THE F5 ALGORITHM IN BUCHBERGER'S STYLE*

Yao SUN · Dingkang WANG

DOI: 10.1007/s11424-011-0218-3 Received: 25 August 2010 / Revised: 13 December 2010 ©The Editorial Office of JSSC & Springer-Verlag Berlin Heidelberg 2011

Abstract The famous F5 algorithm for computing Gröbner basis was presented by Faugère in 2002. The original version of F5 is given in programming codes, so it is a bit difficult to understand. In this paper, the F5 algorithm is simplified as F5B in a Buchberger's style such that it is easy to understand and implement. In order to describe F5B, we introduce F5-reduction, which keeps the signature of labeled polynomials unchanged after reduction. The equivalence between F5 and F5B is also shown. At last, some versions of the F5 algorithm are illustrated.

Key words Buchberger's style, F5 algorithm, Gröbner basis.

1 Introduction

Solving systems of polynomial equations is a basic problem in computer algebra, through which many practical problems can be solved easily. Among all the methods for solving polynomial systems, the Gröbner basis method is one of the most efficient approaches. After the concept of Gröbner basis is proposed in [1], many algorithms have been presented for computing Gröbner basis, including [2–7]. Currently, F5 is one of the most efficient algorithms.

After the F5 algorithm is proposed, many researches have been done. For example, Bardet et al. study the complexity of this algorithm in [8]. Faugère and Ars use the F5 algorithm to attack multivariable systems in [9]. Stegers revisits the F5 algorithm in [10]. Eder discusses the two criteria of the F5 algorithm in [11] and proposes a variation of the F5 algorithm^[12]. Ars and Hashemi present two variation of criteria in [13]. Recently, Gao et al. give a new incremental algorithm in [14]. The current authors discuss the F5 algorithm over boolean ring and present a branch F5 algorithm^[15-16]. We also give a complete proof for the correctness of the F5 or F5-like algorithm in [17].

However, since the original F5 algorithm is reported in programming codes, it seems a bit difficult to understand this famous algorithm very well. In this paper, we revisit the F5 algorithm from our perspective and we simplify F5 to F5B in Buchberger's style, which is equivalent to the original F5 algorithm. We also discuss some versions of the F5 algorithm, such as Incremental F5 algorithm in [3], Non-incremental F5 algorithm reported by Faugère in INSCRYPT 2008 and Matrix F5 algorithm mentioned in [8].

This paper is organized as follows. The main idea of the F5 algorithm is illustrated in Section 3 after some basic notions given in Section 2. In Section 4, F5B is proposed and the

Yao SUN \cdot Dingkang WANG

Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China. Email: sunyao@amss.ac.cn; dwang@mmrc.iss.ac.cn.

^{*}This research is supported by NKBRPC 2011CB302400, NSFC 10971217 and 60821002/F02.

^{\circ} This paper was recommended for publication by Editor Ziming LI.

equivalence of F5 and F5B is shown as well. Some versions of the F5 algorithm are discussed in Section 5. At last, some conclusions are presented in Section 6.

2 Basic Notations

Let K be a field and $K[X] = K[x_1, x_2, \dots, x_n]$ a polynomial ring with coefficients in K. Let \mathbb{N} be the set of non-negative integers and PP(X) the set of power products of $\{x_1, x_2, \dots, x_n\}$, i.e., $PP(X) := \{x^{\alpha} \mid x^{\alpha} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \alpha_i \in \mathbb{N}, i = 1, 2, \dots, n\}$.

Let \prec be an admissible order defined over PP(X). Given $t = x^{\alpha} \in PP(X)$, the degree of t is defined as $\deg(t) := |\alpha| = \sum_{i=1}^{n} \alpha_i$. For a polynomial $0 \neq f \in K[x_1, x_2, \cdots, x_n]$, we have $f = \sum c_{\alpha} x^{\alpha}$. The degree of f is defined as $\deg(f) := \max\{|\alpha|, c_{\alpha} \neq 0\}$ and the leading power product of f is $\operatorname{lpp}(f) := \max\{x^{\alpha}, c_{\alpha} \neq 0\}$ w.r.t. \prec . If $\operatorname{lpp}(f) = x^{\alpha}$, then the leading coefficient and leading monomial of f are defined as $\operatorname{lc}(f) := c_{\alpha}$ and $\operatorname{lm}(f) := c_{\alpha} x^{\alpha}$, respectively.

3 Revisit the F5 Algorithm

In brief, the major contribution of the F5 algorithm is presenting two new criteria: Syzygy Criterion and Rewritten Criterion. Syzygy Criterion is also called F5 Criterion in some papers. Almost all useless computations (redundant S-polynomials) can be removed by these two criteria. Both of the criteria are built on the concept of signature and a special reduction procedure.

In this section, we first illustrate the main idea of Syzygy Criterion and Rewritten Criterion by some simple examples, and then introduce the definition of signature. The special reduction is presented in the next section. For more details about the F5 algorithm, please see [3].

3.1 About Syzygy Criterion

Of the two criteria, Syzygy Criterion is more important and creative. Let us see a simple example.

Example 1 Consider a system in $\mathbb{Q}[x, y, z]$ with the Graded Reverse Lex Order with $x \succ y \succ z$,

$$\begin{cases} f_1 = x^2 + y, \\ f_2 = xy - z. \end{cases}$$

The S-polynomial spoly $(f_1, f_2) = yf_1 - xf_2 = y^2 + xz$, which is not reducible by $\{f_1, f_2\}$. We denote $f_3 = \text{spoly}(f_1, f_2)$. Now, consider the S-polynomial of f_3 and f_2 :

$$spoly(f_3, f_2) = xf_3 - yf_2 = x^2z + yz = zf_1,$$

the leading monomial of f_2 and f_3 are not co-prime, but spoly (f_3, f_2) reduces to 0 by $\{f_1, f_2\}$. Why? What makes this S-polynomial spoly (f_3, f_2) reduce to 0?

If we dig it deeper, we will see that the reason still comes from the syzygy $(f_2, -f_1)$ of the 2-tuple vector (f_1, f_2) . Since $f_3 = yf_1 - xf_2$ and $f_2f_1 - f_1f_2 = 0$, then we have

$$spoly(f_2, f_3) = xf_3 - yf_2 = xyf_1 - (x^2 + y)f_2 = lm(f_2)f_1 - f_1f_2 = (lm(f_2) - f_2)f_1.$$

Thus, it is natural that the S-polynomial spoly (f_3, f_2) reduces to 0 by $\{f_1\}$.

Theoretically, in order to speed up the algorithm for computing Gröbner basis, we have to avoid computing the S-polynomials of the above kind. Now, the question is: how to detect them? As the S-polynomial spoly (f_3, f_2) reduces to 0 due to the syzygy $(f_2, -f_1)$ of the vector (f_1, f_2) , a natural idea is to connect the polynomials f_3 and f_1 .

