Signature-based algorithms for computing Gröbner bases over Principal Ideal Domains

Maria Francis[1], Thibaut Verron[2]

1. Indian Institute of Technology Hyderabad, Hyderabad, India
2. Institute for Algebra, Johannes Kepler University, Linz, Austria

Séminaire *Algebra and Discrete Mathematics*, Johannes Kepler University, Linz

21 March 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...)

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…)

Many algorithms for fields

- First algorithm: Buchberger (1965)
- Optimizations related to selection strategies: “Normal” (1985), “Sugar” (1991)
- Criteria: Buchberger’s coprime and chain criteria (1979), Gebauer-Möller (1988)
- Replace polynomial arithmetic with linear algebra: Lazard (1983), F4 (1999)
- Signature-based criteria: F5 (2002), GVW (2010)…

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...)

Many algorithms for fields

- First algorithm: Buchberger (1965)
- Optimizations related to selection strategies: "Normal" (1985), "Sugar" (1991)
- Criteria: Buchberger's coprime and chain criteria (1979), Gebauer-Möller (1988)
- Replace polynomial arithmetic with linear algebra: Lazard (1983), F4 (1999)
- Signature-based criteria: F5 (2002), GVW (2010)...

And for rings:

- Möller (1988) for general rings and principal domains, Kandri-Rodi Kapur (1988) for Euclidean domains...
- Optimizations and general criteria are still available
- What about signatures?

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...)

Many algorithms for fields

- First algorithm: Buchberger (1965)
- Optimizations related to selection strategies: "Normal" (1985), "Sugar" (1991)
- Criteria: Buchberger's coprime and chain criteria (1979), Gebauer-Möller (1988)
- Replace polynomial arithmetic with linear algebra: Lazard (1983), F4 (1999)
- Signature-based criteria: F5 (2002), GVW (2010)...

And for rings:

- Möller (1988) for general rings and principal domains, Kandri-Rodi Kapur (1988) for Euclidean domains...
- Optimizations and general criteria are still available
- What about signatures?

This work: signature-based algorithms for PIDs

Outline

1. Reminders about Gröbner bases over fields
   - Gröbner bases, Buchberger's algorithm
   - Signatures

2. Algorithms for rings
   - Adding signatures to Möller's weak GB algorithm
   - Adding signatures to Möller's strong GB algorithm

3. Proofs and experiments
   - Skeleton of the proofs
   - Experimental data
   - Future work

Outline

1. Reminders about Gröbner bases over fields
   - Gröbner bases, Buchberger's algorithm
   - Signatures
2. Algorithms for rings
   - Adding signatures to Möller's weak GB algorithm
   - Adding signatures to Möller's strong GB algorithm
3. Proofs and experiments
   - Skeleton of the proofs
   - Experimental data
   - Future work

Definition (Leading term, monomial, coefficient)

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

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

Definition (Weak/strong Gröbner basis)

$G \subset \mathfrak{a} = \langle f_1, \ldots, f_n \rangle$

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

Equivalent if R is a field

Gröbner bases: basic constructions (R is a field)

$f \in A = R[X]$, $G = \{g_1, \ldots, g_s\} \subset A$

Definition (S-polynomial)

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

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

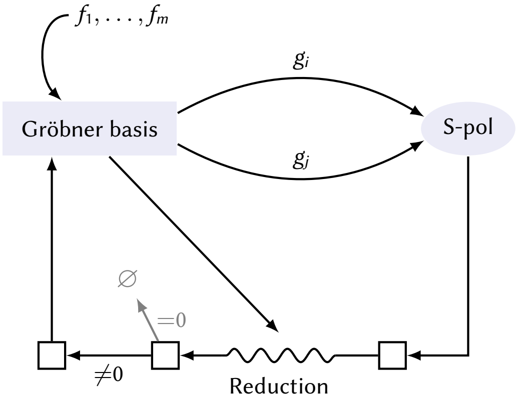
Definition (Reduction)

If $\mathrm{LT}(f) = cX^a \mathrm{LT}(g_i)$, then f reduces to $h = f - cX^a g$ modulo G.

We use the same word for the transitive closure of the relation.

