THE F5 CRITERION REVISED

ALBERTO ARRI AND JOHN PERRY

Abstract. The purpose of this work is to generalize part of the theory behind Faugère's "F5" algorithm. This is one of the fastest known algorithms to compute a Gröbner basis of a polynomial ideal I generated by polynomials $f_1, \ldots, f_m$. A major reason for this is what Faugère called the algorithm's "new" criterion, and we call "the F5 criterion"; it provides a sufficient condition for a set of polynomials G to be a Gröbner basis. However, the F5 algorithm is difficult to grasp, and there are unresolved questions regarding its termination.

This paper introduces some new concepts that place the criterion in a more general setting: $\mathcal{S}$-Gröbner bases and primitive $\mathcal{S}$-irreducible polynomials. We use these to propose a new, simple algorithm based on a revised F5 criterion. The new concepts also enable us to remove various restrictions, such as proving termination without the requirement that $f_1, \ldots, f_m$ be a regular sequence.

1. Introduction

Since their introduction in [3] by B. Buchberger, Gröbner bases and their computation have attracted significant attention in the computer algebra community. The best-known algorithm used to compute a Gröbner basis is the original algorithm due to Buchberger [3], and named after him. Its efficiency has been constantly enhanced through the years, but there remains room for improvement. Various criteria have since been introduced to detect useless computations – for example, [3, 4, 8] — but even so, the algorithm spends most of its time reducing polynomials to zero ("zero reductions").

In [11], Lazard pointed out that one can view the computation of a Gröbner basis as the reduction to row-echelon form of the Macaulay matrix of the ideal. This led to the Staggered Linear Basis algorithm of Gebauer and Möller in [9], as well as the "F4" algorithm of Faugère in [6]. Möller, Mora, and Traverso exploited the relationship between zero reductions and syzygies [12], but although the algorithm they presented successfully detected many zero reductions, in practice it took too much memory and time (see Section 8 of [12]). In [5], Faugère combined aspects of these approaches into algorithm "F5", which for a certain class of polynomial system eliminates *all* zero reductions. This algorithm exhibits impressive performance.

By Faugère's admission, the theory behind the algorithm's new criterion, which we call *the F5 criterion*, is merely sketched, so as to leave more room for examples and an accurate description of the algorithm. The proof of the algorithm's termination and correctness were likewise only outlined. Additionally, some arguments were made under strong assumptions, such as that the input sequence $f_1, \ldots, f_m$ had only principal syzygies (such a sequence is called a *regular* sequence).

We pause a moment to consider some variants of F5. Bardet described an implementation of F5 in matrix form, where termination is ensured by manually supplying a maximal degree [2]. Stegers filled in some details of Faugère's proof in [15], but stopped at two conjectures, one of which Gash later showed to be false [7].

The purpose of this paper is to present a simpler algorithm that illustrates the fundamental principles of F5 without sacrificing termination. We begin by defining a function $\mathcal{S}$ which is equivalent to that of Faugère, then develop a structured theory, introducing new concepts such as *primitive $\mathcal{S}$-irreducible polynomials* and *$\mathcal{S}$-Gröbner bases*. These make the study of the problem more accessible, and suggest a new version of the F5 criterion which depends neither on the regularity of the input, nor on a particular ordering on the module of syzygies.

From this theory, we develop a new, simpler algorithm. We must emphasize that the algorithm is a simple demonstration of the criterion, and not a deep treatment of how to implement a highly efficient algorithm; nevertheless, the new concepts allow us to prove correctness and termination *for any input*. Note that although some F5-style algorithms provide explicit termination mechanisms [2, 7], these mechanisms rely on previously-developed, non-F5 criteria to compute explicitly a maximal degree; by contrast, the termination criterion used here is precisely the generalized F5 criterion used to detect useless computations. Later, we show that if we know that the input is a regular sequence and we use a specific ordering on $\operatorname{Syz}\mathcal{F}$, we can avoid all the reductions to zero. We compare the results to both F5 and the Staggered Linear Basis algorithm, showing how this new algorithm differs from each.

The paper's structure is as follows. Sections 2–4 cover background material; although most of this is relatively straightforward, an important and novel contribution of the paper appears at the end of Section 4 with Proposition 14. The proof of that theorem leads to the concept of *primitive* $\mathcal{S}$-irreducible polynomials, from which we obtain in Section 5 a new characterization theorem for a Gröbner basis (Theorem 18). In Section 6, we use this characterization to formulate the new algorithm, and we prove that it terminates correctly. Section 7 compares this algorithm to the Staggered Linear Basis algorithm and F5, illustrating the differences concretely. Section 8 describes some conclusions and possible future directions.

2. Preliminaries

Let $P = k[x_1, \ldots, x_n]$ be the polynomial ring over the field k with n indeterminates, let μ be any admissible ordering on $\mathbb{T}^n$, the monoid of power products over $x_1, \ldots, x_n$: $\mathbb{T}^n = \{\prod_{i=1}^n x_i^{\alpha_i} \mid \alpha_i \in \mathbb{N}\}$.

Let P^m be the free P-module generated by $\{e_1, \ldots, e_m\}$ and let μ' be any admissible ordering on $\mathbb{T}^n_m$, the set of module terms of P^m: $\mathbb{T}^n_m = \{te_l \mid t \in \mathbb{T}, l \in \{1, \ldots, m\}\}$.

Fix $\mathcal{F} = (f_1, \ldots, f_m) \in P^m$ and let $I \subseteq P$ be the ideal generated by $\mathcal{F}$, and define $v : P^m \to I$ as the P-module homomorphism such that $v(e_i) = f_i$, and let $\operatorname{Syz}\mathcal{F} = \ker v$, so that $\operatorname{Syz}\mathcal{F}$ is the module of syzygies of $\mathcal{F}$, $\operatorname{LT}(\operatorname{Syz}\mathcal{F}) \subseteq \mathbb{T}^n_m$ is set of leading module terms of $\operatorname{Syz}\mathcal{F}$, and $\operatorname{NS}(\operatorname{Syz}\mathcal{F}) = \mathbb{T}^n_m \setminus \operatorname{LT}(\operatorname{Syz}\mathcal{F})$ is the *normal set* of the syzygies of $\mathcal{F}$.

Clearly v is surjective; therefore, as a P-module, ${}^{P^m}\!/_{\operatorname{Syz}\mathcal{F}} \simeq I$. Let $\psi : I \to {}^{P^m}\!/_{\operatorname{Syz}\mathcal{F}}$ be the P-module isomorphism between them. We use the notation $\operatorname{LT}(\cdot)$ for both the leading term of a polynomial in P with respect to μ, and the module leading term of a module element in P^m with respect to μ'. We will use $\operatorname{LC}(f)$, where f is a nonzero polynomial belonging to I, to denote the coefficient of $\operatorname{LT}(f)$.

We are interested in finding a set of polynomials G such that G is a Gröbner basis for I with respect to the ordering μ on $\mathbb{T}^n$.

Definition 1. Let

$$\begin{array}{rccl} \mathcal{S}: & I \setminus \{0\} & \to & \operatorname{NS}(\operatorname{Syz}\mathcal{F}) \\ & f & \mapsto & \operatorname{LT}(\psi(f)), \end{array}$$

where $\mathrm{LT}(\psi(f))$ is the module leading term of the normal form of $\psi(f)$ with respect to the ordering μ' on P^m.