🖄 Springer

The relation $f_3 = yf_1 - xf_2$ means f_3 comes from yf_1 , so we can append a signature $y\mathbf{e}_1$ to f_3 to reflect this fact. Similarly, we also can append a signature $xy\mathbf{e}_1$ to xf_3 , which shows xf_3 comes from $xyf_1 = \ln(f_2)f_1$. Now from the signature $xy\mathbf{e}_1 = \ln(f_2)\mathbf{e}_1$, we are able to understand why the S-polynomial spoly (f_3, f_2) can be reduced to 0.

In more general cases, for the polynomial system $\{f_1, f_2, \dots, f_m\} \subset K[X]$, the syzygies of the *m*-tuple vector $(f_1, f_2, \dots, f_m) \in (K[X])^m$ also result in many S-polynomials reducing to 0. So the Syzygy Criterion is a criterion that detects useless S-polynomials by using syzygies of (f_1, f_2, \dots, f_m) . In the above simple example, the signature of polynomial provides an useful information to detect this kind of unnecessary S-polynomials. Next, we give a mathematical explanation of signatures.

3.2 Signatures and Labeled Polynomials

Consider a polynomial system $\{f_1, f_2, \dots, f_m\} \subset K[X]$ and denote (f_1, f_2, \dots, f_m) a polynomial *m*-tuple in $(K[X])^m$. We call the f_i 's initial polynomials of the ideal $\langle f_1, f_2, \dots, f_m \rangle$, since they are initial generators of ideal $\langle f_1, f_2, \dots, f_m \rangle \subset K[X]$.

Let \mathbf{e}_i be the canonical *i*-th unit vector in the free K[X]-module $(K[X])^m$, i.e., the *i*-th element of \mathbf{e}_i is 1, while the others are 0. Consider the homomorphism map σ over the free K[X]-module $(K[X])^m$:

$$\sigma: (\mathbf{K}[X])^m \longrightarrow \mathbf{K}[X],$$

$$(g_1, g_2, \cdots, g_m) \longmapsto g_1 f_1 + g_2 f_2 + \cdots + g_m f_m$$

Then $\sigma(\mathbf{e}_i) = f_i$. More generally, if $\mathbf{g} = g_1 \mathbf{e}_1 + g_2 \mathbf{e}_2 + \cdots + g_m \mathbf{e}_m$, where $g_i \in \mathbf{K}[X]$ for $1 \leq i \leq m$, then $\sigma(\mathbf{g}) = g_1 f_1 + g_2 f_2 + \cdots + g_m f_m$.

The admissible order \prec on PP(X) extends to the free module $(K[X])^m$ naturally in a POT (position over term) fashion:

$$x^{\alpha}\mathbf{e}_{i} < x^{\beta}\mathbf{e}_{j} (\text{ or } x^{\beta}\mathbf{e}_{j} > x^{\alpha}\mathbf{e}_{i}) \quad \text{iff } \begin{cases} i > j, \\ i = j \text{ and } x^{\alpha} \prec x^{\beta}. \end{cases}$$

Thus, we have $\mathbf{e}_m < \mathbf{e}_{m-1} < \cdots < \mathbf{e}_1$ directly.

With the admissible order $\langle \text{ on } (\mathbb{K}[X])^m$, we can define the leading power product, leading coefficient and leading monomial of a *m*-tuple vector $\mathbf{g} \in (\mathbb{K}[X])^m$. For example, let $\mathbf{g} = (2x^2 + y^2, 3xy) \in (\mathbb{Q}[x, y])^2$ or equivalently $\mathbf{g} = (2x^2 + y^2)\mathbf{e}_1 + 3xy\mathbf{e}_2$ and \prec the Lex order on $PP(x, y) \ (x \succ y)$. Then we have $\operatorname{lpp}(\mathbf{g}) = x^2\mathbf{e}_1$, $\operatorname{lc}(\mathbf{g}) = 2$ and $\operatorname{lm}(\mathbf{g}) = 2x^2\mathbf{e}_1$.

The following is the definition of labeled polynomial and its signature. The idea of labeled polynomials draws lessons from [14].

Definition 1 Let $g \in \langle f_1, f_2, \dots, f_m \rangle$ be a polynomial and $\mathbf{g} \in (\mathbf{K}[X])^m$ an *m*-tuple vector such that $\sigma(\mathbf{g}) = g$. Then we call $\mathcal{G} = (\mathbf{g}, g)$ a labeled polynomial.

For a labeled polynomial \mathcal{G} , we define

- 1) the signature $\operatorname{sign}(\mathcal{G}) := \operatorname{lpp}(\mathbf{g});$
- 2) the polynomial part $poly(\mathcal{G}) := g;$

3) the leading power product $lpp(\mathcal{G}) := lpp(g);$

4) the leading monomial $lm(\mathcal{G}) := lm(g)$.

Suppose $\mathcal{F} = (\mathbf{f}, f), \mathcal{G} = (\mathbf{g}, g)$ are labeled polynomials and cx^{α} is a non-zero monomial, we define scaler multiplication and addition for labeled polynomials as following:

• $cx^{\alpha} \cdot \mathcal{F} = cx^{\alpha}\mathcal{F} = (cx^{\alpha}\mathbf{f}, cx^{\alpha}f).$

•
$$\mathcal{F} + \mathcal{G} = (\mathbf{f} + \mathbf{g}, f + g).$$

Springer

Definition 2 For labeled polynomials \mathcal{F}, \mathcal{G} , we say $[\mathcal{F}, \mathcal{G}] := (u, \mathcal{F}, v, \mathcal{G})$ is a critical pair of \mathcal{F} and \mathcal{G} if u, v are monomials such that $u \operatorname{lm}(\mathcal{F}) = v \operatorname{lm}(\mathcal{G}) = \operatorname{lcm}(\operatorname{lpp}(\mathcal{F}), \operatorname{lpp}(\mathcal{G}))$, and the corresponding S-polynomial of $[\mathcal{F}, \mathcal{G}]$ is denoted by $\operatorname{spoly}(\mathcal{F}, \mathcal{G}) = u\mathcal{F} - v\mathcal{G}$.

3.3 Syzygy Criterion

We are now able to describe the Syzygy Criterion in mathematical words. We begin by the following definition.

Definition 3 Let $\mathcal{F} = (\mathbf{f}, f)$ be a labeled polynomial with $\operatorname{lpp}(\mathbf{f}) = x^{\alpha} \mathbf{e}_i, cx^{\gamma}$ a non-zero monomial and B a set of labeled polynomials. The labeled polynomial $cx^{\gamma}\mathcal{F}$ is said to be divisible by B, if there exists a labeled polynomial $\mathcal{G} = (\mathbf{g}, g) \in B$ with $\operatorname{lpp}(\mathbf{g}) = x^{\beta} \mathbf{e}_j$ such that

1) $\operatorname{lpp}(g) \mid x^{\gamma+\alpha}$, and 2) $\mathbf{e}_i > \mathbf{e}_j$, i.e. i < j. Then the Syzygy Criterion is described as follows.

