f4ncgb: High Performance Gröbner Basis Computations in Free Algebras

Maximilian Heisinger and Clemens Hofstadler

CASC 2025
Dubai, 27 November 2025

Institute for Symbolic Artificial Intelligence, Johannes Kepler University Linz, Austria

JOHANNES KEPLER UNIVERSITY LINZ

FWF
Der Wissenschaftsfonds.

Noncommutative Polynomials

noncommutative = really noncommutative

Noncommutative Polynomials

$$\begin{aligned} \text{noncommutative} &= \text{really noncommutative} \\ &= \text{no commutation rules} \end{aligned}$$

Noncommutative Polynomials

$$\begin{aligned}\text{noncommutative} &= \text{really noncommutative}\\ &= \text{no commutation rules}\\ &= \text{free algebra } K\langle x_1, \ldots, x_n\rangle\end{aligned}$$

Noncommutative Polynomials

$$\begin{aligned} \text{noncommutative} &= \text{really noncommutative} \\ &= \text{no commutation rules} \\ &= \text{free algebra } K\langle x_1, \ldots, x_n \rangle \end{aligned}$$

Noncom. polynomial $\quad c_1 \cdot w_1 + \cdots + c_d \cdot w_d \quad \in K\langle x_1, \ldots, x_n \rangle$

Noncommutative Polynomials

noncommutative = really noncommutative

= no commutation rules

= free algebra $K\langle x_1, \ldots, x_n \rangle$

Noncom. polynomial $\underbrace{\boxed{c_1}}_{\in K} \cdot w_1 + \cdots + \underbrace{\boxed{c_d}}_{\in K} \cdot w_d \quad \in K\langle x_1, \ldots, x_n \rangle$

Noncommutative Polynomials

$$\begin{aligned} \text{noncommutative} &= \text{really noncommutative} \\ &= \text{no commutation rules} \\ &= \text{free algebra } K\langle x_1, \ldots, x_n\rangle \end{aligned}$$

Noncom. polynomial $\quad \overbrace{\boxed{c_1}\cdot\boxed{w_1} + \cdots + \boxed{c_d}\cdot\boxed{w_d}}^{\in K} \in K\langle x_1, \ldots, x_n\rangle$

words over $x_1, \ldots, x_n$

Noncommutative Polynomials

$$\begin{aligned} \text{noncommutative} &= \text{really noncommutative} \\ &= \text{no commutation rules} \\ &= \text{free algebra } K\langle x_1, \ldots, x_n \rangle \end{aligned}$$

$\in K$

Noncom. polynomial $\quad \boxed{c_1} \cdot \boxed{w_1} + \cdots + \boxed{c_d} \cdot \boxed{w_d} \quad \in K\langle x_1, \ldots, x_n \rangle$

words over $x_1, \ldots, x_n$

Example $\quad xyyx + 2xy - yx - 2 \in \mathbb{Q}\langle x, y \rangle$

Noncommutative Polynomials

$$\begin{aligned}\text{noncommutative} &= \text{really noncommutative}\\ &= \text{no commutation rules}\\ &= \text{free algebra } K\langle x_1,\ldots,x_n\rangle\end{aligned}$$

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

Example $\quad xyyx+2xy-yx-2 \in \mathbb{Q}\langle x,y\rangle$

$$\begin{aligned}\text{Multiplication} &= \text{concatenation of words}\\ (xy-1)\cdot(yx+2) &= xyyx+2xy-yx-2\end{aligned}$$

Noncommutative Polynomials

noncommutative = really noncommutative

= no commutation rules

= free algebra $K\langle x_1, \ldots, x_n \rangle$

$\in K$

Noncom. polynomial $\quad \boxed{c_1} \cdot \boxed{w_1} + \cdots + \boxed{c_d} \cdot \boxed{w_d} \quad \in K\langle x_1, \ldots, x_n \rangle$

