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

SIAM Conference on Applied Algebraic Geometry

Mini-symposium *Algebraic methods for polynomial system solving*

13 July 2019, University of Bern, Switzerland

Gröbner bases

$\mathbf{X}^{\mathbf{a}} = X_1^{a_1} \cdots X_n^{a_n}$

- 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...)
- $\mathbb{Z}[X_1, \ldots, X_n]$ is a central object in algebraic geometry

Leading term, monomial, coefficient: R ring, $A = R[X_1, \ldots, X_n]$ with a monomial order $<$

$$f = \overbrace{\underbrace{c}_{\mathrm{LC}(f)} \cdot \underbrace{\mathbf{X}^{\mathbf{a}}}_{\mathrm{LM}(f)}}^{\mathrm{LT}(f)} + \text{ smaller terms}$$

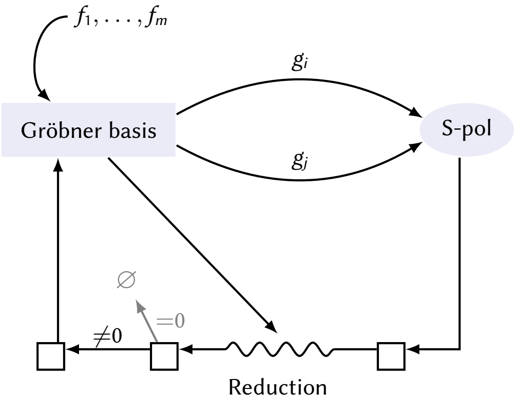
Definition (Weak/strong Gröbner basis)

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

- 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:

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

(Strong) reduction:

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

Why signatures?

Problem: useless and redundant computations

Example with a S-polynomial

$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + p_m f_m$ $\qquad$ $q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + q_m f_m$

$\text{S-Pol}(p, q) = \mu p - \nu q$

Why signatures?

Problem: useless and redundant computations

- 1st idea: keep track of the representation of the ideal elements [Möller, Mora, Traverso 1992]

Example with a S-polynomial

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + p_m f_m \qquad q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + q_m f_m$$

$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + p_m \mathbf{e}_m \qquad \mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + q_m \mathbf{e}_m$$

$$\text{S-Pol}(p, q) = \mu p - \nu q$$

$$\text{S-Pol}(\mathbf{p}, \mathbf{q}) = \mu \left(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + p_m \mathbf{e}_m \right) - \nu \left(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + q_m \mathbf{e}_m \right)$$

Why signatures?

Problem: useless and redundant computations

- 1st idea: keep track of the representation of the ideal elements [Möller, Mora, Traverso 1992]
- 2nd idea: we do not need the full representation, the largest term is enough [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

Example with a S-polynomial

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + 0\, f_m \qquad q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + 0\, f_m$$

$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m \qquad \mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m$$

$$= \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \qquad = \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}$$

"Position over term": $\mathbf{X^a}\mathbf{e}_i < \mathbf{X^b}\mathbf{e}_j$ if $\begin{cases} i < j \\ \text{or } i = j \text{ and } \mathbf{X^a} < \mathbf{X^b} \end{cases}$

$$\text{S-Pol}(p, q) = \mu p - \nu q$$

$$\text{S-Pol}(\mathbf{p}, \mathbf{q}) = \mu\,(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m) - \nu\,(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m)$$

$$= \mu \mathrm{LT}(p_k)\mathbf{e}_k - \nu \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}$$

Why signatures?

Problem: useless and redundant computations

- 1st idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2nd idea: we do not need the full representation, the largest term is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

Example with a S-polynomial

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + 0\, f_m \qquad q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + 0\, f_m$$

$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m \qquad \mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m$$

$$= \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \qquad = \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}$$

"Position over term": $\mathbf{X}^{\mathbf{a}}\mathbf{e}_i < \mathbf{X}^{\mathbf{b}}\mathbf{e}_j$ if $\begin{cases} i < j \\ \text{or } i = j \text{ and } \mathbf{X}^{\mathbf{a}} < \mathbf{X}^{\mathbf{b}} \end{cases}$

$$\text{S-Pol}(p, q) = \mu p - \nu q$$

$$\begin{aligned} \text{S-Pol}(\mathbf{p}, \mathbf{q}) &= \mu\,(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m) - \nu\,(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m) \\ &= \mu \mathrm{LT}(p_k)\mathbf{e}_k - \nu \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms} \\ &= \mu \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \quad \text{if } \mu \mathrm{LT}(p_k) \gtrsim \nu \mathrm{LT}(q_l)\mathbf{e}_l \end{aligned}$$

Why signatures?