Buchberger's criterion

G is a (strong) Gröbner basis $\iff$ for all $i, j \in \{1, \ldots, s\}$, S-Pol$(g_i, g_j)$ reduces to 0 modulo G.



(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:

$$f \rightsquigarrow h = f - cX^a \mathrm{LT}(g)$$

- 1st idea: keep track of the representation $g = \sum_i q_i f_i$ for $g \in \langle f_1, \dots, f_m \rangle$ [Möller, Mora, Traverso 1992]
- Work in the module $A^m = A\mathbf{e}_1 \oplus \cdots \oplus A\mathbf{e}_m$ with $\bar{\cdot} : \mathbf{e}_i \mapsto \bar{\mathbf{e}}_i = f_i$
- Example: S-polynomial: $\text{S-Pol}(\mathbf{g}_i, \mathbf{g}_j) = \dfrac{T(i,j)}{T(i)}\mathbf{g}_i - \dfrac{T(i,j)}{T(j)}\mathbf{g}_j$
- This computation is expensive!

- 2nd idea: we don't need the full representation, the largest term might be enough!

  [Faugère 2002 ; Gao, Volny, Wang 2010 ; Arri, Perry 2011... Eder, Faugère 2017]
- Define a signature $\mathfrak{s}(g)$ of g as

$$\mathfrak{s}(g) = \mathrm{LT}(q_j)\mathbf{e}_j = \mathrm{LT}(\mathbf{g}) \text{ for some } \mathbf{g} = \sum_{i=1}^{m} q_i \mathbf{e}_i \in A^m \text{ with } \bar{\mathbf{g}} = g = \sum_{i=1}^{m} q_i f_i$$

where q_j is the last coef. $\neq 0$

- Signatures are ordered as "position over term":

$$aX^b\mathbf{e}_i < a'X^{b'}\mathbf{e}_j \iff i < j \text{ or } i = j \text{ and } X^b < X^{b'}$$

- Example: S-polynomial: $\text{S-Pol}(\mathbf{g}_i, \mathbf{g}_j) = \frac{T(i,j)}{T(i)}\mathbf{g}_i - \frac{T(i,j)}{T(j)}\mathbf{g}_j$

  Up to permutation, two situations:

  - $\frac{T(i,j)}{T(i)}\mathrm{LT}(\mathbf{g}_i) > \frac{T(i,j)}{T(j)}\mathrm{LT}(\mathbf{g}_j) \quad \rightarrow \quad \mathrm{LT}(\text{S-Pol}(\mathbf{g}_i, \mathbf{g}_j)) = \frac{T(i,j)}{T(i)}\mathrm{LT}(\mathbf{g}_i)$

  - $\frac{T(i,j)}{T(i)}\mathrm{LT}(\mathbf{g}_i) \simeq \frac{T(i,j)}{T(j)}\mathrm{LT}(\mathbf{g}_j) \quad \rightarrow \quad \mathrm{LT}(\text{S-Pol}(\mathbf{g}_i, \mathbf{g}_j)) \leq \frac{T(i,j)}{T(i)}\mathrm{LT}(\mathbf{g}_i)$

- Signatures are ordered as "position over term":

$$aX^b\mathbf{e}_i < a'X^{b'}\mathbf{e}_j \iff i < j \text{ or } i = j \text{ and } X^b < X^{b'}$$

- Example: S-polynomial: $\text{S-Pol}(\mathbf{g}_i, \mathbf{g}_j) = \frac{T(i,j)}{T(i)}\mathbf{g}_i - \frac{T(i,j)}{T(j)}\mathbf{g}_j$

  Up to permutation, two situations:

  - $\frac{T(i,j)}{T(i)}\mathfrak{s}(g_i) > \frac{T(i,j)}{T(j)}\mathfrak{s}(g_j) \quad \to \quad \mathfrak{s}(\text{S-Pol}(g_i, g_j)) = \frac{T(i,j)}{T(i)}\mathfrak{s}(g_i)$

