Noncommutative Gröbner Bases

Theory, Applications, and Software

Clemens Hofstadler
RISC, JKU Linz, Austria
ALBATROSS, Paris, 4 September 2026

JOHANNES KEPLER
UNIVERSITY LINZ

Noncommutative $=$ really noncommutative

$$\begin{aligned}\text{Noncommutative} &= \text{really noncommutative}\\ &= \text{free algebra } K\langle X\rangle = K\langle x_1, \dots, x_n\rangle\end{aligned}$$

$$\begin{aligned}\text{Noncommutative} &= \text{really noncommutative}\\ &= \text{free algebra } K\langle X\rangle = K\langle x_1,\ldots,x_n\rangle\end{aligned}$$

Noncom. polynomial $\quad c_1\cdot w_1+\cdots+c_d\cdot w_d \quad \in K\langle X\rangle$

$$\begin{aligned} \text{Noncommutative} &= \text{really noncommutative} \\ &= \text{free algebra } K\langle X\rangle = K\langle x_1, \ldots, x_n\rangle \end{aligned}$$

Noncom. polynomial $\quad \underbrace{\boxed{c_1} \cdot w_1 + \cdots + \boxed{c_d}}_{\in K} \cdot w_d \quad \in K\langle X\rangle$

$$\begin{aligned}\text{Noncommutative} &= \text{really noncommutative}\\ &= \text{free algebra } K\langle X\rangle = K\langle x_1, \ldots, x_n\rangle\end{aligned}$$

$\in K$

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

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

$$\begin{aligned}\text{Noncommutative} &= \text{really noncommutative}\\ &= \text{free algebra } K\langle X\rangle = K\langle x_1,\ldots,x_n\rangle\end{aligned}$$

Noncom. polynomial $\quad \overbrace{\boxed{c_1}\cdot\boxed{w_1}+\cdots+\boxed{c_d}\cdot\boxed{w_d}}^{\in K} \quad \in K\langle X\rangle$

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

$$xyyx + 2xyz - zyx - 2zz \quad \in \mathbb{Q}\langle x,y,z\rangle$$

$$\text{Noncommutative} = \text{really noncommutative}$$
$$= \text{free algebra } K\langle X\rangle = K\langle x_1, \ldots, x_n\rangle$$

Noncom. polynomial $\quad \overbrace{\boxed{c_1}}^{\in K} \cdot \underbrace{\boxed{w_1}}_{\text{words over } X = \{x_1,\ldots,x_n\}} + \cdots + \overbrace{\boxed{c_d}}^{\in K} \cdot \underbrace{\boxed{w_d}}_{\text{words over } X = \{x_1,\ldots,x_n\}} \quad \in K\langle X\rangle$

$$xyyx + 2xyz - zyx - 2zz \quad \in \mathbb{Q}\langle x, y, z\rangle$$

Addition $\quad (xy - z) + (yx + 2z) = xy + yx + z$

Multiplication $\quad (xy - z) \cdot (yx + 2z) = xyyx + 2xyz - zyx - 2zz$

A nonempty set $I \subseteq K\langle X\rangle$ is a (two-sided) ideal if

$$\begin{aligned} f, g \in I \quad &\Rightarrow \quad f + g \in I \\ f \in I,\ p, q \in K\langle X\rangle \quad &\Rightarrow \quad p \cdot f \cdot q \in I \end{aligned}$$

Ideal generated by $f_1, \ldots, f_r$ denoted by $I = (f_1, \ldots, f_r)$.

A nonempty set $I \subseteq K\langle X\rangle$ is a (two-sided) ideal if

$$\begin{aligned} f, g \in I \quad &\Rightarrow \quad f + g \in I \\ f \in I,\ p, q \in K\langle X\rangle \quad &\Rightarrow \quad p \cdot f \cdot q \in I \end{aligned}$$

Ideal generated by $f_1, \ldots, f_r$ denoted by $I = (f_1, \ldots, f_r)$.

⚠ $K\langle X\rangle$ is not Noetherian! e.g., $(xy^nx \mid n \in \mathbb{N}) \subseteq K\langle x, y\rangle$

A nonempty set $I \subseteq K\langle X\rangle$ is a (two-sided) ideal if

$$f, g \in I \;\Rightarrow\; f + g \in I$$

$$f \in I,\; p, q \in K\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$$

Ideal generated by $f_1, \ldots, f_r$ denoted by $I = (f_1, \ldots, f_r)$.

⚠ $K\langle X\rangle$ is not Noetherian! e.g., $(xy^n x \mid n \in \mathbb{N}) \subseteq K\langle x, y\rangle$

This talk: Gröbner basis theory for finitely generated two-sided ideals.

A nonempty set $I \subseteq K\langle X\rangle$ is a (two-sided) ideal if

$$f, g \in I \quad \Rightarrow \quad f + g \in I$$
$$f \in I,\ p, q \in K\langle X\rangle \quad \Rightarrow \quad p \cdot f \cdot q \in I$$

Ideal generated by $f_1, \ldots, f_r$ denoted by $I = (f_1, \ldots, f_r)$.

$K\langle X\rangle$ is not Noetherian! e.g., $(xy^n x \mid n \in \mathbb{N}) \subseteq K\langle x, y\rangle$

This talk: Gröbner basis theory for finitely generated two-sided ideals.

Noncomm. GB theory $=$ comm. GB theory $-$ finiteness

A nonempty set $I \subseteq K\langle X\rangle$ is a (two-sided) ideal if

$$f, g \in I \;\Rightarrow\; f + g \in I$$
$$f \in I,\ p, q \in K\langle X\rangle \;\Rightarrow\; p \cdot f \cdot q \in I$$

Ideal generated by $f_1, \ldots, f_r$ denoted by $I = (f_1, \ldots, f_r)$.