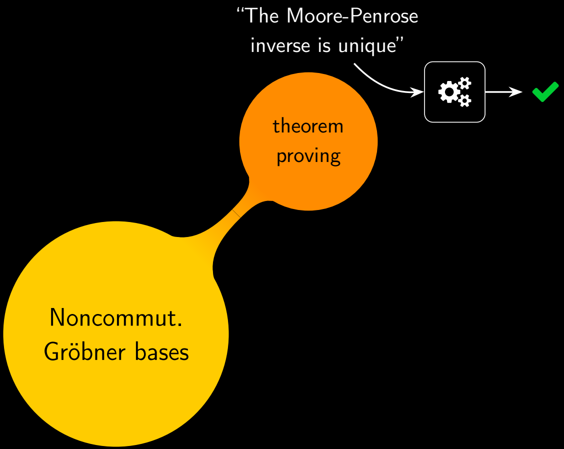
words over $x_1, \ldots, x_n$

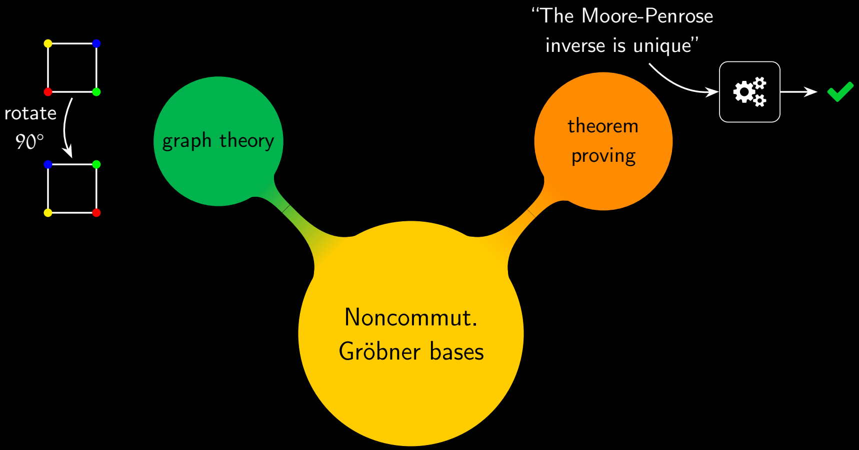
Example $\quad xyyx + 2xy - yx - 2 \in \mathbb{Q}\langle x, y \rangle$

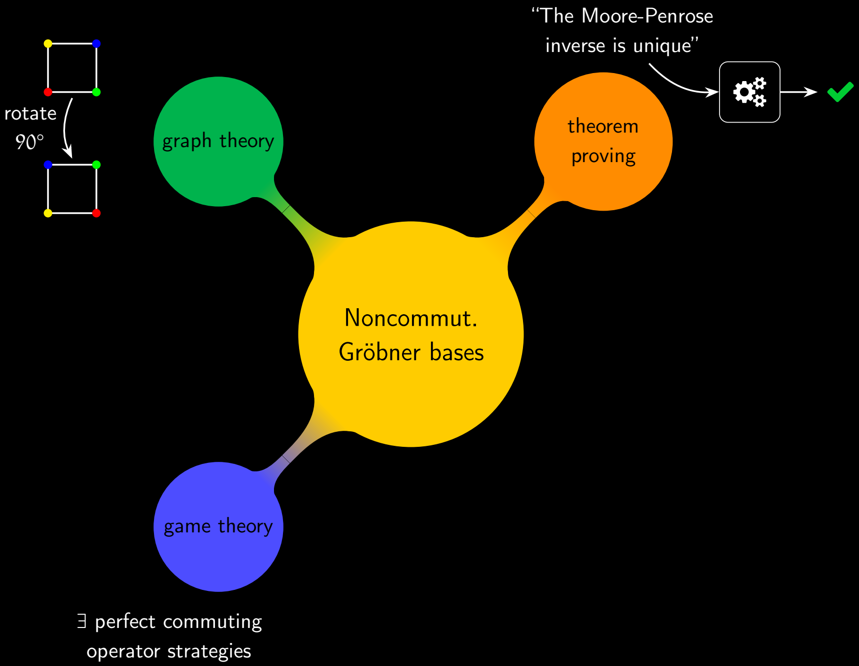
$$\begin{aligned} \text{Multiplication} \quad &= \quad \text{concatenation of words} \\ (xy - 1) \cdot (yx + 2) \quad &= \quad xyyx + 2xy - yx - 2 \end{aligned}$$

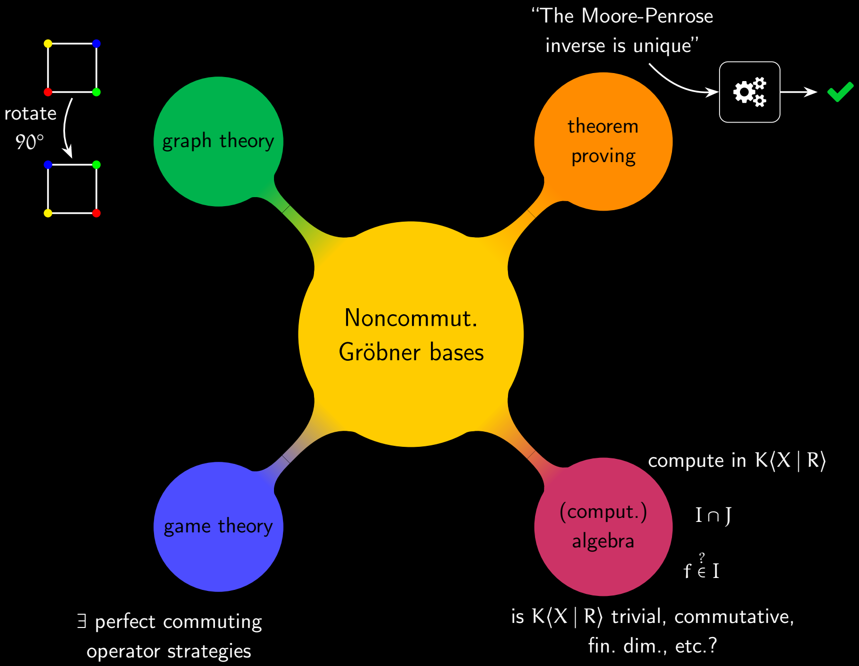
Noncomm. GB theory = comm. GB theory − finiteness