The key idea of Faugère is to keep track of the value of $\mathcal{S}(f)$ for any polynomial f we will work with. It is however clear from the definition that the explicit calculation of $\mathcal{S}$ requires, at least, to know a Gröbner basis of $\operatorname{Syz}\mathcal{F}$ which is computationally expensive to compute, more than a Gröbner basis of I itself. In fact, we will obtain $\mathcal{S}$ from the fact that $\mathcal{S}(f_i) = e_i$ (unless $e_i \in \mathrm{LT}(\operatorname{Syz}\mathcal{F})$) and from other properties of $\mathcal{S}$.

3. Properties of $\mathcal{S}$

Lemma 2 (Properties of $\mathcal{S}$). *Let $f, f_1, f_2 \in I \setminus \{0\}$. The following hold:*

(1) If $\mathcal{S}(f_1) > \mathcal{S}(f_2)$ then:

$$\mathcal{S}(f_1 + f_2) = \mathcal{S}(f_1).$$

(2) If $\mathcal{S}(f_1) = \mathcal{S}(f_2) = \sigma$ and there is no $\lambda \in k^* = k \setminus \{0\}$ such that $f_1 = \lambda f_2$, then there exist α and β in k^* such that:

$$\mathcal{S}(\alpha f_1 + \beta f_2) < \sigma.$$

(3) Let $t \in \mathbb{T}^n$, then

$$\mathcal{S}(tf) = t\mathcal{S}(f) \iff t\mathcal{S}(f) \in \mathrm{NS}(\operatorname{Syz}\mathcal{F}),$$
$$\mathcal{S}(tf) < t\mathcal{S}(f) \iff t\mathcal{S}(f) \in \mathrm{LT}(\operatorname{Syz}\mathcal{F}).$$

Proof. (1) and (2) are trivial.

In order to prove (3), let $\mathcal{S}(f) = \sigma = \tau e_i$. By the definition of $\mathcal{S}$ we have:

$$f = v\left(\alpha\tau e_i + \text{smaller terms}\right),$$

where $\alpha \in k^*$, $\tau \in \mathbb{T}^n$, and the argument of v is in its normal form with respect to $\operatorname{Syz}\mathcal{F}$.

Multiplying both sides by t, we get:

$$tf = v\left(\alpha t\tau e_i + \text{smaller terms}\right).$$

If $t\tau e_i = t\sigma \in \mathrm{NS}(\operatorname{Syz}\mathcal{F})$, the leading term of the normal form of $\alpha t\tau e_i + \cdots$ is $t\sigma$ and, in this case, $\mathcal{S}(tf) = t\sigma = t\mathcal{S}(f)$. Otherwise, $t\sigma \notin \mathrm{NS}(\operatorname{Syz}\mathcal{F})$, so the normal form has a leading term which is strictly smaller than $t\sigma$ and we have $\mathcal{S}(tf) < t\mathcal{S}(f)$. □

Corollary 3. *To decide whether $\mathcal{S}(tf) = t\mathcal{S}(f)$, it suffices to know* $\mathrm{NS}(\operatorname{Syz}\mathcal{F})$ *or, equivalently,* $\mathrm{LT}(\operatorname{Syz}\mathcal{F})$*. Also, if $t\mathcal{S}(f) = \mathcal{S}(g)$ for some $g \in I \setminus \{0\}$, then since $\mathcal{S}(g) \in \mathrm{NS}(\operatorname{Syz}\mathcal{F})$, we can conclude that $t\mathcal{S}(f) = \mathcal{S}(tf)$.*

One of the key concepts of the classic theory of Gröbner bases is the polynomial reduction: one says that $f \in P \setminus \{0\}$ reduces with a $h \in P \setminus \{0\}$, if there exist $\alpha \in k^*$ and $t \in \mathbb{T}^n$ such that $\mathrm{LT}(f - \alpha th) < \mathrm{LT}(f)$, denoted

$$f \xrightarrow{h} g$$

where $g = f - \alpha th$.

We now introduce a special kind of reduction for a polynomial f, which takes in consideration the value of $\mathcal{S}(f)$.

Definition 4 ($\mathcal{S}$-reduction)**.** Let $f, h \in I \setminus \{0\}$, $g \in I$ and $\sigma \in \mathbb{T}^n_m$. We say that f *$\mathcal{S}$-reduces* with respect to σ to g with h,

$$f \xrightarrow{h}_{\mathcal{S},\sigma} g$$

if there are $t \in \mathbb{T}^n$ and $\alpha \in k^*$ such that:

- $\mathrm{LT}(g) < \mathrm{LT}(f)$ and $f - \alpha t h = g$, and
- $\mathcal{S}(th) < \sigma$.

When we omit to specify σ, we assume $\sigma = \mathcal{S}(f)$.

Note that this reduction is defined only for polynomials f which belong to the ideal I, and not for abitrary elements of the ring P. Also, when $\sigma = \mathcal{S}(f)$, since $\mathcal{S}(th) < \mathcal{S}(f)$ we have $\mathcal{S}(g) = \mathcal{S}(f - \alpha t h) = \mathcal{S}(f)$. Hence, when performing one, or more, $\mathcal{S}$-reduction steps with a polynomial:

$$f \xrightarrow{h_0}_{\mathcal{S}} f_1 \xrightarrow{h_1}_{\mathcal{S}} f_2 \xrightarrow{h_2}_{\mathcal{S}} \dots \xrightarrow{h_{k-1}}_{\mathcal{S}} f_k$$

we have $\mathcal{S}(f) = \mathcal{S}(f_1) = \ldots = \mathcal{S}(f_k)$ and $\mathrm{LT}(f) > \mathrm{LT}(f_1) > \ldots > \mathrm{LT}(f_k)$; that is, the value of $\mathcal{S}$ is kept constant, while the leading term decreases.

Let us consider how to characterize those elements which cannot be further $\mathcal{S}$-reduced with respect to a given $\sigma \in \mathbb{T}^n_m$. The following definition is natural:

Definition 5 ($\mathcal{S}$-irreducible polynomial)**.** We say that $f \in I$ is *$\mathcal{S}$-irreducible* with respect to $\sigma \in \mathbb{T}^n_m$ if $f = 0$ or if there is no $h \in I$ which $\mathcal{S}$-reduces f with respect to σ. As before, if we do not specify σ, we assume $\sigma = \mathcal{S}(f)$. Note that this definition depends on the values of I, $\mathcal{F}$ and μ'.

We could look for a criterion which decides whether a given set of nonzero polynomials G is a Gröbner basis by looking at the values of $\mathcal{S}(g)$ for all g in G. However, it is wiser to characterize a set of polynomials with a property similar to that of a Gröbner basis, but which also accounts for $\mathcal{S}$. We therefore introduce the following:

Definition 6 ($\mathcal{S}$-Gröbner basis)**.** We say that $G \subset I$ is an *$\mathcal{S}$-Gröbner basis* if for each $\mathcal{S}$-irreducible polynomial $f \in I \setminus \{0\}$, there exist $g \in G$ and $t \in \mathbb{T}^n$ such that $\mathrm{LT}(tg) = \mathrm{LT}(f)$ and $\mathcal{S}(tg) = \mathcal{S}(f)$.

