The Termination of the F5 Algorithm Revisited

Senshan Pan Yupu Hu Baocang Wang

State Key Laboratory of Integrated Service Networks
Xidian University, Xi'an, China 710071
pansenshan@gmail.com, yphu@mail.xidian.edu.cn, bcwang79@yahoo.com.cn

ABSTRACT

The F5 algorithm [8] is generally believed as one of the fastest algorithms for computing Gröbner bases. However, its termination problem is still unclear. The crux lies in the non-determinacy of the F5 in selecting which from the critical pairs of the same degree. In this paper, we construct a generalized algorithm F5GEN which contain the F5 as its concrete implementation. Then we prove the correct termination of the F5GEN algorithm. That is to say, for any finite set of homogeneous polynomials, the F5 terminates correctly.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms – Analysis of algorithms

Keywords

Gröbner basis; termination; F5; F5GEN

1. INTRODUCTION

In 1965 Buchberger's [3] thesis he described the appropriate framework for the study of polynomial ideals, with the introduction of Gröbner bases. Since then, Gröbner basis has become a fundamental tool of computational algebra and it has found countless applications in coding theory, cryptography and even directions of Physics, Biology and other sciences.

Although Buchberger presented several improvements to his algorithm for computing Gröbner bases in [4], the efficiency is not so good. Recent years have seen a surge in the number of algorithms in computer algebra research, but efficient ones are few. Faugère [8] proposed the idea of signatures and utilized two powerful criteria to avoid useless computation in the F5 algorithm. Faugère and Joux broke the first Hidden Field Equation (HFE) Cryptosystem Challenge (80 bits) by using the F5 algorithm in [9]. The proof of the termination in [8] is based on the hypothesis that the input polynomials are homogeneous and regular, which was labeled as a conjecture in [15]. Gash [12] pointed out that Theorem 2 in [8] is false and he proposed another conjecture for the termination of the F5. The proof under that conjecture, we will show in Section 6.4, can be viewed as the proof for a possible implementation of the F5. In [1], the authors did an inspiring work by constructing a simpler algorithm and proving its termination. [13] gave a generalized TRB algorithm and proposed the "compatible" concept that sheds light on the sufficient and necessary conditions for the termination of the TRB. The author claimed to have proved the termination of the F5, but it can also be viewed as a partial proof of the original F5. Besides, his proofs for the correctness are hard to understand due to mistakes. Though the F5 algorithm seems to terminate for any homogeneous polynomial ideals, the proof of it has been admitted as an open problem in [16, 7, 5]. After our preliminary paper appeared on the arXiv we have learned that independently of our work here, Vasily Galkin tried to give a direct proof of the F5 in [10] without any modifications. His proofs are different from ours, but they are slightly too long to understand for us.

In this paper, we show that the reason why "compatible" property is implicitly satisfied between the monomial order and the module order in almost all signature-based algorithms. We propose the F5GEN algorithm (F5 algorithm with a generalized insertion strategy) to cover the behavior of original F5 of [8]. Then we prove that the F5GEN terminates correctly, which, on the other hand, shows the correct termination of the F5.

The paper is organized as follows. We start by settling basic notations in Section 2. In Section 3, we present the strict definition of the admissible module order. Then two admissible orders and their connection are described in Section 4 and under the "compatible" condition, the top-reduced S-Gröbner basis for a polynomial ideal is proved finite. After that, the F5GEN algorithm is described and its correct termination is proved in Section 5. We compare the F5 of [8] with the F5GEN, and show that the F5 implements the F5GEN in Section 6. In Section 7, we conclude this paper with an open problem.

2. PRELIMINARIES

Let $R = K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over the field K. An **admissible monomial order** $\leq_m$ on the monoid $\mathcal{M} = \{\Pi_{i=1}^n x_i^{a_i} \mid a_i \in \mathbb{N}\}$ is a linear order (i.e. a connex, reflexive, antisymmetric and transitive order) such that (i) $1 \leq_m s, \forall s \in \mathcal{M}$, (ii) $m_1 \leq_m m_2 \Rightarrow m_1 \cdot s \leq_m m_2 \cdot s$, $\forall s, m_1, m_2 \in \mathcal{M}$.

ISSAC'13, June 26–29, 2013, Boston, Massachusetts, USA.

It can be seen that the admissible order $\leq_m$ is a well-order on $\mathcal{M}$. Sometimes we write $\leq$ for $\leq_m$ for brevity. For any $p \in R$, without confusion, we denote $HM(p)$ (resp. $HT(p)$, $HC(p)$) for the head monomial (resp. head term, head coefficient) of p.

Let $\mathcal{I}$ be the ideal generated by the set $F = \{f_1, \ldots, f_d\} \in R$, i.e.,

$$\mathcal{I} =< f_1, \ldots, f_d >= \{p_1 f_1 + \cdots + p_d f_d \,|\, p_1, \ldots, p_d \in R\}.$$

Consider the following R-submodule of $R^d \times R$:

$$\mathcal{P} = \{(\mathbf{u}, p) \in R^d \times R \,|\, \mathbf{u} \cdot \mathbf{f} = p\}, \tag{1}$$

where $\mathbf{f} = (f_1, \ldots, f_d) \in R^d$ and $\mathbf{e}_i$ is ith unit vector of R^d such that the free R-module R^d is generated by the set $\Sigma = \{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$. The element $\alpha = (\mathbf{u}, p)$ in $\mathcal{P}$ we call a **sig-polynomial** and $poly(\alpha)$ is its polynomial part p. A subset $Syz = \{(\mathbf{u}, 0) \in \mathcal{P}\}$ is defined by the **syzygy submodule** for $\mathcal{P}$, and $NS = \mathcal{P} \setminus Syz$ is called the set of **non-syzygy sig-polynomials**. Let $(\mathbf{u}_1, p_1)$ and $(\mathbf{u}_2, p_2)$ be two sig-polynomials in NS. The module generated by syzygies of the form $(p_2\mathbf{u}_1 - p_1\mathbf{u}_2, 0)$ is called a **principal syzygy submodule** PS.

Other basic concepts not presented here can be found in [2].

3. THE ADMISSIBLE MODULE ORDER

Let $\preceq$ be a quasi-order (i.e. a reflexive and transitive order) on M and $N \subseteq M$. Then a subset B of N is called a **Dickson basis** of N w.r.t. $\preceq$ if for every $a \in N$ there exists some $b \in B$ with $b \preceq a$. We say that $\preceq$ has the **Dickson property**, or is a **Dickson quasi-order**, if every subset N of M has a finite Dickson basis w.r.t. $\preceq$.

If $\preceq$ is a (Dickson) quasi-order on M, then we call $(M, \preceq)$ a (Dickson) quasi-ordered set. For example, the natural order $\leq$ on $\mathbb{N}$ has the Dickson property. Similarly, the divisibility relation on $\{x^a \,|\, a \in \mathbb{N}\}$ is a Dickson quasi-order since the map $a \mapsto x^a$ is an isomorphism between $(\mathbb{N}, \leq)$ and $(\{x^a \,|\, a \in \mathbb{N}\}, |)$. Let now $(M, \preceq)$ and $(N, \preceq')$ be quasi-ordered sets, then a quasi-order $\preceq''$ on Cartesian product $M \times N$ is defined as follows:

$$(a, b) \preceq'' (c, d) \;\Leftrightarrow\; a \preceq b \text{ and } c \preceq' d,$$

$\forall (a, b), (c, d) \in M \times N$. The **direct product** of the quasi-order sets $(M, \preceq)$ and $(N, \preceq')$ is denoted by $(M \times N, \preceq'')$. The Dickson property can be derived as follows.

