On Two Signature Variants Of Buchberger's Algorithm Over Principal Ideal Domains

Maria Francis
Indian Institute of Technology Hyderabad
Hyderabad, India
mariaf@iith.ac.in

Thibaut Verron
Institute for Algebra / Johannes Kepler University
Linz, Austria
thibaut.verron@jku.at

ABSTRACT

Signature-based algorithms have brought large improvements in the performances of Gröbner bases algorithms for polynomial systems over fields. Furthermore, they yield additional data which can be used, for example, to compute the module of syzygies of an ideal or to compute coefficients in terms of the input generators.

In this paper, we examine two variants of Buchberger's algorithm to compute Gröbner bases over principal ideal domains, with the addition of signatures. The first one is adapted from Kandri-Rody and Kapur's algorithm [16], whereas the second one uses the ideas developed in the algorithms by L. Pan [22] and D. Lichtblau [17]. The differences in constructions between the algorithms entail differences in the operations which are compatible with the signatures, and in the criteria which can be used to discard elements.

We prove that both algorithms are correct and discuss their relative performances in a prototype implementation in Magma.

CCS CONCEPTS

• **Computing methodologies** → **Algebraic algorithms**;

KEYWORDS

Algorithms, Gröbner bases, Signature-based algorithms, Polynomials over rings, Principal Ideal Domains

ACM Reference Format:
Maria Francis and Thibaut Verron. 2021. On Two Signature Variants Of Buchberger's Algorithm Over Principal Ideal Domains. In . ACM, New York, NY, USA, 8 pages. https://doi.org/XX.XXX/XXXXXX.XXXXXX

1 INTRODUCTION

Gröbner bases over fields, introduced by Buchberger [4], is a fundamental tool in computational ideal theory and algebraic geometry. Very early on, several approaches were proposed to extend the algorithmic theory of Gröbner bases to polynomial rings over rings, a summary of which can be found in [1, 2]. Ideals in polynomial rings over rings have several applications, for instance in number theory [18], or in lattice-based cryptography, where certain residue class polynomial rings over $\mathbb{Z}$ called ideal lattices have been used [11, 19].

There are two ways to define Gröbner bases (GB) over rings, namely weak and strong Gröbner bases, corresponding to two notions of reductions. Of the two, strong GB and reductions are the most similar to fields and the ones we consider in this work. It allows to efficiently compute the normal form of an element; over principal ideal domains (PID's), all ideals admit a strong GB. Different algorithms have been proposed for computing strong bases over PID's [20, 22] and over Euclidean domains [7, 8, 16, 17].

Buchberger's original algorithm for computing Gröbner bases over fields proceeds by computing and reducing S-polynomials. Over rings, the computation of Gröbner bases additionally requires to compute so-called G-polynomials, namely combinations of polynomials which use Bézout coefficients to make the leading coefficient as small as possible. Kandri-Rody and Kapur's algorithm [16] was designed for Euclidean domains but works without any modification over PIDs; it proceeds by computing, for each pair of elements, both their S- and G-polynomials, and adding them to the queue for later processing. Pan's algorithm [22] for PIDs, later refined by Lichtblau [17] for Euclidean domains, observes that for each pair, only one polynomial, S- or G-, is required.

Over fields, it was rapidly noticed that many of the reductions in Buchberger's algorithm are useless, *i.e.*, they eventually reach 0 and are discarded. Optimizations of Buchberger's algorithm that started with Buchberger [5] have focused on how to detect these useless reductions beforehand [21]. A breakthrough came in the early 2000s with the class of so-called signature-based algorithms such as F5 [10] and later GVW [14]. A comprehensive survey of signature-based algorithms can be found in [6]. These algorithms keep track of, for each computed polynomial, its signature, namely the leading term of a representation of the polynomial in terms of the generators of the ideal. This information can be used to detect reductions to 0, and avoid redundant computations.

Furthermore, the computation of a Gröbner basis with signatures allows to recover the coefficients of the elements of the basis in terms of the generators, and to compute the module of syzygies of those generators, without the extra cost of module computations or additional variables [14].

The natural next step is to see whether these signature-based techniques can be generalized to Gröbner basis algorithms over rings. In this direction, a hybrid algorithm was presented in [7] that added signatures to a modified version of Kandri-Rody and Kapur's algorithm. The authors showed with a counter-example that implementing *totally ordered* signatures for rings cannot ensure that the signatures will never decrease/drop during the course of computing the strong GB, which is the key invariant of most

T. Verron was supported by the Austrian FWF grant P31571-N32.

Conference'21, July 2021, Washington, DC, USA

ACM ISBN XXXXXXXXXXXXXXXXXX…$15.00
https://doi.org/XX.XXX/XXXXXX.XXXXXX

signature-based algorithms. The signature-based techniques of [7] could however be used as an efficient preprocessing step to fasten the computations, falling back to the classical techniques when a drop in signature is detected.

In [12], the authors described a theoretical algorithm that computes a weak Gröbner basis with signatures, over PID's, without any signature drop, by using a partial order on the signatures. In this work, we use similar constructions to adapt Kandri-Rody and Kapur's algorithm and Pan/Lichtblau's algorithm to the computation of signature Gröbner bases. For that purpose, we need two constructions: a restriction on the construction of G-polynomials ensuring that we can keep track of their signatures without discarding any; and an analogous construction using Bézout coefficients to obtain elements with small signatures. In the case of Kandri-Rody and Kapur's algorithm, we prove that the powerful cover criterion described in [13] can be applied to eliminate some S-polynomials. In the case of Pan/Lichtblau's algorithm, the nature of the pairs being computed forces us to relax the restrictions on S-polynomials, and limits the scope of the criteria. In both cases, we prove that the algorithms are correct and compute both a signature-Gröbner basis of the ideal, and a basis of the signatures of its syzygies.

We have implemented both algorithms in the computer algebra system Magma [3], with additional optimizations and criteria, and observe that the relaxed restrictions in Pan/Lichtblau tend to lead to the computation of more pairs. We also compare the time taken for computing the signature Gröbner basis and using it to recover information on the module, with Magma implementations of *ad-hoc* functions for that purpose, and show that using signatures allows for a significant speed-up of those operations.

2 NOTATIONS AND PRELIMINARIES

2.1 Conventions and notations

Let $\mathbb{N}$ be the set of all non-negative integers. Let R be a principal ideal domain (PID) that has a unit element and is commutative. We assume that R is effective in the sense that one can perform all the arithmetic operations in R, obtain the gcd of elements and compute Bézout coefficients. A typical example of such a ring is the ring of integers $\mathbb{Z}$, with Euclid's algorithm and the extended Euclid's algorithm.

Let $A = R[x_1, \dots, x_{n_{\text{vars}}}]$ be the polynomial ring in n_{vars} indeterminates $x_1, \dots, x_{n_{\text{vars}}}$ over R. A monomial in A is an element of the form $x_1^{a_1} \dots x_{n_{\text{vars}}}^{a_{n_{\text{vars}}}}$ where $a = (a_1, \dots, a_{n_{\text{vars}}}) \in \mathbb{N}^{n_{\text{vars}}}$. A term in A is $a\mu$, where $a \in R \setminus \{0\}$ and μ is a monomial. The set of terms (resp. monomials) of A is denoted by $\operatorname{Ter}(A)$ (resp. $\operatorname{Mon}(A)$).

A monomial order is an order on $\operatorname{Mon}(A)$ which is compatible with multiplication and well-founded. In the rest of the paper, we assume that A is endowed with an implicit monomial order $<$, and we define as usual the leading monomial lm, the leading term lt and the leading coefficient lc of a given polynomial. By convention, we set $\operatorname{lm}(0) = \operatorname{lt}(0) = \operatorname{lc}(0) = 0$.

Given a pair of polynomials (f, g), we denote $\operatorname{lcmlm}(f, g)$ (resp. $\operatorname{lcmlt}(f, g)$) the least common multiple of the leading monomials (resp. leading terms) of f and g.

Given a set of polynomials $f_1, \dots, f_{n_{\text{polys}}}$ in A, we consider the free module $\mathbf{M} = A^{n_{\text{polys}}}$ with basis $\mathbf{e}_1, \dots, \mathbf{e}_{n_{\text{polys}}}$. For $\alpha \in \mathbf{M}$ with $\alpha = (\alpha_1, \dots, \alpha_{n_{\text{polys}}})$, we define $\overline{\alpha} = \sum \alpha_i f_i$. We define the module

$$\mathcal{I} = \{(\alpha, \overline{\alpha}) : \alpha \in \mathbf{M}\} \subset A^{n_{\text{polys}}+1}.$$

The module $\mathcal{I}$ is isomorphic to $\mathbf{M}$, and in particular it is free with basis $(\mathbf{e}_1, f_1), \dots, (\mathbf{e}_{n_{\text{polys}}}, f_{n_{\text{polys}}})$. The image of the projection of $\mathcal{I}$ onto the last coordinate is the ideal, $\langle f_1, \dots, f_{n_{\text{polys}}} \rangle$.

A syzygy of $\mathcal{I}$ is an element $\mathbf{z} = (\alpha, \overline{\alpha})$ such that $\overline{\alpha} = 0$. The set of all syzygies of $\mathcal{I}$ is denoted by $\operatorname{Syz}(\mathcal{I})$, it is an A-module.

A monomial of $\mathbf{M}$ is an element of the form $\mu\mathbf{e}_i$, with $\mu \in \operatorname{Mon}(A)$ and $i \in [\![1, n_{\text{polys}}]\!]$. A term of $\mathbf{M}$ is an element of the form $c\mathbf{m}$ where $c \in R$ and $\mathbf{m}$ is a monomial of $\mathbf{M}$. As before, the set of terms (resp. monomials) of $\mathbf{M}$ is denoted by $\operatorname{Ter}(\mathbf{M})$ (resp. $\operatorname{Mon}(\mathbf{M})$).

A monomial ordering on $\mathbf{M}$ is an ordering $\prec$ on $\operatorname{Mon}(\mathbf{M})$ with

(1) if $\mathbf{m} \prec \mathbf{n}$, then $\mu\mathbf{m} \prec \mu\mathbf{n}$;
(2) if $\mu < \nu$, then $\mu\mathbf{m} \prec \nu\mathbf{m}$.