    Regular S-polynomial

  - $\frac{T(i,j)}{T(i)}\mathfrak{s}(g_i) \simeq \frac{T(i,j)}{T(j)}\mathfrak{s}(g_j) \quad \to \quad \mathfrak{s}(\text{S-Pol}(g_i, g_j)) \leq \frac{T(i,j)}{T(i)}\mathfrak{s}(g_i)$

    Non regular S-polynomial: possible signature drop

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

Definition (Signature reductions)

$f, g, h \in \langle f_1, \ldots, f_m \rangle$ with signatures, such that f reduces to $h = f - cX^a g$

The reduction is

- a $\mathfrak{s}$-reduction if $X^a\mathfrak{s}(g) \leq \mathfrak{s}(f)$ (*i.e.* $\mathfrak{s}(h) \leq \mathfrak{s}(f)$)
- a regular $\mathfrak{s}$-reduction if $X^a\mathfrak{s}(g) \lneq \mathfrak{s}(f)$ (*i.e.* $\mathfrak{s}(h) = \mathfrak{s}(f)$)

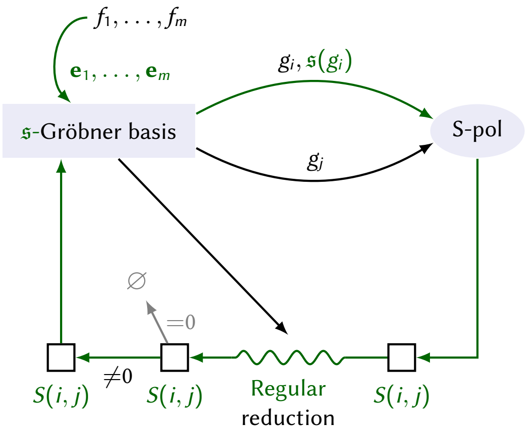
Definition (Signature Gröbner basis)

$G = \{g_1, \ldots, g_s\} \subset \mathfrak{a} = \langle f_1, \ldots, f_m \rangle$ is a (strong) $\mathfrak{s}$-Gröbner basis

iff for all $f \in \mathfrak{a}$, f $\mathfrak{s}$-reduces to 0 modulo G.

Key theorem

- A $\mathfrak{s}$-Gröbner basis is a Gröbner basis
- Every ideal admits a finite $\mathfrak{s}$-Gröbner basis



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

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

(Strong) reduction:

$$f \rightsquigarrow h = f - cX^a \mathrm{LT}(g)$$

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

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

Key property

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

Main consequence

Buchberger's algorithm with signatures is correct and computes a signature GB.

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.

Outline

1. Reminders about Gröbner bases over fields
   - Gröbner bases, Buchberger's algorithm
   - Signatures

2. Algorithms for rings
   - Adding signatures to Möller's weak GB algorithm
   - Adding signatures to Möller's strong GB algorithm

3. Proofs and experiments
   - Skeleton of the proofs
   - Experimental data
   - Future work

Type of rings	General rings	Principal domains	Euclidean domains
Type of GB	Weak	Strong	Strong
Algorithm	Möller weak	Möller strong	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

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	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?

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	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
  - Impossible to avoid signature drops, signatures can decrease

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	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)	[F., V. 2019]	[Eder, Popescu 2017]

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
- This work: partial order disregarding the coefficients
  - No signature drops, signatures don't decrease (but they may not increase)
  - Möller's weak GB algo.: proved for PIDs
  - Möller's strong GB algo.: signatures also for the G-polynomials

Towards weak bases: saturated sets and weak S-polynomials

Definition (Saturated set)

Given a basis $\{g_1, \ldots, g_t\}$, saturated sets are constructed as follows:

1. Pick $J \subset \{1, \ldots t\}$
2. $M(J) \leftarrow \mathrm{lcm}\{\mathrm{LM}(g_j) : j \in J\}$
3. Add to J all $j \in \{1, \ldots, t\}$ such that $\mathrm{LM}(g_j)$ divides $M(J)$

Definition (Weak S-polynomial)

Let $s = \max(J)$, $J^* = J \setminus \{s\}$, and let $c \neq 0$ an element of $\langle \mathrm{LC}(g_j) : j \in J^* \rangle : \langle \mathrm{LC}(g_s) \rangle$.