Criterion 1 — Syzygy Criterion

Let $[\mathcal{F}, \mathcal{G}] := (u, \mathcal{F}, v, \mathcal{G})$ be a critical pair and B a set of labeled polynomials. If either $u\mathcal{F}$ or $v\mathcal{G}$ is divisible by B, then the critical pair $[\mathcal{F}, \mathcal{G}]$ meets the Syzygy Criterion.

Syzygy criterion is also called F5 criterion in some papers. In F5, if a critical pair meets the Syzygy Criterion, then the corresponding S-polynomial is redundant.

Let us review the two simple examples from Subsection 3.1 in the view of Syzygy Criterion. In Example 1, Let $\mathcal{F}_1 = (\mathbf{e}_1, f_1)$ and $\mathcal{F}_2 = (\mathbf{e}_2, f_2)$. Let $\mathcal{F}_3 = \operatorname{spoly}(\mathcal{F}_1, \mathcal{F}_2) = y\mathcal{F}_1 - x\mathcal{F}_2 = (y\mathbf{e}_1 - x\mathbf{e}_2, y^2 + xz)$.

Next, consider the critical pair $[\mathcal{F}_3, \mathcal{F}_2] = (x, \mathcal{F}_3, y, \mathcal{F}_2)$. However, $x\mathcal{F}_3 = (xy\mathbf{e}_1 - x^2\mathbf{e}_2, x(y^2 + xz))$ is divisible by $\{\mathcal{F}_2\}$, so the critical pair $[\mathcal{F}_3, \mathcal{F}_2]$ is also redundant by Syzygy Criterion. And spoly $(\mathcal{F}_3, \mathcal{F}_2)$ does reduce to 0 in Example 1, which verifies the Syzygy Criterion.

3.4 Rewritten Criterion

We next describe the Rewritten Criterion. In fact, Rewritten Criterion is more like a programming technique, which reflects Buchberger's idea: try to reuse as much as possible the previous computations. Let us see the following example.

Example 2 Consider a system in $\mathbb{Q}[x, y]$ with the Graded Reverse Lex Order with $x \succ y$:

$$\begin{cases} f_1 = x^2 + xy, \\ f_2 = x^2 + y. \end{cases}$$

The S-polynomial spoly $(f_1, f_2) = f_1 - f_2 = xy - y$ is not reducible by $\{f_1, f_2\}$. So denote $f_3 = xy - y$. Next we need to consider the S-polynomial spoly $(f_1, f_3) = yf_1 - xf_3$ as well as the S-polynomial spoly $(f_2, f_3) = yf_2 - xf_3$. However, with a further study, we will find that the S-polynomial spoly (f_1, f_3) is not necessary to reduce due to the following observation:

$$\operatorname{spoly}(f_1, f_3) = yf_1 - xf_3 = y(f_1 - f_2) - (yf_2 - xf_3) = y\operatorname{spoly}(f_1, f_2) - \operatorname{spoly}(f_2, f_3).$$

That is, if the S-polynomials $\operatorname{spoly}(f_1, f_2)$ and $\operatorname{spoly}(f_2, f_3)$ have been reduced (or scheduled to reduce), then reducing the S-polynomial $\operatorname{spoly}(f_1, f_3)$ becomes a duplicated job. Rigorous proof needs the knowledge of t-representation. For more details, please see [17].

🖄 Springer

Thus, the Rewritten Criterion is a criterion that detects duplicated reductions of polynomials. The meaning of Rewritten Criterion is much clearer in a variation of the F5 algorithm that uses matrix reduction, which will be discussed in Section 5. Now, we give the mathematical definition of Rewritten Criterion.

Definition 4 Let $\mathcal{F} = (\mathbf{f}, f)$ be a labeled polynomial, cx^{γ} a non-zero monomial in X and B a set of labeled polynomials. The labeled polynomial $cx^{\gamma}\mathcal{F} = (cx^{\gamma}\mathbf{f}, cx^{\gamma}f)$ is said to be rewritable by B, if there exists a labeled polynomial $\mathcal{G} = (\mathbf{g}, g) \in B$, such that:

1) $\operatorname{sign}(\mathcal{G}) | \operatorname{sign}(cx^{\gamma}\mathcal{F})$, i.e. $\operatorname{lpp}(\mathbf{g}) | \operatorname{lpp}(cx^{\gamma}\mathbf{f})$, and

2) labeled polynomial \mathcal{G} is generated later than \mathcal{F} .

The Rewritten Criterion is given as follows.

Criterion 2 — Rewritten Criterion

Let $[\mathcal{F}, \mathcal{G}] := (u, \mathcal{F}, v, \mathcal{G})$ be a critical pair where u, v are monomials in X such that $u \operatorname{Im}(\mathcal{F}) = v \operatorname{Im}(\mathcal{G}) = \operatorname{Icm}(\operatorname{lpp}(\mathcal{F}), \operatorname{lpp}(\mathcal{G}))$, and B a set of labeled polynomials. If either $u\mathcal{F}$ or $v\mathcal{G}$ is rewritable by B, then the critical pair $[\mathcal{F}, \mathcal{G}]$ meets the Rewritten Criterion.

If a critical pair meets the Rewritten Criterion in the F5 algorithm, then it is not necessary to reduce its S-polynomial. Now let us explain the fact in Example 2. The system is $f_1 = x^2 + xy$, $f_2 = x^2 + y \in \mathbb{Q}[x, y]$. Labeled polynomials $\mathcal{F}_1 = (\mathbf{e}_1, f_1)$ and $\mathcal{F}_2 = (\mathbf{e}_2, f_2)$ correspond to f_1 and f_2 , respectively. The S-polynomial of \mathcal{F}_1 and \mathcal{F}_2 is $\mathcal{F}_3 = \mathcal{F}_1 - \mathcal{F}_2 = (\mathbf{e}_1 - \mathbf{e}_2, xy - y)$.

Next, let us see the critical pair $[\mathcal{F}_1, \mathcal{F}_3] = (y, \mathcal{F}_1, x, \mathcal{F}_3)$. Clearly, labeled polynomial \mathcal{F}_3 is generated later than \mathcal{F}_1 , so it is easy to know $y\mathcal{F}_1$ is rewritable by $\{\mathcal{F}_3\}$. Thus, critical pair $[\mathcal{F}_1, \mathcal{F}_3]$ meets the Rewritten Criterion, and hence, it can be removed.

As discussed in this section, both Syzygy Criterion and Rewritten Criterion build on the concept of signature. However, to ensure both criteria correct during the computations, a special reduction procedure is necessary, which is detailed in the next section.

4 Simplify the F5 Algorithm to a Buchberger's Style

In order to simplify the F5 algorithm to a Buchberger's style, the most important step is to rewrite the reduction procedure. The original reduction in the F5 algorithm is described by codes and may return several reduction results each time. In this section, a simplified version of reduction (F5-reduction) is proposed in the first subsection. The F5 algorithm in Buchberger's style (F5B algorithm) is described in the second subsection. We will discuss the equivalence of the F5 and F5B algorithms in the last subsection.

