



Inria

université
PARIS-SACLAY



A data structure for monomial ideals with applications to signature Gröbner basis

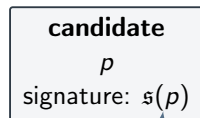
Pierre Lairez, Rafael Mohr & Théo Ternier
MATHEXP, Inria Saclay, France

ISSAC 2026

Oldenburg, Germany – July 14, 2026

Motivation: processing of signatures

Inside the main loop in sGB algorithm (Faugère, 2002)

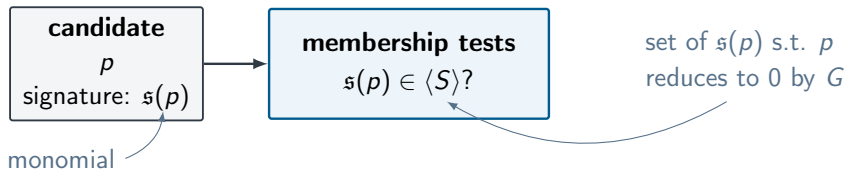


monomial



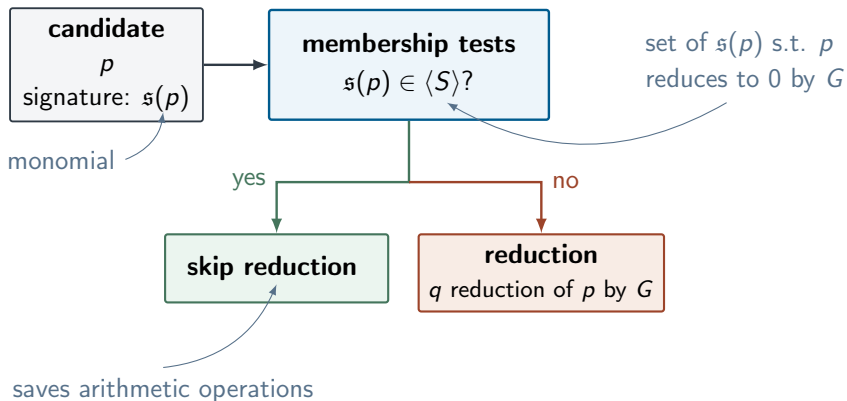
Motivation: processing of signatures

Inside the main loop in sGB algorithm (Faugère, 2002)



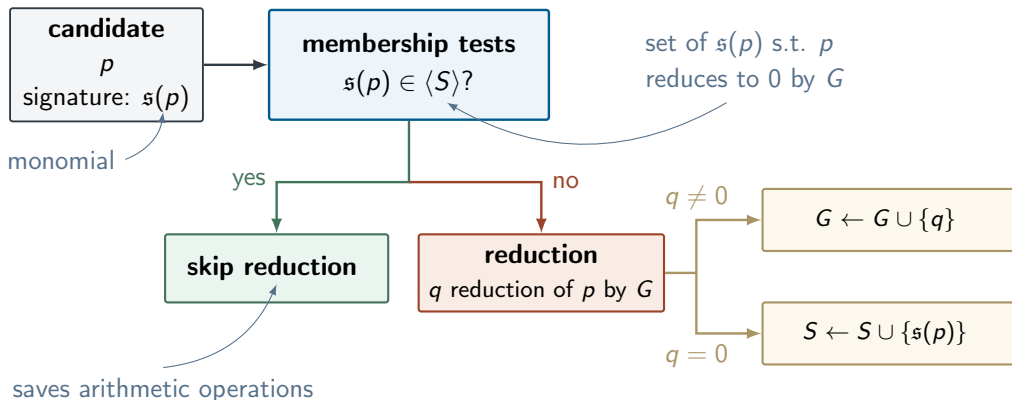
Motivation: processing of signatures

Inside the main loop in sGB algorithm (Faugère, 2002)



Motivation: processing of signatures

Inside the main loop in sGB algorithm (Faugère, 2002)



Motivation: processing of signatures

Inside the main loop in sGB algorithm (Faugère, 2002)

candida

p

signature:

monomial

eco¹⁴: 14 polynomials in 14 variables

All reductions to 0 avoided but...

117,861,802

membership tests in monomial ideals

(*AlgebraicSolving.jl*)

$G \cup \{q\}$

$\cup \{s(p)\}$

saves arithmetic operations

Membership test

Goal: Efficiently test monomial membership in a monomial ideal.

Example: $I = \langle x^2z^3, x^2y^3z, x^3, yz^2 \rangle$ $m = x^2y^2z^2 \in I?$

Membership test

Goal: Efficiently test monomial membership in a monomial ideal.

Example: $I = \langle x^2 z^3, x^2 y^3 z, x^3, yz^2 \rangle$ $m = x^2 y^2 z^2 \in I?$

Membership test

Goal: Efficiently test monomial membership in a monomial ideal.

Example: $I = \langle x^2z^3, x^2y^3z, x^3, yz^2 \rangle$ $m = x^2y^2z^2 \in I?$

Membership test

Goal: Efficiently test monomial membership in a monomial ideal.

Example: $I = \langle x^2z^3, x^2y^3z, x^3, yz^2 \rangle$ $m = x^2y^2z^2 \in I?$

Membership test

Goal: Efficiently test monomial membership in a monomial ideal.

Example: $I = \langle x^2z^3, x^2y^3z, x^3, yz^2 \rangle$ $m = x^2y^2z^2 \in I?$

Membership test

Goal: Efficiently test monomial membership in a monomial ideal.