Remark 7. An $\mathcal{S}$-Gröbner basis depends on:

- the ideal I,
- the term ordering μ on $\mathbb{T}^n$,
- the m-tuple of generators $\mathcal{F}$,
- the ordering μ' on $\mathbb{T}^n_m$.

We will prove in the following section that an $\mathcal{S}$-Gröbner basis is a Gröbner basis in the usual sense. While Definition 6 is not especially useful from a computational point of view, inasmuch as it is quantified over an infinite set, Theorem 18 will provide us an equivalent criterion that is quantified over a finite set. Before we can prove it, however, we need to consider some properties of $\mathcal{S}$-reductions.

4. Properties of $\mathcal{S}$-reductions

In this section we will prove the main facts which will lead to the characterization we are looking for.

Definition 8. Let

$$\begin{array}{rccl} \varphi: & \mathrm{LT}(I) & \to & \mathrm{NS}(\operatorname{Syz}\mathcal{F}) \\ & t & \mapsto & \min\{\mathcal{S}(f) \mid f \in I,\ \mathrm{LT}(f) = t\}. \end{array}$$

In other words, if t belongs to $\mathrm{LT}(I)$, φ is the minimum value $\mathcal{S}$ can take on a polynomial whose leading term is t. It follows that, for any $f \in I \setminus \{0\}$, $\varphi(\mathrm{LT}(f)) \leq \mathcal{S}(f)$ always holds.

Lemma 9. *φ is a bijection, and the inverse function of φ has an explicit formula: $\varphi^{-1}(\sigma) = \min\{t' \in \mathbb{T}^n \mid \exists f \in I, \mathrm{LT}(f) = t', \mathcal{S}(f) = \sigma\}$.*

Proof. We show that φ is both injective and surjective.

Injective:: By way of contradiction, suppose there exist $\sigma \in \mathrm{NS}(\operatorname{Syz}\mathcal{F})$ and $t_1, t_2 \in \mathrm{LT}(I)$ such that $t_1 > t_2$ and $\sigma = \varphi(t_1) = \varphi(t_2)$. Then we can find $f_1, f_2 \in I$ such that $\mathrm{LT}(f_1) = t_1$, $\mathrm{LT}(f_2) = t_2$, and $\mathcal{S}(f_1) = \mathcal{S}(f_2) = \sigma$. By Lemma 2, there exist $\alpha, \beta \in k^*$ such that $\mathcal{S}(\alpha f_1 + \beta f_2) < \sigma$, but $\mathrm{LT}(\alpha f_1 + \beta f_2) = t_1$, and therefore $\varphi(t_1) < \sigma$, contradicting the hypothesis.

Surjective:: Let $\sigma = \tau e_i \in \mathrm{NS}(\operatorname{Syz}\mathcal{F})$, define

$$t = \min\{t' \in \mathbb{T}^n \mid \exists f \in I, \mathrm{LT}(f) = t', \mathcal{S}(f) = \sigma\}.$$

(This set is not empty because it contains $\mathrm{LT}(\tau f_i)$.) Let $f \in I$ be a polynomial with $\mathrm{LT}(f) = t$ and $\mathcal{S}(f) = \sigma$; obviously $\varphi(t) \leq \sigma$. By way of contradiction, suppose that $\varphi(t) < \sigma$. Then there exists $f' \in I$ such that $\mathrm{LT}(f') = t$ and $\mathcal{S}(f') < \sigma$. We can now choose $\alpha, \alpha' \in k^*$ with $\mathrm{LT}(\alpha f + \alpha' f') < t$ such that $\mathcal{S}(\alpha f + \alpha' f') = \sigma$. The existence of $\alpha f + \alpha' f'$ contradicts the minimality of t; therefore, $\varphi(t) = \sigma$.

□

The fact that φ is a bijection will play a crucial role in most of the subsequent proofs.

Theorem 10 (S-reduction theorem)**.** *Let $f \in I$ and $\sigma \in \mathbb{T}^n_m$ such that f is $\mathcal{S}$-irreducible with respect to σ and f is of the form $f = v(\alpha\sigma + \text{smaller terms})$, for some $\alpha \in k^*$.*

Either the following equivalent propositions hold:

(a) $f = 0$,
(b) $\sigma \in \mathrm{LT}(\operatorname{Syz}\mathcal{F})$,

or the following equivalent propositions hold:

(1) $f \neq 0$,
(2) $\sigma \in \mathrm{NS}(\operatorname{Syz}\mathcal{F})$,
(3) $f \neq 0$ *and* $\sigma = \mathcal{S}(f) = \varphi(\mathrm{LT}(f))$.

Proof.

a ⇒ b: Suppose $f = 0$, then $0 = f = v(\alpha\sigma + \cdots)$. It follows that $\sigma \in \mathrm{LT}(\operatorname{Syz}\mathcal{F})$.

b ⇒ a: Assume by way of contradiction that $\sigma \in \mathrm{LT}(\operatorname{Syz}\mathcal{F})$ and $f \neq 0$. Let $t = \mathrm{LT}(f)$, and consider $\sigma' = \varphi(t) \in \mathrm{NS}(\operatorname{Syz}\mathcal{F})$. There exists $g \in I$ such that $\mathrm{LT}(g) = t$ and $\mathcal{S}(g) = \sigma'$; since $\sigma' < \sigma$, g is an $\mathcal{S}$-reductor for f with respect to σ, contradicting the fact that f is $\mathcal{S}$-irreducible. Therefore, $f = 0$.

1 ⇒ 2: Assume by way of contradiction that $f \neq 0$ and $\sigma \notin \mathrm{NS}\,(\operatorname{Syz}\mathcal{F})$. Then $\sigma \in \mathrm{LT}\,(\operatorname{Syz}\mathcal{F})$. Let $t = \mathrm{LT}\,(f)$, and consider $\sigma' = \varphi\,(t) \in \mathrm{NS}\,(\operatorname{Syz}\mathcal{F})$. There exists $g \in I$ such that $\mathrm{LT}\,(g) = t$ and $\mathcal{S}\,(g) = \sigma'$; since $\sigma' < \sigma$, g is an $\mathcal{S}$-reductor for f with respect to σ, constradicting the hypothesis that f is $\mathcal{S}$-irreducible. Therefore, $\sigma \in \mathrm{NS}\,(\operatorname{Syz}\mathcal{F})$.

2 ⇒ 3: Assume $\sigma \in \mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$. Necessarily, $\sigma = \mathcal{S}(f)$. Suppose now that $\sigma \neq \varphi(\mathrm{LT}(f))$; then $\mathcal{S}(f) > \varphi(\mathrm{LT}(f))$. Therefore there exists a polynomial $g \in I$ such that $t = \mathrm{LT}(g) = \mathrm{LT}(f)$ and $\varphi(t) = \mathcal{S}(g) = \varphi(\mathrm{LT}(f)) < \mathcal{S}(f)$. It follows that g is an $\mathcal{S}$-reductor of f, and f is not $\mathcal{S}$-irreducible.