There exists $(b_j)_{j \in J^*}$ such that $\mathrm{LC}(g_s)c = \sum_{j \in J^*} b_j \mathrm{LC}(g_j)$.

The associated weak S-polynomial is

$$\text{S-Pol}(J; c) = c\frac{M(J)}{\mathrm{LM}(g_s)}g_s - \sum_{j \in J^*} b_j \frac{M(J)}{\mathrm{LM}(g_j)}g_j.$$

Definition (Weak reduction)

f weakly reduces to h modulo G if there exists $J \subset \{1, \ldots, t\}$ such that

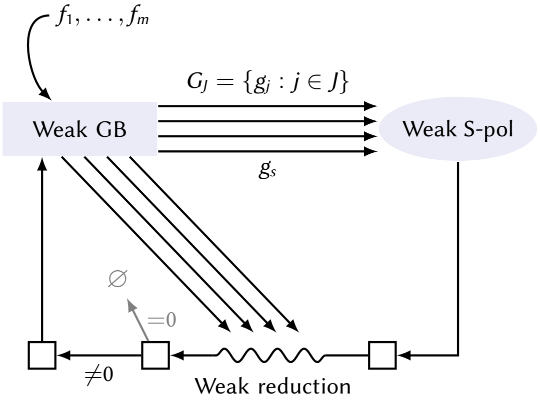
- for all $j \in J$, $\mathrm{LM}(g_j)$ divides $\mathrm{LM}(f)$, say, $X^{a_i}\mathrm{LM}(g_j) = \mathrm{LM}(f)$
- $\mathrm{LC}(f)$ lies in $\langle \mathrm{LC}(g_j) : j \in J \rangle$, say, $\mathrm{LC}(f) = \sum_{j \in J} b_j \mathrm{LC}(g_j)$
- $h = f - \sum_{j \in J} b_j X^{a_j} g_j$

We use the same word for the transitive closure of the relation.

"Möller's criterion"

The following statements are equivalent:

- G is a weak Gröbner basis of $\mathfrak{a} = \langle G \rangle$
- $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(\mathfrak{a}) \rangle$
- For all f in $\mathfrak{a}$, f weakly reduces to 0 modulo G
- For all J and c, the weak S-pol $\text{S-Pol}(J; c)$ weakly reduces to 0 modulo G



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:

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

[Möller 1988]

Definition (Saturated set)

Given a basis $\{g_1, \dots, g_s\}$, saturated sets are constructed as follows:

1. Pick $J \subset \{1, \dots s\}$
2. $M(J) \leftarrow \operatorname{lcm}\{\mathrm{LM}(g_j) : j \in J\}$
3. Add to J all $j \in \{1, \dots, s\}$ such that $\mathrm{LM}(g_j)$ divides $M(J)$

The signature of a saturated set is

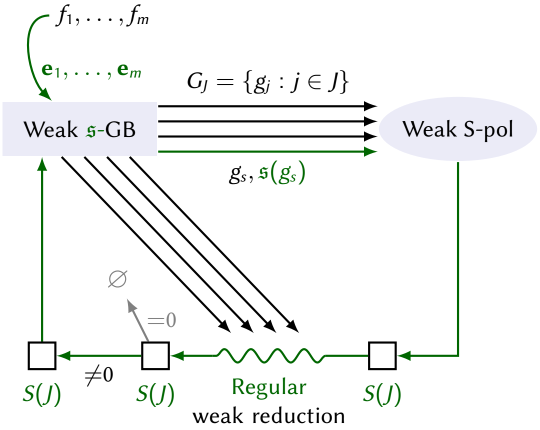
$$S(J) = \max \left(\frac{M(J)}{\mathrm{LM}(g_i)} \mathfrak{s}(g_i) \right)_{i \in J}$$

A regular saturated set is constructed such that this max is reached only once, at $s \in J$.

