

How to Automate Proofs of Operator Statements: Moore-Penrose Inverse – a Case Study

Klara Bernauer¹, Clemens Hofstadler², and Georg Regensburger²

CASC 2023

Havana, Cuba, 28 August 2023

1. Institute for Algebra, Johannes Kepler University Linz, Austria
2. Institute of Mathematics, University of Kassel, Germany

U N I K A S S E L
V E R S I T Ä T

FWF

Der Wissenschaftsfonds.

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 [RMT1, pp. 44–67].

- Every $A \in \mathbb{C}^{m \times n}$ has a unique pseudo-inverse A^\dagger .
- If $A \in \mathbb{R}^{m \times n}$, then A^\dagger is real.
- 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 $A^\dagger = C^*(B^*AC^*)^{-1}B^*$.
- [LH95, p. 38] If $A \in \mathbb{C}^{m \times n}$ of rank $r \leq \min\{m, n\}$ has an SVD $A = U\Sigma V^*$, then its pseudo-inverse is $A^\dagger = V\Sigma^\dagger U^*$, where

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

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

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

- $\mathbf{0}_{mn}^\dagger = \mathbf{0}_{nm}$ and $J_{mn}^\dagger = \frac{1}{mn} J_{mn}$, 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.

- If $\mathbf{x} \neq \mathbf{0}$, $\mathbf{y} \neq \mathbf{0}$, then $(\mathbf{xy}^*)^\dagger = \frac{\mathbf{yx}^*}{\|\mathbf{x}\|^2 \|\mathbf{y}\|^2}$.

- If $\mathbf{x} \neq \mathbf{0}$, then $\mathbf{x}^\dagger = \frac{\mathbf{x}^*}{\|\mathbf{x}\|^2}$.

- Let α be a scalar. Denote

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

Then

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

$$(b) \quad (\text{diag}(\beta_1, \beta_2, \dots, \beta_n))^\dagger = \text{diag}(\beta_1^\dagger, \beta_2^\dagger, \dots, \beta_n^\dagger).$$

- $(A^\dagger)^* = (A^*)^\dagger$; $(A^\dagger)^\dagger = A$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- $AA^\dagger = \text{Proj}_{\text{range}(A)}$; $A^\dagger A = \text{Proj}_{\text{range}(A^\dagger)}$.

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

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

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

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

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

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

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

- If $A = A_1 + A_2 + \dots + A_k$, $A_i^* A_j = 0$, and $A_i A_j^* = 0$, for all $i, j = 1, \dots, k$, $i \neq j$, then $A^\dagger = A_1^\dagger + A_2^\dagger + \dots + A_k^\dagger$.

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

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

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

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

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

$$(c) \quad A^\dagger ABB^*A^* = BB^*A^* \text{ and } BB^\dagger A^*AB = A^*AB.$$

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

$$(e) \quad A^\dagger AB = B(AB)^\dagger AB \text{ and } BB^\dagger A^* = A^*AB(AB)^\dagger.$$

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

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

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

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

- 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 $\text{rank}(A_{11}) = r$. Then

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

where

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

Theory

- Model linear operators by noncomm. polynomials
- Correctness of first-order operator statements
 \iff
nc ideal membership
- Approach is complete
→ **Semi-decision procedure**

Theory

- Model linear operators by noncomm. polynomials
- Correctness of first-order operator statements
 \iff
nc ideal membership
- Approach is complete
→ **Semi-decision procedure**

Software

- SAGEMATH package `operator_gb`*
- Noncomm. Gröbner bases
- Certified nc ideal membership
- Noncomm. ideal arithmetic
- Dedicated methods for proving operator statements

* available at https://github.com/ClemensHofstadler/operator_gb

Theory

- Model linear operators by noncomm. polynomials
- Correctness of first-order operator statements
 \iff
nc ideal membership
- Approach is complete
→ **Semi-decision procedure**

Software

- SAGEMATH package `operator_gb`*
- Noncomm. Gröbner bases
- Certified nc ideal membership
- Noncomm. ideal arithmetic
- Dedicated methods for proving operator statements

* available at https://github.com/ClemensHofstadler/operator_gb

Automated proofs of operator statements

Noncommutative polynomials

Noncommutative polynomials = elements in free algebra $\mathbb{Z}\langle X \rangle$

$$= \sum_{i=1}^d c_i \cdot x_{i,1} \cdots x_{i,k_i}$$

Noncommutative polynomials

Noncommutative polynomials = elements in free algebra $\mathbb{Z}\langle X \rangle$

$$= \sum_{i=1}^d c_i \cdot x_{i,1} \dots x_{i,k_i}$$

finite words over X

Noncommutative polynomials

Noncommutative polynomials = elements in free algebra $\mathbb{Z}\langle X \rangle$

$$= \sum_{i=1}^d c_i \cdot x_{i,1} \dots x_{i,k_i}$$

finite words over X

Multiplication = Concatenation of words

$$(x_1 \dots x_k) \cdot (x'_1 \dots x'_l) = x_1 \dots x_k x'_1 \dots x'_l$$

Noncommutative polynomials

Noncommutative polynomials = elements in free algebra $\mathbb{Z}\langle X \rangle$

$$= \sum_{i=1}^d c_i \cdot x_{i,1} \dots x_{i,k_i}$$

finite words over X

Multiplication = Concatenation of words

$$(x_1 \dots x_k) \cdot (x'_1 \dots x'_l) = x_1 \dots x_k x'_1 \dots x'_l$$

Two-sided ideals For $f_1, \dots, f_r \in \mathbb{Z}\langle X \rangle$

$$(f_1, \dots, f_r) = \left\{ \sum_i \sum_j a_{i,j} \cdot f_i \cdot b_{i,j} \mid a_{i,j}, b_{i,j} \in \mathbb{Z}\langle X \rangle \right\}$$