⚠ $K\langle X\rangle$ is not Noetherian! e.g., $(xy^n x \mid n \in \mathbb{N}) \subseteq K\langle x, y\rangle$

This talk: Gröbner basis theory for finitely generated two-sided ideals.

Noncomm. GB theory $=$ comm. GB theory $-$ finiteness

($\exists$ GB theory for fin. gen. **one-sided** ideals, but that is **trivial**.)

Good news Most of the commutative theory carries over.

Good news Most of the commutative theory carries over.

Reduction if $\mathrm{lm}(f) = a \cdot \mathrm{lm}(g) \cdot b$, then $f \;\rightarrow_g\; f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb$

Good news Most of the commutative theory carries over.

Reduction if $\mathrm{lm}(f) = a \cdot \mathrm{lm}(g) \cdot b$, then $f \rightarrow_g f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb$

Gröbner basis

G is a Gröbner basis of I if $\quad f \in I \iff f \xrightarrow{*}_G 0$

Good news Most of the commutative theory carries over.

Reduction if $\mathrm{lm}(f) = a \cdot \mathrm{lm}(g) \cdot b$, then $f \rightarrow_g f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb$

Gröbner basis

G is a Gröbner basis of I if $f \in I \iff f \xrightarrow{*}_G 0$

S-polynomials lcm-construction $\rightsquigarrow$ overlap & inclusion ambiguities

Good news Most of the commutative theory carries over.

Reduction if $\mathrm{lm}(f) = a \cdot \mathrm{lm}(g) \cdot b$, then $f \rightarrow_g f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb$

Gröbner basis

G is a Gröbner basis of I if $\quad f \in I \iff f \xrightarrow{*}_G 0$

S-polynomials lcm-construction $\rightsquigarrow$ overlap & inclusion ambiguities

commutative

$$\begin{aligned} f &= \quad + \cdots \\ g &= \quad + \cdots \end{aligned}$$

SPol $\quad f - \quad g$

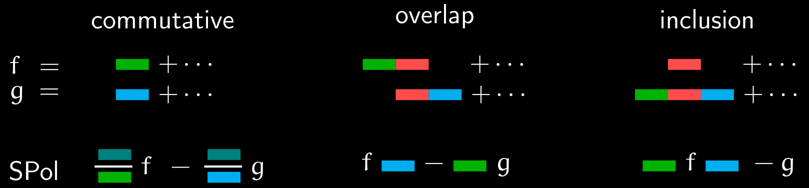
Good news Most of the commutative theory carries over.

Reduction if $\mathrm{lm}(f) = a \cdot \mathrm{lm}(g) \cdot b$, then $f \;\to_g\; f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb$

Gröbner basis

G is a Gröbner basis of I if $\quad f \in I \iff f \xrightarrow{*}_G 0$

S-polynomials lcm-construction $\rightsquigarrow$ overlap & inclusion ambiguities



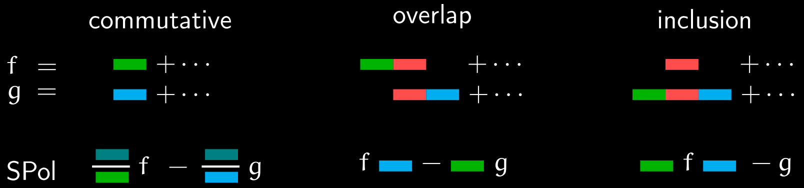
Good news Most of the commutative theory carries over.

Reduction if $\mathrm{lm}(f) = a \cdot \mathrm{lm}(g) \cdot b$, then $f \to_g f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb$

Gröbner basis

G is a Gröbner basis of I if $f \in I \iff f \xrightarrow{*}_G 0$

S-polynomials lcm-construction $\rightsquigarrow$ overlap & inclusion ambiguities



Algorithms Buchberger, F4, F5 all generalize to $K\langle X\rangle$ (and $R\langle X\rangle$).

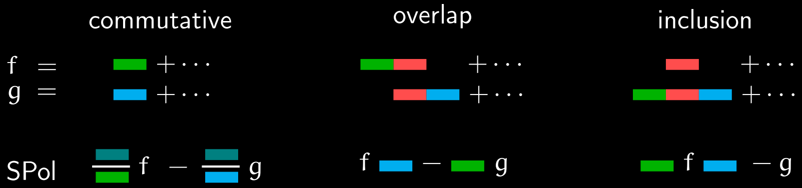
Good news Most of the commutative theory carries over.

Reduction if $\mathrm{lm}(f) = a \cdot \mathrm{lm}(g) \cdot b$, then $f \to_g f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} \cdot agb$

Gröbner basis

G is a Gröbner basis of I if $f \in I \iff f \xrightarrow{*}_G 0$

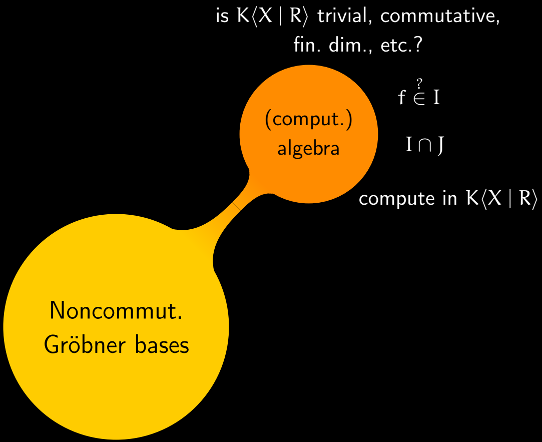
S-polynomials lcm-construction $\rightsquigarrow$ overlap & inclusion ambiguities

