MATHEMATICS OF COMPUTATION
Volume 85, Number 297, January 2016, Pages 449–465
http://dx.doi.org/10.1090/mcom/2969
Article electronically published on May 20, 2015

A NEW FRAMEWORK FOR COMPUTING GRÖBNER BASES

SHUHONG GAO, FRANK VOLNY IV, AND MINGSHENG WANG

Abstract. This paper presents a new framework for computing Gröbner bases for ideals and syzygy modules. It is proposed to work in a module that accommodates any given ideal and the corresponding syzygy module (for the given generators of the ideal). A strong Gröbner basis for this module contains Gröbner bases for both the ideal and the syzygy module. The main result is a simple characterization of strong Gröbner bases. This characterization can detect useless S-polynomials without reductions, thus yields an efficient algorithm. It also explains all the rewritten rules used in F5 and the recent papers in the literature. Rigorous proofs are given for the correctness and finite termination of the algorithm. For any term order for an ideal, one may vary signature orders (i.e. the term orders for the syzygy module). It is shown by computer experiments on benchmark examples that signature orders based on weighted terms are much better than other signature orders. This is useful for practical computation. Also, since computing Göbner bases for syzygies is a main computational task for free resolutions in commutative algebra, the algorithm of this paper should be useful for computing free resolutions in practice.

1. Introduction

Polynomial systems are ubiquitous in mathematics, science and engineering. Gröbner basis theory is one of the most powerful tools for solving polynomial systems and is essential in many computational tasks in algebra and algebraic geometry. Buchberger introduced in 1965 the first algorithm for computing Gröbner bases, and it has been implemented in most computer algebra systems including Maple, Mathematica, Magma, Sage, Singular, Macaulay 2, CoCoA, etc.

There has been extensive effort in finding more efficient algorithms for computing Gröbner bases. In Buchberger's original algorithm (1965, [2]), one has to reduce many useless S-polynomials (i.e., those that reduce to 0 via long division), and each reduction is time consuming. It is natural to avoid useless reductions as much as possible. Buchberger [3, 4] discovered two simple criteria for detecting useless S-polynomials. Note that a reduction of an S-polynomial to 0 corresponds to a syzygy (for the initial list of polynomials). Möller, Mora and Traverso (1992, [19]) go a step further to present an algorithm using the full module of syzygies, however, their algorithm is not very efficient. Faugère (2002, [11]) introduced the idea of signatures and rewriting rules that can detect many useless S-polynomials, hence

Received by the editor July 25, 2013 and, in revised form, May 9, 2014.
2010 *Mathematics Subject Classification.* Primary 13P10, 68W10.
Key words and phrases. Gröbner basis, Buchberger's algorithm, Syzygy module, F5 algorithm, module.
The work presented in this paper was partially supported by the 973 Project (No. 2013CB834203), the National Science Foundation of China under Grant 11171323, and the National Science Foundation of USA under grants DMS-1005369 and CCF-0830481.

saving a significant amount of time. In fact, for a regular sequence of polynomials, his algorithm F5 detects all useless reductions. By computer experiments, Faugère showed that his algorithm F5 is many times faster than previous algorithms. In fact, Faugère and Joux (2003, [12]) solved the first Hidden Field Equation (HFE) Cryptosystem Challenge which involves a system of 80 polynomial equations with 80 variables over the binary field (1996, [21]).

In another direction of research, one tries to speed up the reduction step. Lazard (1983, [17]) pointed out the connection between Gröbner bases and linear algebra, that is, a Gröbner basis can be computed by Gauss elimination of a Sylvester matrix. The XL algorithm of Courtois et al. (2000, [6]) is an implementation of this Sylvester matrix, which was recently improved by Ding et al. (2008, [5]). A more clever approach is the F4 algorithm of Faugère (1999, [10]), which deals with much smaller matrices. F4 is an efficient method for reducing several S-polynomials simultaneously where the basic idea is to apply fast linear algebra methods to the submatrix of the Sylvester matrix consisting of only those rows that are needed for the reductions of a given list of S-polynomials. This method benefits from the efficiency of fast linear algebra algorithms. The main problem with this approach, however, is that the memory usage grows quickly (compared to F5 for example), even for medium systems of polynomials.

F5 as presented in [11] is difficult to understand, the proofs of its correctness and finite termination contain significant gaps. Stegers (2006 [23] filled some details of the proofs under the assumption of two conjectures, but one of which was later shown to be false by Gash (2008 [14]). More recently, Arri and Perry (2011 [1]) presented a simpler theory for signature based algorithms. They gave a revised F5 criterion with correct proof, however, their proof of finite termination is flawed (see details in Section 3).

The main contribution of the current paper is to present a new simple theory for computing Gröbner bases. Every list of polynomials defines an ideal and a syzygy module. Most papers in the literature focus on computing Gröbner bases for ideals, while Gröbner bases for syzygies are computed by a totally different method. We show that the two types of Gröbner bases can be computed by a unified framework. We work in a larger module that contains both the ideal and the syzygy module for a given list of polynomials, and define signatures, J-pairs, and reductions in a natural fashion. A strong Gröbner basis for the big module contains a Gröbner basis for the ideal as well as a Gröbner basis for the syzygy module. Our main result is a simple characterization of strong Gröbner bases (see Theorem 2.4). This characterization has the desirable features that useless J-pairs can be detected without performing any reduction and that J-pairs can be processed in any order. Note that computing Gröbner bases for syzygies is a main computational task for free resolutions in commutative algebra. Our work should be useful for computing free resolutions in practice.

The paper is organized as follows. In Section 2, we introduce the basic concepts and theory for our algorithm. In particular, we define signatures, regular top-reductions, super top-reductions, J-pairs, and strong Gröbner bases. The main result is Theorem 2.4. As a special case, this provides a proof for the correctness of the G2V algorithm in [13], which was missing there. In Section 3, we present our algorithm and give a simple proof for its finite termination. We also present computer experiments on some benchmark examples and compare the times of our

algorithm under different signature orders. In the last section, we discuss how our theory is related to other related works and mention some recent progress since the current paper was initially submitted (in 2010).

2. Theory

Let $R = \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial ring over a field $\mathbb{F}$ with n variables. For any polynomials $g_1, \ldots, g_m \in R$, we define an ideal of R:

$$I = \langle g_1, \ldots, g_m \rangle = \{u_1 g_1 + \cdots + u_m g_m : u_1, \ldots, u_m \in R\} \subseteq R, \tag{2.1}$$

and a submodule of R^m:

$$\mathbf{H} = \{(u_1, \ldots u_m) \in R^m : u_1 g_1 + \cdots + u_m g_m = 0\}, \tag{2.2}$$

which is called *the syzygy module* of $\mathbf{g} = (g_1, \ldots, g_m)$. We would like to develop an algorithm that computes Gröbner bases for both I and $\mathbf{H}$ under any given term orders on R and R^m.

To establish the theoretical foundation for our algorithm, we work in the larger R-module $R^m \times R$ which allows us to handle the ideal I and the syzygy module $\mathbf{H}$ simultaneously. Note that elements of R^m are viewed as row vectors and are denoted by bold letters say $\mathbf{g}, \mathbf{u}$, etc. We consider the following subset of $R^m \times R$:

$$M = \left\{(\mathbf{u}, v) \in R^m \times R : \mathbf{u}\mathbf{g}^t = v\right\}. \tag{2.3}$$

It is an R-submodule of $R^m \times R$ because it is closed under addition and multiplication by R, that is, for any two pairs $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in M$ and any $r_1, r_2 \in R$, we have

$$r_1 p_1 + r_2 p_2 = (r_1 \mathbf{u}_1 + r_2 \mathbf{u}_2, r_1 v_1 + r_2 v_2) \in M.$$

This operation on pairs is performed implicitly by Gröbner basis algorithms when performing reductions, S-polynomials or J-pairs where one just stores the v-part and the leading terms of the $\mathbf{u}$ (namely signatures, see definition below).

