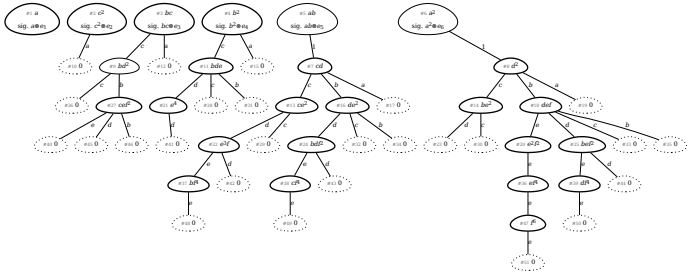


Axioms for a theory of signatures

Pierre Lairez
MATHEXP, Université Paris–Saclay, Inria, France

XLIM, June 11, 2026, Limoges

Signatures

- *Signatures* are monomials attached to polynomials during the computation of a Gröbner basis.

  They make it possible to detect many reductions to zero!

- Faugère, J.-C. (2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). *Proc. ISSAC 2002*, 75–83

  Arri and Perry (2011), Eder and Perry (2011), Eder and Roune (2013), Galkin (2014), Gao, Volny, and Wang (2016), Eder and Faugère (2017), Lairez (2024), etc.

Blind spots of the descriptive theory

Gröbner bases

- ✓ Defined by $\langle \mathrm{lm}\, G \rangle = \mathrm{lm}\langle G \rangle$.
- ✓ Characterized by Buchberger's S-pair criterion
- ✓ Algorithms terminate thanks to Dickson's lemma

Signature bases


What is a signature basis?
(Independently of the input)


What makes signatures consistent?
(Independently of the input)


How to characterize a signature basis?
(In finite terms)


What makes signature algorithms terminate?
(Independently of the precise algorithm)

1. Introduction

2. Properties of signatures

3. Combinatorial characterization of signature bases

4. Algorithms and termination issues

Pivot bases

M is a linear space with a well-ordered basis $\mathcal{M}$.

Induces a function

$$\operatorname{lm} : M \to \mathcal{M} \cup \{0\}$$

$E \subseteq M$ is a *pivot basis* if

$$\forall x \in \langle E \rangle \setminus \{0\}\,, \exists e \in E, \operatorname{lm} x = \operatorname{lm} e.$$

Gröbner bases

- A is a monoid acting linearly on M such that

$$\forall a \in A, \forall f, g \in M, \operatorname{lm} f < \operatorname{lm} g \Leftrightarrow \operatorname{lm}(af) < \operatorname{lm}(ag).$$

  (M is a *monomial module* over A)

- $G \subseteq M$ is a *Gröbner basis* if $AG = \{ag \mid a \in A, g \in G\}$ is a pivot basis.

Signatures

$\mathcal{S}$ is a well-ordered set with an action of A such that

$$\forall a \in A, \forall \sigma, \tau \in \mathcal{S}, \sigma < \tau \Leftrightarrow a\sigma < a\tau,$$
$$\forall a, b \in A, \forall \sigma \in \mathcal{S}, \forall m \in \mathcal{M}, a\sigma \leq b\sigma \implies am \leq bm.$$

A *sigpair* f is an element of $M \times \mathcal{S}$
- $f^\natural$ denotes the polynomial part
- $\operatorname{sig} f$ denotes the $\mathcal{S}$ part

A acts on sigpairs: $(af)^\natural = af^\natural$ and $\operatorname{sig}(af) = a \operatorname{sig} f$.

A *sigset* is a subset $G \subseteq M \times \mathcal{S}$

Notation: for a sigset G,

$$AG^\sigma = \{ag^\natural \mid a \in A, g \in G, a \operatorname{sig} g = \sigma\}$$
$$AG^{\leq\sigma} = \{ag^\natural \mid a \in A, g \in G, a \operatorname{sig} g \leq \sigma\}$$
$$AG^{<\sigma} = \{ag^\natural \mid a \in A, g \in G, a \operatorname{sig} g < \sigma\}$$

The polynomial case...