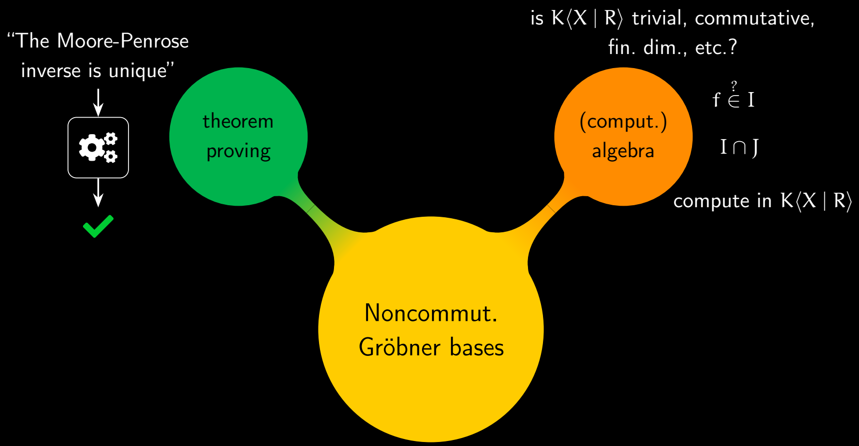


Algorithms Buchberger, F4, F5 all generalize to $K\langle X\rangle$ (and $R\langle X\rangle$).

Bad news Algorithms need not terminate.

Noncommut.
Gröbner bases


is $K\langle X \mid R\rangle$ trivial, commutative,
fin. dim., etc.?
$f \overset{?}{\in} I$
(comput.)
algebra
$I \cap J$
compute in $K\langle X \mid R\rangle$
Noncommut.
Gröbner bases



"The Moore-Penrose inverse is unique"
theorem proving
Noncommut. Gröbner bases
(comput.) algebra
is $K\langle X \mid R\rangle$ trivial, commutative, fin. dim., etc.?
$f \overset{?}{\in} I$
$I \cap J$
compute in $K\langle X \mid R\rangle$

"The Moore-Penrose inverse is unique"

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

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

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

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

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

$$\Longleftrightarrow$$

$$b - c \in (f_1, \ldots, f_{12})$$

"The Moore-Penrose inverse is unique"

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

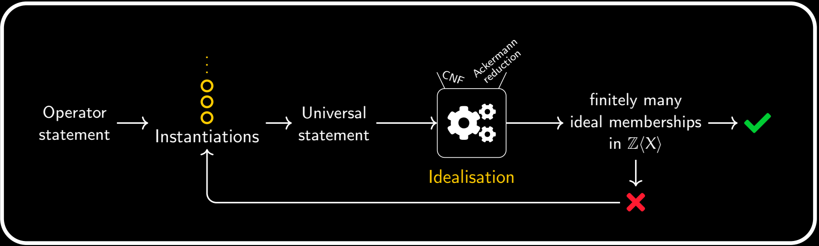
$$aba - a, \qquad bab - b, \qquad b^*a^* - ab, \qquad a^*b^* - ba$$

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

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

$$\Longleftrightarrow$$

$$b - c \in (f_1, \ldots, f_{12})$$



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:*

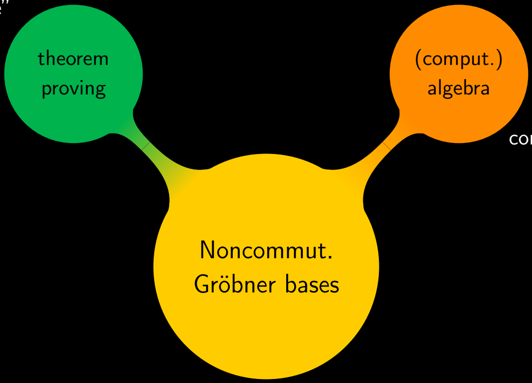
(a) $AB(AB)^\dagger A = ABB^\dagger \Leftrightarrow A^*ABB^\dagger = BB^\dagger A^*A \Leftrightarrow \mathcal{R}(A^*AB) \subseteq \mathcal{R}(B) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,3\}$;
(b) $B(AB)^\dagger AB = A^\dagger AB \Leftrightarrow A^\dagger ABB^* = BB^*A^\dagger A \Leftrightarrow \mathcal{R}(BB^*A^*) \subseteq \mathcal{R}(A^*) \Leftrightarrow B^\dagger A^\dagger \in (AB)\{1,2,4\}$;
(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”

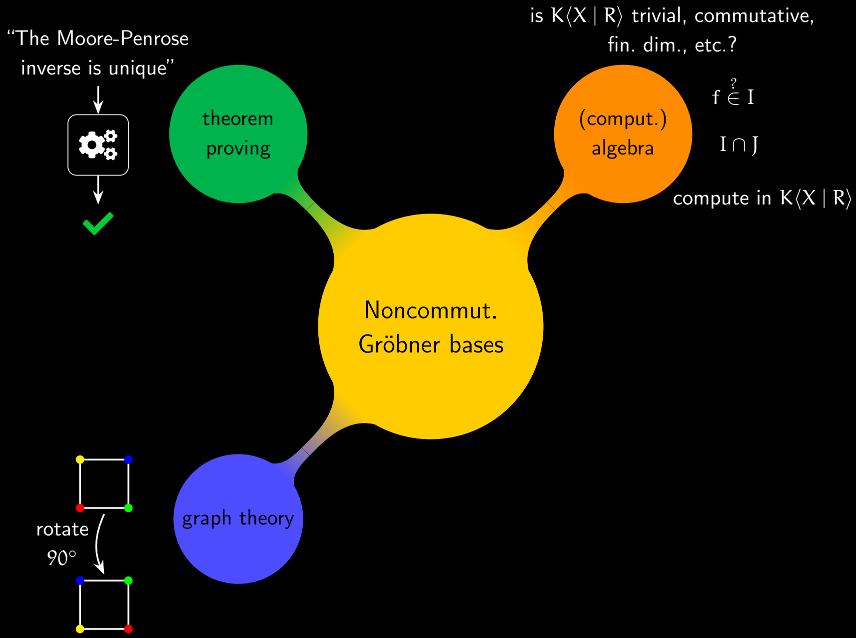
is $K\langle X \mid R\rangle$ trivial, commutative, fin. dim., etc.?