Noncommutative polynomials

Noncommutative polynomials = elements in free algebra $\mathbb{Z}\langle X \rangle$

$$= \sum_{i=1}^d c_i \cdot x_{i,1} \dots x_{i,k_i}$$

finite words over X

Multiplication = Concatenation of words

$$(x_1 \dots x_k) \cdot (x'_1 \dots x'_l) = x_1 \dots x_k x'_1 \dots x'_l$$

Two-sided ideals For $f_1, \dots, f_r \in \mathbb{Z}\langle X \rangle$

$$(f_1, \dots, f_r) = \left\{ \sum_i \sum_j a_{i,j} \cdot f_i \cdot b_{i,j} \mid a_{i,j}, b_{i,j} \in \mathbb{Z}\langle X \rangle \right\}$$

Fact Ideal membership problem $f \stackrel{?}{\in} (f_1, \dots, f_r)$ is semi-decidable (e.g., using Gröbner bases)

Operator statements

Operators

- $0, a, b, c, \dots$
- $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.

Operator statements

Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.

Operator statements

Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.



R

Operator statements

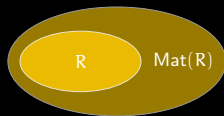
Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.



Operator statements

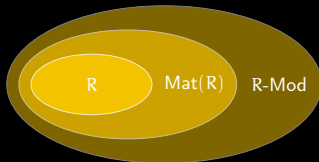
Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.



Operator statements

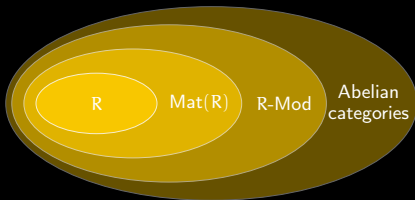
Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.



Operator statements

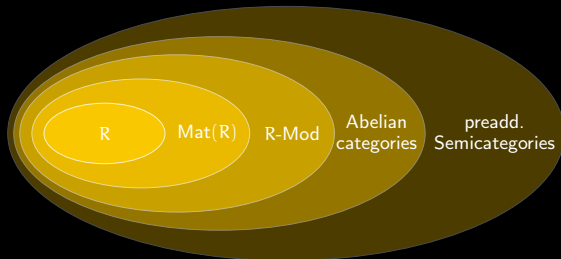
Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.



Operator statements

Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

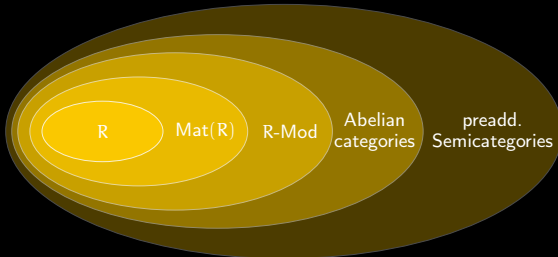
• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.

Operator statements

$s = t, \neg \varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi), \exists x : \varphi, \forall x : \varphi$



Operator statements

Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

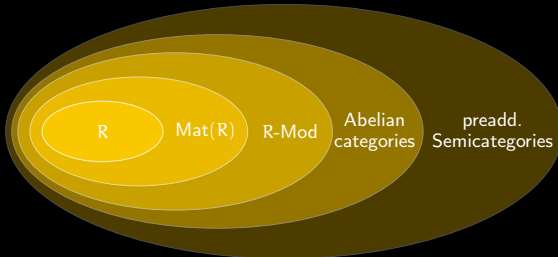
• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.

Operator statements

$s = t, \neg \varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi), \exists x : \varphi, \forall x : \varphi$

Definition An operator statement is **universally true** if it follows from linearity



Operator statements

Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.

Operator statements

$s = t, \neg \varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi), \exists x : \varphi, \forall x : \varphi$

Definition An operator statement is **universally true** if it follows from linearity

- **Fact:** Determining universal truth is **not decidable**
 \Rightarrow Algorithm that terminates on all inputs **cannot exist**

Operator statements

Operators

$*, \cdot^T, \|\cdot\|, \otimes, \dots$

• $0, a, b, c, \dots$

• $s + t, s \cdot t, f(t_1, \dots, t_n)$

Linearity = abelian (partial) addition + assoc. (partial) mult. + dist.

