Signature-based Möller's algorithm for strong Gröbner bases over PIDs

Maria Francis[1], Thibaut Verron[2]

1. Indian Institute of Technology Hyderabad, Hyderabad, India

2. Institute for Algebra, Johannes Kepler University, Linz, Austria

Journées Nationales de Calcul Formel, Luminy, 5 février 2019

Gröbner bases

- Valuable tool for many questions related to polynomial equations (solving, elimination, dimension of the solutions...)
- Classically used for polynomials over fields
- Some applications with coefficients in general rings (elimination, combinatorics...)

Definition (Leading term, monomial, coefficient)

R ring, $A = R[X_1, \ldots, X_n]$ with a monomial order $<$, $f = \sum a_i \mathbf{X}^{b_i}$

- Leading term $\mathrm{LT}(f) = a_i \mathbf{X}^{b_i}$ with $\mathbf{X}^{b_i} > \mathbf{X}^{b_j}$ if $j \neq i$
- Leading monomial $\mathrm{LM}(f) = \mathbf{X}^{b_i}$
- Leading coefficient $\mathrm{LC}(f) = a_i$

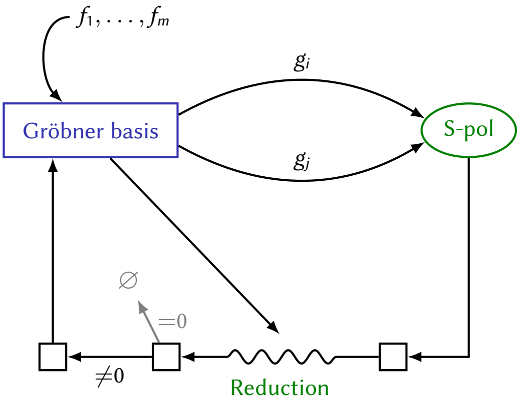
Definition (Weak/strong Gröbner basis)

$G \subset I = \langle f_1, \ldots, f_n \rangle$

- G is a weak Gröbner basis $\iff$ $\langle \mathrm{LT}(f) : f \in I \rangle = \langle \mathrm{LT}(g) : g \in G \rangle$
- G is a strong Gröbner basis $\iff$ for all $f \in I$, f reduces to 0 modulo G

Equivalent if R is a field

Buchberger's algorithm (*R* is a field)



(Strong) S-polynomial:

$$T(i,j) = \mathrm{lcm}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))$$

$$\text{S-Pol}(g_i, g_j) = \frac{T(i,j)}{\mathrm{LT}(g_i)} g_i - \frac{T(i,j)}{\mathrm{LT}(g_j)} g_j$$

(Strong) reduction:

$f \in A, g \in G$ s.t. $\mathrm{LT}(f) = c\mathbf{X}^a \mathrm{LT}(g)$

$f \rightsquigarrow h = f - c\mathbf{X}^a \mathrm{LT}(g)$ (and repeat)

[Faugère 2002 ; Gao, Guan, Volny 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

- Idea: keep track of the representation $g = \sum_i q_i f_i$ for $g \in \langle f_1, \dots, f_m \rangle$
- Work in the module $A^m = Ae_1 \oplus \cdots \oplus Ae_m$
- The algorithm could keep track of the full representation in the module...

  But it is expensive!
- Instead define a signature $\mathfrak{s}(g)$ of g as

$$\mathfrak{s}(g) = \mathrm{LT}(q_j)e_j \text{ for some representation } g = \sum_{i=1}^{m} q_i f_i,\ q_j \text{ being the last non-zero coef.}$$

- Signatures are ordered by

$$a\mathbf{X}^b e_i < a' \mathbf{X}^{b'} e_j \iff i < j \text{ or } i = j \text{ and } \mathbf{X}^b < \mathbf{X}^{b'}$$

- Keeping track of the signature is free if we restrict to regular S-pols and reductions!

Signatures (R is a field)

[Faugère 2002 ; Gao, Guan, Volny 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

- Idea: keep track of the representation $g = \sum_i q_i f_i$ for $g \in \langle f_1, \ldots, f_m \rangle$
- Work in the module $A^m = Ae_1 \oplus \cdots \oplus Ae_m$
- The algorithm could keep track of the full representation in the module...
  But it is expensive!