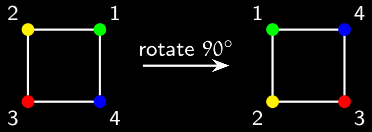
$f \overset{?}{\in} I$

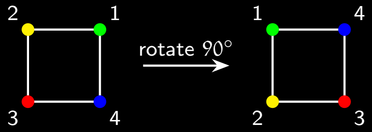
$I \cap J$

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



“The Moore-Penrose inverse is unique”
theorem proving
is K⟨X | R⟩ trivial, commutative, fin. dim., etc.?
(comput.) algebra
$f \overset{?}{\in} I$
$I \cap J$
compute in K⟨X | R⟩
Noncommut. Gröbner bases
graph theory
rotate 90°


2
1
3
4
rotate 90°
1
4
2
3

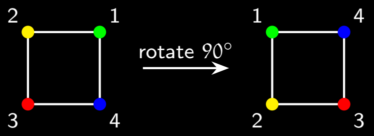


Classical symmetry

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

P permutation matrix s.t.

P commutes with adjacency matrix



Classical symmetry

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

P permutation matrix s.t.

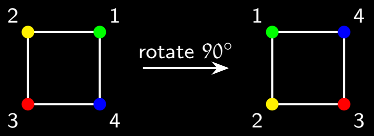
P commutes with adjacency matrix

Quantum symmetry

$$U = \begin{pmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ u_{21} & u_{22} & u_{23} & u_{24} \\ u_{31} & u_{32} & u_{33} & u_{34} \\ u_{41} & u_{42} & u_{43} & u_{44} \end{pmatrix}$$

u_{ij} are **noncommuting** objects s.t.

1. U commutes with adjacency matrix
2. $\sum_k u_{ik} = \sum_k u_{ki} = 1$
3. $u_{ij} = u_{ij}^* = u_{ij}^2$



Classical symmetry

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

P permutation matrix s.t.

P commutes with adjacency matrix

Quantum symmetry

$$U = \begin{pmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ u_{21} & u_{22} & u_{23} & u_{24} \\ u_{31} & u_{32} & u_{33} & u_{34} \\ u_{41} & u_{42} & u_{43} & u_{44} \end{pmatrix}$$

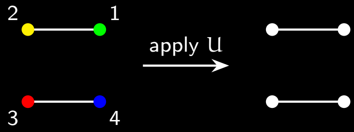
u_{ij} are **noncommuting** objects s.t.

1. U commutes with adjacency matrix
2. $\sum_k u_{ik} = \sum_k u_{ki} = 1$
3. $u_{ij} = u_{ij}^* = u_{ij}^2$

Graph has quantum symmetries

$$\Longleftrightarrow$$

$$[u_{ij}, u_{kl}] \notin (\mathbf{1.}, \mathbf{2.}, \mathbf{3.})$$



Classical symmetry

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

P permutation matrix s.t.

P commutes with adjacency matrix

Quantum symmetry

$$\mathfrak{U} = \begin{pmatrix} p & 1-p & 0 & 0 \\ 1-p & p & 0 & 0 \\ 0 & 0 & q & 1-q \\ 0 & 0 & 1-q & q \end{pmatrix}$$

u_{ij} are **noncommuting** objects s.t.