4.1 F5-Reduction

The signatures of the labeled polynomials are used to detect useless critical pairs by the criteria, but this is not sufficient to ensure the correctness of the F5 algorithm. Only under F5-reduction, which is a special kind of reduction process, the critical pairs detected by the criteria are really useless. The same is true for other F5-like algorithms.

Let us start with the definition of F5-reduction, which is a revised version of the TopReduction function in [3].

Definition 5 Let $\mathcal{F} = (\mathbf{f}, f)$ be a labeled polynomial and B a set of labeled polynomials. The labeled polynomial \mathcal{F} is F5-reducible by B, if there exists $\mathcal{G} = (\mathbf{g}, g) \in B$ such that:

1) $\operatorname{lpp}(g) | \operatorname{lpp}(f)$, denote $x^{\gamma} = \operatorname{lpp}(f)/\operatorname{lpp}(g)$ and $c = \operatorname{lc}(f)/\operatorname{lc}(g)$,

2) $\operatorname{sign}(\mathcal{F}) > \operatorname{sign}(cx^{\gamma}\mathcal{G})$, i.e., $\operatorname{lpp}(\mathbf{f}) > \operatorname{lpp}(cx^{\gamma}\mathbf{g})$,

Springer

3) $cx^{\gamma}\mathcal{G}$ is not divisible by B, and

4) $cx^{\gamma}\mathcal{G}$ is not rewritable by B.

If \mathcal{F} is F5-reducible by B, let $\mathcal{F}' = \mathcal{F} - cx^{\gamma}\mathcal{G}$. Then this procedure: $\mathcal{F} \Longrightarrow_B \mathcal{F}'$ is called one step F5-reduction. If \mathcal{F}' is still F5-reducible by B, then repeat this step until \mathcal{F}' is not F5-reducible by B. Suppose \mathcal{F}^* is the final result that is not F5-reducible by B. We say \mathcal{F} F5-reduces to \mathcal{F}^* by B, and denote it as $\mathcal{F} \Longrightarrow_B^* \mathcal{F}^*$.

Deleting the conditions 3) and 4) does not affect the correctness of algorithm, but leads to redundant computations/reductions.

The key of F5-reduction is the condition $\operatorname{sign}(\mathcal{F}) > \operatorname{sign}(cx^{\gamma}\mathcal{G})$, i.e., $\operatorname{lpp}(\mathbf{f}) > \operatorname{lpp}(cx^{\gamma}\mathbf{g})$, which makes F5-reduction much different from other general reductions. The major function of this condition is to preserve the signature of \mathcal{F} during reductions. Thus a direct result is that, if labeled polynomial \mathcal{F} F5-reduces to \mathcal{F}^* by B (i.e., $\mathcal{F} \Longrightarrow_B^* \mathcal{F}^*$), then the signatures of \mathcal{F} and \mathcal{F}^* are identical, i.e.,

$$\operatorname{sign}(\mathcal{F}) = \operatorname{sign}(\mathcal{F}^*).$$

This property plays a crucial role in the proof for the correctness of the F5B algorithm. For more details, please see [17].

4.2 The F5 Algorithm in Buchberger's Style

With the definitions of Syzygy Criterion, Rewritten Criterion and F5-reduction, we can rewrite the F5 algorithm in Buchberger's style (F5B algorithm).

Algorithm 1 — The F5 algorithm in Buchberger's style (F5B algorithm)

Input: a polynomial *m*-tuple: $(f_1, f_2, \dots, f_m) \in K[X]^m$; and an admissible order \prec . **Output:** The Gröbner basis of the ideal $\langle f_1, f_2, \dots, f_m \rangle \subset K[X]$.

```
begin
     \mathcal{F}_i \longleftarrow (\mathbf{e}_i, f_i) \text{ for } i = 1, 2, \cdots, m
     B \longleftarrow \{\mathcal{F}_i \mid i = 1, 2, \cdots, m\}
     CP \leftarrow \{ \text{critical pair } [\mathcal{F}_i, \mathcal{F}_j] \mid 1 \le i < j \le m \}
     while CP is not empty do
           cp \leftarrow select a critical pair from CP
          CP \leftarrow -CP \setminus \{cp\}
          if cp meets neither Syzygy Criterion nor Rewritten Criterion,
                then
                     SP \leftarrow the S-polynomial of critical pair cp
                     \mathcal{P} the F5-reduction result of \mathcal{S}P by B, i.e., \mathcal{S}P \Longrightarrow_B^* \mathcal{P}
                     if the polynomial of \mathcal{P} is not 0, i.e., poly(\mathcal{P}) \neq 0,
                           then
                                CP \leftarrow CP \cup \{ \text{critical pair } [\mathcal{P}, \mathcal{Q}] \mid \mathcal{Q} \in B \}
                     end if
                     B \leftarrow B \cup \{\mathcal{P}\}
                                                  # no matter whether poly(\mathcal{P}) \neq 0 or not
          end if
     end while
     return {polynomial part of \mathcal{Q} \mid \mathcal{Q} \in B}
end
```

Of course, some auxiliary data are also necessary to be recorded in the implementation.

🖄 Springer

For example, we need to keep the generating order of the labeled polynomials. We can also save labeled polynomials as $(lpp(\mathbf{g}), g)$ instead of (\mathbf{g}, g) during the compution, since only the information of $lpp(\mathbf{g})$ is really used.

The strategy of selecting critical pairs is not specified in the F5B algorithm, instead, we simply use

 $cp \leftarrow$ select a critical pair from CP.

Different strategies of selecting critical pairs will lead to different versions of the F5 algorithm, including the original Incremental F5 algorithm in [3], Non-Incremental F5 algorithm reported by Faugere in recent conference (INSCRYPT 2008), Matrix F5 algorithm mentioned in [8]. All these versions of the F5 algorithm are discussed in the next section.

Moveover, the original F5 algorithm differs from the F5B algorithm only by a strategy of selecting critical pairs as well. Let us see more discussions in the following subsection.

4.3 Equivalence of the F5 and F5B Algorithms

The major difference between $F5^{[3]}$ and F5B is the reduction process. In [3], reduction of S-polynomials is done by the Reduction function. So next, we will focus on showing that the Reduction function is equivalent to a set of F5-reduction with an appropriate strategy of selecting critical pairs. Let us see the TopReduction function first, which is a subfunction of the Reduction function (function 1).