Noncommut.
Gröbner bases


"The Moore-Penrose
inverse is unique"
theorem
proving
Noncommut.
Gröbner bases


“The Moore-Penrose
inverse is unique”
rotate
90°
graph theory
theorem
proving
Noncommut.
Gröbner bases


rotate
90°
graph theory
Noncommut.
Gröbner bases
"The Moore-Penrose
inverse is unique"
theorem
proving
game theory
∃ perfect commuting
operator strategies

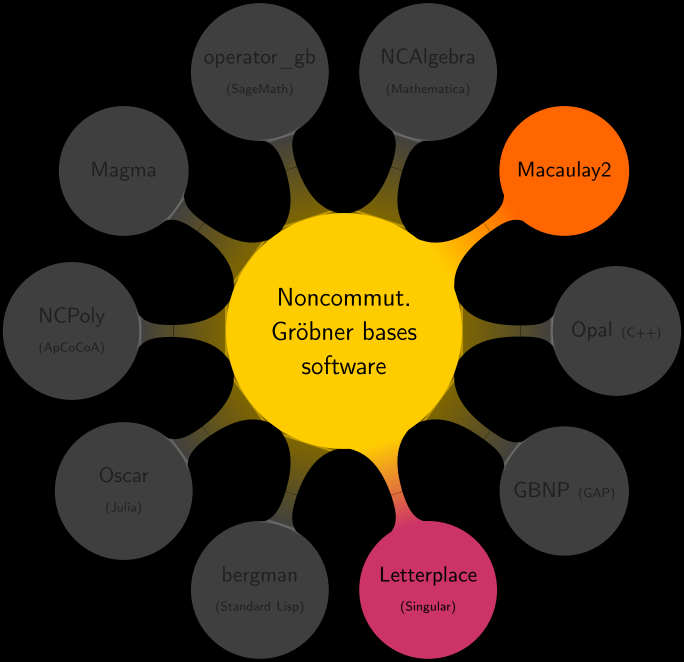


"The Moore-Penrose inverse is unique"
rotate 90°
graph theory
theorem proving
Noncommut. Gröbner bases
game theory
(comput.) algebra
compute in $K\langle X \mid R\rangle$
$I \cap J$
$f \overset{?}{\in} I$
$\exists$ perfect commuting operator strategies
is $K\langle X \mid R\rangle$ trivial, commutative, 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)
Magma
Macaulay2
NCPoly
(ApCoCoA)
Opal (C++)
Oscar
(Julia)
GBNP (GAP)
bergman
(Standard Lisp)
Letterplace
(Singular)