1. $\mathfrak{U}$ commutes with adjacency matrix

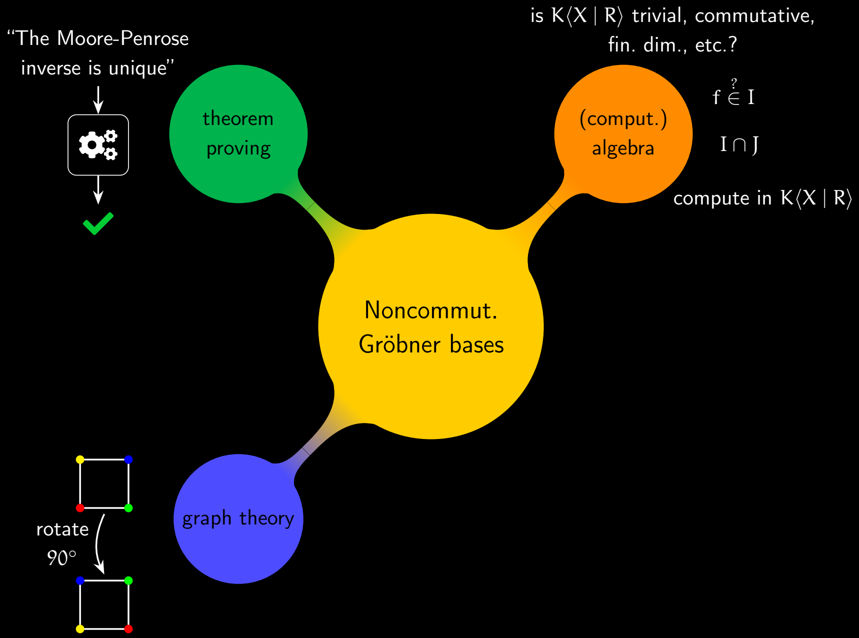
2. $\sum_k u_{ik} = \sum_k u_{ki} = 1$

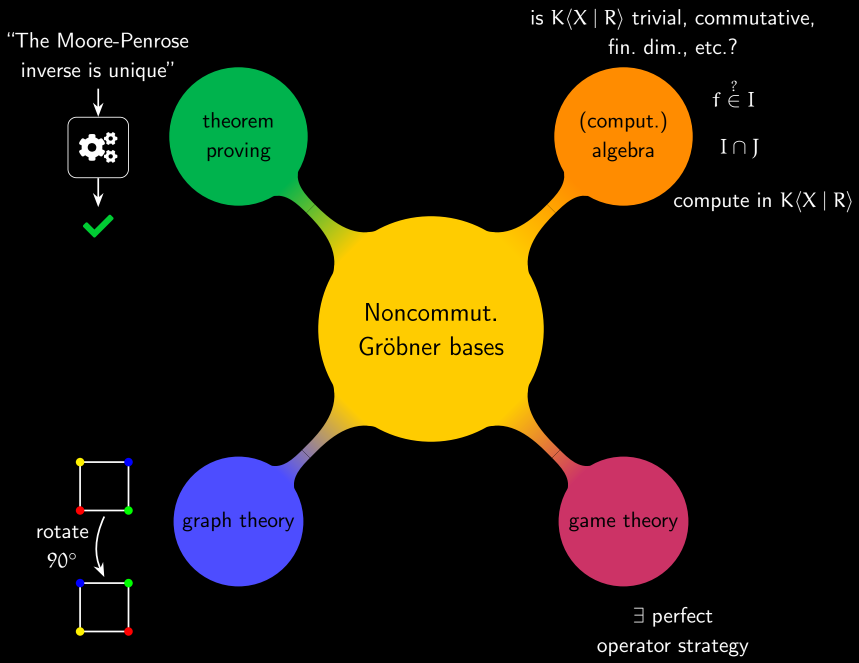
3. $u_{ij} = u_{ij}^* = u_{ij}^2$

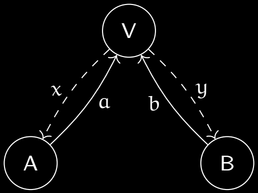
Graph has quantum symmetries

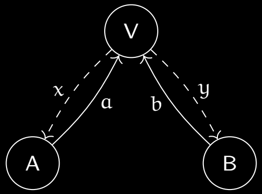
$$\Longleftrightarrow$$

$$[u_{ij}, u_{kl}] \not\in (\mathbf{1.}, \mathbf{2.}, \mathbf{3.})$$

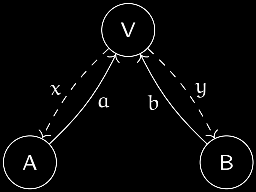

"The Moore-Penrose inverse is unique"
theorem proving
Noncommut. Gröbner bases
(comput.) algebra
is $K\langle X \mid R\rangle$ trivial, commutative, fin. dim., etc.?
$f \overset{?}{\in} I$
$I \cap J$
compute in $K\langle X \mid R\rangle$
graph theory
rotate 90°


"The Moore-Penrose inverse is unique"
theorem proving
is $K\langle X \mid R\rangle$ trivial, commutative, fin. dim., etc.?
(comput.) algebra
$f \overset{?}{\in} I$
$I \cap J$
compute in $K\langle X \mid R\rangle$
Noncommut. Gröbner bases
rotate 90°
graph theory
game theory
$\exists$ perfect operator strategy


V
x
a
b
y
A
B

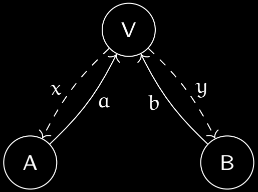


classical	$\subsetneq$	quantum	$\subsetneq$	operator
no co-op		$H_A \otimes H_B$		H



classical	$\subsetneq$	quantum	$\subsetneq$	operator
no co-op		$H_A \otimes H_B$		H

$$\exists \text{ perfect operator strategy} \quad \Rightarrow \quad -1 \notin \mathrm{SOS} + I \ \subseteq \ \mathbb{C}\langle X \rangle$$

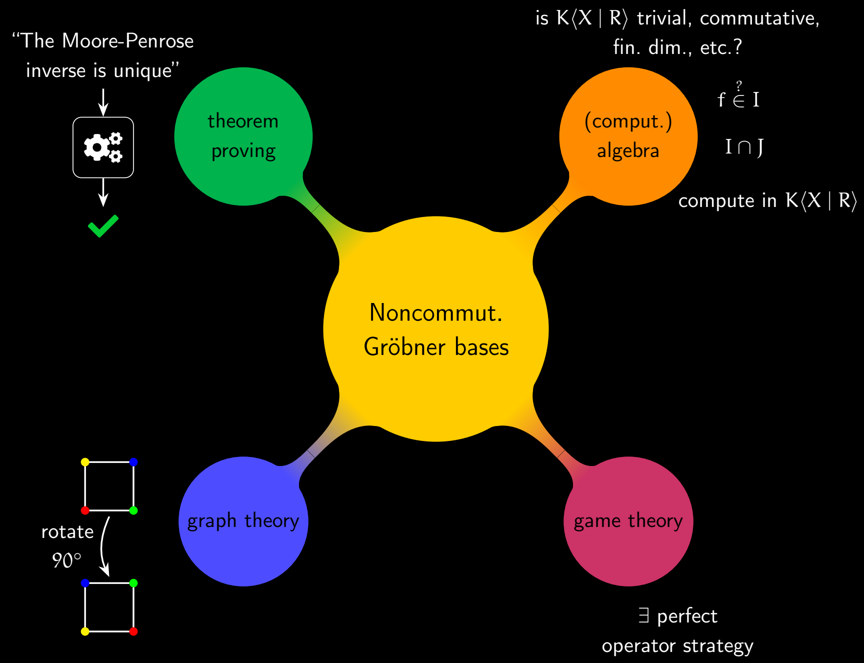


classical	$\subsetneq$	quantum	$\subsetneq$	operator
no co-op		$H_A \otimes H_B$		H