3 ⇒ 1: Obvious.

□

Theorem 10 implies that it only makes sense to consider those polynomials f that are $\mathcal{S}$-irreducible with respect to $\mathcal{S}(f)$. Also, an $\mathcal{S}$-reduction yields 0 if and only if performed with respect to a $\sigma \in \mathrm{LT}(\mathrm{Syz}\,\mathcal{F})$; conversely, if an $\mathcal{S}$-reduction yields a non-zero polynomial, then we know that it was performed with respect to some $\sigma \in \mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$.

Remark 11. Observe that a polynomial f is $\mathcal{S}$-irreducible iff $\mathcal{S}(f) = \varphi(\mathrm{LT}(f))$; otherwise, $\mathcal{S}(f) > \varphi(\mathrm{LT}(f))$, and we could find $g \in I$ such that $\mathrm{LT}(g) = \mathrm{LT}(f)$ and $\mathcal{S}(g) = \varphi(\mathrm{LT}(f))$, so that g would $\mathcal{S}$-reduce f.

In strict analogy with the classic Gröbner basis theory we have the following result:

Proposition 12. *If G is an $\mathcal{S}$-Gröbner basis then for any nonzero $f \in I$ such that f is not $\mathcal{S}$-irreducible, there exists $g \in G$ and $t \in \mathbb{T}^n$ such that:*

- $\mathrm{LT}(tg) = \mathrm{LT}(f)$,
- $\mathcal{S}(tg) = t\mathcal{S}(g) < \mathcal{S}(f)$.

That is, it is always possible to find an $\mathcal{S}$-reductor for f in G.

Proof. Since f is not $\mathcal{S}$-irreducible, take h $\mathcal{S}$-irreducible such that $\mathrm{LT}(f) = \mathrm{LT}(h)$. From the remark above, $\mathcal{S}(h) < \mathcal{S}(f)$, so h is an $\mathcal{S}$-reductor of f. We can then find $t \in \mathbb{T}$ and $g \in G$ such that $t\,\mathrm{LT}(g) = \mathrm{LT}(h) = \mathrm{LT}(f)$ and (using Corollary 3) $\mathcal{S}(tg) = t\mathcal{S}(g) = \mathcal{S}(h)$. □

This fact combined with lemma 9 leads immediately to:

Proposition 13. *If G is an $\mathcal{S}$-Gröbner basis, then G is a Gröbner basis with respect to the ordering μ on $\mathbb{T}^n$.*

Proof. For any $t \in \mathrm{LT}(I)$, Lemma 9 implies that there exists $\sigma \in \mathbb{T}^n_m$ such that $\varphi^{-1}(\sigma) = t$. Let $f \in I$ such that $\mathrm{LT}(f) = t$ and $\mathcal{S}(f) = \sigma$. From Proposition 12, we may assume that f is $\mathcal{S}$-irreducible (if not, $\mathcal{S}$-reduce it). Then $\exists g \in G$, $u \in \mathbb{T}^n$ such that $\mathrm{LT}(ug) = \mathrm{LT}(f) = t$. Hence the set $\{\mathrm{LT}(g) \mid g \in G\}$ generates $\mathrm{LT}(I)$ and $(G) \subseteq I$. Therefore G is a Gröbner basis for I. □

Proposition 14. *Every $\mathcal{S}$-Gröbner basis contains a finite $\mathcal{S}$-Gröbner basis.*

Proof. Let $G = \{g_i\}_{i\in\mathcal{I}}$ be an $\mathcal{S}$-Gröbner basis, and

$$\begin{array}{rccl} \vartheta: & G & \to & P \oplus P^m \\ & g_i & \mapsto & (\mathrm{LT}(g_i), \mathcal{S}(g_i)). \end{array}$$

The image $\vartheta(G)$ generates a P-submodule M of the P-module $P \oplus (P)^m \cong (P)^{m+1}$. This is a noetherian module; therefore, there exists a finite subset $\mathcal{J}$ of $\mathcal{I}$ such that $\vartheta(G')$ generates M, for some $G' = \{g_j\}_{j\in\mathcal{J}}$.

We claim that G' is itself an $\mathcal{S}$-Gröbner basis. To see this, let $f \in I$ be an $\mathcal{S}$-irreducible polynomial. By definition, $\mathcal{S}(f) \in \mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$. Since G is an $\mathcal{S}$-Gröbner basis, we can find a $g_i \in G$ and a $t \in \mathbb{T}^n$ such that $t\mathcal{S}(g_i) = \mathcal{S}(tg_i) = \mathcal{S}(f)$ and $t\,\mathrm{LT}(g_i) = \mathrm{LT}(tg_i) = \mathrm{LT}(f)$

(using Lemma 2(3) for $t\mathcal{S}(g_i) = \mathcal{S}(tg_i)$). If $i \in \mathcal{J}$, then $g_i \in G'$ and we're fine. Otherwise, $i \in \mathcal{I} \setminus \mathcal{J}$; since $\vartheta(g_i) \in M$, there exist $j_i \in \mathcal{J}$ and $t_i \in \mathbb{T}^n$ such that

$$t_i \vartheta(g_{j_i}) = \vartheta(g_i).$$

This implies that $\mathcal{S}(g_i) = t_i \mathcal{S}(g_{j_i}) = \mathcal{S}(t_i g_{j_i})$ and $\mathrm{LT}(g_i) = \mathrm{LT}(t_i g_{j_i})$. Then $\mathcal{S}(tg_i) = \mathcal{S}(t(t_i g_{j_i}))$ and $\mathrm{LT}(tg_i) = \mathrm{LT}(t(t_i g_{j_i}))$, so we have found $g_{j_i} \in G'$ and $t \cdot t_i \in \mathbb{T}^n$ which satisfy the $\mathcal{S}$-Gröbner basis property for f. □

The elements of G' from the proof above will prove critically important when we examine our algorithm, so we will identify them by a special term.

Definition 15 (Primitive S-irreducible polynomial)**.** We say that a nonzero polynomial f $\mathcal{S}$-irreducible with respect to $\mathcal{S}(f)$ is *primitive $\mathcal{S}$-irreducible* if there are no polynomials $f' \in I \setminus \{0\}$ and terms $t \in \mathbb{T}^n$ such that f' is $\mathcal{S}$-irreducible, $\mathrm{LT}(tf') = \mathrm{LT}(f)$ and $\mathcal{S}(tf') = \mathcal{S}(f)$.

The proof of Proposition 14 implies that if we have an $\mathcal{S}$-Gröbner basis G, then we can obtain a finite $\mathcal{S}$-Gröbner basis by keeping a subset of primitive $\mathcal{S}$-irreducible polynomials with different leading terms. Hence there exist $\mathcal{S}$-Gröbner bases which contain only primitive $\mathcal{S}$-irreducible polynomials.

5. The main result

First we adapt the definition of a normal pair in [5] to reflect primitive $\mathcal{S}$-irreducible polynomials.