Examples of orderings on $\mathbf{M}$ are the *position over term* (or PoT) ordering, defined as $\mu\mathbf{e}_i \prec_{\text{PoT}} \nu\mathbf{e}_j$ if $i < j$, or $i = j$ and $\mu < \nu$, and the *term over position* (or ToP) ordering, defined as $\mu\mathbf{e}_i \prec_{\text{ToP}} \nu\mathbf{e}_j$ if $\mu < \nu$, or $\mu = \nu$ and $i < j$.

As in the case of polynomials, a monomial ordering on $\mathbf{M}$ can be extended into a partial term ordering. Let $\mathbf{s} = a\mu\mathbf{e}_i$ and $\mathbf{t} = b\nu\mathbf{e}_j \in \operatorname{Ter}(\mathbf{M})$, we write $\mathbf{s} \simeq \mathbf{t}$ if $\mathbf{s}$ and $\mathbf{t}$ are incomparable, that is, if $\mu = \nu$ and $i = j$. We write $\mathbf{s} = \mathbf{t}$ if $a = b$, $\mu = \nu$ and $i = j$.

We say that $\mathbf{s} \preceq \mathbf{t}$ if $\mathbf{s} \prec \mathbf{t}$ or $\mathbf{s} \simeq \mathbf{t}$, and similarly, $\mathbf{s} \precneqq \mathbf{t}$ implies that $\mathbf{s} \neq \mathbf{t}$. It is harmless because $\simeq$ is an equivalence relation and $\prec$ is a total order on the quotient, so, for example, if $\mathbf{s} \simeq \mathbf{t}$ and $\mathbf{s} \prec \mathbf{u}$, then $\mathbf{t} \prec \mathbf{u}$.

Given an element $\mathbf{p} = (\alpha, \overline{\alpha}) \in \mathcal{I}$, we define the leading term lt, leading monomial lm and leading coefficient lc of $\mathbf{p}$ to be those of $\overline{\alpha}$. The *signature* of $\mathbf{p}$ is the leading term of the module element α for the module monomial ordering $\prec$, *i.e.*, the largest module term appearing in α, and it is denoted as $\operatorname{sig}(\mathbf{p})$.

2.2 Signature Gröbner bases

In this section, we introduce generalizations to rings of constructions used in signature Gröbner bases over fields. These constructions extend those introduced in [12].

The key idea, as in the case of fields, is that for each element $\mathbf{f} = (\alpha, \overline{\alpha})$, we need only keep track of $\operatorname{sig}(\mathbf{f}) = \operatorname{lt}(\alpha)$ and $\overline{\alpha}$, instead of the full module representation α. For that purpose, we restrict to operations which do not cancel the signatures.

Definition 2.1. *Let* $\mathbf{f}, \mathbf{g} \in \mathcal{I}$. *The sum* $\mathbf{f} + \mathbf{g}$ *is called* regular *if* $\operatorname{sig}(\mathbf{f}) \not\simeq \operatorname{sig}(\mathbf{g})$, *and* singular *if* $\operatorname{sig}(\mathbf{f}) = -\operatorname{sig}(\mathbf{g})$.

The nature of the operation yields information about the signature of the result, as follows.

Proposition 2.2. *Let* $\mathbf{f} = (\alpha, \overline{\alpha})$ *and* $\mathbf{g} = (\beta, \overline{\beta}) \in \mathcal{I}$, *let* $\mathbf{h} = (\gamma, \overline{\gamma}) = \mathbf{f} + \mathbf{g}$. *Then,*

- $\mathbf{f} + \mathbf{g}$ *is a regular addition iff* $\operatorname{sig}(\mathbf{h}) = \max(\operatorname{sig}(\mathbf{f}), \operatorname{sig}(\mathbf{g}))$*;*
- $\mathbf{f} + \mathbf{g}$ *is a non-singular addition iff* $\operatorname{sig}(\mathbf{h}) = \operatorname{sig}(\mathbf{f}) + \operatorname{sig}(\mathbf{g}) \simeq \operatorname{sig}(\mathbf{f}) \simeq \operatorname{sig}(\mathbf{g})$*;*
- $\mathbf{f} + \mathbf{g}$ *is a singular addition iff* $\operatorname{sig}(\mathbf{h}) \precneqq \operatorname{sig}(\mathbf{f}) \simeq \operatorname{sig}(\mathbf{g})$.

The proof of the proposition is straightforward. Note that in a singular addition, the signature of the result cannot be computed from the signatures of the summands. This phenomenon is called a *signature drop*, and signature-based algorithms must disallow signature drops, and thus singular operations, in order to keep track of the signatures.

Signature Gröbner bases, as in the case of fields, are characterized by the fact that all elements of the ideal are s-reducible, namely, reducible without increasing the signature. In the case of rings, different notions of reduction exist, namely weak and strong reductions, as well as modular reductions by the coefficients. In this paper, we only consider strong reductions, which require that the leading coefficient of the reducer divides that of the reducee. Those reductions allow to define strong Gröbner bases. In the rest of the paper, we shall omit the "strong" qualificative.

Definition 2.3. *Let $\mathcal{G} \subset \mathcal{I}$ and $\mathbf{f}, \mathbf{h} \in \mathcal{I}$.*

We say that $\mathbf{f}$ (strongly) s-reduces *to* $\mathbf{h}$ *modulo* $\mathcal{G}$ *if there exists* $\mathbf{g}_i \in \mathcal{G}$ *and* $t_i \in \mathrm{Ter}(A)$ *such that*

(1) $\mathrm{lt}(\mathbf{f}) = t_i \mathrm{lt}(\mathbf{g}_i)$
(2) $\mathbf{h} = \mathbf{f} - t_i \mathbf{g}_i$
(3) $t_i \mathrm{sig}(\mathbf{g}_i) \leq \mathrm{sig}(\mathbf{f})$

If the signature inequality is strict, $t_i \mathrm{sig}(\mathbf{g}_i) \lneq \mathrm{sig}(\mathbf{f})$*, it is called a* regular s*-reduction, and if* $t_i \mathrm{sig}(\mathbf{g}_i) = \mathrm{sig}(\mathbf{f})$*, it is called a* singular s*-reduction.*

By abuse of language, we extend these definitions to sequences of reductions. We say that $\mathbf{f}$ *s-reduces (resp. regular s-reduces) to zero if there exists a sequence of s-reductions (resp. regular s-reductions) whose final result has polynomial part equal to 0.*

Remark 2.4. *If* $\mathbf{f}$ s*-reduces to* $\mathbf{h}$ *modulo* $\mathcal{G}$*, then* $\mathrm{sig}(\mathbf{h}) \leq \mathrm{sig}(\mathbf{g})$*, with equality iff the reduction is regular and strict inequality iff the reduction is singular. Note that an s-reduction might be neither regular nor singular, in which case* $\mathrm{sig}(\mathbf{h}) \simeq \mathrm{sig}(\mathbf{f})$*.*

We then recall the definition of (strong) signature Gröbner bases.[1]

Definition 2.5. *Let $\mathcal{G} \subset \mathcal{I}$ and $\mathbf{T} \in \mathrm{Ter}(\mathbf{M})$. $\mathcal{G}$ is called a (strong) signature Gröbner basis (or Sig-GB for short) up to signature $\mathbf{T}$ if every $\mathbf{f} \in \mathcal{I}$ with $\mathrm{sig}(\mathbf{f}) \lneq \mathbf{T}$ is s-reducible modulo $\mathcal{G}$. $\mathcal{G}$ is called a signature Gröbner basis if it is a signature Gröbner basis up to $\mathbf{T}$ for all $\mathbf{T}$.*

The original motivation for the use of signatures is to maintain a list of signatures of known syzygies, and use it to predict reductions to zero. Additionally, the last coordinates of elements of a Sig-GB form a GB in the classical sense. The proof of that fact [6, Lem. 4.6] can be directly extended to rings. So signature-based algorithms allow to compute classical Gröbner bases in a more efficient way.

This use of syzygies applies to our case as well, and requires to define reductions by signatures of syzygies.

Definition 2.6. *Let $\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ and let $\mathbf{f} \in \mathcal{I}$, with $\mathrm{sig}(\mathbf{f}) = a\mu\mathbf{e}_i$, for $a \in R$ and $\mu \in \mathrm{Mon}(A)$. We say that $\mathbf{f}$ is* sig-reducible *modulo $\mathcal{G}_z$ if there exists $\mathbf{z} \in \mathcal{G}_z$ such that $\mathrm{sig}(\mathbf{z})$ divides $\mathrm{sig}(\mathbf{f})$.*

Let $\mathbf{T} \in \mathrm{Mon}(\mathbf{M})$, we say that $\mathcal{G}_z$ is a Sig-basis of syzygies (resp. basis up to $\mathbf{T}$) if any syzygy of $\mathcal{I}$ (resp. syzygy with signature $\lneq \mathbf{T}$) is sig-reducible by $\mathcal{G}_z$.

Proposition 2.7. *Let $\mathcal{G}$ be a Sig-GB up to signature $\mathbf{T}$, $\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ and $\mathbf{f} \in \mathcal{I}$ with $\mathrm{sig}(\mathbf{f}) \leq \mathbf{T}$. If $\mathbf{f}$ is sig-reducible modulo $\mathcal{G}_z$, then $\mathbf{f}$ regular s-reduces to 0 modulo $\mathcal{G}$.*

Proof. Let $\mathbf{z} \in \mathcal{G}_z$ be such that there exists $t \in \mathrm{Ter}(A)$ with $t\mathrm{sig}(\mathbf{z}) = \mathrm{sig}(\mathbf{f})$. Let $\mathbf{g} = \mathbf{f} - t\mathbf{z}$, it has signature $\lneq \mathbf{T}$ so it s-reduces to 0, and since its lt is equal to that of $\mathbf{f}$, $\mathbf{f}$ regular reduces to 0. □

In the classical case, without signatures, it is sometimes convenient to consider expanded sequences of reductions, leading to the notion of standard representation. With signatures, it turns out that a natural generalization of that notion encompasses both s-reductions and sig-reductions.