Example: $I = \langle x^2z^3, x^2y^3z, x^3, yz^2 \rangle$ $m = x^2y^2z^2 \in I?$

Naive algorithm

If n number of variables and N number of generators:

$$O(nN)$$

Membership test

Goal: Efficiently test monomial membership in a monomial ideal.

Example: $I = \langle x^2z^3, x^2y^3z, x^3, yz^2 \rangle$ $m = x^2y^2z^2 \in I?$

Naive algorithm

If n number of variables and N number of generators:

$$O(nN)$$

Our data structure Independent of N

If d is the largest generator degree:

$$O(n \log d)$$

Practical impact

eco¹⁴ runs **3× faster**

- **Divmasks:** Prune some divisibility checks.

For each monomial a store a 64-bit integer $\text{div}(a)$ such that for any monomial b ,

$$a \mid b \implies (\text{div}(a) \& \sim \text{div}(b)) == 0$$

- **Divmasks:** Prune some divisibility checks.

For each monomial a store a 64-bit integer $\text{div}(a)$ such that for any monomial b ,

$$a \mid b \implies (\text{div}(a) \& \sim \text{div}(b)) == 0$$

Mismatch: $a \nmid b$

- **Divmasks:** Prune some divisibility checks.

For each monomial a store a 64-bit integer $\text{div}(a)$ such that for any monomial b ,

$$a \mid b \implies (\text{div}(a) \& \sim \text{div}(b)) == 0$$

Mismatch: $a \nmid b$

Match: compare exponents

- **Divmasks:** Prune some divisibility checks.

For each monomial a store a 64-bit integer $\text{div}(a)$ such that for any monomial b ,

$$a \mid b \implies (\text{div}(a) \& \sim \text{div}(b)) == 0$$

Mismatch: $a \nmid b$

Match: compare exponents

- **Range queries** for membership tests.

Dubé, 1993

Construction: $O(N \log(N)^{n-1})$

Membership: $O(\log(N)^n)$

- **Divmasks:** Prune some divisibility checks.

For each monomial a store a 64-bit integer $\text{div}(a)$ such that for any monomial b ,

$$a \mid b \implies (\text{div}(a) \& \sim \text{div}(b)) == 0$$

Mismatch: $a \nmid b$

Match: compare exponents

- **Range queries** for membership tests.

Dubé, 1993

Construction: $O(N \log(N)^{n-1})$

Membership: $O(\log(N)^n)$

- **BDD-engine** for computations on monomial ideals.

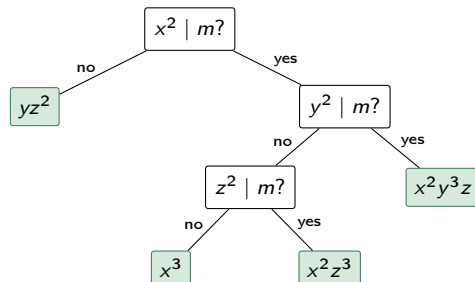
Moreno-Resa, Sáenz de Cabezón, ISSAC 2026