LEMMA 1. *[2] Let $(M, \preceq)$ and $(N, \preceq')$ be Dickson quasi-ordered sets, $(M \times N, \preceq'')$ their direct product. Then $(M \times N, \preceq'')$ is a Dickson quasi-ordered set.*

The immediate corollary is that $(\mathbb{N}^n, \leq')$, the direct product of n copies of the natural numbers $(\mathbb{N}, \leq)$ with their natural ordering, is a Dickson quasi-ordered set. This is Dickson's lemma, and another version of which is given below by an isomorphism: $(a_1, \ldots, a_n) \mapsto \prod_{i=1}^n x_i^{a_i}$, where $(a_1, \ldots, a_n) \in \mathbb{N}^n$.

COROLLARY 1. *[2] The divisibility relation $|$ is a Dickson quasi-order on $\mathcal{M} = \{\prod_{i=1}^n x_i^{a_i} \,|\, a_i \in \mathbb{N}\}$. More explicitly, every non-empty subset S of $\mathcal{M}$ has a finite subset B such that for all $s \in S$, there exists $t \in B$ with $t \,|\, s$.*

Let $\mathcal{M}_d = \{m\mathbf{e}_i \,|\, m \in \mathcal{M}, i \in [1, d]\} \in R^d$ be the $\mathcal{M}$-monomodule. The definition of the divisibility relation $|$ on $\mathcal{M}_d$ is

$$m_1\mathbf{e}_i \,|\, m_2\mathbf{e}_j \Leftrightarrow m_1 | m_2 \text{ and } i = j \in [1, d]. \tag{2}$$

Since $(\mathcal{M}, |)$ is a Dickson quasi-ordered set, by Lemma 1, $(\mathcal{M}_d, |)$ is also a Dickson quasi-ordered set. On $\mathcal{M}_d$, we will define the admissible order similarly.

Definition 1. An **admissible module order** $\leq_s$ is a linear order on $\mathcal{M}_d$ that satisfies the following restrictions.

1. $\mathbf{e}_i \leq_s m\mathbf{e}_i, \forall m\mathbf{e}_i \in \mathcal{M}_d$,
2. $m_1\mathbf{e}_i \leq_s m_2\mathbf{e}_j$ implies $t \cdot m_1\mathbf{e}_i \leq_s t \cdot m_2\mathbf{e}_j$, $\forall t \in \mathcal{M}, \forall m_1\mathbf{e}_i, m_2\mathbf{e}_j \in \mathcal{M}_d$.

As any two elements of $\mathcal{M}_d$ are comparable w.r.t. the linear order $\leq_s$, in this paper we always assume that $\mathbf{e}_1 <_s \cdots <_s \mathbf{e}_d$ without loss of generality.

If no misunderstanding occurs, $\leq_s$ is replaced by $\leq$. By Dickson's lemma and the definition above, the admissible module order $\leq_s$ has the following properties.

PROPOSITION 1. *The admissible $\leq_s$ is a well-order (i.e. a well-founded connex order) on $\mathcal{M}_d$, and it extends the order $|$ on $\mathcal{M}_d$, which means $m_1\mathbf{e}_i \,|\, m_2\mathbf{e}_i$ implies $m_1\mathbf{e}_i \leq_s m_2\mathbf{e}_i$, for all $m_1\mathbf{e}_i, m_2\mathbf{e}_i \in \mathcal{M}_d, i \in [1, d]$.*

It should be noticed that $\leq_s$ may or may not be related to $\leq_m$. The **compatible** property [14] between $\leq_m$ and $\leq_s$ was used by [13] for the proof of termination for the F5 and GVW algorithms: $\sigma\mathbf{e}_j \leq_s \mu\mathbf{e}_j$ if and only if $\sigma \leq_m \mu$. The following section will show that this relation is sufficient for the proof of finiteness.

For any $\alpha = (\mathbf{u}, p) \in \mathcal{P}$, let $\mathcal{S}(\alpha)(resp.\mathcal{S}(\mathbf{u}))$ be the **signature** of α (resp. $\mathbf{u}$), $HM(\alpha) = HM(p)$ the head monomial of α. We call $idx(\alpha) = k$ the **index** of α if $\mathcal{S}(\alpha) = \mu\mathbf{e}_k$.

4. PROPERTIES OF SIG-POLYNOMIALS

Without loss of generality, assume that the $poly(\alpha)$ is always monic for each non-syzygy $\alpha \in NS$. We use the map

$$\begin{aligned} \vartheta : NS &\mapsto \mathcal{M}_d \times \mathcal{M} \\ \alpha &\mapsto (\mathcal{S}(\alpha), HM(\alpha)) \end{aligned}$$

in [1] and call the image $\vartheta(\alpha)$ a **head pair**.

Let α be a non-syzygy one in NS. α is called **top-reducible** by B, if there exists a sig-polynomial $\beta \in B$ satisfying one of the following conditions,

1. $HM(t\beta) = HM(\alpha)$ and $\mathcal{S}(t\beta) <_s \mathcal{S}(\alpha)$,
2. $\mathcal{S}(t\beta) = \mathcal{S}(\alpha)$ and $HM(t\beta) <_m HM(\alpha)$,
3. $HM(t\beta) = HM(\alpha)$ and $\mathcal{S}(t\beta) = \mathcal{S}(\alpha)$, $t \in \mathcal{M}$;

otherwise, α is top-irreducible[1] by B.

The process $\alpha - t\beta$ is called an **$\mathcal{S}$-reduction** (resp. **$\mathcal{M}$-reduction**[2], **super top-reduction**), if item 1 (resp. 2, 3)

[1]By the following lemma, we will see that this notion is the same as that of [11] and the "primitive $\mathcal{S}$-irreducible" of [1].

[2]The term "$\mathcal{M}$-reducible" has a similar meaning as the "M-pair" in [17]. It serves as one type of rewritten criterion which can be traced back in [1, 13, 11]. Defining so because our version of rewritten criterion is unrelated to this term.

is satisfied. β or $t\beta$ of item 1 (resp. 2) is called an $\mathcal{S}$-reducer (resp. $\mathcal{M}$-reducer). Let $\gamma = \alpha - t\beta$, we denote $\alpha \underset{B}{\longrightarrow} \gamma$. $\underset{B}{\overset{*}{\longrightarrow}}$ is the reflexive-transitive closure of $\underset{B}{\longrightarrow}$.

LEMMA 2. *Let α be a non-syzygy one in NS. α is $\mathcal{M}$-reducible by $\mathcal{P}^*$ if and only if it is $\mathcal{S}$-reducible by $\mathcal{P}^*$.*

PROOF. If α is $\mathcal{M}$-reducible, let $t\beta$ be its $\mathcal{M}$-reducer and $\gamma = \alpha - t\beta$. It can be verified readily that $\gamma \in \mathcal{P}^*$ can $\mathcal{S}$-reduce α. The other direction can be proved similarly. □

A set $\mathcal{G} \subset \mathcal{P}$ is called an **S-Gröbner basis** for the module $\mathcal{P}$, if any non-syzygy $\alpha \in NS$ is top-reducible by $\mathcal{G}$. By Lemma 2, each nonzero polynomial in $\mathcal{I}$ can be reduced by $\{poly(\alpha) \,|\, \alpha \in \mathcal{G}, poly(\alpha) \neq 0\}$, a Gröbner basis of $\mathcal{I}$. So the "S-Gröbner basis" is in fact a term in [16], which is a simpler version of "strong Gröbner basis" in [11].