Problem: useless and redundant computations

- 1st idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2nd idea: we do not need the full representation, the largest term is enough
  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]

Example with a S-polynomial

$$p = p_1 f_1 + p_2 f_2 + \cdots + p_k f_k + \cdots + 0\, f_m \qquad q = q_1 f_1 + q_2 f_2 + \cdots + q_l f_l + \cdots + 0\, f_m$$

$$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m \qquad \mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m$$

$$= \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \qquad = \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms}$$

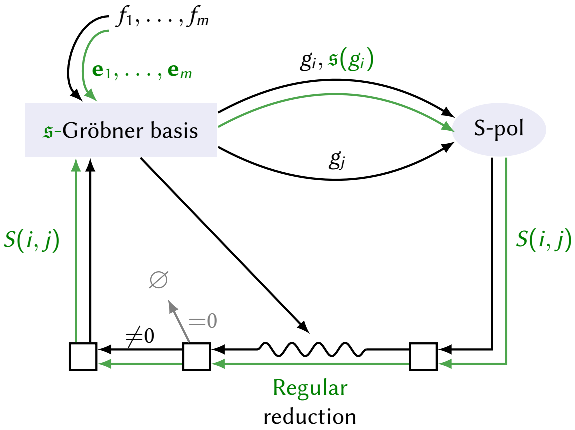
$\mathfrak{s}(p) =$ signature of p

"Position over term": $\mathbf{X}^{\mathbf{a}}\mathbf{e}_i < \mathbf{X}^{\mathbf{b}}\mathbf{e}_j$ if $\begin{cases} i < j \\ \text{or } i = j \text{ and } \mathbf{X}^{\mathbf{a}} < \mathbf{X}^{\mathbf{b}} \end{cases}$

$$\text{S-Pol}(p, q) = \mu p - \nu q$$

$$\begin{aligned} \text{S-Pol}(\mathbf{p}, \mathbf{q}) &= \mu\,(p_1 \mathbf{e}_1 + \cdots + p_k \mathbf{e}_k + \cdots + 0\, \mathbf{e}_m) - \nu\,(q_1 \mathbf{e}_1 + \cdots + q_l \mathbf{e}_l + \cdots + 0\, \mathbf{e}_m) \\ &= \mu \mathrm{LT}(p_k)\mathbf{e}_k - \nu \mathrm{LT}(q_l)\mathbf{e}_l + \text{smaller terms} \\ &= \mu \mathrm{LT}(p_k)\mathbf{e}_k + \text{smaller terms} \quad \text{if } \mu \mathrm{LT}(p_k) \gneq \nu \mathrm{LT}(q_l)\mathbf{e}_l \end{aligned}$$

Regular S-polynomial



(Strong) S-polynomial:

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

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:

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

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

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

Consequences of signatures (R is a field)

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?

Buchberger (1965)
Faugère: F4 (1999)
Field $\vdots$

Context and main results: what about rings?

Field

Buchberger (1965)
Faugère: F4 (1999)
⋮

General (Noetherian) ring

Möller weak (1988)

Context and main results: what about rings?

Buchberger (1965)
Faugère: F4 (1999)
⋮

Field

Möller strong (1988)
Lichtblau (2012)

Principal ideal domain

General (Noetherian) ring

Möller weak (1988)

Context and main results: what about rings?

Buchberger (1965)
Faugère: F4 (1999)
Field ⋮

Euclidean ring — Kandri-Rody, Kapur (1988)

Principal ideal domain — Möller strong (1988)
Lichtblau (2012)

General (Noetherian) ring — Möller weak (1988)

Context and main results: what about rings?

Field	Buchberger (1965) $\longrightarrow$ B. with sig. Faugère: F4 (1999) $\longrightarrow$ F5 (2002) ⋮
Euclidean ring	Kandri-Rody, Kapur (1988)
Principal ideal domain	Möller strong (1988) Lichtblau (2012)
General (Noetherian) ring	Möller weak (1988)

Coefficients
can be thrown away

Coefficients
can be ordered

Main question with signatures: how to order the coefficients of the signatures?