- Instead define a signature $\mathfrak{s}(g)$ of g as

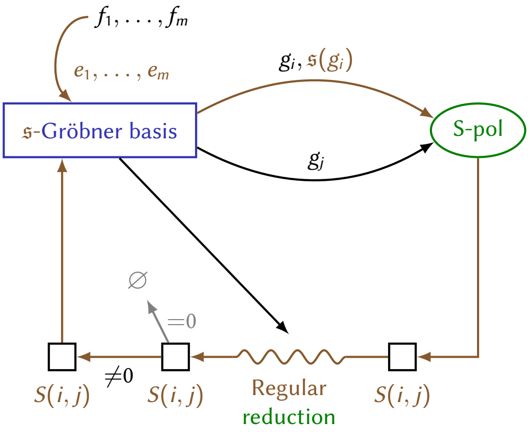
$$\mathfrak{s}(g) = \mathrm{LT}(q_j)e_j \text{ for some representation } g = \sum_{i=1}^{m} q_i f_i,\ q_j \text{ being the last non-zero coef.}$$

- Signatures are ordered by

$$a\mathbf{X}^b e_i < a' \mathbf{X}^{b'} e_j \iff i < j \text{ or } i = j \text{ and } \mathbf{X}^b < \mathbf{X}^{b'}$$

- Keeping track of the signature is free if we restrict to regular S-pols and reductions!

Buchberger's algorithm, with signatures (R is a field)



(Strong) S-polynomial:

$$T(i,j) = \mathrm{lcm}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))$$

$$\text{S-Pol}(g_i, g_j) = \frac{T(i,j)}{\mathrm{LT}(g_i)} g_i - \frac{T(i,j)}{\mathrm{LT}(g_j)} g_j$$

Regular: $\frac{T(i,j)}{\mathrm{LT}(g_i)} \mathfrak{s}(g_i) > \frac{T(i,j)}{\mathrm{LT}(g_j)} \mathfrak{s}(g_j)$

$$S(i,j) = \frac{T(i,j)}{\mathrm{LT}(g_i)} \mathfrak{s}(g_i)$$

(Strong) reduction:

$f \in A, g \in G$ s.t. $\mathrm{LT}(f) = c\mathbf{X}^a \mathrm{LT}(g)$

$f \rightsquigarrow h = f - c\mathbf{X}^a \mathrm{LT}(g)$ (and repeat)

Regular: $\mathfrak{s}(f) > \mathbf{X}^a \mathfrak{s}(g)$

$$\mathfrak{s}(h) = \mathfrak{s}(f)$$

Key property

Buchberger's algorithm with signatures computes GB elements with increasing signatures.

Main consequence

Buchberger's algorithm with signatures is correct!

Then we can add criteria...

Singular criterion: eliminate some redundant computations

If $\mathfrak{s}(g) \simeq \mathfrak{s}(g')$ then after regular reduction, $\mathrm{LM}(g) = \mathrm{LM}(g')$.

F5 criterion: eliminate Koszul syzygies $f_i f_j - f_j f_i = 0$

If $\mathfrak{s}(g) = \mathrm{LT}(g')e_j$ and $\mathfrak{s}(g') = \star e_i$ for some indices $i < j$, then g reduces to 0 modulo the already computed basis.

Context and main results: what about rings?

Type of rings	General rings	Principal domains	Euclidean domains
Type of GB	Weak	Strong	Strong
Algorithm	Möller weak	Möller strong	Lichtblau, Kandri-Rodi Kapur
Techniques	Weak S-pols Weak reductions	Strong S-pols Strong reductions G-pols	Strong S-pols Strong reductions G-pols LC reductions

- Eder, Popescu 2017: total order using absolute value of the coefficients
  $\to$ Impossible to avoid signature drops, signatures can decrease
- F, V 2018: partial order disregarding the coefficients
  $\to$ No signature drops, signatures don't decrease (but they may not increase)
- This work: same technique and results for Möller's strong GB algorithm

Context and main results: what about rings?

