A survey on signature-based Gröbner basis computations

Christian Eder\textsuperscript{1} and Jean-Charles Faugère\textsuperscript{2}
\textsuperscript{1} University of Kaiserslautern
Department of Mathematics
PO box 3049
67653 Kaiserslautern
eder@mathematik.uni-kl.de
\textsuperscript{2} INRIA, Paris-Rocquencourt Center, PolSys Project
UPMC, Univ. Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6
Case 169, 4, Place Jussieu, F-75252 Paris
Jean-Charles.Faugere@inria.fr

Abstract. This paper is a survey on the area of signature-based Gröbner basis algorithms that was initiated by Faugère’s \textsc{F5} algorithm in 2002. We explain the general ideas behind the usage of signatures. We show how to classify the various known variants by 3 different orderings. For this we give translations between different notations and show that besides notations many approaches are just the same. Moreover, we give a general description of how the idea of signatures is quite natural when performing the reduction process using linear algebra. This survey shall help to outline this field of active research.

1 Introduction

Gröbner bases are a fundamental tool in computer algebra with many applications in various areas. In 1965 Buchberger introduced a first algorithmic approach for their computation [16]. Over the years many improvements and optimizations were found, for example, criteria to remove useless elements during the computation [17,18,53].

In 2002 Faugère presented the \textsc{F5} algorithm [33] which was a significant development in Gröbner basis computation. This algorithm used for the first time signatures to detect efficiently useless data. The \textsc{F5} algorithm is well-known for computing no zero reduction, that means no useless computation if the input system is regular.

Beginning 2008, many researchers worked on understanding the new criteria behind \textsc{F5}, which lead to new insights, but also optimizations and new variants of the signature-based approach \cite{3,22,23,29}.

While the question of \textsc{F5}’s termination was still an open one until recently \cite{45,68,69}, many new variants of \textsc{F5} were introduced, for example, \textsc{G2V} \cite{46} resp. \textsc{GVW} \cite{47,49,83} or \textsc{SB} \cite{70,71}.

Moreover, first papers trying to classify all the different variants of signature-based Gröbner basis algorithms came up \cite{30,31,53,68,69,76}.

At the moment the area of signature-based Gröbner basis algorithms is confusing and vast. More and more papers are published proving statements already proven before, and even more publications can be found on “new” variants that boil down to be a known one just with a different notation.

In this paper we try to give a rigorous survey on signature-based Gröbner basis theory, including all variants known up to now. We lay an emphasis on understanding and we show how the variants presented over the last years are mostly differ in small parts only. Moreover, we give the reader a vocabulary book at hand which helps to understand how notations, varying for different authors, coincide.

Since this is a survey, we do not give proofs if they are long, complex, or do not help in understanding the topic. We always explain the idea behind the proofs and refer to the related publication which includes a complete proof. There the reader is then, with our descriptions and explanations, able to understand the

\textsuperscript{*} The author was supported by the EXACTA grant (ANR-09-BLAN-0371-01) of the French National Research Agency.
proof in the used notation and language. Table 1 gives the outline of this paper and can be used as an index for finding the variant the reader might be interested in. Moreover, Figure 1 gives a graphical overview on the connection between the different algorithms that are explained in the following.

In Section 10 we give the problem of proving F5’s termination an in-depth discussion, where we also explain how termination-ensuring variants as described in [4], [28], [51] are still useful from an algorithmic point of view.

Moreover, we present descriptions of signature-based computations using linear algebra for the reduction process, see Sections 3 and 13. Besides [2] which is restricted to F5 this is the first known discussion on this topic and shows how the ideas of signatures rather naturally come up in this setting.

Furthermore, we give in Section 14 detailed experimental results generated with various variants of signature-based Gröbner basis algorithms presented in this survey. There we do not focus on timings, but on the characteristics of the different variants, like size of the resulting Gröbner basis, size of the recovered syzygy module, number of zero reductions and number of operations overall. The code those computations are done with is implemented in SINGULAR [21] and available open-source. Thus the implementation is transparent and the reader is able to understand the different outcomes in the various algorithms.

All in all, this is the first extensive classification of signature-based Gröbner basis algorithms and we hope that it can be used as a useful handbook for researchers and students.

| Name/case          | modification w.r.t. F5 [33] (Section 8)                                                                 | Section | Reference |
|--------------------|----------------------------------------------------------------------------------------------------------|---------|-----------|
| MatrixF5           | uses Macaulay matrices and linear algebra for reduction purposes, does not build S-pairs but generates all multiples of the generators for a given degree step | 3       | [36]      |
| RB                 | generalized algorithm to compare \( \leq_{\text{add}} \) and \( \leq_{\text{rat}} \), special case of RB defined in Section 7 | 7.2     | [31]      |
| F5’                | homogenizes inhomogeneous input, interreduces intermediate Gröbner basis                                 | 8       | [33]      |
| F5”                | uses \( \prec_{d\text{-pot}} \) instead of \( \prec_{\text{pot}} \)                                         | 8       | [33]      |
| F5R                | interreduces intermediate Gröbner basis, uses it only for reduction purposes                             | 8.1     | [72]      |
| F5C                | interreduces intermediate Gröbner basis, uses it for reduction purposes and for creation of new S-pairs | 8.2     | [29]      |
| F5A                | variant of F5C directly using a zero reduction as signature for the syzygy module                         | 8.2     | [30]      |
| iF5A               | variant of F5A recomputing signatures after interreducing between two incremental steps, also iG2V, . . . | 8.2     | [26]      |
| Extended F5 criteria | uses different module monomial orders                                                                      | 8.3     | [5]       |
| F5/2               | adds field equations to the input systems for computations over \( \mathbb{F}_2 \)                         | 9.1     | [36]      |
| bihomogeneous case | uses maximal minors of Jacobian matrices to enlarge system of syzygies                                     | 9.2     | [33]      |
| SAGBI Gröbner bases | uses the Reynolds operator on the syzygy criterion                                                          | 9.3     | [43]      |
| F5GEN              | generalized algorithm for different rewrite orders, applicable with any compatible module monomial order   | 10.1    | [68], [69]|

Continued on the next page →→
| Name/case   | modification w.r.t. F5 \([33]\) (Section [8])                                                                 | Section  | Reference |
|------------|-----------------------------------------------------------------------------------------------------------------|----------|-----------|
| F5t        | uses the Macaulay bound, once it is exceeded the algorithm transforms to Buchberger’s algorithm                  | 10.2     | 50, 51    |
| F5B        | uses two lists of S-pairs: one for usual F5, another one for computing a lower degree bound using Buchberger’s chain criterion | 10.2     | 4         |
| F5+        | distinguishes S-pairs needed for the Gröbner basis and those needed for F5’s correctness only, once only the later ones are left it uses the idea of F5B | 10.2     | 28        |
| Arri & Perry's work | introduces rewrite order \(\leq_{rat}\), works for any compatible module monomial order, directly uses zero reduction as signature for syzygy module, also known by AP | 11.1     | 3         |
| TRB        | generalized algorithm to compare F5 and GVW, also introduces \(\leq_{rat}\) as rewrite order, applicable with any compatible module monomial order | 11.2     | 58        |
| GBGC       | generalized algorithm, uses \(\leq_{rat}\) but also generalizes to use partial rewrite orders, applicable with any compatible module monomial order, later on further generalized to work on algebras of solvable type | 11.3     | 76, 81    |
| G2V        | directly uses zero reduction as signature for syzygy module, rewriting is done implicitly w.r.t. \(\leq_{add}\) | 11.4     | 46        |
| GVW        | generalizes G2V to be applicable with any compatible module monomial order, uses \(\leq_{rat}\) since 2011 (and thus coincides with AP; also known as GVWHS) | 11.5     | 47, 49    |
| SB         | coincides with GVW and AP, \(<_{lt-pot}\) only                                                                 | 11.6     | 70        |
| SSG        | coincides with SB, GVW and AP                                                                                   | 11.7     | 44        |
| ImpG2V     | uses Buchberger’s Product and Chain criterion in G2V (this is also introduced in the 2013 revision of GVW)       | 12        | 49, 54    |
| F4/5       | uses F4-style s-reduction                                                                                        | 13        | 2         |

Table 1: Variants of F5 and their modifications (in the order of appearance in this survey)
Fig. 1. A good decade in signature-based Gröbner basis algorithms (status: March 2014)
2 Notations and terminology

In this section we introduce notations and basic terminology used in this survey. Readers already familiar with signature-based algorithms might skip this section. Still note that notations itself play an important role in the following, especially when comparing different variants of signature-based algorithms. We extend the notation introduced in [31].

Let $\mathcal{R}$ be a polynomial ring over a field $\mathcal{X}$. All polynomials $f \in \mathcal{R}$ can be uniquely written as a finite sum $f = \sum_{\alpha, x \in \mathcal{X}} \kappa_\alpha x^\alpha$ where $\kappa_\alpha \in \mathcal{X}$, $x^\alpha = \prod_{i} x_i$ and $\mathcal{M}$ is minimal. The elements of $\mathcal{M}$ are the terms of $f$. A monomial is a polynomial with exactly one term. A monomial with a coefficient of 1 is monic. Neither monomials nor terms of polynomials are necessarily monic. We write $f \simeq g$ for $f, g \in \mathcal{R}$ if there exists a non-zero $\kappa \in \mathcal{X}$ such that $f = \kappa g$.

Let $\mathcal{R}^m$ be a free $\mathcal{R}$-module and let $e_1, \ldots, e_m$ be the standard basis of unit vectors in $\mathcal{R}^m$. All module elements $a \in \mathcal{R}^m$ can be uniquely written as a finite sum $a = \sum_{\alpha, e_i} \kappa_{\alpha e_i}$ where the $\alpha$ are monomials and $\mathcal{N}$ is minimal. The elements of $\mathcal{N}$ are the terms of $a$. A module monomial is an element of $\mathcal{R}^m$ with exactly one term. A module monomial with a coefficient of 1 is monic. Neither module monomials nor terms of module elements are necessarily monic. Let $\alpha \simeq \beta$ for $\alpha, \beta \in \mathcal{R}^m$ if $\alpha = \kappa \beta$ for some non-zero $\kappa \in \mathcal{X}$.

Let $\leq$ denote two different orders – one for $\mathcal{R}$ and one for $\mathcal{R}^m$: The order for $\mathcal{R}$ is a monomial order, which means that it is a well-order on the set of monomials in $\mathcal{R}$ such that $a \leq b$ implies $ca \leq cb$ for all monomials $a, b, c \in \mathcal{R}$. The order for $\mathcal{R}^m$ is a module monomial order which means that it is a well-order on the set of module monomials in $\mathcal{R}^m$ such that $S \leq T$ implies $CS \leq CT$ for all module monomials $S, T \in \mathcal{R}^m$ and monomials $c \in \mathcal{R}$. We require the two orders to be compatible in the sense that $a \leq b$ if and only if $\alpha \leq \beta$ for all monomials $a, b \in \mathcal{R}$ and $i = 1, \ldots, m$.

Consider a finite sequence of module monomials $f_1, \ldots, f_m \in \mathcal{R}$ that we call the input (polynomials). We call $f_1, \ldots, f_m$ a regular sequence if $f_i$ is a non-zero-divisor on $\mathcal{R} / \langle f_1, \ldots, f_{i-1} \rangle$ for $i = 2, \ldots, m$. For $a = \sum_{i=1}^m a_i e_i$, $a \in \mathcal{R}$ we define the homomorphism $a \mapsto \overline{a}$ from $\mathcal{R}^m$ to $\mathcal{R}$ by $\overline{a} := \sum_{i=1}^m a_i f_i$. An element $a \in \mathcal{R}^m$ with $\overline{a} = 0$ is called a syzygy. The module of all syzygies of $f_1, \ldots, f_m$ is denoted by $\text{syz} (f_1, \ldots, f_m)$.

Next we introduce the notion of signatures together with related structures in the plain polynomial setting.

Definition 2.1.

(a) The lead term $\text{lt} (f)$ of $f \in \mathcal{R} \setminus \{ 0 \}$ is the $\leq$-maximal term of $f$. The lead coefficient $\text{lc} (f)$ of $f$ is the coefficient of $\text{lt} (f)$. For a set $F \subseteq \mathcal{R}$ we define the lead ideal of $F$ by $L(F) := \{ \text{lt} (f) \mid f \in F \}$.

(b) The lead term resp. signature $s (a) \in \mathcal{R}^m \setminus \{ 0 \}$ denotes the $\leq$-maximal term of $a$. If $\alpha e_i = s (a)$ then we call $\text{ind} (\alpha) = i$ the index of $\alpha$.

(c) For $a \in \mathcal{R}^m$ we define the sig-poly-pair of $a$ by $(s (a), \overline{a}) \in \mathcal{R}^m \times \mathcal{R}$.

(d) $\alpha, \beta \in \mathcal{R}^m$ are equal up to sig-poly-pairs if $s (\alpha) = s (\kappa \beta)$ and $\overline{\alpha} = \overline{\kappa \beta}$ for some non-zero $\kappa \in \mathcal{X}$. Correspondingly, $\alpha, \beta$ are said to be equal up to sig-lead-pairs if $s (\alpha) = s (\kappa \beta)$ and $\text{lt} (\overline{\alpha}) = \text{lt} (\overline{\kappa \beta})$ for some non-zero $\kappa \in \mathcal{X}$.

With these definitions every non-syzygy module element $\alpha \in \mathcal{R}^m$ has two main associated characteristics – the signature $s (\alpha) \in \mathcal{R}^m$ and the lead term $\text{lt} (\overline{\alpha}) \in \mathcal{R}$ of its image $\overline{\alpha}$. Lead terms and signatures include a coefficient for mathematical convenience, though an implementation of an signature-based Gröbner Basis algorithm need not store the signature coefficients as we discuss in Sections 3 and 11.

We define some canonical module monomial orders that are useful in the following.

Definition 2.2. Let $< \sqsubseteq$ be a monomial order on $\mathcal{R}$ and let $ae_i, be_j$ be two module monomials in $\mathcal{R}^m$.

(a) $ae_i <_{\text{pot}} be_j$ if and only if either $i < j$ or $i = j$ and $a < b$.

(b) $ae_i <_{\text{top}} be_j$ if and only if either $a < b$ or $a = b$ and $i < j$.

These two orders can be combined with either a weighted degree or a weighted leading monomial:

(a) $ae_i <_{d, \text{pot}} be_j$ if and only if either $\deg (\overline{ae_i}) < \deg (\overline{be_j})$ or $\deg (\overline{ae_i}) = \deg (\overline{be_j})$ and $ae_i <_{\text{pot}} be_j$. In the same way we define $ae_i <_{d, \text{top}} be_j$.

(b) $ae_i <_{d, \text{top}} be_j$ if and only if either $\text{lt} (\overline{ae_i}) < \text{lt} (\overline{be_j})$ or $\text{lt} (\overline{ae_i}) = \text{lt} (\overline{be_j})$ and $ae_i <_{\text{pot}} be_j$. In the same way we define $ae_i <_{d, \text{top}} be_j$. 

5
Note that $<_{lt\text{-}pot}$ is also known as Schreyer’s order, for example, see [56].

The above introduced notation of the orders represent that the position in the module resp. the lead term in the polynomial ring are preferred.

**Example 2.3.** Note that a polynomial can have infinitely many different module representations with distinct signatures. Consider the three input polynomials $f_1 = x^2 - y^2$, $f_2 = xyz - z^2$, and $f_3 = yz^2 - xy$ in $\mathbb{R} = \mathbb{Q}[x,y,z]$ where $<$ denotes the graded reverse lexicographical monomial order. Moreover, assume $<$ to extend to $<_{pot}$ on the set of monomials of $\mathbb{R}^2$. For example, we can represent $f_2$ by $e_2$. Since $f_1 e_3 - f_2 e_1 = 0$ another representation of $f_2$ might be $f_1 e_3 + e_2 - f_2 e_1$. Note that the two representations of $f_2$ have two different signatures, $e_2$ and $\text{lt}(f_1) e_3$, respectively. We also want to point out that $\text{lt}\left(\frac{x(a)}{3}\right) \neq \text{lt}\left(\frac{x}{3}\right)$ is possible: In the above example $\text{lt}\left(s\left(e_2\right)\right) = \text{lt}\left(f_2\right)$, but $\text{lt}\left(s\left(f_1 e_3 + e_2 - f_2 e_1\right)\right) = \text{lt}\left(\text{lt}\left(f_1\right) f_3\right) \neq \text{lt}\left(f_2\right)$.

Finally, we introduce the notion of Gröbner bases. For this, the reduction of polynomials is essential.

**Definition 2.4.** Let $f \in \mathbb{R}$ and let $t$ be a term of $f$. Then we can reduce $t$ by $g \in \mathbb{R}$ if there exists a monomial $b$ such that $\text{lt}(bg) = t$. The outcome of the reduction step is then $f - bg$ and $g$ is called the reducer. When $g$ reduces $t$ we also say for convenience that $bg$ reduces $f$. That way $b$ is introduced implicitly instead of having to repeat the equation $\text{lt}(bg) = t$.

The result of an reduction of $f \in \mathbb{R}$ is an element $h \in \mathbb{R}$ that has been calculated from $f$ by a sequence of reduction steps. Thus, reductions can always be assumed to be done w.r.t. some finite subset $G \subset \mathbb{R}$.

**Definition 2.5.** Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in $\mathbb{R}$. A finite subset $G$ of $\mathbb{R}$ is a Gröbner basis up to degree $d$ for $I$ if $G \subset I$ and for all $f \in I$ with $\text{deg}(f) \leq d$ $f$ reduces to zero w.r.t. $G$. $G$ is a Gröbner basis for $I$ if $G$ is a Gröbner basis in all degrees.

In the very same way one can define Gröbner basis with the notion of standard representations:

**Definition 2.6.** Let $f \in \mathbb{R}$ and $G \subset \mathbb{R}$ finite. A representation $f = \sum_{i=1}^{k} m_i g_i$ with monomials $m_i \neq 0$, $g_i \in G$ pairwise different is called a standard representation if

$$\max \{\text{lt}(m_i g_i) \mid 1 \leq i \leq k\} \leq \text{lt}(f).$$

One can show that if for any $f \in \langle G \rangle$ with $f \neq 0$ $f$ has a standard representation w.r.t. $G$ and $\leq$ then $G$ is a Gröbner basis for $\langle G \rangle$. Moreover, note that the existence of a standard representation does not imply reducibility to zero, see, for example, Exercise 5.63 in [16].

Luckily, Buchberger also gave an algorithmic description of Gröbner bases using the notion of so-called S-polynomials:

**Definition 2.7.** Let $f \neq 0, g \neq 0 \in \mathbb{R}$ and let $\lambda = \text{lcm}(\text{lt}(f), \text{lt}(g))$ be the monic least common multiple of $\text{lt}(f)$ and $\text{lt}(g)$. The S-polynomial between $f$ and $g$ is given by

$$\text{spol}(f, g) := \frac{\lambda}{\text{lt}(f)} f - \frac{\lambda}{\text{lt}(g)} g.$$

**Theorem 2.8 (Buchberger’s criterion).** Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in $\mathbb{R}$. A finite subset $G$ of $\mathbb{R}$ is a Gröbner basis for $I$ if $G \subset I$ and for all $f, g \in G$ $\text{spol}(f, g)$ reduces to zero w.r.t. $G$.

## 3 Matrix F5

Before we approach signature-based Gröbner basis algorithms theoretically let us look at a small Gröbner basis computation. We start with a slightly simplified version of the F5 algorithm, the **MatrixF5**. With this
introduction to the topic we are able to give an easy description of the main ideas behind the classification of signature-based algorithms which is discussed in detail later on. In order to keep this section plain and easy we keep signature-based details at a minimum and focus on presenting their usefulness discarding useless elements from the computation.

Descriptions of MatrixF5 can be also found, for example, in [62,63]. It is first publicly mentioned in [36] and known for breaking challenge 1 of the hidden field equations (HFE) crypto system.

Algebraic systems are solved by computing a Gröbner basis for a corresponding ideal, [16][18]. The link between solving such systems and linear algebra is already very old, see, for example, [62][64]. In 1999 Faugère introduced the F4 algorithm, [32]. A simplified description of this algorithm using signature-based criteria is MatrixF5 which we present here. The important fact is that polynomial reduction coincides with Gaussian elimination in MatrixF5 and thus the process of computing the basis can be illustrated nicely.

Let \( I = \langle f_1, \ldots, f_m \rangle \subset \mathcal{R} \) be the homogeneous input ideal. We want to compute a Gröbner basis for \( I \) w.r.t. a given monomial order \( \prec \). The idea is to incrementally construct Macaulay matrices \( M_d \) which are generalizations of the Sylvester matrix for finitely many (\( > 2 \) possible), multivariate polynomials. In the above setting the rows of \( M_d \) represent the polynomials \( t_{j,k}f_k \) where \( t_{j,k} \) are monomials in \( \mathcal{R} \) such that \( \deg(t_{j,k}f_k) \leq d \) for all \( 1 \leq k \leq m \). The columns of \( M_d \) are labelled by all possible terms \( x^\nu \) such that \( \deg(x^\nu) \leq d \). Moreover, the columns are sorted, from left to right, by decreasing monomial order \( \prec \). Thus a row of \( M_d \) labelled by \( t_{j,k}f_k = \sum_{\nu \in \mathcal{X}} \kappa_{\nu} x^\nu \) has in column \( x^\nu \) entry \( \kappa_{\nu} \in \mathcal{X} \). Note that by the this representation of \( t_{j,k}f_k \), \( \kappa_{o} = 0 \) is possible. Once \( M_d \) is generated, the row echelon form \( N_d \) of \( M_d \) is computed. The rows of \( N_d \) now correspond to polynomials in \( \mathcal{R} \) that generate a Gröbner basis up to degree \( d \) for \( I \). So, in contrast to Gröbner basis algorithms in the vein of Buchberger’s description, MatrixF5 needs another parameter, a degree bound \( D \) up to which the computations are carried out. We introduce the variant of this algorithm using signature-based criteria to improve computations by an example.

Consider the three homogeneous input polynomials \( f_1 = y^2 + 4yz, f_2 = 2x^2 + 3xy + 4y^2 + 3z^2, \) and \( f_3 = 3x^2 + 4xy + 2y^2 \) in \( \mathcal{R} = \mathbb{F}_5[x, y, z] \) where \( \prec \) denotes the graded reverse lexicographical monomial order. By the above description it is clear that the labels \( t_{j,k}f_k \) of the rows coincide with the corresponding signatures \( t_{j,k}e_k \). We want to use these signatures to label the rows of the Macaulay matrices built in the following. Thus we need to extend \( \prec \) on \( \mathcal{R}^3 \), say we use \( \prec_{\text{pot}} \). Let us assume we want to compute a Gröbner basis up to degree \( D = 4 \).

The main idea of using Macaulay matrices is now to calculate all possible elements in \( I \) for a given degree \( d \). In Buchberger’s attempt (Theorem 2.3) one considers \( S \)-polynomials of degree \( d \) and has to find reducers of these. Here we do not need to search for such elements, all possible reducers are already in \( M_d \). So we can focus on the main question: How do signature-based criteria work to improve Gröbner basis computations?

Let us start with the lowest possible degree, \( d = 2 \). Building the Macaulay matrix \( M_2 \) in Figure 2 we label the rows by the corresponding signatures. Throughout the steps of reducing \( M_2 \) we keep track in the label of the rows what computational steps have been done.

One of the reduction steps differs, the last step: Looking at the label of the second row after reducing it with the first row we see that there is a change:

\[
e_2 + e_1 \implies e_3 + 2e_2 + 5e_1.
\]

Since the labels change also in the other reduction steps, the question is, what is special in this step? Looking at the lead term of the module element we see the difference: Before the reduction the label of the row has a lead term of \( e_2 \) w.r.t. \( \prec_{\text{pot}} \), afterwards it is \( e_3 \). In none of the other reduction steps above the lead term changed. And that is the general idea of the signature: We want to easily keep track of where the new rows are coming from. Storing the complete module representation as done above, the overhead of computing a Gröbner basis is too big (see also [65]). Thus, instead of keeping the full module representation, we only store the lead term of it, the signature. Applied to our example above the last step would lead to the situation illustrated in Figure 3.

In other words, we would loose the connection between the second row and \( e_2 \) resp. \( f_2 \). As we see in following, to remember this connection is crucial for the strength of signature-based criteria to remove useless computations.

We agree to not do any such reduction. In terms of the Macaulay matrix this means that
Fig. 2. Computing the row echelon form of $M_2$.

(a) rows are sorted from top to bottom by decreasing signatures, and
(b) the row we reduce with must be below the row to be reduced.

Fig. 3. Change of signature due to a reduction step.