Operator statements

$s = t, \neg \varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi), \exists x : \varphi, \forall x : \varphi$

Definition An operator statement is **universally true** if it follows from linearity

- **Fact:** Determining universal truth is **not decidable**
⇒ Algorithm that terminates on all inputs **cannot exist**
- Best we can hope for: **(effective) semi-decision procedure**
→ Can be obtained using computer algebra

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Quasi-identities

- Classical case of **quasi-identities** well studied (Helton, Stankus, Wavrik '98, Schmitz, Levandovskyy '20, Raab, Regensburger, Hossein Poor '21)

$$\forall \mathbf{X} : \bigwedge_{j=1}^m A_j = B_j \Rightarrow P = Q$$

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Quasi-identities

- Classical case of **quasi-identities** well studied (Helton, Stankus, Wavrik '98, Schmitz, Levandovskyy '20, Raab, Regensburger, Hossein Poor '21)

$$\forall \mathbf{X} : \bigwedge_{j=1}^m A_j = B_j \Rightarrow P = Q$$

Strategy

- Interpret each operator as polynomial in $\mathbb{Z}\langle \mathbf{X} \rangle$ and reformulate each identity $L = R$ as polynomial $L - R$
e.g., $AB = BA \rightsquigarrow ab - ba \in \mathbb{Z}\langle a, b \rangle$
- “Being a consequence” (\Rightarrow) translates into ideal membership

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Quasi-identities

- Classical case of **quasi-identities** well studied (Helton, Stankus, Wavrik '98, Schmitz, Levandovskyy '20, Raab, Regensburger, Hossein Poor '21)

$$\forall \mathbf{X} : \bigwedge_{j=1}^m A_j = B_j \Rightarrow P = Q$$

Strategy

- Interpret each operator as polynomial in $\mathbb{Z}\langle \mathbf{X} \rangle$ and reformulate each identity $L = R$ as polynomial $L - R$
e.g., $AB = BA \rightsquigarrow ab - ba \in \mathbb{Z}\langle a, b \rangle$
- “Being a consequence” (\Rightarrow) translates into ideal membership

Theorem

$$\forall \mathbf{X} : \bigwedge_{j=1}^m A_j = B_j \Rightarrow P = Q \quad \text{iff} \quad p - q \in (\mathbf{a}_1 - \mathbf{b}_1, \dots, \mathbf{a}_m - \mathbf{b}_m)$$

“The Moore-Penrose inverse is unique”

"The Moore-Penrose inverse is unique"

Recall: B is Moore-Penrose inverse of A if

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

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

“The Moore-Penrose inverse is unique”

Recall: B is Moore-Penrose inverse of A if

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

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

Proof Using our software package `operator_gb...`

“The Moore-Penrose inverse is unique”

Recall: B is Moore-Penrose inverse of A if

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

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"

Recall: B is Moore-Penrose inverse of A if

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

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)
```

$$\begin{aligned} b - c = & (-c + c*a*c) + b*c_adj*(-a_adj + a_adj*b_adj*a_adj) \\ & - b*a*c*(-a*b + b_adj*a_adj) - b*(-a + a*c*a)*b \\ & + b*(-a*c + c_adj*a_adj) - b*(-a*c + c_adj*a_adj)*b_adj*a_adj \\ & - (-b + b*a*b) + (-c*a + a_adj*c_adj)*b*a*c \\ & - (-a_adj + a_adj*c_adj*a_adj)*b_adj*c + c*(-a + a*b*a)*c \\ & - (-b*a + a_adj*b_adj)*c + a_adj*c_adj*(-b*a + a_adj*b_adj)*c \end{aligned}$$

"The Moore-Penrose inverse is unique"

Recall: B is Moore-Penrose inverse of A if

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

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)
```

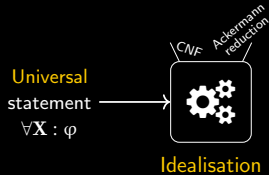
$$\begin{aligned} b - c = & (-c + c*a*c) + b*c_adj*(-a_adj + a_adj*b_adj*a_adj) \\ & - b*a*c*(-a*b + b_adj*a_adj) - b*(-a + a*c*a)*b \\ & + b*(-a*c + c_adj*a_adj) - b*(-a*c + c_adj*a_adj)*b_adj*a_adj \\ & - (-b + b*a*b) + (-c*a + a_adj*c_adj)*b*a*c \\ & - (-a_adj + a_adj*c_adj*a_adj)*b_adj*c + c*(-a + a*b*a)*c \\ & - (-b*a + a_adj*b_adj)*c + a_adj*c_adj*(-b*a + a_adj*b_adj)*c \end{aligned}$$

- Software produces **cofactor representation** (= certificate for ideal membership)
- Cofactor representation is **algebraic proof** requiring only linearity \Rightarrow Statement is **proven in all settings** where linearity holds

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

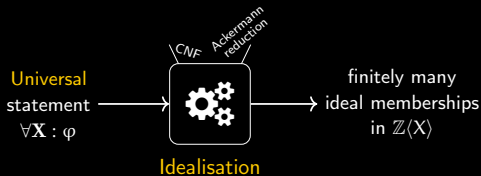
Universal statements



Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

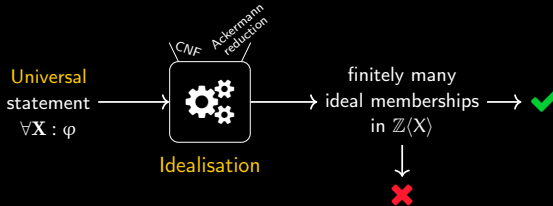
Universal statements



Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Universal statements



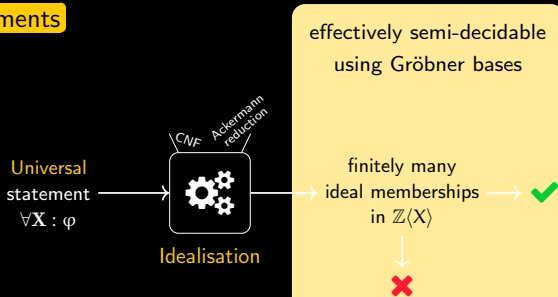
Theorem (H., Raab, Regensburger '22)

A universal statement is universally true iff its idealisation is true

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Universal statements



Theorem (H., Raab, Regensburger '22)

A universal statement is universally true iff its idealisation is true

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].

