Two signature-based variants of Buchberger's algorithm for 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 "Calcul formel", Université de Limoges, 30 mars 2021

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 (cryptography, number theory...)

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

$$f = \overbrace{\underbrace{c}_{\mathrm{lc}(f)} \cdot \underbrace{\mathbf{X}^{\mathbf{a}}}_{\mathrm{lm}(f)}}^{\mathrm{lt}(f)} + \text{ smaller terms}$$

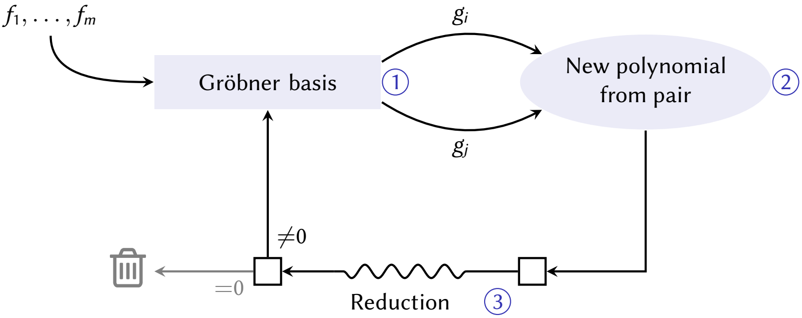
Definition (Weak/strong Gröbner basis)

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

- 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

Strong $\implies$ weak, and they are equivalent if R is a field

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



1. Selection: different strategies
2. Construction: S-polynomials: $\text{S-Pol}(g_i, g_j) = \dfrac{\text{lcmlt}(g_i, g_j)}{\text{lt}(g_i)} g_i - \dfrac{\text{lcmlt}(g_i, g_j)}{\text{lt}(g_j)} g_j$
3. Reduction: if $\text{lt}(f) = t\,\text{lt}(g)$, $f \to f - tg$

Summary of Gröbner basis algorithms over rings

Two questions:

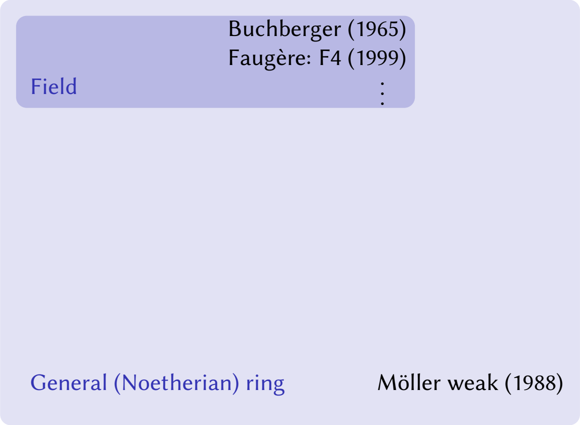
- How to compute S-polynomials?
- How to compute reductions?

Field	Buchberger (1965)	Usual // Usual
	Faugère: F4 (1999)	Usual // Usual (linear algebra)
	⋮	

Summary of Gröbner basis algorithms over rings

Two questions:

- How to compute S-polynomials?
- How to compute reductions?



Field

Buchberger (1965) — Usual // Usual

Faugère: F4 (1999) — Usual // Usual (linear algebra)

⋮

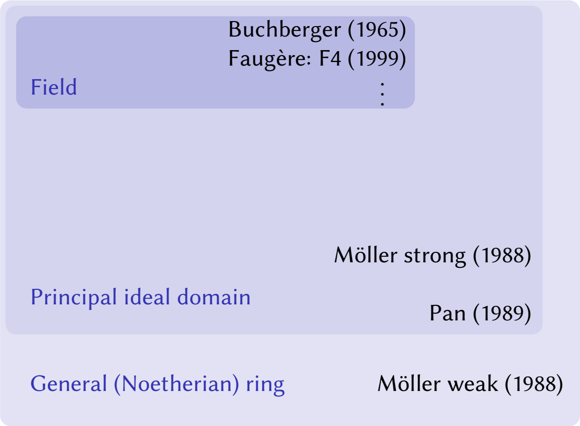
General (Noetherian) ring

Möller weak (1988) — Multiple // Multiple

Summary of Gröbner basis algorithms over rings

Two questions:

- How to compute S-polynomials?
- How to compute reductions?



Field

Buchberger (1965) — Usual // Usual

Faugère: F4 (1999) — Usual // Usual (linear algebra)

⋮

Principal ideal domain

Möller strong (1988) — Usual // Usual with G-pol

Pan (1989) — Usual or G-pols // Usual

General (Noetherian) ring

Möller weak (1988) — Multiple // Multiple

Summary of Gröbner basis algorithms over rings

Two questions:

- How to compute S-polynomials?
- How to compute reductions?

Field	Buchberger (1965)	Usual // Usual
	Faugère: F4 (1999)	Usual // Usual (linear algebra)
	⋮	
Euclidean ring	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Lichtblau (2012)	Usual or G-pols // Usual
Principal ideal domain	Möller strong (1988)	Usual // Usual with G-pol
	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Pan (1989)	Usual or G-pols // Usual
General (Noetherian) ring	Möller weak (1988)	Multiple // Multiple

This work: signature variants of the algos of Kandri-Rody and Kapur, and of Pan/Lichtblau

Why signatures?

Problem: 🗑: useless computations ⟶ ♻

Simple example

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

$p - q = 0$?

Why signatures?

Problem: 🗑: useless computations ⟶ ♻

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

Simple example

$p = p_1 f_1 + p_2 f_2 + \cdots + p_m f_m$

$\mathbf{p} = p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_m \mathbf{e}_m$

$q = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$

$\mathbf{q} = q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_m \mathbf{e}_m$

$p - q = 0?$

$\mathbf{p} - \mathbf{q} = \left(p_1 \mathbf{e}_1 + \cdots + p_m \mathbf{e}_m\right) - \left(q_1 \mathbf{e}_1 + \cdots + q_m \mathbf{e}_m\right)$

Why signatures?

Problem: 🗑: useless 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]

Simple example

$$\begin{aligned} p &= p_1 f_1 + p_2 f_2 + \cdots + p_m f_m \\ \mathbf{p} &= p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_m \mathbf{e}_m \\ &= \operatorname{lt}(p_k)\mathbf{e}_k + \text{smaller terms} \end{aligned}$$

$$\begin{aligned} q &= q_1 f_1 + q_2 f_2 + \cdots + q_m f_m \\ \mathbf{q} &= q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_m \mathbf{e}_m \\ &= \operatorname{lt}(q_l)\mathbf{e}_l + \text{smaller terms} \end{aligned}$$

$$p - q = 0?$$

$$\begin{aligned} \mathbf{p} - \mathbf{q} = {} & (p_1 \mathbf{e}_1 + \cdots + p_m \mathbf{e}_m) - (q_1 \mathbf{e}_1 + \cdots + q_m \mathbf{e}_m) \\ = {} & \operatorname{lt}(p_k)\mathbf{e}_k - \operatorname{lt}(q_l)\mathbf{e}_l + \text{smaller terms} \end{aligned}$$

Why signatures?

Problem: 🗑: useless 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]

Simple example

$$\begin{aligned} p &= p_1 f_1 + p_2 f_2 + \cdots + p_m f_m \\ \mathbf{p} &= p_1 \mathbf{e}_1 + p_2 \mathbf{e}_2 + \cdots + p_m \mathbf{e}_m \\ &= \operatorname{lt}(p_k)\mathbf{e}_k + \text{smaller terms} \end{aligned}$$

$$\begin{aligned} q &= q_1 f_1 + q_2 f_2 + \cdots + q_m f_m \\ \mathbf{q} &= q_1 \mathbf{e}_1 + q_2 \mathbf{e}_2 + \cdots + q_m \mathbf{e}_m \\ &= \operatorname{lt}(q_l)\mathbf{e}_l + \text{smaller terms} \end{aligned}$$

$p - q = 0?$

$$\begin{aligned} \mathbf{p} - \mathbf{q} &= (p_1 \mathbf{e}_1 + \cdots + p_m \mathbf{e}_m) - (q_1 \mathbf{e}_1 + \cdots + q_m \mathbf{e}_m) \\ &= \operatorname{lt}(p_k)\mathbf{e}_k - \operatorname{lt}(q_l)\mathbf{e}_l + \text{smaller terms} \\ &= \operatorname{lt}(p_k)\mathbf{e}_k + \text{smaller terms} \quad \text{if } \operatorname{lt}(p_k)\mathbf{e}_k \gneq \operatorname{lt}(q_l)\mathbf{e}_l \end{aligned}$$

Why signatures?