For $1 \leq i \leq m$, let $\mathbf{E}_i \in R^m$ be the ith unit vector whose ith entry is 1 and other entries are 0. Note that a monomial (or a term) in R is of the form

$$x^\alpha = \prod_{i=1}^{n} x_i^{a_i}$$

where $\alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n$ is any vector of nonnegative integers, and a term in R^m is of the form

$$x^\alpha \mathbf{E}_i$$

where $1 \leq i \leq m$ and $\alpha \in \mathbb{N}^n$. We say $x^\alpha \mathbf{E}_i$ divides $x^\beta \mathbf{E}_j$ if $i = j$ and x^α divides x^β, with the quotient

$$(x^\beta \mathbf{E}_i)/(x^\alpha \mathbf{E}_i) = x^{\beta - \alpha} \in R.$$

Also, the R-module M in (2.3) is generated by

$$(\mathbf{E}_1, g_1), (\mathbf{E}_2, g_2), \ldots, (\mathbf{E}_m, g_m). \tag{2.4}$$

Fix any term order $\prec_1$ on R and any term order $\prec_2$ on R^m (both are compatible with multiplication by monomials in R and there are no infinite decreasing sequences of terms). We emphasize that the order $\prec_2$ may or may not be related to $\prec_1$ in the theory below, though $\prec_2$ is usually *compatible* with $\prec_1$, that is,

$$x^\alpha \prec_1 x^\beta \quad \text{iff} \quad x^\alpha \mathbf{E}_i \prec_2 x^\beta \mathbf{E}_i \text{ for all } 1 \leq i \leq m.$$

For the sake of convenience, we shall use the following convention for leading terms:

$$\mathrm{lm}(v) = \mathrm{lm}_{\prec_1}(v), \quad \mathrm{lm}(\mathbf{u}) = \mathrm{lm}_{\prec_2}(\mathbf{u})$$

for any $v \in R$ and $\mathbf{u} \in R^m$. Note that, for $v \in R$, $\mathrm{lm}(v)$ is a monomial x^α, while, for $\mathbf{u} \in R^m$, $\mathrm{lm}(\mathbf{u})$ is a term $x^\alpha \mathbf{E}_i$ for some $\alpha \in \mathbb{N}^n$ and $1 \le i \le m$. We make the convention that, if $v = 0$, then $\mathrm{lm}(v) = 0$; similarly for $\mathrm{lm}(\mathbf{u})$. This should not cause any confusion, but the reader should keep the two different orders in mind.

We adapt the concepts in [13] to the module $R^m \times R$. For any pair $p = (\mathbf{u}, v) \in R^m \times R$, we call $\mathrm{lm}(\mathbf{u})$ the *signature* of p. Our definition of signatures is different from that of F5 [1,11] where each $v \in I = \langle g_1, \ldots, g_m \rangle$ is associated with a signature:

$$S(v) = \min\{\mathrm{lm}(\mathbf{u}) : \mathbf{u} \in R^m \text{ with } \mathbf{u}\mathbf{g}^t = v\}.$$

The F5 signature is hard to use in practice, while our signature is natural and easy to use.

We define top-reduction similar to the top-reduction in F5. Let $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in R^m \times R$ be any two pairs. When v_2 is nonzero, we say p_1 is *top-reducible* by p_2 if the following two conditions are satisfied:

(i) v_1 is nonzero and $\mathrm{lm}(v_2)$ divides $\mathrm{lm}(v_1)$; and
(ii) $\mathrm{lm}(t\mathbf{u}_2) \preceq \mathrm{lm}(\mathbf{u}_1)$ where $t = \mathrm{lm}(v_1)/\mathrm{lm}(v_2)$.

The corresponding *top-reduction* is then

$$p_1 - ctp_2 = (\mathbf{u}_1 - ct\mathbf{u}_2, v_1 - ctv_2), \tag{2.5}$$

where $c = \mathrm{lc}(v_1)/\mathrm{lc}(v_2)$. The effect of a top-reduction is that the leading monomial in the v-part is decreased without increasing the signature of p_1. Such a top-reduction is called *regular*, if

$$\mathrm{lm}(\mathbf{u}_1 - ct\mathbf{u}_2) = \mathrm{lm}(\mathbf{u}_1),$$

and *super* otherwise. So the signature of $p_1 - ctp_2$ remains the same as p_1 under a regular top-reduction but becomes smaller under a super top-reduction. A super top-reduction happens if

$$\mathrm{lm}(t\mathbf{u}_2) = \mathrm{lm}(\mathbf{u}_1) \text{ and } \frac{\mathrm{lc}(\mathbf{u}_1)}{\mathrm{lc}(\mathbf{u}_2)} = \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}.$$

When $v_2 = 0$, $p_2 = (\mathbf{u}_2, 0) \in M$ corresponds to the syzygy $\mathbf{u}_2$. We say that p_1 is *top-reducible* by a syzygy $p_2 = (\mathbf{u}_2, 0)$ if $\mathbf{u}_2$ is nonzero and $\mathrm{lm}(\mathbf{u}_2)$ divides $\mathrm{lm}(\mathbf{u}_1)$. A top-reduction by a syzygy is always called *super*. Hence, if $p_1 = (\mathbf{u}_1, v_1)$ is super top-reducible by $p_2 = (\mathbf{u}_2, v_2)$ in either case, then $\mathrm{lm}(\mathbf{u}_2)$ divides $\mathrm{lm}(\mathbf{u}_1)$. We note that a pair $(\mathbf{u}_1, 0)$ is never top-reducible by $(\mathbf{u}_2, v_2)$ with $v_2 \neq 0$, and in our algorithm below, we only detect super top-reductions of the two kinds defined here, but never actually perform super top-reductions.

Definition 2.1. A subset G of M is called a strong Gröbner basis for M if every nonzero pair in M is top-reducible by some pair in G.

This definition is similar to the usual definition for Gröbner bases for ideals: a subset G of an ideal I is called a Gröbner basis if the leading term of every polynomial in I is divisible by the leading term of some polynomial in G, that is, every polynomial in I is top-reducible by some polynomial in G.

Proposition 2.2. *Suppose that* $G = \{(\mathbf{u}_1, v_1), (\mathbf{u}_2, v_2), \ldots, (\mathbf{u}_k, v_k)\}$ *is a strong Gröbner basis for* M. *Then*

(1) $\mathbf{G}_0 = \{\mathbf{u}_i : v_i = 0, 1 \le i \le k\}$ *is a Gröbner basis for the syzygy module of* $\mathbf{g} = (g_1, \ldots, g_m)$, *and*
(2) $G_1 = \{v_i : 1 \le i \le k\}$ *is a Gröbner basis for* $I = \langle g_1, \ldots, g_m \rangle$.

Proof. For any $\mathbf{u} = (u_1, \ldots, u_m)$ in the syzygy module of $\mathbf{g}$, we have $(\mathbf{u}, 0) \in M$. By our assumption, $(\mathbf{u}, 0)$ is top-reducible by some pair $(\mathbf{u}_i, v_i)$ in G. Then we must have $v_i = 0$, thus $\mathbf{u}_i \in G_0$ and $\mathrm{lm}(\mathbf{u})$ is reducible by $\mathrm{lm}(\mathbf{u}_i)$. This proves that G_0 is a Gröbner basis for the syzygy module of $\mathbf{g}$.

Now suppose $v \in I$ and is nonzero. Then there exists $\mathbf{u} = (u_1, \ldots, u_m) \in R^m$ so that $\mathbf{u}\mathbf{g}^t = v$, hence $(\mathbf{u}, v) \in M$. Among all such $\mathbf{u}$, we pick one so that $\mathrm{lm}(\mathbf{u})$ is minimum. Since $(\mathbf{u}, v) \in M$, it is top-reducible by some $(\mathbf{u}_i, v_i)$ where $1 \le i \le k$. If $v_i = 0$, then we could use $(\mathbf{u}_i, 0)$ to reduce $(\mathbf{u}, v)$ to get a $\mathbf{u}'$ so that $\mathbf{u}'\mathbf{g}^t = v$ and $\mathrm{lm}(\mathbf{u}')$ is smaller than $\mathrm{lm}(\mathbf{u})$, contradicting to the minimality of $\mathrm{lm}(\mathbf{u})$. So $v_i \neq 0$ and $\mathrm{lm}(v_i)$ divides $\mathrm{lm}(v)$. Hence G_1 is a Gröbner basis for I. □

Remark. Note that $M \subset R^m \times R$ has a Gröbner basis in the classical sense of Burchberger as a submodule of R^{m+1} where the leading term of $(\mathbf{u}, v)$ is $\mathrm{lm}(v)\mathbf{E}_{m+1}$ if $v \neq 0$ and $\mathrm{lm}(\mathbf{u})$ if $v = 0$. The above proposition implies that a strong Gröbner basis for M is a classical Gröbner basis for M as a submodule of R^{m+1}, but the converse may not be true for an arbitrary submodule M of R^{m+1} (as our regular top-reduction must preserve signatures). This is why we call our basis a strong Gröbner basis[1].