- ✓ 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.
- ✓ 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 $A^\dagger = C^*(B^*AC^*)^{-1}B^*$.
- ✓ [LH95, p. 38] If $A \in \mathbb{C}^{m \times n}$ of rank $r \leq \min\{m, n\}$ has an SVD $A = U\Sigma V^*$, then its pseudo-inverse is $A^\dagger = V\Sigma^\dagger U^*$, where

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

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

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

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

- 7. If $\mathbf{x} \neq \mathbf{0}$, $\mathbf{y} \neq \mathbf{0}$, then $(\mathbf{xy}^*)^\dagger = \frac{\mathbf{yx}^*}{\|\mathbf{x}\|^2 \|\mathbf{y}\|^2}$.

- 8. If $\mathbf{x} \neq \mathbf{0}$, then $\mathbf{x}^\dagger = \frac{\mathbf{x}^*}{\|\mathbf{x}\|^2}$.

- ✓ Let α be a scalar. Denote

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

Then

$$\text{✓ } (\alpha A)^\dagger = \alpha^\dagger A^\dagger.$$

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

- ✓ $(A^\dagger)^* = (A^*)^\dagger$; $(A^\dagger)^\dagger = A$.
- ✓ If A is a nonsingular square matrix, then $A^\dagger = A^{-1}$.
- ✓ If U has orthonormal columns or orthonormal rows, then $U^\dagger = U^*$.
- ✓ If $A = A^*$ and $A = A^2$, then $A^\dagger = A$.
- ✓ $A^\dagger = A^*$ 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 $(A^k)^\dagger = (A^\dagger)^k$.
- ✓ If $U \in \mathbb{C}^{m \times n}$ is of rank n and satisfies $U^\dagger = U^*$, then U has orthonormal columns.
- ✓ 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,
 - ✓ if $A \in \mathbb{C}^{m \times n}$ ($m \geq n$) has full rank n , then $A^\dagger = (A^*A)^{-1}A^*$;
 - ✓ if $A \in \mathbb{C}^{m \times n}$ ($m \leq n$) has full rank m , then $A^\dagger = A^*(AA^*)^{-1}$.
- 19. Let $A \in \mathbb{C}^{m \times n}$. Then

$$\text{✓ } A^\dagger A, AA^\dagger, I_n - A^\dagger A, \text{ and } I_m - AA^\dagger \text{ are orthogonal projections.}$$

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

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

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

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

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

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

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

$$\text{✓ } \ker(A) = \ker(A^*A) = \ker(A^\dagger A).$$

$$\text{✓ } \ker(A^\dagger) = \ker(A^*) = \ker(AA^*) = \ker(AA^\dagger).$$

$$\text{(c) } \text{range}(A^\dagger A) \oplus \ker(A^\dagger A) = \mathbb{F}^n.$$

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

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

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

$$\text{✓ } (A^*A)^\dagger = A^\dagger(A^*)^\dagger; \quad (AA^*)^\dagger = (A^\dagger)^\dagger A^\dagger.$$

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

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

$$\text{✓ } A^\dagger ABB^* \text{ and } A^*ABB^\dagger \text{ are both Hermitian matrices.}$$

$$\text{✓ } A^\dagger ABB^*A^* = BB^*A^* \text{ and } BB^\dagger A^*AB = A^*AB.$$

$$\text{✓ } A^\dagger ABB^*A^*ABB^\dagger = BB^*A^*A.$$

$$\text{✓ } A^\dagger AB = B(AB)^\dagger AB \text{ and } BB^\dagger A^* = A^*AB(AB)^\dagger.$$

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

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

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

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

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 $\text{rank}(A_{11}) = r$. Then

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

where

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

“Every matrix has a Moore-Penrose inverse”

“Every matrix has a Moore-Penrose inverse”

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

Claim $\exists X : (PA^*A = A \wedge AA^*Q = A) \Rightarrow \text{pinv}(A, X)$

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

Claim $\exists X : (PA^*A = A \wedge AA^*Q = A) \Rightarrow \text{pinv}(A, X)$

Strategy

- 1 Derive explicit expression for X
- 2 Reformulate statement as a universal statement
- 3 Prove by verifying ideal membership

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

Claim $\exists X : (PA^*A = A \wedge AA^*Q = A) \Rightarrow \text{pinv}(A, X)$

Strategy

- 1 Derive explicit expression for X
- 2 Reformulate statement as a universal statement
- 3 Prove by verifying ideal membership

Proof Using our software package `operator_gb...`

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

Claim $\exists X : (PA^*A = A \wedge AA^*Q = A) \Rightarrow \text{pinv}(A, X)$

Strategy

- 1 Derive explicit expression for X
- 2 Reformulate statement as a universal statement
- 3 Prove by verifying ideal membership

Proof Using our software package `operator_gb...`

```
sage: assumptions = [a - p*a_adj*a,...]
sage: I = NCIdeal(assumptions + pinv(a,x))
sage: I.find_equivalent_expression(x)
```