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


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

An Example

Consider the ideal generated by $f_1, f_2 \in \mathbb{Q}\langle x, y, z\rangle$

$$f_1 = xy + yz \qquad\qquad f_2 = x^2 + xy - yx - y^2.$$

An Example

Consider the ideal generated by $f_1, f_2 \in \mathbb{Q}\langle x, y, z\rangle$

$$f_1 = xy + yz \qquad\qquad f_2 = x^2 + xy - yx - y^2.$$

```
> ideal II = x*y+y*z,x*x+x*y-y*x-y*y;
ideal GG = twostd(II);
2ss3s(2)s4(5)s(9)s(13)s(19)s(23)-5-s(25)s(34)s(38)s(45)s(50)s(61)-------6-s(64)s(78)s(85)s(95)s(108)-s(112)---s(127)s(133)--------
-----7-s(135)s(155)s(165)s(179)s(193)-s(198)---s(215)-s(220)------s(242)-s(248)--------------------8-s(249)s(276)s(290)s(309)s(334)
-s(344)---s(364)-s(370)-----s(394)-s(400)---------s(429)-s(436)------------------------9-s(440)s(475)s(494)s(519)s(550)-s(564)---s
(586)-s(594)-----s(621)-s(628)---------s(659)-s(666)-------------s(704)-s(712)------------(700)----------------------10-s(714)s(75
8)s(783)s(815)s(853)-s(872)---s(909)-s(924)-----s(955)-s(964)-------s(1000)-s(1008)--------(1000)-----s(1048)-s(1056)-------------
------s(1103)-s(1112)------------(1100)------------------------------11-s(1115)s(1169)s(1201)s(1241)s(1287)-s(1312)---s(1356)-s(13
76)-----s(1410)-s(1422)-------s(1462)-s(1472)-----------s(1517)-s(1526)-----------------s(1577)-s(1586)-------------------------s(
1644)-s(1654)-----------------------------------------------------12-s(1657)s(1722)s(1762)s(1811)s(1866)-s(1898)---s(1950)-s(1976)-
----s(2029)-s(2050)-------s(2095)-s(2108)--------(2100)-s(2159)-s(2170)---------------s(2226)-s(2236)---------------------s(2300)-
s(2310)----------(2300)---------------------s(2381)-s(2392)-----------------------------------------------------------------13-s(23
94)s(2471)s(2520)s(2579)s(2644)-s(2684)---s(2745)-s(2778)-----s(2839)-s(2866)-------s(2915)-s(2932)---------s(2988)-s(3002)--(3000
)-----------s(3064)-s(3076)---------------------s(3143)-s(3154)---------------------------s(3231)-s(3242)-------------------------
----------------s(3324)-s(3336)------------------------------------(3300)----------------------------------------14-s(3338)s(3428)
s(3487)s(3557)s(3633)-s(3682)---s(3753)-s(3794)-----s(3864)-s(3898)-------s(3970)-s(3998)---------s(4060)-s(4078)---------s(4147
)-s(4162)-----------------s(4237)-s(4250)-------------------------s(4332)-s(4344)-----------------------------------s(4434)-s(4446
)----------------------------------------------(4400)---s(4543)-s(4556)--------------------------------------------------------(45
00)--------------------------------15-s(4559)s(4663)s(4733)s(4815)s(4903)-s(4962)---s(5044)-s(5094)-----s(5174)-s(5216)-------s(52
97)-s(5332)---------s(5399)-s(5422)-----------s(5497)-s(5516)---------------s(5598)-s(5614)--------------(5600)---------s(5702)-s(
5716)----------------(5700)---------------s(5813)-s(5826)--------------------------(5800)-----------------s(5931)-s(5944)---------
-----------------------------------(5900)---------------s(6056)-s(6070)-----------------------------------------------------------
-----------(6000)----------------------------------16-s(6071)s(6190)s(6272)s(6367)s(6468)-s(6538)---s(6632)-s(6692)-----s(6783)-s(
6834)-------s(6925)-s(6968)---------s(7062)-s(7098)-----------s(7180)-s(7204)----(7200)---------s(7294)-s(7314)--------------(7300
)-----s(7411)-s(7428)----------------------------(7400)-s(7531)-s(7546)-------------------------------------s(7660)-s(7674)-------
--------------------------------------------s(7796)-s(7810)----------(7800)-------------------------------------------------------
------s(7937)-s(7952)----------------------------------------------------(7900)---------------------------------------------------
---------------17-s(7954)s(8089)s(8184)s(8293)s(8408)-s(8490)---s(8597)-s(8668)-----s(8771)-s(8832)-------s(8934)-s(8986)---------
s(9090)-s(9134)-----------s(9222)-s(9252)-------------s(9349)-s(9374)-----------------s(9479)-s(9500)-------------------------s(96
12)-s(9630)------------------------------(9600)-----s(9750)-s(9766)---------------------------------------------s(9897)-s(9912)---
```

```
-----------------------------s(58516)-s(58540)----------------------------------------(58500)----------------------------------
--------------------------------------------------------------------(58400)-----------------------------------------------------
-------s(58874)-s(58898)----------------------------------------------------------------------------------------------------(588
00)------------------------------------------------------------------------------------------------------(58700)----------------
-----------------------s(59239)-s(59264)------------------------------------------------------------------(59200)---------------
--------------------------------------------------------------------------------------(59100)-----------------------------------
-------------------------------------------------------------------(59000)------------------------------------------------------
-------27-s(59265)s(59615)s(59895)s(60199)s(60509)-s(60766)----s(61058)-s(61294)-----s(61572)-s(61788)--------s(62055)-s(62252)-
--------s(62511)-s(62690)-----------s(62944)-s(63106)-------(63100)-------s(63358)-s(63504)----(63500)------------s(63757)-s(638
88)-----------------s(64145)-s(64262)--------------------s(64526)-s(64630)---------------------s(64868)-s(64948)----------------
--------s(65200)-s(65270)----------------------------s(65535)-s(65596)------------------------------------s(65873)-s(65926)-----
---------------------(65900)----------------------s(66214)-s(66260)-------------------------------------------------------------
(66200)---s(66558)-s(66598)---------------------------------------------------------------------------------s(66909)-s(66944)---
------------------------------------------(66900)------------------------------------------------------s(67269)-s(67300)--------
----------------------------------------------------------------------------------------------(67200)---------------------s(6763
6)-s(67664)-----------------------------------------------------------------(67600)---------------------------------------------
------------------------------------------s(68010)-s(68036)------------------------------------(68000)--------------------------
----------------------------------------------------------------------------(67900)---------------------------------------------
---s(68389)-s(68414)---------------(68400)--------------------------------------------------------------------------------------
---------------(68300)------------------------------------------------------------------------------------------------------(682
00)-----s(68775)-s(68800)------------------------------------------------------------------------------------------------------(
68700)------------------------------------------------------------------------------------------------------(68600)-------------
-----------------------------------------------s(69168)-s
```

```
-----------------------------s(58516)-s(58540)----------------------------------------(58500)---------------------------------
-------------------------------------------------------------------(58400)----------------------------------------------------
-------s(58874)-s(58898)--------------------------------------------------------------------------------------------------(588
00)----------------------------------------------------------------------------------------------------(58700)----------------
-----------------------s(59239)-s(59264)----------------------------------------------------------------(59200)---------------