We would like to develop a characterization in terms of G itself that is similar to Buchberger's criterion and can be used to detect useless S-polynomials without performing any reduction. We introduce the concept of J-pairs, similar to S-polynomials in Buchburger's algorithm. Suppose $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in R^m \times R$ are two pairs with v_1 and v_2 both nonzero. We form a joint pair from them as follows. Let

$$t = \mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2)), \quad t_1 = \frac{t}{\mathrm{lm}(v_1)}, \quad t_2 = \frac{t}{\mathrm{lm}(v_2)}.$$

Let $c = \mathrm{lc}(v_1)/\mathrm{lc}(v_2)$ and $T = \max(t_1\mathrm{lm}(\mathbf{u}_1), t_2\mathrm{lm}(\mathbf{u}_2))$. Without loss of generality, we assume $T = t_1\mathrm{lm}(\mathbf{u}_1)$. If

$$\mathrm{lm}(t_1\mathbf{u}_1 - ct_2\mathbf{u}_2) = T, \tag{2.6}$$

then T is called the *J-signature* of p_1 and p_2, while t_1p_1 is called a *J-pair* of p_1 and p_2. We do not define any J-pair for p_1 and p_2 when $\mathrm{lm}(t_1\mathbf{u}_1 - ct_2\mathbf{u}_2) \prec T$, which happens if

$$t_1\mathrm{lm}(\mathbf{u}_1) = t_2\mathrm{lm}(\mathbf{u}_2), \text{ and } \frac{\mathrm{lc}(\mathbf{u}_1)}{\mathrm{lc}(\mathbf{u}_2)} = \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}.$$

In comparison to Buchberger's algorithm, the S-polynomial of v_1 and v_2 is $t_1v_1 - ct_2v_2$. In terms of pairs, this corresponds to a reduction:

$$t_1p_1 - ct_2p_2 = (t_1\mathbf{u}_1 - ct_2\mathbf{u}_2, t_1v_1 - ct_2v_2). \tag{2.7}$$

When (2.6) holds, (2.7) is a regular top-reduction of t_1p_1 by p_2. This means that the J-pair of p_1 and p_2 is defined if and only if (2.7) is a regular top-reduction. Hence the J-pair of any two pairs p_1 and p_2 is always regular top-reducible by p_1 or p_2. We point out that, in the case of S-polynomials, the goal is to cancel the

[1]We should note that the concept of strong Gröbner bases is also used in the literature for Gröbner bases over rings.

leading terms of the element v in the pair (u, v). In our J-pair, the leading terms of the elements v are not cancelled, but will be cancelled in later top-reductions. This seems strange at first glance, but it is useful in saving storage as a J-pair tp_i can be stored simply as a pair (t, i) where i is the index of the pair $p_i = (\mathbf{u}_i, v_i)$, instead of storing the actual pair $(t\mathbf{u}_i, tv_i)$. Also, we never define the J-pair of $p_1 = (\mathbf{u}_1, v_1)$ and $p_2 = (\mathbf{u}_2, v_2)$ when v_1 or v_2 is zero.

Lemma 2.3. *Let t be a monomial in R and $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in R^m \times R$. If tp_1 is regular top-reducible by p_2 (hence both v_1 and v_2 are nonzero), then $t_1 p_1$ is a J-pair of p_1 and p_2, where*

$$t_1 = \frac{lcm(lm(v_1), lm(v_2))}{lm(v_1)} = \frac{lm(v_2)}{\gcd(lm(v_1), lm(v_2))}$$

and t_1 is a divisor of t. Furthermore, $t_1 p_1$ is regular top-reducible by p_2.

Proof. Since tp_1 is regular top-reducible by p_2, we know that both v_1 and v_2 are nonzero and there is a monomial s such that

$$t\,\mathrm{lm}(v_1) = s\,\mathrm{lm}(v_2), \quad t\,\mathrm{lm}(\mathbf{u}_1) = \mathrm{lm}(t\,\mathbf{u}_1 - cs\,\mathbf{u}_2), \tag{2.8}$$

where $c = \mathrm{lm}(v_1)/\mathrm{lm}(v_2)$. Let

$$t_2 = \frac{\mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2))}{\mathrm{lm}(v_2)} = \frac{\mathrm{lm}(v_1)}{\gcd(\mathrm{lm}(v_1), \mathrm{lm}(v_2))}.$$

Then the first equation of (2.8) implies that, for some monomial w,

$$\begin{aligned} t &= \frac{\mathrm{lm}(v_2)}{\gcd(\mathrm{lm}(v_1), \mathrm{lm}(v_2))} w = t_1 w, \text{ and} \\ s &= \frac{\mathrm{lm}(v_1)}{\gcd(\mathrm{lm}(v_1), \mathrm{lm}(v_2))} w = t_2 w. \end{aligned}$$

Hence the second equation of (2.8) implies that $t_1\,\mathrm{lm}(\mathbf{u}_1) = \mathrm{lm}(t_1\mathbf{u}_1 - ct_2\mathbf{u}_2)$. This shows that $t_1 p_1$ is the J-pair of p_1 and p_2, and $t_1 p_1$ is regular top-reducible by p_2. □

Let G be any set of pairs in $R^m \times R$. We say that a pair $p = (\mathbf{u}, v) \in R^m \times R$ is regular top-reducible by G if it is regular top-reducible by at least one pair in G. We call p *eventually super top-reducible* by G if there is a sequence of regular top-reductions of p by pairs in G that reduce p to a pair $(\mathbf{u}', v')$ that is no longer regular top-reducible by G but is super top-reducible by at least one pair in G. Also, we say that a pair $p_1 = (\mathbf{u}_1, v_1)$ is *covered* by a pair $p_2 = (\mathbf{u}_2, v_2)$ if $\mathrm{lm}(\mathbf{u}_2)$ divides $\mathrm{lm}(\mathbf{u}_1)$ and $t\,\mathrm{lm}(v_2) \prec \mathrm{lm}(v_1)$ (strictly smaller) where $t = \mathrm{lm}(\mathbf{u}_1)/\mathrm{lm}(\mathbf{u}_2)$, and we say that a pair p is covered by G if it is covered by some pair in G. Note that there is no reduction at all in checking whether a pair is covered by G.

Theorem 2.4. *Suppose G is a subset of M such that, for any term $T \in R^m$, there is a pair $(\mathbf{u}, v) \in G$ and a monomial t such that $T = t\,lm(\mathbf{u})$. Then the following are equivalent:*

(a) *G is a strong Gröbner basis for M,*
(b) *every J-pair of G is eventually super top-reducible by G,*
(c) *every J-pair of G is covered by G.*

Proof. $(a) \Rightarrow (b)$ Let $p = (\mathbf{u}, v)$ be any J-pair of G. Then p is in M, hence top-reducible by G. We can perform regular top-reductions to p as much as possible, say to get $p' = (\mathbf{u}', v')$ which is not regular top-reducible. Since p' is still in M, it is top-reducible by G, hence must be super top-reducible by G. Therefore, p is eventually super top-reducible by G.

$(b) \Rightarrow (c)$ Let $p = (\mathbf{u}, v)$ be any J-pair from G. Since p is eventually super top-reducible by G, after a sequence of regular top-reductions of p by G, we can get a $p_0 = (\mathbf{u}_0, v_0) \in M$ such that p_0 is not regular top-reducible by G but is super top-reducible by some pair $p_1 = (\mathbf{u}_1, v_1) \in G$. By definition, every J-pair can be regular top-reduced by G, so we have $\mathrm{lm}(v_0) \prec \mathrm{lm}(v)$ and $\mathrm{lm}(\mathbf{u}_0) = \mathrm{lm}(\mathbf{u})$.