Function 1 — TopReduction	
-	labeled polynomial \mathcal{F} , a set of labeled polynomials B , a set of labeled polynomials $do do$ which needs to be reduced further.
De	2-tuple $(Done', Todo')$: both $Done'$ and $Todo'$ are sets of labeled polynomials, while one' contains the result of reduction and $Todo'$ includes the labeled polynomials to reduced further.
begin	
$\mathcal{G} \leftarrow$ a lab	beled polynomial in B such that:
	1) $\operatorname{lpp}(\mathcal{G}) \operatorname{lpp}(\mathcal{F}) \text{ and denote } v = \operatorname{lm}(\mathcal{F})/\operatorname{lm}(\mathcal{G}),$
	2) $v\mathcal{G}$ is not divisible by B , and
	3) $v\mathcal{G}$ is not rewritable by $B \cup \{\mathcal{F}\} \cup Todo$.
	does not exist,
then	
\mathbf{ret}	$\mathbf{urn} \ (\{\mathcal{F}\}, \emptyset)$
else	
if s	ignature $\operatorname{sign}(\mathcal{F}) > \operatorname{sign}(v\mathcal{G}),$
	then
	$\mathbf{return} \ (\emptyset, \{\mathcal{F} - v\mathcal{G})\}$
	else
	$\mathbf{return} \ (\emptyset, \{\mathcal{F}, v\mathcal{G} - \mathcal{F})\}$
end	lif
end if	
end	

Next is the main function of Reduction in [8] (function 2).

Deringer

Function 2 — Reduction

Input: a set of labeled polynomials *Todo* which need to be reduced, a set of labeled polynomials *B*.

Output: the reduction results of *Todo* reducing by the set *B*.

begin

```
\begin{array}{c} Done \longleftarrow \emptyset \\ \textbf{while set } Todo \text{ is not empty,} \\ \textbf{do} \\ \qquad \qquad \mathcal{F} \longleftarrow \text{ the labeled polynomial with minimal signature in set } Todo \\ \qquad \qquad Todo \longleftarrow Todo \setminus \{\mathcal{F}\}, \\ \qquad \qquad (Done', Todo') \longleftarrow TopReduction(\mathcal{F}, B, Todo) \\ \qquad \qquad Done \longleftarrow Done \cup Done' \\ \qquad \qquad Todo \longleftarrow Todo \cup Todo' \\ \textbf{end while} \\ \textbf{return } Done \\ \textbf{end} \end{array}
```

We can also write F5-reduction as a function which is similar to the TopReduction (function 3).

Function 3 — F5-Reduction

Input: a labeled polynomial \mathcal{F} , a set of labeled polynomial B.

Output: a 2-tuple (*Done*, *Todo*): both *Done* and *Todo* are sets of lebeled polynomials, while *Done* contains the result of reduction and *Todo* includes the labeled polynomials to be reduced further.

begin

```
 \begin{array}{l} \mathcal{G} \longleftarrow \text{ a labeled polynomial in } B \text{ such that:} \\ 1) \ \operatorname{lpp}(\mathcal{G}) \mid \operatorname{lpp}(\mathcal{F}) \text{ and denote } v = \operatorname{lm}(\mathcal{F})/\operatorname{lm}(\mathcal{G}), \\ 2) \text{ signature } \operatorname{sign}(\mathcal{F}) > \operatorname{sign}(v\mathcal{G}), \\ 3) \ v\mathcal{G} \text{ is not divisible by } B, \text{ and} \\ 4) \ v\mathcal{G} \text{ is not rewritable by } B. \\ \text{if such } \mathcal{G} \text{ does not exist,} \\ \text{ then} \\ \text{ return } (\{\mathcal{F}\}, \emptyset) \\ \text{ else} \\ \text{ return } (\emptyset, \{\mathcal{F} - v\mathcal{G}\} \\ \text{ end if} \end{array}
```

Thus, the F5-reduction can be used to replace the TopReduction function perfectly in the Reduction function by simply updating the following codes:

 $(Done', Todo') \leftarrow F5$ -Reduction (\mathcal{F}, B) .

Next, let us compare TopReduction and F5-reduction. Let $\mathcal{G} \in B$, $v = \operatorname{lm}(\mathcal{F})/\operatorname{lm}(\mathcal{G})$, and <u>Springer</u> suppose $v\mathcal{G}$ is neither divisible nor rewritable by B or R.

1) For the case $\operatorname{sign}(\mathcal{F}) > \operatorname{sign}(v\mathcal{G})$, there is no difference between the TopReduction and F5-reduction.

2) For the case $\operatorname{sign}(\mathcal{F}) = \operatorname{sign}(v\mathcal{G})$:

i) In TopReduction, labeled polynomial $v\mathcal{G}$ is rewritable by $B \cup \{\mathcal{F}\}$. Thus the labeled polynomial \mathcal{G} can never be selected from B, and nothing is done about \mathcal{G} in TopReduction.

ii) In F5-reduction, no matter which labeled polynomial is used to F5-reduce \mathcal{F} , the reduction result of \mathcal{F} has the same signature with \mathcal{F} and will add to the set B. So when discussing the critical pair $[\mathcal{F}, \mathcal{G}]$ in later loops, this critical pair meets the Rewritten Criterion and is hence rejected. Thus no new labeled polynomial is generated.

3) For the case $\operatorname{sign}(\mathcal{F}) < v \operatorname{sign}(\mathcal{G})$:

i) In TopReduction, the labeled polynomial $v\mathcal{G} - \mathcal{F}$ is calculated immediately and added to set *Todo*. Both labeled polynomials \mathcal{F} and $v\mathcal{G}$ will be reduced in later loops of the *Reduction* function. Notice that the labeled polynomial \mathcal{F} may be selected from set *Todo* in later loops, but in that time, the labeled polynomial \mathcal{G} is not qualified to reduce \mathcal{F} , as $v\mathcal{G} - \mathcal{F}$ has been added to the set *Todo* and hence $v\mathcal{G}$ is rewritable by $B \cup \{\mathcal{F}\} \cup Todo$.

ii) While in F5-reduction, we cannot use the labeled polynomial \mathcal{G} to F5-reduce \mathcal{F} immediately. However, in the F5B algorithm, the critical pair $[\mathcal{F}, \mathcal{G}]$ must be added to the set CP, since labeled polynomial \mathcal{G} is in the set B. Moreover, the S-polynomial of the critical pair $[\mathcal{F}, \mathcal{G}]$ is exactly the labeled polynomial $v\mathcal{G} - \mathcal{F}$. The S-polynomial spoly $(\mathcal{F}, \mathcal{G})$ which can also be computed immediately in the next step if we use an appropriate strategy which selects the critical pair $[\mathcal{F}, \mathcal{G}]$ first.

The third case $\operatorname{sign}(\mathcal{F}) < v\operatorname{sign}(\mathcal{G})$ is most complicated, so we illustrate the last case by a simple example.

Example 3 Consider a system in $\mathbb{Q}[x, y, z]$ with the Graded Reverse Lex Order $(x \succ y \succ z)$:

$$\begin{cases} f_1 = xz^2 + y^2, \\ f_2 = xy + xz, \\ f_3 = yz + z. \end{cases}$$

The corresponding labeled polynomials of f_1 , f_2 and f_3 are $\mathcal{F}_1 = (\mathbf{e}_1, f_1)$, $\mathcal{F}_2 = (\mathbf{e}_2, f_2)$ and $\mathcal{F}_3 = (\mathbf{e}_3, f_3)$, respectively. The labeled polynomial set is $B = \{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3\}$. We need to consider the critical pairs $[\mathcal{F}_1, \mathcal{F}_2] = (y, \mathcal{F}_1, z^2, \mathcal{F}_2)$, $[\mathcal{F}_1, \mathcal{F}_3] = (y, \mathcal{F}_1, xz, \mathcal{F}_3)$ and $[\mathcal{F}_2, \mathcal{F}_3] = (z, \mathcal{F}_2, x, \mathcal{F}_3)$.