Thus for our purpose to keep the signatures, the row echelon form of $M_2$ received by restricting reductions is

$$N_2 = \begin{pmatrix}
   e_3 & \begin{pmatrix} x^2 & xy & y^2 & xz & yz & z^2 \\ 0 & 2 & 0 & 0 & 1 & 3 \end{pmatrix} \\
   e_2 & \begin{pmatrix} 0 & 2 & 0 & 0 & 1 & 3 \end{pmatrix} \\
   e_1 & \begin{pmatrix} 2 & 3 & 0 & 0 & 4 & 3 \end{pmatrix} \\
\end{pmatrix}$$

After computing the row echelon form $N_2$ of the Macaulay matrix $M_2$ we get two new polynomials, namely $f_4 = 2xy + yz + 3z^2$ and $f_5 = 2x^2 + 3xy + 4yz + 3z^2$, corresponding to the first and the second row of $N_2$. $f_3$
and $f_4$ have the same signature $e_3$, thus we can say that there is a connection between them. The same holds for $f_2$ and $f_5$.

$$
\begin{pmatrix}
  x^3 & x^2 y & xy^2 & y^3 & x^2 z & x y z & y^2 z & x z^2 & y z^2 & z^3 \\
  x e_1 & 3 & 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
  y e_1 & 0 & 3 & 4 & 2 & 0 & 0 & 0 & 0 & 0 \\
  z e_1 & 0 & 0 & 0 & 3 & 4 & 2 & 0 & 0 & 0 \\
  x e_2 & 2 & 3 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\
  y e_2 & 0 & 2 & 3 & 4 & 0 & 0 & 0 & 0 & 0 \\
  z e_2 & 0 & 0 & 0 & 2 & 3 & 4 & 0 & 0 & 0 \\
  x e_3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 4 \\
  y e_3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 4 \\
  z e_3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 \\
\end{pmatrix}
$$

Fig. 4. Initial Macaulay matrix $M_3$

$$
\begin{pmatrix}
  x^3 & x^2 y & xy^2 & y^3 & x^2 z & x y z & y^2 z & x z^2 & y z^2 & z^3 \\
  x e_1 & 3 & 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
  y e_1 & 0 & 3 & 4 & 2 & 0 & 0 & 0 & 0 & 0 \\
  z e_1 & 0 & 0 & 0 & 3 & 4 & 2 & 0 & 0 & 0 \\
  x e_2 & 2 & 3 & 0 & 0 & 0 & 4 & 0 & 3 & 0 \\
  y e_2 & 0 & 2 & 3 & 0 & 0 & 0 & 4 & 0 & 3 \\
  z e_2 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 4 & 3 \\
  x e_3 & 0 & 0 & 1 & 0 & 0 & 4 & 0 & 0 & 0 \\
  y e_3 & 0 & 0 & 1 & 0 & 0 & 4 & 0 & 0 & 0 \\
  z e_3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 0 \\
\end{pmatrix}
$$

Fig. 5. Rewriting rows: $f_2 \rightarrow f_5$ (top), $f_3 \rightarrow f_4$ (bottom)

At this point we have not done any reduction in $M_3$ but just used the information stored in the signatures. Let us rearrange the rows of $M_3$ to see how near we are already to a row echelon form:
Next we can go on with degree 3. Generating $M_3$ we get all multiples $xf_i, yf_i,$ and $zf_i$ for $1 \leq i \leq 3$ as it is shown in Figure 4. Looking at $M_3$ more closely we see some relation to $M_2.$ The three steps highlighted correspond to reduction steps that have already occured in degree 2:

\[
xe_2 - xe_1 = x(e_2 - e_1) \\
ye_2 - ye_1 = y(e_2 - e_1) \\
ze_2 - ze_1 = z(e_2 - e_1). \\
\]

Since we have done these reductions already it makes sense to not redo them again, but use the information from $M_2.$ We know that $f_5$ comes from $f_2,$ both share the same signature. So we just rewrite $xf_2, yf_2, zf_2$ by $xf_3, yf_3, zf_3$ in $M_3,$ respectively. The very same holds for $f_3$ and $f_4.$ Figure 5 illustrates this process.

Only rewriting $f_2$ and $f_4$ with “better” elements lead to this matrix in near row echelon form. Again, note that not all elements in the above picture are allowed to reduce freely: The rows highlighted in green can rewrite $x$'s and $y$'s, while the row labelled by signature $xe_3$ is not allowed to reduce the row labelled by $xe_1.$ Otherwise the signature might change. Nevertheless, this row is still allowed to reduce the one labelled with $xe_3.$ Thus we highlighted this row in yellow to illustrate this restriction. The row labelled with $xe_3,$ and highlighted in red, is not allowed to reduce any other row. $xe_3$ is the highest signature in degree 3 w.r.t. $<_{\text{pot}},$ thus any reduction of another row would lead to a change in signatures.

Executing all not signature changing reduction steps we end up with a Gröbner basis up to degree 3 represented by the row echelon form

\[
N_3 = \begin{pmatrix}
xe_2 & xe_1 & ye_2 & ye_1 & ye_3 & ze_2 & ze_1 & ze_3 & z & x & y & z
\end{pmatrix}
\]

Next we are computing a Gröbner basis for $\langle f_1, f_2, f_3 \rangle$ up to degree 4. Again we generate the matrix $M_4$ building all combinations of monomials of degree 2 and $f_i$ for $1 \leq i \leq 3$. This time we notice that $M_4$ consists of $\binom{3}{2} \cdot 3 = 18$ rows and $\binom{3}{3} = 15$ columns. This means that when we are reducing $M_4$ we might end up with rows that reduced to zero (or rows that are multiples of others due to the restricted reduction process).
Nevertheless, these rows correspond to useless steps during a Gröbner basis algorithm. So how can we find out which to remove?

A polynomial reduction to zero corresponds to a syzygy in \( \mathbb{R}^3 \). There are principal (or trivial syzygies) we know already without any previous computations: \( f_1 e_2 - f_2 e_1, f_1 e_3 - f_3 e_1 \) and \( f_2 e_3 - f_3 e_2 \). Let us look at the signatures of these syzygies w.r.t. \( <_{\text{pol}} \):

\[
\begin{align*}
\sigma (f_1 e_2 - f_2 e_1) &= \text{lt} (f_1) e_2 = y^2 e_2, \\
\sigma (f_1 e_3 - f_3 e_1) &= \text{lt} (f_1) e_3 = y^2 e_3, \\
\sigma (f_2 e_3 - f_3 e_2) &= \text{lt} (f_2) e_3 = x^2 e_3.
\end{align*}
\]

We have seen in the degree 3 case that we can rewrite elements with a given signature \( T \) by other elements that have the same signature. Thus for \( T \in \{ y^2 e_2, y^2 e_3, x^2 e_3 \} \) we can just use the above syzygies resp. corresponding trivial relations in \( \mathbb{R} \). So the following 3 elements are exchanged, respectively, in \( M_4 \):

\[
\begin{align*}
y^2 f_2 &\quad \rightarrow \quad f_1 f_2 - f_2 f_1, \\
y^2 f_3 &\quad \rightarrow \quad f_1 f_3 - f_3 f_1, \\
x^2 f_3 &\quad \rightarrow \quad f_2 f_3 - f_3 f_2.
\end{align*}
\]

This means that we would add rows that have only zero entries for \( y^2 e_2, y^2 e_3 \) and \( x^2 e_3 \). Those rows do not play any role during the reduction process of \( M_4 \), so we can remove them directly from the matrix. In the end we receive a matrix \( M_4 \) of dimensions \( 15 \times 15 \), thus we know that when reducing \( M_4 \) to its row reduced echelon form \( N_4 \), all rows are useful. Clearly, as we have done for \( M_3 \), we try to rewrite the 15 rows remaining in \( M_4 \) that correspond to elements \( x^i y^j z^l f_i \) with \( 1 \leq i \leq 3 \) and \( j + k + \ell = 2 \) with elements from \( N_2 \) and \( N_3 \) in order to not repeat calculations already done at a lower degree. Computing the row echelon form of \( M_4 \) we then receive a Gröbner basis for \( \langle f_1, f_2, f_3 \rangle \) up to degree 4.

Let us try to summarize the main ideas behind using signatures when computing Gröbner bases:

- Try to rewrite data and reuse already done calculations.
- Keep track of this rewriting by not changing the signatures during the reduction process.
- If the rewritten data is trivial resp. corresponds to a syzygy (relations that are already known) then discard this data.

**Remark 3.1.** Note that building Macaulay matrices as done in Matrix\textsc{F5} is useful and efficient only if the corresponding polynomial system is dense. Otherwise it makes more sense to combine Buchberger’s S-polynomial attempt with linear algebra. That means, one first searches for all S-polynomials in a given degree \( d \) and all needed reducers and generates a corresponding matrix afterwards. This is the main idea behind Faugère’s \textsc{F4} algorithm ( [32]). In Section [13] we present an efficient way of combining signature-based criteria for discarding useless data with \textsc{F4}.

With this in mind we are able to give a more theoretical introduction to signature-based Gröbner basis computations in the vein of Buchberger’s algorithm.

## 4 Gröbner bases with signatures

In this section we give an introduction to signature-based Gröbner basis algorithms from a mathematical point of view. Thus the content is dedicated to a complete and correct description of the algorithms’ underlying ideas. Motivated by the specialized row echelon forms we presented in Section [3] the notion of a polynomial reduction process taking care of the signatures is introduced. Connections and differences to classic polynomial Gröbner basis theory are explained in detail.

Readers interested in the optimized variants only might skip most of this section, but should at least consider notations introduced in Section[2] and here as we agree on those throughout the paper.
4.1 Signature reduction

In order to keep track of the signatures when reducing corresponding polynomial data we need to adjust Definition 2.4. Sloppy speaking we get a classic polynomial reduction together with a further condition.

**Definition 4.1.** Let $\alpha \in R^m$ and let $t$ be a term of $\alpha$. Then we can $s$-reduce $t$ by $\beta \in R^m$ if

1. there exists a monomial $b$ such that $\text{lt}\left(\frac{b \beta}{\alpha}\right) = t$ and
2. $s\left(\frac{b \beta}{\alpha}\right) \leq s\left(\frac{\alpha}{\alpha}\right)$.

The outcome of the $s$-reduction step is then $\alpha - b \beta$ and $\beta$ is called the $s$-reducer. When $\beta$ $s$-reduces $t$ we also say for convenience that $b \beta$ $s$-reduces $\alpha$. That way $b$ is introduced implicitly instead of having to repeat the equation $\text{lt}\left(\frac{b \beta}{\alpha}\right) = t$.

**Remark 4.2.** Note that Condition (a) from Definition 4.1 defines a classic polynomial reduction step (see 2.4). It implies that $\text{lt}\left(\frac{b \beta}{\alpha}\right) \leq \text{lt}(\alpha)$. Moreover, Condition (b) lifts the above implication to $R^m$ so that it involves signatures. Since we are interested in computing Gröbner Bases in $R$ one can interpret an $s$-reduction of $\alpha$ by $\beta$ as classic polynomial reduction of $\alpha$ to $\beta$ together with Condition (b). Thus an $s$-reduction represents a connection between data in $R$ and corresponding data in $R^m$ when a polynomial reduction takes place.

Just as for classic polynomial reduction, if $\text{lt}\left(\frac{b \beta}{\alpha}\right) \approx \text{lt}(\alpha)$ then the $s$-reduction step is a *top* $s$-reduction step and otherwise it is a *tail* $s$-reduction step. Analogously we define the distinction for signatures: If $s\left(\frac{b \beta}{\alpha}\right) \approx s\left(\frac{\alpha}{\alpha}\right)$ then the reduction step is a *singular* $s$-reduction step and otherwise it is a regular $s$-reduction step.

The result of $s$-reduction of $\alpha \in R^m$ as $\gamma \in R^m$ that has been calculated from $\alpha$ through a sequence of $s$-reduction steps such that $\gamma$ cannot be further $s$-reduced. The reduction is a *tail* $s$-reduction if only tail $s$-reduction steps are allowed and it is a *top* $s$-reduction if only top $s$-reduction steps are allowed. The reduction is a *regular* $s$-reduction if only regular $s$-reduction steps are allowed. A module element $\alpha \in R^m$ is *s-reducible* if it can be $s$-reduced.

If $\alpha$ $s$-reduces to $\gamma$ and $\gamma$ is a syzygy then we say that $\alpha$ $s$-reduces to zero even if $\gamma \neq 0$.

**Example 4.3.** Assume an ideal $I = (f_1, f_2, f_3) \subset R = \mathbb{Q}[x, y, z, t]$ with $f_1 = xyz - z^2t$, $f_2 = x^2y - y^3$ and $f_3 = y^3 - zt^2 - t^3$. Furthermore, $<$ denotes the graded reverse lexicographical monomial order which we extend to $<_{\text{pot}}$ on the set of monomials of $R^3$. Clearly, we have $a_i = e_i$ with $\alpha_i = f_i$ for $i \in \{1, 2, 3\}$. We start with $\mathcal{G} = \{a_1, a_2, a_3\}$.

Looking at $x \alpha_2$ we can regular top $s$-reduce $\text{lt}\left(\frac{x \alpha_2}{\alpha_1}\right)$ with $x \alpha_1$, since $\text{lt}\left(\frac{x \alpha_2}{\alpha_1}\right) = \text{lt}\left(\frac{x \alpha_2}{\alpha_3}\right)$ and $s\left(\frac{x \alpha_1}{\alpha_1}\right) <_{\text{pot}} s\left(\frac{x \alpha_2}{\alpha_3}\right)$. Call the resulting element $\alpha_4 = x \alpha_2 - x \alpha_1$. We can see that we cannot further $s$-reduce $\alpha_4$ since $\text{lt}\left(\frac{x \alpha_2}{\alpha_3}\right) = -y^3z + xz^2t$: The only possible candidate is $\alpha_4$ but $s\left(\frac{x \alpha_2}{\alpha_3}\right) <_{\text{pot}} s\left(\frac{x \alpha_2}{\alpha_3}\right) \neq s\left(\frac{x \alpha_2}{\alpha_3}\right)$. Note that $\frac{x \alpha_2}{\alpha_3} + \frac{x \alpha_4}{\alpha_3}$ would be a correct classical polynomial reduction step, but it contradicts Condition (b) of an $s$-reduction. On the other hand, adding $a_4$ to $\mathcal{G}$ we are able to regular top $s$-reduce $x \alpha_3$ w.r.t. $\mathcal{G}$, namely by $a_4$. We see that whereas from a pure polynomial point of view reducing $\alpha_4$ is the same as $\alpha_3 + \alpha_4$ taking the signatures into account destroys this equality. Only the second operation is a valid $s$-reduction.

Again, we can regular top $s$-reduce $x \alpha_4$ with $y^2 \alpha_1$. This gives a new element $\alpha_5 = x \alpha_4 + y^2 \alpha_1$ whereas $\frac{x \alpha_4}{\alpha_5} = x^2z^2t - y^3z^2t$. Looking at $x \alpha_5 = -x^2y^2z + x^3z^2t$ one can use $\text{lt}\left(\frac{x \alpha_5}{\alpha_1}\right)$ to tail $s$-reduce. Note that this $s$-reduction is singular due to $s\left(\frac{x \alpha_5}{\alpha_1}\right) = x^2 z \varepsilon_2 = s\left(\frac{x \alpha_5}{\alpha_1}\right)$. In other words, $x^2 \alpha_4 - x \alpha_5 = (x^2 z \varepsilon_2 - x^3 \varepsilon_1) - (x^2 z \varepsilon_2 - x^3 \varepsilon_1 + x y^2 \varepsilon_1) = -x y^2 \varepsilon_1$. Thus we see that $x^2 \alpha_4$ $s$-reduces to a syzygy $\gamma = x^2 \alpha_4 - x \alpha_5 - x^2 y \alpha_1$.

**Remark 4.4.**

(a) The implied condition $\text{lt}\left(\frac{b \beta}{\alpha}\right) \leq \text{lt}(\alpha)$ is equivalent to $\text{lt}\left(\frac{\alpha - b \beta}{\alpha}\right) \leq \text{lt}(\alpha)$, so during $s$-reduction it is not allowed to increase the lead term. For tail $s$-reduction we perform only those $s$-reduction steps that do not change the lead term at all. Analogously, the condition $s\left(\frac{b \beta}{\alpha}\right) \leq s\left(\frac{\alpha}{\alpha}\right)$ is equivalent to $s\left(\frac{\alpha - b \beta}{\alpha}\right) \leq s\left(\frac{\alpha}{\alpha}\right)$, so during $s$-reduction it is not allowed to increase the signature. For regular $s$-reduction, we perform only those $s$-reduction steps that do not change the signature at all.

(b) Note that by Lemma 15 in [30] the notion of “being singular top $s$-reducible” is equivalent to what is sometimes in the literature also called “sig-redundant”.

12
Note that analogously to the classic polynomial reduction $s$-reduction is always with respect to a finite basis $\mathcal{G} \subseteq \mathbb{R}^m$. The $s$-reducers in $s$-reduction are chosen from the basis $\mathcal{G}$.

### 4.2 Signature Gröbner bases

Having defined a polynomial reduction process taking signatures into account we are now able to define signature Gröbner bases analogously to classic polynomial Gröbner bases.

**Definition 4.5.** Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in $\mathbb{R}$. A finite subset $\mathcal{G}$ of $\mathbb{R}^m$ is a signature Gröbner basis in signature $T$ for $I$ if all $\alpha \in \mathbb{R}^m$ with $s(\alpha) = T$ $s$-reduce to zero w.r.t. $\mathcal{G}$. $\mathcal{G}$ is a signature Gröbner basis up to signature $T$ for $I$ if $\mathcal{G}$ is a signature Gröbner basis in all signatures $S$ such that $S < T$. $\mathcal{G}$ is a signature Gröbner basis for $I$ if it is a signature Gröbner basis for $I$ in all signatures.

**Lemma 4.6.** Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in $\mathbb{R}$. If $\mathcal{G}$ is a signature Gröbner basis for $I$ then $\{ \alpha | \alpha \in \mathcal{G} \}$ is a Gröbner basis for $I$.

**Proof.** For example, see Section 2.2 in [70].

**Convention 4.7.** In the following, when denoting $\mathcal{G} \subseteq \mathbb{R}^m$ “a signature Gröbner basis (up to signature $T$)” we always mean “a signature Gröbner basis (up to signature $T$) for $I = \langle f_1, \ldots, f_m \rangle$.” We omit the explicit notion of the input ideal whenever it is clear from the context.

As in the classic polynomial setting we want to give an algorithmic description of signature Gröbner bases. For this we introduce the notion of $S$-pairs, similar to Definition 2.7.

**Definition 4.8.**

(a) Let $\alpha, \beta \in \mathbb{R}^m$ such that $\overline{\alpha} \neq 0$, $\overline{\beta} \neq 0$ and let $\lambda = \text{lcm}(\text{lt}(\overline{\alpha}), \text{lt}(\overline{\beta}))$ be the monic least common multiple of $\text{lt}(\overline{\alpha})$ and $\text{lt}(\overline{\beta})$. The $S$-pair between $\alpha$ and $\beta$ is given by

$$\text{spair}(\alpha, \beta) := \frac{\lambda}{\text{lt}(\overline{\alpha})}\alpha - \frac{\lambda}{\text{lt}(\overline{\beta})}\beta.$$

(b) $\text{spair}(\alpha, \beta)$ is singular if $s\left(\frac{\lambda}{\text{lt}(\overline{\alpha})}\alpha\right) \approx s\left(\frac{\lambda}{\text{lt}(\overline{\beta})}\beta\right)$. Otherwise it is regular.

Note that $\text{spair}(\alpha, \beta) \in \mathbb{R}^m$ and $\overline{\text{spair}(\alpha, \beta)} = \text{spol}(\overline{\alpha}, \overline{\beta})$.

**Theorem 4.9.** Let $T$ be a module monomial of $\mathbb{R}^m$ and let $\mathcal{G} \subseteq \mathbb{R}^m$ be a finite basis. Assume that all regular $S$-pairs $\text{spair}(\alpha, \beta)$ with $\alpha, \beta \in \mathcal{G}$ and $s(\text{spair}(\alpha, \beta)) < T$ $s$-reduce to zero and all $e_i$ with $e_i < T$ $s$-reduce to zero. Then $\mathcal{G}$ is a signature Gröbner basis up to signature $T$.

**Proof.** For example, see Theorem 2 in [71].

Note the similarity of Theorem 4.9 and Buchberger’s Criterion for Gröbner bases (Theorem 2.8).

The outcome of classic polynomial reduction depends on the choice of reducer, so the choice of reducer can change what the intermediate bases are in the classic Buchberger algorithm. Lemma 4.10 implies that all $S$-pairs with the same signature yield the same regular $s$-reduced result as long as we process $S$-pairs in order of increasing signature.

**Lemma 4.10.** Let $\alpha, \beta \in \mathbb{R}^m$ and let $\mathcal{G}$ be a signature Gröbner basis up to signature $s(\alpha) = s(\beta)$. If $\alpha$ and $\beta$ are both regular top $s$-reduced then $\text{lt}(\overline{\alpha}) = \text{lt}(\overline{\beta})$ or $\overline{\alpha} = \overline{\beta} = 0$. Moreover, if $\alpha$ and $\beta$ are both regular $s$-reduced then $\overline{\alpha} = \overline{\beta}$.

**Proof.** For example, see Lemma 3 in [71].
Let us simplify our notations a bit using facts from the previous statements.

**Notation 4.11.**
(a) Due to Lemma 4.10 we assume in the following that \( \mathcal{G} \) always denotes a finite subset of \( \mathcal{R}^m \) with the property that for \( \alpha, \beta \in \mathcal{G} \) with \( s(\alpha) \simeq s(\beta) \) it follows that \( \alpha = \beta \).
(b) Theorem 4.9 suggests to consider only regular S-pairs for the computation of signature Gröbner bases. Thus in the following “S-pair” always refers to “regular S-pair”.

**Definition 4.12.** A signature Gröbner basis is minimal if no basis element top \( s \)-reduces any other basis element.

Lemma 4.13 implies that the minimal signature Gröbner basis for an ideal \( I \subset \mathcal{R} \) is unique and is contained in all signature Gröbner bases for \( I \) up to sig-lead pairs.

**Lemma 4.13.** Let \( A \) be a minimal signature Gröbner basis and let \( B \) be a signature Gröbner basis for \( \langle f_1, \ldots, f_m \rangle \). Then it holds for all \( \alpha \in A \) that there exists a non-zero scalar \( \kappa \in \mathcal{K} \) and \( \beta \in B \) such that \( s(\alpha) = \kappa s(\beta) \) and \( \text{lt}(\alpha) = \kappa \text{lt}(\beta) \).

**Proof.** This is an easy corollary of Lemma 4.10. \( \square \)

### 5 Generic signature Gröbner basis computation

In the following we present a generic signature-based Gröbner basis algorithm \( \text{genSB} \) (Algorithm 1). This algorithm works the same way as the classic Gröbner basis algorithm presented by Buchberger in [16]. The main difference is that in \( \text{genSB} \) the computations are lifted from \( \mathcal{R} \) to \( \mathcal{R}^m \) in the way presented in sections 4.1 and 4.2.

\( \text{genSB} \) should be understood as a generic description which does not aim on performance. We see in Section 7 how we can vary \( \text{genSB} \) to receive a template that can be used as a common basis from which all known efficient signature-based Gröbner basis algorithms can be derived.

The classic Buchberger algorithm proceeds by reducing S-polynomials. If an S-polynomial reduces to a polynomial \( h \in \mathcal{R} \), \( h \neq 0 \) then \( h \) is added to the basis so that the S-polynomial now reduces to zero by this larger basis. The classic Buchberger algorithm terminates once all S-polynomials between elements of the basis reduce to zero.

\( \text{genSB} \) does the very same with S-pairs using \( s \)-reductions. Based on Theorem 4.9 once all S-pairs \( s \)-reduced to zero w.r.t. \( \mathcal{G} \), \( \text{genSB} \) terminates with a signature Gröbner basis.

**Algorithm 1** Generic signature-based Gröbner basis algorithm \( \text{genSB} \).

| Require: | Ideal \( I = \langle f_1, \ldots, f_m \rangle \subset \mathcal{R} \), monomial order \( \leq \) on \( \mathcal{R} \) and a compatible extension on \( \mathcal{R}^m \), total order \( \succeq \) on the pairset \( \mathcal{P} \) of S-pairs |
|----------|----------------------------------------------------------------------------------------------------------------------------------|
| Ensure:  | Signature Gröbner basis \( \mathcal{G} \) for \( I \), Gröbner basis \( \mathcal{H} \) for \( \text{syz}(f_1, \ldots, f_m) \) |
| 1: \( \mathcal{G} \leftarrow \emptyset \), \( \mathcal{H} \leftarrow \emptyset \) |
| 2: \( \mathcal{P} \leftarrow \{ e_1, \ldots, e_m \} \) |
| 3: while \( \mathcal{P} \neq \emptyset \) do |
| 4: \( \beta \leftarrow \text{min}_\succeq \mathcal{P} \) |
| 5: \( \mathcal{P} \leftarrow \mathcal{P} \setminus \{ \beta \} \) |
| 6: \( \gamma \leftarrow \text{result of regular \( s \)-reducing} \beta \) |
| 7: if \( \exists \gamma = 0 \) then |
| 8: \( \mathcal{H} \leftarrow \mathcal{H} \cup \{ \gamma \} \) |
| 9: else if \( \gamma \) is not singular top reducible then |
| 10: \( \mathcal{P} \leftarrow \mathcal{P} \cup \{ \text{spair}(\alpha, \gamma) \mid \alpha \in \mathcal{G} \text{ and spair}(\alpha, \gamma) \text{ is regular} \} \) |
| 11: \( \mathcal{G} \leftarrow \mathcal{G} \cup \{ \gamma \} \) |
| 12: return \( (\mathcal{G}, \mathcal{H}) \) |
Thinking about correctness and termination of Algorithm \[ \text{Line 6} \] seems to be problematic: Only regular s-reductions are done in \text{genSB}. Moreover, if a reduction ends with an element \( \gamma \) that is singular top s-reducible w.r.t. \( \mathcal{G} \), \( \gamma \) is not even added to \( \mathcal{G} \). It turns out that singular top s-reductions are useless for the computation of signature Gröbner bases.

**Lemma 5.1.** Let \( \alpha \in \mathbb{R}^m \) and let \( \mathcal{G} \) be a signature Gröbner basis up to \( s(\alpha) \). If \( \alpha \) is singular top s-reducible w.r.t. \( \mathcal{G} \) then \( \gamma \) s-reduces to zero w.r.t. \( \mathcal{G} \).