If $v_1 = 0$, then $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\mathbf{u}_0) = \mathrm{lm}(\mathbf{u})$ and $tv_1 = 0$ is smaller than $\mathrm{lm}(v)$. So we may assume that $v_1 \neq 0$. Since p_0 is super top-reducible by p_1, we see that

$$\frac{\mathrm{lm}(v_0)}{\mathrm{lm}(v_1)} = \frac{\mathrm{lm}(\mathbf{u}_0)}{\mathrm{lm}(\mathbf{u}_1)} = \frac{\mathrm{lm}(\mathbf{u})}{\mathrm{lm}(\mathbf{u}_1)}$$

is a monomial, denoted by t. Then $\mathrm{lm}(\mathbf{u}) = t\,\mathrm{lm}(\mathbf{u}_1)$ and $t\,\mathrm{lm}(v_1) = \mathrm{lm}(v_0) \prec \mathrm{lm}(v)$. This shows that p is covered by $p_1 \in G$, as required by (c).

$(c) \Rightarrow (a)$. We prove by contradiction. Assume that there is a pair $p = (\mathbf{u}, v) \in M$ that is not top-reducible by any pair in G. Among all such pairs p we pick one with minimal signature $T = \mathrm{lm}(\mathbf{u})$. Note that $T \neq 0$. Next, we select a pair $p_1 = (\mathbf{u}_1, v_1)$ from G such that

(*i*) $T = t\,\mathrm{lm}(\mathbf{u}_1)$ for some monomial t (such p_1 exists by the assumption of the theorem), and

(*ii*) $t\,\mathrm{lm}(v_1)$ is minimal among all $p_1 \in G$ satisfying (*i*).

We claim that tp_1 is not regular top-reducible by G. To prove this claim, we suppose that tp_1 is regular top-reducible by some $p_2 = (\mathbf{u}_2, v_2) \in G$, so both v_1 and v_2 are nonzero. We want to derive a contradiction to the condition (*ii*). By Lemma 2.3, the J-pair of p_1 and p_2 is $t_1 p_1$ and is regular top-reducible by p_2, where

$$t_1 = \frac{\mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2))}{\mathrm{lm}(v_1)}, \text{ and } t = t_1 w$$

for some monomial w. By the assumption in (c), the J-pair $t_1 p_1$ is covered by G, hence there is a pair $p_3 = (\mathbf{u}_3, v_3) \in G$ so that $t_3 \mathrm{lm}(v_3) \prec t_1 \mathrm{lm}(v_1)$, where $t_3 = t_1 \mathrm{lm}(\mathbf{u}_1)/\mathrm{lm}(\mathbf{u}_3)$ is a monomial. Then we have

$$T = t\,\mathrm{lm}(\mathbf{u}_1) = w t_1 \mathrm{lm}(\mathbf{u}_1) = w t_3 \mathrm{lm}(\mathbf{u}_3)$$

and

$$w t_3 \mathrm{lm}(v_3) \prec w t_1 \mathrm{lm}(v_1) = t\,\mathrm{lm}(v_1).$$

This violates the condition (*ii*) for the choice of p_1 in G.

Hence we may assume that tp_1 is not regular top-reducible by G. Consider

$$(\overline{\mathbf{u}}, \overline{v}) = p - ctp_1 = (\mathbf{u}, v) - ct(\mathbf{u}_1, v_1), \tag{2.9}$$

where $c = \mathrm{lc}(\mathbf{u})/\mathrm{lc}(\mathbf{u}_1)$ so that $\mathrm{lm}(\overline{\mathbf{u}}) \prec \mathrm{lm}(\mathbf{u}) = T$. Note that $\mathrm{lm}(v) \neq t\,\mathrm{lm}(v_1)$, since otherwise p would be top-reducible by p_1 contradicting the choice of p. Also, as $(\overline{\mathbf{u}}, \overline{v}) \in M$ and $\mathrm{lm}(\overline{\mathbf{u}}) \prec T$, we have that $(\overline{\mathbf{u}}, \overline{v})$ is top-reducible by G. If $(\overline{\mathbf{u}}, \overline{v})$ is top-reducible by some pair $p_2 = (\mathbf{u}_2, v_2) \in G$ with $v_2 = 0$, then we can reduce $(\overline{\mathbf{u}}, \overline{v})$ repeatedly by such pairs to get a new pair $(\tilde{\mathbf{u}}, \overline{v})$ that is not top-reducible by any pair in G with v-part being zero. Note that $(\tilde{\mathbf{u}}, \overline{v})$ is still in M and $\mathrm{lm}(\tilde{\mathbf{u}}) \prec T$.

Hence $(\tilde{\mathbf{u}}, \overline{v})$ is top-reducible by some pair $p_2 = (\mathbf{u}_2, v_2) \in G$ with $v_2 \neq 0$. As $\mathrm{lm}(v) \neq t\,\mathrm{lm}(v_1)$, we consider two cases:

- $\mathrm{lm}(v) \prec t\,\mathrm{lm}(v_1)$. Then $\mathrm{lm}(\overline{v}) = t\,\mathrm{lm}(v_1)$, hence tp_1 is regular top-reducible by p_2 (as $\mathrm{lm}(\tilde{\mathbf{u}}) \prec t\,\mathrm{lm}(\mathbf{u}_1)$). Since tp_1 is not regular top-reducible by any pair in G, this case is impossible.
- $\mathrm{lm}(v) \succ t\,\mathrm{lm}(v_1)$. Then $\mathrm{lm}(\overline{v}) = \mathrm{lm}(v)$, and p is regular top-reducible by p_2, contradicting the fact that p is not top-reducible by any pair in G.

Therefore such a pair p does not exist in M, so every pair in M is top-reducible by G. This proves (a). □

The condition (c) of Theorem 2.4 tells us that any J-pair that is covered by G can be discarded (without performing any reductions). This will greatly speed up the algorithm. As special cases, we have the following two criteria.

Corollary 2.5 (Syzygy Criterion)**.** *If a J-pair is top-reducible by a syzygy, then it can be discarded.*

Note that the property of being covered is transitive, that is, if p_1 is covered by p_2 and p_2 is covered by p_3, then p_1 is covered by p_3. Hence we have the next criterion, which explains the rewritten rule used in F5.

Corollary 2.6 (Signature Criterion)**.** *If a J-pair is covered by a pair in G or covered by another J-pair, then it can be discarded. In particular, among all J-pairs with an equal signature, one just needs to store one of them (the one with the v-part minimal).*

3. Algorithm and finite termination

Our algorithm is based on Theorem 2.4. The basic idea is as follows. Initially, G consists of the pairs in (2.4). So the condition of the theorem is satisfied. From these pairs, we form a list of all J-pairs, discarding any J-pair that is covered by G or another J-pair. In particular, this make sure that we keep only one J-pair for each J-signature (the one whose v-part is minimal). We then take any J-pair from the list of J-pairs (usually the one with minimal signature, and remove this J-pair from the list). Check if this J-pair is covered by G. If yes, discard this J-pair; otherwise, repeatedly perform regular top-reductions to this pair until it is no longer regular top-reducible, say to get $(\mathbf{u}, v)$. If the v part of the resulting pair is zero, then the $\mathbf{u}$ part is a syzygy in $\mathbf{H}$, and we store this vector. If the v part is nonzero, then add this $(\mathbf{u}, v)$ pair to the current G and add new J-pairs of G to the current list of J-pairs. Repeat this process until the list of J-pairs is empty.

We make two improvements on this basic algorithm. First, storing and updating vectors $\mathbf{u} \in R^m$ is expensive. In our computation, we shall make all pairs $(\mathbf{u}, v)$ monic in the sense that the leading coefficient of $\mathbf{u}$ is 1. Then we only store the signature, i.e., the leading term of $\mathbf{u}$. Now suppose $(\mathbf{u}_1, v_1)$ and $(\mathbf{u}_2, v_2)$ are any two monic pairs. Then their J-pair or a top-reduction (regular or super) is determined only by $\mathrm{lm}(\mathbf{u}_1)$, $\mathrm{lm}(\mathbf{u}_2)$, v_1 and v_2. The other terms of $\mathbf{u}_1$ and $\mathbf{u}_2$ are not used at all. Let $T_1 = \mathrm{lm}(\mathbf{u}_1)$ and $T_2 = \mathrm{lm}(\mathbf{u}_2)$ be the signatures of $(\mathbf{u}_1, v_1)$ and $(\mathbf{u}_2, v_2)$, respectively. Suppose we store only (T_1, v_1) and (T_2, v_2). Then (T_1, v_1) is regular top-reducible by (T_2, v_2) when $v_2 \neq 0$, $\mathrm{lm}(v_1)$ is divisible by $\mathrm{lm}(v_2)$, and $tT_2 \prec T_1$, or $tT_2 = T_1$ but $\mathrm{lc}(v_1) \neq \mathrm{lc}(v_2)$. The corresponding top-reduction is

$$v := v_1 - ctv_2,$$

where $t = \mathrm{lm}(v_1)/\mathrm{lm}(v_2)$ and $c = \mathrm{lc}(v_1)/\mathrm{lc}(v_2)$, and furthermore, if $tT_2 = T_1$, then we update v as

$$v := v/(1-c),$$

to keep the $\mathbf{u}$-part of $(\mathbf{u}, v)$ monic where $T_1 = \mathrm{lm}(\mathbf{u})$. Then (T_1, v) is the resulting pair of the reduction, and it replaces (T_1, v_1). Our algorithm below will perform regular top-reductions in this fashion.