Problem: 🗑: useless computations ——→ ♻

- 1^{st} idea: keep track of the representation of the ideal elements
  [Möller, Mora, Traverso 1992]
- 2^{nd} 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]

Simple example

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

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

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

$$\operatorname{sig}(p) = \text{ signature of } p$$

$$p - q = 0?$$

$$\begin{aligned}
\mathbf{p} - \mathbf{q} &= (p_1 \mathbf{e}_1 + \cdots + p_m \mathbf{e}_m) - (q_1 \mathbf{e}_1 + \cdots + q_m \mathbf{e}_m) \\
&= \operatorname{lt}(p_k)\mathbf{e}_k - \operatorname{lt}(q_l)\mathbf{e}_l + \text{smaller terms} \\
&= \operatorname{lt}(p_k)\mathbf{e}_k + \text{smaller terms} \quad \text{if } \operatorname{lt}(p_k)\mathbf{e}_k \gneq \operatorname{lt}(q_l)\mathbf{e}_l
\end{aligned}$$

Regular addition

First ingredient: module term ordering

- Ideal: $I = \langle f_1, \dots, f_m \rangle = \{f = p_1 f_1 + \dots + p_m f_m\} \subset A$
- Module: $\mathcal{I} = \{\mathbf{f} = (p_1, \dots, p_m, f) : f = p_1 f_1 + \dots + p_m f_m\} \subset A^{m+1}$

  Module part Polynomial part
- $\mathcal{I}$ is free with basis $\{(\mathbf{e}_i, f_i) = (0, \dots, 1, \dots, 0, f_i) : i \in \{1 \dots m\}\}$

First ingredient: module term ordering

- Ideal: $I = \langle f_1, \dots, f_m \rangle = \{f = p_1 f_1 + \cdots + p_m f_m\} \subset A$
- Module: $\mathcal{I} = \{\mathbf{f} = (p_1, \dots, p_m, f) : f = p_1 f_1 + \cdots + p_m f_m\} \subset A^{m+1}$

  Module part Polynomial part
- $\mathcal{I}$ is free with basis $\{(\mathbf{e}_i, f_i) = (0, \dots, 1, \dots, 0, f_i) : i \in \{1 \dots m\}\}$

Definition: signatures

- Signature ordering: monomial ordering $\prec$ on $\mathrm{Mon}(A^m) = \{\mu \mathbf{e}_i\}$
- Signature of $\mathbf{f}$: largest term $t\mathbf{e}_i$ with t in the support of p_i

Examples:

- $\mu \mathbf{e}_i \prec_{\mathrm{PoT}} \nu \mathbf{e}_j \iff i < j$, or if equal, $\mu < \nu$

  Position over Term
- $\mu \mathbf{e}_i \prec_{\mathrm{ToP}} \nu \mathbf{e}_j \iff \mu < \nu$, or if equal, $i < j$

  Term over Position

First ingredient: module term ordering

- Ideal: $I = \langle f_1, \dots, f_m \rangle = \{f = p_1 f_1 + \cdots + p_m f_m\} \subset A$
- Module: $\mathcal{I} = \{\mathbf{f} = (p_1, \dots, p_m, f) : f = p_1 f_1 + \cdots + p_m f_m\} \subset A^{m+1}$

  Module part Polynomial part
- $\mathcal{I}$ is free with basis $\{(\mathbf{e}_i, f_i) = (0, \dots, 1, \dots, 0, f_i) : i \in \{1 \dots m\}\}$

Definition: signatures

- Signature ordering: monomial ordering $\prec$ on $\mathrm{Mon}(A^m) = \{\mu \mathbf{e}_i\}$
- Signature of $\mathbf{f}$: largest term $t\mathbf{e}_i$ with t in the support of p_i

Examples:

- $\mu \mathbf{e}_i \prec_{\text{PoT}} \nu \mathbf{e}_j \iff i < j$, or if equal, $\mu < \nu$

  Position over Term
- $\mu \mathbf{e}_i \prec_{\text{ToP}} \nu \mathbf{e}_j \iff \mu < \nu$, or if equal, $i < j$

  Term over Position

Warning: $\prec$ is a partial order on terms

- $\mathbf{s} \simeq \mathbf{t} \iff$ incomparable or equal, it is an equivalence relation
- $\mathbf{s} \preceq \mathbf{t} \iff \mathbf{s} \prec \mathbf{t}$ or $\mathbf{s} \simeq \mathbf{t}$

Second ingredient: s-reductions

Notation: leading terms, monomials, coefficients of elements of $\mathcal{I}$ refer to the polynomial part

Definition: s-reductions

$\mathbf{f}$ s-reduces to $\mathbf{h}$ modulo $\mathbf{g}$ if:

- $t\operatorname{lt}(\mathbf{g}) = \operatorname{lt}(\mathbf{f})$
- $\mathbf{h} = \mathbf{f} - t\mathbf{g}$
- $t\operatorname{sig}(\mathbf{g}) \preceq \operatorname{sig}(\mathbf{f})$

Properties

- $\operatorname{lt}(\mathbf{h}) < \operatorname{lt}(\mathbf{f})$
- $\operatorname{sig}(\mathbf{h}) \preceq \operatorname{sig}(\mathbf{f})$

Definition: signature Gröbner basis

$\mathcal{G} \subset \mathcal{I} \subset A^{m+1}$

- $\mathcal{G}$ is a signature (strong) Gröbner basis $\iff$ for all $\mathbf{f} \in \mathcal{I}$, $\mathbf{f}$ s-reduces to 0 modulo $\mathcal{G}$.

Third ingredient: regular operations

Definition: regular operations

Consider the sum $\mathbf{h} = \mathbf{f} + \mathbf{g}$ with $\mathrm{sig}(\mathbf{f}) \preceq \mathrm{sig}(\mathbf{g})$.

- Regular operation $\iff$ $\mathrm{sig}(\mathbf{f}) \precneq \mathrm{sig}(\mathbf{g}) \longrightarrow \mathrm{sig}(\mathbf{h}) = \mathrm{sig}(\mathbf{g})$ ✓
- Singular operation $\iff$ $\mathrm{sig}(\mathbf{f}) = -\mathrm{sig}(\mathbf{g}) \longrightarrow \mathrm{sig}(\mathbf{h}) \precneq \mathrm{sig}(\mathbf{g})$ (discarded elements)

Third ingredient: regular operations

Definition: regular operations

Consider the sum $\mathbf{h} = \mathbf{f} + \mathbf{g}$ with $\mathrm{sig}(\mathbf{f}) \preceq \mathrm{sig}(\mathbf{g})$.

- Regular operation $\iff$ $\mathrm{sig}(\mathbf{f}) \precnsim \mathrm{sig}(\mathbf{g}) \longrightarrow \mathrm{sig}(\mathbf{h}) = \mathrm{sig}(\mathbf{g})$ ✓
- Singular operation $\iff$ $\mathrm{sig}(\mathbf{f}) = -\mathrm{sig}(\mathbf{g}) \longrightarrow \mathrm{sig}(\mathbf{h}) \precnsim \mathrm{sig}(\mathbf{g})$ (discarded elements)

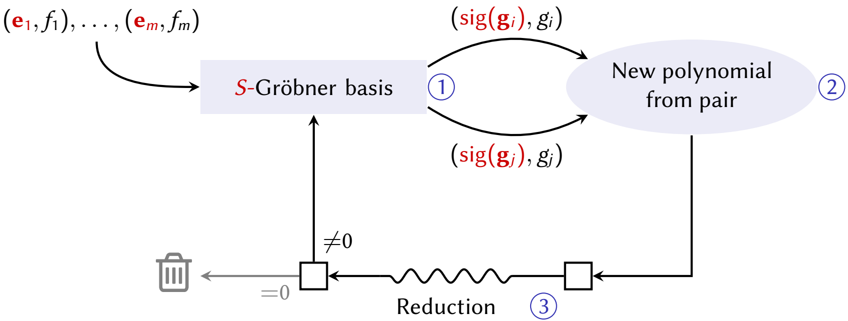
Idea of the signature-based algorithms:

1. Pick next elements with smallest signature
2. Build new elements using regular S-polynomials
3. Only perform regular s-reductions

Key properties

- Signatures do not decrease
- Loop invariant: at signature $\mathbf{s}$, all elements with sig. $\precnsim \mathbf{s}$ s-reduce to 0 mod $\mathcal{G}$
- Sig-poly pairs instead of elements of $\mathcal{I}$: pair $(\mathrm{sig}(\mathbf{f}), f)$

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



$(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)$

S-Gröbner basis ①

$(\mathrm{sig}(\mathbf{g}_i), g_i)$

$(\mathrm{sig}(\mathbf{g}_j), g_j)$

New polynomial from pair ②

$\neq 0$

$= 0$

Reduction ③

1. Selection: non-decreasing signatures
2. Construction: regular S-polynomials: $\text{S-Pol}(\mathbf{g}_i, \mathbf{g}_j) = \frac{\mathrm{lcmlt}(\mathbf{g}_i, \mathbf{g}_j)}{\mathrm{lt}(\mathbf{g}_i)} \mathbf{g}_j - \frac{\mathrm{lcmlt}(\mathbf{g}_i, \mathbf{g}_j)}{\mathrm{lt}(\mathbf{g}_j)} \mathbf{g}_j$
3. Reduction: regular: if $\mathrm{lt}(\mathbf{f}) = t\,\mathrm{lt}(\mathbf{g})$ and $t\,\mathrm{sig}(\mathbf{g}) \lneq \mathrm{sig}(\mathbf{f})$, $\mathbf{f} \to \mathbf{f} - t\mathbf{g}$

Signature of syzygies

Definition: syzygy

- Syzygy of I: $z = (z_1, \ldots, z_m) \in A^m$ such that $z_1 f_1 + \cdots + z_m f_m = 0$
- It corresponds to an element $\mathbf{z} = (z, 0) \in \mathcal{I}$.

We can compute those elements at the same time as a signature Gröbner basis!

Definition: reduction on the signatures

$\mathbf{f} \in \mathcal{I}$ sig-reduces modulo $\mathbf{z} \in \mathrm{Syz}(\mathcal{I})$ if:

- there exists a term t such that $\mathrm{sig}(\mathbf{f}) = t\,\mathrm{sig}(\mathbf{z})$.

The result of the reduction has the same polynomial part as **f** but smaller signature.

Definition: signature basis of syzygies

$\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ such that every syzygy of $\mathcal{I}$ is signature reducible modulo $\mathcal{G}_z$.

Computing signature bases of syzygies?

Reminder: signature Gröbner basis

$\mathcal{G} \subset \mathcal{I}$ is a signature Gröbner basis (SGB) if for all $\mathbf{f} \in \mathcal{I}$, $\mathbf{f}$ is s-reducible modulo $\mathcal{G}$.

Reminder: signature basis of syzygies

$\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ such that every syzygy of $\mathcal{I}$ is signature reducible modulo $\mathcal{G}_z$.

Computing signature bases of syzygies?

Reminder: signature Gröbner basis

$\mathcal{G} \subset \mathcal{I}$ is a signature Gröbner basis (SGB) if for all $\mathbf{f} \in \mathcal{I}$, $\mathbf{f}$ is s-reducible modulo $\mathcal{G}$.

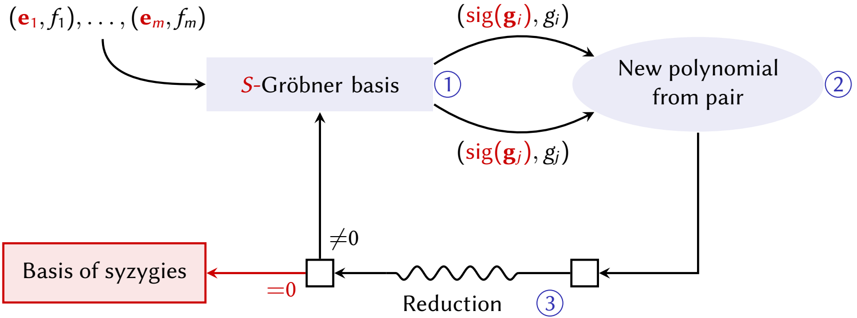
Reminder: signature basis of syzygies

$\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ such that every syzygy of $\mathcal{I}$ is signature reducible modulo $\mathcal{G}_z$.

Fact

Signature Gröbner basis algorithms can compute both bases at the same time.

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



$(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)$

S-Gröbner basis ①

$(\mathrm{sig}(\mathbf{g}_i), g_i)$

$(\mathrm{sig}(\mathbf{g}_j), g_j)$

New polynomial from pair ②

$\neq 0$

Basis of syzygies

$=0$

Reduction ③

1. Selection: non-decreasing signatures
2. Construction: regular S-polynomials: $\text{S-Pol}(\mathbf{g}_i, \mathbf{g}_j) = \frac{\mathrm{lcmlt}(\mathbf{g}_i, \mathbf{g}_j)}{\mathrm{lt}(\mathbf{g}_i)}\mathbf{g}_j - \frac{\mathrm{lcmlt}(\mathbf{g}_i, \mathbf{g}_j)}{\mathrm{lt}(\mathbf{g}_j)}\mathbf{g}_j$
3. Reduction: regular: if $\mathrm{lt}(\mathbf{f}) = t\,\mathrm{lt}(\mathbf{g})$ and $t\,\mathrm{sig}(\mathbf{g}) \lneq \mathrm{sig}(\mathbf{f})$, $\mathbf{f} \to \mathbf{f} - t\mathbf{g}$

Signature criteria

Singular criterion

Assume that:

1. Every $\mathbf{g} \in \mathcal{I}$ with signature $\precnsim \mathbf{T}$ is s-reducible modulo $\mathcal{G}$
2. $\mathbf{f}$ has signature $\mathbf{T}$ and there exists $\mathbf{g} \in \mathcal{G}$ such that $\mathrm{lt}(\mathbf{f}) = t\,\mathrm{lt}(\mathbf{g})$ and $\mathrm{sig}(\mathbf{f}) = t\,\mathrm{sig}(\mathbf{g})$

Then $\mathbf{f}$ s-reduces to 0 modulo $\mathcal{G}$.

Signature criteria

Singular criterion

Assume that:

1. Every $\mathbf{g} \in \mathcal{I}$ with signature $\precnsim \mathbf{T}$ is s-reducible modulo $\mathcal{G}$
2. $\mathbf{f}$ has signature $\mathbf{T}$ and there exists $\mathbf{g} \in \mathcal{G}$ such that $\operatorname{lt}(\mathbf{f}) = t\operatorname{lt}(\mathbf{g})$ and $\operatorname{sig}(\mathbf{f}) = t\operatorname{sig}(\mathbf{g})$

Then $\mathbf{f}$ s-reduces to 0 modulo $\mathcal{G}$.

Syzygy criterion

Assume that:

1. Every $\mathbf{g} \in \mathcal{I}$ with signature $\precnsim \mathbf{T}$ is s-reducible modulo $\mathcal{G}$
2. $\mathbf{f}$ has signature $\simeq \mathbf{T}$ and is sig-reducible by $\mathbf{z} \in \operatorname{Syz}(\mathcal{I})$

Then $\mathbf{f}$ is regular reducible modulo $\mathcal{G}$.

Signature criteria

Singular criterion

Assume that:

1. Every $\mathbf{g} \in \mathcal{I}$ with signature $\precnsim \mathbf{T}$ is s-reducible modulo $\mathcal{G}$
2. $\mathbf{f}$ has signature $\mathbf{T}$ and there exists $\mathbf{g} \in \mathcal{G}$ such that $\operatorname{lt}(\mathbf{f}) = t\operatorname{lt}(\mathbf{g})$ and $\operatorname{sig}(\mathbf{f}) = t\operatorname{sig}(\mathbf{g})$

Then $\mathbf{f}$ s-reduces to 0 modulo $\mathcal{G}$.