**Proof.** If \( \alpha \) is a singular top s-reducible w.r.t. \( \mathcal{G} \) then there exists \( \beta, b \in \mathbb{R} \) such that \( s(\alpha) = s(b \beta) \) and \( \text{lt}(\alpha) = \text{lt}(b \beta) \). If \( \gamma \) denotes the result of the reduction of \( \alpha \) by \( b \beta \) then \( s(\gamma) < s(\alpha) \). Since \( \mathcal{G} \) is a signature Gröbner basis up to \( s(\alpha) \) \( \gamma \) s-reduces to zero w.r.t. \( \mathcal{G} \).

**Theorem 5.2.** Given \( I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{R} \) and a monomial order \( \preceq \) on \( \mathbb{R} \) with a compatible extension on \( \mathbb{R}^m \)
\text{genSB} is an algorithm that computes a signature Gröbner basis \( \mathcal{G} \) for \( I \) and a module \( \mathcal{H} \) generated by a Gröbner basis for \( \text{syz}(f_1, \ldots, f_m) \).

**Proof.** Correctness of \text{genSB} computing signature Gröbner basis for \( I \) is an easy generalization of Theorem 14 in [30]. Allowing any compatible module monomial order on \( \mathbb{R}^m \) does not change the reasoning of the corresponding proof there. On the other hand, using Lemma 5.1 and the fact that \text{genSB} computes \( \mathcal{G} \) by increasing signatures it is an easy exercise. \( \mathcal{H} \) being a Gröbner basis for \( \text{syz}(f_1, \ldots, f_m) \) is clear by Theorem 5.3.

If \( \preceq \) orders \( \mathcal{P} \) by increasing signatures then termination of \text{genSB} follows by Theorem 20 in [31]. Otherwise it is possible that \text{genSB} adds several elements to \( \mathcal{G} \) with the same signature: Assume an intermediate state of \( \mathcal{G} \) to consist of finitely many elements, thus \( \mathcal{P} \) is finite, too. Next the S-pair \( a \alpha - b \beta \) regular s-reduces to \( \gamma \) w.r.t. \( \mathcal{G} \).

(a) \( \gamma \) is top singular s-reducible and thus not added to \( \mathcal{G} \).

(b) There might exists \( \delta \in \mathcal{G} \) such that \( s(\gamma) = s(\delta) \) but \( \text{lt}(\gamma) < \text{lt}(\delta) \). Note that \( \text{lt}(\gamma) \geq 0 \) so for \( s(\gamma) \) there are only finitely many elements in \( \mathcal{G} \).

In the second situation there must be some element \( e \) added to \( \mathcal{G} \) inbetween \( \gamma \) and \( \delta \) such that \( \text{lt}(\gamma) = \text{lt}(\delta) \) and \( s(ee) < s(\delta) \) for some monomial \( e \) in \( \mathbb{R} \). We need to show that cannot be infinitely many steps between \( \delta \) and \( \gamma \). First of all only finitely many steps of lower signature can be done due to our above discussion: There are only finitely many elements in \( \mathcal{G} \) per signature and there are only finitely many signatures below \( s(\gamma) \) handled since \( \mathbb{R} \) and \( \mathbb{R}^m \) are Noetherian. On the other hand, at the moment \( \delta \) was added to \( \mathcal{G} \), there were only finitely many S-pairs of signature \( > s(\delta) \) in \( \mathcal{P} \). As in the situation above, in order to get a new element in a given signature \( \text{signature} \) \( T \) \( > s(\delta) \) new elements of signature \( < \) \( T \) must be added to \( \mathcal{G} \). Also for \( T \) only finitely many sig-poly pairs are possible. Moreover, between \( s(\delta) \) and \( T \) \text{genSB} handles only finitely many elements, again due to the Noetherianess of \( \mathbb{R} \) and \( \mathbb{R}^m \). All in all, between two elements of the same signature \text{genSB} executes finitely many steps. This completes the proof of \text{genSB}'s termination.

The key to prove that \text{genSB} computes a Gröbner basis \( \mathcal{H} \) for the syzygy module is Theorem 5.3 which implies that we can determine generators of the module of syzygies from looking at those S-pairs and \( e \), that regular s-reduce to zero.

**Theorem 5.3.** Let \( \alpha \in \mathbb{R}^m \) be a syzygy and let \( \mathcal{G} \) be a signature Gröbner basis up to signature \( s(\alpha) \). Then there exists a \( \beta \in \mathbb{R}^m \) with \( s(\beta) \) \( \mathcal{G} \) \( \mathcal{G} \) such that \( \beta \) is an S-pair or has the form \( e \), and such that \( \beta \) regular s-reduces to zero.

**Proof.** The proof is clear by Definition 4.5. A variant of Theorem 5.3 is Proposition 2.2 in [49].

**Remark 5.4.** Note that in [76] Sun and Wang where the first to introduce a description of signature-based Gröbner basis algorithms where the order in which S-pairs are handled does not matter. Clearly, the above description of \text{genSB} covers this, since we do not restrict \( \preceq \). We refer the reader interested in a proof of Theorem 5.2 with an emphasis on the pair set order \( \preceq \) to Theorem 2.2 in [76].

Note that due to \( \preceq \) \( \mathcal{G} \) might not be a signature Gröbner basis up to signature \( T \) when \text{genSB} has just handled an S-pair in signature \( T \). There might be S-pairs of signature \( < \) \( T \) which are still in \( \mathcal{P} \). Nevertheless, once \text{genSB} terminates \( \mathcal{G} \) is a signature Gröbner basis for \( I \) and thus a signature Gröbner basis up to signature \( T \) for all \( T \).
For the sake of efficiency one might choose $\preceq$ to order $\mathcal{P}$ by increasing signatures of the S-pairs. As we see in Section 6 such an order respects the criteria to remove useless S-pairs best.

**Definition 5.5.** $\preceq_s$ denotes the order $\preceq$ in a signature-based Gröbner basis algorithm which sorts $\mathcal{P}$ by increasing signature.

**Lemma 5.6.** Let genSB with $\preceq_s$ pick the next S-pair $\alpha$ to be regular s-reduced such that $s(\alpha) = T$. Then $\mathcal{G}$ is a signature Gröbner basis up to signature $T$.

**Proof.** Since genSB with $\preceq_s$ handles S-pairs by increasing signature this is clear by Definition 4.5. \hfill $\square$

**Corollary 5.7.** genSB with $\preceq_s$ computes a minimal signature Gröbner basis for the corresponding input.

**Proof.** A new element $\gamma$ with $\overline{\gamma} \neq 0$ is added to $\mathcal{G}$ only if $\gamma$ is not singular top s-reducible w.r.t. $\mathcal{G}$. The minimality then follows by Lemma 5.6. \hfill $\square$

**Algorithmic Property 5.8.**

(a) Note that Corollary 5.7 does not hold for arbitrary pair set orders $\preceq$: Assume S-pair $\alpha$ being regular s-reduced by genSB to $\overline{\gamma}$ and $\overline{\gamma} \neq 0$. W.l.o.g. we can assume that $\gamma$ is not singular top s-reducible\(^3\). If, later on, genSB regular s-reduces an S-pair from $\mathcal{P}$ to $\beta$ with $s(\beta) < s(\gamma)$ such that $\text{lt}(\overline{\beta}) | \text{lt}(\overline{\gamma})$ then a new S-pair $\epsilon = b\beta - \gamma$ is handled. Hereby $s(\epsilon) = s(\gamma)$ but $\text{lt}(\overline{\epsilon}) < \text{lt}(\overline{\gamma})$. So $\mathcal{G}$ can have several elements in the same signature $T$.

Still, Lemma 4.11 is valid and makes sense: Once all S-pairs of signature $T$ are handled by genSB (in any given order $\preceq_s$) $\mathcal{G}$ is a signature Gröbner basis up to signature $T$ and $\gamma$ can be further regular s-reduced, namely to $\epsilon$. Thus, in Section 4 and in the following we often consider signature Gröbner bases up to some signature $T$. Due to our considerations here, the second part of Remark 5.4 and Lemma 5.6 this makes sense.

(b) As one can easily see, Algorithm 1 does only rely on data provided by $\overline{\gamma}$ and $s(\alpha)$, but it does not need to store $\alpha$ completely. Thus instead of using $\alpha$ one can optimize an implementation of genSB by using $(s(\alpha), \overline{\gamma})$.

Moreover, if one is only interested in a Gröbner basis for $f_1, \ldots, f_m$, genSB can be optimized in the sense that one can restrict $\mathcal{H}$ to store only the initial module of the corresponding syzygy module: Using only sig-poly pairs in Algorithm 1 we are no longer able to store the full module element $\gamma$ in $\mathcal{H}$ at Line 8.

Still one can compute at the same time the initial submodule $\mathcal{H}$ of the syzygy module of $f_1, \ldots, f_m$. In order to do so, one needs to exchange Line 8 with

8: $\mathcal{H} \leftarrow \mathcal{H} \cup \{s(\gamma)\}$

The fact that one can use signature-based Gröbner basis algorithms to compute the initial module of the module of corresponding syzygies was first mentioned in [465].

Signature-based Gröbner basis algorithms like genSB are in the vein of a bigger class of algorithms computing the image and the kernel of a module homomorphism at the same time: In our setting the image is the signature Gröbner basis $\mathcal{G}$ and the kernel is the syzygy module $\mathcal{H}$. Other well-known, Gröbner basis related algorithms of this type are, for example, the MMM algorithm by Marinari, Möller and Mora (165) and the FGLM algorithm by Faugère, Gianni, Lazard and Mora (165). Recently, Sun gave a nice overview on the connections between those algorithms in [173].

### 6 S-Pair Elimination

Until now we have introduced signature Gröbner bases and their computation only to receive a Gröbner basis for some ideal $(f_1, \ldots, f_m)$ and the initial module of syz $(f_1, \ldots, f_m)$. As mentioned in Section 5 genSB should

\(^3\) Otherwise there exists $\delta \in \mathcal{G}$ with $s(\delta) = cs(\gamma)$ and $\text{lt}(\overline{\delta}) = c\text{lt}(\overline{\gamma})$, thus we can just replace $\gamma$ by $\delta$ in the above situation.
be understood as a template and common basis for all signature-based Gröbner basis algorithms. Thus, it is slow and not at all optimized. One main bottleneck of genSB is the high number of s-reductions to zero. As for the classic Buchberger algorithm (see \cite{16,18}) we are searching for criteria to discard such useless computations in advance like we have used known syzygies in MatrixF5 in Section 3.

Assume that genSB regular s-reduces an S-pair in signature $T$ to $\gamma \in R^m$. Then three different situations can appear:

(a) If $\gamma$ is a syzygy then $\gamma$ is added to $\mathcal{K}$ in Line 8.
(b) If $\gamma$ is not syzygy but singular top s-reducible then by Lemma 5.1 $\gamma$ will s-reduce to zero. Thus it is discarded in Line 9.
(c) Otherwise $\gamma$ is used to build new S-pairs with elements in $\mathcal{G}$ (Line 10) and later on itself added to $\mathcal{G}$ (Line 11).

**Definition 6.1.** For the above three cases $T$ is respectively a syzygy, singular or basis signature.

We are interested in the situations where elements are discarded. In the following we take a closer look at syzygy and singular signatures.

### 6.1 Eliminating S-pairs by known syzygies

Clearly, we receive syzygies by s-reductions to zero in genSB, but there are also syzygies immediately known without precomputations as we have already seen in the example computation of MatrixF5 in Section 3.

**Definition 6.2.** The Koszul syzygy between $\alpha, \beta \in \mathcal{G}$ is $\text{ksyz}(\alpha, \beta) = \overline{\beta} \alpha - \overline{\alpha} \beta$. If $s(\overline{\beta} \alpha) \neq s(\overline{\alpha} \beta)$ then the Koszul syzygy is regular. By “Koszul syzygy” we always mean “regular Koszul syzygy”.

Trivial relations resp. principal syzygies are Koszul syzygies. Using those and already computed zero reductions we are able to flag a given signature being predictably syzygy.

**Definition 6.3.** A signature $T$ is predictably syzygy if there exists a syzygy $\sigma \in R^m$ such that $s(\sigma) < T$ and $s(\sigma) | T$.

Being predictably syzygy gives us a nice characterization when computing Gröbner bases.

**Lemma 6.4 (Syzygy criterion).** Let $\alpha, \beta \in \mathcal{G}$, $\gamma = \text{spair}(\alpha, \beta)$ with $s(\gamma)$ being predictably syzygy, and let $\mathcal{G}$ be a signature Gröbner basis up to $s(\gamma)$. Then $\gamma$ s-reduces to zero w.r.t. $\mathcal{G}$. Moreover, if $S$ is a syzygy signature and $S | T$ then $T$ is also a syzygy signature.

**Proof.** If $\gamma$ is predictably syzygy then there exists a syzygy $\sigma \in R^m$ such that $s(\sigma) = s(\gamma)$, $\overline{\gamma} - \overline{\sigma} = \overline{\sigma}$ but $s(\overline{\gamma} - \overline{\sigma}) < s(\gamma)$. By Definition 4.5 $\gamma - \sigma$ s-reduces to zero w.r.t. $\mathcal{G}$, thus also $\gamma$ behaves in this way. \qed

The outcome of Lemma 6.4 is that whenever we handle an S-pair $\gamma$ in a signature-based Gröbner basis algorithm like genSB whose signature is divisible by the signature of a syzygy we can discard $\gamma$.

**Remark 6.5.** Restricting Lemma 6.4 to principal syzygies and the compatible module monomial order used to $<_{pot}$ we get a statement equivalent to the F5 criterion presented in Theorem 1 in \cite{33}.

### 6.2 Uniqueness of S-pairs at a given signature

Next we are looking at the situation where the s-reduction of an S-pair ends with a non-syzygy element $\gamma$ that is singular top s-reducible w.r.t. $\mathcal{G}$. We have already seen in Lemma 5.1 that we can discard such S-pairs in the computations. The remaining question is how to detect such a situation.

Being singular top s-reducible is a special case of the situation where there are two or more S-pairs in the same signature $T$. If so, we only have to regular s-reduce one of them as they all regular s-reduce to the
same thing by Lemma \[4.10\]. Since $s$-reduction proceeds by decreasing the lead term, we can for example try to speed up the process by choosing an S-pair $\gamma$ in signature $T$ whose lead term $\text{lt}(\gamma)$ is minimal. If $s(\text{spair}(\alpha, \beta)) = s(\alpha\alpha)$, then we get the same result from regular $s$-reducing $\text{spair}(\alpha, \beta)$ as for regular $s$-reducing $aa$ by Notation \[4.11\] (b).

All in all we get the following nice description of the singular criterion:

**Lemma 6.6 (Singular criterion).** For any signature $T$ we need to handle exactly one $aa \in R^m$ from

\[
\mathcal{C}_T = \{aa | a \in \mathcal{G}, a \text{ is a monomial and } s(aa) = T\}
\]

computing a signature Gröbner basis.

**Remark 6.7.**

(a) Note that $a$ might not be involved in any S-pair in signature $T$. In this situation at signature $T$ no S-pair is computed resp. $s$-reduced at all.

(b) Note that when computing signature Gröbner bases by signature-based algorithms with an arbitrary pair set order $\preceq$ uniqueness of the elements in signature $T$ is not guaranteed. A situation as pointed out in Property \[5.8\] (a) might appear and thus after having already chosen and regular $s$-reduced an element from $\mathcal{C}_T$, the algorithm might come back to signature $T$ and makes a new choice from $\mathcal{C}_T$.

(c) Lemma \[6.6\] corresponds to rewriting rows in \text{MatrixF5} as done in Section \[3\] Choosing an element in signature $T$ mirrors searching already reduced row echelon forms $N_d$ for better representations of the row labelled by $T$.

What is now left to do is to make a good choice for $aa$ from $\mathcal{C}_T$. For this we need to introduce the notion of a rewriter in the following.

### 7 Rewrite bases

In Section \[6.2\] we have seen that per signature $T$ we only need to take care of one element. In order to make a choice of such an element we need to define an order on $\mathcal{C}_T$. For this the notion of so-called rewriters is introduced in the following. In this section we present a first signature-based Gröbner basis algorithm using S-pair elimination as presented in Section \[6\] This is then the fundamental algorithm we can derive all known, efficient implementations from.

Similar attempts to achieve such a comprehensive representation of signature-based Gröbner basis algorithms are given, for example, in \[58, 76\]. The algorithms presented there, called \text{TRB} and \text{GBGC} are included in Algorithm \[2\] called \text{RB}. Note that in \[31\] there is already an algorithm called \text{RB}, here we generalized it further.

#### 7.1 Combining elimination criteria

Before we introduce the concept of rewriter, let us shortly recall the syzygy criterion: An element $\gamma$ is discarded if there exists a syzygy $\sigma$ such that $s(\sigma) \mid s(\gamma)$, or in other words, there exists a monomial $s \in R$ such that $s(s\sigma) = s(\gamma)$. Thus we have again two elements of the same signature and need to decide which one to handle. Of course, by Remark \[6.7\] we take $s\sigma$ since we know that $s\sigma = 0$ already, so no further computations need to be done in signature $s(s\sigma)$. But this is nothing else but a rewording of Lemma \[6.4\], the syzygy criterion. It follows that we can generalize the set $\mathcal{C}_T$ to

\[
\mathcal{C}_T = \{aa | a \in \mathcal{G} \cup \mathcal{H}, a \text{ is a monomial and } s(aa) = T\}
\]

The only difference between Equation \[1\] and \[2\] is that $a$ is now allowed to be in $\mathcal{H}$, too. With this the two criteria from Section \[6.1\] and \[6.2\] to find useless S-pairs unite to one single criterion. Furthermore, with this only one question remains to be answered when implementing signature-based Gröbner basis algorithms: How to choose the single element from $\mathcal{C}_T$?

Since we have seen that all elements from $\mathcal{C}_T$ “rewrite” the same information for the input ideal $I = \langle f_1, \ldots, f_m \rangle$ at signature $T$ the following naming conventions are reasonable.
Definition 7.1.

(a) A rewrite order \( \preceq \) is a partial order on \( \mathcal{G} \cup \mathcal{H} \) such that \( \preceq \) is a total order on \( \mathcal{G} \).

(b) An element \( a \in \mathcal{G} \) is a rewriter in signature \( T \) if \( s(a) \mid T \). If for a monomial \( a \in \mathcal{R} \) \( s(aa) = T \) we also say for convenience that \( aa \) is a rewriter in signature \( T \). The \( \preceq \)-maximal rewriter in signature \( T \) is the canonical rewriter in signature \( T \). A multiple \( aa \) of a basis element \( a \) is rewriteable if \( a \) is not the canonical rewriter in signature \( s(aa) \).

Remark 7.2. Of course, the definition of a rewrite order in Definition 7.1 is rather generic and not practical. For example, it does not even take care of the elements in \( \mathcal{H} \). Clearly, for optimized computations one want so be the canonical rewriter in signature \( s(\sigma a) \) for \( \sigma \in \mathcal{H} \). Still, in terms of correctness, one do not need to restrict Definition 7.1 to this. We see in the following how explicitly defined rewrite orders can be used to reach efficient implementations of signature-based criteria to discard useless S-pairs.

Example 7.3. Looking again at Example 4.3 we see that \( x^5 \) is a rewrite basis in all signatures \( S < T \). It turns out that in the general description of rewrite bases we are giving here this need not be true at all. Of course it makes sense to define \( a \preceq b \) whenever \( b \in \mathcal{H} \). We come back to this fact once we are explicitly defining rewrite orders in Section 7.3.

Analogously to Section 3.2 in [31] we introduce next the important notion of a rewrite basis. Note that the combination of the syzygy and the singular criterion lead to a much easier notation. We see in the following a strong connection to signature Gröbner bases.

Definition 7.4. \( \mathcal{G} \) is a rewrite basis in signature \( T \) if the canonical rewriter in \( T \) is not regular top \( s \)-reducible. \( \mathcal{G} \) is a rewrite basis up to signature \( T \) if \( \mathcal{G} \) is a rewrite basis in all signatures \( S < T \). \( \mathcal{G} \) is a rewrite basis if \( \mathcal{G} \) is a rewrite basis in all signatures.

Lemma 7.5. If \( \mathcal{G} \) is a rewrite basis up to signature \( T \) then \( \mathcal{G} \) is also a signature Gröbner basis up to \( T \).

Proof. The special case where a rewrite order is a total order on \( \mathcal{G} \) fulfilling \( s(a) \mid s(\beta) \Rightarrow a \preceq \beta \) is presented in Lemma 8 in [31]. Generalizing this proof to our setting is trivial. \( \square \)

7.2 An algorithm computing rewrite bases

Next we present an algorithm quite similar to Algorithm 1 that implements the above mentioned S-pair elimination in the sense that it computes a rewrite basis. We show that depending on the chosen rewrite order the size of the rewrite basis varies.

Algorithm 2 differs from \texttt{genSB} in three points:

(a) In Line 3 \texttt{RB} directly adds the known Koszul syzygies to \( \mathcal{H} \). This increases the number of possible canonical rewriters in \( \mathcal{H} \) in a given signature \( T \).

(b) In Line 7 \texttt{RB} uses Algorithm 3 to check if the S-pair \( b \) is rewriteable or not. If so, \texttt{RB} discards \( b \) and chooses the next S-pair in \( \mathcal{G} \). \texttt{genSB} does not provide any such check.

(c) In Lines 12 and 13 \texttt{RB} takes the currently regular \( s \)-reduced \( \gamma \), generates new regular S-pairs with it and adds \( \gamma \) to \( \mathcal{G} \). Whereas \texttt{genSB} handles only not singular top \( s \)-reducible \( \gamma \), \texttt{RB} runs these steps on all non-syzygy \( \gamma \).

Whereas the first two points are optimizations compared to \texttt{genSB}, the third change seems to be absurd. We have already seen that singular top \( s \)-reducible elements are not needed for \( \mathcal{G} \), so why adding them? The reason is that \texttt{RB} computes rewrite bases, and in order to fulfill the definition it has to add all these elements to \( \mathcal{G} \) nevertheless they are singular top \( s \)-reducible or not. Since \texttt{RB} depends on the chosen rewrite order \( \preceq \)
Algorithm 2 Rewrite basis algorithm RB.

Require: Ideal $I = \langle f_1, \ldots, f_m \rangle \subseteq \mathbb{R}$, monomial order $\preceq$ on $\mathbb{R}$ and a compatible extension on $\mathbb{R}^n$, total order $\preceq$ on the pairset $\mathcal{P}$ of S-pairs, a rewrite order $\preceq$ on $\mathcal{G} \cup \mathcal{H}$

Ensure: Rewrite basis $\mathcal{G}$ for $I$, Gröbner basis $\mathcal{H}$ for $\text{syz}(f_1, \ldots, f_m)$

1: $\mathcal{G} \leftarrow \emptyset$, $\mathcal{H} \leftarrow \emptyset$
2: $\mathcal{P} \leftarrow \{ e_1, \ldots, e_m \}$
3: $\mathcal{H} \leftarrow \{ fe_j - fe_i \mid 1 \leq i < j \leq m \} \subseteq \mathbb{R}^n$
4: while $\mathcal{P} \neq \emptyset$ do
5: \hspace{1em} $\beta \leftarrow \min_\mathcal{P}$
6: \hspace{1em} $\mathcal{P} \leftarrow \mathcal{P} \setminus \{ \beta \}$
7: \hspace{1em} if not Rewritable ($\beta, \mathcal{G} \cup \mathcal{H}, \preceq$) then
8: \hspace{2em} $\gamma \leftarrow \text{result of regular $s$-reducing } \beta$
9: \hspace{2em} if $\gamma = 0$ then
10: \hspace{3em} $\mathcal{H} \leftarrow \mathcal{H} + \{ \gamma \}$
11: \hspace{2em} else
12: \hspace{3em} $\mathcal{P} \leftarrow \mathcal{P} \cup \{ \text{spair} (\alpha, \gamma) \mid \alpha \in \mathcal{G} \text{ and spair} (\alpha, \gamma) \text{ is regular} \}$
13: \hspace{1em} $\mathcal{G} \leftarrow \mathcal{G} \cup \{ \gamma \}$
14: \hspace{1em} return ($\mathcal{G}, \mathcal{H}$)

Algorithm 3 Rewritability check Rewritable for RB.

Require: S-pair $aa - bb \in \mathbb{R}^m$, finite subset $\mathcal{G} \cup \mathcal{H} \in \mathbb{R}^n$, rewrite order $\preceq$ on $\mathcal{G} \cup \mathcal{H}$

Ensure: “True” if S-pair is rewritable; else “false”

1: if $aa$ is rewritable then return true
2: if $bb$ is rewritable then return true
3: return false

we need to store all elements, since they could lead to new canonical rewriters. We see in Section 7.3 how different rewrite orders can affect RB quite a lot.

Analogously to Theorem 5.2, we receive the following statement.

Theorem 7.6. Given $I = \langle f_1, \ldots, f_m \rangle \subseteq \mathbb{R}$, a monomial order $\preceq$ on $\mathbb{R}$ with a compatible extension on $\mathbb{R}^n$, $\preceq_s$ on $\mathcal{P}$ and a rewrite order $\preceq$ on $\mathcal{G} \cup \mathcal{H}$ is an algorithm that computes a rewrite basis $\mathcal{G}$ for $I$ and a module $\mathcal{H}$ generated by a Gröbner basis for $\text{syz}(f_1, \ldots, f_m)$.

Proof. See [31]: Theorem 7 for correctness and Theorem 20 for termination. □

Algorithmic Property 7.7.

(a) In [31] algorithm RB is presented for the first time. Here RB is presented more general in the sense that different pair set orders are allowed. Moreover, generalizing the idea of rewritability to include the syzygy criterion is new in the current presentation.