- Kd-trees

Roune, Stillman, ISSAC 2012

kd-tree of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$

$m = x^2y^2z^2?$



Membership: $O(nN)$

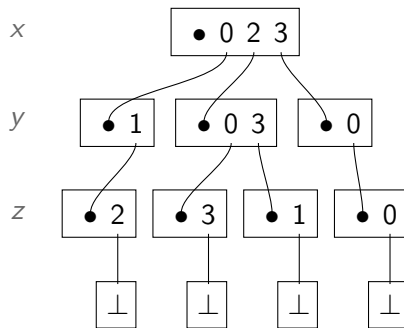
State of the art

- Prefix tree

Milowski, 2004

$$I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$$

$$m = x^2y^2z^2 \in I?$$



Construction: $O(nN)$

Membership: $O(nN)$

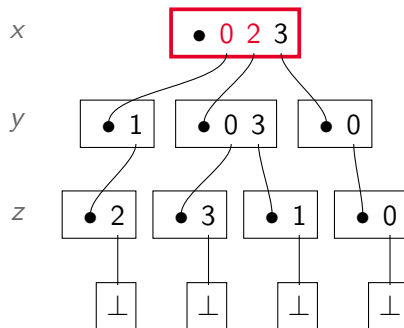
State of the art

- Prefix tree

Milowski, 2004

$$I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$$

$$m = x^2y^2z^2 \in I?$$



Construction: $O(nN)$

Membership: $O(nN)$

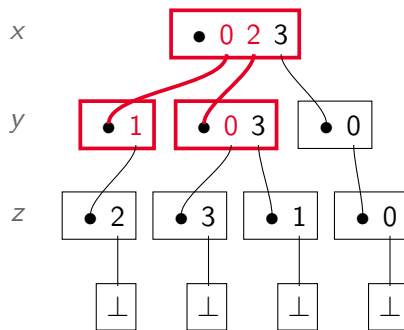
State of the art

- Prefix tree

Milowski, 2004

$$I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$$

$$m = x^2y^2z^2 \in I?$$



Construction: $O(nN)$

Membership: $O(nN)$

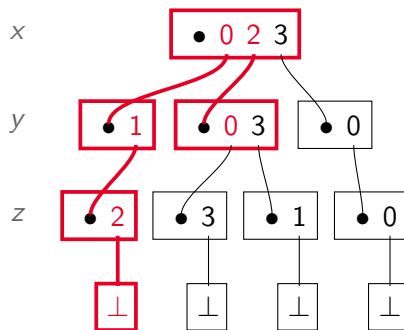
State of the art

- Prefix tree

Milowski, 2004

$$I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$$

$$m = x^2y^2z^2 \in I?$$

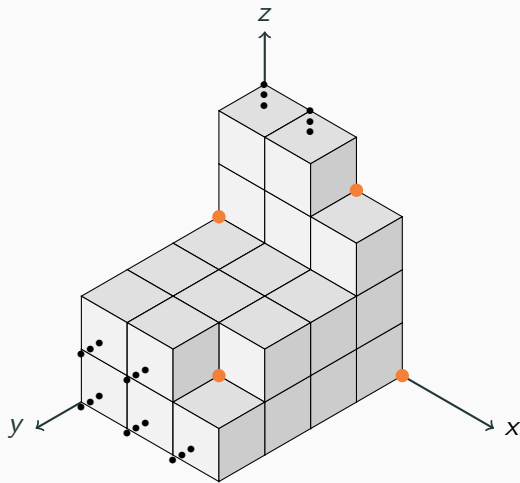


Construction: $O(nN)$

Membership: $O(nN)$

Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$

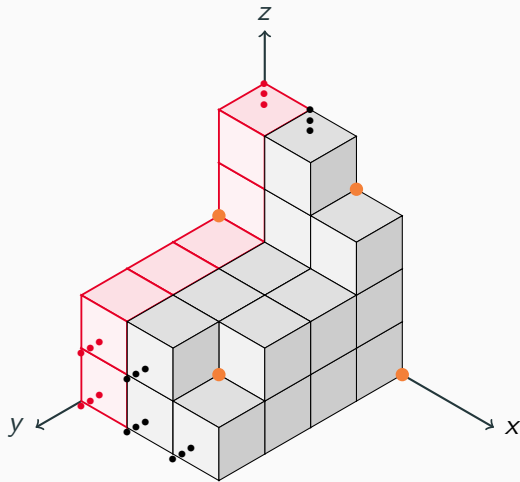
$$I/k = \langle m \in \text{Mon}(y, z) \mid x^k m \in I \rangle$$



Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$

$$I/k = \langle m \in \text{Mon}(y, z) \mid x^k m \in I \rangle$$

$$I/0 = \langle yz^2 \rangle$$



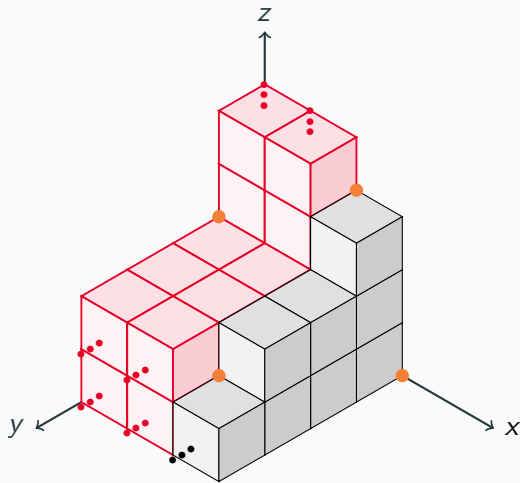
Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$