Since the degree of $\operatorname{lcm}(\operatorname{lpp}(\mathcal{F}_2), \operatorname{lpp}(\mathcal{F}_3)) = xyz$ is 3, which is lower than the other lcm's, we operate the critical pair $[\mathcal{F}_2, \mathcal{F}_3]$ first. Now we can see the major difference between TopReduction and F5-reduction, since there exists a labeled polynomial \mathcal{F}_1 such that $\operatorname{lpp}(\mathcal{F}_1) = xz^2 \mid xz^2 = \operatorname{lpp}(\mathcal{P})$ but signature $\operatorname{sign}(\mathcal{P}) < \operatorname{sign}(\mathcal{F}_1)$.

i) In TopReduction, the labeled polynomial $\mathcal{Q} = \mathcal{F}_1 - \mathcal{P} = (\mathbf{e}_1 - z\mathbf{e}_2 + x\mathbf{e}_3, xz + y^2)$ is calculated. Next, both labeled polynomials \mathcal{P} and \mathcal{Q} add to the set *Todo* for further reductions. In the next loop of the Reduction function, the labeled polynomial $\mathcal{P} = (z\mathbf{e}_2 - x\mathbf{e}_3, xz^2 - xz)$ is irreducible, since the labeled polynomial \mathcal{F}_1 is rewritable by R this time. The labeled polynomial $\mathcal{Q} = (\mathbf{e}_1, xz + y^2)$ is irreducible as well. Then both \mathcal{P} and \mathcal{Q} add to set *Done* and create new critical pairs {[$\mathcal{F}_1, \mathcal{P}$], [$\mathcal{P}, \mathcal{F}_2$], [$\mathcal{P}, \mathcal{F}_3$], [$\mathcal{F}_1, \mathcal{Q}$], [$\mathcal{Q}, \mathcal{F}_2$], [$\mathcal{Q}, \mathcal{F}_3$], [\mathcal{Q}, \mathcal{P}]}. Combined with previous un-operated critical pairs {[$\mathcal{F}_1, \mathcal{F}_2$], [$\mathcal{F}_1, \mathcal{F}_3$], the F5 algorithm continues to operate on these critical pairs.

ii) While in F5-reduction, the labeled polynomial \mathcal{P} is not F5-reducible by set $B = \{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3\}$. So the labeled polynomial \mathcal{P} adds to set B immediately, and creates new critical pairs $\{[\mathcal{F}_1, \mathcal{P}], [\mathcal{P}, \mathcal{F}_2], [\mathcal{P}, \mathcal{F}_3]\}$. Notice that there are still two un-operated critical pairs $\{[\mathcal{F}_1, \mathcal{F}_2], [\mathcal{F}_1, \mathcal{F}_3]\}$. \mathfrak{D} Springer

1226

When using a strategy of selecting critical pairs that selects the critical pair $[\mathcal{F}_1, \mathcal{P}]$ first, the S-polynomial spoly $(\mathcal{F}_1, \mathcal{P}) = \mathcal{F}_1 - \mathcal{P}$ is calculated, and obtain $\mathcal{Q} = \mathcal{F}_1 - \mathcal{P} = (\mathbf{e}_1 - z\mathbf{e}_2 + x\mathbf{e}_3, xz + y^2)$, which is not F5-reducible by set $\{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \mathcal{P}\}$. Then the new critical pairs $\{[\mathcal{F}_1, \mathcal{Q}], [\mathcal{Q}, \mathcal{F}_2], [\mathcal{Q}, \mathcal{F}_3], [\mathcal{Q}, \mathcal{P}]\}$ are created as well.

In both cases, the remaining critical pairs are $\{[\mathcal{P}, \mathcal{F}_2], [\mathcal{P}, \mathcal{F}_3], [\mathcal{F}_1, \mathcal{Q}], [\mathcal{Q}, \mathcal{F}_2], [\mathcal{Q}, \mathcal{F}_3], [\mathcal{Q}, \mathcal{P}], [\mathcal{F}_1, \mathcal{F}_2], [\mathcal{F}_1, \mathcal{F}_3]\}$, since critical pair $[\mathcal{F}_1, \mathcal{P}]$ will be rejected by Rewritten Criterion in TopReduction.

After all, TopReduciton is equivalent to F5-reduction and hence the F5 algorithm is equivalent to the F5B algorithm with an appropriate strategy of selecting critical pairs. However, the F5B algorithm is simpler and easy to understand and analyze. Moreover, by using different strategies (of selecting critical pairs), the F5B algorithm becomes the Incremental F5 algorithm, Non-incremental F5 algorithm and Matrix F5 algorithm which are introduced in the next section.

Since the F5B algorithm is equivalent to the F5 algorithm but much simpler to analyze, we propose a new proof for the correctness of the F5B algorithm in [17]. This new proof does not depend on the strategies of selecting critical pairs, so it also proves the correctness for the other versions of the F5 algorithm. From this new proof, we find that the key of the F5B or F5 algorithm is the special reduction procedure which is a one-way reduction, i.e. only labeled polynomials with lower signatures can be used to reduce labeled polynomials with higher signatures. This fact will be much clearer in the Matrix F5 algorithm introduced later.

5 Some Versions of the F5 Algorithm

In this section, we discuss three versions of the F5 algorithm. They are Incremental F5 algorithm, Non-incremental F5 algorithm and Matrix F5 algorithm.

5.1 Incremental F5 Algorithm

Incremental F5 algorithm is the original F5 algorithm presented in [3]. If the F5B algorithm uses an appropriate strategy of selecting critical pairs, the F5B algorithm becomes the Incremental F5 algorithm.

To describe this strategy appropriately, we need some new notations. For a labeled polynomial $\mathcal{F} = (\mathbf{f}, f)$ whose signature is $\operatorname{sign}(\mathcal{F}) = \operatorname{lpp}(\mathbf{f}) = x^{\alpha} \mathbf{e}_i$, we define the index of \mathcal{F} to be $\operatorname{index}(\mathcal{F}) := i$. Given a critical pair $[\mathcal{F}, \mathcal{G}]$, we also define $\operatorname{index}([\mathcal{F}, \mathcal{G}]) := \min{\operatorname{index}(\mathcal{F}), \operatorname{index}(\mathcal{G})}$. Then the strategy for incremental F5B algorithms can be described as follows:

 $j \leftarrow \max\{\operatorname{index}([\mathcal{F}, \mathcal{G}]) \mid [\mathcal{F}, \mathcal{G}] \in CP\},\$

 $cp \leftarrow$ select a critical pair from CP with index j.