Then

$$\mathfrak{s}(\text{S-Pol}(J; s; c)) = cS(J)$$

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

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

Weak reduction:

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

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

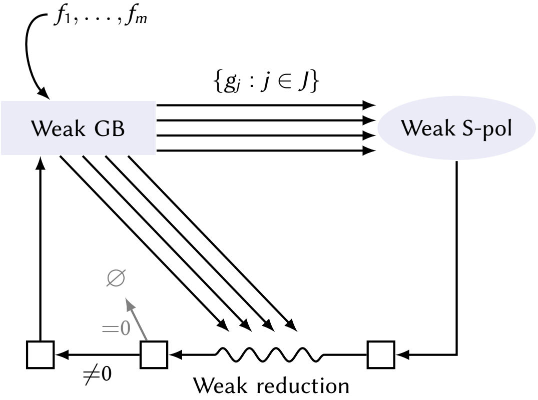
$$\mathfrak{s}(h) = \mathfrak{s}(f)$$

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

[Möller 1988]

[F, V 2018]

Outline



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

The syzygy lifting theorem (R is a Noetherian ring)

$G = \{g_1, \ldots, g_s\}$

Definition

A term-syzygy of G is $S = \sum_{i=1}^{s} s_i \varepsilon_i \in A^s$, whose syzygy polynomial $\bar{S} = \sum s_i g_i$ satisfies $\mathrm{LT}(\bar{S}) \lneq \max(\mathrm{LT}(s_i g_i))$.

Syzygy lifting theorem

The following statements are equivalent:

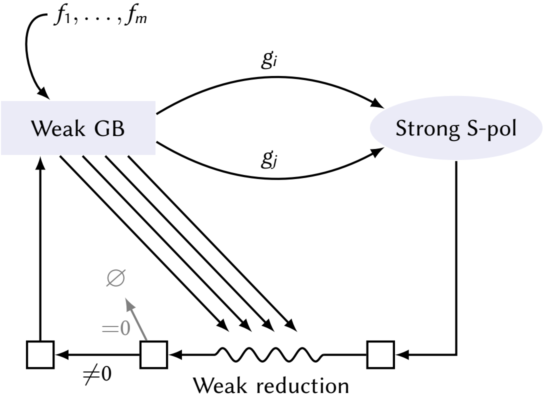
- G is a (weak/strong) Gröbner basis
- If $\mathcal{S}$ is a basis of term-syzygies of G, for all $S \in \mathcal{S}$, $\bar{S}$ (weakly/strongly) red. to 0 mod. G.

- Buchberger's criterion:
  (Strong) S-polynomials form a basis of term-syzygies over a field
- Buchberger's chain criterion:
  Some S-pols can be removed without compromising the basis
- Möller's criterion:
  Weak S-polynomials form a basis of term-syzygies in general

Why is life easier with PIDs (1/2)

Principal syzygies / Strong S-polynomials

If R is a principal ring, then principal syzygies (of the form $c_i X^{a_i} \varepsilon_i - c_j X^{a_j} \varepsilon_j$)
form a basis of term syzygies.



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

Why is life easier with PIDs (2/2)

Principal syzygies / Strong S-polynomials

If R is a principal ring, then principal syzygies (of the form $c_i X^{a_i} \varepsilon_i - c_j X^{a_j} \varepsilon_j$) form a basis of term syzygies.

Definition (G-polynomials)

From a Bézout relation $\gcd(\mathrm{LC}(f), \mathrm{LC}(g)) = u\mathrm{LC}(f) + v\mathrm{LC}(g)$,

the G-polynomial of f and g is defined as

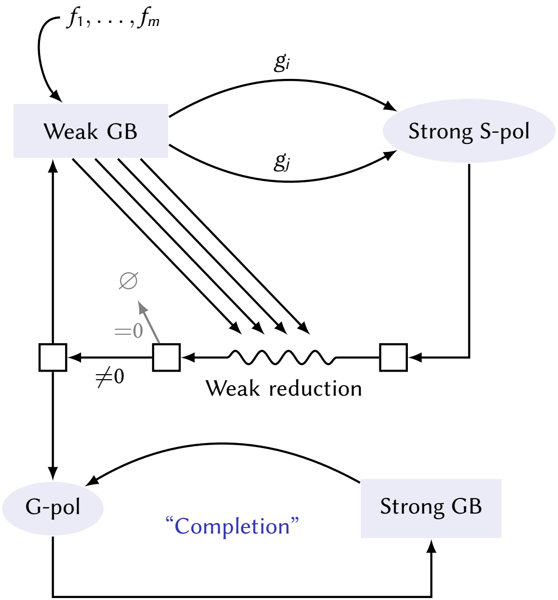
$$\text{G-Pol}(f, g) = u\frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(f)} f + v\frac{\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(g)} g$$