Context and main results: what about rings?

Buchberger (1965) $\longrightarrow$ B. with sig.
Faugère: F4 (1999) $\longrightarrow$ F5 (2002)

Field

$\vdots$

Euclidean ring — Kandri-Rody, Kapur (1988)

Principal ideal domain — Möller strong (1988), Lichtblau (2012)

General (Noetherian) ring — Möller weak (1988)

Coefficients can be thrown away

Coefficients can be ordered

Main question with signatures: how to order the coefficients of the signatures?

With a total order, signature drops cannot be avoided [Eder, Popescu 2017]

Context and main results: what about rings?

Field

Buchberger (1965) $\longrightarrow$ B. with sig.

Faugère: F4 (1999) $\longrightarrow$ F5 (2002)

$\vdots$

Euclidean ring — Kandri-Rody, Kapur (1988)

Principal ideal domain — Möller weak (1988), Möller strong (1988), Lichtblau (2012)

General (Noetherian) ring — Möller weak (1988)

Coefficients can be thrown away

Coefficients can be ordered

Coefficients must be kept but can be ignored

Main question with signatures: how to order the coefficients of the signatures?

With a total order, signature drops cannot be avoided [Eder, Popescu 2017]

But with a partial order, signatures cannot decrease [Francis, V. 2018] (weak)

Context and main results: what about rings?

Buchberger (1965) $\longrightarrow$ B. with sig.
Faugère: F4 (1999) $\longrightarrow$ F5 (2002)
$\vdots$

Field	Buchberger (1965) $\longrightarrow$ B. with sig.; Faugère: F4 (1999) $\longrightarrow$ F5 (2002); $\vdots$
Euclidean ring	Kandri-Rody, Kapur (1988)
Principal ideal domain	Möller weak (1988); Möller strong (1988); Lichtblau (2012)
General (Noetherian) ring	Möller weak (1988)

Coefficients can be thrown away

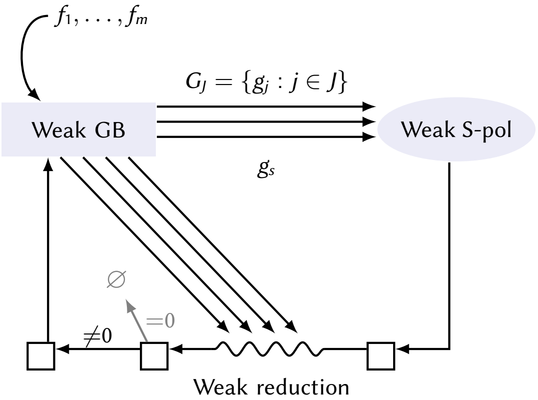
Coefficients can be ordered

Coefficients must be kept but can be ignored

Main question with signatures: how to order the coefficients of the signatures?

With a total order, signature drops cannot be avoided [Eder, Popescu 2017]

But with a partial order, signatures cannot decrease [Francis, V. 2018] (weak) [Francis, V. 2019] (strong)



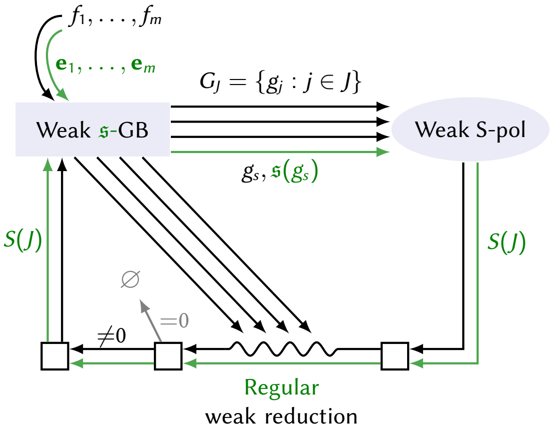
Weak S-polynomial:

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

Weak reduction:

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

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



Weak S-polynomial:

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

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

Weak reduction:

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

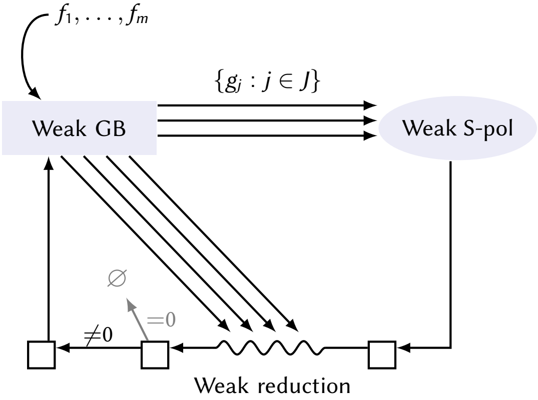
Regular: $\forall\, i,\ \mathfrak{s}(f) > \mathbf{X}^{\mathbf{a}_i}\mathfrak{s}(g_i)$

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

Theorem [Francis, V., 2018]

Signatures $\mathfrak{s}$ do not decrease.

The algorithm is correct.

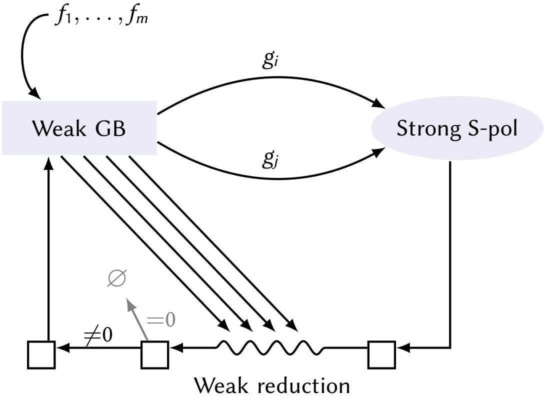


Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

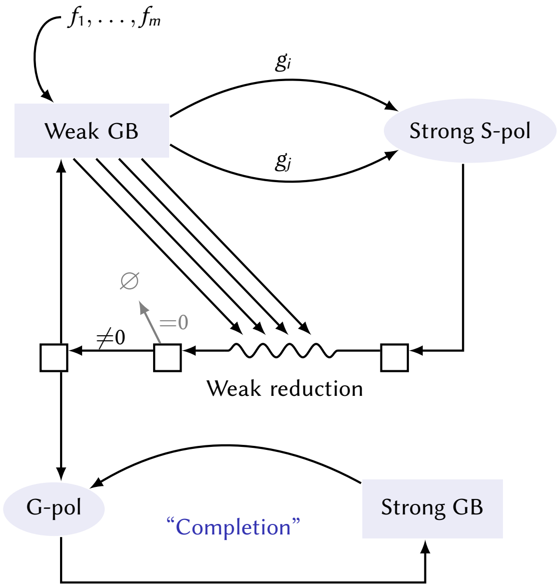


Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger



Weak S-pols and reductions:

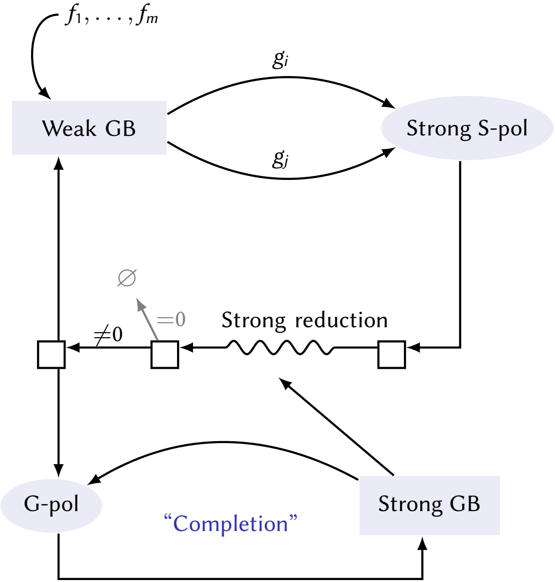
Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

$$h = \text{G-Pol} = u\frac{\mathrm{lcm}(\ldots)}{\mathrm{LM}(f)}f + v\frac{\mathrm{lcm}(\ldots)}{\mathrm{LM}(g)}g$$



Weak S-pols and reductions:

Same as in Möller's weak GB

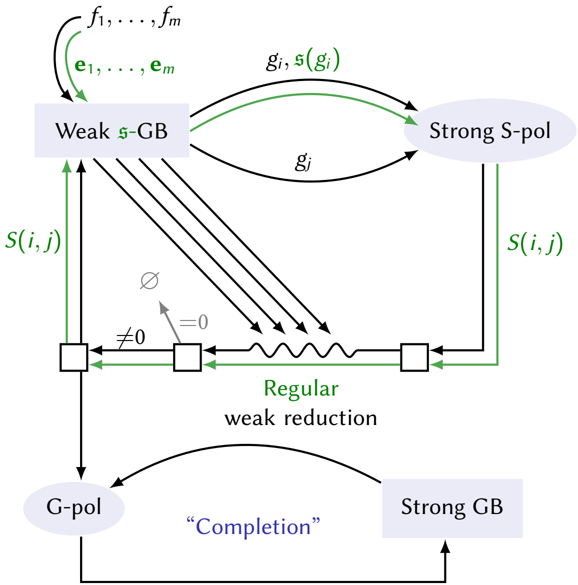
Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

$$h = \text{G-Pol} = u\frac{\mathrm{lcm}(\dots)}{\mathrm{LM}(f)}f + v\frac{\mathrm{lcm}(\dots)}{\mathrm{LM}(g)}g$$

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



Weak S-pols and reductions:

Same as in Möller's weak GB

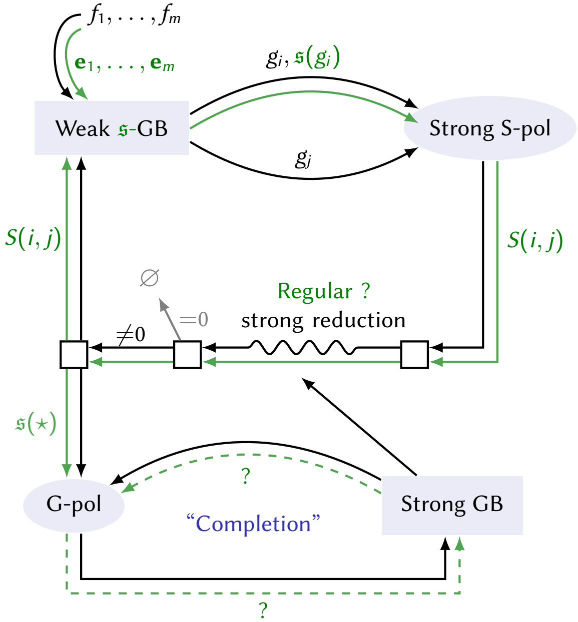
Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

$$h = \text{G-Pol} = u\frac{\mathrm{lcm}(\ldots)}{\mathrm{LM}(f)}f + v\frac{\mathrm{lcm}(\ldots)}{\mathrm{LM}(g)}g$$

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



Weak S-pols and reductions:

Same as in Möller's weak GB

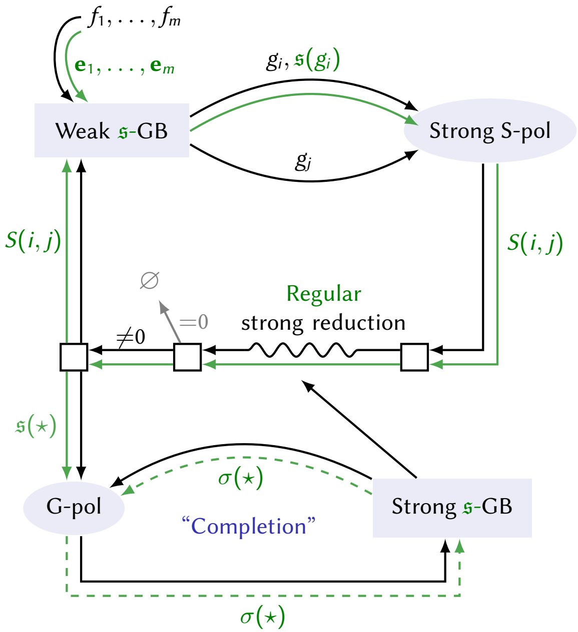
Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

$$h = \text{G-Pol} = u\frac{\text{lcm}(\ldots)}{\text{LM}(f)}f + v\frac{\text{lcm}(\ldots)}{\text{LM}(g)}g$$