-------------------------------------------------------------------------------------(59100)----------------------------------
------------------------------------------------------------------(59000)-----------------------------------------------------
-------27-s(59265)s(59615)s(59895)s(60199)s(60509)-s(60766)---s(61058)-s(61294)-----s(61572)-s(61788)-------s(62055)-s(62252)-
--------s(62511)-s(62690)-----------s(62944)-s(63106)------(63100)-------s(63358)-s(63504)----(63500)-----------s(63757)-s(638
88)-----------------s(64145)-s(64262)-------------------s(64526)-s(64630)---------------------s(64868)-s(64948)---------------
--------s(65200)-s(65270)---------------------------s(65535)-s(65596)-----------------------------------s(65873)-s(65926)-----
---------------------(65900)---------------------s(66214)-s(66260)------------------------------------------------------------
(66200)---s(66558)-s(66598)-------------------------------------------------------------------------------s(66909)-s(66944)---
-----------------------------------------(66900)-----------------------------------------------------s(67269)-s(67300)--------
--------------------------------------------------------------------------------------------(67200)---------------------s(6763
6)-s(67664)----------------------------------------------------------------(67600)--------------------------------------------
-----------------------------------------s(68010)-s(68036)------------------------------------(68000)-------------------------
---------------------------------------------------------------------------(67900)--------------------------------------------
---s(68389)-s(68414)--------------(68400)-------------------------------------------------------------------------------------
---------------(68300)----------------------------------------------------------------------------------------------------(682
00)-----s(68775)-s(68800)----------------------------------------------------------------------------------------------------(
68700)----------------------------------------------------------------------------------------------------(68600)-------------
----------------------------------------------s(69168)-s
```

```
-------------------------------------------------(351300)--------------------------------------------------------------------
-----------------------s(352009)-s(352044)---------------------------------------------(352000)------------------------------
---------------------------------------------------------------------(351900)------------------------------------------------
---------------------------------------------------(351800)------------------------------------------------------------------
---------------------------------(351700)---------------------------------------------------------------------------------s(
475)-s(352510)----------(352500)---------------------------------------------------------------------------------------------
------(352400)-----------------------------------------------------------------------------------------------------(352300)-
-------------------------------------------------------------------------------------------------(352200)--------------------
-------------------------------------------------------------------------------(352100)--------------------------------------
--------------------------------s(352941)-s(352976)--------------------------------------------------------------------------
(352900)-----------------------------------------------------------------------------------------------------(352800)--------
-------------------------------------------------------------------------------------------(352700)--------------------------
-------------------------------------------------------------------------(352600)--------------------------------------------
-------------------------------------------------------(352500)--------------------------------------------------------------
-s(353405)-s(353440)-----------------------------------------(353400)--------------------------------------------------------
-------------------------------------------(353300)--------------------------------------------------------------------------
------------------------(353200)---------------------------------------------------------------------------------------------
------(353100)-----------------------------------------------------------------------------------------------------(353000)-
-------------------------------------------------------------------------------------------------(352900)--------------------
----------------------------------------------s(353863)-s(353898)------------------------------------------------------------
-------------------------------------(353800)--------------------------------------------------------------------------------
------------------(353700)---------------------------------------------------------------------------------------------------
```

```
)----------------------------------------------------------------------------------------------------(2200)--------------------
---------------------------------------------------------------------------------(2100)---------------------------------------
-------------------------------------------------------------(2000)-----------------------------------------------------------
-----------------------------------------(1900)-------------------------------------------------------------------------------
---------------------(1800)---------------------------------------------------------------------------------------------------
-(1700)----------------------------------------------------------------------------------------------------(1600)-------------
---------------------------------------------------------------------------------------(1500)---------------------------------
-------------------------------------------------------------------(1400)-----------------------------------------------------
-----------------------------------------------(1300)-------------------------------------------------------------------------
---------------------------(1200)---------------------------------------------------------------------------------------------
-------(1100)----------------------------------------------------------------------------------------------------(1000)-------
---------------------------------------------------------------------------------------------(900)----------------------------
------------------------------------------------------------------------(800)-------------------------------------------------
---------------------------------------------------(700)----------------------------------------------------------------------
------------------------------(600)-------------------------------------------------------------------------------------------
---------(500)----------------------------------------------------------------------------------------------------(400)-------
---------------------------------------------------------------------------------------------(300)----------------------------
------------------------------------------------------------------------(200)-------------------------------------------------
---------------------------------------------------(100)----------------------------------------------------------------------
------------------------------
product criterion:0 chain criterion:1726044
shift V criterion:648631356
Auf Wiedersehen.
singular demo.sing  4511.08s user 21.85s system 64% cpu 1:56:58.99 total
(base) clemenshofstadler@Clemenss-MacBook-Air demo %
```