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

Claim $\exists X : (PA^*A = A \wedge AA^*Q = A) \Rightarrow \text{pinv}(A, X)$

Strategy

- 1 Derive explicit expression for X
- 2 Reformulate statement as a universal statement
- 3 Prove by verifying ideal membership

Proof Using our software package `operator_gb...`

```
sage: assumptions = [a - p*a_adj*a, ...]
sage: I = NCIdeal(assumptions + pinv(a,x))
sage: I.find_equivalent_expression(x)

[x - a_adj*q*x, x - a_adj*p*x,
 x - a_adj*q*p_adj, x - a_adj*x_adj*x]
```

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

Claim $\exists X : (PA^*A = A \wedge AA^*Q = A) \Rightarrow \text{pinv}(A, X)$

Strategy

- 1 Derive explicit expression for X
- 2 Reformulate statement as a universal statement
- 3 Prove by verifying ideal membership

Proof Using our software package `operator_gb...`

```
sage: assumptions = [a - p*a_adj*a, ...]
sage: I = NCIdeal(assumptions + pinv(a,x))
sage: I.find_equivalent_expression(x)
[x - a_adj*q*x, x - a_adj*p*x,
 x - a_adj*q*p_adj, x - a_adj*x_adj*x]
```

“Every matrix has a Moore-Penrose inverse”

Fact: A matrix $\Rightarrow \exists P, Q : PA^*A = A$ and $AA^*Q = A$

Claim $\exists X : (PA^*A = A \wedge AA^*Q = A) \Rightarrow \text{pinv}(A, X)$

Strategy

- 1 Derive explicit expression for X
- 2 Reformulate statement as a universal statement
- 3 Prove by verifying ideal membership

Proof Using our software package `operator_gb...`

```
sage: assumptions = [a - p*a_adj*a, ...]
sage: I = NCIdeal(assumptions + pinv(a,x))
sage: I.find_equivalent_expression(x)
```

```
[x - a_adj*q*x, x - a_adj*p*x,
  x - a_adj*q*p_adj, x - a_adj*x_adj*x]
```

$\Rightarrow X = A^*QP^*$ is MP-inverse of A
(can be certified using the software)

Existential statements

In the previous example, we found a suitable expression.

Question Was this just luck?

Existential statements

In the previous example, we found a suitable expression.

Question Was this just luck? – **No!**

Existential statements

In the previous example, we found a suitable expression.

Question Was this just luck? – **No!**

Reason **Herbrand's theorem** (Herbrand '30)

An existential statement is universally true if and only if explicit expressions exist and can be constructed as polynomial expressions in terms of the basic operators appearing in the statement.

Existential statements


In the previous example, we found a suitable expression.

Question Was this just luck? – **No!**

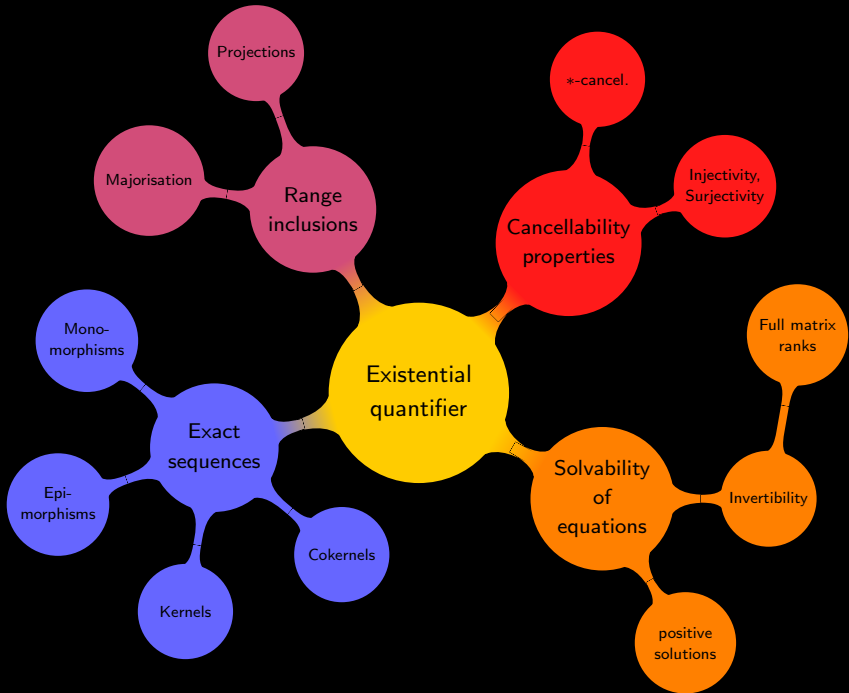
Reason **Herbrand's theorem** (Herbrand '30)

An existential statement is universally true if and only if explicit expressions exist and can be constructed as polynomial expressions in terms of the basic operators appearing in the statement.

- Enumerating all possible expressions is hopeless
- Requires **good heuristics** → provided by **computer algebra**
- Several heuristics implemented in `operator_gb`
(ansatz, variable elimination, ideal/subalgebra intersections, . . .)