Syzygy criterion

Assume that:

1. Every $\mathbf{g} \in \mathcal{I}$ with signature $\precnsim \mathbf{T}$ is s-reducible modulo $\mathcal{G}$
2. $\mathbf{f}$ has signature $\simeq \mathbf{T}$ and is sig-reducible by $\mathbf{z} \in \operatorname{Syz}(\mathcal{I})$

Then $\mathbf{f}$ is regular reducible modulo $\mathcal{G}$.

F5 criterion (PoT ordering)

If $\mathbf{g} \in \mathcal{I}$ has signature $\star\mathbf{e}_j$, then $\operatorname{lt}(\mathbf{g})\mathbf{e}_i$ is the signature of a syzygy whenever $i > j$.

Why do we care about signature Gröbner bases?

First, they are Gröbner bases.

Theorem

If $\mathcal{G}$ is a signature Gröbner basis, the set of its polynomial parts forms a Gröbner basis.

Why do we care about signature Gröbner bases?

First, they are Gröbner bases.

Theorem

If $\mathcal{G}$ is a signature Gröbner basis, the set of its polynomial parts forms a Gröbner basis.

But better, they also give information on the module $\mathcal{I}$!

Theorem [Gao, Volny, Wang, 2015]

Let $G = \{(\mathbf{s}_i, g_i)\}$ be the sig-poly pairs of a SGB,
and $G_z = \{(\mathbf{z}_i, 0)\}$ be the sig-poly pairs of a signature basis of syzygies. Then:

- one can reconstruct a corresponding SGB $\mathcal{G}$ and signature basis of syzygies $\mathcal{G}_z$
- $\mathcal{G}$ is a "basis with coordinates" allowing to recover coefs in terms of the input polynomials
- $\mathcal{G}_z$ is a Gröbner basis of the module of syzygies of I

Those are typically expensive computations.

Sketch of the construction

In
- $G = \{(\mathbf{s}_i, g_i)\}$ the sig-poly pairs of a SGB
- $G_z = \{(\mathbf{z}_i, 0)\}$ the sig-poly pairs of a sig-basis of syzygies

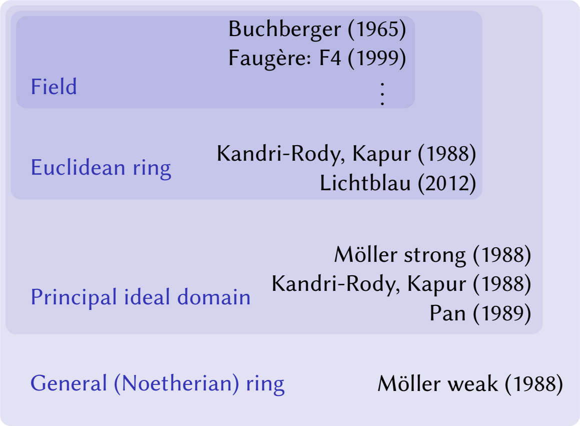
Out
- the corresponding SGB $\mathcal{G} = \{\mathbf{g}_1, \dots, \mathbf{g}_r\}$
- the corresponding sig-basis of syzygies $\mathcal{G}_z$

1. $\mathcal{G} \leftarrow \{(\mathbf{e}_i, f_i) : i \in \{1, \dots, m\}\}$ (reducing if needed)
2. For $(\mathbf{s}_i, g_i) \in G$ in increasing order of signatures, do
   - 2.1 Find $\mathbf{g}_j \in \mathcal{G}$ s.t. there exists a term t with $t\mathrm{sig}(\mathbf{g}_j) = \mathbf{s}_i$ and $t\mathrm{lm}(\mathbf{g}_j)$ minimal
   - 2.2 Perform regular reductions of $t\mathbf{g}_j$ by $\mathcal{G}$ until not reducible
   - 2.3 Add the result to $\mathcal{G}$
3. With $\mathcal{G}$ known, reconstruct $\mathcal{G}_z$ in the same way

Summary of Gröbner basis algorithms over rings

Two questions:

- How to compute S-polynomials?
- How to compute reductions?



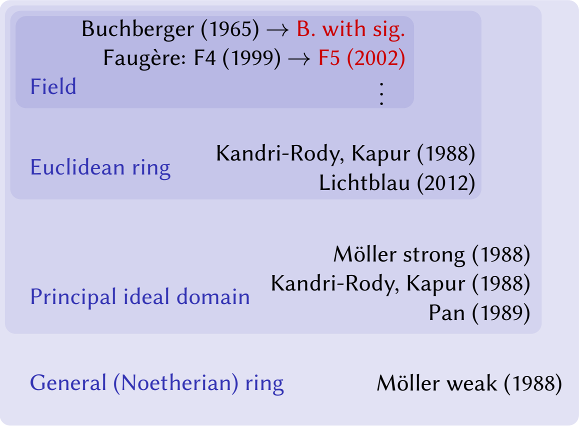
Field	Buchberger (1965)	Usual // Usual
	Faugère: F4 (1999)	Usual // Usual (linear algebra)
	⋮	
Euclidean ring	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Lichtblau (2012)	Usual or G-pols // Usual
Principal ideal domain	Möller strong (1988)	Usual // Usual with G-pol
	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Pan (1989)	Usual or G-pols // Usual
General (Noetherian) ring	Möller weak (1988)	Multiple // Multiple

Summary of Gröbner basis algorithms over rings with signatures

Two questions:

- How to compute S-polynomials?
- How to compute reductions?
- How to order signatures?

Case of fields: partial order is enough



Field	Buchberger (1965) → B. with sig.	Usual // Usual
	Faugère: F4 (1999) → F5 (2002)	Usual // Usual (linear algebra)
	⋮	
Euclidean ring	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Lichtblau (2012)	Usual or G-pols // Usual
Principal ideal domain	Möller strong (1988)	Usual // Usual with G-pol
	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Pan (1989)	Usual or G-pols // Usual
General (Noetherian) ring	Möller weak (1988)	Multiple // Multiple

Summary of Gröbner basis algorithms over rings with signatures

Three questions:

- How to compute S-polynomials?
- How to compute reductions?
- How to order signatures?

Case of fields: partial order is enough
[Eder, Pfister, Popescu 2017]: cannot order coefs

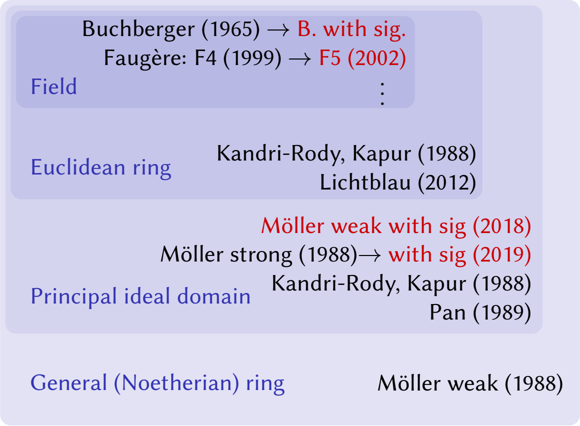
Field	Buchberger (1965) → B. with sig.	Usual // Usual
	Faugère: F4 (1999) → F5 (2002)	Usual // Usual (linear algebra)
	⋮	
Euclidean ring	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Lichtblau (2012)	Usual or G-pols // Usual
Principal ideal domain	Möller strong (1988)	Usual // Usual with G-pol
	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Pan (1989)	Usual or G-pols // Usual
General (Noetherian) ring	Möller weak (1988)	Multiple // Multiple

Summary of Gröbner basis algorithms over rings with signatures

Three questions:

- How to compute S-polynomials?
- How to compute reductions?
- How to order signatures?