Let us see an easy example. Let $\{f_1, f_2, f_3, f_4\} \subset K[X]$ be the initial polynomials. Then at the beginning, set CP contains all the critical pairs: $[\mathcal{F}_1, \mathcal{F}_2], [\mathcal{F}_1, \mathcal{F}_3], \dots, [\mathcal{F}_3, \mathcal{F}_4]$. By the above strategy, j = 3 at the beginning. So the critical pairs with index 1 or 2 (such as $[\mathcal{F}_2, \mathcal{F}_4]$) cannot be selected unless all the critical pairs with index 3 have been operated. This means the critical pairs with index 1 or 2 can only be operated when the Gröbner basis of ideal $\langle f_3, f_4 \rangle$ is obtained. Similarly, critical pairs with index 1 (such as $[\mathcal{F}_1, \mathcal{F}_3]$) can be selected/operated only when the Gröbner basis of ideal $\langle f_2, f_3, f_4 \rangle$ is computed.

5.2 Non-incremental F5 Algorithm

Faugère also presents a Non-incremental F5 algorithm in a recent conference (INSCRPT 2008). For example, it can use a strategy of selecting critical pairs like

 $d \leftarrow \min\{\deg(\operatorname{lcm}(\operatorname{lpp}(\mathcal{F}), \operatorname{lpp}(\mathcal{G}))) \mid [\mathcal{F}, \mathcal{G}] \in CP\},\$

 $cp \leftarrow$ select a critical pair from CP with degree d.

In this case, for example, the critical pair $[\mathcal{F}_1, \mathcal{F}_3]$ with index 1 may be operated earlier (not necessarily after the Gröbner basis of ideal $\langle f_2, f_3, \cdots, f_m \rangle$ is obtained).

However, this Non-incremental F5 algorithm is not really non-incremental. Since all the critical pairs should be operated sooner or later, the output of algorithm still contains the Gröbner bases of the ideal $\langle f_i, f_{i+1}, \dots, f_m \rangle$ where 1 < i < m. To transform the F5 algorithm to a real non-incremental algorithm, we need to change the order of signatures. This is detailed in [13, 17].

5.3 Matrix F5 Algorithm

The most efficient version of the F5 algorithm is the *Matrix* F5 algorithm, which is an F5 algorithm that utilizes the matrix techniques introduced by the F4 algorithm when reducing S-polynomials. The *Matrix* F5 algorithm improves the original F5 algorithm in data structure, so the *Matrix* F5 algorithm differs from the F5B algorithm only by a strategy of selecting critical pairs as well. Let us see the following example from [3].

Example 4 Consider the homogeneous system in $\mathbb{F}_{23}[x, y, z]$ with the Graded Reverse Lex Order $(x \succ y \succ z)$ by the Matrix F5 algorithm. Here we set parameter b = 0 directly.

$$\begin{cases} f_3 = x^2 + 18xy + 19y^2 + 8xz + 5yz + 7z^2, \\ f_2 = 3x^2 + 7xy + 22xz + 11yz + 22z^2 + 8y^2, \\ f_1 = 6x^2 + 12xy + 4y^2 + 14xz + 9yz + 7z^2. \end{cases}$$

In order to compute the Gröbner basis of $\langle f_1, f_2, f_3 \rangle$, we set $\mathcal{F}_1 = (\mathbf{e}_1, f_1), \mathcal{F}_2 = (\mathbf{e}_2, f_2)$ and $\mathcal{F}_3 = (\mathbf{e}_3, f_3)$. Next consider the critical pairs $[\mathcal{F}_1, \mathcal{F}_2] = (1, \mathcal{F}_1, 1, \mathcal{F}_2), [\mathcal{F}_1, \mathcal{F}_3] = (1, \mathcal{F}_1, 1, \mathcal{F}_3)$ and $[\mathcal{F}_2, \mathcal{F}_3] = (1, \mathcal{F}_2, 1, \mathcal{F}_3)$. Like the F4 algorithm, we use the part $1 \times f_1, 1 \times f_2, 1 \times f_3$ to build the matrix of degree 2 in order to reduce the S-polynomials generated from these three critical pairs together:

$$A_{2} = \begin{array}{c} x^{2} & xy & y^{2} & xz & yz & z^{2} \\ f_{3} & \begin{pmatrix} 1 & 18 & 19 & 8 & 5 & 7 \\ 3 & 7 & 8 & 22 & 11 & 22 \\ 6 & 12 & 4 & 14 & 9 & 7 \end{pmatrix}$$

and after triangulation of the matrix A_2 :

$$B_{2} = \frac{f_{3}}{f_{1}} \begin{pmatrix} x^{2} & xy & y^{2} & xz & yz & z^{2} \\ 1 & \underline{18} & 19 & 8 & 5 & 7 \\ 0 & 1 & 3 & 2 & 4 & -1 \\ 0 & \underline{0} & 1 & -11 & -3 & -5 \end{pmatrix}$$

and two "new" polynomials appear: $f_4 = xy + 4yz + 2xz + 3y^2 - z^2$ ($\mathcal{F}_4 = (-\mathbf{e}_2 + 3\mathbf{e}_3, f_4)$ and $\operatorname{sign}(\mathcal{F}_4) = \mathbf{e}_2$) and $f_5 = y^2 - 11xz - 3yz - 5z^2$ ($\mathcal{F}_5 = (-4\mathbf{e}_1 + 16\mathbf{e}_2 - \mathbf{e}_3, f_5)$ and $\operatorname{sign}(\mathcal{F}_5) = \mathbf{e}_1$), which are the reduction results of the S-polynomials $\operatorname{spoly}(\mathcal{F}_1, \mathcal{F}_2)$, $\operatorname{spoly}(\mathcal{F}_1, \mathcal{F}_3)$ and $\operatorname{spoly}(\mathcal{F}_2, \mathcal{F}_3)$.

Deringer

For simplifying the statement, we will use the signatures of polynomials to replace the signatures of the corresponding labeled polynomials without confusions in the following of this example.

Notice that the signature of the polynomial f_4 is \mathbf{e}_2 , which corresponds to the label on the left of that row (underlined \underline{f}_2 in the matrix B_2).

Also we remark that the underlined <u>18</u> is not reduced by f_4 since the signature of f_3 is \mathbf{e}_3 which is smaller than \mathbf{e}_2 (the signature of f_4). While the underlined <u>0</u> is reduced, since $\mathbf{e}_1 \succ \mathbf{e}_2$. This shows that the reduction procedure in the F5 algorithm is a one-way reduction.