(b) If $<_{\text{pot}}$ is used then RB computes $\mathcal{G}$ and $\mathcal{H}$ incremental by increasing indices. Thus it makes sense to optimize Algorithm 2 to recompute $\mathcal{H}$ once the computations in a new index $k$ starts: At this point we have a Gröbner basis $\mathcal{G} = \{ a_1, \ldots, a_{k-1} \} \subseteq \mathbb{R}$ for $\langle f_1, \ldots, f_{i-1} \rangle$. Defining $a_k = e_k$ such that $\overrightarrow{a_k} := f_i$ we can add for $j < k$ $\overrightarrow{a_k} \overrightarrow{a_j} - \overrightarrow{a_k} \overrightarrow{a_j} f_i$ to $\mathcal{H}$.

(c) Note that in spite of Theorem 5.2 we have to limit Theorem 7.6 for RB: Whereas one can show that genSB terminates for any chosen pair set order $\preceq$ we restrict RB to $\preceq_s$. The problem is the interplay between $\preceq_s$ and $\preceq$: It is possible to choose both in a way such that RB adds the same sig-poly pair to $\mathcal{G}$. This is possible due to the fact that RB does not check for singular top $s$-reducibility when adding new elements to $\mathcal{G}$ (since this shall be handled by the more general and flexible rewritability criterion and thus $\preceq_s$).

By the ideas of [76] it is noted in [48] that GVW can compute Gröbner bases by handling S-pairs in any given order. This coincides with our descriptions of genSB and RB. Moreover, we show that not only GVW can do so, but all known efficient implementations of RB, for example, also F5.
(d) Note that there is a strong connection between the signature and the so-called sugar degree. It is shown in [25] that using $\preceq_s$ combined with a degree compatible monomial order $< s$ a signature-based Gröbner basis algorithm refines the sugar degree order of critical pairs.

(e) Since all known signature-based Gröbner basis algorithms are special cases of RB their correctness and termination is clear with Theorem 7.6 Later on, we discuss the topic of termination further, especially for FS in Section 10. There we do not give full proofs, but refer the reader interested in more details on proving termination to the corresponding papers. A small selection might be already mentioned here:

- [31, 45, 56, 69] for FS and variants.
- [3, 31, 43, 68, 70] for GVW, SB and variants.

Note that due to Lemma 5.6, Corollary 5.7 as well as the definition of rewritability in 7.1 choosing Lemma 7.10 (Slight variant of Lemma 11 in [25]) as the best possible choice for an efficient computation of $G$ and $\mathcal{X}$. Thus we restrict ourselves in Theorems 7.6 to this situation.

Moreover, let us agree in the remaining of the paper on the following:

**Convention 7.8.** If not otherwise stated we assume $\preceq = \preceq_s$.

If RB can make use of the rewritability checks, is the resulting rewrite basis, and thus signature Gröbner basis smaller?

**Lemma 7.9.** Given $I = \langle f_1, \ldots, f_m \rangle \subset R$ and a monomial order $\preceq$ on $R$ with a compatible extension on $R^m$ the basis computed by genSB is always a subset of the one computed by RB up to sig-poly pairs.

**Proof.** Due to $\preceq_s$ this follows directly from Corollary 5.7.\qed

The optimization we achieve when switching from genSB to RB lies in the fact that genSB regular s-reduces many more elements to zero w.r.t. $G$, whereas RB can detect, and thus discard, such an s-reduction in advance.

The following two lemmata are of importance when we compare different rewrite rules and specific implementations of RB.

**Lemma 7.10 (Slight variant of Lemma 11 in [31]).** Let $\alpha \in R^m$, let $G$ be a rewrite basis up to signature $s(\alpha)$ and let $t$ be a regular s-reducible term of $T$. Then there exists a regular s-reducer $b\beta$ which is

- not regular top s-reducible,
- not rewritable and
- not syzygy.

**Proof.** Let $M_t$ be the set of all regular s-reducers of $t$. Let $c\gamma \in M_t$ of minimal possible signature $T$, and let $b\beta$ be the canonical rewriter in signature $T$. By definition, $b\beta$ is not rewritable. Since $s(c\gamma) < s(\alpha)$ $b\beta$ is not regular top s-reducible.

Moreover, there cannot exist a $d\delta \in M_t$ such that $d\delta$ regular top s-reduces $c\gamma$ as otherwise $s(d\delta) < T$. By Lemma 4.10 $\text{lt}(b\beta) = \text{lt}(c\gamma)$ and thus $b\beta \in M_t$.

If there exists $\sigma \in \langle \mathcal{X} \rangle$ such that $s(\sigma) = T$ then $b\beta - \sigma \in M_t$ since $b\beta \in M_t$, but $s(b\beta - \sigma) < T$. This is a contradiction.\qed

**Lemma 7.11.** Let $G$ be a rewrite basis up to signature $T$, and let $aa$ be the canonical rewriter in signature $T$. Then RB s-reduces an $S$-pair in signature $T$ if and only if $aa$ is regular top s-reducible and $T$ is not predictably syzygy.

**Proof.** See Lemma 12 in [31].\qed

**Remark 7.12.** In [76] Sun and Wang explain a generalized criterion for signature-based Gröbner basis algorithms which is used in [48] by Gao, Volny and Wang to generalize the original description of the GVW
algorithm given in \cite{47}. For this a partial order on $\mathcal{R}^* \times \mathcal{R}$ is defined. Note that this is included in our combined criterion described in Section 7.1. This is very similar to the rewrite order we defined in 7.1. Still there are some slight differences: Sun and Wang call a partial order on $\mathcal{R}^* \times \mathcal{R}$ admissible if for any S-pair $aa - b\beta$ that $s$-reduced to $\gamma$ with $s(\gamma) = s(aa)$ it holds that $a \preceq \gamma$. Clearly, this is covered by our definition of a rewrite order. Still an admissible partial order could lead to several chains of ordered elements in $\mathcal{G}$ which are not connected to each other. This would mean that a possible canonical rewriter in signature $T$ in chain $C_i$ cannot be used to discard a useless S-pair which consists of a generator in chain $C_j$. So for each chain $C_i$ we would receive an own set of rewriters in signature $T$:

$$\mathcal{C}_{T,C_i} = \{ aa | a \in \mathcal{G} \cup \mathcal{H}, a \text{ is a monomial and } s(aa) = T, a \text{ is in chain } C_i \}.$$ 

Note that correctness and also termination of RB is not effected by this, but the criterion is not as efficient as it is using a total order $\succeq$ on $\mathcal{G}$.

All in all, the efficiency of RB depends on

(a) the order in which S-pairs are handled, and
(b) the strength of the detection of useless S-pairs.

We know already that $\preceq_s$ is the best possible order for $\mathcal{G}$ in terms of the size of the resulting signature Gröbner basis and the efficiency of the $s$-reduction steps. The second point, as well as the size of $\mathcal{G}$ also depend on the chosen rewrite order. So as a final step on our way understanding signature-based Gröbner basis algorithms we have to investigate the overall impact of rewrite orders.

### 7.3 Choosing a rewrite order

When thinking about a possible rewrite order to choose we should look again the set of all possible rewriters in signature $T$:

$$\mathcal{C}_T = \{ aa | a \in \mathcal{G} \cup \mathcal{H}, a \text{ is a monomial and } s(aa) = T \}.$$

We want to choose the canonical rewriter $aa$ in $T$ for further considerations in RB and discard all other elements. It is clear that we want to choose $aa$ in terms of “being easier to $s$-reduce than the other elements in $\mathcal{C}_T$”. From the point of view of Gröbner basis computations there are two canonical selections:

(a) $a$ has been added to $\mathcal{G}$ latest for all $\beta \in \mathcal{H}$ such that $b\beta \in \mathcal{C}_T$. Here we hope that $a$ is better $s$-reduced w.r.t. $\mathcal{G}$ and thus $aa$ might be easier to handle in the following.
(b) Let $\text{lt}(a\alpha) \leq \text{lt}(b\beta)$ for any $b\beta \in \mathcal{C}_T$. Choosing $aa$ as canonical rewriter in signature $T$ we expect the fewest possible $s$-reduction steps.

It turns out that all signature-based Gröbner basis algorithms known until now choose one of the above options. Thus it makes sense to have a closer look at those.

**Definition 7.13.** Let $a, \beta \in \mathcal{G} \cup \mathcal{H}$ during a computation of RB.

(a) We say that $a \preceq_{\text{add}} \beta$ if $\beta \in \mathcal{H}$ or $a$ has been added to $\mathcal{G}$ before $\beta$ is added to $\mathcal{G}$. Break ties arbitrarily.
(b) We say that $a \preceq_{\text{rat}} \beta$ if $s(a) \text{lt}(\beta) < s(\beta) \text{lt}(a\alpha)$ or if $s(a) \text{lt}(\beta) = s(\beta) \text{lt}(a\alpha)$ and $s(a) < s(\beta)$.

**Remark 7.14.**

(a) Using $\preceq_s$ in RB $a \preceq_{\text{add}} \beta$ for $a, \beta \in \mathcal{G}$ induces that $s(a) < s(\beta)$.
(b) The suffix “rat” of $\preceq_{\text{rat}}$ refers to the usual notation of this rewrite order, for example, in \cite{31,45}. There the ratios of the signature and the polynomial lead term are compared:

$$\frac{s(a)}{\text{lt}(a\alpha)} < \frac{s(\beta)}{\text{lt}(\beta)}.$$

Multiplying both sides of the inequality by $\text{lt}(a\alpha) \text{lt}(\beta)$ we get the representation of $\preceq_{\text{rat}}$ as in Definition 7.13 (\cite{9}). We prefer the notation without ratios due to two facts: First of all we do not need to extend $<$ on the ratios and introduce negative exponents. Secondly, we can handle $\text{lt}(a\alpha) = 0$ for elements $a \in \mathcal{H}$.
Lemma 7.15. If there exists \( \gamma \in \mathcal{H} \) such that \( \gamma \in \mathcal{C}_T \) then all \( \alpha \)-pairs in signature \( T \) are discarded in \( \text{RB} \) using either \( \preceq_{\text{add}} \) or \( \preceq_{\text{rat}} \).

Proof. If \( \gamma \in \mathcal{H} \cap \mathcal{C}_T \) then for all \( \alpha \) in \( \mathcal{G} \cap \mathcal{C}_T \) it holds by definition that \( \alpha \preceq_{\text{add}} \gamma \). Furthermore, \( \alpha \preceq_{\text{rat}} \gamma \) due to \( s(\alpha) \log \beta < s(\beta) \log \) where \( \log \beta = 0 \). Thus no S-pair in signature \( T \) is handled by \( \text{RB} \). □

Corollary 7.16. If \( f_1, \ldots, f_m \in \mathcal{R} \) form a regular sequence then there is no \( \alpha \)-reduction to zero while \( \text{RB} \) computes a signature Gröbner basis for \( \langle f_1, \ldots, f_m \rangle \) using \( \prec_{\text{pol}} \).

Proof. The homology of the Koszul complex \( K^* \) associated to the regular sequence \( \langle f_1, \ldots, f_m \rangle \) has the property that \( H_t(K^*) = 0 \) for \( t > 0 \). Thus, there exist only Koszul syzygies of the form \( \overline{\alpha} = \alpha_1 \ldots \alpha_{\ell-1} \in \mathcal{R}^m \) where \( \overline{\alpha} = \{ \alpha_1, \ldots, \alpha_{\ell-1} \} \) is the intermediate Gröbner basis for \( \langle f_1, \ldots, f_{\ell-1} \rangle \) and \( \alpha_k = e_k \in \mathcal{R}^m \) such that \( \sum_{i=1}^{k-1} \alpha_i = f_i \).

Corollary 7.17. If \( f_1, \ldots, f_m \in \mathcal{R} \) form a homogeneous regular sequence then there is no \( \alpha \)-reduction to zero while \( \text{RB} \) computes a signature Gröbner basis for \( \langle f_1, \ldots, f_m \rangle \) using \( \prec_{\text{pol}} \).

Proof. This is clear by Corollary 7.16 and the fact that \( \text{RB} \) computes the signature Gröbner basis for the input ideal by increasing polynomial degree. Thus at each new degree step \( \beta \) is already a \( d' \)-Gröbner basis for \( \langle f_1, \ldots, f_m \rangle \) for all \( d' < d \). □

Another question to answer is why Rewritable is allowed to check both generators of an S-pair and not only the one with higher signature.

Lemma 7.18. Assume \( \text{RB} \) computing a signature Gröbner basis for \( \langle f_1, \ldots, f_m \rangle \) using \( \preceq_{\text{add}} \) or \( \preceq_{\text{rat}} \). If Rewritable returns “true” for input S-pair \( \alpha a - \beta b \), \( s(\alpha a) > s(\beta b) \) due to \( \beta b \) being rewritable then \( \text{RB} \) can discard \( \alpha a - \beta b \).

Proof. If \( \beta b \) is rewritable then there exists \( \gamma \in \mathcal{G} \cup \mathcal{H} \), \( \gamma \neq \beta \) such that \( \gamma \) is the canonical rewriter in \( s(\beta b) \). Let \( s(\gamma) = s(\beta b) \) for some monomial \( c \). Since \( \beta \preceq \gamma \) and \( \gamma \preceq \delta \) is either \( \preceq_{\text{add}} \) or \( \preceq_{\text{rat}} \) it follows from Definition 7.13 that \( \log \beta \geq \log \gamma \). Two situations can happen:

(a) If \( \log \gamma = \log (\beta b) \) then \( \text{RB} \) handles the S-pair \( \alpha a - \gamma c \).

(b) If \( \log \gamma < \log (\beta b) \) then there exists \( \delta_i \in \mathcal{G} \) and monomials \( d_i \) such that \( \beta b = \sum_{i=1}^{\ell} d_i \delta_i + e_\gamma \) and \( s(d_i \delta_i) < s(\beta b) \) for all \( i \in \{1, \ldots, \ell\} \) since \( \mathcal{G} \) is a signature Gröbner basis up to \( s(\beta b) \). Thus \( \text{RB} \) handles for some \( k \in \{1, \ldots, k\} \) \( \alpha a - \delta_k \beta_k \) using \( \langle \alpha, \delta_k \rangle \) for some monomial \( \lambda \geq 1 \). Note that this case includes \( \gamma \in \mathcal{H} \). □

Note that whereas we have to handle elements in \( \mathcal{H} \) explicitly for \( \preceq_{\text{add}} \) there is no need to do so for \( \preceq_{\text{rat}} \): If \( \beta \in \mathcal{H} \) then for any \( \alpha \in \mathcal{G} \) \( s(\alpha) \log (\beta b) = 0 \leq s(\beta) \log (\gamma) \).

Lemma 7.19. If \( \text{RB} \) uses \( \preceq_{\text{rat}} \) as rewrite order then there exists no singular top \( \beta \)-reducible element in \( \mathcal{G} \).

Proof. \( \text{RB} \) only regular \( \beta \)-reduces an S-pair in a non-syzygy signature \( T \) if \( \mathcal{G} \) is not already a rewrite basis in signature \( T \) (see Lemma 7.11), i.e. only if the canonical rewriter \( \alpha a \in \mathcal{G} \) is regular top \( \beta \)-reducible. Let \( \beta b \) be such a regular \( \beta \)-reducer of \( \alpha a \). Let \( \alpha a - \beta b \) regular \( \beta \)-reduce to \( \gamma \). Assume there exists \( \delta \in \mathcal{G} \) such that \( s(\delta) = T \) and \( \log (\delta) = s(\gamma) \). Since \( \alpha a \) is the canonical rewriter in signature \( T \) w.r.t. \( \preceq_{\text{rat}} \) it holds that

\[ \log (\delta) \geq \log (\alpha a) > \log (\gamma) \.

This contradicts the existence of such an element \( \delta \in \mathcal{G} \). □

Corollary 7.20. Using \( \preceq_{\text{rat}} \) as rewrite order \( \text{RB} \) computes a minimal signature Gröbner basis.
The question is now if there exist examples where $\text{RB}$ using $\leq_{\text{add}}$ computes a signature Gröbner basis with more elements than the one achieved by $\text{RB}$ using $\leq_{\text{rat}}$.

**Example 7.21.** Let $\mathcal{K}$ be the finite field with 7 elements and let $\mathcal{R} = \mathcal{K}[x, y, z, t]$. Let $<$ be the graded reverse lexicographical monomial order which we extend to $<_{\text{rat}}$ on $\mathcal{R}$. Consider the input ideal $I$ generated by $f_1 = yz - 2t^2, f_2 = xy + t^2$, and $f_3 = x^2z + 3xt^2 - 2yt^2$. We present the calculations done by $\text{RB}$ using $\leq_{\text{add}}$ in Figure 6.

$$
\begin{array}{|c|c|c|c|}
\hline
\alpha_i \in \mathcal{R} & \text{reduced from} & \text{lt}(\alpha_i) & s(\alpha_i) \\
\hline
\alpha_1 & e_1 & yz & e_1 \\
\alpha_2 & e_2 & xy & e_2 \\
\alpha_3 & \text{spair}(\alpha_2, \alpha_1) = za_2 - xa_1 & xt^2 & z e_2 \\
\alpha_4 & e_3 & x^2z & e_3 \\
\alpha_5 & \text{spair}(\alpha_4, \alpha_2) = ya_4 - xa_2 & y^2t^2 & y e_3 \\
\alpha_6 & \text{spair}(\alpha_4, \alpha_3) = t^2a_4 - xa_3 & z^2t^2 & t e_3 \\
\alpha_7 & \text{spair}(\alpha_6, \alpha_1) = ya_6 - z^2t^2a_1 & y^2t^4 & y^2 e_3 \\
\hline
\end{array}
$$

Fig. 6. Computations for $\text{RB}$ in Example 7.21

$\text{RB}$ with $\leq_{\text{rat}}$ regular $s$-reduce the same S-pairs except the last one: In signature $yt^2e_3$ we have $ya_6, t^2a_5 \in \mathcal{K}yt^2e_3$. $\leq_{\text{add}}$ prefers $ya_6$ over $t^2a_5$, thus the S-pair $ya_6 - z^2t^2a_1$ is handled. $\leq_{\text{rat}}$ on the other hand has $t^2a_5$ as canonical rewriter in signature $yt^2e_3$ as $\text{lt}(t^2a_5) = y^2t^4 < y^2t^2 = \text{lt}(y a_6)$. With this choice no S-pair in signature $yt^2e_3$ is handled and thus $\text{RB}$ terminates.

Note that the canonical rewriter in signature $yt^2e_3$ w.r.t. $\leq_{\text{rat}}$ is not regular top $s$-reducible. So by Lemma 7.11 $\text{RB}$ does not reduce any S-pair in this signature. $\leq_{\text{add}}$ chooses its canonical rewriter $ya_6$ wrong in the sense that $ya_6$ can be further reduced, but only until it reaches $t^2a_5$. Whereas this computation is important for $\text{RB}$ in order to compute a rewrite basis w.r.t. $\leq_{\text{add}}$, it is not needed to achieve a signature Gröbner basis for $I$.

We conclude this section with the following summary: As we have seen $\text{RB}$ is mainly parametrized by three properties:

(a) the monomial order $<$ and its extension to $\mathcal{R}^m$,

(b) the pair set order $\leq$ on $\mathcal{R}$, and

(c) the rewrite order $\leq$.

We see that even though there are so many different notions of signature-based Gröbner algorithms in the literature, all those implementations boil down to variations of two of the above mentioned three orders: All known algorithms have in common to use $\leq_s$ on $\mathcal{R}$.

**Remark 7.22.** Note that such attempts of generalizing the description of signature-based Gröbner basis algorithms have already been done, for example, in [58][68][69][76]. As we have already pointed out in the introduction of this section all of these characterizations are similar and included in our attempt using $\text{RB}$. The difference in notation are rather obvious (see also sections 8–11), thus we relinquish to give comparisons further than the ones depicted already in Sections 6 and 7.

Next we discuss known and efficient implementations of signature-based Gröbner basis algorithms as variants of $\text{RB}$. Note that all algorithms described in the following can be implemented with any compatible extension to the monomial order. When algorithms were initially presented with a fixed module monomial order we take care of this. Still, the only real difference of the implements boils down to the rewrite orders used.

---

4 There is some slight difference in the original presentation of $\text{F5}$ in [63] which is discussed in Property 8.3 [6].
8 Faugère’s F5 algorithm and variants

In 2002 Faugère presented the F5 algorithm (33). This was the first publication of a signature-based Gröbner basis algorithm and introduced the notion of a signature.

In [31] the connection between RB and F5 is already given, so we give a short review and refer for details to that paper. F5, as presented in [33] uses \( \prec_{pot} \) as extension of the underlying monomial order \( \prec \).

Remark 8.1. In [31] it is assumed that F5 uses \( \leq_{\text{add}} \) as its rewrite order. Note that this is not true for the initial presentation of F5 in [33]: F5 uses \( \prec_{pot} \), so it computes incrementally a Gröbner basis for \( \{f_1, \ldots, f_i\} \) for increasing \( i \). For each such index \( i \) the algorithm stores a list of so-called “rewrite rules”: RULE\(_i\). The S-pairs are first taken by minimal possible degree \( d := \deg(\alpha \beta) \) for \( \alpha \beta \) being a generator of an S-pair. Once this choice is done this list of S-pairs, denoted by \( \mathcal{P}_i \), is handled by subalgorithm Spol. There S-pairs are checked by the criteria set and using a corresponding pair set order \( \leq_{\text{add}} \). Still, as discussed in sections 6 and 7 the best possible pair set order is \( \leq_s \) and it is shown in [25] that F5 can easily be equipped with it.

The fact about not handling S-pairs by increasing signatures we describe in more detail in Property 5.3. The problem of ordering the rewrite rules is more difficult: As described in [33], F5 might not use \( \leq_{\text{add}} \) as rewrite order: For F5 the canonical rewriter in signature \( T \) is the element in RULE, which was added last. But at the time of concatenation the S-pairs are not sorted by increasing signature! So the following situation can happen: Assume we have two S-pairs in degree \( d \) with signatures \( \alpha e_i \) and \( \beta e_j \). We can assume that in \( \mathcal{P}_i \) they are ordered like \( [\ldots, \alpha e_i, \ldots, \beta e_j, \ldots] \). Let us assume that both S-pairs are not rewritable, so we reduce both. Now, after \( \mathcal{P}_i \) is sorted by increasing signature, F5 first reduces the S-pair with signature \( \alpha e_i \), to \( \alpha \), and later on the one with signature \( \beta e_j \) to \( \beta \). Generating new S-pairs we could have two S-pairs in \( \mathcal{P}_{i+1} \) with signature \( x \gamma y e_i ; \) spol \((\alpha, \gamma)\) and spol \((\beta, \delta)\). In this situation, F5 would remove spol \((\beta, \delta)\) and keep spol \((\alpha, \gamma)\) since the signature \( \gamma e_i \) was added to RULE\(_i\) after \( \beta e_j \) had been added. So in our notation \( \alpha \) is the canonical rewriter in signature \( x \gamma y e_i \). Clearly, using \( \leq_{\text{add}} \) \( \alpha \) is the canonical rewriter in \( x \gamma y e_i \).

Since \( \beta \) was computed after \( \alpha \) from the algorithm’s point of view \( \beta \) might be the better element. So it makes sense to optimize F5 as presented in [33] to use \( \leq_{\text{add}} \).

Moreover, note that in [31] the authors assume this optimization already. For a complete proof of termination of F5 as presented in [33] we refer the reader to [45].

In the following we assume that F5 uses \( \leq_{\text{add}} \) as rewrite order, then the only difference left from its original description is now the fact that F5 checks the possible \( s \)-reducers \( b \beta \) of an element \( \alpha \) if they are not syzygy and not rewritable.

Lemma 8.2 (Lemma 15 in [31]). Let \( \alpha \in \mathbb{R}^m \), let \( t \) be a term of \( \mathcal{T} \) and let \( \mathcal{G} \) be a rewrite basis up to signature \( s(\alpha) \). Then \( t \) is regular \( s \)-reducible if and only if it is reducible in F5.

Proof. Follows also from Lemma 7.10. □

So from Lemma 8.2 it follows that checking possible reducers by Rewritable in RB does not change the algorithm’s behaviour and is thus optional. In Section 13 we see that the idea of checking the \( s \)-reducers by the criteria comes from a linear algebra point of view.

Let us underline the following characteristics of F5.

\footnote{Strictly speaking this is not completely true, F5 as presented in [33] uses \( \prec_{pot} \) defined by \( \alpha e_i \prec_{pot} \beta e_j \), if and only if \( i > j \) or \( i = j \) and \( \alpha < \beta \). The only difference is to prefer the element of lower index instead of the one of higher index. In order to unify notations we assume in the following that F5 means “F5 uses \( \prec_{pot} \) as module monomial order”.

25
Algorithmic Property 8.3.

(a) Note that, even so we assume the optimization of F5's rewrite order as described in Remark 8.1, F5 still does not completely implement $\leq_{\text{add}}$ but a slightly different rewrite order: The requirement $\alpha \leq \beta$ whenever $\beta \in \mathcal{H}$ from $\leq_{\text{add}}$ is relaxed to $\beta = \text{syz} \{ e_i, e_j \}$ for $1 \leq i < j \leq m$. Thus non-Koszul syzygies in $\mathcal{H}$ have the same priority as elements in $\mathcal{G}$. The idea to improve computations by using zero reductions directly instead was introduced first in an arXiv preprint of [33] by Arri and Perry in 2009 as well as in [45] by Gao, Guan and Volny.

(b) Note that in [33], the F5 algorithm is described in the vein of using linear algebra for the reduction steps (see Section 14 for more details). Instead of ordering the pair set by increasing signatures it is ordered by increasing degree of the corresponding S-polynomial. A subset $\mathcal{P}_d$ of S-pairs at minimal given degree $d$ is then handled by the reduction procedure. There, all these S-pairs (corresponding to degree $d$ polynomials) are sorted by increasing signature. As already discussed in [25], for homogeneous input this coincides with using $\preceq_s$ since then the degree of the polynomial part and the degree of the signature are the same. For inhomogeneous input F5's attempt might not coincide with $\preceq_s$. In [45] Galkin has given a proof for termination of F5 taking care of this situation. Note that in such a situation one might either prefer to use $\preceq_s$ (as pointed out in [25]) or saturate resp. desaturate the elements during the computation of the algorithm.

