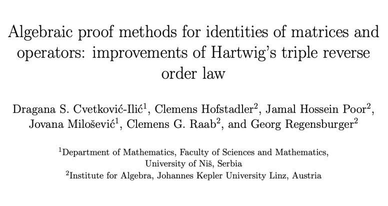
$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^N} \longrightarrow \mathbb{Q}$$

Reading each x_i as a boolean variable, $\cdot$ as $\wedge$, and $+$ as XOR, the problem becomes a prop. formula. Use SAT solver to compute solution.

Given a root over $\mathbb{Z}_{2^n}$, we can lift it to a root over $\mathbb{Z}_{2^{n+1}}$ by linear algebra (Hensel lifting).

Once we have a root over $\mathbb{Z}_{2^N}$ with N large enough, we can perform rational reconstruction to recover a root over $\mathbb{Q}$.

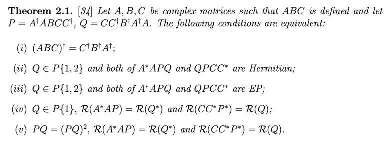
Counterexamples in practice



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

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

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



Theorem 2.1. [*34*] *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) $(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$;

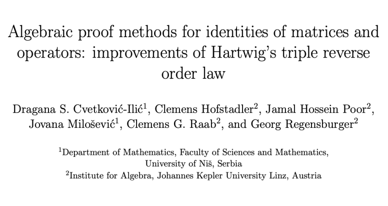
(ii) $Q \in P\{1,2\}$ *and both of* A^*APQ *and* $QPCC^*$ *are Hermitian;*

(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* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

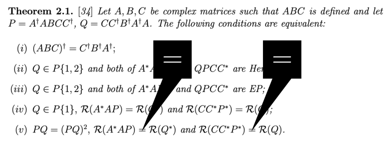
Counterexamples in practice



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

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

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



Theorem 2.1. [34] *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^*A $QPCC^*$ *are Her*

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

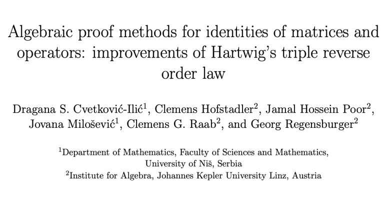
(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}($ $)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}($ $)$;

(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

$=$

$=$

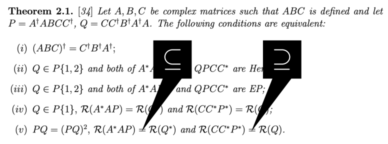
Counterexamples in practice



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

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

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



Theorem 2.1. *[34] 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^*A … $QPCC^*$ *are Her*…

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

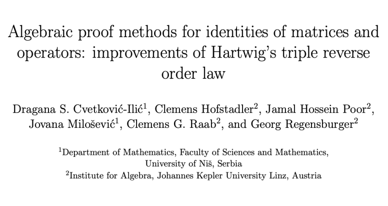
(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q$…$)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}($…$)$;

(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

$\subseteq$

$\supseteq$

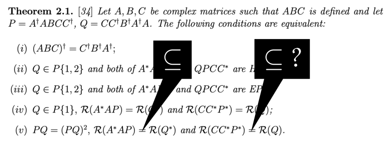
Counterexamples in practice



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

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

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



Theorem 2.1. [34] *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^*A $QPCC^*$ *are* H

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

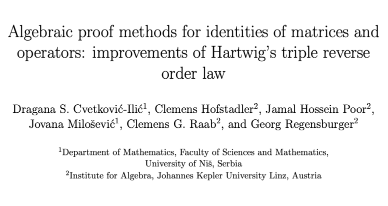
(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}($ $)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}($ $)$;

(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

$\subseteq$

$\subseteq$?

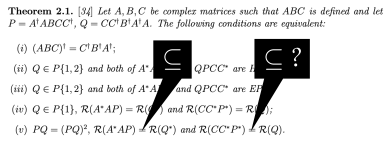
Counterexamples in practice



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

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

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



Theorem 2.1. [34] *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^*A $QPCC^*$ *are* H

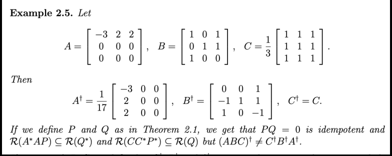
(iii) $Q \in P\{1,2\}$ *and both of* A^*A *and* $QPCC^*$ *are* EP

(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}($ $)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}($ $)$;

(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

$\subseteq$

$\subseteq$?