Type of rings	General rings	Principal domains	Euclidean domains
Type of GB	Weak	Strong	Strong
Algorithm	Möller weak	Möller strong	Lichtblau, Kandri-Rodi Kapur
Techniques	Weak S-pols Weak reductions	Strong S-pols Strong reductions G-pols	Strong S-pols Strong reductions G-pols LC reductions
With signatures			

Main difficulty: how to order the signatures with their coefficients?

- Eder, Popescu 2017: total order using absolute value of the coefficients
  → Impossible to avoid signature drops, signatures can decrease
- F, V 2018: partial order disregarding the coefficients
  → No signature drops, signatures don't decrease (but they may not increase)
- This work: same technique and results for Möller's strong GB algorithm

Context and main results: what about rings?

Type of rings	General rings	Principal domains	Euclidean domains
Type of GB	Weak	Strong	Strong
Algorithm	Möller weak	Möller strong	Lichtblau, Kandri-Rodi Kapur
Techniques	Weak S-pols Weak reductions	Strong S-pols Strong reductions G-pols	Strong S-pols Strong reductions G-pols LC reductions
With signatures			Eder, Popescu 2017

Main difficulty: how to order the signatures with their coefficients?

- Eder, Popescu 2017: total order using absolute value of the coefficients
  $\rightarrow$ Impossible to avoid signature drops, signatures can decrease
- F, V 2018: partial order disregarding the coefficients
  $\rightarrow$ No signature drops, signatures don't decrease (but they may not increase)
- This work: same technique and results for Möller's strong GB algorithm

Context and main results: what about rings?

Type of rings	General rings	Principal domains	Euclidean domains
Type of GB	Weak	Strong	Strong
Algorithm	Möller weak	Möller strong	Lichtblau, Kandri-Rodi Kapur
Techniques	Weak S-pols Weak reductions	Strong S-pols Strong reductions G-pols	Strong S-pols Strong reductions G-pols LC reductions
With signatures	F, V 2018 (for PIDs)		Eder, Popescu 2017

Main difficulty: how to order the signatures with their coefficients?

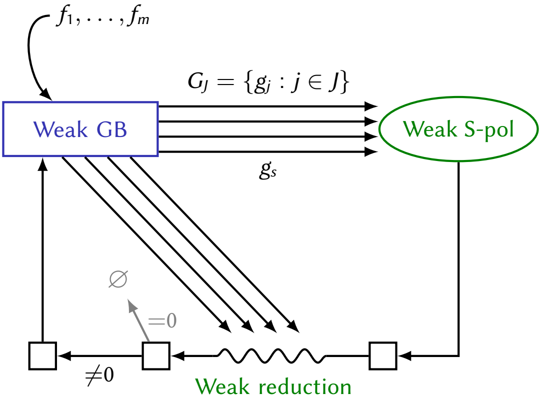
- Eder, Popescu 2017: total order using absolute value of the coefficients
  $\rightarrow$ Impossible to avoid signature drops, signatures can decrease
- F, V 2018: partial order disregarding the coefficients
  $\rightarrow$ No signature drops, signatures don't decrease (but they may not increase)
- This work: same technique and results for Möller's strong GB algorithm

Context and main results: what about rings?

Type of rings	General rings	Principal domains	Euclidean domains
Type of GB	Weak	Strong	Strong
Algorithm	Möller weak	Möller strong	Lichtblau, Kandri-Rodi Kapur
Techniques	Weak S-pols Weak reductions	Strong S-pols Strong reductions G-pols	Strong S-pols Strong reductions G-pols LC reductions
With signatures	F, V 2018 (for PIDs)	This work	Eder, Popescu 2017

Main difficulty: how to order the signatures with their coefficients?

- Eder, Popescu 2017: total order using absolute value of the coefficients
  $\rightarrow$ Impossible to avoid signature drops, signatures can decrease
- F, V 2018: partial order disregarding the coefficients
  $\rightarrow$ No signature drops, signatures don't decrease (but they may not increase)
- This work: same technique and results for Möller's strong GB algorithm



[Möller 1988]

Weak S-polynomial:

$$M(J) = \mathrm{lcm}(\mathrm{LM}(g_j) : j \in J)$$

$$\text{S-Pol}(G_J) = c\frac{M(J)}{\mathrm{LM}(g_s)}g_s - \sum b_j \frac{M(J)}{\mathrm{LM}(g_j)}g_j$$