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

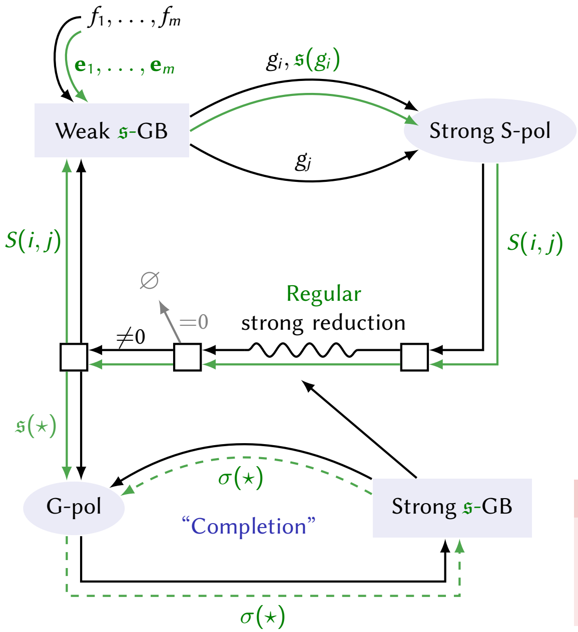
G-polynomial:

$$h = \text{G-Pol} = u\frac{\operatorname{lcm}(\ldots)}{\operatorname{LM}(f)}f + v\frac{\operatorname{lcm}(\ldots)}{\operatorname{LM}(g)}g$$

$$\sigma(h) = \max\left(\frac{\mathbf{x^c}}{\mathbf{x^a}}\mathfrak{s}(f), \frac{\mathbf{x^c}}{\mathbf{x^b}}\sigma(g)\right)$$

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

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:

$$h = \text{G-Pol} = u\frac{\mathrm{lcm}(\dots)}{\mathrm{LM}(f)}f + v\frac{\mathrm{lcm}(\dots)}{\mathrm{LM}(g)}g$$

$$\sigma(h) = \max\left(\frac{\mathbf{x}^{\mathbf{c}}}{\mathbf{x}^{\mathbf{a}}}\mathfrak{s}(f), \frac{\mathbf{x}^{\mathbf{c}}}{\mathbf{x}^{\mathbf{b}}}\sigma(g)\right)$$

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

Theorem [Francis, V., 2019]

Signatures ($\mathfrak{s}$ and σ) do not decrease.

The algorithm is correct.

Results

- Signature-based variant of Möller's strong GB algorithm
  - Computes strong $\mathfrak{s}$-Gröbner bases over principal domains without signature drops
  - 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 (red)	Added as pairs, not S-pols: Copr.	Chain	Added as S-pols, not reduced: F5	Sing.	Reduced, thrown away: 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 (62)	157	153	115	1	6	0

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

Algorithm	Pairs	S-pols (red)	Copr.	Chain	F5	Sing.	1-sing.	0 red.
Strong, no sigs	2712	837	759	1116	0	0	0	739
Strong, sigs	1594	603 (206)	509	517	388	9	84	0

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

Results and future work

- Signature-based variant of Möller's strong GB algorithm
  - Computes strong $\mathfrak{s}$-Gröbner bases over principal domains without signature drops
  - Proof of correctness and termination
  - Compatible with Buchberger's criteria and signature criteria
- Implemented and tested in Magma
- Main bottlenecks: basis and coefficients growth
- Next steps
  - More inclusive singular criterion against basis growth
  - Lichtblau's idea: mixing S-pols and G-pols in a single basis
  - Euclidean reduction of coefficients against coefficient growth
  - In each case, need to prove that the new algorithm is correct

---

Thank you for your attention!

More information and references:

- Möller's weak GB with signatures ▶ Maria Francis and Thibaut Verron (Feb. 2018). 'A Signature-Based Algorithm for Computing Gröbner Bases over Principal Ideal Domains'. In: *Mathematics in Computer Science, Special issue on the ACA 2018 Conference*. To appear. arXiv: 1802.01388 [cs.SC]
- Möller's strong GB with signatures ▶ Maria Francis and Thibaut Verron (Jan. 2019). 'Signature-based Möller's Algorithm for strong Gröbner Bases over PIDs'. In: *ArXiv e-prints*. arXiv: 1901.09586 [cs.SC]