Example 2.5. *Let*

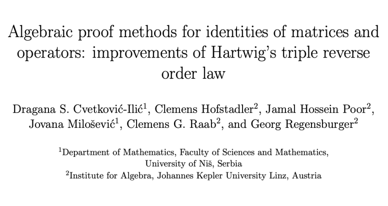
$$A = \begin{bmatrix} -3 & 2 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad C = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

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 $\mathcal{R}(A^*AP) \subseteq \mathcal{R}(Q^*)$ and $\mathcal{R}(CC^*P^*) \subseteq \mathcal{R}(Q)$ but $(ABC)^\dagger \neq C^\dagger B^\dagger A^\dagger$.

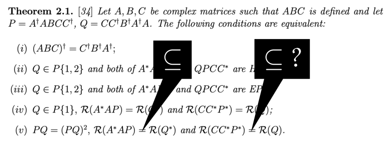
Counterexamples in practice



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

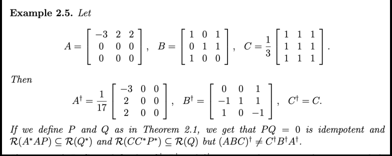
Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

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



Theorem 2.1. [34] *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^*A $QPCC^*$ *are* H
- (iii) $Q \in P\{1,2\}$ *and both of* A^*A *and* $QPCC^*$ *are* EP
- (iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}($ $)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}($ $)$;
- (v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.



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

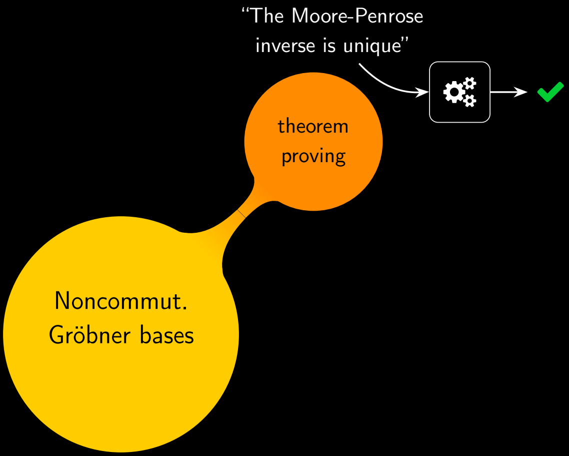
$$A^\dagger = \frac{1}{17}\begin{bmatrix} -3 & 0 & 0 \\ 2 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix}, \quad B^\dagger = \begin{bmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 1 & 0 & -1 \end{bmatrix}, \quad C^\dagger = C.$$

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

```
sage: from operator_gb import *
sage: F.<a,b,c,...> = FreeAlgebra(QQ)
sage: assumptions = [a*b*a - a,...]
sage: claim = abc_dag - c_dag*b_dag*a_dag
sage: counterexample(assumptions, claim)
```

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

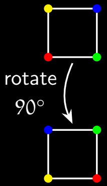
$$A^\dagger = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad B^\dagger = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad C^\dagger = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

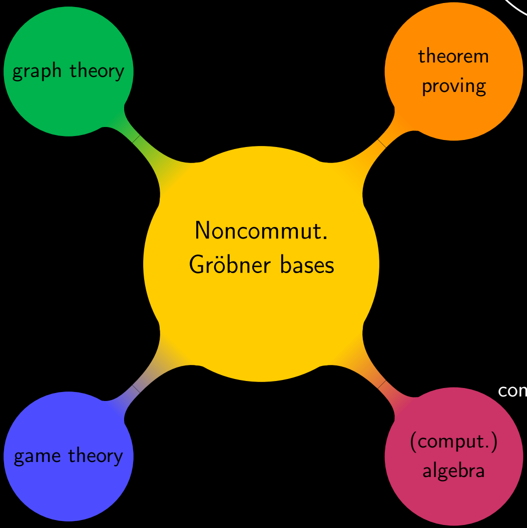


“The Moore-Penrose inverse is unique”