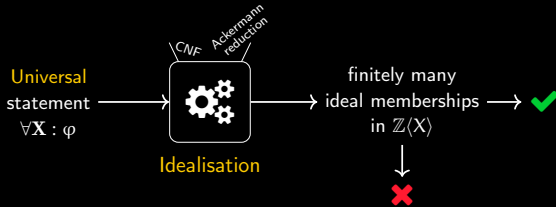
Existential
quantifier



Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Universal statements



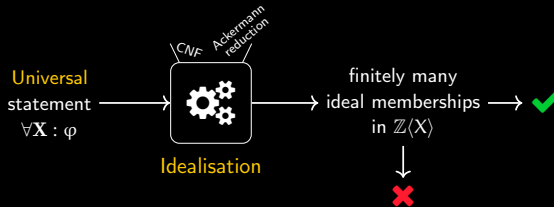
Theorem (H., Raab, Regensburger '22)

A universal statement is universally true iff its idealisation is true

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

Universal statements



Theorem (H., Raab, Regensburger '22)

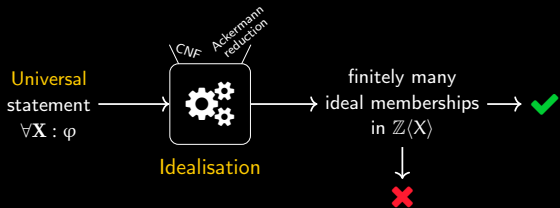
A universal statement is universally true iff its idealisation is true

To treat **all operator statements** \rightsquigarrow combine with **Herbrand's theorem**
+ **Heuristics**

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

General operator statements



Theorem (H., Raab, Regensburger '22)

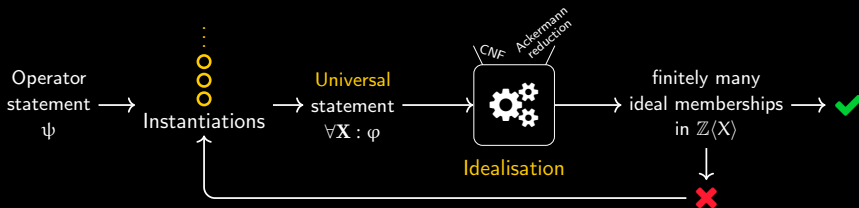
A universal statement is universally true iff its idealisation is true

To treat **all operator statements** \rightsquigarrow combine with **Herbrand's theorem**
+ **Heuristics**

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

General operator statements



Theorem (H., Raab, Regensburger '22)

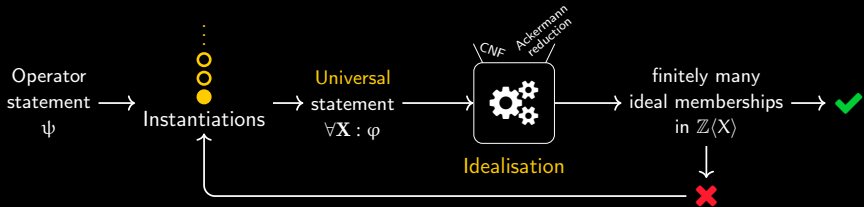
A universal statement is universally true iff its idealisation is true

To treat **all operator statements** \rightsquigarrow combine with **Herbrand's theorem**
+ **Heuristics**

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

General operator statements



Theorem (H., Raab, Regensburger '22)

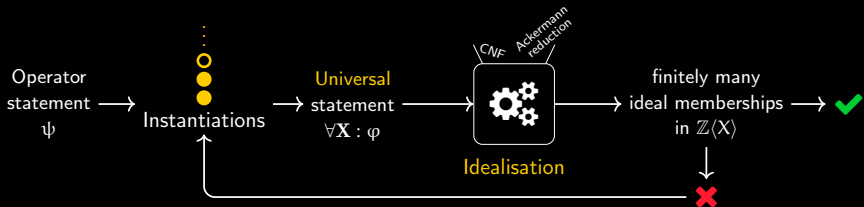
A universal statement is universally true iff its idealisation is true

To treat **all operator statements** \rightsquigarrow combine with **Herbrand's theorem**
+ **Heuristics**

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

General operator statements



Theorem (H., Raab, Regensburger '22)

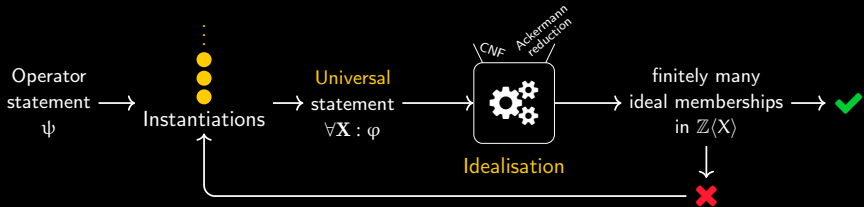
A universal statement is universally true iff its idealisation is true

To treat **all operator statements** \rightsquigarrow combine with **Herbrand's theorem**
+ **Heuristics**

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

General operator statements



Theorem (H., Raab, Regensburger '22)

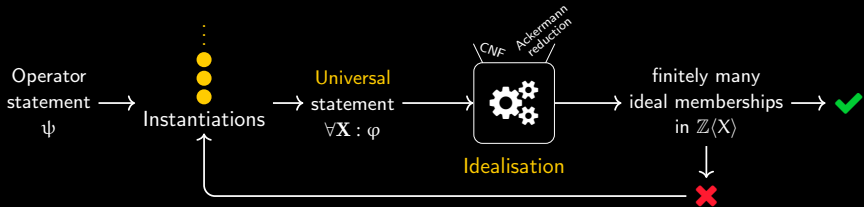
A universal statement is universally true iff its idealisation is true

To treat **all operator statements** \rightsquigarrow combine with **Herbrand's theorem**
+ **Heuristics**

Determining universal truth

Idea Translate universal truth of formula into polynomial predicate

General operator statements



Theorem (H., Raab, Regensburger '22)

An operator statement is universally true iff the procedure terminates and returns \checkmark

To treat **all operator statements** \rightsquigarrow combine with **Herbrand's theorem** + **Heuristics**

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].