$$I/k = \langle m \in \text{Mon}(y, z) \mid x^k m \in I \rangle$$

$$I/0 = \langle yz^2 \rangle$$

$\cap$

$$I/1 = \langle yz^2 \rangle$$



Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$

$$I/k = \langle m \in \text{Mon}(y, z) \mid x^k m \in I \rangle$$

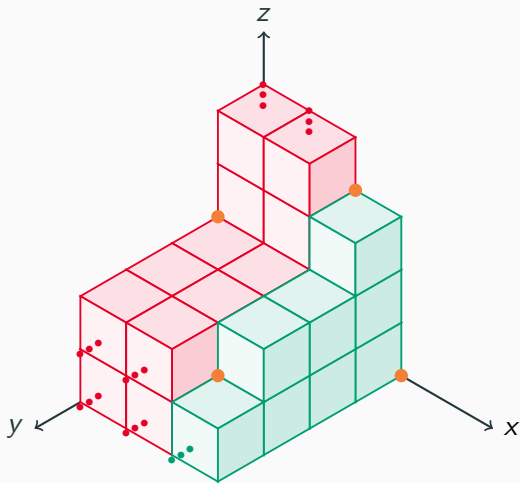
$$I/0 = \langle yz^2 \rangle$$

$\cap$

$$I/1 = \langle yz^2 \rangle$$

$\cap$

$$I/2 = \langle yz^2, z^3, y^3z \rangle$$



Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$

$$I/k = \langle m \in \text{Mon}(y, z) \mid x^k m \in I \rangle$$

$$I/0 = \langle yz^2 \rangle$$

$\cap$

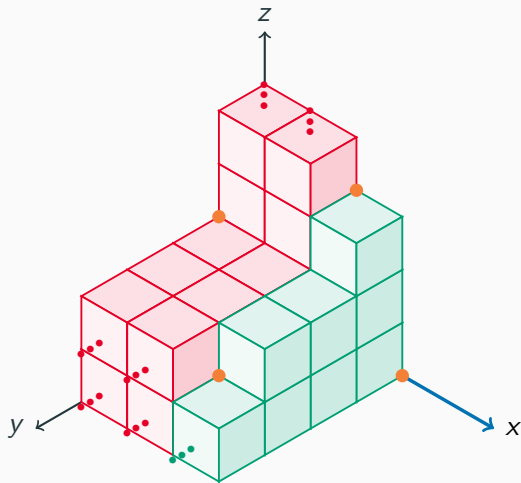
$$I/1 = \langle yz^2 \rangle$$

$\cap$

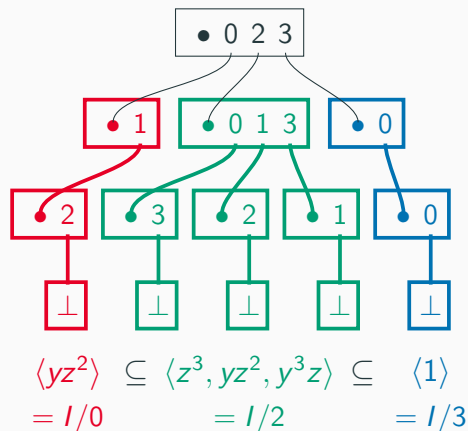
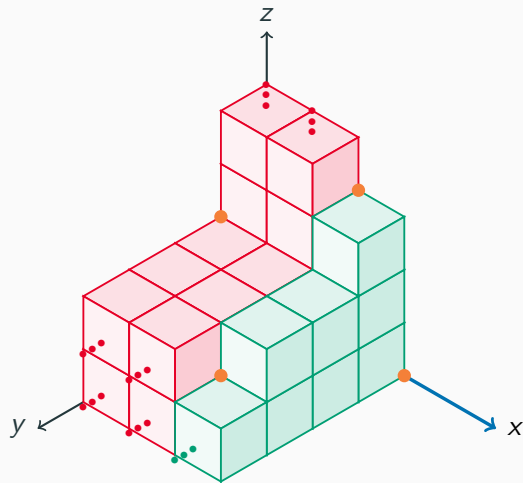
$$I/2 = \langle yz^2, z^3, y^3z \rangle$$

$\cap$

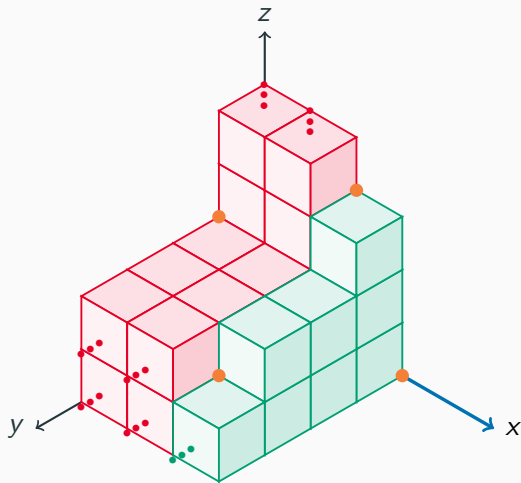
$$I/3 = \langle yz^2, z^3, y^3z, 1 \rangle$$



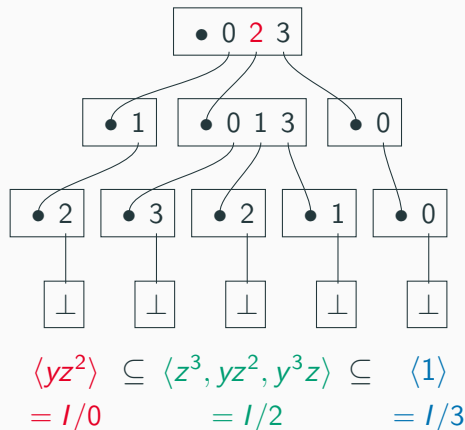
Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$



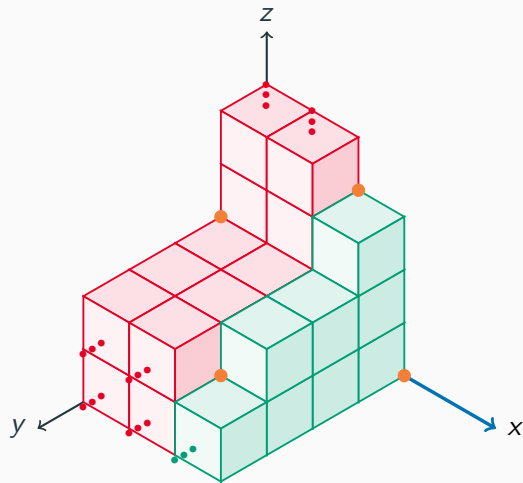
Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$



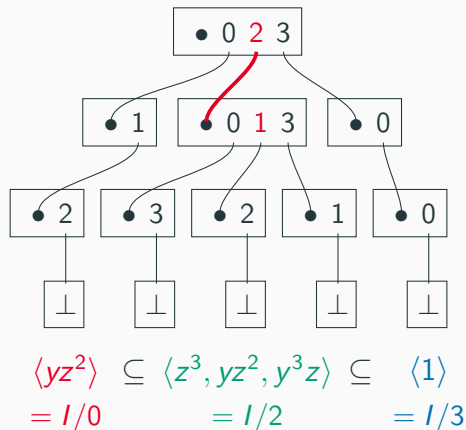
Membership: $m = \mathbf{x}^2 y^2 z^2 \in I?$



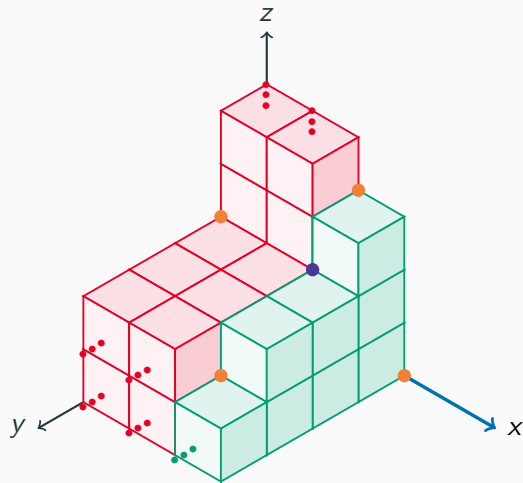
Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$