Case of fields: partial order is enough
[Eder, Pfister, Popescu 2017]: cannot order coefs
[Francis, V. 2018]: partial order is enough



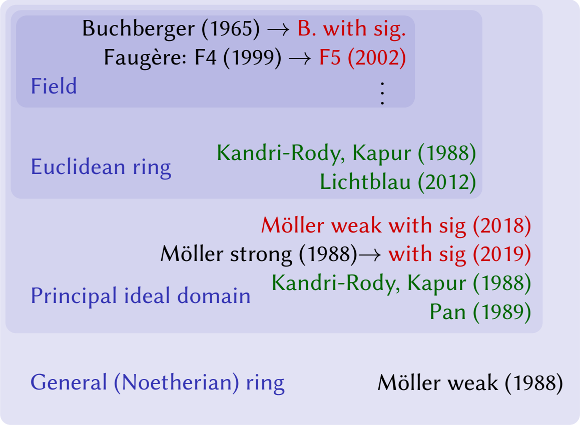
Field	Buchberger (1965) → B. with sig.	Usual // Usual
	Faugère: F4 (1999) → F5 (2002)	Usual // Usual (linear algebra)
	⋮	
Euclidean ring	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Lichtblau (2012)	Usual or G-pols // Usual
Principal ideal domain	Möller weak with sig (2018)	
	Möller strong (1988)→ with sig (2019)	Usual // Usual with G-pol
	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Pan (1989)	Usual or G-pols // Usual
General (Noetherian) ring	Möller weak (1988)	Multiple // Multiple

Summary of Gröbner basis algorithms over rings with signatures

Three questions:

- How to compute S-polynomials?
- How to compute reductions?
- How to order signatures?

Case of fields: partial order is enough
[Eder, Pfister, Popescu 2017]: cannot order coefs
[Francis, V. 2018]: partial order is enough



Field	Buchberger (1965) → B. with sig.	Usual // Usual
	Faugère: F4 (1999) → F5 (2002)	Usual // Usual (linear algebra)
	⋮	
Euclidean ring	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Lichtblau (2012)	Usual or G-pols // Usual
Principal ideal domain	Möller weak with sig (2018)	
	Möller strong (1988)→ with sig (2019)	Usual // Usual with G-pol
	Kandri-Rody, Kapur (1988)	Usual and G-pols // Usual
	Pan (1989)	Usual or G-pols // Usual
General (Noetherian) ring	Möller weak (1988)	Multiple // Multiple

What are G-polynomials?

Example: $f = 3x$, $g = 2y$, $I = \langle f, g \rangle$

- Not a strong Gröbner basis: $xy = yf - xg \in I$ is not reducible by f or g
- Adding $\text{S-Pol}(f, g) = 0$ does not help
- $\text{G-Pol}(f, g) = xy$

What are G-polynomials?

Example: $f = 3x$, $g = 2y$, $I = \langle f, g \rangle$

- Not a strong Gröbner basis: $xy = yf - xg \in I$ is not reducible by f or g
- Adding $\text{S-Pol}(f, g) = 0$ does not help
- $\text{G-Pol}(f, g) = xy$

Definition

$\mathbf{f}, \mathbf{g} \in \mathcal{I}$, u, v Bézout coefficients for $\mathrm{lc}(\mathbf{f}), \mathrm{lc}(\mathbf{g})$

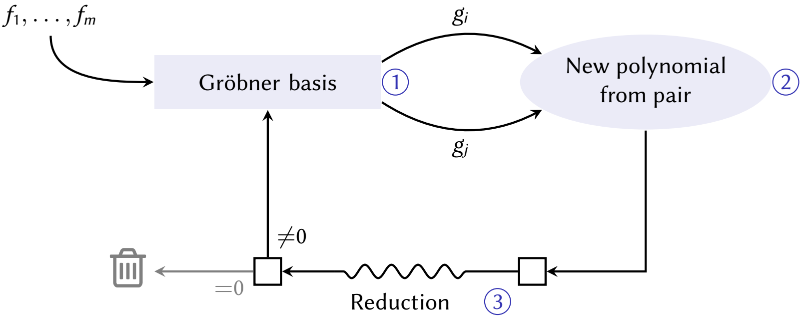
- $\text{G-Pol}(\mathbf{f}, \mathbf{g}) = u \dfrac{\mathrm{lcmlm}(\mathbf{f}, \mathbf{g})}{\mathrm{lm}(\mathbf{f})} \mathbf{f} + v \dfrac{\mathrm{lcmlm}(\mathbf{f}, \mathbf{g})}{\mathrm{lm}(\mathbf{g})} \mathbf{g}$

Main properties

- $\mathrm{lc}(\text{G-Pol}(\mathbf{f}, \mathbf{g})) = \mathrm{gcdlc}(\mathbf{f}, \mathbf{g})$
- If $\mathrm{lt}(\mathbf{f}) = t_1 \mathrm{lt}(\mathbf{g}_1) + t_2 \mathrm{lt}(\mathbf{g}_2)$, then $\mathbf{f}$ is reducible by $\text{G-Pol}(\mathbf{g}_1, \mathbf{g}_2)$
- One can always choose u, v such that

$$\mathrm{sig}(\text{G-Pol}(\mathbf{f}, \mathbf{g})) \simeq \max\left(\frac{\mathrm{lcmlm}(\mathbf{f}, \mathbf{g})}{\mathrm{lm}(\mathbf{f})} \mathrm{sig}(\mathbf{f}), \frac{\mathrm{lcmlm}(\mathbf{f}, \mathbf{g})}{\mathrm{lm}(\mathbf{g})} \mathrm{sig}(\mathbf{g})\right)$$

Kandri-Rody and Kapur's algorithm (*R* is a PID)



1. Selection: different strategies
2. Construction: S-polynomial

   and G-polynomial if $\mathrm{lc}(g_i)$ and $\mathrm{lc}(g_j)$ do not divide each other
3. Reduction

G-polynomials for syzygies

Need a similar construction to capture all possible combinations of syzygy signatures.

Definition

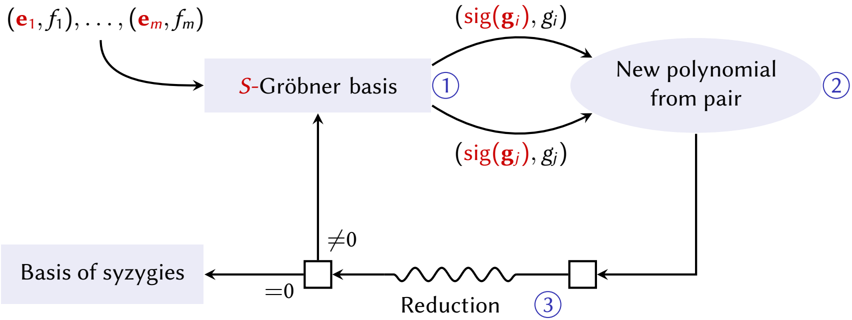
$\mathbf{z}_1, \mathbf{z}_2 \in \mathrm{Syz}(\mathcal{I})$ with $\mathrm{sig}(\mathbf{z}_i) = a_i m_i \mathbf{e}_j$; u, v Bézout coefficients for a_1, a_2

- $\text{G-Pol}(\mathbf{z}_1, \mathbf{z}_2) = u\dfrac{\mathrm{lcm}(m_1, m_2)}{m_1}\mathbf{z}_1 + v\dfrac{\mathrm{lcm}(m_1, m_2)}{m_2}\mathbf{z}_2$

Main properties

- $\mathrm{sig}(\text{G-Pol}(\mathbf{z}_1, \mathbf{z}_2)) = \gcd(a_1, a_2)\mathrm{lcm}(m_1, m_2)\mathbf{e}_j$
- If $\mathrm{sig}(\mathbf{f}) = t_1\mathrm{sig}(\mathbf{z}_1) + t_2\mathrm{sig}(\mathbf{z}_2)$, then $\mathbf{f}$ is sig-reducible by $\text{G-Pol}(\mathbf{z}_1, \mathbf{z}_2)$
- No need to be careful about the choice of u, v

Kandri-Rody and Kapur's algorithm, with signatures (R is a PID)



$(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)$

S-Gröbner basis ①

$(\mathrm{sig}(\mathbf{g}_i), g_i)$

$(\mathrm{sig}(\mathbf{g}_j), g_j)$

New polynomial from pair ②

Basis of syzygies

$\neq 0$

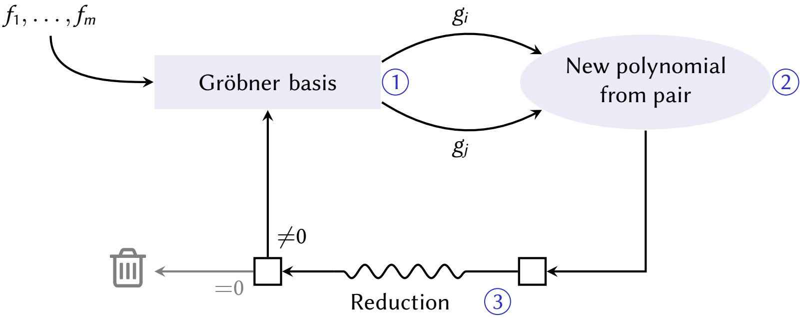
$=0$

Reduction ③

1. Selection: non-decreasing signatures
2. Construction: regular S-polynomial

   and G-polynomial if $\mathrm{lc}(\mathbf{g}_i)$ and $\mathrm{lc}(\mathbf{g}_j)$ do not divide each other
3. Reduction: regular

Pan/Lichtblau's algorithm (*R* is a PID)



1. Selection: different strategies
2. Construction: S-polynomial if one of $\mathrm{lc}(g_i)$ and $\mathrm{lc}(g_j)$ divides the other

   or G-polynomial if $\mathrm{lc}(g_i)$ and $\mathrm{lc}(g_j)$ do not divide each other
3. Reduction

Why does it work?