Weak reduction:

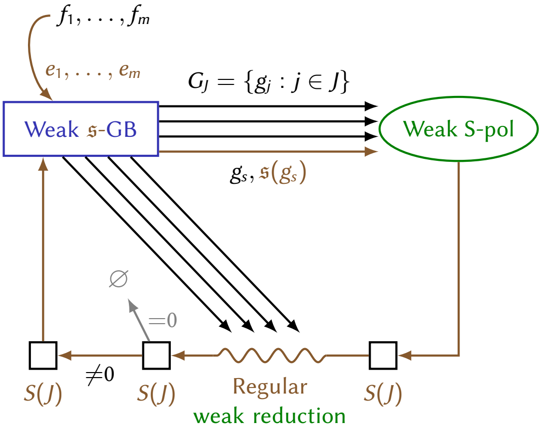
$f \in A, g_1, \ldots, g_k \in G$ s.t.

$$\begin{cases} \mathrm{LM}(f) = \mathbf{X}^{a_i}\mathrm{LT}(g_i) \\ \mathrm{LC}(f) = \sum c_i \mathrm{LC}(g_i) \end{cases}$$

$$f \rightsquigarrow h = f - \sum c_i \mathbf{X}^{a_i} g_i$$

(and repeat)

Möller's weak GB algorithm, with signatures (R is a Principal Ideal Domain)



[Möller 1988]

[F, V 2018]

Weak S-polynomial:

$$M(J) = \mathrm{lcm}(\mathrm{LM}(g_j) : j \in J)$$

$$\text{S-Pol}(G_J) = c\frac{M(J)}{\mathrm{LM}(g_s)}g_s - \sum b_j \frac{M(J)}{\mathrm{LM}(g_j)}g_j$$

Regular: $\forall\, j,\ \frac{M(J)}{\mathrm{LM}(g_s)}\mathfrak{s}(g_s) > \frac{M(J)}{\mathrm{LM}(g_j)}\mathfrak{s}(g_j)$

$$S(J) = c\frac{M(i,j)}{\mathrm{LM}(g_i)}\mathfrak{s}(g_i)$$

Weak reduction:

$f \in A, g_1, \dots, g_k \in G$ s.t.

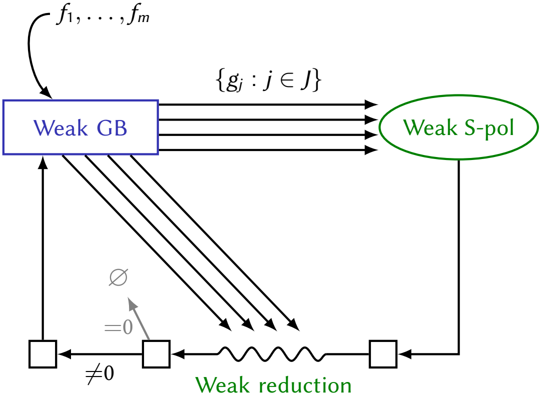
$$\begin{cases} \mathrm{LM}(f) = \mathbf{X}^{a_i}\mathrm{LT}(g_i) \\ \mathrm{LC}(f) = \sum c_i \mathrm{LC}(g_i) \end{cases}$$

$f \rightsquigarrow h = f - \sum c_i \mathbf{X}^{a_i} g_i$

(and repeat)