An Example

```
(base) clemenshofstadler@Clemenss-MacBook-Air demo % ./f4ncgb -m 10000 -d 75 demo.ms > demo.gb
[f4ncgb] ==== Input Parameters ====
[f4ncgb] Characteristic:    0
[f4ncgb] Max. Iterations:   10000
[f4ncgb] Max. amb. degree:  75
[f4ncgb] Monomial order:    z < y < x
[f4ncgb] Nr. threads:       1
[f4ncgb] Output file:       None. Writing output to console.
[f4ncgb] Proof logging:     off
[f4ncgb] Tracer:            on
[f4ncgb] PID of F4NCGB:     11942
[f4ncgb] ==== Starting Gröbner Basis Computation ====
```

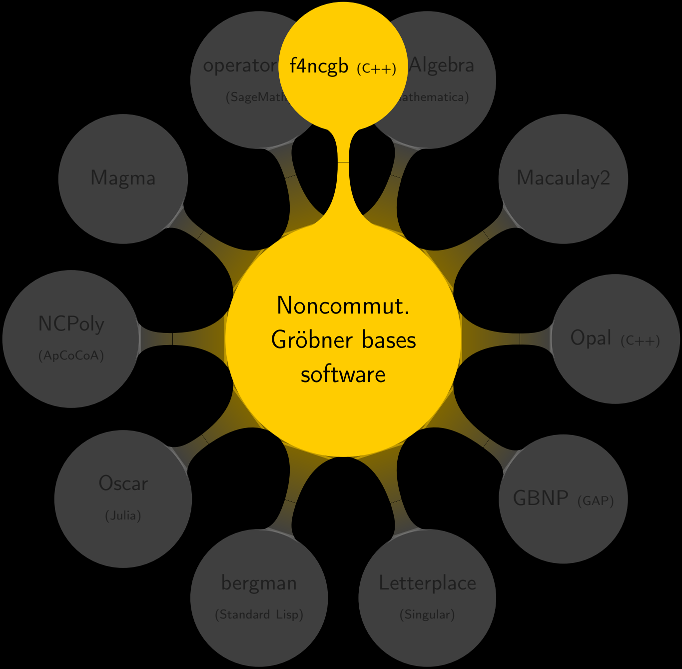
An Example

```
(base) clemenshofstadler@Clemenss-MacBook-Air demo % ./f4ncgb -m 10000 -d 75 demo.ms > demo.gb
[f4ncgb] ==== Input Parameters ====
[f4ncgb] Characteristic:    0
[f4ncgb] Max. Iterations:   10000
[f4ncgb] Max. amb. degree:  75
[f4ncgb] Monomial order:    z < y < x
[f4ncgb] Nr. threads:       1
[f4ncgb] Output file:       None. Writing output to console.
[f4ncgb] Proof logging:     off
[f4ncgb] Tracer:            on
[f4ncgb] PID of F4NCGB:     11942
[f4ncgb] ==== Starting Gröbner Basis Computation ====
[f4ncgb] ==== Basis computation finished ====
[f4ncgb]
[f4ncgb] maximum resident set size:              245744.00 MB
[f4ncgb] store find calls:                         13478136
[f4ncgb] store find hits:                           88.36 %
[f4ncgb] parse input:                                0.00 (0.00 %)
[f4ncgb] computing ambiguities:                      2.06 (25.76 %)
[f4ncgb]   computing overlaps:                       0.34 (4.20 %)
[f4ncgb]   computing inclusions:                     0.04 (0.52 %)
[f4ncgb] handling critical pairs:                    0.44 (5.47 %)
[f4ncgb] symbolic preprocessing:                     0.42 (5.26 %)
[f4ncgb] linear algebra:                             4.28 (53.44 %)
[f4ncgb]   Gauss elimination:                        3.95 (49.37 %)
[f4ncgb]     reduce (CPU-time):                      3.81 (47.60 %) /#t: 3.81 (47.60 %)
[f4ncgb]   CRT:                                      0.00 (0.02 %)
[f4ncgb]   rat. reconstruction:                      0.00 (0.02 %)
[f4ncgb] construct new elements:                     0.02 (0.24 %)
[f4ncgb] other:                                      0.00 (0.00 %)
[f4ncgb]
[f4ncgb] total process time:                         8.01 seconds
(base) clemenshofstadler@Clemenss-MacBook-Air demo %
```