Definition 16 (Normal Pair)**.** Given $g_1, g_2 \in I \setminus \{0\}$, let $\mathrm{Spol}(g_1, g_2) = u_1 g_1 - u_2 g_2$ be the S-polynomial of g_1 and g_2; that is, $u_i = \frac{\mathrm{lcm}(\mathrm{LT}(g_1),\mathrm{LT}(g_2))}{\mathrm{LC}(g_i)\,\mathrm{LT}(g_i)}$. We say that (g_1, g_2) is a *normal pair* if:

(1) g_i is a primitive $\mathcal{S}$-irreducible polynomial for $i = 1, 2$,
(2) $\mathcal{S}(u_i g_i) = \mathrm{LT}(u_i)\mathcal{S}(g_i)$ for $i = 1, 2$,
(3) $\mathcal{S}(u_1 g_1) \neq \mathcal{S}(u_2 g_2)$.

Remark 17. With this definition, if (g_1, g_2) is a normal pair, then

$$\mathcal{S}(\mathrm{Spol}(g_1, g_2)) = \max(\mathcal{S}(u_1 g_1), \mathcal{S}(u_2 g_2))$$

will always hold. In addition, if $\mathcal{S}(u_1 g_1) > \mathcal{S}(u_2 g_2)$, then $u_1 \neq 1$, as if u_1 were 1, g_2 would be an $\mathcal{S}$-reductor of g_1. Therefore $\mathcal{S}(\mathrm{Spol}(g_1, g_2)) > \max(\mathcal{S}(g_1), \mathcal{S}(g_2))$.

Theorem 18 (F5 criterion)**.** *Suppose that G is a set of $\mathcal{S}$-irreducible polynomials of I, such that:*

- *for each $i = 1, \ldots, m$ such that $e_i \notin \mathrm{LT}(\mathrm{Syz}\,\mathcal{F})$ there exists $g_i \in G$ such that $\mathcal{S}(g_i) = e_i$, and*
- *for any $g_1, g_2 \in G$ such that (g_1, g_2) is a normal pair, there exist $g \in G$ and $t \in \mathbb{T}^n$ such that tg is $\mathcal{S}$-irreducible and $\mathcal{S}(tg) = \mathcal{S}(\mathrm{Spol}(g_1, g_2))$.*

Then G is a $\mathcal{S}$-Gröbner basis of I.

Remark 19 (Rewritable criterion). Note that the second condition does not explicitly involve the S-polynomial of a pair (g_1, g_2), but cares only about $\mathcal{S}(\mathrm{Spol}(g_1, g_2))$. Hence, we can think of this as a criterion to choose elements of $\mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$ instead of polynomials. Additionally, if two or more normal pairs are such that $\mathcal{S}$ takes the same value on their S-polynomials, we can freely consider just one of them.

Proof. As noted at the end of the previous section, we may, without loss of generality, assume that the elements of G are primitive $\mathcal{S}$-irreducible and have distinct leading terms. By way of contradiction, suppose that there exists a minimal $\sigma \in \mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$ and an $\mathcal{S}$-irreducible $f \in I\backslash\{0\}$ with $\mathcal{S}(f) = \sigma$ and the $\mathcal{S}$-Gröbner basis property does not hold for f and σ. That is, for all $g \in G$ and for all $t \in \mathbb{T}^n$, $\mathrm{LT}(tg) \neq \mathrm{LT}(f)$ or $\mathcal{S}(tg) \neq \mathcal{S}(f)$.

The first hypothesis implies that there exist at least one primitive $\mathcal{S}$-irreducible $g \in G$ and some $\tau \in \mathbb{T}^n$ such that $\tau\mathcal{S}(g) = \mathcal{S}(f) = \sigma$; among the possible choices for g and τ, pick one which minimizes $\mathrm{LT}(\tau g)$. By Lemma 2(3), $\mathcal{S}(\tau g) = \tau\mathcal{S}(g) = \sigma$. Hence $\mathrm{LT}(\tau g) \neq \mathrm{LT}(f)$. By Remark 11, $\mathcal{S}(f) = \varphi(\mathrm{LT}(f))$, and by Lemma 9, $\mathrm{LT}(\tau g) > \mathrm{LT}(f)$. In addition, we have $\mathcal{S}(\tau g) = \mathcal{S}(f) = \varphi(\mathrm{LT}(f)) \neq \varphi(\mathrm{LT}(\tau g))$, so again by Remark 11, τg is not $\mathcal{S}$-irreducible.

By Lemma 2(2), there exist $\alpha, \beta \in k^*$ such that $\mathcal{S}(\alpha f + \beta\tau g) = \sigma'$ for some $\sigma' < \sigma$. Since σ was chosen to be the minimal element of $\mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$ such that the $\mathcal{S}$-Gröbner basis property does not hold, Definition 6 and Proposition 12 applied to $\alpha f + \beta\tau g$ imply that there exist $g' \in G$ and $\tau' \in \mathbb{T}^n$ such that $\mathrm{LT}(\tau' g') = \mathrm{LT}(\alpha f + \beta\tau g) = \mathrm{LT}(\tau g)$ and

$$\mathcal{S}(\tau' g') = \tau'\mathcal{S}(g') \leq \mathcal{S}(\alpha f + \beta\tau g) = \sigma' < \sigma = \mathcal{S}(\tau g).$$

Clearly $g \neq g'$.

It follows that (g, g') is a normal pair. From the second hypothesis, we know that there exist $g'' \in G$ and $\tau'' \in \mathbb{T}^n$ such that $\tau'' g''$ is $\mathcal{S}$-irreducible and $\mathcal{S}(\tau'' g'') = \mathcal{S}(\mathrm{Spol}(g, g'))$. Write $\hat{\tau}\,\mathrm{Spol}(g, g') = \gamma\tau g - \gamma'\tau' g'$, for some $\gamma, \gamma' \in k^*$, where $\hat{\tau}$ is the gcd of τ and τ'. Since (g, g') is a normal pair and $\sigma \in \mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$,

$$\sigma = \tau\mathcal{S}(g) = \widehat{\tau}\mathcal{S}(\mathrm{Spol}(g, g')) = \widehat{\tau}\mathcal{S}(\tau'' g'') = \mathcal{S}(\widehat{\tau}\tau'' g'').$$

By Remark 11, $\mathcal{S}(\tau'' g'') = \varphi(\mathrm{LT}(\tau'' g''))$, so we have

$$\mathrm{LT}(\tau'' g'') = \varphi^{-1}(\mathcal{S}(\tau'' g'')) \leq \mathrm{LT}(\mathrm{Spol}(g, g')).$$

Multiplying both sides by $\hat{\tau}$, we have

$$\mathrm{LT}(\hat{\tau}\tau'' g'') \leq \mathrm{LT}(\gamma\tau g - \gamma'\tau' g') < \mathrm{LT}(\tau g).$$

The existence of g'' and $\hat{\tau}\tau''$ contradicts the choice of g and τ. □

6. The algorithm

We shall now present a simple algorithm which computes as $\mathcal{S}$-Gröbner basis of an ideal based on the criterion. This algorithm is quite different from Faugère's, in that it is a direct application of the criterion. In particular, it does not involve reductions that yield more then one result, nor the more rigorous simplification rules. See Section 7.2 for a detailed discussion.