Completion

The completion $C(F)$ of $F = \{f_1, \ldots, f_r\}$ is defined as follows:

- $C(\varnothing) = \varnothing$
- $C(F \cup f_{r+1}) = C(F) \cup \{f_{r+1}\} \cup \{\text{G-Pol}(h, f_{r+1}) : h \in C(F)\}$

G is a weak Gröbner basis $\iff$ $C(G)$ is a strong Gröbner basis.



Weak S-pols and reductions:

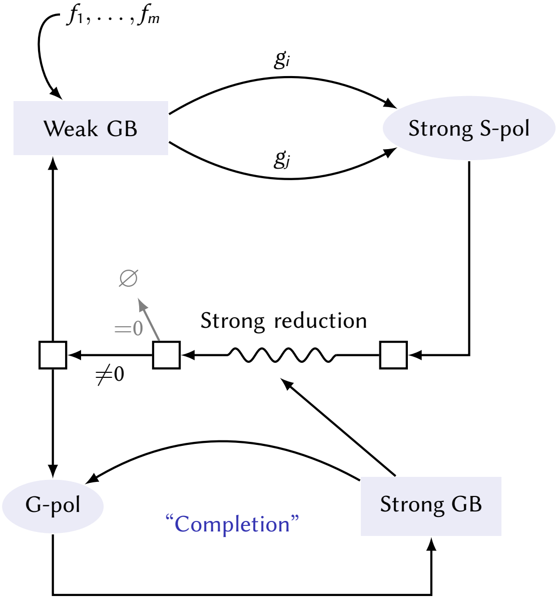
Same as in Möller's weak GB

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:

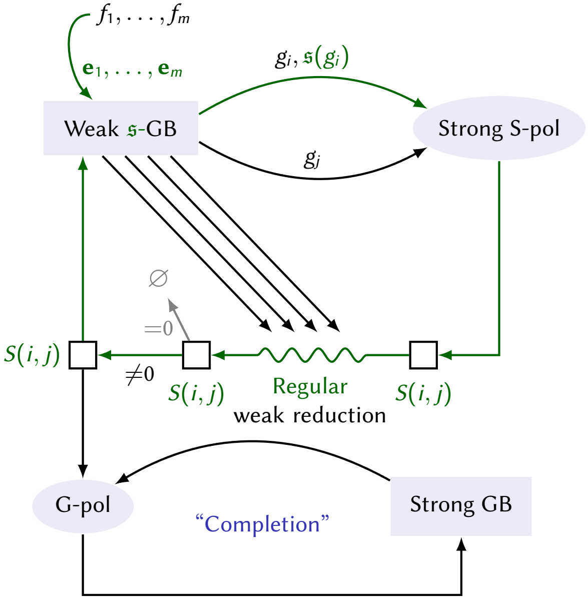
Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

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



Weak S-pols and reductions:

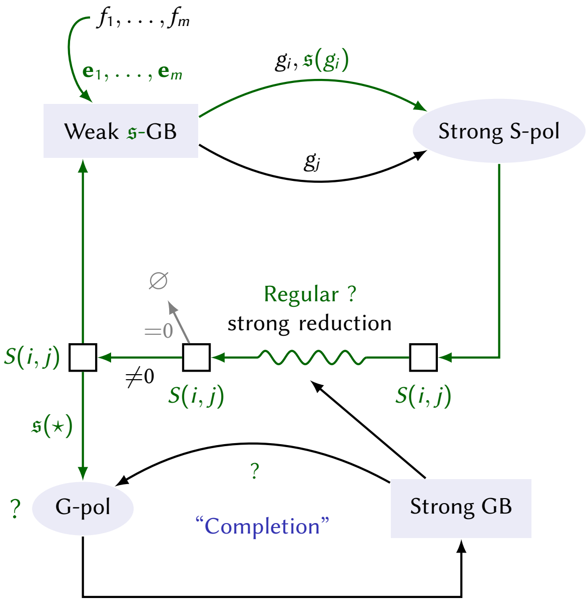
Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