theorem proving

Noncommut. Gröbner bases





Noncommut. Gröbner bases

graph theory

theorem proving

game theory

(comput.) algebra

“The Moore-Penrose inverse is unique” ✓

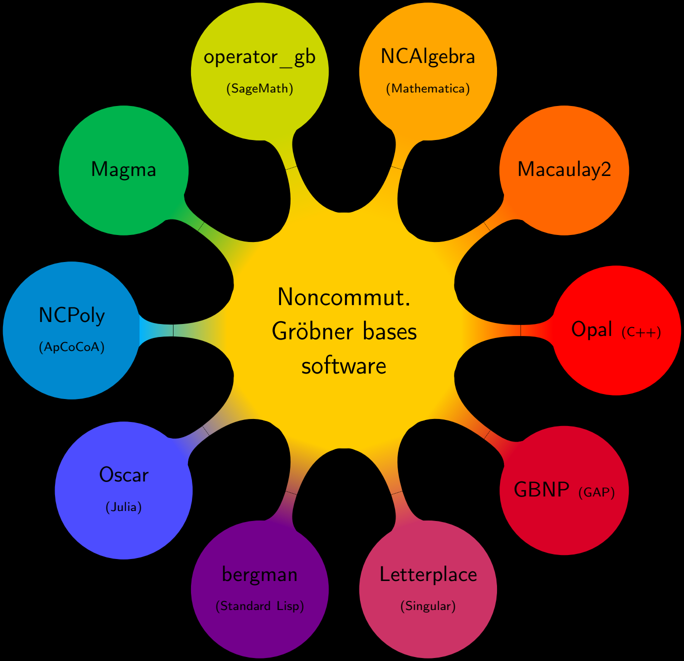
compute in $K\langle X \mid R\rangle$

$I \cap J$

$f \overset{?}{\in} I$

$\exists$ perfect commuting operator strategies

is $K\langle X \mid R\rangle$ trivial, commutative, fin. dim., etc.?



Noncommut. Gröbner bases software

operator_gb (SageMath)

NCAlgebra (Mathematica)

Macaulay2

Opal (C++)

GBNP (GAP)

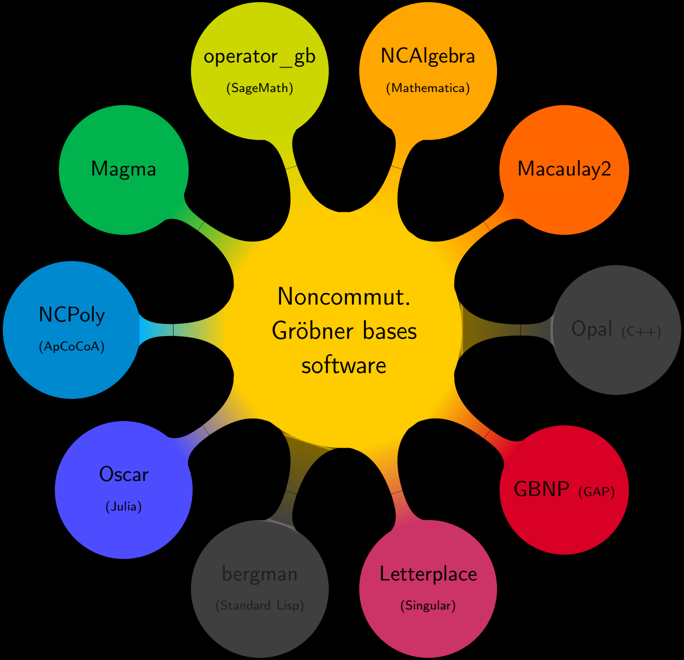
Letterplace (Singular)

bergman (Standard Lisp)

Oscar (Julia)

NCPoly (ApCoCoA)

Magma



Noncommut. Gröbner bases software

operator_gb (SageMath)

NCAlgebra (Mathematica)

Macaulay2

Opal (C++)

GBNP (GAP)

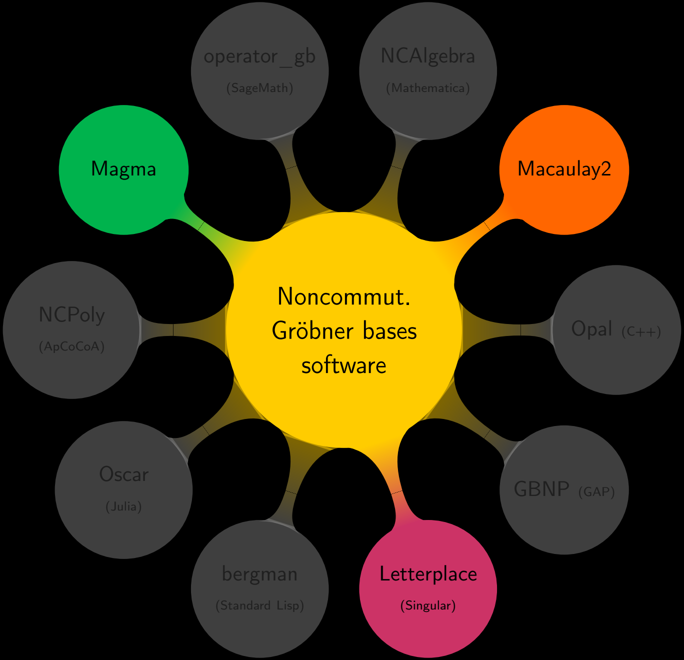
Letterplace (Singular)