One first problem is that to check condition 2 of definition 16 we need to know $\mathrm{LT}(\mathrm{Syz}\,\mathcal{F})$, since

$$\mathcal{S}(tf) = t\mathcal{S}(f) \iff t\mathcal{S}(f) \notin \mathrm{LT}(\mathrm{Syz}\,\mathcal{F}).$$

We almost never know this before hand; therefore, we introduce a new variable L, a subset of $\mathrm{LT}(\mathrm{Syz}\,\mathcal{F})$. At the beginning of the algorithm, we simply assume $L = \varnothing$. We make use of L whenever we need to check if $t\mathcal{S}(f) = \mathcal{S}(tf)$ by checking whether $t\mathcal{S}(f)$ belongs to $\langle L\rangle \subseteq P^m$, the P-module generated by L. We then replace condition 2 of definition 16 by:

$$\mathcal{S}(u_i g_i) = \mathrm{LT}(u_i)\mathcal{S}(g_i) \iff \mathrm{LT}(u_i)\mathcal{S}(g_i) \notin \langle L\rangle.$$

By doing so, we end up considering more pairs than we should, but we do not skip any legitimate pair.

So, when (g_1, g_2) is a normal pair (with the weakened condition 2), we calculate a polynomial $f = \mathrm{Spol}(g_1, g_2)$ and a $\sigma = \max(u_1 g_1, u_2 g_2)$. Thereafter we $\mathcal{S}$-reduce f with respect to σ. Note that σ satisfies the hypothesis of Theorem 10. If the $\mathcal{S}$-reduction yields 0, we know that $\sigma \in \mathrm{LT}(\mathrm{Syz}\,\mathcal{F})$; accordingly, we enlarge L by inserting σ. Otherwise, we obtain a nonzero polynomial, which tells us that $\sigma = \mathcal{S}(f)$.

G is the set which will contain the $\mathcal{S}$-Gröbner basis; we add elements to G as we find them. For each element g we add to G, we also store $\mathcal{S}(g)$; thus, G is more precisely a set of pairs (g, σ). When an $\mathcal{S}$-reduction returns a nonzero polynomial f, we insert f into G. Initially, $G = \emptyset$, rather than a set containing $\{f_i\}$, since we do not know if f_i is $\mathcal{S}$-irreducible.

B is the set of pairs of the form (f, σ), where f is a polynomial that we $\mathcal{S}$-reduce with respect to σ. Initially, we know that $\mathcal{S}(f_i) = e_i$; therefore, we initialize $B = \{(f_i, e_i)\}_{i=1}^m$.

The idea of the algorithm is to build an $\mathcal{S}$-Gröbner basis by finding its elements in ascending value of $\mathcal{S}$; that is, always to choose $(f, \sigma) \in B$ such that σ is minimal. (See step 4c.)

Remark 20. In virtue of remark 19, for each σ we can keep in B at most one polynomial f such that $\mathcal{S}(f) = \sigma$. For the same reason we can, at any time, remove (f, σ) from B if we can find another polynomial f' such that $\mathcal{S}(f') = \sigma$ and $\mathrm{LT}(f') < \mathrm{LT}(f)$.

In practice we will remove from B a pair (f, σ) if we can find a $t \in \mathbb{T}^n$ and a $(f', \sigma') \in G \cup B$ such that $t\sigma' = \sigma$ and $t\,\mathrm{LT}(f') < \mathrm{LT}(f)$.

The pseudo code of the algorithm is the following:

```
Input:: $\mathcal{F} = (f_1, \ldots, f_m)$: an element of $P^m$,
    $\mu$: an ordering on $\mathbb{T}^n$,
    $\mu'$: an ordering on $\mathbb{T}^n_m$.
    Output:: $G$: an $\mathcal{S}$-Gröbner basis of $I = (f_1, \ldots, f_m)$.
  (1) $L := \varnothing$
  (2) $G := \varnothing$
  (3) $B := \{(f_1, e_1), \ldots, (f_m, e_m)\}$
  (4) While $B \neq \varnothing$
      (a) $B := \{(f, \sigma) \in B \mid \sigma \notin \langle L \rangle\}$
      (b) Remove from $B$ any $(f, \sigma)$ such that we can find $(f', \sigma') \in G \cup B$, $t \in \mathbb{T}^n$
          satisfying $t\sigma' = \sigma$ and $\mathrm{LT}(tf') < \mathrm{LT}(f)$
      (c) Pick $(f, \sigma) \in B$ with minimal $\sigma$.
      (d) $f := \mathcal{S}$-reduce$(f, \sigma, G)$
      (e) If $f \neq 0$ then
          (i) $B := \mathrm{UpdatePairs}(L, G, B, (f, \sigma))$
          (ii) $G := G \cup \{(f, \sigma)\}$
      (f) Else
          (i) $L := L \cup \{\sigma\}$
  (5) Return $\{g : (g, \sigma) \in G\}$
```

Note that, since L may change during each iteration, some pairs we assumed to be normal turn out not to be normal. We remove those in step 4a.

In step 4b we implement the idea presented in Remark 20. Note that this is an optimization; the algorithm will successfully terminate without this line.

We still have to describe the two procedures Algorithm 6 invokes. The first is $\mathcal{S}$*-reduce*:

```
[$\mathcal{S}$-reduce]
  Input:: $f$: an element of $I$,
      $\sigma$: an element of $\mathbb{T}^n_m$,
      $G$: a set that contains the elements $(g, \mathcal{S}(g))$ of an $\mathcal{S}$-Gröbner basis with $\mathcal{S}(g) < \sigma$.
      Output:: $f$: an $\mathcal{S}$-irreducible polynomial with respect to $\sigma$.
    (1) $f := f / \mathrm{LC}(f)$
    (2) While $\exists (g, \mathcal{S}(g)) \in G, t \in \mathbb{T}^n$ such that $t \, \mathrm{LT}(g) = \mathrm{LT}(f)$ and $t\mathcal{S}(g) < \sigma$
        (a) $f := f - tg / \mathrm{LC}(g))$
        (b) If $f = 0$ then Return 0
        (c) $f := f / \mathrm{LC}(f)$
    (3) Return $f$
```

This algorithm takes as input a polynomial f and a $\sigma \in \mathbb{T}^n_m$ and, as long as there is an $\mathcal{S}$-reductor for f in G, performs $\mathcal{S}$-reduction steps. Because of the hypothesis on G we know we obtain an $\mathcal{S}$-irreducible polynomial with respect to σ.

The second is *UpdatePairs*:

```
[UpdatePairs]
  Input:: $L$: a subset of $\mathrm{LT}(\mathrm{Syz}\,\mathcal{F})$,
      $G$: a set that contains the elements $(g, \mathcal{S}(g))$ of a $\mathcal{S}$-Gröbner basis with $\mathcal{S}(g) < \sigma$,
      $B$: a set that contains elements $(g, \sigma_g)$ of polynomials that have yet to be considered,
      $(f, \mathcal{S}(F))$: where $f \in I \setminus \{0\}$.
      Output:: $B'$: a set of pairs $(f', \sigma)$ that satisfy Theorem 10, produced by the criterion.
    (1) $B' := \varnothing$
    (2) For each $(g, \mathcal{S}(g)) \in G$, if $(f, g)$ is a normal pair
        (a) Compute $u_1$, $u_2$ such that $\mathrm{Spol}(f, g) = u_1 f + u_2 g$
        (b) $\sigma := \max(u_1 \mathcal{S}(f), u_2 \mathcal{S}(g))$
        (c) $B' := B' \cup \{(\mathrm{Spol}(f, g), \sigma)\}$
    (3) Return $B' \cup B$
```

Proposition 21. *Algorithm 6 terminates.*

Proof. First we show that step 4(f)i is executed only a finite number of times.