* $M = K[x_1, \ldots, x_n]$
* $\mathcal{M} = \left\{ x_1^{\alpha_1} \cdots x_n^{\alpha_n} \;\middle|\; \alpha_1, \ldots, \alpha_n \in \mathbb{N} \right\}$, with any monomial order
* $A = \mathcal{M}$
* $\mathcal{S} = \mathcal{M} \times \{1, \ldots, n\}$, with TOP order (compare $\mathcal{M}$ first, break ties with the indices), or POT order (compare the indices first, break ties with $\mathcal{M}$).

… but also

- ✓ $M = K[\mathbf{x}]^n$ (the module case, very important!)
- ✓ $M = K[x^2, xy, y^2]$ (monomials on a lattice)
- ✓ $M = K[t^2, t^3]$ (missing monomials)
- ✓ $M = K[x_1, \ldots, x_n]\langle \partial_1, \ldots, \partial_n \rangle$ (Weyl/Ore algebras)
- ✓ $M = K\{x_1, \ldots, x_n\}$ (free algebra)
- ✗ $M = K[[x, y]]$ (local orderings)
- ✗ $M = \mathbb{Z}[x, y]$ (non-field coefficient ring)

Signature bases

- A sigset $G \subseteq M \times \mathcal{S}$ is a *signature basis* if $AG^{\leq\sigma}$ is a pivot basis, for all $\sigma \in \mathcal{S}$.
- If G is a signature basis, then $G^{\natural}$ is a Gröbner basis:
  - $AG^{\natural} = \cup_{\sigma\in\mathcal{S}} AG^{\leq\sigma}$
  - The union of an increasing family of pivot bases is a pivot basis.
- To complete a sigset into a signature basis, one allowed operation (*sigsafe extension*):

$$G \to G \cup \left\{\left(\lambda a f^{\natural} + h, \operatorname{sig}(af)\right)\right\},$$

with $\lambda \in K^{\times}$, $a \in A$, $f \in G$, $h \in \langle AG^{<\operatorname{sig}(af)}\rangle$.

Prebases

- A sigset G is a *prebasis* if

$$\forall \sigma \in \mathcal{S}, \forall f \in AG^{\sigma}, f \text{ generates } \langle AG^{\leq \sigma} \rangle / \langle AG^{<\sigma} \rangle .$$

- This defines what it means for signatures to be consistent.
  Two elements with the same signature are substitutable.
- A sigsafe extension of a prebasis is a prebasis.

Forging prebases

- Given $H \subseteq M$, can we *forge* signatures to turn it into a prebasis?
- Assume that the action of A on $\mathcal{M}$ is *free*:

$$\forall a, b \in A, \forall m \in \mathcal{M}, \mathrm{lm}(am) = \mathrm{lm}(bm) \Rightarrow a = b.$$

Write $H = \{g_1, \ldots, g_r\}$.
Choose $\mathcal{S} = \mathcal{M} \times \{1, \ldots, r\}$ (with POT or TOP ordering).
The monoid A acts on $\mathcal{S}$ through the $\mathcal{M}$ part only.
Define

$$G = \{(g_i, (\mathrm{lm}\, g_i, i)) \mid 1 \leq i \leq r\}.$$

Then $G^\natural = H$ and G is a prebasis: for all $\sigma \in \mathcal{S}$, $\#AG^\sigma \leq 1$.