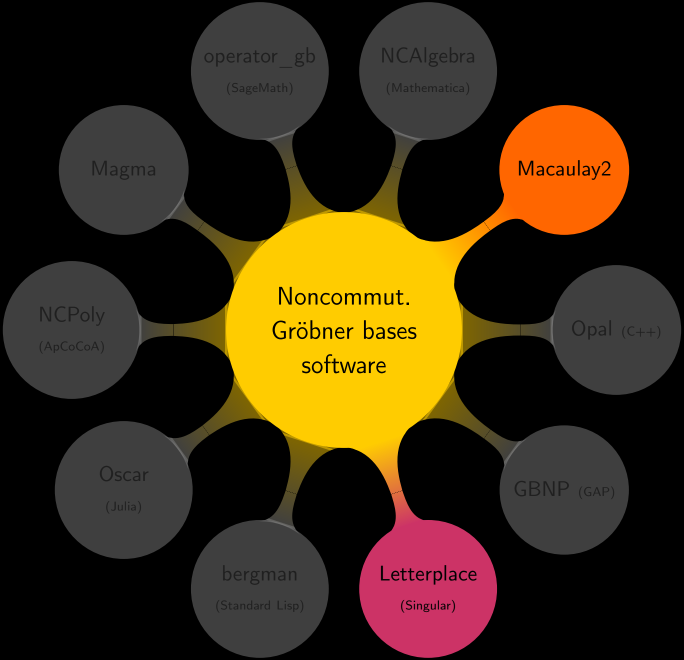
$\exists$ perfect operator strategy $\quad \Rightarrow \quad -1 \notin \mathrm{SOS} + I \subseteq \mathbb{C}\langle X \rangle$

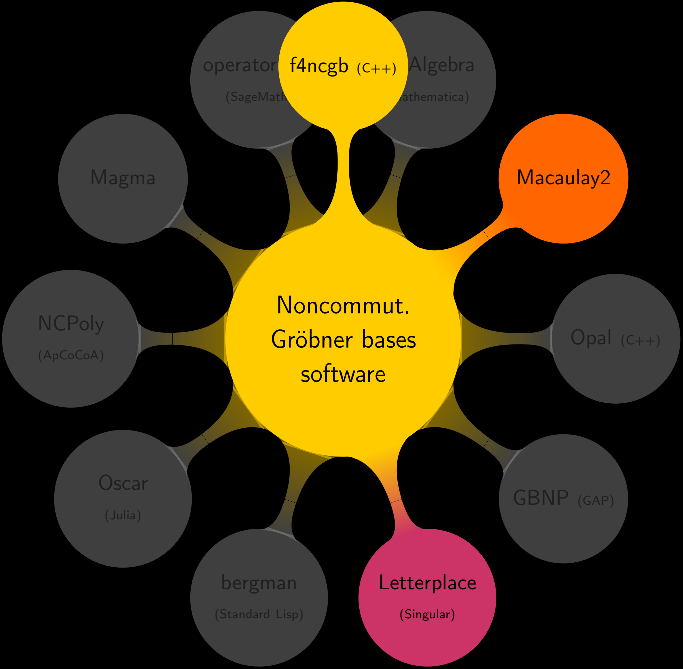
noncomm. GB + SDP $\quad \Rightarrow \quad -1 \in \mathrm{SOS} + I$

$\Rightarrow \quad \nexists$ perfect operator strategy


"The Moore-Penrose inverse is unique"
theorem proving
Noncommut. Gröbner bases
is $K\langle X \mid R\rangle$ trivial, commutative, fin. dim., etc.?
(comput.) algebra
$f \stackrel{?}{\in} I$
$I \cap J$
compute in $K\langle X \mid R\rangle$
graph theory
rotate 90°
game theory
$\exists$ perfect operator strategy

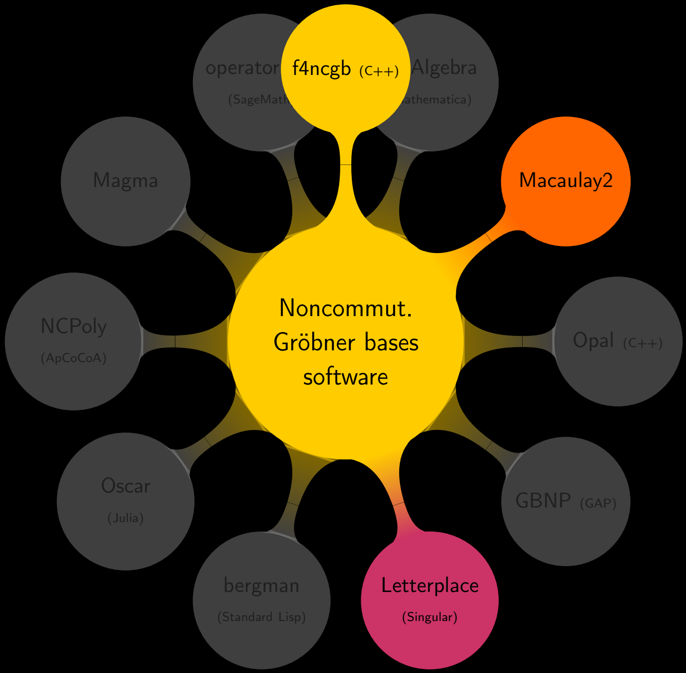

Noncommut.
Gröbner bases
software
operator_gb
(SageMath)
NCAlgebra
(Mathematica)
Macaulay2
Opal (C++)
GBNP (GAP)
Letterplace
(Singular)
bergman
(Standard Lisp)
Oscar
(Julia)
NCPoly
(ApCoCoA)
Magma