Example	Letterplace	f4ncgb 1 core	f4ncgb 4 cores	f4ncgb 16 cores
`4nilp5s-10`	1282	150	79	63
`braid3-16`	18 953	105	34	18
`braidXY-12`	1847	62	52	52
`holt_G3562h-17`	>43 200	25 021	12 671	6824
`lascala_neuh-13`	171	9	5	4
`lp1-15`	24 166	266	179	155
`lv2d10-100`	>43 200	48	27	47
`malle_G12h-100`	4142	89	74	73

(Timings in sec)


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


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

f4ncgb

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 $p < 2^{31}$
- Several orders of magnitude faster than current state of the art
- Proof logging via cofactor representations
- Also part of OSCAR SYMBOLIC TOOLS

Data structures

- Monomials are shared
- Coefficients are shared
- Prefix tree for divisions

Algorithms

- Noncomm. F4 algorithm
- Sparse linear algebra (multi-modular, parallelized, probabilistic)
- Proof logging

f4ncgb

Data structures

- Monomials are shared
- Coefficients are shared
- Prefix tree for divisions

Algorithms

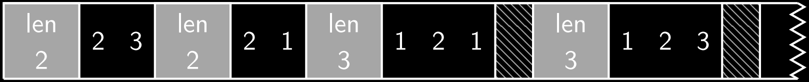
- Noncomm. F4 algorithm
- Sparse linear algebra (multi-modular, parallelized, probabilistic)
- Proof logging

f4ncgb

Monomials & Polynomials

Represent vars by index according to mon. order: $x_1 < x_2 < \cdots < x_n$

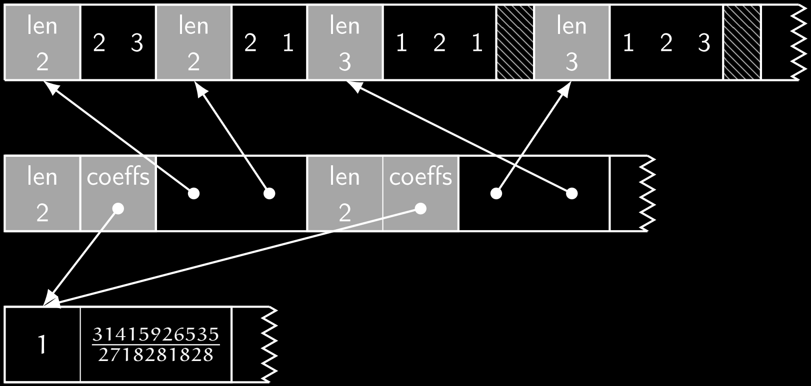
$$\begin{array}{ccccccc} x_1 & < & x_2 & < & \cdots & < & x_n \\ \downarrow & & \downarrow & & & & \downarrow \\ 1 & & 2 & & & & n \end{array}$$



Monomials & Polynomials

Represent vars by index according to mon. order: $x_1 < x_2 < \cdots < x_n$

$$\begin{array}{ccccc} x_1 & < x_2 & < \cdots < & x_n \\ \downarrow & \downarrow & & \downarrow \\ 1 & 2 & & n \end{array}$$



Monomial Divisibility Tests

Observation: divisor candidates are always the same (lm's of the GB)

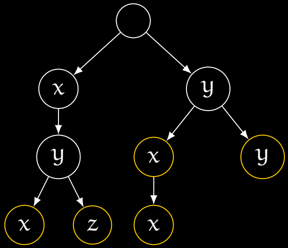
Exploit this information $\rightsquigarrow$ keep prefix tree of all leading monomials

Monomial Divisibility Tests

Observation: divisor candidates are always the same (lm's of the GB)

Exploit this information $\rightsquigarrow$ keep prefix tree of all leading monomials

$$G = \{\, xyx - \ldots,\; xyz + \ldots,\; yx + \ldots,\; yxx - \ldots,\; yy + \ldots \}$$

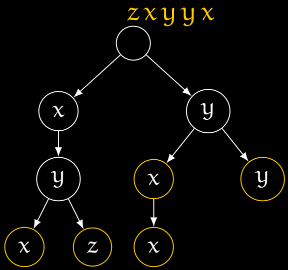


Monomial Divisibility Tests

Observation: divisor candidates are always the same (lm's of the GB)