Regular: $\forall\, i,\ \mathfrak{s}(f) > \mathbf{X}^{a_i}\mathfrak{s}(g_i)$

$$\mathfrak{s}(h) = \mathfrak{s}(f)$$

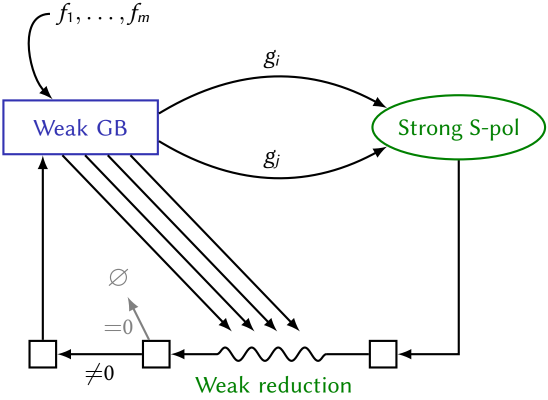


Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

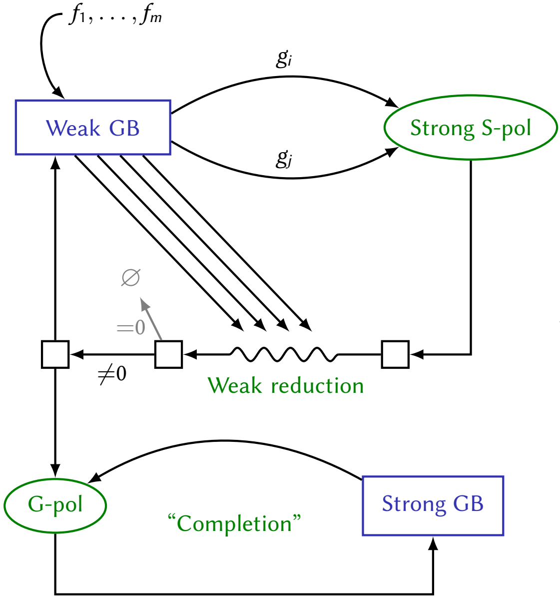


Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

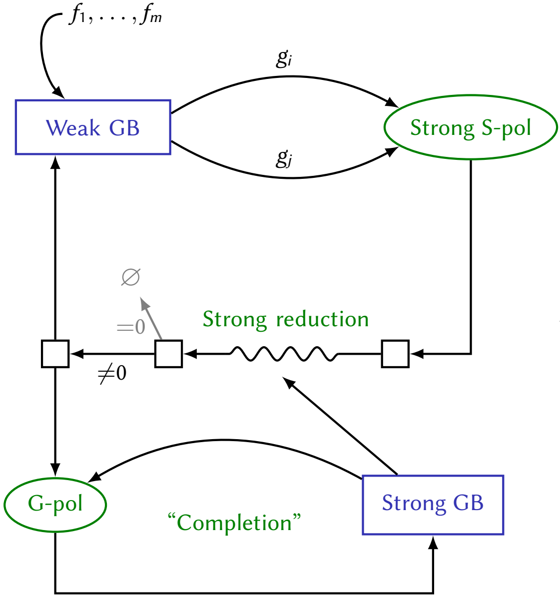
G-polynomial:

$$f = a\mathbf{X}^{\alpha} + \ldots,\ g = b\mathbf{X}^{\beta} + \ldots$$

$$\mathbf{X}^{\gamma} = \mathrm{lcm}(\mathbf{X}^{\alpha}, \mathbf{X}^{\beta})$$

$$d = \gcd(a, b) = au + bv$$

$$h = \text{G-Pol}(f, g) = u\frac{\mathbf{X}^{\gamma}}{\mathbf{X}^{\alpha}}f + v\frac{\mathbf{X}^{\gamma}}{\mathbf{X}^{\beta}}g = d\,\mathbf{X}^{\gamma} + \ldots$$



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

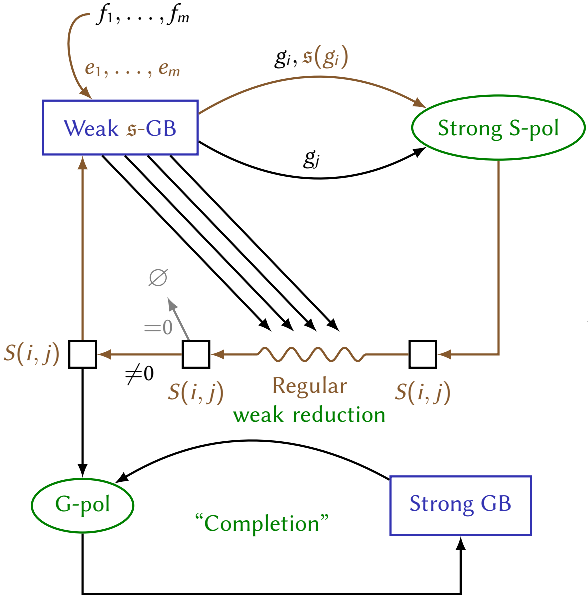
$$f = a\mathbf{X}^\alpha + \dots, \; g = b\mathbf{X}^\beta + \dots$$

$$\mathbf{X}^\gamma = \mathrm{lcm}(\mathbf{X}^\alpha, \mathbf{X}^\beta)$$

$$d = \gcd(a, b) = au + bv$$

$$h = \text{G-Pol}(f, g) = u\frac{\mathbf{X}^\gamma}{\mathbf{X}^\alpha}f + v\frac{\mathbf{X}^\gamma}{\mathbf{X}^\beta}g = d\,\mathbf{X}^\gamma + \dots$$