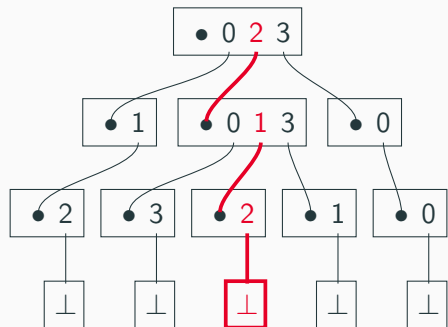
Membership: $m = x^2y^2z^2 \in I?$



Geometric representation: staircase of $I = \langle yz^2, x^2z^3, x^2y^3z, x^3 \rangle$

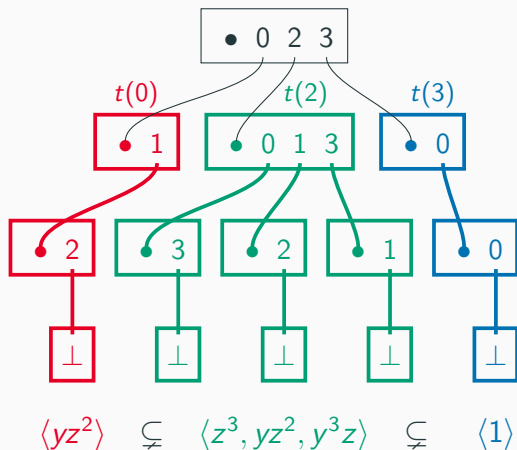


Membership: $m = x^2y^2z^2 \in I?$



$$\begin{aligned} \langle yz^2 \rangle &\subseteq \langle z^3, yz^2, y^3z \rangle \subseteq \langle 1 \rangle \\ &= I/0 &= I/2 &= I/3 \end{aligned}$$

Ideal n -trees

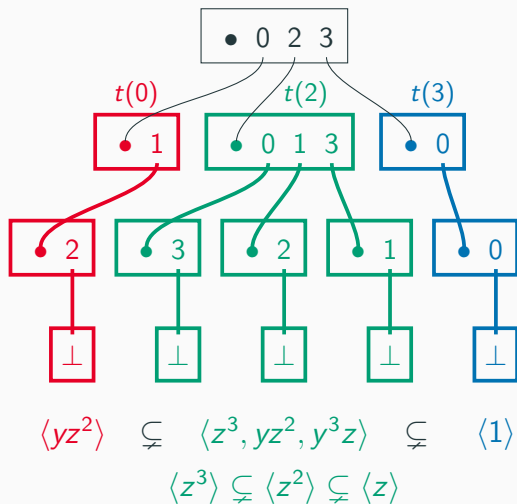


Ideal n -trees

A n -tree t is ideal if $n = 0$ or $n > 0$ and

- $\forall e, f \in \text{dom}(t),$
 $e < f \implies \mathbb{I}(t(e)) \subsetneq \mathbb{I}(t(f))$

Ideal n -trees



Ideal n -trees

A n -tree t is ideal if $n = 0$ or $n > 0$ and

- $\forall e, f \in \text{dom}(t),$
 $e < f \implies \mathbb{I}(t(e)) \subsetneq \mathbb{I}(t(f))$
- $\forall e \in \text{dom}(t),$
 $t(e)$ is ideal

Insertion to build an ideal n -tree

In sGB computations: monomials are inserted one by one

Let $m = x_1^{m_1} \dots x_n^{m_n}$

Ideal n -tree of $\langle m \rangle$:



Insertion to build an ideal n -tree

In sGB computations: monomials are inserted one by one

Let $m = x_1^{m_1} \dots x_n^{m_n}$

I a monomial ideal, t its ideal n -tree. We define:

$\text{ins}(t, m)$

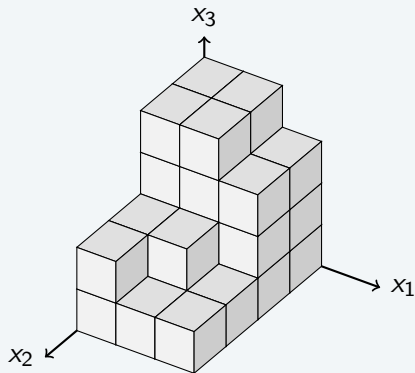
the ideal n -tree of $I + \langle m \rangle$

Ideal n -tree of $\langle m \rangle$:



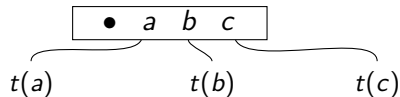
Insertion of $m = x_1^{m_1} m'$ in the ideal n -tree t of I

Geometric intuition



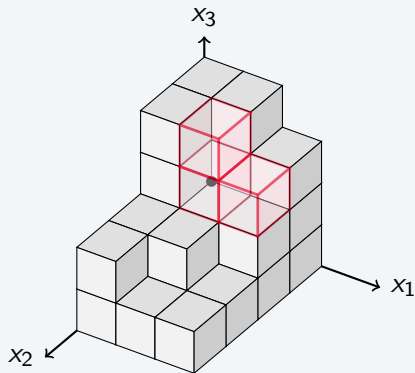
before insertion

Tree before insertion



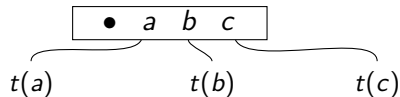
Insertion of $m = x_1^{m_1} m'$ in the ideal n -tree t of I