All non-syzygy top-irreducible sig-polynomials form a special kind of S-Gröbner basis called the **top-reduced S-Gröbner basis** $\mathcal{H}$ for $\mathcal{P}$. The signature of a top-irreducible sig-polynomial is called a **top-irreducible signature** w.r.t. $\mathcal{P}$. Besides, we call two sig-polynomials α and β **equivalent** if $\beta \neq \alpha$ and $\vartheta(\beta) = \vartheta(\alpha)$. If we store only one for all equivalent sig-polynomials in $\mathcal{H}$, for fixed orders $\leq_m$ and $\leq_s$, the top-reduced S-Gröbner basis $\mathcal{H}$ is uniquely determined by the module $\mathcal{P}$ up to equivalence. Those top-reducible sig-polynomials in $\mathcal{P} \setminus \mathcal{H}$ are also called **redundant sig-polynomials**.

Since $(\mathcal{M}, |)$ and $(\mathcal{M}_d, |)$ are Dickson quasi-ordered sets, by Lemma 1, we have $(\mathcal{M}_d \times \mathcal{M}, |^*)$ is also a Dickson quasi-ordered set of which the order $|^*$ is defined as follows:

$$\vartheta(\alpha) \,|^*\, \vartheta(\beta) \Leftrightarrow \mathcal{S}(\alpha) \,|\, \mathcal{S}(\beta) \text{ and } HM(\alpha) \,|\, HM(\beta), \qquad (3)$$

where $\alpha, \beta \in \mathcal{P}^*$.

The proofs of [1, Prop. 14] and [7, Lem. 15] implicitly use the "compatible" property. Here, we reprove the following results to show that "compatible" property is a sufficient condition for the finiteness of the top-reduced S-Gröbner basis.

LEMMA 3. *Let α and β be two arbitrary sig-polynomials in $\mathcal{P}^*$ such that $\vartheta(\alpha) \,|^*\, \vartheta(\beta)$. If the admissible monomial order $\leq_m$ and the admissible module order $\leq_s$ are compatible, then β is top-reducible by α.*

PROOF. Let s and t be two monomials in $\mathcal{M}$ such that $s = \mathcal{S}(\beta)/\mathcal{S}(\alpha)$ and $t = HM(\beta)/HM(\alpha)$. There are three cases as follows.

1. If $s = t$, then β is super top-reducible by α.
2. If $s <_m t$, then $sHM(\alpha) <_m HM(\beta)$, i.e., β is $\mathcal{M}$-reducible by α.
3. If $s >_m t$, as $\leq_m$ and $\leq_s$ are compatible, $t\mathcal{S}(\alpha) <_s \mathcal{S}(\beta)$, i.e., β is $\mathcal{S}$-reducible by α.

□

By the above lemma and the Dickson property of $|^*$, we have the following truth.

THEOREM 1. *The top-reduced S-Gröbner basis for $\mathcal{P}$ is finite.*

It can be seen that the "compatible" property is a sufficient condition for the finiteness of the top-reduced S-Gröbner basis $\mathcal{H}$. Below we provide an example by extracting the proof of [13, Th. 13] to show that we may get an infinite $\mathcal{H}$ if the "compatible" property is not satisfied.

Example 1. Let $\leq_{m^*} = \leq_{invlex}$ be the inverse lexicographical order[3] on $\mathcal{M}$ and let $\leq_{s^*}$ be the order on $\mathcal{M}_d$ with the following definition: $m\mathbf{e}_i <_{s^*} m'\mathbf{e}_j$ if

1. $i > j$,
2. $i = j$, $m <_{lex} m'$,

where $\leq_{lex}$ is the lexicographical order on $\mathcal{M}$. Particularly, we have $m\mathbf{e}_i = m'\mathbf{e}_j$, if $i = j$ and $m = m'$.

Readers can verify that $\leq_{m^*}$ (resp. $\leq_{s^*}$) is an admissible monomial (resp. module) order and $\leq_{m^*}$ and $\leq_{s^*}$ are not compatible. Let the polynomials to be computed are $f_1 = x_1$ and $f_2 = x_3x_2 - x_3x_1$, the initialized sig-polynomials $\alpha_1 = (\mathbf{e}_1, x_1)$ and $\alpha_2 = (\mathbf{e}_2, x_3x_2 - x_3x_1)$. We have

$$\alpha_3 = x_2x_3\alpha_1 - x_1\alpha_2 = (x_2x_3\mathbf{e}_1, x_3x_1^2),$$

and α_3 cannot be top-reduced by α_1 and α_2. It can be inferred that α_3 is top-irreducible and we can generate infinite top-irreducible sig-polynomials

$$\alpha_k = x_2\alpha_{k-1} - x_1^{k-2}\alpha_2 = (x_2^{k-2}x_3\mathbf{e}_1, x_3x_1^{k-1}),$$

for $k \geq 3$. As they are not pairwise equivalent (i.e., their head pairs are unequal), $\mathcal{H}$ is an infinite sequence $\{\alpha_\ell\}_{\ell \in \mathbb{N}^*}$.

Hence, in the remaining sections of this paper we will assume that the admissible monomial order $\leq_m$ and the admissible module order $\leq_s$ are compatible. Suppose there are two sig-polynomials $\alpha, \beta \in NS$. Denote by $\Gamma_{\alpha\beta}$ the least common multiple $lcm(HM(\alpha), HM(\beta))$. Let $m_\alpha = \frac{\Gamma_{\alpha\beta}}{HM(\alpha)}$ and $m_\beta = \frac{\Gamma_{\alpha\beta}}{HM(\beta)}$. If $m_\alpha\mathcal{S}(\alpha) >_s m_\beta\mathcal{S}(\beta)$, then $m_\alpha\alpha$ is called the (**first**) **J-pair** (cf. [11]) of α and β; $m_\beta\beta$ is called the **second J-pair** w.r.t. $m_\alpha\alpha$; α (resp. β) is called the **first** (resp. **second**) **component** of $m_\alpha\alpha$; m_α (resp. m_β) is called the **multiplier** of α (resp. β).

5. THE F5GEN ALGORITHM

5.1 Pseudo code

Without loss of generality, we assume that inter-reducing the input $\{f_1, \ldots, f_d\}$ (i.e. reducing each polynomial by the rest) does not lead to zero cancellation. It can be deduced $\mathbf{e}_1, \ldots, \mathbf{e}_d$ are top-irreducible signatures as in [17]. Let α be a non-syzygy one in NS of signature $\mathbf{e}_i$, $i \in [1, d]$. If α is $\mathcal{M}$-reducible by $\mathcal{P}^*$, a repeated $\mathcal{S}$-reduction of α by $\mathcal{P}^*$ would generate an $\mathcal{S}$-irreducible sig-polynomial β. By Lemma 2, β is also $\mathcal{M}$-irreducible. As β cannot be super top-reduced by $\mathcal{P}^*$, β is a top-irreducible sig-polynomial and $\mathbf{e}_i$ is a top-irreducible signature.

Note that in the computation process of the F5GEN, there may exist syzygies in $\mathcal{G}$. Let S be a set of polynomials (resp. sig-polynomials), sort(S, $\leq_m$ (resp. $\leq_s$)) means that we arrange S by ascending head monomials (resp. signatures) of polynomials (resp. sig-polynomials) with respect to the order $\leq_m$ (resp. $\leq_s$).

[3] $\mu \leq_{invlex} \sigma$ if μ has smaller degree in the last variable for which they differ.