Example

* $M = K[x, y]$
* $\mathcal{M} = \{x^a y^b \mid a, b \in \mathbb{N}\}$, with grevlex order
* $A = \mathcal{M}$
* $\mathcal{S} = \mathcal{M} \times \{1, 2, 3\}$, with TOP order (compare $\mathcal{M}$ first, break ties with the indices)

* $g_1 = \underline{x^2 y^2} - 1$
  $g_2 = \underline{y^5} - x^2 y$
  $g_3 = \underline{x^5} - xy^2$

  This is a prebasis:

$$G = \left\{ \left(g_1, x^2 y^2 \, e_1 \right), \left(g_2, y^5 \, e_2 \right), \left(g_3, x^5 \, e_3 \right) \right\}$$

Prebases and Gröbner bases

- Let $H \subseteq M$ and $\mathcal{S} = \mathcal{M}$. Then

  $$\{(h, \operatorname{lm} h) \mid h \in H\} \text{ is a prebasis} \Leftrightarrow H \text{ is a Gröbner basis.}$$

- Let S be a monomial module over A,
  let $\phi : S \to M$ be an A-linear map, and
  let $H \subseteq S$.
  Then

  $$H \text{ is a Gröbner basis} \Rightarrow \{(\phi(h), \operatorname{lm} h) \mid h \in H\} \text{ is a prebasis.}$$

- When parts of the input are already Gröbner bases, we can forge signatures that exploit them.

Example: sum of ideals

We have a Gröbner basis $\{f_1, \ldots, f_r\}$ for some submodule I of M, and a Gröbner basis $\{g_1, \ldots, g_s\}$ for some submodule J.

How to compute a Gröbner basis for the submodule $I + J$?

Use the prebasis

$$\{(f_1, \mathrm{lm}(f_1)\, e_1), \ldots, (f_r, \mathrm{lm}(f_r)\, e_r), (g_1, \mathrm{lm}(g_1)\, e_{r+1}), \ldots, (g_s, \mathrm{lm}(g_s)\, e_{r+s})\}$$

Use the prebasis

$$\{(f_1, \mathrm{lm}(f_1)\, e_1), \ldots, (f_r, \mathrm{lm}(f_r)\, e_1), (g_1, \mathrm{lm}(g_1)\, e_2), \ldots, (g_s, \mathrm{lm}(g_s)\, e_2)\},$$

because

$$\{(f_i, 0)\}_{1 \le i \le r} \cup \{(0, g_j)\}_{1 \le j \le s}$$

is a Gröbner basis in M^2.

Top reduction

Let G be a sigset.
A sigpair f is *G-reduced* if

$$\operatorname{lm} f^{\natural} \notin \operatorname{lm}(AG^{<\operatorname{sig} f})$$
$$= \left\{ \operatorname{lm}(ag^{\natural}) \;\middle|\; a \in A, g \in G, a \operatorname{sig} g < \operatorname{sig} f \right\}.$$

(Only the leading monomial matters.)

If f is *not* G-reduced, then there is a sigpair g such that:

- g is G-reduced
- $\operatorname{sig} g = \operatorname{sig} f$
- $\operatorname{lm} g^{\natural} < \operatorname{lm} f^{\natural}$
- $G \cup \{g\}$ is a sigsafe extension of G
  (that is $g^{\natural} \equiv f^{\natural} \mod \langle AG^{<\operatorname{sig} f} \rangle$)

Rewrite bases

A prebasis G is a *rewrite basis* at $\sigma \in \mathcal{S}$ if either:

- $\forall f \in AG, \operatorname{sig} f \neq \sigma$; or
- $\exists f \in AG, \operatorname{sig} f = \sigma$ and f is G-reduced.

A prebasis G is a *rewrite basis* if it is a rewrite basis at every $\sigma \in \mathcal{S}$.

A rewrite basis is a signature basis.

The prebasis property is subtle, but satisfied *by design*.
The rewrite property is purely *combinatorial*: it depends only on the signatures and leading monomials of the elements of G, not the actual coefficients.

This is a simplified form of the definition proposed by Eder and Roune (2013).

Example

* $g_1 = \underline{x^2y^2} - 1 \quad g_2 = \underline{y^5} - x^2y \quad g_3 = \underline{x^5} - xy^2$

$$G = \left\{\left(g_1, x^2y^2\, e_1\right), \left(g_2, y^5\, e_2\right), \left(g_3, x^5\, e_3\right)\right\}$$

* The smallest signature at which it is not a rewrite basis is $\sigma = x^2y^5\, e_2$:

$$AG^\sigma = \left\{x^2 g_2\right\} = \left\{\left(\underline{x^2y^5} - x^4y, x^2y^5\, e_2\right)\right\},$$

and there is a top reduction of $x^2 g_2$ by $y^3 g_1$.
So AG^σ does not contain any $\rightarrow_G$-reduced element.