bergman (Standard Lisp)

Oscar (Julia)

NCPoly (ApCoCoA)

Magma


Noncommut. Gröbner bases software

Magma

operator_gb (SageMath)

NCAlgebra (Mathematica)

Macaulay2

Opal (C++)

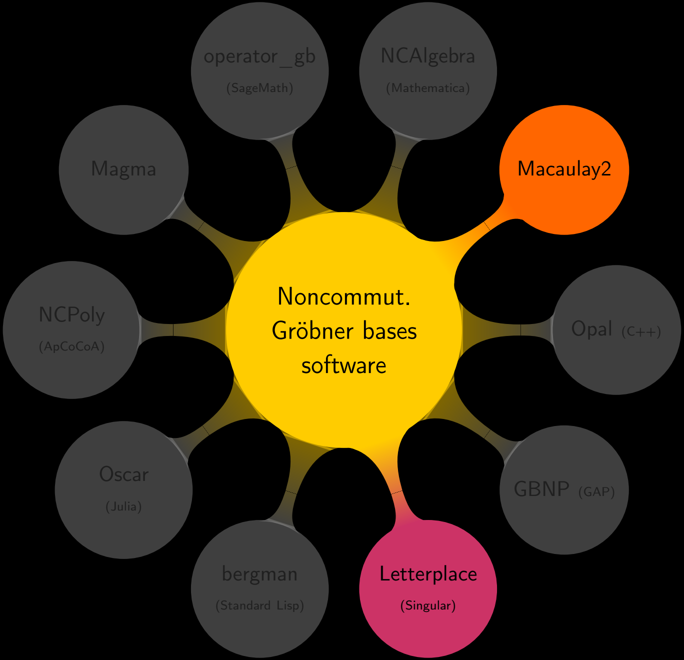
GBNP (GAP)

Letterplace (Singular)

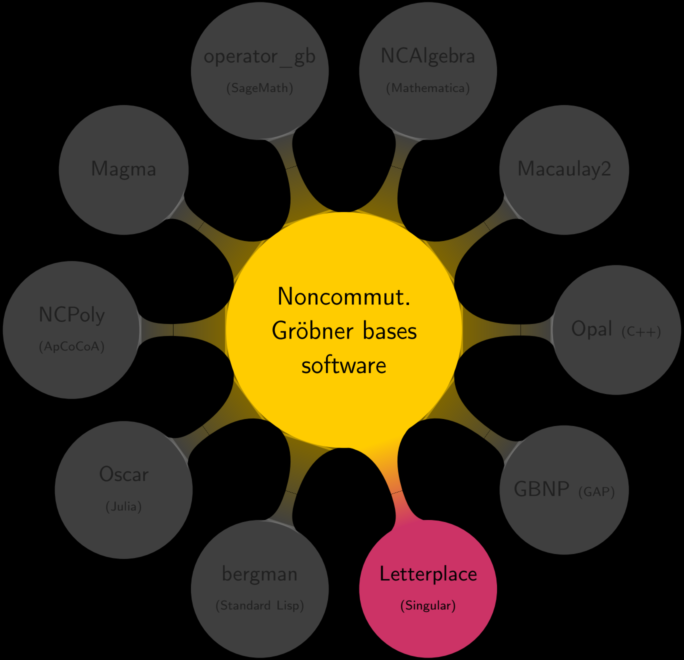
bergman (Standard Lisp)

Oscar (Julia)

NCPoly (ApCoCoA)



Noncommut. Gröbner bases software
operator_gb (SageMath)
NCAlgebra (Mathematica)
Macaulay2
Opal (C++)
GBNP (GAP)
Letterplace (Singular)
bergman (Standard Lisp)
Oscar (Julia)
NCPoly (ApCoCoA)
Magma



Noncommut. Gröbner bases software

operator_gb (SageMath)