Because of step 4a, at a given time, we only consider σ that do not belong to L; so when we execute step 4(f)i we really enlarge the P-module generated by L. Since P^m is noetherian this can happen only a finite number of times.

Also, that step 4(e)i is executed only a finite number of times. First note that if f is not primitive $\mathcal{S}$-irreducible (that is, f is only $\mathcal{S}$-irreducible), then Algorithm 6 does nothing, so no new polynomials are generated. In the proof of Proposition 14, we see that an $\mathcal{S}$-Gröbner basis contains only a finite number of primitive $\mathcal{S}$-irreducible polynomials. This completes the proof. □

Theorem 22. *Algorithm 6 computes an $\mathcal{S}$-Gröbner basis of I.*

Proof. This is a direct consequence of criterion of Theorem 18: Previous remarks have shown that G contains only $\mathcal{S}$-irreducible polynomials, and the initial value of B ensures that the algorithm satisfies the first condition. For the second condition, for each normal pair (g_1, g_2), we ensure that we have a polynomial f and a monomial t such that $\mathcal{S}(tf) = \mathcal{S}(\mathrm{Spol}(g_1, g_2))$. □

The fact that non-primitive $\mathcal{S}$-irreducible polynomials do not generate any new pairs plays a *central* role in this proof of termination. Without it, the thesis does not hold: if we drop condition (1) of Definition 16, it is possible that the algorithm could enter an infinite loop, computing an infinite number of polynomials of the form $t_i f$ where $\{t_i\}$ is an infinite set of terms and f is an $\mathcal{S}$-irreducible polynomial and each of the $t_i f$ is $\mathcal{S}$-irreducible itself. (This occurs, for example, in the implementation of [15].)

7. Comparison with previous work

In this section, we consider how this algorithm is both similar and different to two algorithms in past work: the staggered linear basis algorithm of Gebauer and Möller [9] and the F5 algorithm of Faugère [5]. We also illustrate explicit differences on three particular examples.

7.1. Comparison with Staggered Linear Bases.

The Staggered Linear Basis algorithm (in the rest of this section, SLB) [9] introduced a special kind of Gröbner basis.

Definition 23. The set $B \subset I$ is a *staggered linear basis of the ideal I if for all $f \in P$*

- if $f, g \in B$ and $\mathrm{LT}(f) = \mathrm{LT}(g)$, then $f = g$; and
- if $t \in \mathbb{T}$ and $tf \in B$, then $f \in B$.

A full review of SLB is beyond the scope of this paper, but it is worth comparing to the present algorithm because both use trivial syzygies to detect zero reductions. To facilitate the explanation, we temporarily adopt the notation $t_i = \mathrm{LT}(f_i)$ and $t_{i,j} = \mathrm{lcm}(t_i, t_j)$.

SLB tracks monomial ideals for each polynomial among the generators. Initially, we have

$$Z_i = (t_1, t_2, \ldots, t_{i-1}).$$

Critical pairs (f_i, f_j) (with $i < j$) are rejected whenever $t_{ij}/t_j \in Z_i$. If instead the S-polynomial of (f_i, f_j) is computed, then Z_j is expanded by adding the ideal generated by t_{ij}/t_j. If reduction of the S-polynomial results in a new polynomial f_k being added to the basis, SLB also creates a new ideal

$$Z_k = (Z_j + (t_i)) : (t_{ij}/t_j) + (t_1, \ldots, t_{k-1}).$$

Despite the use of principal syzygies in the initial definition of Z_i, a fundamental difference between the algorithms lies in the fact that SLB does not compute, let alone consider, the leading module term $\mathcal{S}(f)$ of any polynomials. So a polynomial can be $\mathcal{S}$-irreducible even if it is top-reducible, and the normal pairs of the F5 Criterion are not the same as the critical pairs of SLB. As a result, the approach in SLB behaves quite differently, and fails to detect certain zero reductions detected by F5 and the present algorithm.

7.2. Comparison with F5.

At first glance, algorithm 6 may appear very different from the F5 algorithm. However, if we define μ' to be

$$te_i <_{\mu'} se_j \iff \begin{cases} i < j \quad \text{or} \\ i = j \text{ and } t < s \end{cases}$$

for any $t, s \in \mathbb{T}^n$ and $1 \leq i, j \leq m$, there is an interesting relationship between $\mathcal{S}$-Gröbner bases and $\mathrm{LT}(\operatorname{Syz}\mathcal{F})$. Define, for $1 \leq l \leq m$, $\pi_l : P^m \to P$ as the projection on the l-th component, then

$$\pi_l(\operatorname{PSyz}\mathcal{F}) = (f_1, \ldots, f_{l-1}) \tag{7.1}$$

where $\operatorname{PSyz}(\mathcal{F})$ is the P-module of principal syzygies, defined as $\operatorname{PSyz}(\mathcal{F}) = \langle f_i e_j - f_j e_i \rangle_P \subseteq P^m$; $\operatorname{PSyz}(\mathcal{F})$ is clearly a P-submodule of $\operatorname{Syz}(\mathcal{F})$.

Suppose we have $f \in I \setminus \{0\}$ and we know $\mathcal{S}(f) = te_i$, for some $t \in \mathbb{T}^n$. It follows from the definition of $\mathcal{S}$ that $f \in (f_1, \ldots, f_i)$. Hence, (7.1) implies that

$$\mathrm{LT}(f)e_{i+j} \in \mathrm{LT}(\operatorname{PSyz}(\mathcal{F})) \quad \text{for some } j \geq 1.$$

With this choice for μ', we can improve the performance of Algorithm 6 by adding an instruction right after step 4(e)ii:

$$L := L \cup \{\mathrm{LT}(f)e_{i+1}, \mathrm{LT}(f)e_{i+2}, \ldots, \mathrm{LT}(f)e_m\},$$

where $\sigma = te_i$ for some $t \in \mathbb{T}^n$. In other words, whenever we find a new element of G, we also find new elements of L.

Also, due to the ordering on P^m, the structure of an $\mathcal{S}$-Gröbner basis G is very special. We find the elements of G in ascending value of $\mathcal{S}$: we first find all the elements g such that $\mathcal{S}(g) = te_1$ for some $t \in \mathbb{T}^n$, then those g such that $\mathcal{S}(g) = te_2$ for some $t \in \mathbb{T}^n$ and so on. Is easy to see that the real value of f_l is never considered in any computation, until the algorithm has finished producing all the elements of G with $\mathcal{S}(g) = te_i$ for some $t \in \mathbb{T}^n$ and $i < l$. If we make the further assumption that $\operatorname{Syz}(\mathcal{F}) = \operatorname{PSyz}(\mathcal{F})$, we conclude that the algorithm never reduces a polynomial to 0, since we discover every leading term of the syzygies in advance.