Note that $x^2 g_2$ does not reduce $y^3 g_1$ because $\mathrm{sig}(x^2 g_2) > \mathrm{sig}(y^5 g_1)$, so G is a rewrite basis at $x^2y^5\, e_1$. The symmetry of critical pairs is broken by the signatures.

The meta-algorithm

input G a prebasis
output A sigsafe extension of G that is a rewrite basis

1 **while** G is not a rewrite basis**:**
2 pick σ at which G is not a rewrite basis
3 pick $f \in AG$ with $\operatorname{sig} f = \sigma$
4 $g \leftarrow G$-reduction of f
5 $G \leftarrow G \cup \{g\}$
6 **return** G

- How to check that G is a rewrite basis?
  If not, how to pick a signature at which it is not a rewrite basis?
- The algorithm is correct, but it may not terminate, even in the polynomial case...

Why do signatures cut useless computations?

We need to deal with at most one element per signature, because we know that there is at most one pivot to discover.

(This is analogous to Hilbert-driven algorithms.)

When we encounter a reduction to zero in signature σ, the sigpair $(0, \sigma)$ is inserted in G.

For every signature τ that is a multiple of σ, $(0, \tau)$ is an element of AG that is G-reduced.

$\rightsquigarrow$ We don't need to deal with these signatures anymore. Reductions to zero that are consequences of another one are automatically eliminated.

The Faugère criterion

Let G be a prebasis. A signature σ is *critical* if there are $f \in G$ and $a \in A$ such that:

- $\sigma = a \operatorname{sig} f$
- af is not G-reduced
- $\forall b, c \in A, bc \operatorname{sig} f = \sigma$ and $c \operatorname{sig} f < \sigma \implies cf$ is G-reduced

Under Noetherian hypotheses,
there are only finitely many critical signatures.
They are easy to compute and update.

In the polynomial setting,

$$\operatorname{crit}(G) \subseteq \left\{ \frac{\max\left(\operatorname{lm}(g) \operatorname{sig}(f), \operatorname{lm}(f) \operatorname{sig}(g)\right)}{\gcd(\operatorname{lm} f, \operatorname{lm} g)} \,\middle|\, f, g \in G \text{ distinct} \right\}.$$

If G is a rewrite basis at every critical signature,
then G is a rewrite basis.

Noetherian hypotheses

- Divisibility defines a partial order $\trianglelefteq$ on $\mathcal{M}$ and $\mathcal{S}$:

  $m \trianglelefteq n$ if $\exists a \in A, am = n$.

  A partial order $\trianglelefteq$ is a *well partial order* if for any sequence $(x_i)_{i \geq 0}$,

  $\exists i < j, x_i \trianglelefteq x_j$.

- We assume that divisibility is a well partial order on $\mathcal{S}$ and $\mathcal{M}$.

  $\rightsquigarrow$ It is also a well partial order on $\mathcal{M} \times \mathcal{S}$.

The base algorithm, Faugère (2002) style

while G is not a rewrite basis at every $\sigma \in \mathrm{crit}(G)$**:**
  pick the **smallest** $\sigma \in \mathrm{crit}(G)$ at which G is not a rewrite basis
  pick $af \in AG$ with $a \operatorname{sig} f = \sigma$ and f **most *recent***
  $g \leftarrow G$-reduction of af
  $G \leftarrow G \cup \{g\}$
return G

Termination proved by Galkin (2014).

The $\mathrm{crit}(G)$ notation conveniently puts nontrivial computations under the rug.
How to make them efficient is not completely understood yet. See Lairez, Mohr, and Ternier (2026) for a recent improvement.