Idea:

- Let f and g with $a = \mathrm{lc}(f)$ and $b = \mathrm{lc}(g)$ not dividing each other, let $d = \mathrm{gcdlc}(f, g)$
- How to recover $\text{S-Pol}(f, g) = \frac{b}{d}\mu f - \frac{a}{d}\nu g$?

Why does it work?

Idea:

- Let f and g with $a = \mathrm{lc}(f)$ and $b = \mathrm{lc}(g)$ not dividing each other, let $d = \mathrm{gcdlc}(f, g)$
- How to recover $\text{S-Pol}(f, g) = \frac{b}{d}\mu f - \frac{a}{d}\nu g$?
- The algorithm computes $h = \text{G-Pol}(f, g) = u\mu f + v\nu g$, with $\mathrm{lc}(h) = d$

Why does it work?

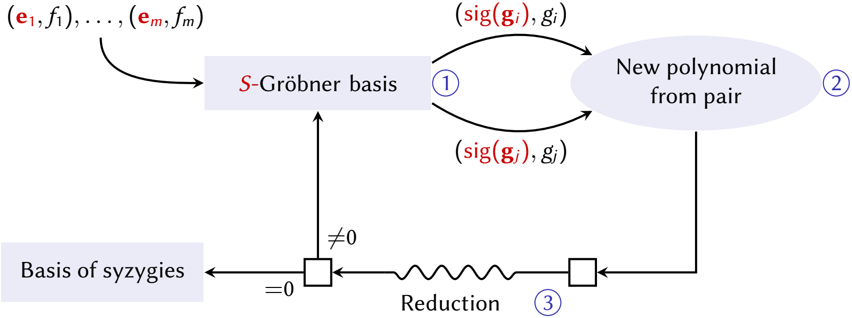
Idea:

- Let f and g with $a = \mathrm{lc}(f)$ and $b = \mathrm{lc}(g)$ not dividing each other, let $d = \mathrm{gcdlc}(f, g)$
- How to recover $\text{S-Pol}(f, g) = \frac{b}{d}\mu f - \frac{a}{d}\nu g$?

- The algorithm computes $h = \text{G-Pol}(f, g) = u\mu f + v\nu g$, with $\mathrm{lc}(h) = d$
- $\mathrm{lc}(h)$ divides both $\mathrm{lc}(f)$ and $\mathrm{lc}(g)$, and the algorithm computes the S-polynomials:

$$\begin{aligned}
\text{S-Pol}(f, h) &= \mu f - \frac{a}{d}h = \left(1 - \frac{ua}{d}\right)\mu f - \frac{av}{d}\mu g \\
&= \frac{vb}{d}\mu f - \frac{av}{d}\nu g = v\text{S-Pol}(f, g) \\
\text{S-Pol}(g, h) &= u\text{S-Pol}(f, g)
\end{aligned}$$

Pan/Lichtblau's algorithm, with signatures (R is a PID)



1. Selection: non-decreasing signatures
2. Construction: non-singular S-polynomial if one of $\mathrm{lc}(\mathbf{g}_i)$ and $\mathrm{lc}(\mathbf{g}_j)$ divides the other

   or G-polynomial if $\mathrm{lc}(\mathbf{g}_i)$ and $\mathrm{lc}(\mathbf{g}_j)$ do not divide each other
3. Reduction: regular

Why does it work?

Idea:

- Let $\mathbf{f}$ and $\mathbf{g}$ with $a = \mathrm{lc}(\mathbf{f})$ and $b = \mathrm{lc}(\mathbf{g})$ not dividing each other, let $d = \mathrm{gcdlc}(\mathbf{f}, \mathbf{g})$
- How to recover $\text{S-Pol}(\mathbf{f}, \mathbf{g}) = \frac{b}{d}\mu\mathbf{f} - \frac{a}{d}\nu\mathbf{g}$?

- The algorithm computes $\mathbf{h} = \text{G-Pol}(\mathbf{f}, \mathbf{g}) = u\mu\mathbf{f} + v\nu\mathbf{g}$, with $\mathrm{lc}(\mathbf{h}) = d$
- $\mathrm{lc}(\mathbf{h})$ divides both $\mathrm{lc}(\mathbf{f})$ and $\mathrm{lc}(\mathbf{g})$, and the algorithm computes the S-polynomials:

$$\begin{aligned}
\text{S-Pol}(\mathbf{f}, \mathbf{h}) &= \mu\mathbf{f} - \frac{a}{d}\mathbf{h} = \left(1 - \frac{ua}{d}\right)\mu\mathbf{f} - \frac{av}{d}\mu\mathbf{g} \\
&= \frac{vb}{d}\mu\mathbf{f} - \frac{av}{d}\nu\mathbf{g} = v\text{S-Pol}(\mathbf{f}, \mathbf{g}) \\
\text{S-Pol}(\mathbf{g}, \mathbf{h}) &= u\text{S-Pol}(\mathbf{f}, \mathbf{g})
\end{aligned}$$

Why does it work?

Idea:

sig $\mathbf{s}$ $\mathbf{t}$ with $\mu\mathbf{s} \gneq \nu\mathbf{t}$

- Let $\mathbf{f}$ and $\mathbf{g}$ with $a = \mathrm{lc}(\mathbf{f})$ and $b = \mathrm{lc}(\mathbf{g})$ not dividing each other, let $d = \mathrm{gcdlc}(\mathbf{f}, \mathbf{g})$
- How to recover $\text{S-Pol}(\mathbf{f}, \mathbf{g}) = \frac{b}{d}\mu\mathbf{f} - \frac{a}{d}\nu\mathbf{g}$?
- The algorithm computes $\mathbf{h} = \text{G-Pol}(\mathbf{f}, \mathbf{g}) = u\mu\mathbf{f} + v\nu\mathbf{g}$, with $\mathrm{lc}(\mathbf{h}) = d$
- $\mathrm{lc}(\mathbf{h})$ divides both $\mathrm{lc}(\mathbf{f})$ and $\mathrm{lc}(\mathbf{g})$, and the algorithm computes the S-polynomials:

$$\begin{aligned}
\text{S-Pol}(\mathbf{f}, \mathbf{h}) &= \mu\mathbf{f} - \frac{a}{d}\mathbf{h} = \left(1 - \frac{ua}{d}\right)\mu\mathbf{f} - \frac{av}{d}\mu\mathbf{g} \\
&= \frac{vb}{d}\mu\mathbf{f} - \frac{av}{d}\nu\mathbf{g} = v\text{S-Pol}(\mathbf{f}, \mathbf{g}) \\
\text{S-Pol}(\mathbf{g}, \mathbf{h}) &= u\text{S-Pol}(\mathbf{f}, \mathbf{g})
\end{aligned}$$

Why does it work?