Definition 2.8. *Let $\mathcal{G} = \{\mathbf{g}_1, \dots, \mathbf{g}_r\} \subset \mathcal{I}$, $\mathcal{G}_z = \{\mathbf{z}_1, \dots, \mathbf{z}_s\} \subset \mathrm{Syz}(\mathcal{I})$ and $\mathbf{h} \in \mathcal{I}$. Let $t_u^{(1)} \in \mathrm{Ter}(A)$, $i_u \in [\![1, r]\!]$, where $u \in [\![1, k]\!]$ and $k \in \mathbb{N}$, $t_v^{(2)} \in \mathrm{Ter}(A)$, $j_v \in [\![1, s]\!]$, where $v \in [\![1, l]\!]$ and $l \in \mathbb{N}$, be such that the equality*

$$\mathbf{h} = \textstyle\sum_{u=1}^{k} t_u^{(1)} \mathbf{g}_{i_u} + \sum_{v=1}^{l} t_v^{(2)} \mathbf{z}_{j_v} \qquad (1)$$

holds in $\mathcal{I}$, with

(1) $\mathrm{lt}(t_1^{(1)} \mathbf{g}_{i_1}) > \mathrm{lt}(t_2^{(1)} \mathbf{g}_{i_2}) \geq \mathrm{lt}(t_3^{(1)} \mathbf{g}_{i_3}) \geq \cdots \geq \mathrm{lt}(t_k^{(1)} \mathbf{g}_{i_k})$*;*
(2) for all $u \in [\![1, k]\!]$, $\mathrm{sig}(t_u^{(1)} \mathbf{g}_{i_u}) \leq \mathrm{sig}(\mathbf{h})$*;*
(3) $\mathrm{sig}(t_1^{(2)} \mathbf{z}_{j_1}) \gneq \mathrm{sig}(t_2^{(2)} \mathbf{z}_{j_2}) \geq \mathrm{sig}(t_3^{(2)} \mathbf{z}_{j_3}) \geq \ldots \geq \mathrm{sig}(t_l^{(2)} \mathbf{z}_{j_l})$*;*
(4) for all $v \in [\![1, l]\!]$, $\mathrm{sig}(t_v^{(2)} \mathbf{z}_{j_v}) \leq \mathrm{sig}(\mathbf{h})$.

If such a decomposition exists, we say that (1) *is a* standard Sig-representation *of* $\mathbf{h}$ *with respect to* $(\mathcal{G}, \mathcal{G}_z)$*.*

Proposition 2.9. *Let $\mathcal{G} \subset \mathcal{I}$, $\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ such that every element of $\mathcal{I}$ admits a standard Sig-representation by $(\mathcal{G}, \mathcal{G}_z)$. Then $\mathcal{G}$ is a Sig-GB and $\mathcal{G}_z$ is a Sig-basis of syzygies.*

Proof. Let $\mathbf{h} \in \mathcal{I}$. By assumption it admits a standard Sig-representation as in (1). If $\mathbf{h}$ is not a syzygy, then by property 1 on the leading terms, $\mathrm{lt}(\mathbf{h}) = t_1^{(1)} \mathrm{lt}(\mathbf{g}_{i_1})$, and by property 2 on the signatures, this is an s-reduction of $\mathbf{h}$. If $\mathbf{h}$ is a syzygy, then again by the property on the leading terms, $k = 0$, and properties 3 and 4 on the signatures imply that $\mathbf{h}$ is sig-reducible by $\mathbf{z}_{j_1}$. □

We recall how S-polynomials are defined with signatures. First, we give some definitions associated with pairs of module elements.

Definition 2.10. *Let $\mathbf{f}, \mathbf{g} \in \mathcal{I}$, $t_{\mathbf{f}} = \frac{\mathrm{lcmlt}(\mathbf{f},\mathbf{g})}{\mathrm{lt}(\mathbf{f})}$, $t_{\mathbf{g}} = \frac{\mathrm{lcmlt}(\mathbf{f},\mathbf{g})}{\mathrm{lt}(\mathbf{g})}$.*

The term degree of the pair $(\mathbf{f}, \mathbf{g})$ is $\mathrm{tdeg}(\mathbf{f}, \mathbf{g}) = \mathrm{lcmlt}(\mathbf{f}, \mathbf{g}) = t_{\mathbf{f}} \mathrm{lt}(\mathbf{f}) = t_{\mathbf{g}} \mathrm{lt}(\mathbf{g})$. The monomial degree $\mathrm{mdeg}(\mathbf{f}, \mathbf{g})$ of the pair $(\mathbf{f}, \mathbf{g})$ is the monomial part of the term degree.

The pair $(\mathbf{f}, \mathbf{g})$ is called regular if $t_{\mathbf{f}} \mathrm{sig}(\mathbf{f}) \not\simeq t_{\mathbf{g}} \mathrm{sig}(\mathbf{g})$ and it is called singular if $t_{\mathbf{f}} \mathrm{sig}(\mathbf{f}) + t_{\mathbf{g}} \mathrm{sig}(\mathbf{g}) = 0$. The signature of the pair $(\mathbf{f}, \mathbf{g})$ is $\mathrm{sig}(\mathbf{f}, \mathbf{g}) = \max(t_{\mathbf{f}} \mathrm{sig}(\mathbf{f}), -t_{\mathbf{g}} \mathrm{sig}(\mathbf{g}))$.

Definition 2.11. *Let $\mathbf{f}$ and $\mathbf{g} \in \mathcal{I}$. The S-polynomial of $\mathbf{f}$ and $\mathbf{g}$ is*

$$\text{S-Pol}(\mathbf{f}, \mathbf{g}) = \frac{\mathrm{lcmlt}(\mathbf{f}, \mathbf{g})}{\mathrm{lt}(\mathbf{f})} \mathbf{f} - \frac{\mathrm{lcmlt}(\mathbf{f}, \mathbf{g})}{\mathrm{lt}(\mathbf{g})} \mathbf{g}.$$

Remark 2.12. *Let $\mathbf{h} = \text{S-Pol}(\mathbf{f}, \mathbf{g})$. Then $\mathrm{sig}(\mathbf{h}) \leq \mathrm{sig}(\mathbf{f}, \mathbf{g})$, with equality iff the pair $(\mathbf{f}, \mathbf{g})$ is regular, and strict inequality iff it is singular.*

In order to ensure that elements are strongly s-reducible modulo $\mathcal{G}$, we need to compute G-polynomials[2]. The G-polynomial of f_1

[1] In [14], a signature GB is called a strong GB. We use Sig-GB here to avoid conflict with the existing notion of strong GB over rings.

[2] Terminology and notations vary: this construction is called T-polynomial in [20], *SL* in [22], CP2 critical pairs in [16], S-polynomial of type 1 in [17], G-polynomial in [2] and GCD-polynomial in [7, 8].

and f_2 is a polynomial f such that any linear combination of f_1 and f_2 not cancelling the leading terms is reducible by f. It is defined by using Bézout relations to make the leading coefficient as small as possible.

Definition 2.13. *Let* $\mathbf{f}$ *and* $\mathbf{g} \in \mathcal{I}$. *Let* u, v *be Bézout coefficients of* $\mathrm{lc}(\mathbf{f})$ *and* $\mathrm{lc}(\mathbf{g})$*, that is,* $u\mathrm{lc}(\mathbf{f}) + v\mathrm{lc}(\mathbf{g}) = \gcd(\mathrm{lc}(\mathbf{f}), \mathrm{lc}(\mathbf{g}))$. *The G-polynomial of* $\mathbf{f}$ *and* $\mathbf{g}$ *associated to* (u, v) *is defined as*

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

The coefficients u and v are not uniquely determined, and we can use this fact to ensure that G-polynomials *never* represent a singular operation.

Proposition 2.14. *Let* $\mathbf{f}$ *and* $\mathbf{g} \in \mathcal{I}$. *Then there exists* u, v *such that* $\mathrm{sig}(\text{G-Pol}_{u,v}(\mathbf{f}, \mathbf{g})) \simeq \mathrm{sig}(\mathbf{f}, \mathbf{g})$.

Proof. If the pair is regular, there is nothing to prove, and any pair of Bézout coefficients works. Otherwise, let $a = \mathrm{lc}(\mathbf{f})$, $b = \mathrm{lc}(\mathbf{g})$, $c = \mathrm{lc}(\mathrm{sig}(\mathbf{f}))$, $d = \mathrm{lc}(\mathrm{sig}(\mathbf{g}))$, and $g = \gcd(a, b)$. We want to prove that there exists u, v such that $au + bv = g$ and $cu + dv \neq 0$. If $ad - bc = 0$, $a(cu + dv) = c(au + bv) \neq 0$, so again any pair of Bézout coefficients works. Otherwise, assume that $au + bv = 0$, $cu + dv = 0$, and consider the pair $u' = u + b$, $v' = v - a$. Then $au' + bv' = g$ and $cu' + dv' = bc - ad \neq 0$. □

Remark 2.15. *With the notations of the proof,* $\text{G-Pol}_{u',v'}(\mathbf{f}, \mathbf{g}) = \text{G-Pol}_{u,v}(\mathbf{f}, \mathbf{g}) - \text{S-Pol}(\mathbf{f}, \mathbf{g})$.

In practice, we shall always consider such a pair of Bézout coefficients, and call the corresponding G-polynomial *the* G-polynomial of $\mathbf{f}$ and $\mathbf{g}$, denoted by $\text{G-Pol}(\mathbf{f}, \mathbf{g})$. Note that $\mathrm{sig}(\text{G-Pol}(\mathbf{f}, \mathbf{g})) \simeq \mathrm{sig}(\mathbf{f}, \mathbf{g})$ and $\mathrm{lm}(\text{G-Pol}(\mathbf{f}, \mathbf{g})) = \mathrm{mdeg}(\mathbf{f}, \mathbf{g})$.

Definition 2.16. *Let* $\mathcal{G} \subset \mathcal{I}$. *We say that* $\mathcal{G}$ *is* complete *if every G-polynomial of elements of* $\mathcal{G}$ *is s-reducible modulo* $\mathcal{G}$.