Geometric intuition



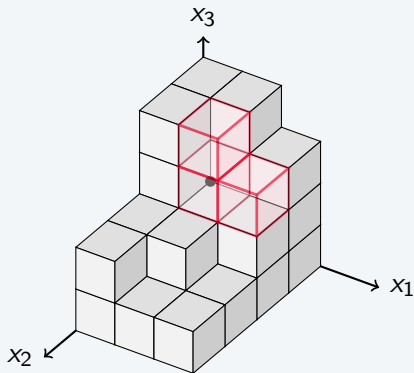
insert $m = x_1^{m_1} m'$

Tree before insertion



Insertion of $m = x_1^{m_1} m'$ in the ideal n -tree t of l

Geometric intuition



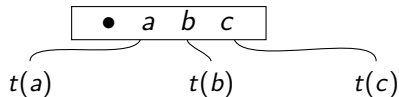
update slices $e \geq m_1$

Quotients

$$e < m_1 : (l + \langle m \rangle) / e = l / e$$

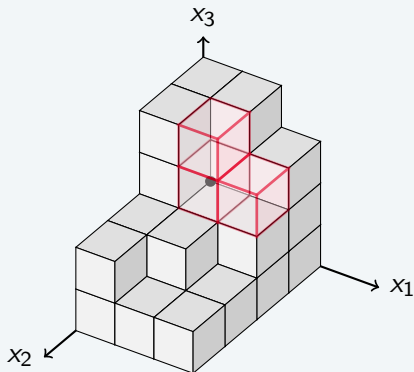
$$e \geq m_1 : (l + \langle m \rangle) / e = l / e + \langle m' \rangle$$

Tree before insertion



Insertion of $m = x_1^{m_1} m'$ in the ideal n -tree t of l

Geometric intuition



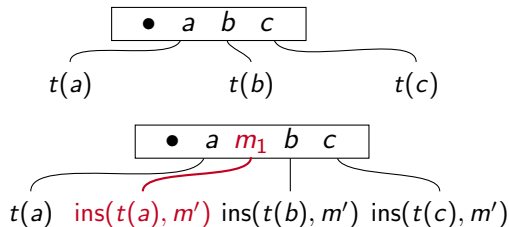
update slices $e \geq m_1$

Quotients

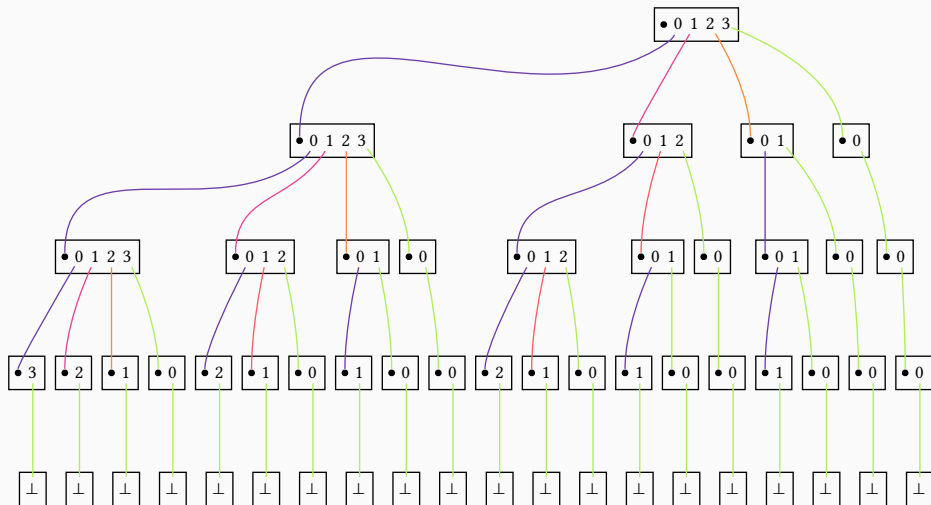
$$e < m_1 : (l + \langle m \rangle) / e = l / e$$