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



Weak S-pols and reductions:

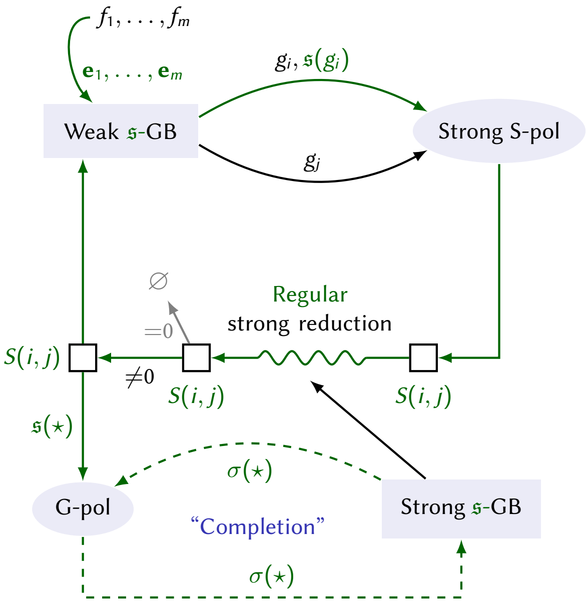
Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

G-polynomial:

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



Weak S-pols and reductions:

Same as in Möller's weak GB

Strong S-pols and reductions:

Same as in Buchberger

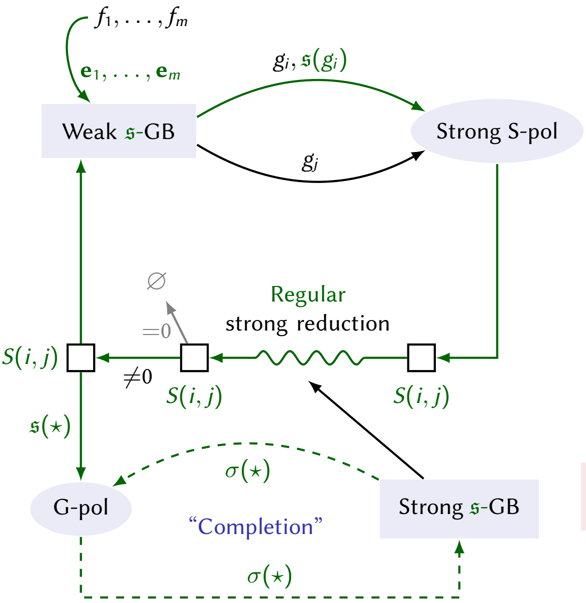
G-polynomial:

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

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

$\sigma(h)$ 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:

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

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

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

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

Outline

1. Reminders about Gröbner bases over fields
   - Gröbner bases, Buchberger's algorithm
   - Signatures
2. Algorithms for rings
   - Adding signatures to Möller's weak GB algorithm
   - Adding signatures to Möller's strong GB algorithm
3. Proofs and experiments
   - Skeleton of the proofs
   - Experimental data
   - Future work

Tool for the proof: signature version of the lifting theorem

Definition (Signatures for term-syzygies)

- Signature of $S = \sum_{i=1}^{s} s_i \varepsilon_i$: $\mathfrak{s}(S) = \max\{\mathrm{LT}(s_i)\mathfrak{s}(g_i) | s_i \neq 0\}$
- S-basis of term-syzygies: basis such that every element can be represented without a signature drop:

  $\{\Sigma_1, \ldots, \Sigma_k\}$ such that for all term-syzygy S, there exists $\tau_1, \ldots, \tau_k$ such that
  - $S = \sum_{i=1}^{k} \tau_i \Sigma_i$
  - $\mathfrak{s}(S) \simeq \max\{\mathrm{LT}(\tau_i) S(\Sigma_i) | \tau_i \neq 0\}$

Syzygy lifting theorem, signature version

The following statements are equivalent:

- G is a (weak/strong) $\mathfrak{s}$-Gröbner basis
- If $\mathcal{S}$ is a S-basis of term-syzygies of G, for all $S \in \mathcal{S}$, $\bar{S}$ (weakly/strongly) red. to 0 mod. G.