- ✓ Every $A \in \mathbb{C}^{m \times n}$ has a unique pseudo-inverse A^\dagger .
- ✓ If $A \in \mathbb{R}^{m \times n}$, then A^\dagger is real.
- ✓ 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 $A^\dagger = C^*(B^*AC^*)^{-1}B^*$.
- ✗ [LH95, p. 38] If $A \in \mathbb{C}^{m \times n}$ of rank $r \leq \min\{m, n\}$ has an SVD $A = U\Sigma V^*$, then its pseudo-inverse is $A^\dagger = V\Sigma^\dagger U^*$, where

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

- ✗ [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

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

- ✓ $\mathbf{0}_{mn}^{\dagger} = \mathbf{0}_{nm}$ and $J_{mn}^{\dagger} = \frac{1}{mn} J_{mn}$, 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.

✓ If $\mathbf{x} \neq \mathbf{0}$, $\mathbf{y} \neq \mathbf{0}$, then $(\mathbf{xy}^*)^\dagger = \frac{\mathbf{yx}^*}{\|\mathbf{x}\|^2 \|\mathbf{y}\|^2}.$

✓ If $\mathbf{x} \neq \mathbf{0}$, then $\mathbf{x}^\dagger = \frac{\mathbf{x}^*}{\|\mathbf{x}\|^2}.$

- ✓ Let α be a scalar. Denote

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

Then

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

✗ $(\text{diag}(\beta_1, \beta_2, \dots, \beta_n))^\dagger = \text{diag}(\beta_1^\dagger, \beta_2^\dagger, \dots, \beta_n^\dagger).$

- ✗ $(A^\dagger)^* = (A^*)^\dagger; \quad (A^\dagger)^\dagger = A.$
- ✗ If A is a nonsingular square matrix, then $A^\dagger = A^{-1}.$
- ✗ If U has orthonormal columns or orthonormal rows, then $U^\dagger = U^*.$
- ✗ If $A = A^*$ and $A = A^2$, then $A^\dagger = A.$
- ✗ $A^\dagger = A^*$ if and only if A^*A is idempotent.
- ✗ If A is normal and k is a positive integer, then $AA^\dagger = A^\dagger A$ and $(A^k)^\dagger = (A^\dagger)^k.$
- ✗ If $U \in \mathbb{C}^{m \times n}$ is of rank n and satisfies $U^\dagger = U^*$, then U has orthonormal columns.
- ✗ If $U \in \mathbb{C}^{m \times m}$ and $V \in \mathbb{C}^{n \times n}$ are unitary matrices, then $(UAV)^\dagger = V^*A^\dagger U^*.$
- ✗ $A^\dagger = (A^*A)^\dagger A^* = A^*(AA^*)^\dagger.$ In particular,
 - ✓ if $A \in \mathbb{C}^{m \times n}$ ($m \geq n$) has full rank n , then $A^\dagger = (A^*A)^{-1}A^*;$
 - ✓ if $A \in \mathbb{C}^{m \times n}$ ($m \leq n$) has full rank m , then $A^\dagger = A^*(AA^*)^{-1}.$
- ✗ Let $A \in \mathbb{C}^{m \times n}$. Then