Möller's strong GB algorithm, with signatures (R is a PID)



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

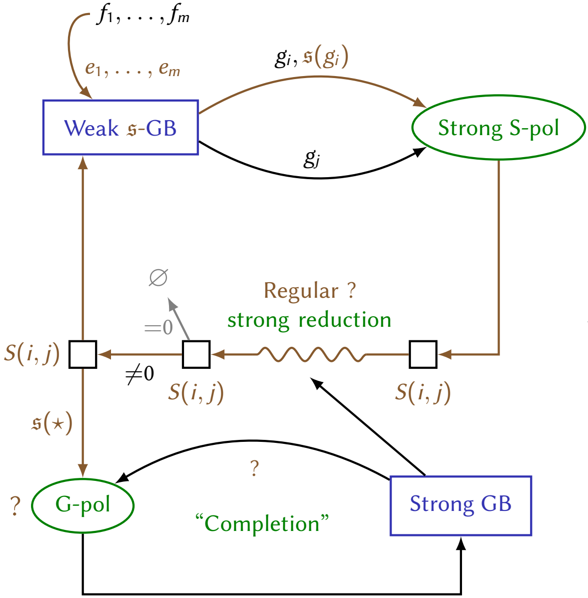
$$f = a\mathbf{X}^\alpha + \dots,\ g = b\mathbf{X}^\beta + \dots$$

$$\mathbf{X}^\gamma = \operatorname{lcm}(\mathbf{X}^\alpha, \mathbf{X}^\beta)$$

$$d = \gcd(a,b) = au + bv$$

$$h = \text{G-Pol}(f,g) = u\frac{\mathbf{X}^\gamma}{\mathbf{X}^\alpha}f + v\frac{\mathbf{X}^\gamma}{\mathbf{X}^\beta}g = d\,\mathbf{X}^\gamma + \dots$$

Möller's strong GB algorithm, with signatures (R is a PID)



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

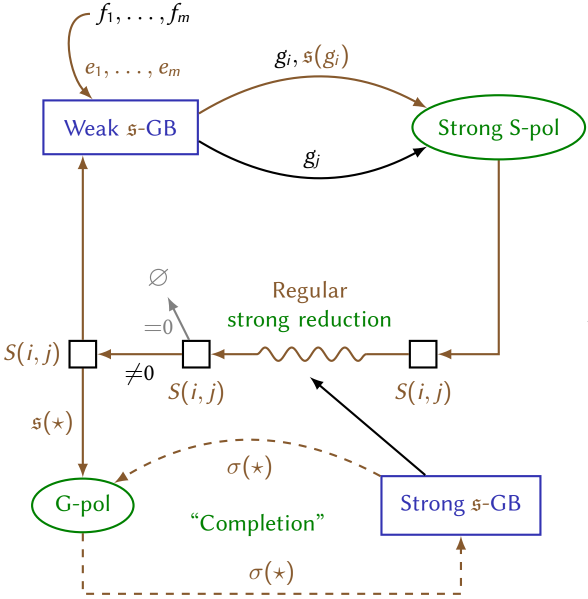
$$f = a\mathbf{X}^\alpha + \dots,\ g = b\mathbf{X}^\beta + \dots$$

$$\mathbf{X}^\gamma = \operatorname{lcm}(\mathbf{X}^\alpha, \mathbf{X}^\beta)$$

$$d = \gcd(a,b) = au + bv$$

$$h = \text{G-Pol}(f,g) = u\frac{\mathbf{X}^\gamma}{\mathbf{X}^\alpha} f + v\frac{\mathbf{X}^\gamma}{\mathbf{X}^\beta} g$$
$$= d\,\mathbf{X}^\gamma + \dots$$