$$e \geq m_1 : (l + \langle m \rangle) / e = l / e + \langle m' \rangle$$

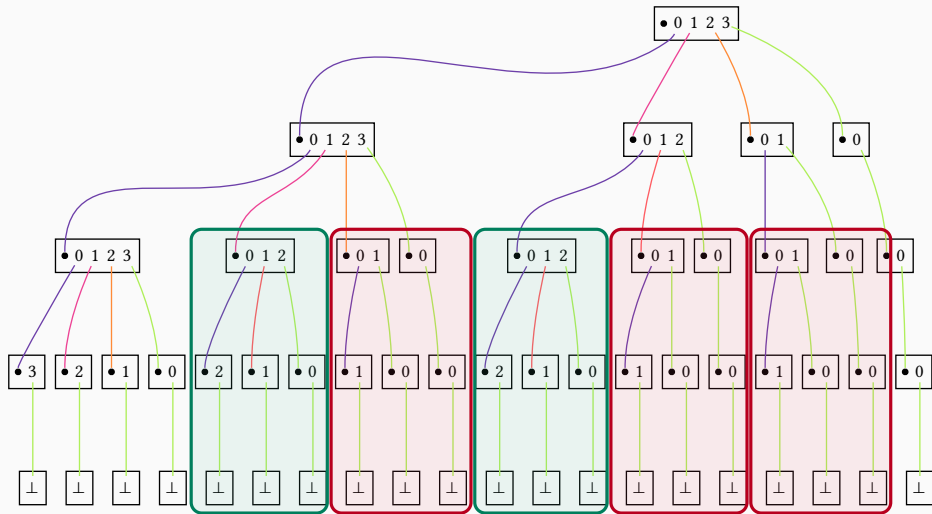
Tree update after insertion



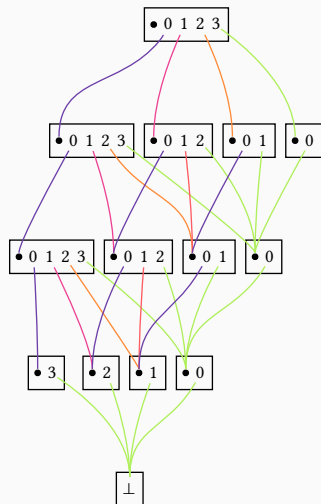
Problem of width for ideal n -trees



Problem of width for ideal n -trees



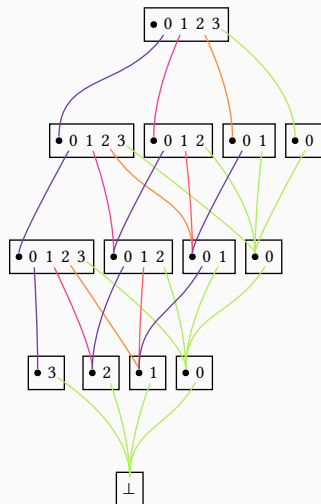
Solved problem of width with maximal sharing



Maximal sharing

Invariant: *structurally equal iff physically equal.*

Solved problem of width with maximal sharing

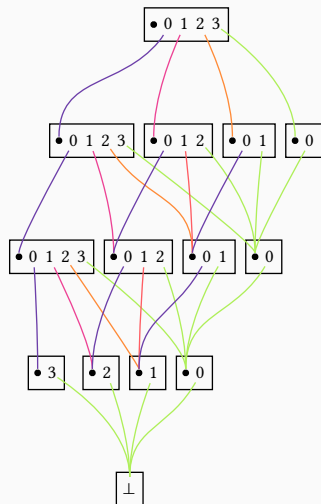


Maximal sharing

Invariant: *structurally equal* iff *physically equal*.

- Identical subtrees are stored only once.

Solved problem of width with maximal sharing

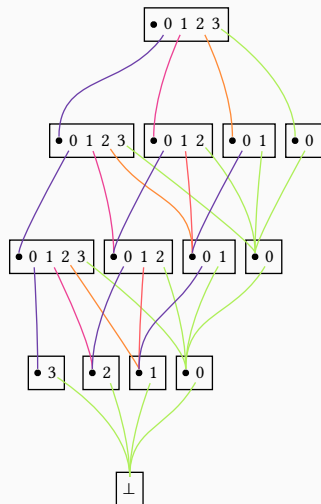


Maximal sharing

Invariant: *structurally equal* iff *physically equal*.

- Identical subtrees are stored only once.
- Memory savings by avoiding duplication.

Solved problem of width with maximal sharing

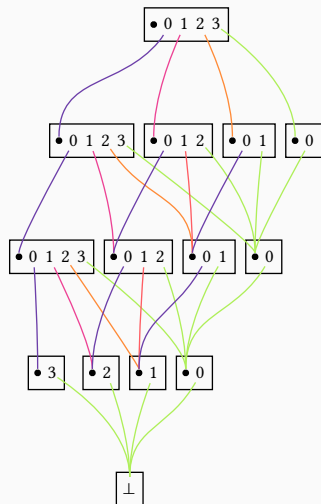


Maximal sharing

Invariant: *structurally equal* iff *physically equal*.

- Identical subtrees are stored only once.
- Memory savings by avoiding duplication.
- Enables memoization.