(c) Furthermore, thinking in terms of linear algebra also explains why in [33] higher signature reductions lead to new S-pairs which are directly added to the ToDo list in subalgorithm TopReduction and not prolonged to the situation when a new element is added $\mathcal{G}$ as it is done in RB: Assuming homogeneous input, in a Macaulay matrix $M_d$ (see, for example, Section 3) all corresponding rows are already stored. Thus a higher signature S-pair (in RB et al. due to single polynomial s-reduction prolonged to a later step) corresponds to a reduction of a row by some other one below. All possible S-pairs of degree $d$ are handled at once thus one can directly execute the new S-pair without generating it later on.

Clearly, the F5 criterion and the Rewritten criterion are just special cases of the syzygy criterion (Lemma 6.4) and the singular criterion (Lemma 6.6), respectively. For even more details on how to translate notions like “canonical rewriter” to F5 equivalents like “rewrite rules” we refer to [31] Section 5.

Moreover, F5 implements the s-reduction process different to the description in RB: Instead of prolonging an s-reduction $\alpha - b \beta$ with a reducer $b \beta$ of signature $s(b \beta) > s(\alpha)$ to the generation of the S-pair $b \beta - \alpha$ later on, F5 directly adds $b \beta - \alpha$ to the todo list of the current degree in Reduction. Assuming homogeneous input this makes sense. Again, we see in Section 13 that this is coming from an F4-style implementation of the s-reduction process.

In the last decade several optimizations and variants of F5 where presented. Using RB we can easily categorize them.

Variants & Specifications 8.4. In [33] three variants of F5 are mentioned shortly without going into detail about their modifications:

(a) F5' denotes a variant of F5 similar to FSR (see Section 8.1) resp. FSC (see Section 8.2). For inhomogeneous input one can optimize computations by homogenizing the computations of the intermediate Gröbner basis $G_i$ for $\{ f_1, \ldots, f_j \}$. Before adding the homogenized $f_{i+1}$ one dehomogenizes $G_i$ and introduces $G_i^{\text{deh}}$ to $B_i$. This $B_i$ can then be used for checks with the syzygy criterion as well as for reduction purposes. We refer to sections 8.1 and 8.2 for details on signature handling in this situation.

(b) F5'' denotes the variant of F5 using $\leq_{\text{MP} \text{-} \text{pot}}$ as compatible module monomial order. Thus, instead of an incremental computation w.r.t. the initial generators $f_1, \ldots, f_m$ the algorithm handles elements by increasing degree. Note that in case of regular input F5'' computes no zero reduction, whereas this is possible for $\leq_{\text{LM} \text{-} \text{pot}}$.

(c) The variant MatrixF5 which uses linear algebra for reduction purposes is described in Section 3 in detail.

Note that besides the variants presented in the following there are even more publications about optimizations and generalizations of the F5 algorithm for computing Gröbner bases, for example, see [39, 41]. Also the main results in these publications are presented for F5, they do not depend on the Gröbner basis algorithm used. Here we are giving a survey especially for signature-based Gröbner basis algorithms, thus taking care of not signature-based tailored research is out of scope of this publication.

Moreover, there are first works in using signature-based criteria for computing involutive bases ( [54, 55]).
8.1 F5R – Improved lower-index s-reduction

In 2005 Stegers reviewed F5 in [72]. There he introduced a new variant of F5 improving the reduction process. Due to the incremental structure of RB when using ≤pot one first computes a signature Gröbner basis for \( \langle f_1, f_2 \rangle \), then for \( \langle f_1, f_2, f_3 \rangle \), and so on. Since the intermediate bases need not be minimal Stegers suggested to use in step \( k \) of the algorithm not \( \mathcal{G}_k \) for reduction purposes. Instead it is preferable to reduce the corresponding Gröbner basis \( \mathcal{G}_k = \{ \alpha \mid \alpha \in \mathcal{G}_{k-1} \} \) to the reduced Gröbner basis \( \mathcal{B}_k \) for \( \langle f_1, \ldots, f_{k-1} \rangle \). Since for all elements handled by RB in iteration step \( k \) the signature has an index \( k \) and all elements in \( \mathcal{G}_{k-1} \) have signature index at most \( k - 1 \) s-reductions are always allowed when using <pot and the signatures need not be checked.

Note that \( \mathcal{B}_{k-1} \) is only used for the reduction purposes, new S-pairs are still generated using elements in \( \mathcal{G}_{k-1} \) since otherwise the signatures would not be correct.

8.2 FSC – Improved S-pair generation

Based on Stegers’ idea, Eder and Perry presented in 2009 the F5C algorithm in [29]. Whereas F5R uses the reduced Gröbner basis \( \mathcal{B}_{k-1} \) for \( \langle f_1, \ldots, f_{k-1} \rangle \) only for reduction purposes, FSC extends this to the generation of new S-pairs in iteration step \( k \).

Once RB finishes computing \( \mathcal{G}_{k-1} \) one reduces the corresponding Gröbner basis \( \mathcal{G}_{k-1} \) to \( \mathcal{B}_{k-1} \) as described above. Let \( \mathcal{B}_{k-1} = \{ e_1, \ldots, e_m \} \), then one introduces \( \mathcal{G}_{k-1} = \{ e_1, \ldots, e_m \} \). Moreover, one has to redefine the homomorphism \( \alpha \rightarrow \overline{\alpha} \) to go from \( \mathcal{R}^m \) to \( \mathcal{R} \) by sending \( e_i \) to \( g_i \) for all \( i \in \{ 1, \ldots, m \} \).

Starting iteration step \( k \), RB now computes the signature Gröbner basis for \( \langle g_1, \ldots, g_m, f_k \rangle \). Of course, at that point another extension of the homomorphism \( \alpha \rightarrow \overline{\alpha} \) has to be done, since now we are mapping \( \mathcal{R}^{m+1} \rightarrow \mathcal{R} \).

We define that \( \mathcal{B}_{m+1} := f_k \).

It is shown in Theorem 32 and Corollary 33 of [29] that with this resetting of the signatures the number of useless s-reductions is not increased, but instead the number of S-pairs generated in step \( k \) is decreased.

Variants & Specifications 8.5.

(a) Due to Property 8.3 (\( e \)) one also wants to implement F5C using \( \leq \text{add} \) in order to use zero reductions directly. In 2011, Eder and Perry denoted this variant F5A in [30].

(b) In [25] Eder improves the idea of F5C slightly: By symbolically generating S-pairs of elements in \( \mathcal{G}_{k-1} \) (they all already reduce to zero) signatures useful for discarding S-pairs in iteration step \( k \) can be made available a bit earlier. Thus, in terms of RB, \( \mathcal{R} \) is initialized not only with the signatures of the Koszul syzygies but also with the signatures of other, already known syzygies. The idea presented there can be used in any incremental signature-based Gröbner basis algorithm. The corresponding variants are denoted, for example, iF5C and iG2V.

8.3 Extended F5 criteria

In 2010, Ars and Hashemi published [5] in which they generalized the F5 criterion and the Rewritten criterion in the sense of using different extensions of the monomial order \( < \) on \( \mathcal{R}^m \). These variants are achieved by using RB not with <pot but one of the following two orders proposed in [5].

**Definition 8.6.** Let \( < \) be a monomial order on \( \mathcal{R} \) and let \( a e_i \) be j be two module monomials in \( \mathcal{R}^m \).

(a) \( a e_i <_j b e_j \) if and only if either

\[
\text{a lt } (e_i) < b \text{ lt } (e_j) \quad \text{or} \quad \text{a lt } (e_i) = b \text{ lt } (e_j) \quad \text{and} \quad \text{lt } (e_i) < \text{lt } (e_j).
\]

\( ^6 \) Note that for \( < \), to be a total order we need to ensure that \( \text{lt } (e_i) \neq \text{lt } (e_j) \) whenever \( i \neq j \). Having the input ideal \( I = \langle f_1, \ldots, f_m \rangle \) this can be achieved by an interreduction of the \( f_i \)’s before entering RB.
An easy way to improve F5's performance over small finite fields is to add the field equations to $\mathcal{H}$. When breaking the first hidden field equations (HFE) challenge in 2003 (see also Figure 1). The improvements in those variants are not specific to signature-based Gröbner basis algorithms, thus we waive to discuss them here.

It is clear that in the future a lot more improvements in this direction can be expected. Exploiting algebraic structures helps to find more syzygies on the one hand and to increase the independence of polynomials on the other hand. Both has a positive influence on the computation of (signature) Gröbner bases.

### 9 Exploiting algebraic structures

In this section we present variants of F5 that use knowledge of underlying algebraic structures in order to improve the computations. Note that there exist more variants doing this besides the 3 ones we are discussing here, see, for example, [39–41]. The improvements in those variants are not specific to signature-based Gröbner basis algorithms, thus we waive to discuss them here.

9.1 F5/2 – Improved computations over $\mathbb{F}_2$

An easy way to improve F5’s performance over small finite fields is to add the field equations to $\mathcal{H}$. When breaking the first hidden field equations (HFE) challenge in 2003 (see also Figure 1). The improvements in those variants are not specific to signature-based Gröbner basis algorithms, thus we waive to discuss them here.

It is clear that in the future a lot more improvements in this direction can be expected. Exploiting algebraic structures helps to find more syzygies on the one hand and to increase the independence of polynomials on the other hand. Both has a positive influence on the computation of (signature) Gröbner bases.

9.1 F5/2 – Improved computations over $\mathbb{F}_2$

An easy way to improve F5’s performance over small finite fields is to add the field equations to $\mathcal{H}$. When breaking the first hidden field equations (HFE) challenge in 2003 (see also Figure 1). The improvements in those variants are not specific to signature-based Gröbner basis algorithms, thus we waive to discuss them here.

It is clear that in the future a lot more improvements in this direction can be expected. Exploiting algebraic structures helps to find more syzygies on the one hand and to increase the independence of polynomials on the other hand. Both has a positive influence on the computation of (signature) Gröbner bases.

### 9.2 An F5 variant for bihomogeneous ideals generated by polynomials of bidegree (1, 1)

In 2012 Faugère, Safey El-Din and Spaenlehauer published a variant of F5 dedicated to multihomogeneous, in particular, bihomogeneous systems generated by bilinear polynomials (see Corollary 7.16). The main result is to exploit the algebraic structure of bilinear systems to enlarge $\mathcal{H}$.

In Corollary 7.16 we see that RB and thus also F5 computes no reduction to zero if the input sequence is regular. Whereas a randomly chosen homogeneous polynomial system is regular, this is not the case for multihomogeneous polynomial systems. Those systems appear, for example, in cryptography or coding theory. Due to the non-regularity F5 does not remove all zero reductions.

Let $f_1, \ldots, f_m \in \mathcal{H}[x_0, \ldots, x_n, y_0, \ldots, y_n]$ be bilinear polynomials, let $F_i$ denote the sequence $f_1, \ldots, f_i$ and let $I_i$ denote the ideal $\langle F_i \rangle$. The main result is that the kernel of the Jacobian matrices $\text{jac}_x(F_i)$ and $\text{jac}_y(F_i)$ w.r.t. $x_0, \ldots, x_n$ and $y_0, \ldots, y_n$, respectively, correspond to those reductions to zero F5 does not detect. In general, all elements in these kernels are vectors of maximal minors of the corresponding Jacobian matrices.

Assuming the incremental structure of F5 by using $<_{pot}$ it is shown that the ideal $I_{i-1} : f_i$ is spanned by $I_{i-1}$ and the maximal minors of $\text{jac}_x(F_{i-1})$ (for $i - 1 > n_x$) and $\text{jac}_y(F_{i-1})$ (for $i - 1 > n_y$). The lead ideal of $I_{i-1} : f_i$ corresponds to the zero reductions associated to $f_i$. In order to get rid of them one needs to get results for the ideals generated by the maximal minors of the Jacobian matrices. In [38] it is shown that in general Gröbner bases for these ideals w.r.t. the graded reverse lexicographical order are linear combinations of the generators. Thus, once a Gröbner basis of $I_{i-1}$ is known (which we can assume due to the incremental
structure of F5) one can efficiently compute a Gröbner basis of \( I_{l-1} : f \). It follows that for generic bilinear systems this variant of F5 does not compute any zero reduction.

It follows that for RB all one has to do is to add the computation of the maximal minors of the jacobian matrices and add the corresponding syzygies resp. signatures to \( \mathcal{X} \) in Line 3 of Algorithm 2.

### 9.3 A\n\( F5 \) variant for SAGBI Gröbner bases

Faugère and Rahmany presented in 2009 an adjusted variant of F5 for computing so-called SAGBI Gröbner bases (\[43\]). A SAGBI Gröbner basis is the analogon of a Gröbner basis for ideals in \( \mathcal{X}(R) \)-subalgebras. We introduce notation as much as needed to explain the changes in F5, in particular, MatrixF5. For more details on the theory of SAGBI bases we refer, for example, to \[60\].

In this subsection let \( G \subseteq GL(n, \mathcal{X}) \) be a subgroup of \( n \times n \) invertible matrices over \( \mathcal{X} \). Moreover, we assume that \( \mathcal{X} \) has characteristic zero or \( p \) such that \( p \) and \( |G| \) are coprime.

**Definition 9.1.**

(a) A polynomial \( f \in \mathcal{R} \) is called invariant (w.r.t. \( G \)) if \( f(Ax) = f(x) \) for all \( A \in G \). The set of all polynomials of \( \mathcal{R} \) invariant w.r.t. \( G \) is denoted \( \mathcal{R}^G \).

(b) For \( |G| < \infty \) the Reynolds operator (for \( G \)) is the map \( \mathcal{R} : \mathcal{R} \rightarrow \mathcal{R}^G \) defined by \( \mathcal{R}(f) = \frac{1}{|G|} \sum_{g \in G} f(gx) \).

**Proposition 9.2 (\[20\]).** Let \( \mathcal{R} \) be the Reynolds operator for a finite group \( G \subseteq GL(n, \mathcal{X}) \). Then the following properties hold:

(a) \( \mathcal{R} \) is \( \mathcal{X} \)-linear.

(b) \( f \in \mathcal{R} \Rightarrow \mathcal{R}(f) \in \mathcal{R}^G \).

(c) \( f \in \mathcal{R}^G \Rightarrow \mathcal{R}(f) = f \).

Even if \( \mathcal{R}^G \) might not be finite dimensional as \( \mathcal{X} \)-vector space, there exists a decomposition in finite dimensional homogeneous components, \( \mathcal{R}^G = \oplus_{d \geq 0} \mathcal{R}_d \). For any term \( t \in \mathcal{R} \), \( \mathcal{R}(t) \) is a homogeneous invariant, called orbit sum. Clearly, the set of orbit sums is a vector space basis for \( \mathcal{R}^G \).

Here we assume that \( f_1, \ldots, f_m \) are homogeneous, invariant polynomials in \( \mathcal{R} \) and \( I \) resp. \( I^G \) represent the ideal generated by \( f_1, \ldots, f_m \) in \( \mathcal{R} \) resp. \( \mathcal{R}^G \).

**Definition 9.3.**

(a) A subset \( F \subseteq I^G \) is a SAGBI Gröbner basis for \( I^G \) (up to degree \( d \)) if \( \{ \lt(f) \mid f \in F \} \) generates the lead ideal of \( I^G \) as an ideal over the algebra \( \{ \lt(f) \mid f \in \mathcal{R}^G \} \) (up to degree \( d \)).

(b) Let \( f, g, p \in \mathcal{R}^G \) such that \( f \neq 0 \neq p \). \( f \) SG-reduces to \( g \) modulo \( p \) if there exists a term \( t \) of \( f \) such that there exists an \( s \) in the set of lead terms of \( \mathcal{R}^G \) such that \( s \lt(p) = t \) and \( g = f - \frac{\mathcal{R}(s)}{\mathcal{R}(p)} \mathcal{R}(g)p \).

Clearly, one can speak of SG-reduction w.r.t. a finite subset \( F \subseteq \mathcal{R}^G \). With this a SAGBI Gröbner basis can be defined similar to a usual Gröbner basis:

**Proposition 9.4.** Let \( F \) be a subset of an ideal \( I^G \subseteq \mathcal{R}^G \). The following are equivalent:

(a) \( F \) is a SAGBI Gröbner basis for \( I^G \).

(b) Every \( h \in I^G \) SG-reduces to zero w.r.t. \( F \).

Note that a SAGBI Gröbner basis might not be finite.

Instead of using elimination techniques in order to compute a SAGBI Gröbner basis for a given ideal \( I^G \subseteq \mathcal{R}^G \) one can use the ideas of Théry who presented in \[82\] a variant of Buchberger’s algorithm.

Faugère and Rahmany use in \[43\] the MatrixF5 description of F5 to present the modifications: Let \( f_1, \ldots, f_m \in \mathcal{R}^G \) be the homogeneous input elements. First one defines the so-called invariant Macaulay matrix \( M_{d,i} \) generated by \( \mathcal{R}(f_{i,k}) \) for \( 1 \leq k \leq i \) and terms \( t_{j,k} \) such that \( \deg(t_{j,k}) = d - \deg(f_j) \). Two modifications to the usual Macaulay matrix have to be made:

\[ \text{Note that } \mathcal{R} = \oplus_{d \geq 0} \mathcal{R}_d \text{ and that the action of } G \text{ preserves the homogeneous components.} \]
or labelling the columns by the usual monomials $m_i$ they are indexed by $\mathcal{N}(m_i)$.

Besides this no further changes need to be done. The variant of $\text{MatrixF5}$ presented here assumes $\preceq_{\text{pot}}$ as module monomial order and $\preceq_{\text{add}}$ as rewrite order. One checks for any row labelled by $\mathcal{N}(t_{jk}e_k)$ if $f_k$ is the canonical rewriter in signature $\sigma(t_{jk}e_k)$ and removes the row otherwise. In the description of $\text{MatrixF5}$ this is equivalent to the existence of a row with corresponding lead term $t_{jk}$ in a matrix that was previously reduced to row echelon form.

10 F5 and the quest of termination

Until 2012 there was still no complete proof of $F5$’s termination given. Thus a lot of variants of $F5$ where published in the meantime which have small adjustments in order to ensure termination.

The main problem with the proof of $F5$’s termination given in $[33]$ is Theorem 2: It assumes that if the input of $F5$ is a regular sequence of homogeneous elements then $F5$ does enlarge the lead ideal after each call of the subalgorithm $\text{Reduction}$. In Section 8 of $[33]$ an example of $F5$ computing a Gröbner basis for a regular sequence of three homogeneous elements is given. In the last call of $\text{Reduction}$ only one element, $r_{10}$, is added to $\mathcal{G}$ with $\text{lt}(\{r_{10}\}) = y^5t^2$. In degree $d = 7$ $F5$ has already added element $r_{8}$ to $\mathcal{G}$ with $\text{lt}(\{r_{8}\}) = y^3t^2$. Thus the statement of Theorem 2, on which the proof of termination of $F5$ in $[33]$ is based on, is not true.

10.1 Proving F5’s termination

At least since Galkin’s proof in $[45]$ termination of $F5$ is clear. Several other publications include proofs of $F5$’s termination, most of them are only slight variants or simplifications of Galkin’s (see $[68, 69]$), some are proving termination for slight variants of $F5$ (see $[31]$). The main idea is based on partitioning $\mathcal{G}$ into sets

$$R_r := \left\{ \alpha_i \mid \text{lt}(\alpha_i) = r \right\}$$

for given ratios $r$. The proof of $F5$’s termination is then done in two steps:

(a) One shows that there are only finitely many non-empty sets $R_r$.

(b) $R_r < \infty$ for any non-empty set $R_r$.

As one can easily see, this attempt can be used for any signature-based Gröbner basis algorithm related to $\text{RB}$, thus also termination of $\text{Gvw}$ and variants (see Section $[11]$) can be handled in the same way.

In $[68]$ and $[69]$ Pan, Hu and Wang present another attempt in proving $F5$’s termination. For this they do not only focus on $F5$ but give generalized algorithms in order to use known termination of algorithms like $\text{Gvw}$ (see Section $[11.5]$). They give a generalized $F5$ algorithm called $\text{F5Gen}$ for which they can easily prove termination in the vein of Eder and Perry’s proof of termination of general signature-based Gröbner basis algorithms given in $[30]$. Both publications use the notation introduced by $\text{G2V}$ resp. $\text{Gvw}$ and then further adopted by Huang in $[53]$. We refer to the corresponding sections $[11.2]$ and $[11.5]$ respectively for a dictionary translating the notation given here to theirs. Moreover, note that $[69]$ takes care of the problem with the insertion of rewrite rules in the original $F5$ algorithm discussed in Remark $[5.1]$. Instead of using lists Rule, for rewrite rules they directly check rewrivatability by the order of elements in $\mathcal{G}$ as done in $\text{RB}$, too. $\text{F5Gen}$ now has a generalized insertion strategy for new elements in $\mathcal{G}$, called $\text{Insert\_F5Gen}$. This mirrors the usage of different rewrite orders $\preceq$ as explained in Section $[7]$ Whereas $[69]$ focusses on $F5$, $[68]$ covers also $\text{Gvw}$ and variants.

In $[31]$ Eder and Roune give an easier proof for $F5$’s termination assuming that $F5$ uses $\preceq_{\text{add}}$ as rewrite order, see Remark $[5.1]$.

10.2 Variants of F5 to ensure termination algorithmically

The following variants are still not deprecated, they generate lower degree bounds for an earlier termination of $F5$. All the changes presented here can easily be transferred to $\text{RB}$. Furthermore, note that all the following
ideas for modifying $F5$ to ensure termination assume homogeneous input. The main difference to proving $F5$'s termination directly as explained in Section 10.1 is that the variants presented next provide algorithmic, termination ensuring modifications to $F5$.

**F5t – Using the Macaulay bound.** In [50] and [51] Gash presents the variant $F5t$ which makes use of the Macaulay bound $M$ (see, for example, [49, 62, 63]) for regular sequences. Once the degree of the polynomials treated in the algorithm exceed $2M$ redundant elements (i.e. elements $\alpha$ such that $\text{lt}(\alpha)$ is already in the lead ideal of the current partly computed Gröbner basis) are added to a different set $D$. Whenever $F5$ returns such a redundant element $\alpha$, $\overline{\alpha}$ is reduced (not $s$-reduced!) completely w.r.t. $G \cup D$. All corresponding signatures and rewrite rules are marked to be invalid. Any newly computed $S$-pair with one generator out of $D$ is handled without signature-based criteria checks and just completely reduced (again, not $s$-reduced!) w.r.t. $G \cup D$. Whereas termination and correctness are ensured in this approach, performance really becomes a problem. Depending on the input it often introduces an enormous number of zero reductions for elements generated out of $D$. Moreover, as for $F5B$, taking care of two different lists of elements at the same time, is a bottleneck, too.

**Using Buchberger’s chain criterion.** In 2005, Ars defended his PhD thesis ([4]). There a different variant of $F5$ is presented which was later on denoted by $F5B$ in [28]. In this variant a degree bound of the algorithm is computed with the help of Buchberger’s chain criterion. Besides the usual pair set $P$ a second set $P^*$ is stored. Whereas $P$ is still used for the actual computations with $F5$ $P^*$ has only the purpose to find a degree bound $d$ for the algorithm. Whenever new $S$-pairs are computed the ones which are not detected by Buchberger’s chain criterion are added to $P^*$. After updating $P^*$ $d$ is set to the highest degree of any $S$-pair in $P^*$. Once the degrees of all $S$-pairs in $P$ exceed $d$ then by Buchberger’s chain criterion the polynomial part of the computed signature Gröbner basis up to degree $d$ is already a Gröbner basis for the input ideal.

*Algorithmic Property 10.1.* $F5B$ uses linear algebra instead of polynomial $s$-reduction. We refer to Section 13 for further details on such an implementation of the reduction process.

**F5+ – Keeping track of redundancy.** In 2011, as a last termination dedicated variant before Galkin’s proof in [45], Eder, Gash and Perry present $F5+$ in [28]. The main contribution is the distinction between so-called “GB-critical pairs” and “$F5$-critical pairs”. A GB-critical pair corresponds to an $S$-pair $aa - b\beta$ whereas $\text{lt}(\alpha)$ and $\text{lt}(\beta)$ are not already in the lead ideal of the current state of the computed Gröbner basis. An $F5$-critical pair is an $S$-pair which does not correspond to a GB-critical pair, i.e. at least one generator is redundant. Whereas GB-critical pairs are needed to be checked for the resulting Gröbner basis, $F5$-critical pairs seem to be superfluous, but this is not always the case: Due to the rewritable signature criterion it might happen that an GB-critical pair is discarded and instead a corresponding $F5$-critical pair is $s$-reduced later on. Only since the $F5$-critical pair is taken care of the algorithm’s correctness is ensured. This means that even if at a given degree $d$ there is no GB-critical pair left, one might need to $s$-reduce corresponding $F5$-critical pairs in this degree. The idea is now to store all, by $F5$’s signature-based criteria discarded GB-critical pairs in a second list $P^*$, and keep all usual critical pairs (resp. $S$-pairs) in $P$. As long as the degree of the currently handled elements in $P$ is smaller or equal to the maximal degree of elements in $P^*$ the algorithm needs to carry on due to the above discussion. Once the degree exceeds the maximal degree of an element in $P^*$ Buchberger’s chain criterion is used: If all elements in $P^*$ can be removed by it then the algorithm can terminate. This is due to the fact that in $P^*$ all for the resulting Gröbner basis needed, but due to rewritings discarded GB-critical pairs are stored. Once it is ensured (by Buchberger’s chain criterion) that those reduce to zero, we know that we already reached a Gröbner basis of the input.