Another improvement is to use trivial syzygies. We will store the leading terms of known syzygies in a list called H. Let (T_1, v_1) and (T_2, v_2) be any two pairs from the Gröbner basis computed so far, where v_1 and v_2 are both nonzero. There are $\mathbf{u}_i \in R^m$ such that $\mathrm{lm}(\mathbf{u}_i) = T_i$ and $(\mathbf{u}_i, v_i) \in M$ for $1 \le i \le 2$. Then we have

$$v_2(\mathbf{u}_1, v_1) - v_1(\mathbf{u}_2, v_2) = (v_2\mathbf{u}_1 - v_1\mathbf{u}_2, 0) \in M.$$

Hence $v_2\mathbf{u}_1 - v_1\mathbf{u}_2$ is a syzygy of $(g_1, \ldots, g_m)$. Its leading term is

$$T = \max(T_1\mathrm{lm}(v_2), T_2\mathrm{lm}(v_1)),$$

provided that $T_1\mathrm{lm}(v_2) \neq T_2\mathrm{lm}(v_1)$ or $T_1\mathrm{lm}(v_2) = T_2\mathrm{lm}(v_1)$ but $\mathrm{lc}(v_1) \neq \mathrm{lc}(v_2)$. When $T_1\mathrm{lm}(v_2) = T_2\mathrm{lm}(v_1)$ and $\mathrm{lc}(v_1) = \mathrm{lc}(v_2)$, the leading terms in $v_2\mathbf{u}_1$ and $v_1\mathbf{u}_2$ cancel each other. In that case, we don't know the leading term of the syzygy, so we just ignore such a syzygy. In all other cases, our algorithm will add T to the list H. The leading terms of these syzygies are obtained free (i.e., without performing any reductions), thus saving time.

The algorithm is described more precisely in Figure 3.1 below. As mentioned above, we use H to record leading terms of syzygies. In addition to H, our algorithm uses two more lists to store the pairs $(T_1, v_1), (T_2, v_2), \ldots, (T_k, v_k)$ with $v_i \neq 0$ for $1 \le i \le k$. This list will be stored as

$$U = [T_1, T_2, \ldots, T_k], \quad V = [v_1, v_2, \ldots, v_k].$$

Then $G = [U, V]$ represents the whole list $(T_1, v_1), (T_2, v_2), \ldots, (T_k, v_k)$.

Theorem 3.1. *Suppose the term order in R is compatible with the term order in R^m. Then the algorithm in Figure* 3.1 *terminates in finitely many steps with a strong Gröbner basis for M.*

Proof. The correctness of the algorithm follows directly from Theorem 2.4, as the property of being covered is transitive and Step 2 makes sure the condition (c) is satisfied. Also, note that at Step 4b, the pair $(T, \tilde{v})$ is never super top-reducible by G, otherwise (T, v) would be covered by G. We next prove the finite termination of the algorithm. For any two pairs $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in M$, we say that p_1 divides p_2 if $\mathrm{lm}(\mathbf{u}_1) \mid \mathrm{lm}(\mathbf{u}_2)$ and $\mathrm{lm}(v_1) \mid \mathrm{lm}(v_2)$. We list the pairs in G in exactly the same order as they were obtained (not including $(T, 0)$ for $T \in H$):

$$(E_1, g_1), (E_2, g_2), \ldots, (E_m, g_m), (T_1, v_1), (T_2, v_2), \ldots, (T_i, v_i), \ldots$$

Then there exist $\mathbf{u}_i \in R^m$ so that $\mathrm{lm}(\mathbf{u}_i) = T_i$ and $P_i = (u_i, v_i) \in m$ for $i \ge 1$. We claim that, for all $i < j$, p_i does not divide p_j. Suppose otherwise, say $p_i = (\mathbf{u}_i, v_i)$ divides $p_j = (\mathbf{u}_j, v_j)$ for some $i < j$. Then there are monomials $t_1, t_2 \in R$ so that

$$\mathrm{lm}(v_j) = t_1\mathrm{lm}(v_i), \quad \mathrm{lm}(\mathbf{u}_j) = t_2\mathrm{lm}(\mathbf{u}_i).$$

Suppose $t_1 \prec t_2$ (in R). Then $t_1\mathrm{lm}(\mathbf{u}_i) \prec t_2\mathrm{lm}(\mathbf{u}_i) = \mathrm{lm}(\mathbf{u}_j)$ (since the term orders are compatible). Thus p_j is regular top-reducible by p_i, contradicting to Step 3 which makes sure that all pairs added to G are not regular top-reducible by G. Thus we must have $t_2 \preceq t_1$. Then $t_2\mathrm{lm}(v_i) \preceq t_1\mathrm{lm}(v_i) = \mathrm{lm}(v_j)$. Let $p = (\mathbf{u}, v)$ be

	Algorithm for computing Gröbner bases
Input:	$g_1, \ldots, g_m \in R = \mathbb{F}[x_1, \ldots, x_n]$ and term orders for R and R^m
Output:	A Gröbner basis for $I = \langle g_1, \ldots, g_m \rangle$ and a Gröbner basis for $\mathrm{lm}(\mathbf{H})$, the leading terms of a Gröbner basis of the syzygy module
Variables:	U a list of terms T_i, representing signatures of $(\mathbf{u}_i, v_i) \in M$, V a list of polynomials for v_i such that $(\mathbf{u}_i, v_i) \in M$, H a list for $\mathrm{lm}(\mathbf{u})$ where $\mathbf{u} \in R^m$ is a syzygy found so far, JP a list of pairs (x^α, i), which represents a J-pair $x^\alpha(\mathbf{u}_i, v_i)$ formed from the ith pair in $G = [U, V]$ where x^α is a monomial.
Step 0.	Let $G = [U, V]$ where $U = [\mathbf{E}_1, \ldots, \mathbf{E}_m]$ and $V = [g_1, \ldots, g_m]$. Find the leading terms of the principle syzygies $g_j\mathbf{E}_i - g_i\mathbf{E}_j$ for $1 \le i < j \le m$, and store them in H. Compute all the J-pairs of $(\mathbf{E}_1, g_1), \ldots, (\mathbf{E}_m, g_m)$, discarding the J-pairs that are covered by G, H, or other J-pairs.
Step 1.	Take any pair (x^α, i) from JP (say with minimal signature), and delete it from JP. Let $(T, v) = x^\alpha(T_i, v_i)$.
Step 2.	If (T, v) is covered by $G = [U, V]$ or H, then discard it and go to Step 5.
Step 3.	Reduce the pair (T, v) repeatedly by G using only regular top-reductions until it is not regular top-reducible, say to get $(T, \tilde{v})$.
Step 4a.	If $\tilde{v} = 0$, then append T to H, and delete every J-pair in JP whose signature is divisible by T.
Step 4b.	If $\tilde{v} \neq 0$, then (b1) Add the leading terms of the principle syzygies, $\tilde{v}T_j - v_jT$ for $1 \le j \le \lvert U\rvert$, to H (and delete any redundant ones), (b2) Form new J-pairs between $(T, \tilde{v})$ and (T_j, v_j), $1 \le j \le \lvert U\rvert$, and insert into JP, discarding all such J-pairs that are covered by G, H, or other J-pairs, and (b3) Append $(T, \tilde{v})$ to G (i.e. T to U and v to V).
Step 5.	While JP is not empty, go to Step 1.
Return:	V and H.