Idea:

sig $\mathbf{s}$ $\mathbf{t}$ with $\mu\mathbf{s} \gneq \nu\mathbf{t}$

- Let $\mathbf{f}$ and $\mathbf{g}$ with $a = \operatorname{lc}(\mathbf{f})$ and $b = \operatorname{lc}(\mathbf{g})$ not dividing each other, let $d = \operatorname{gcdlc}(\mathbf{f}, \mathbf{g})$
- How to recover $\text{S-Pol}(\mathbf{f}, \mathbf{g}) = \frac{b}{d}\mu\mathbf{f} - \frac{a}{d}\nu\mathbf{g}$? Regular, sig $\simeq \mu\mathbf{s}$
- The algorithm computes $\mathbf{h} = \text{G-Pol}(\mathbf{f}, \mathbf{g}) = u\mu\mathbf{f} + v\nu\mathbf{g}$, with $\operatorname{lc}(\mathbf{h}) = d$
- $\operatorname{lc}(\mathbf{h})$ divides both $\operatorname{lc}(\mathbf{f})$ and $\operatorname{lc}(\mathbf{g})$, and the algorithm computes the S-polynomials:

$$\begin{aligned}\text{S-Pol}(\mathbf{f}, \mathbf{h}) &= \mu\mathbf{f} - \frac{a}{d}\mathbf{h} = \left(1 - \frac{ua}{d}\right)\mu\mathbf{f} - \frac{av}{d}\mu\mathbf{g} \\ &= \frac{vb}{d}\mu\mathbf{f} - \frac{av}{d}\nu\mathbf{g} = v\text{S-Pol}(\mathbf{f}, \mathbf{g}) \\ \text{S-Pol}(\mathbf{g}, \mathbf{h}) &= u\text{S-Pol}(\mathbf{f}, \mathbf{g})\end{aligned}$$

Why does it work?

Idea:

sig $\mathbf{s}$ $\mathbf{t}$ with $\mu\mathbf{s} \gnsim \nu\mathbf{t}$

- Let $\mathbf{f}$ and $\mathbf{g}$ with $a = \mathrm{lc}(\mathbf{f})$ and $b = \mathrm{lc}(\mathbf{g})$ not dividing each other, let $d = \mathrm{gcdlc}(\mathbf{f}, \mathbf{g})$
- How to recover $\text{S-Pol}(\mathbf{f}, \mathbf{g}) = \frac{b}{d}\mu\mathbf{f} - \frac{a}{d}\nu\mathbf{g}$? Regular, sig $\simeq \mu\mathbf{s}$

  sig $\simeq \mu\mathbf{s}$
- The algorithm computes $\mathbf{h} = \text{G-Pol}(\mathbf{f}, \mathbf{g}) = u\mu\mathbf{f} + v\nu\mathbf{g}$, with $\mathrm{lc}(\mathbf{h}) = d$
- $\mathrm{lc}(\mathbf{h})$ divides both $\mathrm{lc}(\mathbf{f})$ and $\mathrm{lc}(\mathbf{g})$, and the algorithm computes the S-polynomials:

$$\begin{aligned}\text{S-Pol}(\mathbf{f}, \mathbf{h}) &= \mu\mathbf{f} - \frac{a}{d}\mathbf{h} = \left(1 - \frac{ua}{d}\right)\mu\mathbf{f} - \frac{av}{d}\mu\mathbf{g} \\ &= \frac{vb}{d}\mu\mathbf{f} - \frac{av}{d}\nu\mathbf{g} = v\text{S-Pol}(\mathbf{f}, \mathbf{g}) \\ \text{S-Pol}(\mathbf{g}, \mathbf{h}) &= u\text{S-Pol}(\mathbf{f}, \mathbf{g})\end{aligned}$$

Why does it work?

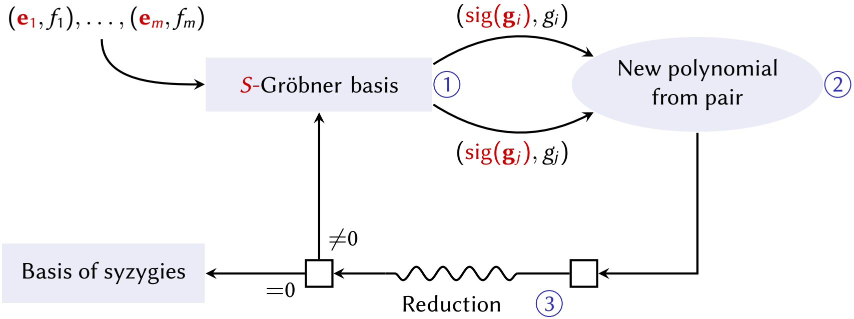
Idea:

sig $\mathbf{s}$ $\mathbf{t}$ with $\mu\mathbf{s} \gneq \nu\mathbf{t}$

- Let $\mathbf{f}$ and $\mathbf{g}$ with $a = \mathrm{lc}(\mathbf{f})$ and $b = \mathrm{lc}(\mathbf{g})$ not dividing each other, let $d = \mathrm{gcdlc}(\mathbf{f}, \mathbf{g})$
- How to recover $\text{S-Pol}(\mathbf{f}, \mathbf{g}) = \frac{b}{d}\mu\mathbf{f} - \frac{a}{d}\nu\mathbf{g}$? Regular, sig $\simeq \mu\mathbf{s}$
- The algorithm computes $\mathbf{h} = \overset{\text{sig} \simeq \mu\mathbf{s}}{\text{G-Pol}(\mathbf{f}, \mathbf{g})} = u\mu\mathbf{f} + v\nu\mathbf{g}$, with $\mathrm{lc}(\mathbf{h}) = d$
- $\mathrm{lc}(\mathbf{h})$ divides both $\mathrm{lc}(\mathbf{f})$ and $\mathrm{lc}(\mathbf{g})$, and the algorithm computes the S-polynomials:

$$\begin{aligned}
\text{S-Pol}(\mathbf{f}, \mathbf{h}) &= \overset{\simeq \mu\mathbf{s}}{\mu\mathbf{f}} - \overset{\simeq \mu\mathbf{s}}{\frac{a}{d}\mathbf{h}} = \overset{\text{not regular}}{\left(1 - \frac{ua}{d}\right)\mu\mathbf{f} - \frac{av}{d}\mu\mathbf{g}} \\
&= \frac{vb}{d}\mu\mathbf{f} - \frac{av}{d}\nu\mathbf{g} = v\text{S-Pol}(\mathbf{f}, \mathbf{g}) \\
\text{S-Pol}(\mathbf{g}, \mathbf{h}) &= u\text{S-Pol}(\mathbf{f}, \mathbf{g})
\end{aligned}$$

Pan/Lichtblau's algorithm, with signatures (*R* is a PID)



$(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)$

S-Gröbner basis ①

$(\mathrm{sig}(\mathbf{g}_i), g_i)$

New polynomial
from pair ②

$(\mathrm{sig}(\mathbf{g}_j), g_j)$

$\neq 0$

Basis of syzygies

$= 0$

Reduction ③

1. Selection: non-decreasing signatures
2. Construction: non-singular S-polynomial if one of $\mathrm{lc}(\mathbf{g}_i)$ and $\mathrm{lc}(\mathbf{g}_j)$ divides the other

   or G-polynomial if $\mathrm{lc}(\mathbf{g}_i)$ and $\mathrm{lc}(\mathbf{g}_j)$ do not divide each other
3. Reduction: regular

Comparison of the algorithms

Theorem: general criterion for correctness

Let $\mathcal{G} \subset \mathcal{I}$ and $\mathcal{G}_z \subset \mathrm{Syz}(I)$ be such that:

- for all i, there is an element with signature $\mathbf{e}_i$ in $\mathcal{G} \cup \mathcal{G}_z$
- all regular S-pols of $\mathcal{G}$ s-reduce to 0 mod $\mathcal{G}$
- if those reductions are regular, their result is sig-reducible mod $\mathcal{G}_z$
- all G-pols of $\mathcal{G}$ are s-reducible mod $\mathcal{G}$
- all G-pols of $\mathcal{G}_z$ are sig-reducible mod $\mathcal{G}_z$

Then $\mathcal{G}$ is a SGB and $\mathcal{G}_z$ is a sig-basis of syzygies.