Therefore, we may say that, in this case, Algorithm 6 is *incremental*, as it first produces an $\mathcal{S}$-Gröbner basis of (f_1), then an $\mathcal{S}$-Gröbner basis of (f_1, f_2) and so on, and avoids all the reductions to zero; this behavior is the same as Faugère's F5 algorithm.

We can couch the use of "simplification rules" in F5 [5, sect. 6], also called the *rewritable criterion*, in vocabulary similar to that used in this paper: F5's algorithm to compute S-polynomials (SPol) discards any (te_i, f) when

- there exists some other $(t'e_i, f') \in G \cup B \cup B'$ such that $t \mid t'$, and
- f' was computed *before* f.

This concept is related to Remark 19 in this paper; roughly we know we can "decide" how to obtain an $\mathcal{S}$-irreducible polynomial with a given signature. We prefer to start with a polynomial with the smallest leading term we know of, while in F5 just the first generated polynomial is kept.

This parallel carries over to the computation of L, which here is used to prevent the computation of any $te_i \in \mathrm{LT}\left(\operatorname{Syz}\mathcal{F}\right)$ more than once. When a polynomial is reduced to zero in F5, the simplification rule is added even though the polynomial is discarded, and this rule ensures that any polynomial f with $\mathcal{S}\left(f\right) = t'e_i$, where $t \mid t'$, is not computed. In other words, F5 has an implicit provision for avoiding the computation of non-trivial syzygies, like the algorithm here.

7.3. **Concrete examples.**

We examine how all three examples perform on three "standard" systems:

Algorithm	**Number of zero reductions** MMT92	Cyclic-5	Cyclic-6	Katsura-5
Staggered Linear Basis	3	46	446	10
F5	0	0	16	0
Algorithm 6	0	0	8	0

Table 1. Number of zero reductions during execution of algorithms SLB, F5, and Algorithm 6.

Algorithm (size of red. GB)	**Size of basis** MMT92	Cyclic-5	Cyclic-6	Katsura-5
Staggered Linear Basis	8	38	99	22
F5	10	39	202	30
Algorithm 6	10	39	155	30

Table 2. Size of the Gröbner basis computed by algorithms SLB, F5, and Algorithm 6.

- the system “MMT92”, $F = \{yz^3 - x^2t^2, xz^2 - y^2t, x^2y - z^2t\}$ from [5] (this seems first to appear in non-homogenized form in [12]);
- the homogenized Cyclic-5 system; and
- the homogenized Katsura-5 system.

We consider

(1) the number of zero reductions; and
(2) the size of the Gröbner basis generated.

The tests were carried out in unoptimized implementations of each algorithm in Sage [16, 1, 14, 13], and are available online.

The results are in Tables 1 and 2. Table 1 shows that the Staggered Linear Basis algorithm computes some zero reductions *even though* the systems are regular sequences. Neither F5 nor Algorithm 6 computes any zero reductions except in Cyclic-6, which is not a regular sequence. In that system, Algorithm 6 computes a smaller basis, and it computes fewer zero reductions. This appears to be due to the fact that it proceeds by ascending signature (line 4c) rather than by ascending lcm (compare to algorithm Spol in [5]).

8. Conclusions and future work

This paper has reformulated the F5 criterion, which in its original form is due to [5], and provided a new proof of this criterion's correctness. We have introduced the ideas of *$\mathcal{S}$-Gröbner basis* and *$\mathcal{S}$-irreducible polynomials,* and have shown that if a set of polynomials G satisfies the F5 criterion, then G is an $\mathcal{S}$-Gröbner basis and not just a Gröbner basis. In this new setting, we were able to drop many restrictions present in [5]: we can freely choose any ordering on P^m, and there is no need to for the sequence $(f_1, \ldots, f_m)$ to be regular.

Our statement of the criterion is quite different from the original: we require that all the polynomials in the set G be $\mathcal{S}$-irreducible; we require that if $e_i \notin \mathrm{NS}(\mathrm{Syz}\,\mathcal{F})$, then there exist $g \in G$ such that $\mathcal{S}(g) = e_i$; and we impose a condition on the *signature* $\mathcal{S}(\mathrm{Spol}(g_1, g_2))$, rather than the usual condition that

$$\mathrm{Spol}\left(g_1, g_2\right) = \sum_{i=1}^{\#G} h_i g_i \quad \text{such that} \quad h_i \neq 0 \implies \mathrm{LT}\left(h_i\right) \mathrm{LT}\left(g_i\right) \leq \mathrm{LT}\left(\mathrm{Spol}\left(g_1, g_2\right)\right).$$

(Faugère calls this latter condition $o\left(\mathrm{Spol}\left(g_1, g_2\right)\right)$.) We also changed the definition of *normal pair* by adding a new condition: the fact that we can consider only primitive $\mathcal{S}$-irreducible polynomials.

We then proposed a simple algorithm to show an application of the new criterion. The algorithm presented here is mainly demonstrative, and does not include many "obvious" optimizations such as holding off on the computation of a new polynomial f until it is actually needed in step 4d of Algorithm 6.

The authors would like to thank the referees for helpful and instructive comments that improved the paper.

References

[1] Martin Albrecht and John Perry. Implementation of Faugère's F5 algorithm. Sage library, 2008.

[2] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, LIP6, 2006.

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

[4] Bruno Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In E. W. Ng, editor, *Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation, Marseille, June 26-28, 1979*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21, Berlin - Heidelberg - New York, 1979. Springer.

[5] J. C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *ISSAC '02: Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, New York, NY, USA, 2002. ACM Press.

[6] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.

[7] Justin Gash. *On Efficient Computation of Gröbner Bases*. Ph.D. dissertation, Indiana University, Bloomington, IN, 2008.

[8] R. Gebauer and H. Möller. A new implementation of Buchberger's algorithm. 1987.

[9] Rudiger Gebauer and Hans Möller. Buchberger's algorithm and staggered linear bases. In *Proceedings of SYMSAC 1986 (Waterloo/Ontario)*, pages 218–221. ACM Press, 1986.

[10] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra*, volume 1. Springer, 2000.

[11] Daniel 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, pages 146–156. Springer LNCS, 1983.

[12] H. Michael Möller, Teo Mora, and Carlo Traverso. Gröbner bases computation using syzygies. In *ISSAC '92: Papers from the international symposium on Symbolic and algebraic computation*, pages 320–328, New York, NY, USA, 1992. ACM.

[13] John Perry. Implementation of staggered linear basis algorithm. Sage library, 2008.

[14] John Perry. Implementation of arri's F5 variant. Sage library, 2010.

[15] Till Stegers. Faugere's F5 algorithm revisited. Cryptology ePrint Archive, Report 2006/404, 2006. `http://eprint.iacr.org/`.

[16] William Stein. *Sage: Open Source Mathematical Software (Version 4.1.1)*. The Sage Group, 2010. `www.sagemath.org`.

Scuola Normale Superiore di Pisa - Piazza dei Cavalieri, 7 - 56126 Pisa, Italy
Current address: Microsoft Corporation
E-mail address: arri@sns.it

University of Southern Mississippi, Hattiesburg, MS USA
E-mail address: john.perry@usm.edu