FIGURE 3.1

the J-pair that was reduced to p_j by the algorithm. Then $\mathrm{lm}(\mathbf{u}) = \mathrm{lm}(\mathbf{u}_j) = T_j$ and $\mathrm{lm}(v_j) \prec \mathrm{lm}(v)$ (as a J-pair is always regular top-reducible). Hence the J-pair p is covered by p_i, hence should have been discarded at Step 2 of the algorithm. Therefore we have a sequence

$$(T_1, \mathrm{lm}(v_1)), (T_2, \mathrm{lm}(v_2)), \ldots, (T_i, \mathrm{lm}(v_i)), \ldots . \tag{3.1}$$

where none of them is divisible by any previous one.

We introduce new variables

$$y_i = (y_{i1}, y_{i2}, \ldots, y_{in}), \quad 1 \le i \le m.$$

Each pair $(x^\alpha E_i, x^\beta)$ corresponds to a term $y_i^\alpha x^\beta$, a monomial in the variables x_i's and y_{ij}'s. Then the pairs in (3.1) gives us a list of monomials in the variables x_i and y_{ij} with the property that no one is divisible by any previous one. Since every polynomial ring over a field is Noetherian, the ascending chain condition tells us that this list of monomials must be finite. Therefore, G is finite. □

Remarks on Finite Termination. We would like to make a few remarks about proofs of finite termination that have appeared in the literature.

(a) We remark that Huang (2010 [16]) was the first person who gave a correct proof of finite termination for signature-based algorithms when the J-pairs are processed in increasing order. The proof for the general case (when J-pairs are processed in arbitrary order) is partly due to Sun and Wang (2013, [25], especially the part for $t_2 \preceq t_1$.

(b) Huang gave a counter example when the orders for R and R^m are not compatible. For convenience of the reader, we reproduce his example here. Let $g_1 = x_2, g_2 = x_1 - x_2 \in R = \mathbb{F}[x_1, x_2]$. Suppose that the term order in R is the lex order with $x_2 \prec_1 x_1$ and the term order for R^2 is defined by position and then the reverse lex order with $E_2 \prec_2 E_1$ and $x_1 E_i \prec_2 x_2 E_i$ for $i = 1, 2$. So the two orders are not compatible. Starting with the pairs (E_1, x_2) and $(E_2, x_1 - x_2)$, every signature-based algorithm will produce the infinite sequence:

$$(x_1^k E_1 - (x_1^{k-1} x_2 + x_1^{k-2} x_2^2 + \cdots + x_2^k) E_2, \quad x_2^k), \quad k = 2, 3, \cdots$$

in which no pair is top-reducible by any other pair (including (E_1, x_2) and $(E_2, x_1 - x_2)$). Hence every signature-based algorithm will not have finite termination for these term orders.

(c) We would like to mention that the proofs of finite termination in Hashemi and Ars [15] and Arri and Perry [1] have flaws. In [15], the proof of Proposition 4.1 assumes that the each time a new polynomial is added to the current Gröbner basis, the ideal generated by its leading terms strictly increases (just like Buchburger's algorithm). This is not true in general, as a polynomial may be reducible by the current Gröbner basis in the sense of Buchburger's algorithm but such a reduction may increase signature, hence not allowed in F5 algorithm. This is demonstrated by the example in (b).

(d) In [1], the authors claim finite termination of their algorithm for any term orders $\prec_1$ on R and $\prec_2$ on R^m assuming that the two orders are compatible (as hinted by the word "admissible" at the beginning of Section 2). However, their proof of Proposition 14 is flawed. More precisely, they assumed that if an R-module N of $R^m \times R$ is generated by a set of elements of the form

$$(x^{\beta_j} E_{i_j}, x^{\alpha_j}), \quad j = 1, 2, \ldots,$$

then, for every element $(\mathbf{u}, v) \in N$, the element $(\mathrm{lm}(\mathbf{u}), \mathrm{lm}(v))$ is divisible by one of the generators, that is, there is a monomial $t \in R$ and some j so that

$$(\mathrm{lm}(\mathbf{u}), \mathrm{lm}(v)) = t\,(x^{\beta_j} E_{i_j}, x^{\alpha_j}).$$

This is not true in general. Here is a counterexample. Let $R = \mathbb{F}[x, y]$ under lex with $x \succ y$ and R^2 under POT order with $E_1 = (1, 0) \succ E_2 = (0, 1)$. Consider the R-submodule N generated by

$$(E_1, x), \quad (E_2, x), \quad (E_2, y).$$

Then $(E_1, y) = (E_1, x) - (E_2, x) + (E_2, y) \in N$, but (E_1, y) is not divisible by any of the three generators.

(e) In Step 1, if one always picks the pair from JP with minimal signature, then the strong Gröbner basis G computed by the algorithm is minimal in

the sense that no element in G is top-reducible by another element in G. This is proved in Volny's thesis [28].

Computing Gröbner bases for the syzygy module. Our algorithm as presented in Figure 3.1 only calculates the leading terms of a Gröbner basis of the syzygy module. While one has the option of modifying the algorithm to compute syzygies instead of leading terms of syzygies, there is a more efficient method. Suppose that the algorithm terminates with lists U, V and H, then we can compute a minimal Gröbner basis for the syzygy module as follows.

Order the signatures in U in increasing order, say

$$\mathbf{E}_1, \ldots, \mathbf{E}_m, T_{m+1}, \ldots, T_\ell.$$

Note that some of the $\mathbf{E}_i$'s may appear in T_i's, as $(\mathbf{E}_i, g_i)$ may be regular top-reducible by other pairs. Each i from $m+1$ to ℓ, suppose we have computed

$$(\mathbf{u}_1, v_1), \ldots, (\mathbf{u}_m, v_m), \ldots, (\mathbf{u}_{i-1}, v_{i-1}), \tag{3.2}$$

where $(\mathbf{u}_k, v_k) = (\mathbf{E}_k, g_k)$ for $1 \le k \le m$, and $\operatorname{lm}(\mathbf{u}_k) = T_k$ for $k > m$. Find $j < i$ and a monomial t so that $T_i = t \operatorname{lm}(\mathbf{u}_j)$ and $t \operatorname{lm}(v_j)$ is minimal, and perform regular top-reductions of $t(\mathbf{u}_j, v_j)$ by (3.2) until it is not regular top-reducible. Denote the resulting pair by $(\mathbf{u}_i, v_i)$. By the end of this loop, we get ℓ pairs

$$(\mathbf{u}_1, v_1), \ldots, (\mathbf{u}_m, v_m), (\mathbf{u}_{m+1}, v_{m+1}), \ldots, (\mathbf{u}_\ell, v_\ell) \tag{3.3}$$

in M, whose signatures are exactly those in U.

To get a Gröbner basis for the syzygy module, do the following. For each term T in H, find a pair $(\mathbf{u}_i, v_i)$, $1 \le i \le \ell$, so that $T = t \operatorname{lm}(\mathbf{u}_i)$ and $t \operatorname{lm}(v_i)$ is minimal. Then perform regular top-reductions of $t(\mathbf{u}_i, v_i)$ by (3.3) until the v-part is zero and the $\mathbf{u}$-part is a syzygy with leading term equal to T. If T comes from a trivial syzygy, then no reductions are required. All these syzygies form a minimal Gröbner basis for the $(g_1, \ldots, g_m)$-syzygy module with respect to the term order $\prec_2$.

This algorithm takes advantage of the signatures already computed in U and H, thus saving time that would be used in processing J-pairs.

4. Impact of different signature orders

Now we discuss how the choice of signature orders impacts on the efficiency of the algorithm. In many applications, one just wants a Gröbner basis for the ideal but does not care about the syzygies. In such applications, we have tremendous freedom in the choice of signature orders. We shall see that, for a fixed term order on R, different term orders on R^m (compatible with that of R) will have significant impact on the performance of the algorithm.

Let $\prec$ be any fixed term order on R. We consider four term orders on R^m as follows:

(POT) $x^\alpha \mathbf{E}_i \prec x^\beta \mathbf{E}_j$ if $i < j$, or $i = j$ and $x^\alpha \prec x^\beta$;
(TOP) $x^\alpha \mathbf{E}_i \prec x^\beta \mathbf{E}_j$ if $x^\alpha \prec x^\beta$, or $x^\alpha = x^\beta$ and $i < j$;
(**g**1) **g**-weighted degree followed by TOP: $x^\alpha \mathbf{E}_i \prec x^\beta \mathbf{E}_j$ if $\deg(x^\alpha g_i) < \deg(x^\beta g_j)$, or $\deg(x^\alpha g_i) = \deg(x^\beta g_j)$ and $x^\alpha \mathbf{E}_i \prec_{top} x^\beta \mathbf{E}_j$, where deg is for total degree;
(**g**2) **g**-weighted term followed by POT: $x^\alpha \mathbf{E}_i \prec x^\beta \mathbf{E}_j$ if $\operatorname{lm}(x^\alpha g_i) \prec \operatorname{lm}(x^\beta g_j)$, or $\operatorname{lm}(x^\alpha g_i) = \operatorname{lm}(x^\beta g_j)$ and $x^\alpha \mathbf{E}_i \prec_{pot} x^\beta \mathbf{E}_j$.