NCAlgebra (Mathematica)

Macaulay2

Opal (C++)

GBNP (GAP)

Letterplace (Singular)

bergman (Standard Lisp)

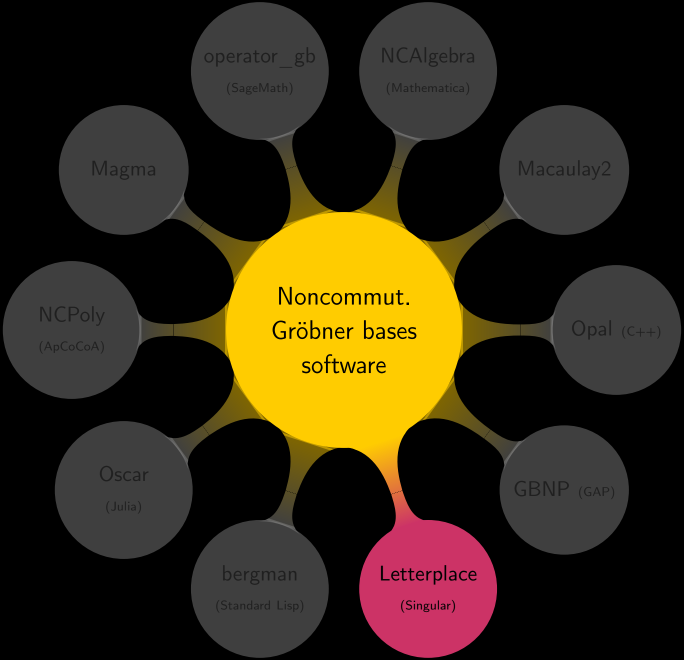
Oscar (Julia)

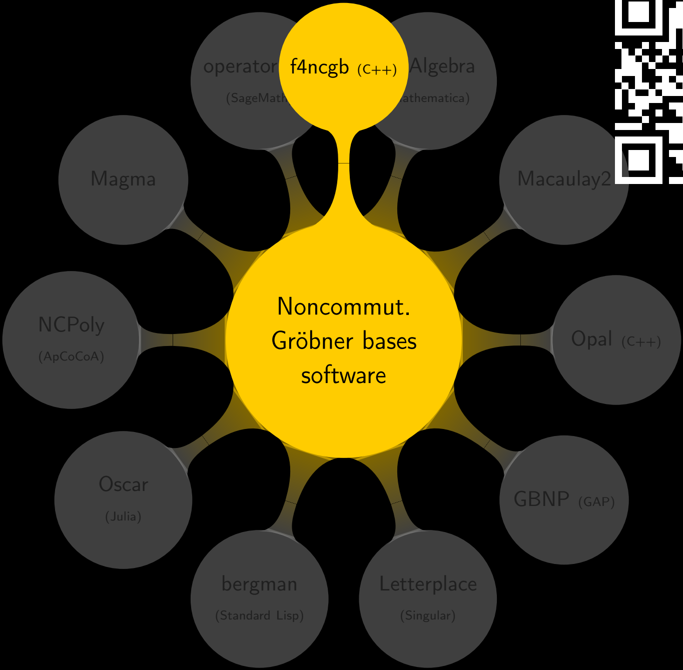
NCPoly (ApCoCoA)