Kandri-Rody, Kapur	Pan/Lichtblau
S-pol if regular	S-pol is non-singular and lc divides
G-pol if lc does not divide	G-pol if lc does not divide
Regular reductions	Regular reductions

Comparison of the algorithms

Theorem: general criterion for correctness

Let $\mathcal{G} \subset \mathcal{I}$ and $\mathcal{G}_z \subset \mathrm{Syz}(I)$ be such that:

- for all i, there is an element with signature $\mathbf{e}_i$ in $\mathcal{G} \cup \mathcal{G}_z$
- all regular S-pols of $\mathcal{G}$ s-reduce to 0 mod $\mathcal{G}$
- if those reductions are regular, their result is sig-reducible mod $\mathcal{G}_z$
- all G-pols of $\mathcal{G}$ are s-reducible mod $\mathcal{G}$
- all G-pols of $\mathcal{G}_z$ are sig-reducible mod $\mathcal{G}_z$

Then $\mathcal{G}$ is a SGB and $\mathcal{G}_z$ is a sig-basis of syzygies.

Kandri-Rody, Kapur	Pan/Lichtblau
S-pol if regular	S-pol is non-singular and lc divides
G-pol if lc does not divide	G-pol if lc does not divide
Regular reductions	Regular reductions
More criteria?	More criteria?

Super-reducibility

Super-reducible criterion in the case of fields

- **f** is super reducible modulo **g** if $t\mathrm{sig}(\mathbf{g}) \simeq \mathrm{sig}(\mathbf{f})$ and $t\mathrm{lt}(\mathbf{g}) = \mathrm{lt}(\mathbf{f})$
- $\mathbf{h} = \mathbf{f} - t\mathbf{g}$ is a singular s-reduction
- If **h** s-reduces to 0 mod $\mathcal{G}$, then**f** s-reduces to 0 mod $\mathcal{G}$
- Consequence: we can exclude super-reducible polynomials

Super-reducible criterion in the case of rings

- **f** is super reducible modulo **g** if $t\mathrm{sig}(\mathbf{g}) = \mathrm{sig}(\mathbf{f})$ and $t\mathrm{lt}(\mathbf{g}) \simeq \mathrm{lt}(\mathbf{f})$
- $\mathbf{f}' = \mathbf{f} - t\mathbf{g}$ is not a reduction!
- If $\mathbf{f}'$ s-reduces to 0 mod $\mathcal{G}$ and G-pols of $\mathcal{G}$ s-reduce to 0, then **f** s-reduces to 0 mod $\mathcal{G}$
- Consequence: we can exclude super-reducible S-polynomials

Cover property

Definition: cover property in the case of fields

The pair $(\mathbf{f}_1, \mathbf{f}_2)$ is covered by $\mathbf{g} \in \mathcal{G} \cup \mathcal{G}_z$ if:

- there exists a term t such that $\mathrm{sig}(S\text{-Pol}(\mathbf{f}_1, \mathbf{f}_2)) = t\,\mathrm{sig}(\mathbf{g})$
- $t\,\mathrm{lt}(\mathbf{g}) < \mathrm{lcmlm}(\mathbf{f}_1, \mathbf{f}_2)$ (with $\mathrm{lt}(\mathbf{g}) = 0$ if syzygy)

Cover property

Definition: cover property in the case of fields

The pair $(\mathbf{f}_1, \mathbf{f}_2)$ is covered by $\mathbf{g} \in \mathcal{G} \cup \mathcal{G}_z$ if:

- there exists a term t such that $\mathrm{sig}(\text{S-Pol}(\mathbf{f}_1, \mathbf{f}_2)) = t\mathrm{sig}(\mathbf{g})$
- $t\mathrm{lt}(\mathbf{g}) < \mathrm{lcmlm}(\mathbf{f}_1, \mathbf{f}_2)$ (with $\mathrm{lt}(\mathbf{g}) = 0$ if syzygy)

Definition: cover property in the case of rings

The pair $(\mathbf{f}_1, \mathbf{f}_2)$ is covered by $\mathbf{g} \in \mathcal{G}$ and $\mathbf{z} \in \mathcal{G}_z$ if:

- there exist terms t_g, t_z such that $\mathrm{sig}(\text{S-Pol}(\mathbf{f}_1, \mathbf{f}_2) = t_g\mathrm{sig}(\mathbf{g}) + t_z\mathrm{sig}(\mathbf{z})$
- $t_g\mathrm{lt}(\mathbf{g}) < \mathrm{lcmlm}(\mathbf{f}_1, \mathbf{f}_2)$

Correctness criterion with the cover property

Reminder: general criterion for correctness

Let $\mathcal{G} \subset \mathcal{I}$ and $\mathcal{G}_z \subset \mathrm{Syz}(I)$ be such that:

- for all i, there is an element with signature $\mathbf{e}_i$ in $\mathcal{G} \cup \mathcal{G}_z$
- all regular S-pols of $\mathcal{G}$ s-reduce to 0 mod $\mathcal{G}$
- if those reductions are regular, their result is sig-reducible mod $\mathcal{G}_z$
- all G-pols of $\mathcal{G}$ are s-reducible mod $\mathcal{G}$
- all G-pols of $\mathcal{G}_z$ are sig-reducible mod $\mathcal{G}_z$

Then $\mathcal{G}$ is a SGB and $\mathcal{G}_z$ is a sig-basis of syzygies.

Correctness criterion with the cover property

Theorem: cover criterion for correctness

Let $\mathcal{G} \subset \mathcal{I}$ and $\mathcal{G}_z \subset \mathrm{Syz}(I)$ be such that:

- for all i, there is an element with signature $\mathbf{e}_i$ in $\mathcal{G} \cup \mathcal{G}_z$
- all regular S-pols of $\mathcal{G}$ are covered by a pair of $\mathcal{G}$, $\mathcal{G}_z$
- all G-pols of $\mathcal{G}$ are s-reducible modulo $\mathcal{G}$
- all G-pols of $\mathcal{G}_z$ are sig-reducible mod $\mathcal{G}_z$

Then $\mathcal{G}$ is a SGB and $\mathcal{G}_z$ is a sig-basis of syzygies.

This criterion is convenient...

- in practice, because it allows to eliminate many elements
- in theory, because it allows for a simpler proof of correctness

But it requires that all regular S-pols of $\mathcal{G}$ be covered, which Pan/Lichtblau a priori cannot enforce.

Quantitative comparison between the algorithms

System	Algorithm	Total pairs	Reduced	To zero	Time (s)
Katsura-4	Kandri-Rody, Kapur	420	188	0	1.35
	Pan/Lichtblau	855	412	0	1.6
Katsura-5	Kandri-Rody, Kapur	248	723	0	32.40
	Pan/Lichtblau	7178	3983	0	79.87
Cyclic-5	Kandri-Rody, Kapur	221	63	0	0.37
	Pan/Lichtblau	347	158	0	0.71
Cyclic-6	Kandri-Rody, Kapur	3019	742	8	200.33
	Pan/Lichtblau	9672	5782	8	616.82

- Toy implementation of both algorithms in Magma
- Kandri-Rody and Kapur is almost always more efficient than Pan/Lichtblau
- It is not due to the lack of cover criterion

Indicative timings

System	S-GB (s)	Recons. (s)	**Total (s)**	GB (s)	**GB + coefs (s)**	**Syz. basis (s)**
Cyclic-5	0.4	0.1	**0.5**	0.01	**954.6**	**954.8**
Cyclic-6	200.3	10.6	**210.9**	2.08	**>24h**	**>24h**

- Signature algorithms: Kandri-Rody and Kapur, reconstruction
- Classical algorithm: Magma's built-in `GroebnerBasis`, `IdealWithFixedBasis` and `SyzygyMatrix`

Conclusion

This work

- Two signature-based algorithms for PID's following closely Buchberger's algorithm
- Compatible with powerful criteria such as super-reducibility and the cover criterion
- Additional criteria and optimizations are available (coprime criterion, Gebauer-Möller criteria, coefficient reductions...)
- Toy implementation in Magma

Future directions

- Linear algebra algorithms à la F4
- Improve implementation
- Extend use of signature bases

Conclusion

This work

- Two signature-based algorithms for PID's following closely Buchberger's algorithm
- Compatible with powerful criteria such as super-reducibility and the cover criterion
- Additional criteria and optimizations are available (coprime criterion, Gebauer-Möller criteria, coefficient reductions...)
- Toy implementation in Magma

Future directions

- Linear algebra algorithms à la F4
- Improve implementation
- Extend use of signature bases

Thanks for your attention!