Algorithm 1 The F5GEN Algorithm (F5 algorithm with a generalized insertion strategy)

1: **inputs:**
$F = \{f_1, \ldots, f_d\} \in R$, a list of polynomials
$\leq_m$ an admissible monomial order on $\mathcal{M}$
$\leq_s$, an admissible module order on $\mathcal{M}_d$ such that $\leq_s$ is compatible with $\leq_m$ and $\mathbf{e}_1 <_s \cdots <_s \mathbf{e}_d$
2: **outputs:**
a Gröbner basis of $\mathcal{I} =< f_1, \ldots, f_d >$
3: inter-reduce F and F :=sort($\{f_1, \ldots, f_d\}$, $\leq_m$), $F_i = (\mathbf{e}_i, f_i)$ for $i \in [1, d]$
4: **init:**
$CP := \{J - pair[F_i, F_j] \,|\, 1 \leq i < j \leq d\}$,
$\mathcal{G} = \{F_i \,|\, i \in [1, d]\}$
5: **while** $CP \neq \emptyset$ **do**
6: γ :=select_F5(CP) and $CP := CP \backslash \{\gamma\}$
7: **if** $\mathcal{S}(\gamma) \notin \mathcal{S}(PS)$ and γ is not rewritable by $\mathcal{G}$ **then**
8: $\gamma \xrightarrow[\mathcal{G}]{*} \alpha$
9: $\mathcal{G}$:=insert_F5GEN(α, $\mathcal{G}$, γ)
10: **if** $poly(\alpha) \neq 0$ **then**
11: $CP := CP \cup \{J - pair(\alpha, \beta) \,|\, \forall \beta \in \mathcal{G} \backslash Syz, \beta \neq \alpha\}$
12: **return** $\{poly(\alpha) \,|\, \alpha \in \mathcal{G} \setminus Syz\}$

Algorithm 2 select_F5

1: **inputs:**
CP, a set of J-pairs
2: $i := min\{idx(\delta) | \delta \in CP\}$ and
$CP^i := \{\delta \in CP \,|\, idx(\delta) = i\}$
3: $D := min\{deg(\mathcal{S}(\delta)) | \delta \in CP^i\}$ and
$CP^i_D := \{\delta \in CP^i \,|\, deg(\mathcal{S}(\delta)) = D\}$
4: $\gamma :=$ any J-pair in CP^i_D
5: **return** γ

The select_F5 function seems to be too cumbersome for applications, but it simulates fairly well the process of selecting critical pairs in the F5 algorithm of [8]. In fact, if γ is replaced by the $\leq_s$-minimal J-pair at line 6, we can also obtain another version of the F5GEN and its proof is similar to that in Subsection 5.3. This paper is tailored to deal with the F5 algorithm, so we do not consider other selection strategies here. Call a J-pair γ being considering if the F5GEN algorithm is executing the while-loop where γ is selected at line 6. If the algorithm has completed that while-loop, γ has been considered, otherwise γ has not been considered.

Algorithm 3 rewritable

1: **inputs:**
$m\mathcal{G}(k)$, a J-pair
$\mathcal{G} := \{\mathcal{G}(1), \ldots, \mathcal{G}(r)\}$
2: **outputs:**
true if $\mathcal{S}(m\mathcal{G}(k))$ is a multiple of another sig-polynomial appearing later than $\mathcal{G}(k)$ in $\mathcal{G}$
3: find the first position j_b and the last position j_e in $\mathcal{G}$ such that $idx(\mathcal{G}(k)) = idx(\mathcal{G}(j_b)) = idx(\mathcal{G}(j_e))$
4: **for** $i = j_e$ **to** j_b **do**
5: **if** $\mathcal{S}(\mathcal{G}(i)) \,|\, \mathcal{S}(m\mathcal{G}(k))$ **then**
6: **return** $i \neq k$
7: **return false**

Algorithm 4 insert_F5GEN

1: **inputs:**
α, a sig-polynomial
$\mathcal{G} := \{\mathcal{G}(1), \ldots, \mathcal{G}(r)\}$
$\gamma = m\mathcal{G}(k)$, the J-pair which is $\mathcal{S}$-reduced to α
2: find the first position j_b and the last position j_e in $\mathcal{G}$ such that

$$idx(\mathcal{G}(j_b)) = idx(\mathcal{G}(j_e)) = idx(\alpha) = idx(\gamma)$$

3: insert α into $\mathcal{G}$ after $\mathcal{G}(i)$, where $j_b - 1 \leq i \leq j_e$, such that α appears later in $\mathcal{G}$ than $\mathcal{G}(k)$ (i.e., $k \leq i \leq j_e$)
4: **return**

It is important to note that after the execution of line 3 in the insert_F5GEN function, α is in $\mathcal{G}$: α in $\mathcal{G}$ may be of the form $\mathcal{G}(k+1)$ or $\mathcal{G}(k+100)$ ($k + 100 \leq j_e + 1$). We will show that the original F5 algorithm of [8], which did not specify an order when adding critical pairs of the same degree into $Rule[idx(\alpha)]$, can be viewed as a restricted case of the insertion strategy.

5.2 Simplifications compared with F5

If $\mathbf{s}$ is the signature (not necessary top-irreducible) in $\mathcal{S}(\mathcal{P}^*)$, we denote by $\mathcal{P}_{\leq_s(\mathbf{s})}$ the subset of sig-polynomials in $\mathcal{P}$ of which the signatures are smaller than or equal to $\mathbf{s}$ and denote by $\mathcal{G}_{\leq_s(\mathbf{s})}$ the S-Gröbner basis for $\mathcal{P}_{\leq_s(\mathbf{s})}$. That is, any non-syzygy sig-polynomial in $\mathcal{P}_{\leq_s(\mathbf{s})}$ is top-reducible by $\mathcal{G}_{\leq_s(\mathbf{s})}$. $\mathcal{P}_{\leq_s(\mathbf{s})}$ and $\mathcal{G}_{<_s(\mathbf{s})}$ are defined similarly.

We denote by **F5-reduction** the process of checking the **F5-criteria** (i.e. line 7 of the F5GEN algorithm) for the $\mathcal{S}$-reducer.[4] We think that omitting the F5-criteria check for

[4]The terms F5-reduction and F5-criteria are summarized from the pseudo code of the F5 algorithm of [8].

the $\mathcal{S}$-reducers at line 8 as in [7] would not affect the correct termination of this algorithm. However, Galkin pointed out that the simplifications above are not as obvious as we imaged. Using the idea of [10], we have the following lemma to confirm this point but our result is slightly different from Corollary 35 of [10].

LEMMA 4. *Assume the F5GEN has computed correctly up to signature* $\mathbf{s}$ *(i.e.,* $\mathcal{G} = \mathcal{G}_{<_s(\mathbf{s})}$ *and the F5GEN has not considered any sig-polynomial of signature* $\mathbf{s}$*). Let* $\zeta \in NS$ *be a non-syzygy one of signature* $\mathbf{s}$*. If* ζ *can be* $\mathcal{S}$*-reduced by* $\mathcal{G}$*, it would also be F5-reduced by the updated* $\mathcal{G}$ *after finite runs through the while-loop.*

The detailed proof can be seen in the appendix.

Therefore, in the remaining part of this paper the sole reduction used will be $\mathcal{S}$-reduction and the F5-criteria check for the second J-pair will be omitted too because the second J-pair is also an $\mathcal{S}$-reducer.

5.3 Proof of F5GEN

Define an order $\preceq_p$ on $\mathcal{P}^*$ in the following way:

$$\alpha \preceq_p \beta \Leftrightarrow HM(\alpha)\mathcal{S}(\beta) \leq_s HM(\beta)\mathcal{S}(\alpha)$$

This order are closely related to the terms defined earlier. If α is $\mathcal{S}$-reducible by β, then $(HM(\alpha)/HM(\beta))\mathcal{S}(\beta) <_s \mathcal{S}(\alpha)$ and $\alpha \prec_p \beta$. If β is $\mathcal{M}$-reducible by α, then

$$(\mathcal{S}(\beta)/\mathcal{S}(\alpha))HM(\alpha) <_m HM(\beta)$$

and $idx(\alpha) = idx(\beta)$. As $<_s$ and $<_m$ are compatible, $\alpha \prec_p \beta$.