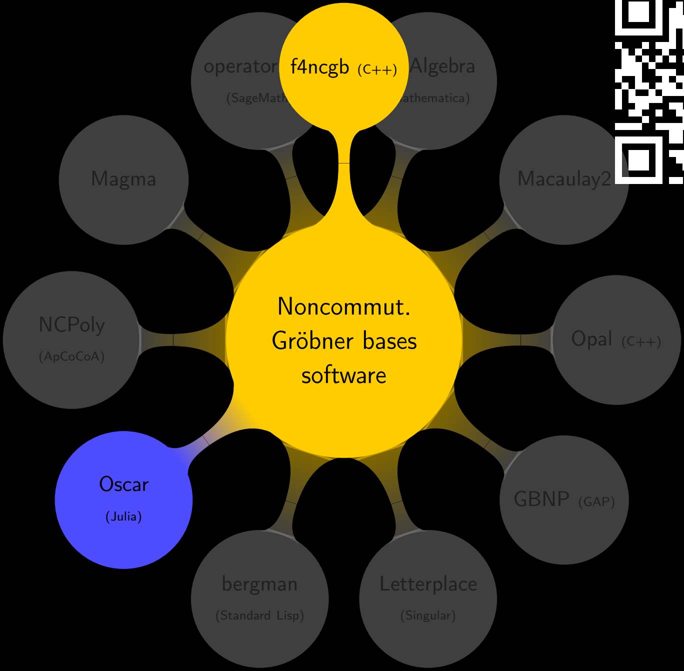
Magma

Example	Letterplace	Macaulay2	f4ncgb		
			1 core	4 cores	16 cores
4nilp5s-10	1282	875	150	79	63
braid3-16	18 953	14 291	105	34	18
braidX-18	>43 200	>43 200	1977	601	260
braidXY-12	1847	18 887	62	52	52
holt_G3562h-17	>43 200	>43 200	25 021	12 671	6824
lascala_neuh-13	171	37	9	5	4
lp1-15	24 166	33 923	266	179	155
lv2d10-100	>43 200	24 930	48	27	47
malle_G12h-100	4142	163	89	74	73

(Timings in sec)


operator_gb
(SageMath)
NCAlgebra
(Mathematica)
Magma
Macaulay2
NCPoly
(ApCoCoA)
Noncommut. Gröbner bases software
Opal (C++)
Oscar
(Julia)
GBNP (GAP)
bergman
(Standard Lisp)
Letterplace
(Singular)


Noncommut. Gröbner bases software
f4ncgb (C++)
Algebra
athematica)
Macaulay2
Opal (C++)
GBNP (GAP)
Letterplace
(Singular)
bergman
(Standard Lisp)
Oscar
(Julia)
NCPoly
(ApCoCoA)
Magma
operator
(SageMath



Noncommut. Gröbner bases software

f4ncgb (C++)

operator (SageMath

Algebra

athematica)

Magma

Macaulay2

NCPoly (ApCoCoA)

Opal (C++)

Oscar (Julia)

GBNP (GAP)

bergman (Standard Lisp)

Letterplace (Singular)

Algebraic Automated Theorem Proving

$$=$$

Proving statements about linear operators
with computer algebra

Linear operators $\longrightarrow$ noncommutative polynomials in free algebra

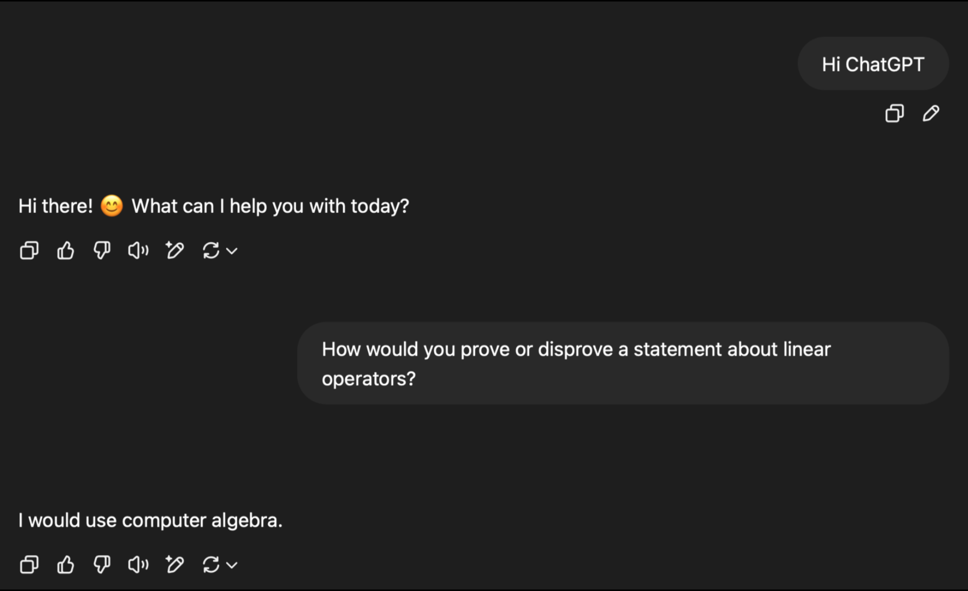
Operator statement $\longrightarrow$ ideal membership $f \overset{?}{\in} I$

Proof $\longrightarrow$ explicit linear combination

We can also. . .

. . . compute short(est) proofs of true statements.

. . . compute counterexamples for false statements.



Hi ChatGPT

Hi there! 😊 What can I help you with today?

How would you prove or disprove a statement about linear operators?

I would use computer algebra.