- ✓ $A^\dagger A, AA^\dagger, I_n - A^\dagger A,$ and $I_m - AA^\dagger$ are orthogonal projections.
- ✗ $\text{rank}(A) = \text{rank}(A^\dagger) = \text{rank}(AA^\dagger) = \text{rank}(A^\dagger A).$
- ✗ $\text{rank}(I_n - A^\dagger A) = \text{rank}(A) = n - \text{rank}(A).$
- ✗ $\text{rank}(I_m - AA^\dagger) = m - \text{rank}(A).$
- ✗ $AA^\dagger = \text{Proj}_{\text{range}(A)}; \quad A^\dagger A = \text{Proj}_{\text{range}(A^\dagger)}.$
- ✗ Suppose that $A \in F^{m \times n}$, where $F = \mathbb{C}$ or \mathbb{R} . Then
 - ✓ $\text{range}(A) = \text{range}(AA^*) = \text{range}(AA^\dagger).$
 - ✓ $\text{range}(A^\dagger) = \text{range}(A^*) = \text{range}(A^*A) = \text{range}(A^\dagger A).$
 - ✓ $\ker(A) = \ker(A^*A) = \ker(A^\dagger A).$
 - ✓ $\ker(A^\dagger) = \ker(A^*) = \ker(AA^*) = \ker(AA^\dagger).$
 - ✓ $\text{range}(A^\dagger A) \oplus \ker(A^\dagger A) = F^m.$
 - ✓ $\text{range}(AA^\dagger) \oplus \ker(AA^\dagger) = F^m.$
- ✗ If $A = A_1 + A_2 + \dots + A_k, A_i A_j^* = 0,$ and $A_i A_j^* = 0,$ for all $i, j = 1, \dots, k, i \neq j,$ then $A^\dagger = A_1^\dagger + A_2^\dagger + \dots + A_k^\dagger.$
- ✗ If A is an $m \times r$ matrix of rank r and B is an $r \times n$ matrix of rank r , then $(AB)^\dagger = B^\dagger A^\dagger.$
- ✗ $(A^*)^\dagger = A^\dagger(A^\dagger)^\dagger; \quad (AA^*)^\dagger = (A^\dagger)^\dagger A^\dagger.$
- ✗ [Gre66] Each one of the following conditions is necessary and sufficient for $(AB)^\dagger = B^\dagger A^\dagger:$
 - ✓ $\text{range}(BB^*A^*) \subseteq \text{range}(A^*)$ and $\text{range}(A^*AB) \subseteq \text{range}(B).$
 - ✓ $A^\dagger ABB^*$ and A^*ABB^\dagger are both Hermitian matrices.
 - ✓ $A^\dagger ABB^*A^* = BB^*A^*$ and $BB^\dagger A^*AB = A^*AB.$
 - ✓ $A^\dagger ABB^*A^*ABB^\dagger = BB^*A^*A.$
 - ✓ $A^\dagger AB = B(AB)^\dagger AB$ and $BB^\dagger A^* = A^*AB(AB)^\dagger.$
- ✗ $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger,$ where \otimes denotes the Kronecker product.
- ✗ $A^\dagger = \lim_{\alpha \rightarrow 0} A^*(\alpha I + AA^*)^{-1} = \lim_{\alpha \rightarrow 0} (\alpha I + A^*A)^{-1} A^*.$
- ✗ $A^\dagger = \sum_{j=1}^{\infty} A^*(I + AA^*)^{-j} = \sum_{j=1}^{\infty} (I + A^*A)^{-j} A^*.$
- ✗ (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 $\lim_{E \rightarrow 0} (A + E)^\dagger = A^\dagger$ if and only if there is $\epsilon > 0$ such that $\text{rank}(A + E) = \text{rank}(A)$ when $\|E\|_2 \leq \epsilon.$
- ✗ 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 $\text{rank}(A_{11}) = r.$ Then

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

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

Applications

- Handbook of Linear Algebra (20 ✓ / 6 ✓ / 4 ✗)

Applications

- Handbook of Linear Algebra (20 ✓ / 6 ✓ / 4 ✗)
 - yields ideals with ≤ 70 generators in ≤ 18 indeterminates
 - cofactor representations consist of ≤ 226 terms
 - all proofs take ~ 15 seconds altogether

Applications

- Handbook of Linear Algebra (20 ✓ / 6 ✓ / 4 ✗)
 - yields ideals with ≤ 70 generators in ≤ 18 indeterminates
 - cofactor representations consist of ≤ 226 terms
 - all proofs take ~ 15 seconds altogether
- Recent results in operator theory
 - *Reverse order law of the Moore-Penrose inverse* (Djordjević, Dinčić '09)
 - they: *We use [. . .] decompositions of Hilbert spaces*
 - we: purely algebraic proofs \Rightarrow our proofs **generalise results**

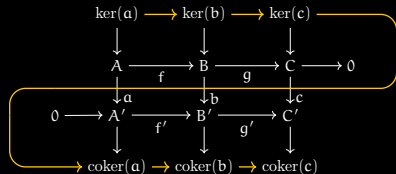
Applications

- Handbook of Linear Algebra (20 ✓ / 6 ✓ / 4 ✗)
 - yields ideals with ≤ 70 generators in ≤ 18 indeterminates
 - cofactor representations consist of ≤ 226 terms
 - all proofs take ~ 15 seconds altogether
- Recent results in operator theory
 - *Reverse order law of the Moore-Penrose inverse* (Djordjević, Dinčić '09)
 - they: *We use [. . .] decompositions of Hilbert spaces*
 - we: purely algebraic proofs \Rightarrow our proofs **generalise results**
- New results (Cvetković-Ilić, H., Hossein Poor, Milošević, Raab, Regensburger '21)
 - software used to **find minimal assumptions**

Applications

- Handbook of Linear Algebra (20 ✓ / 6 ✓ / 4 ✗)
 - yields ideals with ≤ 70 generators in ≤ 18 indeterminates
 - cofactor representations consist of ≤ 226 terms
 - all proofs take ~ 15 seconds altogether
- Recent results in operator theory
 - *Reverse order law of the Moore-Penrose inverse* (Djordjević, Dinčić '09)
 - they: *We use [...] decompositions of Hilbert spaces*
 - we: purely algebraic proofs \Rightarrow our proofs **generalise results**
- New results (Cvetković-Ilić, H., Hossein Poor, Milošević, Raab, Regensburger '21)
 - software used to **find minimal assumptions**

- Diagram lemmas (Five lemma, Nine lemma, Snake lemma, ...)



F

Hi chatGPT



Hello! How can I assist you today?



F

Imagine you are a mathematician and you want to prove a statement about linear operators.
What do you do?



I would use computer algebra.



 Regenerate response

Send a message



Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT May 24 Version](#)