It can be deduced that $\preceq_p$ is a well-order on $\mathcal{P}^*$ as $\leq_s$ is the well-order and the $\preceq_p$-minimal elements on $\mathcal{P}^*$ are $\{(\mathbf{u}, g) \in \mathcal{P}^* \mid g = 0\}$.

From the idea of [13, Th. 13], we derive a crucial lemma for the termination.

LEMMA 5. *Let* $\alpha \in NS$ *be the non-syzygy top-irreducible one of the maximum signature. After finite while-loops, assume that the F5GEN algorithm has computed correctly up to signature* $\mathbf{s}$*, where* $\mathbf{s} >_s \mathcal{S}(\alpha)$*. Then the F5GEN would terminate.*

PROOF. By the assumption the S-Gröbner basis $\mathcal{G}$ is a finite set, we denote by $\{\mathcal{G}(k_1), \ldots, \mathcal{G}(k_w)\}$ all non-syzygy ones in $\mathcal{G}$. Then we use a permutation ς of $\{1, \ldots, w\}$ to ensure that

$$\mathcal{G}(k_{\varsigma(1)}) \succeq_p \cdots \succeq_p \mathcal{G}(k_{\varsigma(w)})$$

since $\preceq_p$ is a well-order. All the remainders in CP can be counted in a vector $N_{CP} = (n_1, \ldots, n_w) \in \mathbb{N}^w$ as follows. n_j stands for the number of J-pairs $\preceq_p$-equal to $\mathcal{G}(k_{\varsigma(j)})$, $j \in [1, w]$.

Consider the relation between N_{CP} and $N_{CP'}$ after two consecutive runs through the while-loop w.r.t the lexicographical order, denoted by $<_{lex}$. Let

$$N_{CP} = (n_1, \ldots, n_w) \text{ and } N_{CP'} = (n'_1, \ldots, n'_w),$$

we have $N_{CP} >_{lex} N_{CP'}$ whenever the leftmost non-zero component, say $n_a - n'_a$, is positive, where $a \in [1, w]$. During an execution of the loop, a J-pair γ is extracted from CP, which will be either discarded or $\mathcal{S}$-reduced to an $\mathcal{S}$-irreducible sig-polynomial β. If $\beta \neq 0$, new J-pairs η would be generated at line 11. Whether the first components of η would be β or not, $\eta \preceq_p \beta \prec_p \gamma$ always holds. Because η can be super top-reduced by $\mathcal{G}$, $N_{CP} >_{lex} N_{CP'}$ and the algorithm would terminate because $<_{lex}$ on $\mathbb{N}^w$ is well-founded. □

The following lemma shows under what condition a top-irreducible sig-polynomial can be computed by the F5GEN algorithm.

LEMMA 6. *Let* α *be a non-syzygy top-irreducible one in* NS*. After finite steps, assume that the F5GEN has computed correctly up to a top-irreducible signature* $\mathcal{S}(\alpha)$*.* $\mathcal{G}$ *would be* $\mathcal{G}_{\leq_s(\mathcal{S}(\alpha))}$ *after finite runs of the loop.*

PROOF. Suppose $\mathcal{G}$ does not contain any sig-polynomial of signature equivalent to α since otherwise $\mathcal{G} = \mathcal{G}_{\leq_s(\mathbf{s})}$. As $\mathbf{e}_1, \ldots, \mathbf{e}_d$ are top-irreducible signatures, we first prove that there is a J-pair in CP can pass F5-criteria by distinguishing between two cases.

1. If $\mathcal{S}(\alpha) = \mathbf{e}_v$ for some $v \in [1, d]$, there is at least one sig-polynomial of signature $\mathbf{e}_v$ in $\mathcal{G}$ (e.g., $(\mathbf{e}_v, f_v)$), so we can choose one of signature $\mathbf{e}_v$ in the maximum position of $\mathcal{G}_{\leq_s(\mathbf{s}_i)}$, denoted by γ. Since γ is $\mathcal{M}$-reducible by α, by Lemma 2 it must be $\mathcal{S}$-reducible by $\mathcal{G}$. Then γ is a J-pair in CP and can pass the F5-criteria check at line 7 of the F5GEN algorithm.

2. If $\mathcal{S}(\alpha) \neq \mathbf{e}_v$ for all $v \in [1, d]$, as $\mathcal{G}$ is a finite set, there exists a non-syzygy $\beta \in \mathcal{G}$ and a monomial $m \geq 1$ such that $\mathcal{S}(m\beta) = \mathcal{S}(\alpha) \notin \mathcal{S}(PS)$ and $m\beta$ is not rewritable by $\mathcal{G}$.[5] Since $m\beta$ can be $\mathcal{M}$-reduced by α, by Lemma 2 it can also be $\mathcal{S}$-reduced by some non-syzygy top-irreducible one in $\mathcal{G}$, say δ. If $m = 1$, then β would be a J-pair in CP and pass the F5-criteria check.

   If $m \neq 1$, we denote by $m_\beta\beta$ the J-pair of β and δ, where $m_\beta \mid m$. Assume for a contradiction that m_β properly divides m. As the F5GEN has considered $\mathcal{S}(m_\beta\beta)$ and β rewrites α, either $\mathcal{S}(m_\beta\beta) = \mathcal{S}(PS)$ or $m_\beta\beta$ is rewritable by $\mathcal{G}$.

   If $\mathcal{S}(m_\beta\beta) = \mathcal{S}(PS)$, then $\mathcal{S}(m\beta)$ would be in $\mathcal{S}(PS)$, a contradiction. If $m_\beta\beta$ is rewritable by $\mathcal{G}$, let $\eta \in \mathcal{G}$ be the sig-polynomial rewriting $m_\beta\beta$. As η appears later in $\mathcal{G}$ than β and

   $$\mathcal{S}(\eta) \mid \mathcal{S}(m_\beta\beta) \mid \mathcal{S}(m\beta),$$

   $m\beta$ is rewritable by η, a contradiction.

   Therefore, $m_\beta = m$, i.e., $\gamma = m\beta$ is the J-pair of two non-syzygy β and δ such that $\mathcal{S}(\alpha) = \mathcal{S}(\gamma) \notin \mathcal{S}(PS)$ and γ is not rewritable by $\mathcal{G}$.

Then we prove that such a J-pair γ can be extracted after finite runs of the while-loop. If the F5GEN has not considered the sig-polynomial of index $idx(\alpha)$, since $\mathcal{G} = \mathcal{G}_{<_s(\mathcal{S}(\alpha))}$ and the F5GEN is incremental, the F5GEN would consider sig-polynomial of index $idx(\alpha)$ after finite runs of the loop by Lemma 5. If the F5GEN is considering the sig-polynomial of index $idx(\alpha)$, from the pseudo code of the select_F5 function we know that γ would be extracted after finite steps. As γ can pass the F5-criteria, $\mathcal{G}$ would be $\mathcal{G}_{\leq_s(\mathcal{S}(\alpha))}$. □

[5] We choose the sig-polynomial in the maximum position of $\mathcal{G}$ that its signature divides $\mathcal{S}(\alpha)$.