Solved problem of width with maximal sharing



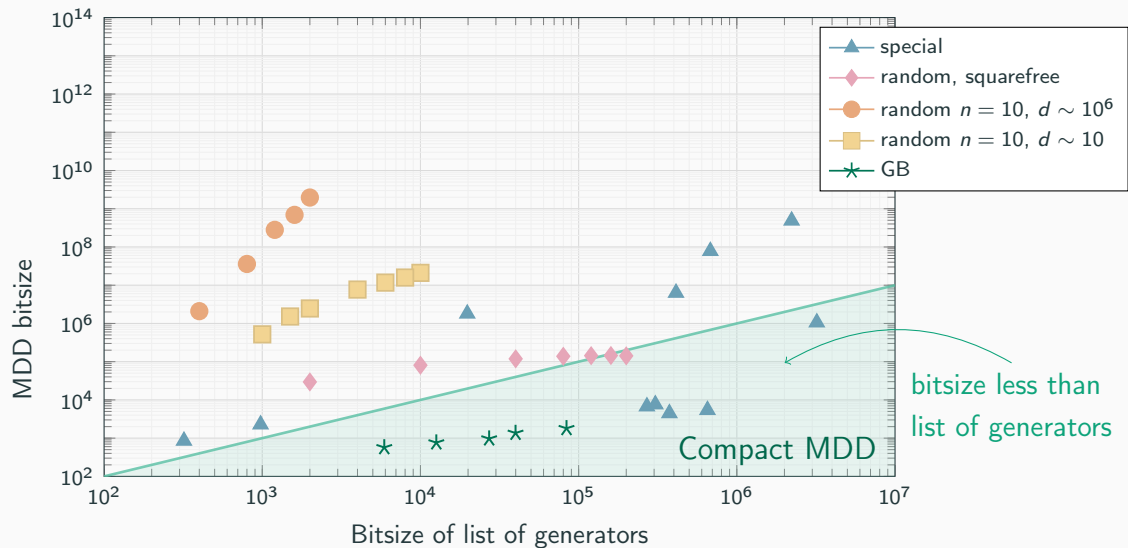
Maximal sharing

Invariant: *structurally equal iff physically equal.*

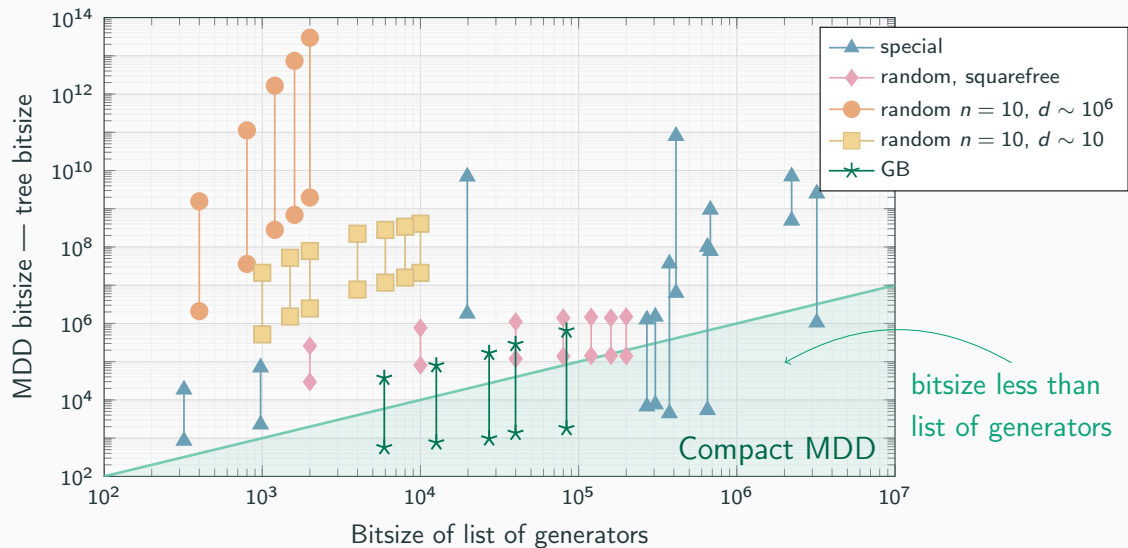
- Identical subtrees are stored only once.
- Memory savings by avoiding duplication.
- Enables memoization.

Result: Manipulation of ideal n -trees much faster and with less memory.

Experimental data on the bitsize of MDDs



Experimental data on the bitsize of MDDs



Initial ideal of eco^{14} (from Gröbner basis computations)



Bitsize of list of generators: 39928

Bitsize of MDD: 1360

Benchmarks on *AlgebraicSolving.jl*

name	<i>AlgebraicSolving.jl</i>		<i>AlgebraicSolving.jl</i> with MDD						
	time	% sig.	time	% sig.	test	MDD	size	nb tests	×
katsura ¹¹	4s	86%	2s	79%	0.04s	0.06s	81	388k	1.8
katsura ¹²	27s	83%	14s	70%	0.17s	0.27s	103	1.5M	2.0
katsura ¹³	3m21	82%	1m47	69%	0.71s	1.14s	125	5.9M	1.9
cyclic ⁷	1s	98%	0.8s	98%	0.02s	0.02s	43	240k	1.6
cyclic ⁸	1m08	95%	32s	89%	0.50s	0.36s	80	4.1M	2.1
eco ¹⁴	3h22	90%	1h09	68%	5.79s	0.92s	173	118M	2.9
noon ⁷	10s	87%	3s	60%	0.08s	0.02s	71	985k	3.1
noon ⁸	2m34	82%	44s	34%	0.63s	0.10s	101	7.4M	3.5
noon ⁹	1m18	99%	1m23	99%	0.58s	0.10s	71	7.2M	0.9

AlgebraicSolving.jl

Christian Eder (Kaiserslautern), Mohab Safey El Din (Sorbonne Université), Rafael Mohr (Leuven) and Rémi Prébet (Lyon).

Benchmarks on *AlgebraicSolving.jl*

name	<i>AlgebraicSolving.jl</i>		<i>AlgebraicSolving.jl</i> with MDD						
	time	% sig.	time	% sig.	test	MDD	size	nb tests	×
katsura ¹¹	4s	86%	2s	79%	0.04s	0.06s	81	388k	1.8
katsura ¹²	27s	83%	14s	70%	0.17s	0.27s	103	1.5M	2.0
katsura ¹³	3m21	82%	1m47	69%	0.71s	1.14s	125	5.9M	1.9
cyclic ⁷	1s	98%	0.8s	98%	0.02s	0.02s	43	240k	1.6
cyclic ⁸	1m08	95%	32s	89%	0.50s	0.36s	80	4.1M	2.1
eco ¹⁴	3h22	90%	1h09	68%	5.79s	0.92s	173	118M	2.9
noon ⁷	10s	87%	3s	60%	0.08s	0.02s	71	985k	3.1
noon ⁸	2m34	82%	44s	34%	0.63s	0.10s	101	7.4M	3.5
noon ⁹	1m18	99%	1m23	99%	0.58s	0.10s	71	7.2M	0.9

AlgebraicSolving.jl

Christian Eder (Kaiserslautern), Mohab Safey El Din (Sorbonne Université), Rafael Mohr (Leuven) and Rémi Prébet (Lyon).

MDD bitsize

Initial ideals from GB computations:

- Generic coordinates:
Borel-fixed (Galligo, 1974)

$$O(ndN)$$

- Generic systems: conjectured to be
Weakly revlex (Moreno–Socias, 1991)

$$O(nd^2)$$

Find reducer

Go beyond yes/no membership:

$m \in I \rightsquigarrow$ minimal generator index

Improve the symbolic part

Applications in commutative algebra

Hilbert series