The base algorithm, Arri and Perry (2011) style

while G is not a rewrite basis at every $\sigma \in \operatorname{crit}(G)$**:**
  pick the **smallest** $\sigma \in \operatorname{crit}(G)$ at which G is not a rewrite basis
  pick $af \in AG$ with $a \operatorname{sig} f = \sigma$ and $a \operatorname{lm} f$ **minimal**
  $g \leftarrow G$-reduction of af
  $G \leftarrow G \cup \{g\}$
return G

Change the reductant selection to obtain an easier termination proof.

The base algorithm, Gao, Volny, and Wang (2016) style

1 **while** G is not a rewrite basis at every $\sigma \in \mathrm{crit}(G)$**:**
2 pick $\sigma \in \mathrm{crit}(G)$ at which G is not a rewrite basis ⚡ **out of order**
3 pick $af \in AG$ with $a \operatorname{sig} f = \sigma$ and $a \operatorname{lm} f$ **minimal**
4 $g \leftarrow G$-reduction of af
5 $G \leftarrow G \cup \{g\}$
6 **return** G

⚡ In practice, it is more efficient to process signatures *in order*,
BUT, some variants of F5 (for example F5 with saturation, or F5/F4),
can be interpreted as a standard F5 with *out of order* signature processing.
So we need to understand termination in this case.

The base algorithm, Lairez (2024) style

1 **while** G is not a rewrite basis at every $\sigma \in \mathrm{crit}(G)$**:**
2 pick $\sigma \in \mathrm{crit}(G)$ at which G is not a rewrite basis ⚡ **out of order**
3 pick $af \in AG$ with $a \operatorname{sig} f = \sigma$ and f **ancestor-maximal**
4 $g \leftarrow G$-reduction of af
5 $G \leftarrow G \cup \{g\}$
6 **return** G

The *parent* of $g \in G$ inserted on line 5 is the $f \in G$ from which g comes. This defines a partial order on G: the *ancestor relation*. The constraint in the algorithm is: don't pick f if you can choose one of its children instead.

Faugère's choice (f most recent) is ancestor-maximal.
Arri and Perry's choice ($a \operatorname{lm} f$ minimal) is ancestor-maximal.

Termination of the GVW algorithm

1 **while** G is not a rewrite basis at every $\sigma \in \operatorname{crit}(G)$:
2 pick $\sigma \in \operatorname{crit}(G)$ at which G is not a rewrite basis ⚡ **out of order**
3 pick $af \in AG$ with $a \operatorname{sig} f = \sigma$ and $a \operatorname{lm} f$ **minimal**
4 $g \leftarrow G$-reduction of af
5 $G \leftarrow G \cup \{g\}$
6 **return** G

For contradiction, let $g_1, g_2, \ldots$ be the infinite sequence of sigpairs added to G.

- By Noetherianity, there is some $i < j$ and $a, b \in A$ such that $a \operatorname{sig} g_i = \operatorname{sig} g_j$ and $b \operatorname{lm} g_i = \operatorname{lm} g_j$.
- If $b \operatorname{sig} g_i < \operatorname{sig} g_j$, then g_i is not $\{g_i\}$-reduced. ✗
- Assume $b \operatorname{sig} g_i \geq \operatorname{sig} g_j$.
  Since $\operatorname{sig} g_j = a \operatorname{sig} g_i$, this implies that $\operatorname{lm} g_j = b \operatorname{lm} g_i \geq a \operatorname{lm} g_i$.
- If $\operatorname{lm} g_j = a \operatorname{lm} g_i$, then G was already a rewrite basis at $\operatorname{sig} g_j$ when g_j is inserted. ✗
- So $\operatorname{lm} g_j > a \operatorname{lm} g_i$, but this contradicts the minimality on line 3. ✗