It is always possible to make $\mathcal{G}$ complete by adding G-polynomials to $\mathcal{G}$ until the property holds. We use a similar process, but on the signatures, to create syzygies with small signature coefficients.

Definition 2.17. *Let* $\mathbf{z}_1, \mathbf{z}_2 \in \mathrm{Syz}(\mathcal{I})$ *with respective signatures* $a_k\mu_k\mathbf{e}_i$, $k = 1, 2$, *sharing the same index* i. *Let* $d = \gcd(a_1, a_2)$, *and let* u_1, u_2 *be Bézout coefficients. Let* $\mu = \mathrm{lcm}(\mu_1, \mu_2)$. *The* sigG-combination *of* $\mathbf{z}_1$ *and* $\mathbf{z}_2$ *is defined as*

$$\text{sigG-Comb}(\mathbf{z}_1, \mathbf{z}_2) = u_1\frac{\mu}{\mu_1}\mathbf{z}_1 + u_2\frac{\mu}{\mu_2}\mathbf{z}_2,$$

and its signature is $d\mu\mathbf{e}_i$. *Note that contrary to the case of polynomials, the result does not depend on the choice of* u_1 *and* u_2.

Let $\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$, *we say that* $\mathcal{G}_z$ *is* sigG-complete *if any* sigG-combination $\mathbf{z}$ *of elements of* $\mathcal{G}_z$ *is sig-reducible by* $\mathcal{G}_z$.

We conclude this section with a few definitions which will give useful criteria to prove the correctness and for detecting useless syzygies in Algorithm 1 given below. These constructions are adapted from the ones defined for the GVW algorithm over fields [13]. The first definition is that of super reducible elements[3].

Definition 2.18. *Let* $\mathcal{G} \subset \mathcal{I}$, *and* $\mathbf{f} \in \mathcal{I}$. $\mathbf{f}$ *is* super reducible *by* $\mathcal{G}$ *if there exists* $\mathbf{g} \in \mathcal{G}$ *and* $t \in \mathrm{Ter}(A)$ *such that* $\mathrm{sig}(\mathbf{f}) = t\mathrm{sig}(\mathbf{g})$ *and* $\mathrm{lm}(t\mathbf{g}) = \mathrm{lm}(\mathbf{f})$.

Note that unlike in the case of fields, we do not require that a super reduction is a reduction. However, under some hypotheses, an element which is super reducible is necessarily s-reducible.

Proposition 2.19. *Let* $\mathcal{G} \subset \mathcal{I}$ *be complete, and let* $\mathbf{f} \in \mathcal{I}$. *If* $\mathbf{f}$ *is super reducible by* $\mathcal{G}$*, then* $\mathbf{f}$ *is* s*-reducible by* $\mathcal{G}$.

Proof. Assume for a contradiction that $\mathbf{f}$ is super reducible by $\mathcal{G}$, not s-reducible, and has minimal signature for this property. Let $\mathbf{g}_1$ be such that there exists $t_1 \in \mathrm{Ter}(A)$ with $\mathrm{sig}(\mathbf{f}) = t_1\mathrm{sig}(\mathbf{g}_1)$ and $\mathrm{lm}(t_1\mathbf{g}_1) = \mathrm{lm}(\mathbf{f})$. If $\mathrm{lt}(t_1\mathbf{g}_1) = \mathrm{lt}(\mathbf{f})$, then $\mathbf{g}_1$ is a s-reducer of $\mathbf{f}$.

Otherwise, $\mathrm{lm}(\mathbf{f} - t_1\mathbf{g}_1) = \mathrm{lm}(\mathbf{f})$. Since $\mathrm{sig}(\mathbf{f} - t_1\mathbf{g}) \lnsim \mathrm{sig}(\mathbf{f})$, by minimality of $\mathrm{sig}(\mathbf{f})$, $\mathbf{f} - t_1\mathbf{g}$ is s-reducible modulo $\mathcal{G}$. Let $\mathbf{g}_2$ be such a reducer, with $\mathrm{lt}(\mathbf{f} - t_1\mathbf{g}_1) = t_2\mathbf{g}_2$, and so $\mathrm{lt}(\mathbf{f}) = t_1\mathrm{lt}(\mathbf{g}_1) + t_2\mathrm{lt}(\mathbf{g}_2)$. The signature satisfies $t_2\mathrm{sig}(\mathbf{g}_2) \preceq \mathrm{sig}(\mathbf{f} - t_1\mathbf{g}_1) \lnsim \mathrm{sig}(t_1\mathbf{g}_1)$. Let $\mathbf{g}_3 = \text{G-Pol}(\mathbf{g}_1, \mathbf{g}_2)$, by definition of the G-pol there exists $t_3 \in \mathrm{Ter}(A)$ such that $t_3\mathrm{lt}(\mathbf{g}_3) = \mathrm{lt}(\mathbf{f})$, and $t_3\mathrm{sig}(\mathbf{g}_3) \simeq t_1\mathrm{sig}(\mathbf{g}_1) \simeq \mathrm{sig}(\mathbf{f})$. By hypothesis $\mathbf{g}_3$ is s-reducible by $\mathcal{G}$, and a s-reducer of $\mathbf{g}_3$ is a s-reducer of $\mathbf{f}$. □

The last definition is that of the covered property.

Definition 2.20. *Let* $(\mathbf{f}_1, \mathbf{f}_2) \in \mathcal{I}^2$ *be a pair. Let* $\mathcal{G} \subset \mathcal{I}$ *and* $\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$. *The pair* $(\mathbf{f}_1, \mathbf{f}_2)$ *is* covered by $(\mathcal{G}, \mathcal{G}_z)$ *if there exists* $\mathbf{g} \in \mathcal{G}$, $\mathbf{z} \in \mathcal{G}_z$, $t, t^{(z)} \in \mathrm{Ter}(A)$ *such that*

- *if* $t \neq 0$, $\mathrm{sig}(\mathbf{f}, \mathbf{g}) \simeq t\mathrm{sig}(\mathbf{g})$;
- *if* $t^{(z)} \neq 0$, $\mathrm{sig}(\mathbf{f}, \mathbf{g}) \simeq t^{(z)}\mathrm{sig}(\mathbf{z})$;
- $\mathrm{sig}(\mathbf{f}, \mathbf{g}) = t\mathrm{sig}(\mathbf{g}) + t^{(z)}\mathrm{sig}(\mathbf{z})$;
- $\mathrm{lm}(t\mathbf{g}) < \mathrm{mdeg}(\mathbf{f}, \mathbf{g})$.

This cover criterion looks more complicated to implement than in the case of fields, due to the need to consider linear combinations. However, one can use sigG-combinations of elements of $\mathcal{G}$ and elements of $\mathcal{G}_z$ to compute elements with signature as small as possible and same leading monomial, and reduce the cover test to a single divisibility test.

3 ADDING SIGNATURES TO KANDRI-RODY AND KAPUR'S ALGORITHM

3.1 Description of the algorithm

The first algorithm which we present in this paper is a signature-enabled version of Kandry-Rody and Kapur's algorithm. The algorithm works similarly to Buchberger's algorithm, but adds both S- and G-polynomials to the basis. The signature variant follows the construction of the GVW algorithm [13, 14].

The correctness of the algorithm is stated by the following theorem (proved in Section 3.2), and adapted from [14, Thm. 2.4].

Theorem 3.1. *Let* $\mathcal{G} \subset \mathcal{I}$ *complete ,* $\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ sigG*-complete, such that for all signatures* $\mathbf{T}$*, there exists some* $\mathbf{g} \in \mathcal{G} \cup \mathcal{G}_z$ *such that* $\mathrm{sig}(\mathbf{g})$ *divides* $\mathbf{T}$. *Assume that every regular pair of elements of* $\mathcal{G}$ *is covered by* $(\mathcal{G}, \mathcal{G}_z)$. *Then,* $\mathcal{G}$ *is a Sig-Gröbner basis and* $\mathcal{G}_z$ *is a Sig-basis of syzygies.*

The algorithm ensures that all the assumptions of the theorem hold:

[3] In the paper [12], the notion was called 1-singular reducible.

- $\mathcal{G}$ is complete and $\mathcal{G}_z$ is sigG-complete because G-polynomials are added to the queue of pairs to be reduced for addition into $\mathcal{G}$, and sigG-combinations to $\mathcal{G}_z$;
- there exists, for all $\mathbf{T}$, a $\mathbf{g}$ with $\mathrm{sig}(\mathbf{g})$ dividing $\mathrm{sig}(\mathbf{T})$, because we process all elements $(\mathbf{e}_i, f_i)$, thus ensuring that there is an element with signature $\mathbf{e}_i$ in either $\mathcal{G}$ or $\mathcal{G}_z$ for all i;
- every regular pair is covered by $(\mathcal{G}, \mathcal{G}_z)$ because, for each regular pair, we compute the corresponding S-polynomial, reduce it and add the result to the basis, thus creating a covering element for the pair.

The resulting algorithm is described in Algorithm 1. Note that for each element $\mathbf{f} = (\alpha, \overline{\alpha}) \in \mathcal{I}$, we only keep track of $\mathrm{sig}(\mathbf{f}) = \mathrm{lt}(\alpha)$ and $\overline{\alpha}$. The routines SigReduce and RegularReduce compute the sig-reduction of a signature by a basis of syzygies (the result being either 0 or the signature itself), and the regular reduction of an element of $\mathcal{I}$ by a Sig-GB, respectively.

A technical point is that the theorem allows to eliminate S-polynomials obtained from a pair which is covered, but not necessarily G-polynomials. This requires to keep track of how each element was computed. In the pseudo-code algorithm, we do it by keeping for each new element its so-called type, which can take three values: N, indicating a polynomial from the input; $\mathrm{S}(i, j)$, indicating the S-polynomial of $\mathbf{g}_i$ and $\mathbf{g}_j$; and $\mathrm{G}(i, j)$, indicating the G-polynomial of $\mathbf{g}_i$ and $\mathbf{g}_j$.

On top of that, we add some tests to eliminate some G-polynomials. Firstly, if $\mathrm{lc}(\mathbf{g}_i)$ divides $\mathrm{lc}(\mathbf{g}_j)$, then one can choose the Bézout coefficients such that $\text{G-Pol}(\mathbf{g}_i, \mathbf{g}_j)$ is a multiple of $\mathbf{g}_i$, and thus it is automatically s-reducible modulo $\mathcal{G}$.