Exploit this information $\rightsquigarrow$ keep prefix tree of all leading monomials

$$G = \{\, xyx - \dots,\; xyz + \dots,\; yx + \dots,\; yxx - \dots,\; yy + \dots \}$$

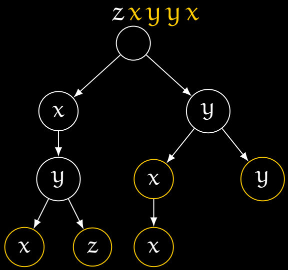


Monomial Divisibility Tests

Observation: divisor candidates are always the same (lm's of the GB)

Exploit this information $\rightsquigarrow$ keep prefix tree of all leading monomials

$$G = \{\, xyx - \ldots,\quad xyz + \ldots,\quad yx + \ldots,\quad yxx - \ldots,\quad yy + \ldots \}$$

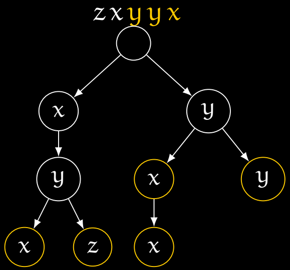


Monomial Divisibility Tests

Observation: divisor candidates are always the same (lm's of the GB)

Exploit this information $\rightsquigarrow$ keep prefix tree of all leading monomials

$$G = \{\, xyx - \dots,\; xyz + \dots,\; yx + \dots,\; yxx - \dots,\; yy + \dots \}$$

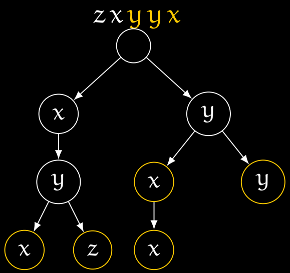


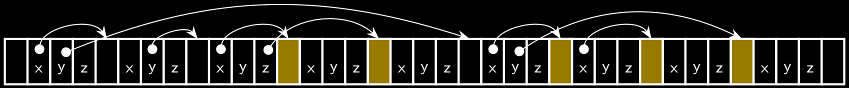
Monomial Divisibility Tests

Observation: divisor candidates are always the same (lm's of the GB)

Exploit this information $\rightsquigarrow$ keep prefix tree of all leading monomials

$$
G = \{\, xyx - \ldots,\; xyz + \ldots,\; yx + \ldots,\; yxx - \ldots,\; yy + \ldots \}
$$





Data structures

- Monomials are shared
- Coefficients are shared
- Prefix tree for divisions

Algorithms

- Noncomm. F4 algorithm
- Sparse linear algebra (multi-modular, parallelized, probabilistic)
- Proof logging

f4ncgb

Data structures

- Monomials are shared
- Coefficients are shared
- Prefix tree for divisions

Algorithms

- Noncomm. F4 algorithm
- Sparse linear algebra (multi-modular, parallelized, probabilistic)
- Proof logging

f4ncgb

Proof Logging

Proof Logging

Given input $f_1, \dots, f_r$, write each $g \in GB$ as

$$g = \sum_j p_j \cdot f_j \cdot q_j$$

"*cofactor representation*"

with $p_j, q_j \in K\langle X \rangle$.

Proof Logging

Given input $f_1, \ldots, f_r$, write each $g \in GB$ as

$$g = \sum_j p_j \cdot f_j \cdot q_j \qquad \text{“\textit{cofactor representation}”}$$

with $p_j, q_j \in K\langle X\rangle$.

Cofactor representations certify ideal membership.

Can be computed during Gaussian elimination:

Proof Logging

Given input $f_1, \ldots, f_r$, write each $g \in \mathrm{GB}$ as

$$g = \sum_j p_j \cdot f_j \cdot q_j \qquad \text{“\textit{cofactor representation}”}$$

with $p_j, q_j \in K\langle X \rangle$.

Cofactor representations certify ideal membership.

Can be computed during Gaussian elimination:

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

Proof Logging

Given input $f_1, \ldots, f_r$, write each $g \in GB$ as

$$g = \sum_j p_j \cdot f_j \cdot q_j \qquad \text{"\textit{cofactor representation}"}$$

with $p_j, q_j \in K\langle X \rangle$.

Cofactor representations certify ideal membership.

Can be computed during Gaussian elimination:

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

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

Substitution yields representations w.r.t. $f_1, \ldots, f_r$ (⚠ exp. blowup!)

Data structures

- Monomials are shared
- Coefficients are shared
- Prefix tree for divisions

Algorithms

- Noncomm. F4 algorithm
- Sparse linear algebra (multi-modular, parallelized, probabilistic)
- Proof logging

f4ncgb

f4ncgb

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 $p < 2^{31}$
- Several orders of magnitude faster than current state of the art
- Proof logging via cofactor representations
- Also part of OSCAR SYMBOLIC TOOLS