*Algorithmic Property 10.2.* $F5+$ starts checking $P^*$ only once the degree of elements in $P$ exceeds the maximal degree of all GB-critical pairs removed by $F5$’s signature-based criteria, not before. Since $F5B$ does not take care of the connection between $F5$-critical pairs and GB-critical pairs, it has to check $P^*$ in each step. Moreover, $F5+$ stores and checks in $P^*$ only GB-critical pairs that are also discarded by $F5$’s signature-based criteria. Only for such a GB-critical pair a corresponding $F5$-critical pair might be necessary for the correctness of the algorithm.
For a generic system $F5B$ might find a lower degree bound than $F5+$. Moreover, note that both variants are able to terminate the algorithm once a constant is found: Due to checking $\mathcal{P}$ by Buchberger’s chain criterion all other S-pairs are removed at this point.

11 Signature-based Gröbner basis algorithms using $\leq_{\text{rat}}$

Besides $F5$ all other known signature-based Gröbner basis algorithms use $\leq_{\text{rat}}$.\footnote{There are some minor exceptions we take care of in the followng, too.} We can easily see that those instantiations of $RB$, like $GVW$ or $SB$, mostly coincide and just differ in notation.

11.1 Arri and Perry’s work – AP

Aberto Arri released in 2009 a first preprint of his paper with John Perry, \cite{3}. There the first mention of $\leq_{\text{rat}}$ can be found. The paper reviews $F5$’s criteria given in \cite{33} and presents a signature-based Gröbner basis algorithm depending on one criterion only. There it is also called “$F5$ criterion” but it is equivalent to choosing the canonical rewriter in signature $T$ from ‘$\mathcal{P}$’ w.r.t. $\leq_{\text{rat}}$.

\textit{Vocabulary} 11.1. The notions “$\mathcal{P}$-reduction” and ”$\mathcal{P}$-Gröbner basis” coincide with $s$-reduction and signature Gröbner basis, respectively.

\textit{Algorithmic Property} 11.2.

(a) \textit{AP} implements $RB$ with $\leq_{\text{rat}}$ and can use any compatible module monomial order $\prec$.

(b) \textit{AP} is (nearly simultaneously with $G2V$, see Section 11.4) the first signature Gröbner basis algorithm adding signatures of zero reductions directly to $\mathcal{P}$.

(c) \textit{AP}’s $\mathcal{P}$-reduction is (also nearly simultaneously with $G2V$’s implementation of $s$-reduction, see Section 11.4) the first one without checking the reducers with the signature-based criteria (see also Lemma 7.11).

11.2 The TRB algorithm – top reductional basis

Lei Huang was one of the first researchers comparing different signature-based Gröbner basis algorithms. In 2010 he presented his $TRB$ algorithm in \cite{58}, where the name comes from the wording “top reductional basis”.

\textit{Vocabulary} 11.3. A top reductional prime element coincides with the notion “not regular top $s$-reducible” given in Section 4.1 and a top reductional basis is just a signature Gröbner basis.

The $TRB$ algorithm does not focus on efficiency, but is a more general algorithmic presentation of signature-based computations and included in $RB$: In \cite{58} specializations of $TRB$ are given that coincide with other known algorithms, like $TRB-F5$, $TRB-EF5$\footnote{See Section 8.3.} and $TRB-GVW$\footnote{See Section 11.5.}. Moreover, the most optimized variant $TRB-MJ$ is presented which coincides with $RB$ using $\leq_{\text{rat}}$ and $\sqsubseteq_{\mathcal{P}}$. Hereby “MJ” stands for “minimal joint multiplied pair” which corresponds to choose at a given signature $T$ the canonical rewriter with minimal possible lead term, that means using $\leq_{\text{rat}}$.

11.3 The GBGC algorithm – generalized criteria

In 2011, Sun and Wang presented the $GBGC$ algorithm in \cite{76}. This algorithm is also a general one and included in $RB$. This is, besides $RB$, the only signature-based Gröbner basis algorithm that considers different pair set orders $\leq$. As already mentioned in Remark 7.12 $GBGC$ is presented to use partial orders on $\mathcal{G}$ as rewrite orders which is not efficient for discarding useless S-pairs.
Vocabulary 11.4.

(a) The “generalized criterion” the algorithm's name comes from can be directly translated to choosing the canonical rewriter in signature $T$ in $\mathcal{C}_{\text{cal}}$ w.r.t. a given rewrite order $\leq$.

(b) Note that whereas we decide to call the element maximals w.r.t. a rewrite order the canonical rewriter in a given signature, in [76] the minimum is chosen. More particular, $\alpha \leq \beta$ chosen there coincides with $\frac{1}{\alpha} \leq_{\text{rat}} \frac{1}{\beta}$. So GBGC still implements RB with $\leq_{\text{rat}}$, there is just a slight difference in notation.

Algorithmic Property 11.5. GBGC implements the test for regular $s$-reduction considering the coefficients of the signatures. Thus, a reduction of a term $t$ of $\alpha$ with some $b\beta$ such that $s(\alpha) = s(b\beta)$ is called super-regular if the coefficients of $s(\alpha)$ and $s(b\beta)$ differ. This definition comes initially from [46]. By the definitions in Section 4.1 we call this a singular top $s$-reduction.

The following lemma shows that there is no need to consider coefficients of signatures at all, i.e. there cannot exist a super-regular top reduction without a regular top $s$-reduction.

Lemma 11.6. In RB there cannot exist a super-regular reduction of a term $t$ without a regular $s$-reduction of $t$.

Proof. See Fact 24 in [30]. $\square$

Thus GBGC can be completely described by RB.

Variants & Specifications 11.7.

(a) In [78] Sun and Wang use a signature Gröbner basis resulting from a computation of RB to decide the ideal membership problem for $I$. This is straightforward since the polynomial part of $\mathcal{G}$ is already a polynomial Gröbner basis. The other fact is that signatures can be used for the representation problem of an element in $I$. Also this is straightforward, since if you compute with the full module element $\alpha \in \mathcal{R}^m$ the signature Gröbner basis $\mathcal{G}$ stores already the full information. If one is using RB with sig-poly pairs [78] proposes just an algorithm to recover the full module representation of elements in the Gröbner basis.

(b) In 2012, Sun, Wang, Ma and Zhang have presented the SGB algorithm in [81]. SGB is a signature-based Gröbner basis algorithm for computations in algebras of solvable type (for example, see [59]) like the Weyl algebra or quantum groups. As a rewrite order $\leq_{\text{rat}}$ is used, which they denote as “GVW-order”.

Besides adjusting the polynomial arithmetic for the corresponding algebras no changes with respect of the signature-based tools have to be made.

11.4 The G2V algorithm

The G2V algorithm refers to Gao, Guan and Volny and was first presented in 2010. Its description is published in [46]. A high-level implementation in SINGULAR is available under

\[\text{http://www.math.clemson.edu/~sgao/code/g2v.sing}\]

As mentioned already in Property 5.3 G2V was, after the description in [3], the first algorithm who used non-Koszul syzygies directly in the syzygy criterion. The algorithm is described in the vein of F5’s description in [33] and thus based on using $<_{\text{pot}}$ as module monomial order, which leads to an incremental Gröbner basis algorithm.

In [46] the authors describe for the first time how G2V and thus signature-based Gröbner basis algorithms in general can be used to compute a Gröbner basis for the syzygy module, by considering not only the signatures, but the full module representations. Still, this leads to the overhead of carrying out all computations in $\mathcal{R}^m$, too.

Algorithmic Property 11.8. The two most important new features in G2V compared to F5 as presented in [33] are

\[\text{More details on the changes in GVW's rewrite order over the years can be found in Section 11.5.}\]
In order to discuss the second difference, let us first introduce some vocabulary.

It follows that when it comes to signatures, coefficients need not be taken into account at all.

Vocabulary 11.9. In [46] notation is a bit different:

(a) Instead of considering sig-poly pairs \((s(\alpha), \overline{a})\), pairs \((u, v)\) are \(R^2\) are considered. This is possible since \(G2V\) is presented only for \(\prec_{pot}\), thus an incremental computation of \(G\) is achieved. So any signature \(s(\alpha) \in R^m\) is always of the type \(s(\alpha) = se_k\) where \(s \in \mathcal{M}\) and \(k\) is the currently highest index of an element considered. So one can remove \(e_k\) without any problem, since all signatures share this module generator for the current incremental step. So one gets a representation \((s, \overline{a}) \in R^2\) corresponding to \((u, v)\).

(b) Next pairs \((u_1, v_1)\) and \((u_2, v_2)\) are considered. Let \(\lambda = lcm(\text{lt}(v_1), \text{lt}(v_2))\) and define \(t_i := \frac{\lambda}{\text{lt}(\overline{v})}\). Then \((t_1(u_1, v_1), t_2(u_2, v_2))\) is called the J-pair of \((u_1, v_1)\) and \((u_2, v_2)\). This corresponds to the notion of our S-pairs. “\(J\)” denotes “joint”, thus also parts of the J-pair have special notation: In the above setting \(t_i v_i\) are called J-polynomials and \(t_i\text{lt}(u_i)\) are J-signatures.

The other difference to F5 mentioned in Property [11.8] is not so obvious at the first look. Whenever a new \(c \gamma\) may be added to \(G\) the authors state in the pseudo code of the algorithm to “store only one J-pair for each distinct J-signature”. This clearly is a rewritable signature criterion, but no explicit statement on which element shall be kept and which shall be removed. Looking into the \textsc{Singular} code of \(G2V\) provided by the authors (see link above) one can see that in the procedure \textsc{insertPairs} the newly generated element by \(c \gamma\) is taken whereas \(aa\), previously added to \(G\), is removed if \(s(aa) = s(c \gamma)\). Thus \(G2V\) implements \(\leq_{\text{add}}\) as rewrite rule and not \(\leq_{\text{rat}}\). The reason we keep \(G2V\) in this section is that it is the historical predecessor of GVW which uses (in its current version) \(\leq_{\text{rat}}\) (see below).

One difference left is the fact that in the provided code for \(G2V\) only one generator of an S-pair resp. J-pair is stored in \(G\). Thus an S-pair reduction \(aa - b \beta\) might not take place, but instead there might exist a better reducer \(c \gamma\) instead of \(b \beta\). This is an implicit statement of the rewritable criterion on the second generator of the S-pair.

Lemma 11.10. After adding \(aa\) from the S-pair \(aa - b \beta\) to \(G\) in \(G2V\), if there exists another regular top s-reducer \(c \gamma\) of \(aa\) which is not rewritable then \(b \beta\) is rewritable.

Proof. If there exists another regular s-reducer \(\gamma \in G\) which is, at the moment \(aa\) is started to be regular s-reduced, not rewritable, then instead of \(aa - b \beta\) the regular s-reduction \(aa - c \gamma\) takes place for some monomial \(c\). Since \(\text{lt}(b \beta) = \text{lt}(c \gamma)\) and \(s(b \beta), s(c \gamma) < s(aa)\) three situations may happen:

(a) If \(s(c \gamma) = s(b \beta)\) then we can assume w.l.o.g. that \(\gamma\) is the canonical rewriter in signature \(s(b \beta)\). Thus \(b \beta\) is rewritable.

(b) If \(s(c \gamma) > s(b \beta)\) then the S-pair \(c \gamma - b \beta\) has been already s-reduced to an element \(\delta \in G\). Since \(s(\delta) = s(c \gamma)\) and \(G2V\) uses \(\leq_{\text{add}}\) \(\delta\) is the canonical rewriter in signature \(s(c \gamma)\) and thus \(c \gamma\) is rewritable, a contradiction to our assumption.

(c) If \(s(b \beta) > s(c \gamma)\) then the S-pair \(b \beta - c \gamma\) has been already reduced to an element \(\delta \in G\), this time \(s(\delta) = s(b \beta)\). By the same argument as above \(b \beta\) is rewritable.

All in all, \(G2V\) (as presented in [46]) implements \(RB\) with \(\prec_{pot}\) and \(\leq_{\text{add}}\).

Algorithmic Property 11.11. Lemma 11.10 might suggest that \(G2V\) as presented in [46] makes use of the rewritability. Looking at the \textsc{Singular} code provided it turns out that this is not the fact: In procedure \textsc{findReductor} a reducer of the same index is searched for in \(G\). This search starts from the initially added element of current index to \(G\). Thus the first possible regular top s-reducer found might not be a “better” choice, where “better” is meant in terms of the rewrite order \(\leq_{\text{add}}\).
11.5 The GVW algorithm

Later in 2010, Gao, Volny and Wang published [47] in which they describe the algorithm GVW. In this first presentation GVW generalizes G2V in the sense that compatible module monomial orders can be used freely instead of restricting to only $<_{\text{pot}}$. Still, $\preceq_{\text{add}}$ is used as rewrite order in this version of GVW.

The work of Huang (see Section 11.2) and Sun and Wang (see Section 11.3) resulted in an algorithm denoted GVWHS in Volny’s PhD thesis ([83]) in 2011. GVWHS uses $\preceq_{\text{rat}}$ as rewrite order, besides this fact it coincides with GVW.

In 2011 and later, the initial GVW paper [47] has been updated to [48]. There GVW already uses $\preceq_{\text{rat}}$ as rewrite order.

**Vocabulary 11.12.**

(a) In the current state of the GVW paper defining the canonical rewriter w.r.t. $\preceq_{\text{rat}}$ is called eventually super top-reducible resp. covered by $\mathcal{G}$. Moreover, note that a strong Gröbner basis in the setting of the GVW paper coincides with the union $\mathcal{G} \cup \mathcal{H}$ here.

(b) With the above definition of a strong Gröbner bases, speaking of detecting all useless S-pairs resp. J-pairs the “uselessness” needs to be understood in terms of $\mathcal{G} \cup \mathcal{H}$: Clearly, a zero reduction of an S-pair is not useless in these terms since it leads to a new syzygy that is not a multiple of an element of $\mathcal{H}$ already. Thus one needs to be careful and not mix this up with the uselessness of an S-pair w.r.t. a usual polynomial Gröbner basis resp. a signature Gröbner basis $\mathcal{G}$.

Let us sum up the historic development of GVW: G2V implements RB with $<_{\text{pot}}$ and $\preceq_{\text{add}}$. GVW is introduced as G2V with the option to use different compatible module monomial orders, but still implementing $\preceq_{\text{add}}$. Due to the work of Huang ([58]) and Sun and Wang ([76]), GVW nowadays is understood as the algorithm Volny denotes in his PhD thesis as GVWHS: RB with no restriction on the compatible module monomial order and $\preceq_{\text{rat}}$ as rewrite order.

Note that in [49] the 2013 revision of GVW a new step in considering more principal syzygies is added. We discuss this in Section 12.

11.6 The SB algorithm

Roune and Stillman presented the SB algorithm at ISSAC’12 ([70]). As Eder and Roune have already pointed out in [31] SB is RB implemented with $\preceq_{\text{rat}}$ as rewrite order. The RB algorithm presented here is only a slight generalization of the one given in [31], allowing different pair set orders and reduce the syzygy criterion to a special case of the rewritable signature criterion.

**Remark 11.13.** Note that Roune and Stillman lay an emphasis on implementational aspects and data structures. For this purpose an extended version of their ISSAC’12 paper is available ([71]) in which different data representations are compared and discussed extensively.

11.7 The SSG algorithm

In 2012 Galkin described in [44] the SSG algorithm, where “ssg” stands for “simple signature-based”. Comparing SSG to RB both coincide once we choose $\preceq_{\text{rat}}$ as rewrite order. In [44] Galkin defines a partial order $<_{\mathcal{H}}$ on sig-poly pairs ($\mathcal{H}$ denotes the set of all sig-poly pairs) in the following way:

\[
(s(\alpha), \overline{\alpha}) <_{\mathcal{H}} (s(\beta), \overline{\beta}) \iff s(\beta) \text{ lt}(\overline{\alpha}) < s(\alpha) \text{ lt}(\overline{\beta}).
\]

12 Please note that there are different versions of the GVW paper which refer to [47], [48] and [49] respectively.

13 March 2014

14 Note that usually the term strong Gröbner basis denotes special Gröbner bases in polynomial rings over Euclidean domains like $\mathbb{Z}$.
Moreover, syzygies are treated to be smaller w.r.t. \( <_H \) than any non-syzygy. From this it follows that \((s(\alpha), \bar{x}) <_H (s(\beta), \bar{y})\) coincides with \( \frac{1}{\alpha} \leq_{\text{rat}} \frac{1}{\beta} \). In part 4 (b) of the pseudo code of the SSG algorithm the rewritable signature criterion is then implemented in the following way (adjusted to our notation):

\[
\mathcal{S} \leftarrow \mathcal{S} \setminus \left\{ \alpha \in \mathcal{S} \mid \exists \beta \in \mathcal{G} \text{ such that } \frac{1}{\beta} \leq_{\text{rat}} \frac{1}{\alpha} \text{ and } s(\beta) \mid s(\alpha) \right\}
\]

With the above described connection between \( <_H \) and \( \leq_{\text{rat}} \) one directly sees that this is just RB’s rewrite procedure using \( \leq_{\text{rat}} \).

12 Using Buchberger’s criteria in signature-based Gröbner basis algorithms

A natural question coming to one’s mind is how RB’s rewrite criterion is related to Buchberger’s Product and Chain criterion, [16][17][61]. Both predict useless computations in advance, but how do both attempts relate to each other? Does one include the other, or are there cases where one side is not able to cover the other side completely? It turns out that one can easily combine both classes of criteria, even more one can show that the rewrite criterion includes Buchberger’s criteria “most of the time”. It is more or less a question about how much overhead one wants to add to RB in order to track principal syzygies on the go. For a detailed discussion on the algebraic nature of this relation we refer to [27].

In 2008 [50] Gash presented a first discussion on using Buchberger’s Product and Chain criterion in signature-based algorithms. Moreover, Gerdt and Hashemi presented an improved variant of G2V in [54] making use of these criteria. In 2013, Gao, Volny and Wang presented a revised version of GVW in [49] that adds another step to store more principal syzygies. We shortly cover these variants in the following.

12.1 Buchberger’s criteria

Let us give a short review of Buchberger’s Product and Chain criterion:

**Lemma 12.1 (Product criterion [16][17]).** Let \( f, g \in \mathcal{R} \) with \( \text{lcm} \left( \text{lt} \left( f \right) , \text{lt} \left( g \right) \right) = \text{lt} \left( f \right) \text{lt} \left( g \right) \). Then \( \text{spol} \left( f, g \right) \) reduces to zero w.r.t. \( \{ f, g \} \).

In the above situation we also say that the S-polynomial \( \text{spol} \left( f, g \right) \) fulfills the Product criterion.

**Lemma 12.2 (Chain criterion [17][61]).** Let \( f, g, h \in \mathcal{R} \), and let \( G \subset \mathcal{R} \) be a finite subset. If it holds that \( \text{lt} \left( h \right) \mid \text{lcm} \left( \text{lt} \left( f \right) , \text{lt} \left( g \right) \right) \), and if \( \text{spol} \left( f, h \right) \) and \( \text{spol} \left( h, g \right) \) have a standard representation w.r.t. \( G \) resp., then \( \text{spol} \left( f, g \right) \) has a standard representation w.r.t. \( G \).

The question is now how do those criteria relate to the rewrite criterion in signature-based Gröbner basis algorithms. Gash gave a first proof that the Product criterion can be used in a signature-based algorithm without any problem due to the fact that the reductions w.r.t. \( \{ \alpha, \beta \} \) are regular \( s \)-reductions when considering \( \bar{x} = f \) and \( \bar{y} = g \) in Lemma [12.1]. Furthermore Gash proved that a version of Lemma [12.2] where the signatures corresponding to \( f, g, \) and \( h \) are restricted can be used in RB.

In 2014 Eder presented in [27] a proof that the Chain criterion is completely included in the rewrite criterion of RB, without any further restrictions. Moreover, the problem of being not able to predict all zero reductions that are found by the Product criterion is explained there in detail. A small counterexample for RB using \( \text{lt-pot} \) is given. Furthermore, it is still an open question whether RB using \( \text{lt-pot} \) completely covers the Product criterion. So it seems that the relation between Buchberger’s criteria and signature-based ones are depending on the chosen module monomial order.

Also the question of using Buchberger’s criteria in RB is answered, there are two possible implementations of a combination of the criteria: The first one explicitly, the second one more subtle.
12.2 ImpG2V – a Gebauer-Möller-like G2V

In [54], Gerdt and Hashemi present ImpG2V, a variant of G2V. In their variant they add 3 new conditions to be checked which coincides with the three steps in Gebauer-Möller’s implementation of Buchberger’s algorithm, see [53]. Moreover, they show that adding these conditions can be done without corrupting signatures, thus ImpG2V is still a correct and terminating signature-based Gröbner basis algorithm with the rewrite criterion implemented as usual (see Theorem 4.1 in [54]).

Note that due to the results in [27] it is not needed to check the Chain criterion explicitly since it is completely covered by the rewrite criterion.

12.3 GVW’s 2013 revision

In 2013 Gao, Volny and Wang revised GVW again, with the current status being presented in [49]. In this version of GVW a new step is inserted, namely an additional computation of principal syzygies even though the regular s-reduced γ might not fulfill \( \gamma = 0 \). In [49], this is Step 4b (b1) of Figure 3.1. In our notation this would be after Line 11 of Algorithm 2. Even though \( \gamma \) is not zero, all new possible principal syzygies are generated and added to \( \mathcal{H} \). Afterwards \( \mathcal{H} \) is interreduced. This has two impacts:

(a) On the one hand new syzygies might be added such that more useless computations can be predicted and removed in advance. Clearly, with this attempt also all useless computations predicted by Buchberger’s product criterion (representing exactly some of these principal syzygies) are detected, too.

(b) On the other hand a lot of these new principal syzygies added to \( \mathcal{H} \) may have signatures that are just multiples of signatures already available in \( \mathcal{H} \). Thus the overhead might be rather high compared to the benefits.

Clearly, GVW’s attempt adding all possible principal syzygies does not give more information to the rewrite criterion than testing for Buchberger’s product criterion directly and adding the corresponding signature to \( \mathcal{H} \) accordingly. In terms of efficient implementations it seems that checking the product criterion explicitly introduces less overhead than generating new principal syzygies whenever a new element \( \gamma \) is added to \( \mathcal{H} \).

Whereas the first variant adds 1 syzygy resp. signature to \( \mathcal{H} \) when it is needed, the second one always tries to recover all such relations and afterwards checks, which ones can be removed from \( \mathcal{H} \) being just multiples of each other.

13 s-reductions using linear algebra

As already pointed out in Section 8 F5 is presented in [33] in the vein of implementing the s-reduction process using linear algebra. MatrixF5, presented in Section 8, is efficient once the system of polynomial equations is dense. Clearly, this is not always the case, and thus, selecting S-pairs to be reduced is more convenient compared to building full Macaulay matrices at a given degree \( d \). The first presentation of such an S-pair generating algorithm using linear algebra for reduction purposes is the F4 algorithm (32). Here we present a variant of F4 that uses signature-based criteria to detect reductions to zero resp. rows reducing to zero in advance. This leads to smaller changes in the implementation of some subalgorithms of F4 corresponding to the switch from usual polynomial reduction to s-reduction. Albrecht and Perry describe a possible implementation of this, called F4/5 in [2].

Algorithmic Property 13.1. Note that the variant F4/5 described in [2] differs from F5 by more than replacing the polynomial s-reduction by linear algebra:

(a) Instead of incrementally computing the Gröbner basis for \( \langle f_1, \ldots, f_m \rangle \) computations are done by increasing degrees: Whereas F5 proceeds by index first, F4/5 prefers the degree of the polynomials over the index. This corresponds to switching from \( \prec_{pot} \) to \( \prec_{d-pot} \).

(b) Instead of sorting the generators by decreasing index, they are ordered by increasing index (see also Footnote 5).

(c) Due to the switch from \( \prec_{pot} \) to \( \prec_{d-pot} \) the rewrite rules Rule, might not be sorted by increasing degree when only appending new rules as done in [33]. Thus the subalgorithm Add Rule takes care of sorting
Rule: by increasing degree. Note that as mentioned in Remark 8.1 this still need not ensure a sorting of Rule: by increasing signature.

Giving a full description of the ideas behind the F4 algorithm out of scope of this survey, we refer the readers interested to [32]. Here we explain in detail an F4-style variant of RB. With this any known implementation of signature-based Gröbner basis algorithms described in sections 8 and 11 can be modified in the same way to use linear algebra for reduction purposes.

Algorithm 4 Rewrite basis algorithm using linear algebra F4-RB.