THEOREM 2. *For any finite subset $F = \{f_1, \ldots, f_d\}$ of polynomials in R, the F5GEN algorithm terminates correctly.*

PROOF. We proceed by induction on top irreducible sig-polynomials. The base case is vacuously true. As the induction step is guaranteed by Lemma 6 and top-reduced S-Gröbner basis is finite by Theorem 1, we would get an S-Gröbner basis after finite while-loops of the F5GEN. Then we can prove the termination of the F5GEN by Lemma 5. □

6. COMPARISON WITH F5

6.1 Orderings for rewritten

In the original F5 algorithm of [8], the admissible module order, denoted by $\leq_{s_0}$[6], is compatible with the admissible monomial order $\leq_m$. Let α and β be two arbitrary sig-polynomials in NS and $m_\alpha = \frac{\Gamma_{\alpha\beta}}{HM(\alpha)}, m_\beta = \frac{\Gamma_{\alpha\beta}}{HM(\beta)}$. Because the input polynomials $F = \{f_1, \ldots, f_d\}$ of the F5 algorithm are homogeneous, F5-reducing a sig-polynomial does not lead to a decrease in the degree of its polynomial part and

$$deg(HM(\alpha)) = deg(\mathcal{S}(\alpha)) + deg(HM(f_{idx(\alpha)}))$$

always holds. Assume that $m_\alpha\mathcal{S}(\alpha) >_s m_\beta\mathcal{S}(\beta)$. During the ith run through the **F5** function of [8], sorting critical pairs by the degrees of $\Gamma_{\alpha\beta}$ equals sorting them by the degrees of $m_\alpha\mathcal{S}(\alpha)$ because these critical pairs share the index i. Therefore, line 2 and 3 of the select_F5 function in this paper do the same thing as the **F5** function did.

The crux of proving the termination of the F5 algorithm of [8] is the author did not specify that critical pairs of the smallest degree are chosen in what sequence. This causes the non-determinacy of the ordering in $Rule[i]$ and the answer to the question whether a sig-polynomial is rewritable. Any proof by breaking ties using a concrete ordering would be a proof for one implementation of the F5. For example, the TRB-F5 algorithm of [13] selects the $\leq_{s_0}$-minimal one from CP_D^i[7] at the beginning of each run through the while-loop, if there are more than one J-pairs in CP_D^i. In addition, sig-polynomials are added at the head of $Rule[i]$ in [13]. We will give an example to show that, upon input a set of homogeneous polynomials, the original F5 with different concrete orderings (on critical pairs of the same degree) may output different results. In the insert_F5GEN function of this paper, we generalize the insertion strategy in $\mathcal{G}$ which covers all possible orderings in $Rule[i]$ for all i.

6.2 Criteria

Instead of sorting sig-polynomials in $\mathcal{G}$ in the F5GEN algorithm, the original F5 algorithm uses an array $Rule[i]$ to store sig-polynomials of index i, for each $i \in [1, d]$. The sig-polynomial of F5-reduction from a J-pair γ appears earlier in $Rule[i]$ than the first component of γ. So the insertion strategy of $Rule[i]$ of [8] satisfies (inversely) the description of the insert_F5GEN function. Besides, if α appears in $Rule[i]$ later than $\beta \in Rule[i]$, $deg(\mathcal{S}(\alpha)) \geq deg(\mathcal{S}(\beta))$ always holds, whereas in $\mathcal{G}$ it may not hold. That means the rewritten criterion here is more generalized than the one in [8].

[6]That is, $\mu\mathbf{e}_i <_{s_0} \sigma\mathbf{e}_j$ if $i > j$ or $i = j$ and $\mu <_m \sigma$.

[7]CP_D^i is not a notation in [13], but is used for summarizing the operations in the TRB-F5.

In [8], checking whether a sig-polynomial of index i is a normal form of itself w.r.t. the computed S-Gröbner basis of index greater than i can be viewed as a relaxation of principal syzygy check because two sig-polynomials of index i can also generate a principal syzygy sig-polynomial. Therefore, the criteria of the F5 is an implementation of the criteria of the F5GEN algorithm.

6.3 Orderings for reduction

It is important to note that the sig-polynomial selected at each time for the **TopReduction** function is determinate: the $\mathcal{S}$-minimal J-pair[8] in the minimal degree J-pairs of the current index, say i, is always selected by the F5. In our F5GEN algorithm, any J-pair in CP_D^i can be selected for $\mathcal{S}$-reduction, a relaxation of the F5. In addition, by the discussion in Section 5.2, we can add the check for the $\mathcal{S}$-reducers and the second J-pairs w.r.t. the J-pairs in CP without affecting the correct termination of the F5GEN. Hence the F5 algorithm of [8] is one implementation of the F5GEN.

6.4 Example

For the original F5 algorithm, [12] made a conjecture on which the termination is based. That is, there will not be a sig-polynomial added in $\mathcal{G}$ such that it is super top-reducible by a sig-polynomial already in $\mathcal{G}$. We doubt the truth of the conjecture and prove Lemma 5 without that conjecture. The example given in [12] can also serve as a counterexample to show that the sig-polynomials generated by the F5 have one element super top-reducible by another one.

Example 2. The admissible monomial order $\leq_m$ is the degree reverse lexicographical order ($x >_m y >_m z >_m t$) and the input polynomials are $(x^2y - z^2t, xz^2 - y^2t, yz^3 - x^2t^2)$. The admissible module order $\leq_{s_0}$ is automatically specified. The head pairs of the S-Gröbner basis generated in [12] are

$$\begin{aligned}
\vartheta(r_3) &= (\mathbf{e}_3, x^2y), & \vartheta(r_2) &= (\mathbf{e}_2, xz^2),\\
\vartheta(r_4) &= (xy\mathbf{e}_3, xy^3t), & \vartheta(r_5) &= (xyz^2\mathbf{e}_2, z^6t),\\
\vartheta(r_1) &= (\mathbf{e}_1, yz^3), & \vartheta(r_6) &= (x\mathbf{e}_1, y^3zt),\\
\vartheta(r_7) &= (x^2\mathbf{e}_1, z^5t), & \vartheta(r_9) &= (x^2z\mathbf{e}_1, y^5t^2),\\
\vartheta(r_8) &= (x^3\mathbf{e}_1, x^5t^2), & \vartheta(r_{10}) &= (z^3t\mathbf{e}_1, y^6t^2),\\
\vartheta(r_{11}) &= (x^3z\mathbf{e}_1, x^5zt^2).
\end{aligned}$$

Comparing the S-Gröbner basis in [8], only one more sig-polynomial r_{11} of head pair $\vartheta(r_{11}) = (x^3z\mathbf{e}_1, x^5zt^2)$ is generated. We can see that r_{11} can be super top-reduced by r_8.

The reason for two different S-Gröbner bases computed by the same algorithm lies in that the positions of r_9 and r_8 in $Rule[1]$ are different and r_{11} is the sig-polynomial F5-reduced from the J-pair $x{\cdot}r_9$. The original F5 did not specify that the critical pairs of the same degree should be added into $Rule[i]$ in what sequence, so the case of r_9 appearing earlier in $Rule[1]$ than r_8[9] is possible as the degrees of their signatures are the same. In that case, r_{11} is kept in contrast to the example in [8]. Therefore, if the conjecture is assumed to be correct, the proof of the correct termination would be only a partial proof.

[8]It makes no difference to consider J-pairs instead of the result of Spoly in [8] when the signature and degree of a sig-polynomial are taken into consideration.

[9]We assume that new elements are added at the beginning of $Rule[i]$.

7. CONCLUSION

This paper presents a proof of the correct termination of the F5GEN algorithms under the condition that the admissible monomial order and the admissible module order are compatible. And the F5GEN is a generalization of the F5 algorithm, so the termination of the F5 is solved.

In fact, our original goal was to prove the F5GEN with the following generalization.