Möller's strong GB algorithm, with signatures (R is a PID)



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

$f = a\mathbf{X}^{\alpha} + \dots,\ g = b\mathbf{X}^{\beta} + \dots$

$\mathbf{X}^{\gamma} = \operatorname{lcm}(\mathbf{X}^{\alpha}, \mathbf{X}^{\beta})$

$d = \gcd(a, b) = au + bv$

$$h = \text{G-Pol}(f, g) = u\frac{\mathbf{X}^{\gamma}}{\mathbf{X}^{\alpha}} f + v\frac{\mathbf{X}^{\gamma}}{\mathbf{X}^{\beta}} g = d\,\mathbf{X}^{\gamma} + \dots$$

$\sigma(h) = \max\left(\frac{\mathbf{X}^{\gamma}}{\mathbf{X}^{\alpha}}\mathfrak{s}(f), \frac{\mathbf{X}^{\gamma}}{\mathbf{X}^{\beta}}\sigma(g)\right)$

$\sigma(h)$ may be $> \mathfrak{s}(\text{G-Pol}(f, g))$!

Results

- Signature-based variant of Möller's strong GB algorithm
  - Computes strong $\mathfrak{s}$-Gröbner bases over principal domains
  - Signatures (even σ) do not decrease throughout the algorithm
  - Proof of correctness and termination
  - Compatible with Buchberger's criteria and signature criteria
- Implemented and tested in Magma

Experimental data

Toy implementation of the algorithm in Magma:
`https://github.com/ThibautVerron/SignatureMoller`

Algorithm	Pairs	S-pols	Coprime	Chain	F5	Sing.	1-sing.	0 red.
Weak, sigs	2227	51	0	0	2125	51	0	0
Strong, no sigs	1191	344	251	596	0	0	0	282
Strong, sigs	472	178	157	153	115	1	6	0

Katsura-3 system (in $\mathbb{Z}[X_1, \dots, X_4]$)

Algorithm	Pairs	S-pols	Coprime	Chain	F5	Sing.	1-sing.	0 red.
Strong, no sigs	2712	837	759	1116	0	0	0	739
Strong, sigs	1594	603	509	517	388	9	84	0

Katsura-4 system (in $\mathbb{Z}[X_1, \dots, X_5]$)

Results and future work

- Signature-based variant of Möller's strong GB algorithm
  - Computes strong $\mathfrak{s}$-Gröbner bases over principal domains
  - Signatures (even σ) do not decrease throughout the algorithm
  - Proof of correctness and termination
  - Compatible with Buchberger's criteria and signature criteria
- Implemented and tested in Magma
- Main bottlenecks: basis growth and coefficient swell
- Next steps, work on those problems:
  - For basis growth: more inclusive singular criterion?
  - For coefficient swell: further optimizations over Euclidean rings?
  - Lichtblau / Kandri-Rodi, Kapur's idea : Euclidean reduction of leading coefficients

Results and future work

- Signature-based variant of Möller's strong GB algorithm
  - Computes strong $\mathfrak{s}$-Gröbner bases over principal domains
  - Signatures (even σ) do not decrease throughout the algorithm
  - Proof of correctness and termination
  - Compatible with Buchberger's criteria and signature criteria
- Implemented and tested in Magma
- Main bottlenecks: basis growth and coefficient swell
- Next steps, work on those problems:
  - For basis growth: more inclusive singular criterion?
  - For coefficient swell: further optimizations over Euclidean rings?
  - Lichtblau / Kandri-Rodi, Kapur's idea : Euclidean reduction of leading coefficients

Thank you for your attention!

More information and references:

- Möller's weak GB with signatures ► Maria Francis and Thibaut Verron (2018). 'A Signature-based Algorithm for Computing Gröbner Bases over Principal Ideal Domains'. In: *ArXiv e-prints*. arXiv: `1802.01388 [cs.SC]`
- Möller's strong GB with signatures ► Maria Francis and Thibaut Verron (2019). 'Signature-based Möller's Algorithm for strong Gröbner Bases over PIDs'. In: *ArXiv e-prints*. arXiv: `1901.09586 [cs.SC]`