Require: Ideal \( I = \langle f_1, \ldots, f_n \rangle \subseteq R \), monomial order \( \preceq \) on \( R \) and a compatible extension on \( R^m \), total order \( \triangleleft \) on the

pairset \( \mathcal{P} \) of S-pairs, a rewrite order \( \preceq \) on \( \mathcal{F} \cup \mathcal{H} \)

Ensure: Rewrite basis \( \mathcal{F} \) for \( I \), Gröbner basis \( \mathcal{H} \) for \( \text{syz}(f_1, \ldots, f_n) \)

1: \( \mathcal{F} \leftarrow \emptyset \), \( \mathcal{H} \leftarrow \emptyset \), \( d \leftarrow 0 \)
2: \( \mathcal{P} \leftarrow \{ e_1, \ldots, e_m \} \)
3: \( \mathcal{H} \leftarrow \{ e_i - e_j \mid 1 \leq i < j \leq m \} \subseteq R^m \)
4: while \( \mathcal{F} \neq \emptyset \) do
5: \( d \leftarrow d + 1 \)
6: \( \mathcal{P}_d \leftarrow \text{Select}(\mathcal{P}) \)
7: \( \mathcal{P} \leftarrow \mathcal{P} \setminus \mathcal{P}_d \)
8: \( \mathcal{L}_d \leftarrow \{ a \alpha, b \beta \mid a \alpha - b \beta \in \mathcal{P}_d \} \)
9: \( \mathcal{L}_d \leftarrow \text{Symbolic Preprocessing}(\mathcal{L}_d, \mathcal{F}) \)
10: \( \mathcal{M}_d \leftarrow \text{matrix gen. by rows corr. to } \overline{aa} \text{ for } a \alpha \in \mathcal{L}_d \) (sorted by signatures)
11: \( \mathcal{N}_d \leftarrow \text{row echelon form of } \mathcal{M}_d \) computed without row swapping
12: \( \mathcal{G}_d \leftarrow \{ \gamma \mid \gamma \text{ corresponding to a row in } \mathcal{N}_d \} \)
13: \( \mathcal{G}_d^+ \leftarrow \{ \gamma \in \mathcal{G}_d \mid \text{lt}(\overline{\gamma}) \neq \text{lt}(\overline{aa}) \text{ for } a \alpha \in \mathcal{L}_d, s(\gamma) = s(aa) \} \)
14: while \( \mathcal{G}_d^+ \neq \emptyset \) do
15: \( \gamma \leftarrow \min(\mathcal{G}_d^+) \)
16: \( \mathcal{G}_d^+ \leftarrow \mathcal{G}_d^+ \setminus \{ \gamma \} \)
17: if \( \gamma = 0 \) then
18: \( \mathcal{H} \leftarrow \mathcal{H} + \{ \gamma \} \)
19: else
20: \( \mathcal{P} \leftarrow \mathcal{P} \cup \{ \text{spair}(a, \gamma) \mid a \in \mathcal{F} \text{ and spair}(a, \gamma) \text{ is regular} \} \)
21: \( \mathcal{F} \leftarrow \mathcal{F} \cup \{ \gamma \} \)
22: return \((\mathcal{F}, \mathcal{H})\)

The main difference between RB and F4-RB is the usage of linear algebra for the reduction process in the later one. Instead of fulfilling s-reductions on each new S-pair, F4-RB implements a variant of F4’s reduction process: In Line 6 we no longer need to choose only one single S-pair as done in RB but a subset of \( \mathcal{P} \) can be taken at once. The generators of those symbolic S-pairs are then stored in \( \mathcal{L}_d \) (Line 8). Subalgorithm Symbolic Preprocessing is then precomputing all possible reducers of the elements in \( \mathcal{L}_d \). Due to the additional structure of the signatures one has to change this part slightly compared to an implementation in the F4 Algorithm. This is discussed in Property 13.3. After all elements needed to execute in the \( d \text{th} \) reduction step of the algorithm are stored in \( \mathcal{L}_d \) a corresponding matrix \( \mathcal{M}_d \) w.r.t. \( \gamma \) is constructed: The rows of \( \mathcal{M}_d \) represent the elements \( \overline{aa} \) for \( a \alpha \in \mathcal{L}_d \), the columns represent the corresponding monomials in \( R \) ordered w.r.t. \( \triangleleft \). As in the Matrix F5 Algorithm each row has a signature, namely \( s(aa) \). As mentioned already in Section 4.1 s-reductions on the polynomial side correspond to fixing an order on the rows in \( \mathcal{M}_d \). Thus the computation of the row echelon form of \( \mathcal{M}_d \) in Line 11 is done without row swapping.

Variants & Specifications 13.2.

(a) As already mentioned in Property 5.8(b) for an efficient implementation one would use \((s(\alpha), \overline{\gamma})\) instead of \( \gamma \) in F4-RB. Algorithm 4 as presented here works with full module elements, that means when computing the row echelon form one needs to keep track of all corresponding module operations in \( a \alpha \) for each such row in \( \mathcal{M}_d \). Focussing on the computation of a Gröbner basis and using only \((s(aa), \overline{\gamma})\) this overhead disappears completely due to the fact that row swaps are not allowed and thus the signatures corresponding to rows in \( \mathcal{M}_d \) do not change throughout the whole process.
In Algorithm 5 we state the pseudo code of a signature respecting variant of Symbolic Preprocessing from [32].

Algorithm 5 Symbolic Preprocessing respecting signatures.

Require: a finite subset \( \mathcal{V} \) of \( \mathbb{R}^m \), a finite subset \( \mathcal{G} \) of \( \mathbb{R}^m \)

Ensure: a finite subset \( \mathcal{V} \) of \( \mathbb{R}^m \)

1: \( D \leftarrow \{ \text{lt} ( \beta ) \mid \beta \in \mathcal{V} \} \)
2: \( C \leftarrow \{ \text{monomials of } \beta \mid \beta \in \mathcal{V} \} \)
3: while \( C \neq D \) do
4: \( m \leftarrow \max (C \setminus D) \)
5: \( D \leftarrow D \cup [m] \)
6: \( \mathcal{Y} \leftarrow 0 \)
7: for \( \gamma \in \mathcal{G} \) do
8: \( \text{if } \exists \gamma \in \mathcal{M} \text{ such that } m = \text{lt} ( \gamma f ) \text{ and not Rewritable } ( \gamma f, \mathcal{G}, \mathcal{H}, \leq ) \text{ then} \)
9: \( \mathcal{Y} \leftarrow \mathcal{Y} \cup \{\gamma f\} \)
10: \( ee \leftarrow \text{element of minimal signature in } \mathcal{Y} \)
11: \( \mathcal{U} \leftarrow \mathcal{U} \cup [ee] \)
12: \( C \leftarrow C \cup \{ \text{monomials of } \gamma f \} \)
13: return \( \mathcal{U} \)

Algorithmic Property 13.3. Algorithm 5 has undergone several small changes compared to the version presented in [32]:

(a) From lines [7] to [9] the algorithm loops over all elements \( \gamma \in \mathcal{G} \) searching for a possible, not rewritable reducer of the monomial \( m \). If successful we add the multiplied reducer to an intermediate set \( \mathcal{Y} \). Instead of the original Symbolic Preprocessing algorithm we do not stop after finding a first possible reducer here. The idea is to take in Line 10 the single reducer \( ee \) of minimal signature from \( \mathcal{Y} \). The smaller the signature of \( ee \) the bigger is the probability that \( ee \) might be an allowed reducer of some other row in \( M_d \) for term \( \text{lt} ( \gamma f ) \).

(b) Let \( aa \in \mathcal{U} \) such that \( m \) is a monomial in \( \overline{aa} \) and \( aa \) is of maximal signature for all such elements in \( \mathcal{U} \). Note that it is still possible that \( s(ee) > s(aa) \). If \( m = \text{lt} ( \overline{aa} ) \) this corresponds to the creation of a new S-pair \( \text{spair} ( e, a ) = ee - aa \). Note that in Algorithm 2 the generation of this S-pair is postponed: There only regular s-reductions are computed in Line 8. S-pair \( \text{spair} ( e, a ) \) is generated in Line 12 first. Moreover, note that there does not exist another reducer \( e' e' \) such that \( m - e' e' \) corresponds to a regular s-reduction since \( ee \) is chosen to be minimal w.r.t. its signature.

(c) Due to Lines 5 and 10 the reducer for \( m \) is uniquely defined. This choice depends on the chosen rewrite order \( \leq \) as well as the module monomial order \( < \). Furthermore, one can exchange Line 10 by another choice, for example, the element in \( \mathcal{Y} \) which is most sparse or the one which has the lowest coefficient bound. Thus using the ideas of [15] is possible. Note that such changes may put a penalty on the efficiency of the algorithm due to introducing many more S-pairs as the chosen reducer might not be of minimal possible signature. Still, correctness and termination are not affected.

An optimization of \( F4 \) given in [32] is the usage of the Simplify subalgorithm: Simplify tries to exchange generators of S-polynomials and found reducers in Symbolic Preprocessing with “better ones”: Polynomial products \( uf \in \mathcal{R} \) are tried to be exchanged by elements \( \#g \) where \( \text{lt} ( g ) = \text{lt} ( tf ) \) for a divisor \( t \) of \( u \). In [32] the normal strategy for choosing critical pairs is used, that means, computations are done by increasing
The implementation is done in the computer algebra system Singular. Polynomials are random dense in the corresponding number of variables. The systems are available under order. The random systems are defined by 3 parameters on the input generators: samples of \( 3 \times 10^6 \) from the field of characteristic \( 32003 \), with graded reverse lexicographical monomial order. In the following we present experimental results of Gröbner basis benchmarks and random systems. All algorithms are officially available in Singular.

Due to the signatures this is not so easy in our setting: What if a simplification of \( a a \) by \( \frac{a}{b} \) leads to \( s\left(\frac{a}{b}\right) > s(aa) \? In Property 13.3 \( \bullet \) we have seen that the rewrite order \( \preceq \) as well as the module monomial order < uniquely define the reducer of a monomial \( m \). This definition incorporates the ideas of Simplify in the signature-based world.

Variants & Specifications 13.4. Let us finish with the following notes on the idea of simplification in F4-like signature-based Gröbner basis algorithms.

(a) Besides the way Simplify is presented in \[32\] other ways of choosing a better reducer are possible. In \[15\] Brickenstein gives various choices. In the signature-based world this is reflected by the different implementations of the rewrite order \( \preceq \) and the module monomial order <.

(b) If we assume \( <_{\text{pot}} \) as module monomial order then we can make use of the incremental behaviour of the computations: Assume that we are computing the Gröbner basis for \( \langle f_1, \ldots, f_i \rangle \) having already computed one for \( \langle f_1, \ldots, f_{i-1} \rangle \), say \( \mathcal{G}_{i-1} \). Now we can implement F4’s Simplify routine without any changes for elements in \( \mathcal{G}_{i-1} \). All reducers from \( \mathcal{G}_{i-1} \) have a lower signature due to its index < \( i \). Thus, as already described in \[33\] we do not need to check them by any criterion. Moreover, simplifying any such reducer by another element from a computation during a previous iteration step the corresponding signature still has index < \( i \). Furthermore, assuming FSC (see Section 8.2) we can assume \( \mathcal{G}_{i-1} \) to be reduced to \( B_{i-1} \) which optimizes the choice of reducers even more. Since adding Simplify to F4-RB respectively Symbolic Preprocessing is straightforward in this situation we do not give explicit pseudo code for this.

(c) Moreover, exchanging \( \mathcal{G}_i^+ \) with \( \mathcal{G}_i \) in the argument of the while loop in Line 12 of Algorithm 4 one can trigger a Simplify-like process: Since all non-zero elements are added to \( \mathcal{G} \), only the S-pairs generated by the best reduced elements are not rewritten. Of course this feature is paid dearly for by generating all the useless S-pairs in first place due to the redundant elements in \( \mathcal{G} \).

14 Experimental results

In the following we present experimental results of Gröbner basis benchmarks and random systems. All systems are computed over a field of characteristic 32003, with graded reverse lexicographical monomial order. The random systems are defined by 3 parameters on the input generators:

HRandom (\# vars=\# equations, minimal degree, maximal degree) (homogeneous)

Random (\# vars=\# equations, minimal degree, maximal degree) (affine)

Polynomials are random dense in the corresponding number of variables. The systems are available under

https://github.com/ederc/singular-benchmarks

The implementation is done in the computer algebra system Singular (\[21\]). Signature-based Gröbner basis algorithms are officially available in Singular starting version 4.0.14.

We do not add timings since we do not want to start a fastest implementation contest. We are interested in presenting the size of the basis, the number of syzygies found and used, the number of reductions as well as the complete number of operations, that means, multiplications. Those are the numbers that are unique to the different variants of signature-based Gröbner basis implementations. Any real new variant might compute numbers different to those presented in the following.

\[15\] All examples in this survey are computed with the commit 5d25c42ce5a7cfe24a13632fa0f7cc6b85961cbb available under https://github.com/Singular/Sources
All algorithms using $\prec_{\text{pot}}$ are implemented with the ideas of F5' resp. F5C, that means, inbetween the incremental steps of computing the signature Gröbner basis the intermediate bases are reduced and new signatures are generated (see Section [5.2]). This leads to three facts:

(a) The number of elements in $\mathcal{H}$ increases. The number is usually much higher than the ones for the computation w.r.t. $\prec_{\text{lt-pot}}$ or $\prec_{\text{d-pot}}$.

(b) The difference in the size of the resulting signature Gröbner basis between using $\leq_{\text{add}}$ and $\leq_{\text{rat}}$ diminishes: Since both computations are starting the last iteration step with the same number of elements (using the reduced Gröbner basis) only differences during the last incremental step are captured. Thus mostly the differences in the size of $\mathcal{G}$ are much bigger for the computations w.r.t. $\prec_{\text{lt-pot}}$.

(c) When counting the number of reduction steps as well as the number of overall operations, one needs to distinguish between the $s$-reductions done by RB and the number of usual reductions done inbetween two incremental steps when interreducing the intermediate Gröbner bases. In the tables below we give for computations w.r.t. $\prec_{\text{pot}}$ the values for $s$-reductions as well as the values for all reductions including the interreduction steps. Clearly, for $\prec_{\text{lt-pot}}$ and $\prec_{\text{d-pot}}$ there is no interreduction due to non-incremental execution.

Remark 14.1.

(a) Note that the behaviour for computations w.r.t. $\prec_{\text{d-top}}$ is not optimal. Choosing this module monomial order leads to very long running times in most of the cases. Thus we do not include the corresponding results.

(b) The differences when adding Buchberger's Product and Chain criterion to RB as described in Section [12] are subtle and do not change the overall behaviour of RB. In order not to overload our tables with even more variants of RB we do not cover those differences here. With the information and discussions given in this survey the reader is able to understand the differences to experimental results given in [27,49,54] which focus on this setting.

We have to distinguish different ways of computation in the following:

(a) RB can fulfill only top $s$-reductions or full $s$-reductions (including tail $s$-reductions).

(b) The examples can be affine or homogeneous.

Note that the differences between only top $s$-reductions and full $s$-reductions are only found in the number of $s$-reductions and the number of operations. Therefore the other tables do not include a differentiation between those two. Next we present the results for homogeneous respectively affine input. These values have two different ways of being used:

(a) The reader new to signature-based Gröbner basis algorithms can get a feeling for the behaviour of this kind of algorithm. One can easily compare the results presented here with the outcome of SINGULAR’s Gebauer-Möller implementation.

(b) For researchers trying to improve signature-based Gröbner basis algorithms those numbers are good reference points in order to see what kind of optimizations are achieved.

The corresponding figures after the corresponding tables give a graphical overview of the behaviour of the different variants for the random systems w.r.t. increasing number of generators.

Moreover note that we stopped the computations for affine random systems at 12 resp. for homogeneous random systems at 13 generators for variants using only top $s$-reductions since running time was too long. For full $s$-reductions we could go on until 14 generators.
14.1 Experimental results for homogeneous systems

| Benchmark   | $<\text{pot}>$ | $<\text{k-pot}>$ | $<\text{d-pot}>$ | $<\text{rat}>$ | $<\text{lt-pot}>$ | $<\text{add}>$ |
|-------------|----------------|-----------------|-----------------|-----------------|-----------------|----------------|
| cyclic-7    | 36             | 36              | 145             | 145             | 36              | 36             |
| cyclic-8    | 244            | 244             | 672             | 672             | 244             | 244            |
| eco-10      | 247            | 247             | 367             | 367             | 247             | 247            |
| eco-11      | 502            | 502             | 749             | 749             | 502             | 502            |
| f-633       | 3              | 3               | 9               | 9               | 3               | 3              |
| f-744       | 190            | 190             | 259             | 259             | 190             | 190            |
| katsura-11  | 0              | 0               | 353             | 353             | 0               | 0              |
| katsura-12  | 0              | 0               | 640             | 640             | 0               | 0              |
| noon-8      | 0              | 0               | 294             | 294             | 0               | 0              |
| noon-9      | 0              | 0               | 682             | 682             | 0               | 0              |
| HRandom(6,2,2) | 0            | 26             | 26              | 26              | 0               | 0              |
| HRandom(7,2,2) | 0            | 49             | 49              | 49              | 0               | 0              |
| HRandom(7,2,4) | 0            | 80             | 80              | 80              | 0               | 0              |
| HRandom(7,2,6) | 0            | 635            | 635             | 635             | 0               | 0              |
| HRandom(8,2,2) | 0            | 102            | 102             | 102             | 0               | 0              |
| HRandom(8,2,4) | 0            | 345            | 345             | 345             | 0               | 0              |
| HRandom(9,2,2) | 0            | 181            | 181             | 181             | 0               | 0              |
| HRandom(10,2,2) | 0           | 339            | 339             | 339             | 0               | 0              |
| HRandom(11,2,2) | 0           | 590            | 590             | 590             | 0               | 0              |
| HRandom(12,2,2) | 0           | 1083           | 1083            | 1083            | 0               | 0              |
| HRandom(13,2,2) | 0           | 1867           | 1867            | 1867            | 0               | 0              |
| HRandom(14,2,2) | 0           | 3403           | 3403            | 3403            | 0               | 0              |

Table 2. # zero reductions (homogeneous)
| Benchmark                  | only top s-reductions | full s-reductions |
|---------------------------|-----------------------|-------------------|
|                           | $\leq_{\text{pot}}$ | $\leq_{\text{d-pot}}$ | $\leq_{\text{pot}}$ | $\leq_{\text{d-pot}}$ |
|                           | $\leq_{\text{add}}$ | $\leq_{\text{rat}}$ | $\leq_{\text{add}}$ | $\leq_{\text{rat}}$ |
| cyclic-7 (incl. interred) | 217.181              | 217.992            | 218.237              | 218.123            |
|                           | 217.455              | 217.209            | 218.094              | 217.630            |
| cyclic-8 (incl. interred) | 222.575              | 221.346            | 222.755              | 222.331            |
|                           | 222.067              | 221.156            | 223.638              | 223.325            |
| eco-10 (incl. interred)   | 19.038               | 18.726             | 19.053               | 19.053             |
|                           | 20.984               | 21.007             | 20.984               | 21.007             |
| f-633 (incl. interred)    | 23.567               | 23.604             | 23.521               | 23.521             |
|                           | 23.567               | 23.604             | 23.521               | 23.521             |
| f-744 (incl. interred)    | 29.846               | 29.713             | 29.726               | 29.726             |
|                           | 29.846               | 29.713             | 29.726               | 29.726             |
| katsura-11 (incl. interred)| 17.126              | 17.121             | 17.126               | 17.126             |
|                           | 17.126               | 17.121             | 17.126               | 17.126             |
| noon-8 (incl. interred)   | 18.506               | 18.560             | 18.506               | 18.560             |
|                           | 18.506               | 18.560             | 18.506               | 18.560             |
| noon-9 (incl. interred)   | 18.560               | 18.680             | 18.560               | 18.680             |
|                           | 18.560               | 18.680             | 18.560               | 18.680             |
| HRandom(6, 2, 2) (incl. interred)| 16.822            | 16.822            | 16.822               | 16.822            |
| HRandom(7, 2, 2) (incl. interred)| 19.082            | 21.094            | 19.082               | 21.094            |
| HRandom(7, 2, 4) (incl. interred)| 13.327            | 13.327            | 13.327               | 13.327            |
| HRandom(7, 2, 6) (incl. interred)| 20.604            | 20.604            | 20.604               | 20.604            |
| HRandom(7, 2, 8) (incl. interred)| 21.354            | 21.354            | 21.354               | 21.354            |
| HRandom(8, 2, 2) (incl. interred)| 24.421            | 24.421            | 24.421               | 24.421            |
| HRandom(8, 2, 4) (incl. interred)| 15.431            | 15.538            | 15.431               | 15.538            |
| HRandom(8, 2, 6) (incl. interred)| 20.638            | 20.638            | 20.638               | 20.638            |
| HRandom(8, 2, 8) (incl. interred)| 21.606            | 21.606            | 21.606               | 21.606            |
| HRandom(9, 2, 2) (incl. interred)| 21.666            | 21.666            | 21.666               | 21.666            |
| HRandom(9, 2, 4) (incl. interred)| 21.635            | 21.635            | 21.635               | 21.635            |
| HRandom(10, 2, 2) (incl. interred)| 17.596            | 17.679            | 17.596               | 17.679            |
| HRandom(10, 2, 4) (incl. interred)| 19.493            | 19.949            | 19.493               | 19.949            |
| HRandom(11, 2, 2) (incl. interred)| 20.187            | 20.187            | 20.187               | 20.187            |
| HRandom(12, 2, 2) (incl. interred)| 19.093            | 19.093            | 19.093               | 19.093            |
| HRandom(13, 2, 2) (incl. interred)| 20.345            | 20.345            | 20.345               | 20.345            |
| HRandom(14, 2, 2) (incl. interred)| 20.004            | 20.004            | 20.004               | 20.004            |
| HRandom(15, 2, 2) (incl. interred)| 20.524            | 20.524            | 20.524               | 20.524            |

Table 5. $\leq s$-reductions (incl. interreductions) (homogeneous)
| Benchmark          | <pot | only top s-reductions | full s-reductions |
|--------------------|------|-----------------------|-------------------|
|                    | $S_{add}$ | $S_{rat}$ | $S_{add}$ | $S_{rat}$ | $S_{add}$ | $S_{rat}$ | $S_{add}$ | $S_{rat}$ |
| cyclic-7 (incl. interred) | 24.276 | 23.871 | 24.024 | 23.996 | 23.851 | 23.467 | 24.050 | 23.598 | 24.130 | 23.709 | 24.062 | 23.578 | 24.319 | 23.866 |
| cyclic-8 (incl. interred) | 21.017 | 20.896 | 20.867 | 20.836 | 20.867 | 20.836 | 20.867 | 20.836 | 20.963 | 20.927 | 20.932 | 20.905 |
| eco-10 (incl. interred) | 24.854 | 24.691 | 24.478 | 24.507 | 24.954 | 24.656 | 24.954 | 24.656 | 24.854 | 24.691 | 24.478 | 24.507 |
| eco-11 (incl. interred) | 27.765 | 27.629 | 27.634 | 27.643 | 27.634 | 27.643 | 27.634 | 27.643 | 27.765 | 27.629 | 27.634 | 27.643 |
| f-633 (incl. interred) | 27.881 | 27.392 | 27.686 | 27.707 | 27.686 | 27.707 | 27.686 | 27.707 | 27.881 | 27.392 | 27.686 | 27.707 |
| katsura-11 (incl. interred) | 30.655 | 30.500 | 30.655 | 30.500 | 30.655 | 30.500 | 30.655 | 30.500 | 30.655 | 30.500 | 30.655 | 30.500 |
| katsura-12 (incl. interred) | 33.729 | 33.679 | 33.729 | 33.679 | 33.729 | 33.679 | 33.729 | 33.679 | 33.729 | 33.679 | 33.729 | 33.679 |
| noon-8 (incl. interred) | 28.100 | 27.867 | 28.100 | 27.867 | 28.100 | 27.867 | 28.100 | 27.867 | 28.100 | 27.867 | 28.100 | 27.867 |
| noon-9 (incl. interred) | 28.300 | 28.285 | 28.300 | 28.285 | 28.300 | 28.285 | 28.300 | 28.285 | 28.300 | 28.285 | 28.300 | 28.285 |
| HRandom(6, 2, 2) (incl. interred) | 21.628 | 21.412 | 21.628 | 21.412 | 21.628 | 21.412 | 21.628 | 21.412 | 21.628 | 21.412 | 21.628 | 21.412 |
| HRandom(7, 2, 2) (incl. interred) | 21.502 | 21.515 | 21.502 | 21.515 | 21.502 | 21.515 | 21.502 | 21.515 | 21.502 | 21.515 | 21.502 | 21.515 |
| HRandom(7, 2, 4) (incl. interred) | 21.537 | 21.570 | 21.537 | 21.570 | 21.537 | 21.570 | 21.537 | 21.570 | 21.537 | 21.570 | 21.537 | 21.570 |
| HRandom(7, 2, 6) (incl. interred) | 21.515 | 21.570 | 21.515 | 21.570 | 21.515 | 21.570 | 21.515 | 21.570 | 21.515 | 21.570 | 21.515 | 21.570 |
| HRandom(8, 2, 2) (incl. interred) | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 |
| HRandom(8, 2, 4) (incl. interred) | 21.558 | 21.598 | 21.558 | 21.598 | 21.558 | 21.598 | 21.558 | 21.598 | 21.558 | 21.598 | 21.558 | 21.598 |
| HRandom(9, 2, 2) (incl. interred) | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 |
| HRandom(10, 2, 2) (incl. interred) | 21.517 | 21.610 | 21.517 | 21.610 | 21.517 | 21.610 | 21.517 | 21.610 | 21.517 | 21.610 | 21.517 | 21.610 |
| HRandom(11, 2, 2) (incl. interred) | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 |
| HRandom(12, 2, 2) (incl. interred) | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 |
| HRandom(13, 2, 2) (incl. interred) | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 | 21.430 | 21.453 |
| HRandom(14, 2, 2) (incl. interred) | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 | 21.351 | 21.426 |