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

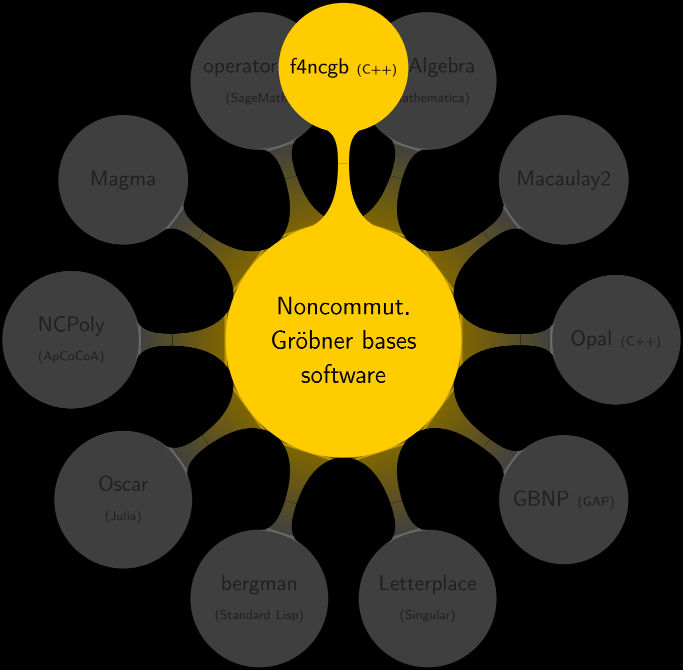

Noncommut. Gröbner bases software
f4ncgb (C++)
Algebra
Macaulay2
Opal (C++)
GBNP (GAP)
Letterplace (Singular)
bergman (Standard Lisp)
Oscar (Julia)
NCPoly (ApCoCoA)
Magma
operator

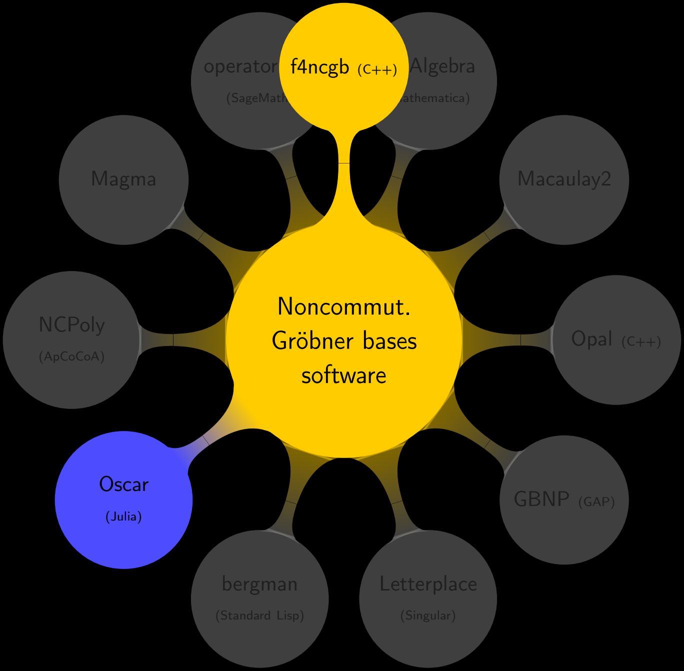
Example	Letterplace	Macaulay2	f4ncgb 1 core	f4ncgb 4 cores	f4ncgb 16 cores
`4nilp5s-10`	1217	875	30	18	12
`braid3-16`	18 314	14 291	10	5	4
`braidX-18`	>43 200	>43 200	140	55	30
`braidXY-12`	1608	18 887	10	7	6
`holt_G3562h-17`	>43 200	>43 200	45	38	36
`lascala_neuh-13`	167	37	1	1	1
`lp1-15`	24 166	33 923	111	86	83
`lv2d10-100`	>43 200	24 930	10	10	10
`malle_G12h-100`	3934	163	36	35	37

(Timings in sec)



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


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)


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

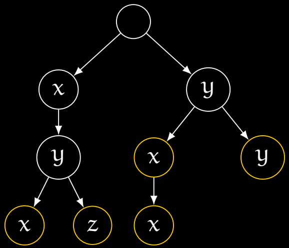
f4ncgb **(read "fancy-gb")**

Open-source C++ library that ports commutative advancements to the noncommutative setting.