Secondly, thanks to Proposition 2.7, we know that we can immediately disregard any element whose signature is divisible by that of a syzygy. This partially extends the cover criterion to G-polys.

Thirdly, note that we cannot use Proposition 2.19 to eliminate G-polynomials which would be super reducible: indeed, that proposition requires that $\mathcal{G}$ be complete, and the G-polynomial being processed might be necessary for that. Furthermore, the G-polynomial $\text{G-Pol}(\mathbf{g}_i, \mathbf{g}_j)$ is always super reducible by at least one of $\mathbf{g}_i, \mathbf{g}_j$.

However, if $\mathbf{f} \in \mathcal{I}$ is both super reducible and s-reducible by $\mathbf{g} \in \mathcal{G}$, that is, if there exists $t \in \mathrm{Ter}(A)$ such that $t\mathrm{sig}(\mathbf{g}) = \mathrm{sig}(\mathbf{f})$ and $t\mathrm{lt}(\mathbf{g}) = \mathrm{lt}(\mathbf{f})$, then the proof of Proposition 2.19 shows that $\mathbf{f}$ is s-reducible by $\mathcal{G}$, without any hypothesis of completeness. Thus such an element can be immediately discarded.

For some signature orderings, it is also possible to predict in advance the signature of some syzygies, with the F5 criterion. This criterion can be implemented in our setting exactly as in the case of fields, for instance by adding signatures to $\mathcal{G}_z$, and we do not detail it here.

3.2 Proof

The proof of Theorem 3.1 is adapted from the proof of [14, Thm. 2.4].

Proof of Th. 3.1. We prove the implication by contradiction. Assume that there exists $\mathbf{f} \in \mathcal{I}$ such that $\mathbf{f}$ is not s-reducible modulo $\mathcal{G}$ and $\mathbf{f}$ is not sig-reducible modulo $\mathcal{G}_z$, and pick $\mathbf{f}$ with minimal signature $\mathbf{T}$ for this property. Let $\mathbf{g}_1 \in \mathcal{G}$, $\mathbf{z}_1 \in \mathcal{G}_z$, $t, t_{z_1} \in \mathrm{Ter}(A)$ such that $\mathbf{T} = t\mathrm{sig}(\mathbf{g}_1) + t_{z_1}\mathrm{sig}(\mathbf{z}_1)$ and such that $\mathrm{lm}(t\mathbf{g}_1)$ is minimal for that property. By hypothesis, such a decomposition exists (with either $t_1 = 0$ or $t_{z_1} = 0$).

First, we prove that $t\mathbf{g}_1$ is not regular s-reducible modulo $\mathcal{G}$. Indeed, if it were, let $\mathbf{g}_2$ be a regular reducer of $t\mathbf{g}_1$. Consider the pair $(\mathbf{g}_1, \mathbf{g}_2)$, let $\mu = \mathrm{lcmlm}(\mathbf{g}_1, \mathbf{g}_2)$ and let $\sigma = \mathrm{sig}(\mathbf{g}_1, \mathbf{g}_2)$. By properties of the lcm, there exist some terms t_1, t_2 such that $\mu = \mathrm{lm}(t_1\mathbf{g}_1)$, $\sigma = t_1\mathrm{sig}(\mathbf{g}_1)$, and $t_1 t_2 = t$. Furthermore, since $\mathbf{g}_2$ is a regular reducer of $t\mathbf{g}_1$, the pair $(\mathbf{g}_1, \mathbf{g}_2)$ is regular ([14, Lemma. 2.3]).

By assumption, the pair is covered by $(\mathcal{G}, \mathcal{G}_z)$, so there exists $\mathbf{g}_3 \in \mathcal{G}$, $\mathbf{z}_2 \in \mathcal{G}_z$, $t_3, t_{z_2} \in \mathrm{Ter}(A)$, such that $\sigma = t_3\mathrm{sig}(\mathbf{g}_3) + t_{z_2}\mathrm{sig}(\mathbf{z}_2)$, and $\mathrm{lm}(t_3\mathbf{g}_3) < \mu$. So all in all, $\mathbf{T} = t_2 t_3\mathrm{sig}(\mathbf{g}_3) + t_{z_1}\mathrm{sig}(\mathbf{z}_1) + t_{z_2}\mathrm{sig}(\mathbf{z}_2)$. and $\mathrm{lm}(t_2 t_3\mathbf{g}_3) < \mathrm{lm}(t_1 t_2\mathbf{g}_1) = \mathrm{lm}(t\mathbf{g}_1)$. Let $\mathbf{z}_3$ be $\text{sigG-Comb}(\mathbf{z}_1, \mathbf{z}_2)$, its signature divides the sum $t_{z_1}\mathrm{sig}(\mathbf{z}_1) + t_{z_2}\mathrm{sig}(\mathbf{z}_2)$, and thus, the existence of $(\mathbf{g}_3, \mathbf{z}_3)$ contradicts the minimality of $\mathrm{lm}(g_1)$.

So $t\mathbf{g}_1$ is not regular s-reducible modulo $\mathcal{G}$. Now we consider two distinct cases, depending on whether $\mathbf{f}$ is a syzygy or not.

If $\mathbf{f}$ is not a syzygy, $\mathrm{lm}(\mathbf{f}) \neq \mathrm{lm}(t\mathbf{g}_1)$, because otherwise $\mathbf{f}$ would be super reducible by $\mathbf{g}_1$ and thus, since $\mathcal{G}$ is complete, s-reducible by $\mathcal{G}$. Let $\mathbf{f}_1 = \mathbf{f} - t\mathbf{g}_1 - t_{z_1}\mathbf{z}_1$, so $\mathrm{sig}(\mathbf{f}_1) \lnsim \mathbf{T}$, and $\mathrm{lt}(\mathbf{f}_1) = \max(\mathrm{lt}(\mathbf{f}), t\mathrm{lt}(\mathbf{g}_1))$. Since $\mathrm{sig}(\mathbf{f}_1) \lnsim \mathbf{T}$, by minimality of $\mathbf{f}$, $\mathbf{f}_1$ s-reduces to 0 modulo $\mathcal{G}$. But since $\mathrm{lt}(\mathbf{f}_1) = \max(\mathrm{lt}(\mathbf{f}), t\mathrm{lt}(\mathbf{g}_1))$, any s-reduction of $\mathbf{f}_1$ is a regular reduction of either $\mathbf{f}$ or $t\mathbf{g}_1$, which is a contradiction.

If $\mathbf{f}$ is a syzygy, we proceed similarly, but now $\mathrm{lm}(\mathbf{f}) = 0$. So the fact that $\mathbf{f}_1$ is s-reducible implies that $t\mathbf{g}_1$ must be regular reducible, which is impossible. So $t\mathbf{g}_1 = 0$ and $\mathbf{f}$ is sig-reducible by $\mathbf{z}_1$. □

4 ADDING SIGNATURES TO PAN/LICHTBLAU'S ALGORITHM

4.1 Description of the algorithm

The second algorithm which we present is adapted from that of Lichtblau [17], which is itself adapted from that of Pan [22]. Similar to the previous algorithm, this algorithm also adds S- and G-polynomials to the basis, but it tries to limit the growth of the length of the queue by adding at most one new polynomial for each pair, either an S- or a G-polynomial, by the following construction.

Definition 4.1. *Let* $\mathbf{f}, \mathbf{g} \in \mathcal{I}$. *The SG-polynomial of* $\mathbf{f}$ *and* $\mathbf{g}$ *is defined as:*

$$\text{SG-Pol}(\mathbf{f}_1, \mathbf{f}_2) = \begin{cases} \text{S-Pol}(\mathbf{f}, \mathbf{g}) & \textit{if } \mathrm{lc}(\mathbf{f}) \mid \mathrm{lc}(\mathbf{g}) \textit{ or } \mathrm{lc}(\mathbf{g}) \mid \mathrm{lc}(\mathbf{f}) \\ \text{G-Pol}(\mathbf{f}, \mathbf{g}) & \textit{otherwise.} \end{cases}$$

Note that compared to the previous algorithm, it leads to computing fewer S-polynomials, but not fewer G-polynomials, since it is always useless to compute a G-polynomial when one of the leading coefficients divides the other. The correctness of the algorithm is ensured by the following theorem, which will be proved in Section 4.2.

Theorem 4.2. *Let* $\mathcal{G} \subset \mathcal{I}$ *complete and* $\mathcal{G}_z \subset \mathrm{Syz}(\mathcal{I})$ sigG-*complete such that*

- $\forall\, i \in [\![1, n_{\mathrm{polys}}]\!]$, $(\mathbf{e}_i, f_i)$ *has a standard Sig-rep. w.r.t.* $(\mathcal{G}, \mathcal{G}_z)$*;*
- *any non-singular SG-polynomial of elements of* $\mathcal{G}$ *has a standard Sig-representation w.r.t.* $(\mathcal{G}, \mathcal{G}_z)$*.*

Then $\mathcal{G}$ *is a Sig-Gröbner basis and* $\mathcal{G}_z$ *is a Sig-basis of syzygies.*

The reason why this construction is sufficient is that if $\mathrm{lc}(\mathbf{f})$ and $\mathrm{lc}(\mathbf{g})$ do not divide each other, then the S-polynomial of $\mathbf{f}$ and $\mathbf{g}$ can be expressed in terms of the S-polynomials of $\mathbf{f}$, $\mathbf{g}$ and