Table 6. # multiplications (incl. interreductions) (homogeneous)
14.2 Experimental results for affine systems

| Benchmark  | $\mathcal{S}_{\text{std}}$ | $\mathcal{S}_{\text{d}}$ | $\mathcal{S}_{\text{l}}$ | $\mathcal{S}_{\text{pot}}$ |
|------------|-----------------------------|--------------------------|--------------------------|-----------------------------|
| cyclic-7   | 36                          | 36                       | 145                      | 145                         |
| cyclic-8   | 244                         | 244                      | 672                      | 672                         |
| eco-10     | 0                           | 0                        | 367                      | 367                         |
| eco-11     | 0                           | 0                        | 749                      | 749                         |
| f-633      | 1                           | 1                        | 9                        | 9                           |
| f-744      | 1                           | 1                        | 259                      | 259                         |
| katsura-11 | 0                           | 0                        | 353                      | 353                         |
| katsura-12 | 0                           | 0                        | 640                      | 640                         |
| noon-8     | 0                           | 0                        | 294                      | 294                         |
| noon-9     | 0                           | 0                        | 682                      | 682                         |
| Random(6,2,2) | 0                  | 0                        | 26                      | 26                          |
| Random(7,2,2) | 0                  | 0                        | 49                      | 49                          |
| Random(8,2,2) | 0                  | 0                        | 102                     | 102                         |
| Random(9,2,2) | 0                  | 0                        | 181                     | 181                         |
| Random(10,2,2) | 0                 | 0                        | 339                     | 339                         |
| Random(11,2,2) | 0                 | 0                        | 590                     | 590                         |
| Random(12,2,2) | 0                 | 0                        | 1083                    | 1083                        |
| Random(13,2,2) | 0                 | 0                        | 1867                    | 1867                        |
| Random(14,2,2) | 0                 | 0                        | 3403                    | 3403                        |

Table 7. # zero reductions (affine)

| Benchmark  | $\mathcal{S}_{\text{std}}$ | $\mathcal{S}_{\text{d}}$ | $\mathcal{S}_{\text{l}}$ | $\mathcal{S}_{\text{pot}}$ |
|------------|-----------------------------|--------------------------|--------------------------|-----------------------------|
| cyclic-7   | 779                         | 679                      | 871                      | 848                         |
| cyclic-8   | 3559                        | 2775                     | 4074                     | 3658                        |
| eco-10     | 522                         | 405                      | 541                      | 478                         |
| eco-11     | 1055                        | 774                      | 1092                     | 965                         |
| f-633      | 60                          | 58                       | 61                       | 59                          |
| f-744      | 468                         | 442                      | 377                      | 348                         |
| katsura-11 | 762                         | 743                      | 553                      | 553                         |
| katsura-12 | 1473                        | 1474                     | 1076                     | 1076                        |
| noon-8     | 1384                        | 1390                     | 1384                     | 1389                        |
| noon-9     | 3743                        | 3750                     | 3743                     | 3749                        |
| Random(6,2,2) | 58                  | 58                      | 39                       | 39                          |
| Random(7,2,2) | 113                  | 113                    | 67                       | 67                          |
| Random(8,2,2) | 212                  | 212                    | 128                      | 128                         |
| Random(9,2,2) | 365                  | 366                    | 223                      | 223                         |
| Random(10,2,2) | 677                 | 677                    | 426                      | 426                         |
| Random(11,2,2) | 1327                | 1357                   | 767                      | 767                         |
| Random(12,2,2) | 2502                | 2537                   | 1463                     | 1463                        |
| Random(13,2,2) | 4879                | 4879                   | 2708                     | 2708                        |
| Random(14,2,2) | 9259                | 9259                   | 5142                     | 5142                        |

Table 8. Size of $\mathcal{H}$ (affine)
| Benchmark          | only top s-reductions | full s-reductions |
|--------------------|------------------------|-------------------|
|                    | $<_{\text{pot}}$ | $<_{\text{rat}}$ | $<_{\text{pot}}$ | $<_{\text{rat}}$ | $<_{\text{pot}}$ | $<_{\text{rat}}$ | $<_{\text{pot}}$ | $<_{\text{rat}}$ |
|                    | $\Delta_{\text{add}}$ | $\Delta_{\text{rat}}$ | $\Delta_{\text{add}}$ | $\Delta_{\text{rat}}$ | $\Delta_{\text{add}}$ | $\Delta_{\text{rat}}$ | $\Delta_{\text{add}}$ | $\Delta_{\text{rat}}$ |
| cyclic-7           | 217.136              | 218.774           | 218.247              | 218.117           | 218.093              | 217.836           | 216.792              | 216.492           |
| (incl. interred)   |                       |                   |                       |                   |                       |                   |                       |                   |
|                     | 217.383              | 217.133           | 217.383              | 217.133           | 217.383              | 217.133           | 217.383              | 217.133           |
|                    | 213.941              | 214.851           | 213.941              | 214.851           | 213.941              | 214.851           | 213.941              | 214.851           |
| cyclic-8           |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 222.800              | 222.093           | 222.800              | 222.093           | 222.800              | 222.093           | 222.800              | 222.093           |
| eco-10             |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 217.687              | 217.687           | 217.687              | 217.687           | 217.687              | 217.687           | 217.687              | 217.687           |
| eco-11             |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 218.181              | 217.170           | 218.181              | 217.170           | 218.181              | 217.170           | 218.181              | 217.170           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| i-633              | 29.644               | 29.426            | 29.644               | 29.426            | 29.644               | 29.426            | 29.644               | 29.426            |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| noon-8             |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 29.730               | 29.526            | 29.730               | 29.526            | 29.730               | 29.526            | 29.730               | 29.526            |
| noon-9             |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 215.535              | 215.361           | 215.535              | 215.361           | 215.535              | 215.361           | 215.535              | 215.361           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| katsura-11         | 218.636              | 218.627           | 218.636              | 218.627           | 218.636              | 218.627           | 218.636              | 218.627           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| katsura-12         | 222.478              | 222.438           | 222.478              | 222.438           | 222.478              | 222.438           | 222.478              | 222.438           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| noon-8             | 218.103              | 218.103           | 218.103              | 218.103           | 218.103              | 218.103           | 218.103              | 218.103           |
| noon-9             |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 218.103              | 218.103           | 218.103              | 218.103           | 218.103              | 218.103           | 218.103              | 218.103           |
| Random(6, 2, 2)    | 210.026              | 210.189           | 210.026              | 210.189           | 210.026              | 210.189           | 210.026              | 210.189           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(7, 2, 2)    |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 211.342              | 211.434           | 211.342              | 211.434           | 211.342              | 211.434           | 211.342              | 211.434           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(8, 2, 2)    | 213.632              | 213.752           | 213.632              | 213.752           | 213.632              | 213.752           | 213.632              | 213.752           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(9, 2, 2)    |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 215.964              | 216.212           | 215.964              | 216.212           | 215.964              | 216.212           | 215.964              | 216.212           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(10, 2, 2)   | 216.106              | 216.210           | 216.106              | 216.210           | 216.106              | 216.210           | 216.106              | 216.210           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(11, 2, 2)   | 218.019              | 218.225           | 218.019              | 218.225           | 218.019              | 218.225           | 218.019              | 218.225           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(12, 2, 2)   | 220.089              | 220.170           | 220.089              | 220.170           | 220.089              | 220.170           | 220.089              | 220.170           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(13, 2, 2)   |                       |                   |                       |                   |                       |                   |                       |                   |
|                    | 225.117              | 225.165           | 225.117              | 225.165           | 225.117              | 225.165           | 225.117              | 225.165           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(14, 2, 2)   | 222.409              | 222.476           | 222.409              | 222.476           | 222.409              | 222.476           | 222.409              | 222.476           |
|                    |                       |                   |                       |                   |                       |                   |                       |                   |
| Random(15, 2, 2)   | 224.512              | 224.597           | 224.512              | 224.597           | 224.512              | 224.597           | 224.512              | 224.597           |

Table 10. # s-reductions (incl. interreductions) (affine)
| Benchmark      | only top s-reductions | full s-reductions |
|---------------|-----------------------|-------------------|
|               | \( <_{\text{pot}} \) | \( <_{\text{rat}} \) | \( <_{\text{d-pot}} \) | \( <_{\text{rat}} \) | \( <_{\text{pot}} \) | \( <_{\text{rat}} \) | \( <_{\text{d-pot}} \) | \( <_{\text{rat}} \) |
| cyclic-7      | 224.53                | 223.830           | 224.008                | 223.989                | 223.866                | 223.482                | 224.065                | 223.612                | 224.220                | 224.105                | 224.229                | 223.832                |
| (incl. interred) | 224.366                | 223.968           | 225.662                | 225.354                | 226.632                | 226.367                | 226.365                | 226.349                | 226.361                | 226.357                | 227.973                | 226.076                |
| cyclic-8      | 231.169               | 230.276           | 231.963                | 232.960                | 232.957                | 232.960                | 231.091                | 230.092                | 231.091                | 232.960                | 232.960                | 232.960                |
| eco-10        | 223.161               | 222.336           | 224.002                | 224.002                | 224.002                | 224.002                | 224.002                | 224.002                | 224.002                | 224.002                | 224.002                | 224.002                |
| (incl. interred) | 226.502                | 226.807           | 227.974                | 228.933                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                |
| eco-11        | 226.823               | 225.662           | 227.974                | 228.933                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                | 229.067                |
| noon-9        | 221.867               | 221.751           | 222.854                | 223.352                | 224.052                | 224.052                | 224.052                | 224.052                | 224.052                | 224.052                | 224.052                | 224.052                |
| Random(6, 2, 2) | 215.466               | 216.176           | 216.867                | 217.352                | 218.052                | 218.052                | 218.052                | 218.052                | 218.052                | 218.052                | 218.052                | 218.052                |
| Random(7, 2, 2) | 216.683               | 217.001           | 217.918                | 218.352                | 219.052                | 219.052                | 219.052                | 219.052                | 219.052                | 219.052                | 219.052                | 219.052                |
| Random(8, 2, 2) | 219.896               | 220.017           | 220.918                | 221.352                | 222.052                | 222.052                | 222.052                | 222.052                | 222.052                | 222.052                | 222.052                | 222.052                |
| Random(9, 2, 2) | 217.745               | 217.956           | 218.219                | 218.756                | 219.456                | 219.456                | 219.456                | 219.456                | 219.456                | 219.456                | 219.456                | 219.456                |
| Random(10, 2, 2) | 222.856               | 222.990           | 223.352                | 224.352                | 225.352                | 225.352                | 225.352                | 225.352                | 225.352                | 225.352                | 225.352                | 225.352                |
| Random(11, 2, 2) | 225.888               | 226.020           | 226.352                | 227.352                | 228.352                | 228.352                | 228.352                | 228.352                | 228.352                | 228.352                | 228.352                | 228.352                |
| Random(12, 2, 2) | 228.820               | 228.889           | 229.352                | 230.352                | 231.352                | 231.352                | 231.352                | 231.352                | 231.352                | 231.352                | 231.352                | 231.352                |
| Random(13, 2, 2) | 231.836               | 231.880           | 232.352                | 233.352                | 234.352                | 234.352                | 234.352                | 234.352                | 234.352                | 234.352                | 234.352                | 234.352                |
| Random(14, 2, 2) | 234.771               | 234.821           | 235.352                | 236.352                | 237.352                | 237.352                | 237.352                | 237.352                | 237.352                | 237.352                | 237.352                | 237.352                |

Table 11. \# multiplications (incl. interreductions) (affine)

14.3 Observations

From the experimental results stated here one can make several observations when it comes to signature-based Gröbner basis algorithms:
Fig. 7. Number of multiplications for homogeneous random examples by increasing number of generators, all of degree 2.
Fig. 8. Number of multiplications for affine random examples by increasing number of generators, all of degree 2
Thus any known algorithm, like F5 survey can also be used as a reference for researchers interested in this topic. and gave a dictionary for translating different notations used in the corresponding publications. Thus this variants of each other and not complete new algorithms as possibly assumed. We covered all variants known different ways. The variations are based on 3 different orders:

\begin{itemize}
  \item[(a)] Ensuring termination algorithmically as presented in Section 10.2 can lead to earlier termination and thus improved behaviour of the algorithm by using different techniques to detect the completeness of \(\mathcal{G}\).
  \item[(b)] Exploiting algebraic structures is an area of high research at the moment (Section 9). Developments in this direction might have a huge impact on the computations of (signature) Gröbner bases in the near future and are promising in decreasing the complexity of computations.
  \item[(c)] Using linear algebra for the reduction process as illustrated in Section 13 is another field where a lot more optimizations can be expected. At the moment, restrictions to \(s\)-reductions lead to restrictions swapping rows during the Gaussian Elimination. Getting more flexible and possibly able to use (at least some of) the ideas from [42] is still an open problem.
  \item[(d)] If we are only interested in computing a Gröbner basis for some input system, can one generalize the usage of signatures and find an intermediate representation between sig-poly pairs \((s(\alpha), \mathcal{G})\) \(\in \mathbb{R}^m \times \mathbb{R}\) and full module representations \(\alpha \in \mathbb{R}^m\)? Where is the breaking point of using more terms from the
\end{itemize}
module representation in order to interreduce the syzygy elements even further and not adding too much overhead in time and memory?

Even though quite different notations are used by researchers, the algorithms are two of a kind, mostly they are even just the same. We hope that this survey helps to give a better understanding on signature-based Gröbner basis algorithms. Moreover, we would like to give researchers new to this area a guide to find their way through the enormous number of publications that have been released on this topic over the last years. Even more, we hope to encourage experts with this survey to collaborate and to push the field of Gröbner basis computations even further.

References

1. Albrecht, M., Cid, C., Fauè, J.-C., and Perret, L. On the relation between the MXL family of algorithms and Gröbner basis algorithms. http://www-salsa.lip6.fr/~jcf/Papers/ACFP12.pdf, 2012. (in press).
2. Albrecht, M. and Perry, J. The F5 Criterion revised. Journal of Symbolic Computation, 46(2):1017–1029, June 2011. Preprint online at arxiv.org/abs/1012.3664
3. Ars, G. Applications des bases de Gröbner à la cryptographie. PhD thesis, Université de Rennes 1, 2005.
4. Ars, G. and Hashemi, A. Extended F5 Criterion. Journal of Symbolic Computation, MEGA 2009 special issue, 45(12):1330–1340, 2010.
5. M. Bardet. Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie. PhD thesis, Université Paris 6, 2004.
6. Bardet, M. On the Complexity of a Gröbner Basis Algorithm. INRIA Algorithms seminar 2002–2004, 2004.
7. Bardet, M., Fauè, J.-C., and Salvy, B. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. http://www-salsa.lip6.fr/~jcf/Papers/43BF.pdf, November 2004.
8. Bardet, M., Fauè, J.-C., Salvy, B., and Yang, B.Y. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. http://www-salsa.lip6.fr/~jcf/Papers/BFS05.pdf, May 2005.
9. Becker, T., Weispfenning, V., and Kredel, H. Gröbner Bases. Graduate Texts in Mathematics, Springer Verlag, 1993.
10. Bigatti, A. M., Caboara, M., and Robbiano, L. Computing Inhomogeneous Gröbner Bases. Journal of Symbolic Computation, 46:498–510, 2011.
11. Bigatti, A. M., La Scala, R., and Robbiano, L. Computing toric ideals. Journal of Symbolic Computation, 27:351–365, 1999.
12. Bosma, W., Cannon, J., and Playoust, C. The Magma algebra system. I. The user language. Journal of Symbolic Computation, 24(3-4):235–265, 1997. http://magma.maths.usyd.edu.au/magma/.
13. Buchberger, B. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, University of Innsbruck, 1965.
14. Buchberger, B. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In EUROSAM ‘79, An International Symposium on Symbolic and Algebraic Manipulation, volume 72 of Lecture Notes in Computer Science, pages 3–23, Springer, 1979.
15. Decker, W., Greuel, G.-M., Pfister, G., and Schönemann, H. SINGULAR 4-0-0 — A computer algebra system for polynomial computations, 2014. http://www.singular.uni-kl.de
16. Eder, C. A new attempt on the F5 Criterion. The Computer Science Journal of Moldova, 16:4–14, 2008.
17. Eder, C. On the criteria of the F5 Algorithm. preprint math.AC/0804.2033, 2008.
18. Eder, C. Signature-based algorithms to compute standard bases. PhD thesis, University of Kaiserslautern, Germany, 2012. https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/2975
19. Eder, C. Predicting zero reductions in Gröbner basis computations. submitted to Journal of Symbolic Computation, preprint at http://arxiv.org/abs/1404.0161, 2014.
28. Eder, C., Gash, J., and Perry, J. Modifying Faugère’s F5 Algorithm to ensure termination. ACM SIGSAM Communications in Computer Algebra, 45(2):70–89, 2011. http://arxiv.org/abs/1006.0318
29. Eder, C. and Perry, J. F5: A Variant of Faugère’s F5 Algorithm with reduced Gröbner bases. Journal of Symbolic Computation, MEGA 2009 special issue, 45(12):1442–1458, 2010. dx.doi.org/10.1016/j.jsc.2010.06.019
30. Eder, C. and Perry, J. Signature-based Algorithms to Compute Gröbner Bases. In ISSAC 2011: Proceedings of the 2011 international symposium on Symbolic and algebraic computation, pages 99–106, 2011.
31. Eder, C. and Roune, B. H. Signature Rewriting in Gröbner Basis Computation. In ISSAC 2013: Proceedings of the 2013 international symposium on Symbolic and algebraic computation, pages 331–338, 2013.
32. Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra, 139(1–3):61–88, June 1999. http://www.salsa.lip6.fr/~jcf/Papers/F99a.pdf
33. Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In ISSAC’02, Villeneuve d’Ascq, France, pages 75–82, July 2002. Revised version from http://fgbfrs.lip6.fr/jcf/Publications/index.html
34. Faugère, J.-C. Algebraic cryptanalysis of HFE using Gröbner bases. 2003. INRIA Research Report, n 4738.
35. Faugère, J.-C., Gianni, P. M., Lazard, D., and Mora, T. Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering. Journal of Symbolic Computation, 16(4):329–344, 1993.
36. Faugère, J.-C. and Joux, A. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. 2729:44–60, 2003.
37. Faugère, J.-C., Safey El Din, M., and Spaenlehauer, P.-J. Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology. In ISSAC ’10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation, ISSAC ’10, pages 257–264, New York, NY, USA, 2010. ACM. Best Student Paper Award.
38. Faugère, J.-C., Safey El Din, M., and Spaenlehauer, P.-J. Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity. Journal of Symbolic Computation, 46(4):406–437, 2011. Available online 4 November 2010.
39. Faugère, J.-C., Safey El Din, M., and Verron, T. On the complexity of Computing Gröbner Bases for Quasi-homogeneous Systems. In Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation, ISSAC ’13, pages 189–196, New York, NY, USA, 2013. ACM.
40. Faugère, J.-C. and Svartz, J. Solving polynomial systems globally invariant under an action of the symmetric group and to the equilibria of n vertices in the plane. In Proceedings of the 37th international symposium on International symposium on symbolic and algebraic computation, ISSAC ’12, pages 170–178, New York, NY, USA, 2012. ACM.
41. Faugère, J.-C. and Svartz, J. Gröbner Bases of ideals invariant under a Commutative group : the Non-modular Case. In Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation, ISSAC ’13, pages 347–354, New York, NY, USA, 2013. ACM.
42. Faugère, J.-C. and Lachartre, S. Parallel Gaussian Elimination for Gröbner bases computations in finite fields. In M. Moreno-Maza and J.L. Roch, editor, Proceedings of the 4th International Workshop on Parallel and Symbolic Computations in Computer Algebra, PASCO ’10, pages 10, pages 89–97, New York, NY, USA, July 2010. ACM.
43. Faugère, J.-C. and Rahmany, S. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In ISSAC ’09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation, ISSAC ’09, pages 151–158, New York, NY, USA, 2009. ACM.
44. Galkin, V. Simple signature-based Groebner basis algorithm. http://arxiv.org/abs/1205.6050 2012.
45. Galkin, V. Termination of original F5. http://arxiv.org/abs/1203.2402 2012.
46. Gao, S., Guan, Y., and Volny IV, F. A new incremental algorithm for computing Gröbner bases. In ISSAC ’10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation, pages 13–19. ACM, 2010.
47. Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases. http://eprint.iacr.org/2010/641 2010.
48. Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases (rev. 2011). http://www.math.clemson.edu/~sgao/papers/gvw.pdf 2011.
49. Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases (rev. 2011). http://www.math.clemson.edu/~sgao/papers/gvw_R130704.pdf 2013.
50. Gash, J. M. On efficient computation of Gröbner bases. PhD thesis, University of Indiana, Bloomington, IN, 2008.
51. Gash, J. M. A provably terminating and speed-competitive variant of F5 – F5t. submitted to the Journal of Symbolic Computation, 2009.
52. Gebauer, R. and Möller, H. M. Buchberger’s algorithm and staggered linear bases. In Proceedings of the fifth ACM symposium on Symbolic and algebraic computation, SYMSAC ’86, pages 218–221, New York, NY, USA, 1986. ACM.
53. Gebauer, R. and Möller, H. M. On an installation of Buchberger’s algorithm. Journal of Symbolic Computation, 6(2–3):275–286, October/December 1988.
54. Gerdt, V. P. and Hashemi, A. On the use of Buchberger criteria in G2V algorithm for calculating Gröbner bases. Program. Comput. Softw., 39(2):81–90, March 2013.
55. Gerdt, V. P., Hashemi, A., and M.-Alizadeh, B. Involutive Bases Algorithm Incorporating F5 Criterion. J. Symb. Comput., 59:1–20, 2013.
56. Greuel, G.-M. and Pfister, G. *A Singular Introduction to Commutative Algebra*. Springer Verlag, 2nd edition, 2007.
57. Hashemi, A., Benyamin, M.-A., and Riahi, M. Invariant G2V algorithm for computing SAGBI-Gröbner bases. *Science China Mathematics*, pages 1–15, 2012.
58. Huang, L. A new conception for computing Gröbner basis and its applications. *Sci. China Ser. F: Informatics & Computational Science*, 54(12):2452–2465, 2011.
59. Hashemi, A., Benyamin, M.-A., and Riahi, M. Invariant G2V algorithm for computing SAGBI-Gröbner bases. *Science China Mathematics*, pages 1–15, 2012.
60. Kapur, D. and Madlener, K. A completion procedure for computing a canonical basis for a k-subalgebra. *Computers and Mathematics with Applications*, pages 1–11, 1989.
61. Kollreider, C. and Buchberger, B. An improved algorithmic construction of Gröbner-bases for polynomial ideals. *SIGSAM Bull.*, 12:27–36, May 1978.
62. D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *EUROCAL '83, European Computer Algebra Conference*, volume 162 of *Springer LNCS*, pages 146–156, 1983.
63. Macaulay, F. S. On some Formulæ in Elimination. *Proceedings of the London Mathematical Society*, 33(1):3–27, 1902.
64. Macaulay, F. S. *The algebraic theory of modular systems*. Cambridge University Press, 1916.
65. Marinari, M. G., Möller, H. M., and Mora, T. Gröbner Bases Of Ideals Defined By Functionals With An Application To Ideals Of Projective Points. *Appl. Alg. in Eng. Comm. and Comp.*, 4:103–145, 1993.
66. Möller, H. M., Mora, T., and Traverso, C. Gröbner bases computation using syzygies. In *ISSAC 92: Papers from the International Symposium on Symbolic and Algebraic Computation*, pages 320–328, 1992.
67. Mora, T. Solving Polynomial Equation Systems B:Macaulay's Paradigm and Gröbner Technology: Macaulay's Paradigm and Gröbner Technology: v. 2 (Encyclopedia of Mathematics and its Applications). Cambridge University Press, 2005.
68. Pan, S., Hu, Y., and Wang, B. The Termination of Algorithms for Computing Gröbner Bases. *http://arxiv.org/abs/1202.3524*, 2012.
69. Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. In *ISSAC 2012: Proceedings of the 2012 international symposium on Symbolic and algebraic computation*, pages 291–298, 2013.
70. Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. In *ISSAC 2012: Proceedings of the 2012 international symposium on Symbolic and algebraic computation*, 2012.
71. Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. *http://arxiv.org/abs/1206.6940*, 2012.
72. Stegers, T. Faugère's F5 Algorithm revisited. Master's thesis, Technische Universität Darmstadt, revised version 2007.
73. Sun, Y. Signature-Based Gröbner Basis Algorithms — Extended MMM Algorithm for computing Gröbner bases. *http://arxiv.org/abs/1308.2371*, 2013.
74. Sun, Y. and Wang, D. K. A New Proof of the F5 Algorithm. *http://www.mmrc.iss.ac.cn/mmpreprints/*, 2009.
75. Sun, Y. and Wang, D. K. A New Proof for the correctness of the F5(F5-like) algorithm. *http://arxiv.org/abs/1004.0084*, 2010.
76. Sun, Y. and Wang, D. K. A generalized criterion for signature related Gröbner basis algorithms. In *ISSAC 2011: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, pages 337–344, 2011.
77. Sun, Y. and Wang, D. K. Solving detachability problem for the polynomial ring by signature-based Gröbner basis algorithms. *http://arxiv.org/abs/1108.1301*, 2011.
78. Sun, Y. and Wang, D. K. The F5 algorithm in Buchberger's style. *J. Syst. Sci. Complex.*, 24(6):1218–1231, 2011.
79. Sun, Y. and Wang, D. K. A new proof for the correctness of the F5 algorithm. *Sci. China Math.*, 56(4):745–756, 2013.
80. Sun, Y. and Wang, D. K. Extending the GVW algorithm to compute Gröbner bases. *Submitted to Sci. China Math.*, 2013.
81. Sun, Y., Wang, D. K., Ma, D. X., and Zhang, Y. A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras. In *ISSAC 2012: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, pages 351–358, 2012.
82. Nicolas M. Thiéry. Computing minimal generating sets of invariant rings of permutation groups with sagbi-gröbner bases. *DM-CCG*, pages 315–328, 2001.
83. Volny, F. *New algorithms for computing Gröbner bases*. PhD thesis, Clemson University, 2011.
84. Wichmann, T. Der FGLM-Algorithmus: verallgemeinert und implementiert in *Singular*. *Diploma thesis at the university of Kaiserslautern*, 1997.
85. Zobnin, A. I. Generalization of the F5 algorithm for calculating Gröbner bases for polynomial ideals. *Programming and Computer Software*, 36:75–82, 2010. *http://dx.doi.org/10.1134/S0361768810020040*