TABLE 4.1. Runtimes in seconds

Test Case (# gen)	POT	TOP	**g**1	**g**2
Katsura5 (22)	0.00	0.00	0.00	0.01
Katsura6 (41)	0.02	0.04	0.04	0.04
Katsura7 (74)	0.46	0.36	0.36	0.34
Katsura8 (143)	4.20	2.97	2.99	2.82
Schrans-Troost (128)	1.54	3.72	3.75	3.94
F633 (76)	0.07	0.43	0.36	0.06
Cyclic 6 (99)	0.04	0.66	0.64	0.07
Cyclic 7 (443)	5.40	253.75	252.02	7.49

All of the four signature orders are compatible with the order in R, hence our algorithm has finite termination by Theorem 3.1. We remark that, under the POT order, our algorithm is incremental like F5 [11] and the G2V algorithm [13]. The reason is as follows. Suppose that, in Step 1 of our algorithm, one always picks the J-pair with minimal signature. Then, under POT order, one always first picks J-pairs with signatures containing $\mathbf{E}_1$, then those with $\mathbf{E}_2$, etc. This means that it computes Gröbner bases for $\langle g_1\rangle$, $\langle g_1, g_2\rangle$, ..., $\langle g_1, g_2, \ldots, g_m\rangle$, just like G2V and F5. The only difference is that the intermediate bases may not be reduced and nonleading terms are not reduced as in the computation of normal forms.

Another remark is that our algorithm under the **g**1 order roughly corresponds to the F4 [10] and XL algorithms [6]. In the XL algorithm, one performs row reductions on a matrix whose rows correspond to all polynomials $x^\alpha g_i$, $1 \le i \le m$, with total degree of $x^\alpha g_i$ smaller than some bound. Our algorithm basically works with only some of those rows that correspond to J-signatures. So our algorithm needs much less storage space.

We did a straightforward implement of our algorithm in C++ (without any optimization) and ran it on an Intel Core 2 Quad 2.66 GHz processor. We used various benchmark examples as used by other researchers (e.g. [8]). These examples are very small, so the the actual running times do not tell us how the algorithm performs for large examples. However, these examples are sufficient to indicate how different signature orders behave (under the same computing environment). We collected data from each example under each term ordering for comparison. Table 4.1 list the runtimes in seconds for each of the four term orderings. In examining the timings, we find that **g**2 seems to be a clear winner among the four term orders.

Tables 4.2 and 4.3 list the sizes of the Gröbner bases for each term ordering and the maximum memory used during the execution of each example. These are the Gröbner bases produced by the algorithm before any interreduction occurs to produce a reduced Gröbner basis. Note that the numbers in parentheses shows the size of a minimal Gröbner basis for the ideal $\langle g_1, \ldots, g_m\rangle$. Again, we see that **g**2 processing much fewer J-pairs than the other signature orderings. Hence, in practical implementation, the term order **g**2 should be preferred.

5. Related recent works and conclusions

This paper was originally presented in ISSAC 2010, July 25–29, Münich, Germany, and has gone through several revisions. In the 2010 version, Theorem 2.4 had only (a) and (b). The condition (c) was introduced in the 2011 version (see

TABLE 4.2. Sizes of Gröbner bases for different signature orders

Test Case (# gen)	POT	TOP	**g**1	**g**2
Katsura5 (22)	67	64	64	27
Katsura6 (41)	73	91	91	44
Katsura7 (74)	224	175	175	80
Katsura8 (143)	448	343	343	151
Schrans-Troost (128)	398	133	133	134
F633 (76)	135	184	170	106
Cyclic 6 (99)	155	1189	1189	188
Cyclic 7 (443)	749	9237	9237	846

TABLE 4.3. Maximal memory used (MB) for different signature orders

Test Case (# gen)	POT	TOP	**g**1	**g**2
Katsura5 (22)	5.16	4.92	4.95	4.62
Katsura6 (41)	5.73	6.44	6.45	5.41
Katsura7 (74)	14.48	13.72	13.70	8.34
Katsura8 (143)	53.17	45.56	46.14	22.94
Schrans-Troost (128)	55.75	17.84	17.84	18.89
F633 (76)	7.91	10.09	8.89	6.05
Cyclic 6 (99)	5.88	26.55	26.86	6.06
Cyclic 7 (443)	43.36	2772.00	2764.00	42.06

https://eprint.iacr.org/2010/641). In the meantime, many other papers on signature based algorithms have been published. The referees suggested that we provide comments about how our work is related to these recent papers in the literature (up to 2013). It is impossible to write in this paper a detailed comparison to all these papers, instead we try to point out the main connections.

Characterizations of signature based Gröbner bases. Faugère [11] give a direct analogue of Buchberger's criterion for the situation with signatures. This is described in his Theorem 1, which says that a list G of polynomials with signatures is a Gröbner basis if and only if every normalized S-pair has a standard representation with respect G and the signatures. In our language, this roughly says that a generating subset G of M is a strong Gröbner basis if and only if every J-pair of G can be top-reduced to zero.

Arri and Perry [1] give a better criterion as described in their Theorem 18 (F5 Criterion). In fact, their F5 criterion corresponds to our condition (b). To see this, we recall that, in [1, 11], for any polynomial $v \in \mathbf{I} = \langle g_1, \ldots, g_m \rangle$, the signature of v is defined as

$$S(v) = \min\{\mathrm{lm}(\mathbf{u}) : \mathbf{u} \in R^m \text{ with } \mathbf{u}\mathbf{g}^t = v\}.$$

The main condition of their F5 criterion (in characterizing G as a Gröbner basis) is quoted here:

> *for any $g_1, g_2 \in G$ such that (g_1, g_2) is a normal pair, there exists $g \in G$ and a monomial t such that tg is S-irreducible and*
>
> $$S(tg) = S(\mathrm{Spol}(g_1, g_2)).$$

This condition means the following. Suppose $S(g) = T_1$ and $S(\mathrm{Spol}(g_1, g_2)) = T_2$. On the one hand, the condition that tg is S-irreducible implies that $S(tg) = tT_1$ and (T_1, g) is not regular top-reducible by any pair in M. On the other hand, let v be the polynomial obtained from $\mathrm{Spol}(g_1, g_2)$ via regular top-reductions by M so that (T_2, v) is S-irreducible. Then $S(tg) = S(\mathrm{Spol}(g_1, g_2))$ means that $tT_1 = T_2$. Hence both (tT_1, tg) and (T_2, v) are S-irreducible with the same signature. Then we must have $\mathrm{lm}(tg) = \mathrm{lm}(v)$, thus (T_2, v) is super top-reducible by (T_1, g). This means that the S-pair $(T_2, \mathrm{Spol}(g_1, g_2))$ is eventually super top-reducible by G. Hence their condition is roughly our condition (b).

Condition (c) appears for the first time as a clear criterion for signature based Gröbner bases in the 2011 version of the current paper. It is simple and easy to use. We shall show below how it explains the rewritten rules used in the F5 algorithm and in all the recent papers in the literature.

Condition (c) and rewritten rules. In [11], rewritten rules are introduced to eliminate many S-pairs in F5. Since the mathematical meaning of the rewritten rules in F5 is not clear, several authors have tried to formulate this rule more precisely; see for example [1, 7, 9, 20, 22, 25, 27]. In our language, the F5 rewritten rules can be summarized as follows (as described in [7]):

(S) if the signature of a critical pair is divisible by some term in H, then this pair is rewritable (so discarded), where H is the collection of leading terms of all trivial syzygies and the signatures of critical pairs that are reduced to 0 known so far;

(R) a pair (T, v) (from a critical pair) is rewritable (so discarded) if

(R1) there is a pair $(T_1, v_1) \in G$ or in JP so that T_1 divides T and v_1 was computed before v.