CONJECTURE 1. *At line 6 of the F5GEN algorithm, assume that any J-pair can be selected from CP. Then the F5GEN terminates correctly.*

We tend to think the above is true because with $\leq_s$-minimal J-pair in CP instead of the cumbersome select_F5 function, the correct termination of the F5GEN would be proved similarly. Unfortunately, we face hurdles in proving the corresponding Lemma 4 (to be specific, Lemma 7) and Lemma 5 for that conjecture. Therefore, we leave that conjecture as an **open problem**.

8. ACKNOWLEDGMENTS

We would like to thank Christian Eder, John Perry and Vasily Galkin for valuable feedback and discussions on this work. Comments by Yao Sun, Dingkang Wang and Xiaodong Ma greatly improved this paper. We are indebted to the anonymous referee for a careful reading of this paper and many useful suggestions. Yupu Hu is partially supported by the National Natural Science Foundation of China (No. 61173151). Baocang Wang would like to thank partial supported of the National Natural Science Foundation of China (No. 61173152).

9. REFERENCES

[1] A. Arri and J. Perry. The F5 criterion revised. *Journal of Symbolic Computation*, 46(9):1017–1029, 2011.

[2] T. Becker, H. Kredel, and V. Weispfenning. *Gröbner bases: a computational approach to commutative algebra*. Springer-Verlag, London, UK, April 1993.

[3] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, Austria, 1965.

[4] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. In *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21. Springer Berlin Heidelberg, 1979.

[5] C. Eder, J. Gash, and J. Perry. Modifying Faugère's F5 algorithm to ensure termination. *ACM Communications in Computer Algebra*, 45(1/2):70–89, July 2011.

[6] C. Eder and J. Perry. F5C: A variant of Faugère's F5 algorithm with reduced Gröbner bases. *Journal of Symbolic Computation*, 45(12):1442–1458, 2010.

[7] C. Eder and J. Perry. Signature-based algorithms to compute Gröbner bases. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 99–106, New York, USA, 2011. ACM.

[8] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 27th international symposium on Symbolic and algebraic computation*, ISSAC '02, pages 75–83, New York, USA, 2002. ACM.

[9] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer Berlin Heidelberg, 2003.

[10] V. Galkin. Termination of original F5. Preprint, arXiv: 1203.2402 [math.AC], March 2012.

[11] S. Gao, F. Volny, and M. Wang. A new algorithm for computing Gröbner bases. Cryptology ePrint Archive, Report 2010/641, December 2010.

[12] J. Gash. *On efficient computation of Gröbner bases*. PhD thesis, Indiana University, USA, 2009.

[13] L. Huang. A new conception for computing Gröbner basis and its applications. Preprint, arXiv: 1012.5425 [cs.SC], December 2010.

[14] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1*. Computational Commutative Algebra. Springer, 2000.

[15] T. Stegers. Faugère's F5 algorithm revisited. Master's thesis, Technische Universität Darmstadt, 2005.

[16] Y. Sun and D. Wang. A generalized criterion for signature related Gröbner basis algorithms. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 337–344, New York, USA, 2011. ACM.

[17] F. Volny. *New Algorithms for Computing Gröbner Bases*. PhD thesis, Clemson University, 2011.

APPENDIX

During an execution of the while-loop of the F5GEN algorithm, assume that $\mathcal{G}$ computed is the set of finite sig-polynomials. Let $\mathcal{G}(j)$ and $\mathcal{G}(k)$ be two sig-polynomials in $\mathcal{G}$. We adopt the order $\lessdot$ in [10], which is defined as follows. $m_j\mathcal{G}(j) \lessdot m_k\mathcal{G}(k)$ if

1. $m_j\mathcal{S}(\mathcal{G}(j)) <_s m_k\mathcal{S}(\mathcal{G}(k))$,
2. $m_j\mathcal{S}(\mathcal{G}(j)) = m_k\mathcal{S}(\mathcal{G}(k))$ and $j > k$ (i.e., $\mathcal{G}(j)$ appears later in $\mathcal{G}$ than $\mathcal{G}(k)$),

where m_j and m_k are two monomials in $\mathcal{M}$. Particularly, $m_j\mathcal{G}(j)$ is $m_k\mathcal{G}(k)$ if $m_j\mathcal{S}(\mathcal{G}(j)) = m_k\mathcal{S}(\mathcal{G}(k))$ and $j = k$. It can be seen that $\lessdot$ is a well-order on $\mathcal{M} \times \mathcal{G}$, because $\leq_s$ is a well-order and $\mathcal{G}$ is finite.

Below we will introduce representations that are inspired by the ideas of [6, 10]. Let α be a sig-polynomial, if

$$poly(\alpha) = \sum_{k=1}^{\ell} p_k \cdot poly(\mathcal{G}(i_k)), \mathcal{G}(i_k) \in \mathcal{G}, \tag{4}$$

$\sum_{k=1}^{\ell} p_k\mathcal{G}(i_k)$ is called an ($\mathcal{G}$-)**representation** of α. Each $m_{k_v}\mathcal{G}(i_k)$ is called an **element** of the representation, where $p_k = \sum_v c_{k_v} m_{k_v}$, $0 \neq c_{k_v} \in K$ and $m_{k_v} \in \mathcal{M}$. Of course, we can store all elements of a representation in an array $A \in (\mathcal{M} \times \mathcal{G})^v$ of size v such that $A_1 \succcurlyeq \cdots \succcurlyeq A_v$. Let another $\mathcal{G}$-representation of α be $\sum_{k=1}^{\ell'} p'_k\mathcal{G}(j_k)$ and its array of elements be $A' \in (\mathcal{M} \times \mathcal{G})^{v'}$. The representation A' is called $\lessdot$-smaller than A if A' has $\lessdot$-smaller element at the

leftmost position for which they differ[10]. If $\mathcal{S}(p_k\mathcal{G}(i_k)) \leq_s \mathcal{S}(\alpha), \forall k \in [1,\ell]$, the $\mathcal{G}$-representation is called **$\mathcal{S}$-safe** (i.e. the term "signature-safe" in [10]). Let t be a monomial in $\mathcal{M}$. The $\mathcal{S}$-safe $\mathcal{G}$-representation is called a **t-representation** if $HM(p_k\mathcal{G}(i_k)) \leq_m t, \forall k \in [1,\ell]$. We can give few examples for those representations.

Example 3. Let $\mathcal{G}(j) = (\mathbf{u}, p) \in \mathcal{G}$ be a sig-polynomial and m be a monomial.

- $m\mathcal{G}(j)$ itself is an $\mathcal{S}$-safe representation of $m\mathcal{G}(j)$, called a **trivial representation**.
- Assume that $\mathcal{G}(j) \notin \{F_1, \ldots, F_d\}$. As $\mathcal{G}$ is initialized with $\{F_1, \ldots, F_d\}$, $\sum_{k=1}^{d} m \cdot u_k F_k$ is an $\mathcal{S}$-safe $\mathcal{G}$-representation of $m\mathcal{G}(j)$, where $(u_1, \ldots, u_d) = \mathbf{u} \in R^d$. It is called a **signature representation**[11]. It is important to note that we have

  $$\mathcal{S}(mHM(u_k)F_k) <_s \mathcal{S}(m\mathcal{G}(j)), \forall k \in [1,d],$$

  except one, say w, such that

  $$\mathcal{S}(mHM(u_w)F_w) = \mathcal{S}(m\mathcal{G}(j)).$$

  Clearly, $\mathcal{G}(j)$ appears later than F_w by the insertion strategy of the F5GEN, i.e., $m\mathcal{G}(j) \lessdot mHM(u_w)F_w$. So the trivial representation $m\mathcal{G}(j)$ is $\lessdot$-smaller than the signature representation $\sum_{k=1}^{d} m \cdot u_k F_k$.
- Let $\alpha = (\mathbf{u}, 0)$ be a principal syzygy sig-polynomial generated by $\mathcal{G}(i)$ and $\mathcal{G}(j)$ in $\mathcal{G}$. That is,

  $$\alpha = poly(\mathcal{G}(i))\mathcal{G}(j) - poly(\mathcal{G}(j))\mathcal{G}(i),$$

  which is an $\mathcal{S}$-safe $\mathcal{G}$-representation.