- Gröbner basis computation in $\mathbb{Q}\langle X\rangle$ and $\mathbb{Z}_p\langle X\rangle$ for prime $p < 2^{31}$
- Noncommutative F4 with specialized data structures, linear algebra, etc.
- Elimination orders & Proof logging
- Default implementation in OSCAR SYMBOLIC TOOLS

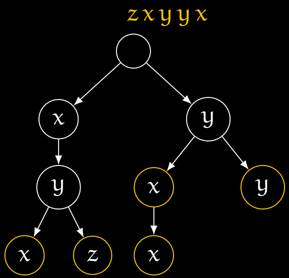
- (Compressed) monomials in bump-pointer allocator + hash map
- Prefix tree of GB-LMs for divisibility tests

$$\mathrm{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$$



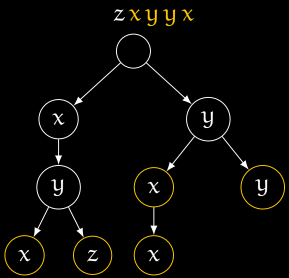
- (Compressed) monomials in bump-pointer allocator + hash map
- Prefix tree of GB-LMs for divisibility tests

$\mathsf{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$



- (Compressed) monomials in bump-pointer allocator + hash map
- Prefix tree of GB-LMs for divisibility tests

$$\mathrm{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$$

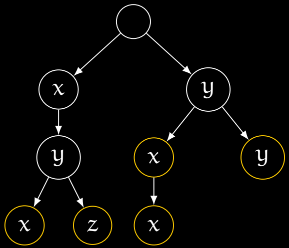


- (Compressed) monomials in bump-pointer allocator + hash map

- Prefix tree of GB-LMs for divisibility tests

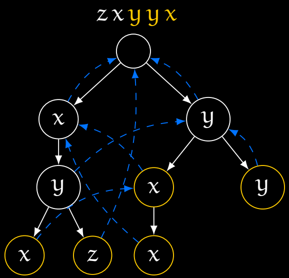
$\mathsf{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$

$z\,x\,y\,y\,x$



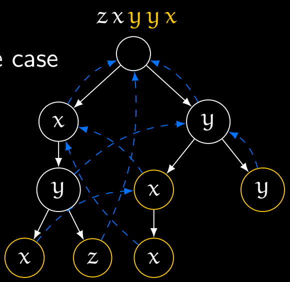
- (Compressed) monomials in bump-pointer allocator + hash map
- Prefix tree of GB-LMs for divisibility tests

$\mathsf{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$



- (Compressed) monomials in bump-pointer allocator + hash map
- Prefix tree of GB-LMs for divisibility tests
- Multimodular linear algebra over $\mathbb{Q}$
  - Uses (almost) all tricks from commutative case
  - Sparser than in the commutative case
  - Lift the matrices $\rightsquigarrow$ correctness guarantee

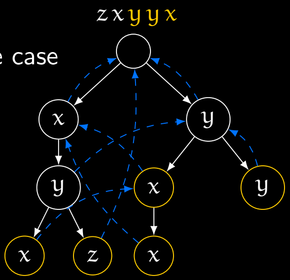
$\mathrm{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$



- (Compressed) monomials in bump-pointer allocator + hash map
- Prefix tree of GB-LMs for divisibility tests

$\mathsf{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$

- Multimodular linear algebra over $\mathbb{Q}$
    - Uses (almost) all tricks from commutative case
    - Sparser than in the commutative case
    - Lift the matrices $\rightsquigarrow$ correctness guarantee



- Proof logging via cofactor representations

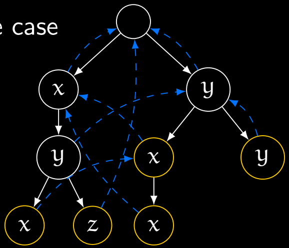
$$\begin{pmatrix} — & p_1 & — \\ & \vdots & \\ — & p_k & — \end{pmatrix} \rightsquigarrow \text{RRef}$$

- (Compressed) monomials in bump-pointer allocator + hash map
- Prefix tree of GB-LMs for divisibility tests

$\mathsf{LM}(G) = \{xyx, xyz, yx, yxx, yy\}$

- Multimodular linear algebra over $\mathbb{Q}$
  - Uses (almost) all tricks from commutative case
  - Sparser than in the commutative case
  - Lift the matrices $\rightsquigarrow$ correctness guarantee

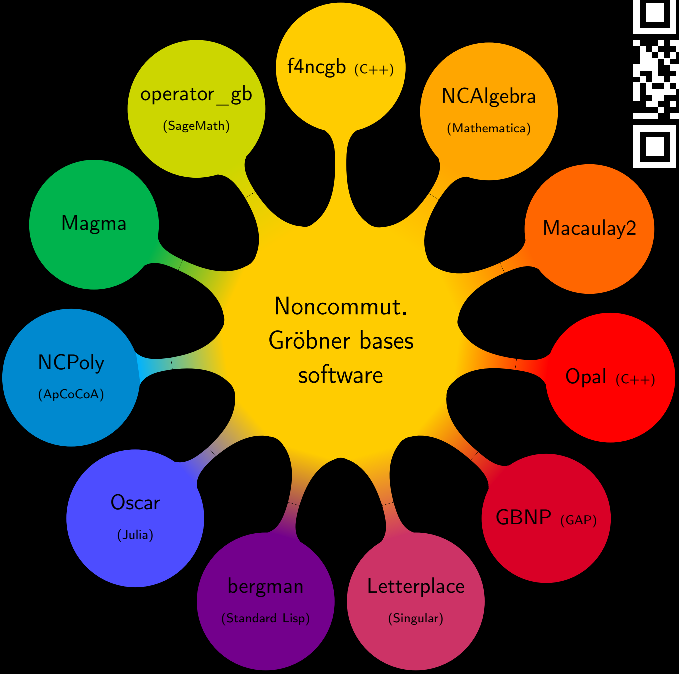
$z\,x\,y\,y\,x$



- Proof logging via cofactor representations

$$T \cdot \begin{pmatrix} — & p_1 & — \\ & \vdots & \\ — & p_k & — \end{pmatrix} = \mathsf{RRef}$$

Rows of T give cofactor representations of g_i in terms of $f_1, \ldots, f_r$ and $g_1, \ldots, g_{i-1}$.


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