Algorithm 1: Kandri-Rody - Kapur's algo., with signatures

```
Input  : $F \subset A$
Output : $\mathcal{G} \subset \mathrm{Ter}(\mathbf{M}) \times A$ Sig-GB of $\mathcal{I}$, $\mathcal{G}_z \subset \mathrm{Ter}(\mathbf{M}) \times \{0\}$
         Sig-basis of syzygies of $\mathcal{I}$
$\mathcal{G} \leftarrow \emptyset$; $\mathcal{G}_z \leftarrow \emptyset$; $r \leftarrow 0$;
$Q \leftarrow [(\mathbf{e}_i, f_i, \mathrm{N})$ for $i \in \{1, \dots, m\}]$;
while $Q$ is not empty :
    Take and remove $(\mathbf{s}, f, \mathtt{type})$ from $Q$, with $\mathbf{s}$ minimal;
    if $\exists\, \mathrm{z} \in \mathcal{G}_z$ s.t. $\mathrm{sig}(\mathrm{z})$ divides $\mathbf{s}$ :
        pass ;                              /* Prop. 2.7 */
    elif type is $\mathrm{S}(i, j)$ and $(\mathrm{g}_i, \mathrm{g}_j)$ is covered by $(\mathcal{G}, \mathcal{G}_z)$ :
        pass ;                      /* Cover criterion */
    else:
        $g \leftarrow \mathrm{RegularReduce}((\mathbf{s}, f), \mathcal{G})$;
        if $g = 0$ :
            Add $\mathbf{s}$ to $\mathcal{G}_z$, together with sigG-combinations;
        elif $\exists\, \mathrm{g}_i \in \mathcal{G}$ s.t. $\mathrm{lt}(\mathrm{g}_i)\mathbf{s} = \mathrm{lt}(g)\mathrm{sig}(\mathrm{g}_i)$ :
            pass ;        /* Super and s-reducible */
        else:
            $\mathrm{g}_{r+1} \leftarrow (\mathbf{s}, g)$, add it to $\mathcal{G}$;
            for $i \in \{1, \dots, r\}$ :
                $\mathbf{t} \leftarrow \mathrm{sig}(\mathrm{g}_i, \mathrm{g}_{r+1})$;
                if the pair $(\mathrm{g}_i, \mathrm{g}_{r+1})$ is regular :
                    Add $(\mathbf{t}, \text{S-Pol}(\mathrm{g}_i, \mathrm{g}_{r+1}), \mathrm{S}(i, r+1))$ to $Q$
                if none of $\mathrm{lc}(\mathrm{g}_i), \mathrm{lc}(\mathrm{g}_{r+1})$ divides the other :
                    Add $(\mathbf{t}, \text{G-Pol}(\mathrm{g}_i, \mathrm{g}_{r+1}), \mathrm{G}(i, r+1))$ to $Q$
return $\mathcal{G}, \mathcal{G}_z$
```

$\mathbf{h} = \text{G-Pol}(\mathbf{f}, \mathbf{g})$. However, it forces us to also compute non-regular S-polynomials as long as they are non-singular: indeed, $\mathrm{sig}(\mathbf{f}, \mathbf{g}) \simeq \mathrm{sig}(\mathbf{h})$, and $\mathrm{sig}(\mathbf{h}) \simeq \mathrm{sig}(\mathbf{f}, \mathbf{h}) \simeq \mathrm{sig}(\mathbf{g}, \mathbf{h})$ because $\mathrm{lm}(\mathbf{h})$ is equal up to coefficient to the term degree of $\text{S-Pol}(\mathbf{f}, \mathbf{g})$, $\text{S-Pol}(\mathbf{f}, \mathbf{h})$ and $\text{S-Pol}(\mathbf{g}, \mathbf{h})$. So any linear combination of $\text{S-Pol}(\mathbf{f}, \mathbf{h})$ and $\text{S-Pol}(\mathbf{g}, \mathbf{h})$, which is necessary to recover $\text{S-Pol}(\mathbf{f}, \mathbf{g})$, will necessarily be non-regular. The theorem implies that even if we accept all non-singular S-polynomials, the algorithm is correct.

Allowing non-regular S-polynomials also means that we cannot *a priori* use the cover criterion in our algorithm: the algorithm would not ensure that all regular pairs are covered, but rather, only those for which the SG-polynomial is actually an S-polynomial. We can however eliminate S-polynomials which are super reducible, since Proposition 2.19 ensures that they s-reduce to 0.

The rest of the algorithm, including the processing of syzygies, is done in exactly the same way as in Algorithm 1.

4.2 Proof

The proof of Theorem 4.2 is adapted from that of [22] and [17] with the addition of signatures. First, we prove a useful technical lemma.

LEMMA 4.3. *Let* $\mathcal{G} = \{\mathrm{g}_1, \dots, \mathrm{g}_r\} \subset \mathcal{I}$ *and* $\mathbf{T} \in \mathrm{Ter}(\mathbf{M})$ *such that*

- *for all* $\mathrm{g} \in \mathcal{I}$ *with* $\mathrm{sig}(\mathrm{g}) \precsim \mathbf{T}$, g *s-reduces to 0 modulo* $\mathcal{G}$*;*
- *for all* $\mathrm{g}_i, \mathrm{g}_j \in \mathcal{G}$ *such that* $\text{SG-Pol}(\mathrm{g}_i, \mathrm{g}_j)$ *is non-singular and* $\mathrm{sig}(\mathrm{g}_i, \mathrm{g}_j) \preceq \mathbf{T}$, $\text{SG-Pol}(\mathrm{g}_i, \mathrm{g}_j)$ *s-reduces to* 0 *modulo* $\mathcal{G}$.

Let $\mathrm{g}_i, \mathrm{g}_j \in \mathcal{G}$ *such that* $\mathrm{lc}(\mathrm{g}_j)$ *divides* $\mathrm{lc}(\mathrm{g}_i)$. *Then any (possibly singular) linear combination of* g_i *and* g_j *with signature at most* $\mathbf{T}$ *s-reduces to* 0 *modulo* $\mathcal{G}$.

Algorithm 2: Pan/Lichtblau's algo., with signatures

```
Input  : $F \subset A$
Output : $\mathcal{G} \subset \mathrm{Ter}(\mathbf{M}) \times A$ Sig-GB of $\mathcal{I}$, $\mathcal{G}_z \subset \mathrm{Ter}(\mathbf{M}) \times \{0\}$
         Sig-basis of syzygies of $\mathcal{I}$
$\mathcal{G} \leftarrow \emptyset$; $\mathcal{G}_z \leftarrow \emptyset$; $r \leftarrow 0$;
$Q \leftarrow [(\mathbf{e}_i, f_i, \mathrm{N})$ for $i \in \{1, \dots, m\}]$;
while $Q$ is not empty :
    Take and remove $(\mathbf{s}, f, \mathtt{type})$ from $Q$, with $\mathbf{s}$ minimal;
    if $\exists\, \mathrm{z} \in \mathcal{G}_z$ s.t. $\mathrm{sig}(\mathrm{z})$ divides $\mathbf{s}$ :
        pass ;                              /* Prop. 2.7 */
    else:
        $g \leftarrow \mathrm{RegularReduce}((\mathbf{s}, f), \mathcal{G})$;
        if $g = 0$ :
            Add $\mathbf{s}$ to $\mathcal{G}_z$, together with sigG-combinations;
        elif type is G and $\exists\, \mathrm{g}_i \in \mathcal{G}$ s.t. $\mathrm{lt}(\mathrm{g}_i)\mathbf{s} = \mathrm{lt}(g)\mathrm{sig}(\mathrm{g}_i)$
        or type is S and $(\mathbf{s}, g)$ is super reducible by $\mathcal{G}$ :
            pass ;                     /* Prop. 2.19 */
        else:
            $\mathrm{g}_{r+1} \leftarrow (\mathbf{s}, g)$, add it to $\mathcal{G}$;
            for $i \in \{1, \dots, r\}$ :
                $\mathbf{t} \leftarrow \mathrm{sig}(\mathrm{g}_i, \mathrm{g}_{r+1})$;
                if the pair $(\mathrm{g}_i, \mathrm{g}_{r+1})$ is non-singular and
                 either of $\mathrm{lc}(\mathrm{g}_i), \mathrm{lc}(\mathrm{g}_{r+1})$ divides the other :
                    Add $(\mathbf{t}, \text{S-Pol}(\mathrm{g}_i, \mathrm{g}_{r+1}), \mathrm{S}(i, r+1))$ to $Q$
                if none of $\mathrm{lc}(\mathrm{g}_i), \mathrm{lc}(\mathrm{g}_{r+1})$ divides the other :
                    Add $(\mathbf{t}, \text{G-Pol}(\mathrm{g}_i, \mathrm{g}_{r+1}), \mathrm{G}(i, r+1))$ to $Q$
return $\mathcal{G}, \mathcal{G}_z$
```

PROOF. Let $\mathrm{m}_i = \mathrm{lm}(\mathrm{g}_i)$, $\mathrm{m}_j = \mathrm{lm}(\mathrm{g}_j)$, and $\mathrm{m}_{i,j} = \mathrm{lcmlm}(\mathrm{g}_i, \mathrm{g}_j)$. Consider a linear combination $\mathbf{h} = t_i \mathrm{g}_i + t_j \mathrm{g}_j$. Without loss of generality, combining the reductions, we may assume that t_i and t_j are terms. If $\mathrm{lm}(t_i \mathrm{g}_i) \neq \mathrm{lm}(t_j \mathrm{g}_j)$, say $\mathrm{lm}(t_i \mathrm{g}_i) > \mathrm{lm}(t_j \mathrm{g}_j)$, there is nothing to prove, as $\mathbf{h}$ can be reduced by g_i, then g_j.

So assume that $\mathrm{lm}(t_i \mathrm{g}_i) = \mathrm{lm}(t_j \mathrm{g}_j)$. Note that $\mathrm{m}_{i,j}$ divides the common multiple $\mathrm{lm}(t_i \mathrm{g}_i) = \mathrm{lm}(t_j \mathrm{g}_j)$, say, $\mathrm{lm}(t_i \mathrm{g}_i) = t' \mathrm{m}_{i,j}$. By assumption on the leading coefficients, there exists $c \in R$ such that $\mathrm{lt}(t_i \mathrm{g}_i) = t_i t' \frac{\mathrm{m}_{i,j}}{\mathrm{m}_i} \mathrm{lt}(\mathrm{g}_i) = t_i t' c \frac{\mathrm{m}_{i,j}}{\mathrm{m}_j} \mathrm{lt}(\mathrm{g}_j)$.