Then Lemma 4 is proved as follows.

Proof. Suppose ζ cannot be F5-reduced by the present $\mathcal{G}$. Let $m\mathcal{G}(k)$ be a non-syzygy sig-polynomial $\mathcal{S}$-reducing ζ. Either $\mathcal{S}(m\mathcal{G}(k)) \in \mathcal{S}(PS)$ or $m\mathcal{G}(k)$ is rewritable by $\mathcal{G}$.

1. If $\mathcal{S}(m\mathcal{G}(k))$ is in $\mathcal{S}(PS)$, there is a principal syzygy sig-polynomial $(\mathbf{u}', 0)$, such that $m'\mathcal{S}(\mathbf{u}') = m\mathcal{S}(\mathcal{G}(k))$. Adding $(c \cdot m\mathbf{u}', 0)$ to $m\mathcal{G}(k)$, we can obtain a sig-polynomial $(\mathbf{u}^*, m \cdot poly(\mathcal{G}(k)))$ such that $\mathcal{S}(\mathbf{u}^*) <_s m\mathcal{S}(\mathcal{G}(k))$. The signature representation $\sum_t u_t^* F_t$ of $(\mathbf{u}^*, m \cdot poly(\mathcal{G}(k)))$ is a representation of $m\mathcal{G}(k)$ $\lessdot$-smaller than the trivial representation $m\mathcal{G}(k)$. If the signature of an element $m_{t_v}F_t \in \sum_t u_t^* F_t$ is in $\mathcal{S}(PS)$, we can find an $\mathcal{S}$-safe $\mathcal{G}$-representation $\lessdot$-smaller than $\sum_t u_t^* F_t$ by the same method discussed above.
2. If $m\mathcal{G}(k)$ is rewritable by $\mathcal{G}$, let $\mathcal{G}(j)$ be the one rewriting $m\mathcal{G}(k)$. So $j > k$ and $\mathcal{S}(m'\mathcal{G}(j)) = \mathcal{S}(m\mathcal{G}(k))$, i.e., $m'\mathcal{G}(j) \lessdot m\mathcal{G}(k)$. As $m\mathcal{G}(k)$ and $m'\mathcal{G}(j)$ share a common $\lessdot$-maximum element, say m^*F_w with

   $$w = idx(m\mathcal{G}(k)) = idx(m'\mathcal{G}(j)),$$

   by canceling m^*F_w, $m\mathcal{G}(k)$ has an $\mathcal{S}$-safe representation of the form

   $$m'\mathcal{G}(j) + \sum_t p_t F_t, \tag{5}$$

   which is $\lessdot$-smaller than the trivial $\mathcal{G}$-representation $m(SG)'(k)$. Similarly, if $m_{t_v}F_t$ in representation (5) can be rewrite by $\mathcal{G}_{\leq_s(\mathbf{s}_i)}$, we would obtain a $\lessdot$-smaller $\mathcal{S}$-safe $\mathcal{G}$-representation.

Because $\lessdot$ is a well-order on $\mathcal{M} \times \mathcal{G}$, we can ensure that there is an $\mathcal{S}$-safe $\mathcal{G}$-representation of $m\mathcal{G}(k)$ such that each element is neither in PS nor rewritable by $\mathcal{G}$. Together with the following lemma, we would have an $\mathcal{S}$-safe $HM(m\mathcal{G}(k))$-representation such that each element would be neither in PS nor rewritable by updated $\mathcal{G}$ after finite while-loops. Therefore, there exists a sig-polynomial in updated $\mathcal{G}$ F5-reducing $m\mathcal{G}(k)$. □

Making use of the proof for Lemma 32 of [10], we can obtain a short lemma below.

Lemma 7. *Assume the F5GEN has computed correctly up to signature* $\mathbf{s}$. *Let* $\sum_t p_t\mathcal{G}(j_t)$ *be an* $\mathcal{S}$*-safe* $\mathcal{G}$*-representation of* $m\mathcal{G}(k)$, *where* $m\mathcal{S}(\mathcal{G}(k)) <_s \mathbf{s}$. *We assume that each element* $m_{t_y}\mathcal{G}(j_t)$ *is neither in* PS *nor rewritable by* $\mathcal{G}$. *If there exists an element* $m_{t_v}\mathcal{G}(j_t)$ *such that* $HM(m_{t_v}\mathcal{G}(j_t)) > HM(m\mathcal{G}(k))$, *where* $m_{t_v} \in p_t$, $m\mathcal{G}(k)$ *would have an* $\mathcal{S}$*-safe* $\mathcal{G}$*-representation* $\lessdot$*-smaller than* $\sum_t p_t\mathcal{G}(j_t)$ *after finite runs through the while-loop.*

Proof. Because $poly(m\mathcal{G}(k)) = \sum_t p_t \cdot poly(\mathcal{G}(j_t))$ and $HM(m_{t_v}\mathcal{G}(j_t)) > HM(m\mathcal{G}(k))$, there exists another element $m_{r_w}\mathcal{G}(j_r)$ such that

$$HM(m_{r_w}\mathcal{G}(j_r)) = HM(m_{t_v}\mathcal{G}(j_t)).$$

Let m' and m'' be two monomials such that

$$HM(m'\mathcal{G}(j_t)) = HM(m''\mathcal{G}(j_r)) = lcm(\mathcal{G}(j_t), \mathcal{G}(j_r))$$

and $m'\mathcal{S}(\mathcal{G}(j_t)) > m''\mathcal{S}(\mathcal{G}(j_r))$. If $m'\mathcal{G}(j_t)$ had been considered by the F5GEN algorithm, there would be a sig-polynomial in current $\mathcal{G}$ rewriting $m'\mathcal{G}(j_t)$, a contradiction. From the selection strategy of the F5GEN, we know that $deg(m'\mathcal{S}(\mathcal{G}(j_t)) = deg(\mathbf{s})$ and $m'\mathcal{G}(j_t)$ has not been considered. Obviously, the F5GEN cannot generate infinite J-pairs such that their signatures are of a fixed degree. So $m'\mathcal{G}(j_t)$ would be output at line 6 of the algorithm after finite runs through the while-loop. By the assumption of the lemma, the J-pair $m'\mathcal{G}(j_t)$ can pass the F5-criteria of the F5GEN algorithm and would be F5-reduced to a new sig-polynomial $\mathcal{G}(\ell)$ stored into $\mathcal{G}$. Hence

$$\mathcal{S}(\mathcal{G}(\ell)) = m'\mathcal{S}(\mathcal{G}(j_t)) \text{ and } \ell > j_t,$$

i.e., $\mathcal{G}(\ell) \lessdot m'\mathcal{G}(j_t)$ and $\mathcal{G}(\ell)$ can rewrite the element $m'\mathcal{G}(j_t)$. By the method of case (2) in the above lemma, we can find an $\mathcal{S}$-safe $\mathcal{G}$-representation $\lessdot$-smaller than $\sum_t p_t\mathcal{G}(j_t)$. □

[10]The comparison is proceeded by padding with zeros at the right of the shorter array if A and A' are not of equal length.
[11]Different from the input-representation defined in [10], the signature representation of a fixed sig-polynomial is unique.