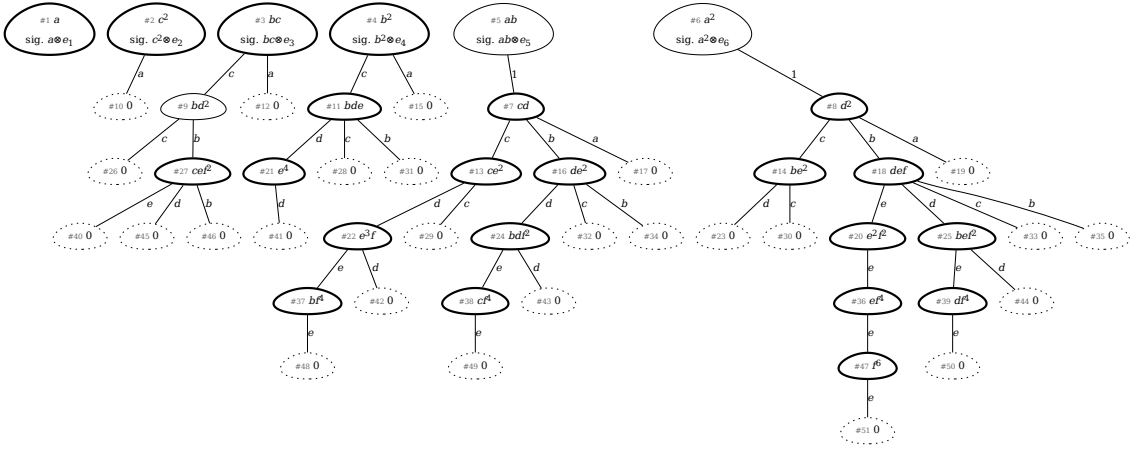
Termination of Lairez's algorithm

* If f is an older brother of g then $\operatorname{sig} f$ does not divide $\operatorname{sig} g$, because of the *ancestor-maximal* pick.
  By Noetherianity of $\mathcal{S}$, an element has finitely many children.

* Consider an infinite lineage $g_1, g_2, \dots$ (a chain where each element is the child of the previous one)
  There are some $i < j$ and $b \in A$ such that $b \operatorname{lm} g_i = \operatorname{lm} g_j$.
  The ancestor relation implies that there is some $a \in A$ such that $a \operatorname{sig} g_i = \operatorname{sig} g_j$ and $a \operatorname{lm} g_i > \operatorname{lm} g_j$.
  Since g_j is $\{g_i\}$-reduced, we have $b \operatorname{sig} g_i \geq \operatorname{sig} g_j = a \operatorname{sig} g_i$. This contradicts $b \operatorname{lm} g_i = \operatorname{lm} g_j < a \operatorname{lm} g_i$.

* By König's lemma the family tree is finite.

A family tree, a.k.a. sigtree (Katsura 6)



References I

Arri, A., & Perry, J. (2011). The F5 criterion revised. *J. Symb. Comput.*, *46*(9), 1017–1029.

Eder, C., & Faugère, J.-C. (2017). A survey on signature-based algorithms for computing Gröbner bases. *J. Symb. Comput.*, *80*(3), 719–784.

Eder, C., & Perry, J. (2011). Signature-based algorithms to compute Gröbner bases. *Proc. ISSAC 2011*, 99–106.

Eder, C., & Roune, B. H. (2013). Signature rewriting in Gröbner basis computation. *Proc. ISSAC 2013*, 331–338.

Faugère, J.-C. (2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). *Proc. ISSAC 2002*, 75–83.

Galkin, V. V. (2014). Termination of the F5 algorithm. *Program. Comput. Softw.*, *40*(2), 47–57.

Gao, S., Volny, F., & Wang, M. (2016). A new framework for computing Gröbner bases. *Math. Comp.*, *85*(297), 449–465.

Lairez, P. (2024). Axioms for a theory of signature bases. *J. Symb. Comput.*, *123*, 102275.

Lairez, P., Mohr, R., & Ternier, T. (2026). A data structure for monomial ideals with applications to signature Gröbner bases. *Proc. ISSAC 2026* to appear.