If $\mathrm{lm}(\mathbf{h}) = \mathrm{lm}(t_i g_i)$, the leading term of $\mathbf{h}$ is

$$\mathrm{lt}(\mathbf{h}) = \mathrm{lt}(t_i \mathrm{g}_i) + \mathrm{lt}(t_j \mathrm{g}_j) = (t_i c + t_j) t' \frac{\mathrm{m}_{i,j}}{\mathrm{m}_j} \mathrm{lt}(\mathrm{g}_j)$$

and $\mathbf{h}$ is reducible by g_j. This reduction is a s-reduction by construction.

The remaining case is the case where $\mathrm{lt}(\mathbf{h}) < \mathrm{lm}(t_i \mathrm{g}_i) = \mathrm{lm}(t_j \mathrm{g}_j)$. In this case, there exists a term t such that $t_i = t \frac{\mathrm{m}_{i,j}}{\mathrm{m}_i}$ and $t_j = ct \frac{\mathrm{m}_{i,j}}{\mathrm{m}_j}$, and $\mathbf{h} = t\text{S-Pol}(\mathrm{g}_i, \mathrm{g}_j)$. If the pair $(\mathrm{g}_i, \mathrm{g}_j)$ is non-singular, then by hypothesis, $\text{S-Pol}(\mathrm{g}_i, \mathrm{g}_j) = \text{SG-Pol}(\mathrm{g}_i, \mathrm{g}_j)$ s-reduces to 0 modulo $\mathcal{G}$, and so does $\mathbf{h} = t\text{S-Pol}(\mathrm{g}_i, \mathrm{g}_j)$. If the pair is singular, then $\mathrm{sig}(\mathbf{h}) \precsim t\mathrm{sig}(\mathrm{g}_i, \mathrm{g}_j) \preceq \mathbf{T}$, and by hypothesis, $\mathbf{h}$ s-reduces to 0 modulo $\mathcal{G}$. □

PROOF OF TH. 4.2. Write $\mathcal{G} = \{\mathrm{g}_1, \dots, \mathrm{g}_r\}$ and $\mathcal{G}_z = \{\mathrm{z}_1, \dots, \mathrm{z}_s\}$. For all i, j, let $\mathrm{c}_i = \mathrm{lc}(\mathrm{g}_i)$, $\mathrm{m}_i = \mathrm{lm}(\mathrm{g}_i)$ and $\mathrm{m}_{i,j} = \mathrm{lcmlm}(\mathrm{g}_i, \mathrm{g}_j)$. Let $\mathbf{h} \in \mathcal{I}$ with signature $\mathbf{T}$ be such that $\mathbf{h}$ is not s-reducible modulo $\mathcal{G}$. Assume that $\mathbf{T}$ is minimal for this property, and that among such elements of $\mathcal{I}$ with signature $\mathbf{T}$, $\mathrm{lm}(\mathbf{h})$ is minimal.

Consider a decomposition of $\mathbf{h}$ with respect to $\mathcal{G}$,

$$\mathbf{h} = \textstyle\sum_{u=1}^{k} \tau_u \mathbf{g}_{i_u} + \sum_{v=1}^{l} t_v^{(z)} \mathbf{z}_{j_v}, \tag{2}$$

such that for all u, v, $\operatorname{lt}(\tau_u \mathbf{g}_{i_u}) \geq \operatorname{lt}(\tau_{u+1} \mathbf{g}_{i_{u+1}})$, $\max(\tau_u \operatorname{sig}(\mathbf{g}_{i_u})) \preceq \mathbf{T}$, $\max(t_v^{(z)} \operatorname{sig}(\mathbf{z}_{j_v})) \preceq \mathbf{T}$ and $t_v^{(z)} \operatorname{sig}(\mathbf{z}_{j_v}) \geq t_{v+1}^{(z)} \operatorname{sig}(\mathbf{z}_{j_{v+1}})$. Such a representation exists, by definition of the signature of $\mathbf{h}$ and the first hypothesis on $\mathcal{G}$. Assume that, among such representation, this one is minimal in the sense that $\operatorname{lm}(\tau_1 \mathbf{g}_{i_1})$ is minimal, and the largest j such that $\operatorname{lm}(\tau_j \mathbf{g}_{i_j}) = \operatorname{lm}(\tau_1 \mathbf{g}_{i_1})$ is minimal for this property. For all u, let $\chi_u = \operatorname{lc}(\tau_u)$.

Case 1: $\mathbf{h}$ *is not a syzygy.* We want to prove that $\operatorname{lm}(\tau_1 \mathbf{g}_{i_1}) > \operatorname{lm}(\tau_2 \mathbf{g}_{i_2})$. It will in particular imply that $\operatorname{lt}(\mathbf{h}) = \operatorname{lt}(\tau_1 \mathbf{g}_{i_1})$, and thus that $\mathbf{h}$ is s-reducible modulo $\mathcal{G}$. By minimality of $\operatorname{lm}(\mathbf{h})$, this will prove that $\mathbf{h}$ s-reduces to 0 modulo $\mathcal{G}$.

In order to reach a contradiction, assume that $\operatorname{lm}(\tau_1 \mathbf{g}_{i_1})$=$\operatorname{lm}(\tau_1 \mathbf{g}_{i_2})$. By definition of the least common multiplier, there exists $m \in \operatorname{Mon}(A)$ such that $\operatorname{lm}(\tau_1 \mathbf{g}_{i_1}) = \operatorname{lm}(\tau_2 \mathbf{g}_{i_2}) = m\, \mathrm{m}_{i_1,i_2}$.

If c_{i_1} divides c_{i_2} or c_{i_2} divides c_{i_1}, then by Lemma 4.3, and expanding the s-reductions, $\tau_1 \mathbf{g}_{i_1} + \tau_2 \mathbf{g}_{i_2}$ admits a standard Sig-representation, which can be substituted in the representation (2), contradicting minimality.

For the other case, by assumption the G-polynomial of $\mathbf{g}_{i_1}$ and $\mathbf{g}_{i_2}$ is s-reducible modulo G, so there exists $\mathbf{g}_{i_3} \in G$ such that

a. $\mathrm{c}_{i_1} \mathrm{m}_{i_1,i_2}$ is divisible by $\operatorname{lt}(\mathbf{g}_{i_3})$, say, $t_1' \operatorname{lt}(\mathbf{g}_{i_3}) = \mathrm{c}_{i_1} \mathrm{m}_{i_1,i_2}$;
b. $t_1' \operatorname{sig}(\mathbf{g}_{i_3}) \preceq \operatorname{sig}(\mathbf{g}_{i_1}, \mathbf{g}_{i_2})$;
c. $\mathrm{c}_{i_2} \mathrm{m}_{i_1,i_2}$ is divisible by $\operatorname{lt}(\mathbf{g}_{i_3})$, say, $t_2' \operatorname{lt}(\mathbf{g}_{i_3}) = \mathrm{c}_{i_2} \mathrm{m}_{i_1,i_2}$;
d. $t_2' \operatorname{sig}(\mathbf{g}_{i_3}) \preceq \operatorname{sig}(\mathbf{g}_{i_1}, \mathbf{g}_{i_2})$.

In particular, c_{i_3} divides c_{i_1}, say, $\mathrm{c}_{i_1} = a_1' \mathrm{c}_{i_3}$. So the SG-polynomial of $\mathbf{g}_{i_1}$ and $\mathbf{g}_{i_3}$ is an S-polynomial, and by Lemma 4.3, it s-reduces to 0 modulo $\mathcal{G}$. So it admits a standard Sig-representation

$$\text{SG-Pol}(\mathbf{g}_{i_1}, \mathbf{g}_{i_3}) = \frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_1}} \mathbf{g}_{i_1} - a_1 \frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_3}} \mathbf{g}_{i_3} = \sum_{j \geq 1} t_j^{(1)} \mathbf{g}_{i_j}^{(1)} + \sum \text{syz.},$$

where $\sum$ syz. is a linear combination of elements of $\mathcal{G}_z$. So

$$\frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_1}} \mathbf{g}_{i_1} = a_1 \frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_3}} \mathbf{g}_{i_3} + \sum_{j \geq 1} t_j^{(1)} \mathbf{g}_{i_j}^{(1)} + \sum \text{syz.},$$

with $\operatorname{lt}(t_j^{(1)} \mathbf{g}_{i_j}^{(1)}) \leq \operatorname{lt}(\text{S-Pol}(\mathbf{g}_{i_1}, \mathbf{g}_{i_3})) < \mathrm{m}_{i_1,i_3}$. Since m_{i_1,i_2} is divisible by m_{i_3}, m_{i_1,i_2} is divisible by m_{i_1,i_3}, say, $\mathrm{m}_{i_1,i_2} = \mu_1 \mathrm{m}_{i_1,i_3}$. So all in all,

$$\begin{aligned}
\tau_1 \mathbf{g}_{i_1} &= \chi_1 m \mu_1 \frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_1}} \mathbf{g}_{i_1} \\
&= \chi_1 z_1 m \mu_1 \frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_3}} \mathbf{g}_{i_3} + \sum_{j \geq 1} \chi_1 z_1 m \mu_1 t_j^{(1)} \mathbf{g}_{i_j}^{(1)} + \sum \text{syz.}
\end{aligned}$$

and it is a standard representation of $\tau_1 \mathbf{g}_1$. Furthermore, since the signature of $\mathbf{g}_{i_3}$ is bounded (property b.), it is also a standard Sig-representation.

Similarly, there exists z_2, μ_2 and $(t_j^{(2)}, i_j)$ such that

$$\begin{aligned}
\tau_2 \mathbf{g}_{i_2} &= \chi_2 m \mu_2 \frac{\mathrm{m}_{i_2,i_3}}{\mathrm{m}_{i_2}} \mathbf{g}_{i_2} \\
&= \chi_2 a_2 m \mu_2 \frac{\mathrm{m}_{i_2,i_3}}{\mathrm{m}_{i_3}} \mathbf{g}_{i_3} + \sum_{j \geq 1} \chi_2 a_2 m \mu_2 t_j^{(2)} \mathbf{g}_{i_j}^{(2)} + \sum \text{syz.}
\end{aligned}$$

and it is a standard Sig-representation.