Since the mathematical meaning of (R1) is not clear, Arri and Perry [1] replaced it by,

(R2) there is a pair $(t_1\mathbf{E}_i, v_1) \in G$ or in JP so that t_1 divides t and $t_2\mathrm{lm}(v_1) \prec \mathrm{lm}(v)$ where $t_2 = t/t_1$.

In [9, 20, 25, 27], they define more general rewrite orders, but (R2) is the essential one.

Note that (R2) means that (T, v) is covered by G, hence a special case of Condition (c). To see that (S) is also a special case of Condition (c), let $T_1 \in H$ and $T_1 = \mathrm{lm}(\mathbf{u}_1)$ for some syzygy $p_1 = (\mathbf{u}_1, 0) \in M$. For any J-pair or critical pair $p = (\mathbf{u}, v) \in M$ with $v \neq 0$ and $\mathrm{lm}(\mathbf{u})$ divisible by T_1, we have $\mathrm{lm}(\mathbf{u}) = tT_1$ and $0 \cdot t \prec t\mathrm{lm}(v)$, so p is always covered by G (since, in Theorem 2.4, G includes all the syzygies computed). Hence (S) is also a special case of Condition (c).

The condition (R2) is implied by the F5 criterion in [1] or by our condition (b). However, Arri and Perry did not prove that (R2) is sufficient for a Gröbner basis. Using F5 criterion or our condition (b), one has to process J-pairs in increasing order, while the condition (c) has no such constraint at all, one can process J-pairs in any order, which may be useful in practical implementation. Furthermore, if the J-pairs are processed in increasing order, then one actually gets a minimal Gröbner basis [28]. Also, note that Ma et al. [24] apply our algorithm to solvable polynomial algebras, and Sun [26] gives a nice connection of our algorithm to the MMM algorithm [18].

Conclusions. We have introduced a framework and a simple criterion for computing Gröbner bases for both ideals and syzygy modules. Computing syzygies has traditionally been approached separately by different methods, however, our paper shows that it can be handled simultaneously with Gröbner bases for ideals and helps speed up the computation. Our characterization (b) is a generalization of Burchberger's criterion for ideals, but (c) is totally different and it is more computing friendly as it detects useless J-pairs without any reduction. Condition (c) makes it easy to understand the rewritten rules used in the literature. We presented a complete proof of correctness and finite termination, and we showed via benchmark examples that different signature orders may have dramatic impact on the time for computing Gröbner bases for ideals. We hope that the simplicity of our characterization of strong Gröbner bases is useful for implementations in practical Gröbner basis computation for ideals as well as for syzygy modules.

Acknowledgements

The authors would like to thank Dingkang Wang, Yao Sun and Lei Huang for helpful discussions as well as the referees for useful comments.

References

[1] A. Arri and J. Perry, *The F5 criterion revised*, J. Symbolic Comput. **46** (2011), no. 9, 1017–1029, DOI 10.1016/j.jsc.2011.05.004. MR2819324 (2012h:13051)

[2] B. Buchberger, *Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal*, Ph.D. thesis, Leopold-Franzens University, 1965.

[3] B. Buchberger, *Gröbner-bases: An Algorithmic Method in Polynomial Ideal Theory.*, Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985 (English).

[4] B. Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner-bases*, Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin-New York, 1979, pp. 3–21. MR575678 (82e:14004)

[5] J. Buchmann and J. Ding (eds.), *Post-quantum Cryptography*, Lecture Notes in Computer Science, vol. 5299, Springer, Berlin, 2008. MR2789106 (2012e:94002)

[6] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, Advances in cryptology—EUROCRYPT 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 392–407, DOI 10.1007/3-540-45539-6_27. MR1772028

[7] C. Eder and J. Perry, *Signature-based algorithms to compute Gröbner bases*, ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2011, pp. 99–106, DOI 10.1145/1993886.1993906. MR2895200

[8] C. Eder and J. Perry, *F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases*, J. Symbolic Comput. **45** (2010), no. 12, 1442–1458, DOI 10.1016/j.jsc.2010.06.019. MR2733388 (2011m:68298)

[9] C. Eder and B.H. Roune, *Signature rewriting in gröbner basis computation*, ISSAC 2013: Proceedings of the 2013 international symposium of symbolic and algebraic computation (2013), 331–228.

[10] J.-C. Faugére, *A new efficient algorithm for computing Gröbner bases* (F_4), J. Pure Appl. Algebra **139** (1999), no. 1-3, 61–88, DOI 10.1016/S0022-4049(99)00005-5. Effective methods in algebraic geometry (Saint-Malo, 1998). MR1700538 (2000c:13038)

[11] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero* (F_5), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2002, pp. 75–83 (electronic), DOI 10.1145/780506.780516. MR2035234 (2005c:13033)

[12] J.-C. Faugère and A. Joux, *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases*, Advances in cryptology—CRYPTO 2003, Lecture Notes in Comput. Sci., vol. 2729, Springer, Berlin, 2003, pp. 44–60, DOI 10.1007/978-3-540-45146-4_3. MR2093185 (2005e:94140)

[13] S. Gao, Y. Guan, and F. Volny IV, *A new incremental algorithm for computing Groebner bases*, ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2010, pp. 13–19, DOI 10.1145/1837934.1837944. MR2920531

[14] J. Gash, *On efficient computation of Gröbner bases*, Ph.D. dissertation, Indiana University, Bloomington, IN (2008).

[15] A. Hashemi and G. Ars, *Extended* F_5 *criteria*, J. Symbolic Comput. **45** (2010), no. 12, 1330–1340, DOI 10.1016/j.jsc.2010.06.013. MR2733382 (2012a:68297)

[16] L. Huang, *A new conception for computing Gröbner basis and its applications*, CoRR **arXiv:1012.5425v2** (2010).

[17] D. Lazard, *Gröbner-bases, Gaussian elimination and resolution of systems of algebraic equations*, EUROCAL '83: Proceedings of the European Computer Algebra Conference on Computer Algebra (London, UK), Springer-Verlag, 1983, pp. 146–156.

[18] M. G. Marinari, H. M. Möller, and T. Mora, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, Appl. Algebra Engrg. Comm. Comput. **4** (1993), no. 2, 103–145, DOI 10.1007/BF01386834. MR1223853 (94g:13019)

[19] H. M. Möller, T. Mora, and C. Traverso, *Gröbner bases computation using syzygies*, ISSAC '92: Papers from the international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM, 1992, pp. 320–328.

[20] S. Pan, Y. Hu, and B. Wang, *The termination of the f5 algorithm revisited*, ISSAC 2013: Proceedings of the 2013 International Symposium of Symbolic and Algebraic Computation (2013), 291–298.

[21] J. Patarin, *Asymmetric cryptography with a hidden monomial and a candidate algorithm for* $\simeq 64$ *bits asymmetric signatures*, Advances in cryptology—CRYPTO '96 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 1109, Springer, Berlin, 1996, pp. 45–60, DOI 10.1007/3-540-68697-5_4. MR1480670 (99b:94040)

[22] B. H. Roune and M. Stillman, *Practical Gröbner Basis Computation*, ISSAC'12: Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation (Grenoble, France), ACM, 2012.

[23] T. Stegers, *Faugère's F5 algorithm revisited*, Cryptology ePrint Archive **Report 2006/404** (2006).

[24] Y. Sun, D. K. Wang, D. X. Ma, and Y. Zhang, *A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras*, ISSAC'12: Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation (Grenoble, France), ACM, 2012, pp. 351–358.

[25] Y. Sun and D.K. Wang, *Extending the gvw algorithm to compute gröbner bases*, Submitted to Sci. China Math. (2013).

[26] Y. Sun, *Signature-based gröbner basis algorithms extended MMM algorithm for computing Gröbner bases*, CoRR **arXiv:1308.2371** (2013).

[27] Y. Sun and D. Wang, *A generalized criterion for signature related Gröbner basis algorithms*, ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2011, pp. 337–344, DOI 10.1145/1993886.1993936. MR2895230

[28] F. Volny IV, *New algorithms for computing Gröbner bases*, PhD thesis, Clemson University (2011).

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634-0975

E-mail address: sgao@clemson.edu

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634-0975

E-mail address: fvolny4@gmail.com

Information Security Lab, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100190, People's Republic of China

E-mail address: mingsheng_wang@aliyun.com