Skeleton of the proof (R is a PID)

[F., V. 2018]

1. Reg. weak S-pols s-red. to 0 $\Longrightarrow$ weak S-GB

$\longleftrightarrow$

Möller's weak GB algorithm with signatures is correct

Skeleton of the proof (R is a PID)

[F., V. 2018]

1. Reg. weak S-pols s-red. to 0 $\Longrightarrow$ weak S-GB

Möller's weak GB algorithm with signatures is correct

2. Reg. weak S-pols form a S-basis of term syzygies

Weak S-pol rewriting

3. Reg. strong S-pols form a S-basis of term syzygies

Signature lifting thm

Möller's strong GB algorithm with signatures is correct

[F., V. 2019]

[F., V. 2018]

1. Reg. weak S-pols s-red. to 0 $\Longrightarrow$ weak S-GB

Möller's weak GB algorithm with signatures is correct

2. Reg. weak S-pols form a S-basis of term syzygies

Weak S-pol rewriting

3. Reg. strong S-pols form a S-basis of term syzygies

Chain criterion syz. rewriting

(If $T(k)$ divides $T(i,j)$)

$$\Sigma(i,k) = \frac{T(i,k)}{T(i)}\Sigma(i,k) - \frac{T(j,k)}{T(j)}\Sigma(j,k)$$

4. Reg. strong S-pols not eliminated by the chain crit. form a S-basis of term syzygies

Signature lifting thm

Möller's strong GB algorithm with signatures is correct

[F., V. 2019]

Experimental data (1/2)

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

			Added as pairs, not S-pols		Added as S-pols, not reduced		Reduced, thrown away	
Algorithm	Pairs	S-pols (red)	Copr.	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	488	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	1629	603 (206)	509	517	388	9	84	0

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

Experimental data (2/2)

Toy implementation of the algorithms in Magma:

`https://github.com/ThibautVerron/SignatureMoller`

System	Möller with sigs	Native F4 from Magma
Katsura 3	0.05 s	0.01 s
Katsura 4	0.30 s	0.10 s
Katsura 5	5.71 s	5.74 s
Katsura 6	2055.66 s	251.10 s

Timings

Results

- Signature-based algorithms for GB over principal domains
  - Möller's weak GB algorithm: computes a weak basis, useful as a theoretical tool
  - Möller's strong GB algorithm: computes a strong basis
  - In both cases: proof of correctness and termination, signatures do not decrease
  - Compatible with signature criteria (+ Buchberger criteria for the strong algo.)
- Toy implementation in Magma, with some first optimizations

Results and future work

- Signature-based algorithms for GB over principal domains
  - Möller's weak GB algorithm: computes a weak basis, useful as a theoretical tool
  - Möller's strong GB algorithm: computes a strong basis
  - In both cases: proof of correctness and termination, signatures do not decrease
  - Compatible with signature criteria (+ Buchberger criteria for the strong algo.)
- Toy implementation in Magma, with some first optimizations
- Main bottlenecks
  - Weak GB algo.: computation of the saturated sets (cost exp. in the size of the GB)
  - Strong GB algo.: basis growth and coefficient swell

Results and future work

- Signature-based algorithms for GB over principal domains
  - Möller's weak GB algorithm: computes a weak basis, useful as a theoretical tool
  - Möller's strong GB algorithm: computes a strong basis
  - In both cases: proof of correctness and termination, signatures do not decrease
  - Compatible with signature criteria (+ Buchberger criteria for the strong algo.)
- Toy implementation in Magma, with some first optimizations
- Main bottlenecks
  - Weak GB algo.: computation of the saturated sets (cost exp. in the size of the GB)
  - Strong GB algo.: basis growth and coefficient swell
- Current and future work
  - Optimizations to counter those bottlenecks
  - Selection strategies? Degree over Position over Term ordering? F4/F5?
  - Does Möller's weak GB algo. work for more general rings? For example UFDs?
- End goal
  - Competitive implementation of the algorithms

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]