Table 1: Comparison between Algo. 1 and Algo. 2

System	Algo 1		Algo. 2	
	Pairs/red./to 0	Time	Pairs/red./to 0	Time
Katsura-4	420/188/0	1.35	855/412/0	1.60
Katsura-5	2048/723/0	32.40	7178/3983/0	79.87
Cyclic-5	221/63/0	0.37	347/158/0	0.71
Cyclic-6	3019/742/8	200.33	9672/5782/8	616.82

We can group both representations together, and obtain a standard Sig-representation of $\tau_1 \mathbf{g}_{i_1} + \tau_2 \mathbf{g}_{i_2}$

$$\begin{aligned}
\tau_1 \mathbf{g}_{i_1} + \tau_2 \mathbf{g}_{i_2} &= \chi_1 a_1 m \mu_1 \frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_3}} \mathbf{g}_{i_3} + \chi_2 a_2 m \mu_2 \frac{\mathrm{m}_{i_2,i_3}}{\mathrm{m}_{i_3}} \mathbf{g}_{i_3} + \sum \dots \\
&= \left(\chi_1 c_1' \mu_1 \frac{\mathrm{m}_{i_1,i_3}}{\mathrm{m}_{i_3}} + \chi_2 a_2 \mu_2 \frac{\mathrm{m}_{i_2,i_3}}{\mathrm{m}_{i_3}} \right) m \mathbf{g}_{i_3} + \sum \dots \\
&= \left(\chi_1 a_1 + \chi_2 a_2 \right) \frac{\mathrm{m}_{i_1,i_2}}{\mathrm{m}_{i_3}} m \mathbf{g}_{i_3} + \sum \dots
\end{aligned}$$

which, substituted into (2), contradicts the minimality assumption.

Case 2: $\mathbf{h}$ *is a syzygy.* The same proof as above, if $\operatorname{lt}(\mathbf{h}) = 0$, implies that $k = 0$ in (2). Now, consider, among all decompositions of the form (2), one where $j = \max(v : t_v^{(z)} \operatorname{sig}(\mathbf{z}_{j_v})) \simeq t_1^{(z)} \operatorname{sig}(\mathbf{z}_{j_1})$ is minimal. Assume that $j > 0$, and thus $t_1^{(z)} \operatorname{sig}(\mathbf{z}_{j_1}) \simeq t_2^{(z)} \operatorname{sig}(\mathbf{z}_{j_2})$. Then, by assumption, the sigG-comb. of $\mathbf{z}_1$ and $\mathbf{z}_2$ is sig-reducible by $\mathcal{G}_z$, thus, there exists $t_1' \in \operatorname{Ter}(A)$ and $j_1' \in \{1, \dots, s\}$ such that $t_1' \operatorname{sig}(\mathbf{z}_{j_1'}) = t_1^{(z)} \operatorname{sig}(\mathbf{z}_{j_1}) + t_2^{(z)} \operatorname{sig}(\mathbf{z}_{j_2})$, and so $\mathbf{z} := t_1^{(z)} \mathbf{z}_1 + t_2^{(z)} \mathbf{z}_2 - t_1' \operatorname{sig}(\mathbf{z}_{j_1'})$ has signature $\precnsim \mathbf{T}$. So subtracting $\mathbf{z}$ from the decomposition (2) results in a decomposition with fewer terms matching the signature of $\mathbf{h}$, contradicting the minimality of j. □

5 ALGORITHMS IN PRACTICE

5.1 Further optimizations

In this section, we briefly describe additional criteria which can be used to eliminate elements. Firstly, in both algorithms, one can use Buchberger's coprime and chain criteria (either as-is or using Gebauer and Möller's implementation). Buchberger's criterion does not require any modification to work with signatures, whereas the chain criterion needs to ensure that the signature of the pairs used to discard the redundant one is small enough [15]. Note that in all cases, we need to consider terms (with their coefficients) and not just monomials. For Lichtblau's algorithm, refined versions of those criteria relaxing the condition on the coefficients have been described in [17] and can also be used here.

We have already stated that some criteria can be used to eliminate pairs based on their signatures. We have also already mentioned the idea of the F5 criterion, filling the basis of syzygies with the signatures of predictable syzygies, as well as the possibility of discarding G-polynomials which are sig-reducible by $\mathcal{G}_z$, or which are super reducible and s-reducible by $\mathbf{g} \in \mathcal{G}$. Similarly, in Lichtblau's algorithm, one can discard any S-polynomial which is super reducible by $\mathcal{G}$.

A natural question is whether the cover criterion would allow to systematically discard G-polynomials in Algorithm 1, or to discard

Table 2: Comparative timings for module computations with the signature-based algorithms and with Magma (in seconds)

System	With signatures (Algo. 1)			Magma		
	Sig-GB	Recons.	**Total**	GB	**GB with coordinates**	**Module of syzygies**
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**

new elements in Algorithm 2 (including non-regular S-polynomials). Experimentally, it appears that indeed, most such elements which are covered can be discarded without impacting the correctness of the algorithm.

Another point which can have a large impact on the complexity is the choice of the order of the pairs, *i.e.* , how to break ties between elements with signatures which are $\simeq$. A strategy which seems to yield good results over $\mathbb{Z}$ is to compare the absolute value of the coefficient of the signatures, so as to create super reducers and covering candidates sooner.

We have only mentioned top reductions, namely, reductions of the leading coefficient, but as usual, the definitions generalize to allow reductions of the rest of the terms. Finally, we have only defined reductions where the leading coefficient of the reducer divides the coefficient to be reduced. In some rings, and in particular in the case of Euclidean rings, it is also possible to perform modular reductions on the coefficients without impacting the correctness of the result. This significantly improves the performances of the algorithm. The same can be done for sig-reductions.

5.2 Experimental data

We have written a prototype implementation of both algorithms in Magma[4], for the PoT ordering and $R = \mathbb{Z}$. We report in Table 1 data on the number of pairs being processed, reduced and reduced to zero for different benchmark systems (Katsura-n and Cyclic-n), as well as indicative computation times. In practice, it appears that Algo. 1 is more efficient than Algo. 2, both in terms of number of computed pairs and in time. This appears to be due to the relaxed restrictions allowing non-singular polynomials, more than the lack of criteria.

Our prototype implementation of both algorithms of the paper is slower than Magma's implementation of F4 [9] over $\mathbb{Z}$ for merely computing Gröbner bases. As mentioned earlier, the computation of signatures also allows to compute the coefficients of the elements of the Gröbner basis in terms of the input, and a basis of the module of syzygies, by performing and tracking s-reductions [14]. The process only depends on the definition of a Sig-GB and a Sig-basis of syzygies, and therefore works in our setting as well. In Table 2, we give the computation time for this reconstruction using Algo. 1, as well as comparable routines in Magma[5]. In several instances, we observe that the use of signatures gives a significant speed-up for those computations.

One particularity of signature-based algorithms over rings is that, due to the partial order on the signatures, they typically compute a large number of elements with incomparable signatures. This problem does not appear over fields, and future work will focus on ways to eliminate more of those elements, or to speed-up the computations at a given signature (for instance using linear algebra techniques similar to F4).

[4] https://gitlab.com/thibaut.verron/signature-groebner-rings

[5] Groebner of an IdealWithFixedBasis for a GB with coordinates, and SyzygyMatrix for a basis of the syzygy module.

REFERENCES

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases.* American Mathematical Society, 7 1994.

[2] T. Becker, H. Kredel, and V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra.* Springer-Verlag, 4 1993.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, University of Innsbruck, Austria, 1965.

[5] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. In *International Symposium on Symbolic and Algebraic Manipulation*, pages 3–21. Springer, 1979.

[6] C. Eder and Jean-Charles Faugère. A Survey on Signature-based Algorithms for Computing Gröbner Bases. *Journal of Symbolic Computation*, 80:719–784, 2017.

[7] C. Eder, G. Pfister, and A. Popescu. On Signature-Based Gröbner Bases over Euclidean Rings. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 141–148, New York, NY, USA, 2017. ACM.

[8] C. Eder, G. Pfister, and A. Popescu. Standard bases over Euclidean domains. *Journal of Symbolic Computation*, 102:21 – 36, 2021.

[9] Jean-Charles Faugère. A New Efficient Algorithm for Computing Gröbner Bases (F4). *Journal of Pure and Applied Algebra*, 139(1):61–88, 1999.

[10] Jean Charles Faugère. A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[11] M. Francis and A. Dukkipati. On Ideal Lattices, Gröbner Bases and Generalized Hash Functions. *Journal of Algebra and Its Applications*, 2017.

[12] M. Francis and T. Verron. A signature-based algorithm for computing Gröbner bases over principal ideal domains. *Mathematics in Computer Science*, Dec 2019.

[13] S. Gao and F. Guan, Y.and Volny IV. A New Incremental Algorithm for Computing Gröbner bases. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, pages 13–19. ACM, 2010.

[14] S. Gao, Volny IV, and M. F, Wang. A new framework for computing Gröbner bases. *Mathematics of Computation*, 85(297):449–465, May 2015.

[15] V. P. Gerdt and A. Hashemi. On the use of Buchberger criteria in G^2V algorithm for calculating Gröbner bases. *Program. Comput. Softw.*, 39(2):81–90, 2013. Translated from Programmirovanie **39** (2013), no. 2.

[16] A. Kandri-Rody and D. Kapur. Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain. *J. Symbolic Comput.*, 6(1):37–57, 1988.

[17] D. Lichtblau. Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.*, 56(1):177–194 (2013), 2012.

[18] D. Lichtblau. Applications of Strong Gröbner Bases over Euclidean Domains. *Int. J. Algebra*, 7(5-8):369–390, 2013.

[19] V. Lyubashevsky and D. Micciancio. Generalized Compact Knapsacks Are Collision Resistant. In *ICALP (2)*, pages 144–155, 2006.

[20] H. M. Möller. On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation*, 6(2-3):345–359, 1988.

[21] H M. Möller, T. Mora, and C. Traverso. Gröbner bases computation using syzygies. In *Papers from the international symposium on Symbolic and algebraic computation*, pages 320–328, 1992.

[22] L. Pan. On the D-bases of polynomial ideals over principal ideal domains. *J. Symbolic Comput.*, 7(1):55–69, 1989.