The next step is to consider the newly generated critical pairs: $[\mathcal{F}_1, \mathcal{F}_4] = (y, \mathcal{F}_1, x, \mathcal{F}_4)$, $[\mathcal{F}_4, \mathcal{F}_2] = (x, \mathcal{F}_4, y, \mathcal{F}_2)$, $[\mathcal{F}_4, \mathcal{F}_3] = (x, \mathcal{F}_4, y, \mathcal{F}_3)$, $[\mathcal{F}_5, \mathcal{F}_4] = (x, \mathcal{F}_5, y, \mathcal{F}_4)$, $[\mathcal{F}_5, \mathcal{F}_1] = (x^2, \mathcal{F}_5, y^2, \mathcal{F}_5)$, $[\mathcal{F}_5, \mathcal{F}_2] = (x^2, \mathcal{F}_5, y^2, \mathcal{F}_2)$ and $[\mathcal{F}_5, \mathcal{F}_3] = (x^2, \mathcal{F}_5, y^2, \mathcal{F}_3)$. We select these pairs by degree and build the matrix A_3 of degree 3 in order to operate the following critical pairs together,

$$\begin{split} & [\mathcal{F}_1, \mathcal{F}_4] = (y, \mathcal{F}_1, x, \mathcal{F}_4), \\ & [\mathcal{F}_4, \mathcal{F}_2] = (x, \mathcal{F}_4, y, \mathcal{F}_2), [\mathcal{F}_4, \mathcal{F}_3] = (x, \mathcal{F}_4, y, \mathcal{F}_3), \\ & [\mathcal{F}_5, \mathcal{F}_4] = (x, \mathcal{F}_5, y, \mathcal{F}_4). \end{split}$$

We only need to consider the parts $y \times f_3$, $y \times f_4$, $x \times f_4$, $x \times f_5$, since the parts $y \times f_2$, $y \times f_1$ are rewritable by \mathcal{F}_4 and \mathcal{F}_5 respectively.

Like the F4 algorithm, the parts $y \times f_3$, $y \times f_4$, $x \times f_4$, $x \times f_5$ are the rows to be reduced in the matrix, and we also need to select rows that are use to reduce these rows. Since power products y^3 , x^2z , xyz, y^2z appear in the parts yf_3 , yf_4 , xf_4 , xf_5 , we should add parts yf_5 , xf_3 , zf_4 , zf_5 to matrix A_3 in order to eliminate these power products.

Now we have the matrix A_3 of degree 3. This matrix is ordered by the signatures of each row, which are listed in the round brackets:

and after triangulation (ordered by the leading power products of each row):

and the polynomials $f_6 = y^3 + 8y^z + xz^2 + 18yz^2 + 15z^3$ ($\mathcal{F}_6 = ((15x + 18y + 12z)\mathbf{e}_2 + (x + 7y + 17z)\mathbf{e}_3, f_6)$ and sign(\mathcal{F}_6) = $x\mathbf{e}_2$), $f_7 = xz^2 + 11yz^2 + 13z^3$ ($\mathcal{F}_7 = ((18y + 18z)\mathbf{e}_1 + (10x + 2y)\mathbf{e}_3, f_6)$ Springer

 $9y + 20z)\mathbf{e}_2 + (16x + 13y + 13z)\mathbf{e}_3, f_7)$ and $\operatorname{sign}(\mathcal{F}_7) = y\mathbf{e}_1)$ and $f_8 = yz^2 + 18z^3$ ($\mathcal{F}_8 = ((11x + 11y - 3z)\mathbf{e}_1 + (21y + 9z)\mathbf{e}_2 + (3x + 7y - 3z)\mathbf{e}_3, f_8)$ and $\operatorname{sign}(\mathcal{F}_8) = x\mathbf{e}_1)$ are the reduction results of the S-polynomials of degree 3. Notice that although $\operatorname{lpp}(f_6) = y^3 = y\operatorname{lpp}(f_5)$, labeled polynomial \mathcal{F}_6 is not F5-reducible by \mathcal{F}_5 . Thus f_6 is still a "new" polynomial.

Now the Rewritten Criterion is much clearer. When building the matrix A_3 , we list the signatures of each row in round brackets. Labeled polynomials with the same signatures will play the same role in the matrix, so among the labeled polynomials with the same signatures, it suffices to deal with the latest results (that is why we care about the creating order of labeled polynomials). If we add the row xf_3 (xe_3) to matrix A_3 , replacing the polynomials $zf_4, yf_4, xf_4, zf_5, yf_5, zf_5$ by polynomials $zf_2, yf_2, xf_2, zf_1, yf_1, xf_1$ will lead to the same triangular form B_3 .

Also the one-way reduction is evident in the matrix B_3 . Let us see the row $\underline{xf_4}$ ($\mathbf{xe_2}$). The underlined $\underline{0}$, $\underline{0}$ are reduced by rows zf_3 ($z\mathbf{e}_3$) and zf_4 ($z\mathbf{e}_2$) respectively, while underlined $\underline{8}$, $\underline{1}$, $\underline{18}$ are not eliminated by rows zf_5 ($z\mathbf{e}_1$), $\underline{yf_5}$ ($y\mathbf{e}_1$) and $\underline{xf_5}$ ($x\mathbf{e}_1$). The reason lies in the one-way reduction. More specifically, the signatures of rows zf_3 ($z\mathbf{e}_3$) and zf_4 ($z\mathbf{e}_2$) are $z\mathbf{e}_3$ and $z\mathbf{e}_2$, both of which are smaller than the signature $x\mathbf{e}_2$ of row $\underline{xf_4}$ ($x\mathbf{e}_2$). Thus, the rows zf_3 ($z\mathbf{e}_3$) and zf_4 ($z\mathbf{e}_2$) are able to reduce row $\underline{xf_4}$ ($x\mathbf{e}_2$). However, we have signatures $z\mathbf{e}_1, y\mathbf{e}_1, x\mathbf{e}_1 \succ x\mathbf{e}_2$, so the rows zf_5 ($z\mathbf{e}_1$), $\underline{yf_5}$ ($y\mathbf{e}_1$) and $\underline{xf_5}$ ($x\mathbf{e}_1$) are not qualified to reduce the row $\underline{xf_4}$ ($x\mathbf{e}_2$). Remark that, since only the rows $\underline{xf_4}$ ($x\mathbf{e}_2$), $\underline{yf_5}$ ($y\mathbf{e}_1$) and $\underline{xf_5}$ ($x\mathbf{e}_1$) are worth saving, the others rows are not fully reduced in matrix B_3 .

However, we must realize that, although the two new criteria of the F5 algorithm could reject almost all useless computations, the one-way reduction results in a poorer efficiency of eliminating matrix than the F4 algorithm. So it is really difficult to tell which of the F4 and F5 algorithms is faster the other, especially in large examples.

6 Conclusions

In this paper, we rewrite F5 as F5B in Buchberger's style. We show that the F5B algorithm is equivalent to the original F5 algorithm. It is very easy to understand and implement F5B. The key of the F5B algorithm is the F5-reduction, which is a one-way reduction according to the signatures and their generating orders. F5B is also a useful tool to analyze F5 and F5-like algorithms. Although the F5 algorithm has good theoretical results for avoiding useless computations, the one-way reduction slows down the efficiency of algorithm more or less. It is desirable to have a more careful analysis of this issue, and we hope to work on it in the future.

7 Acknowledgements

We would like to thank S. H. Gao and X. S. Gao for helpful discussions and suggestions.

References

- B. Buchberger, Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, PhD thesis, Innsbruck, 1965.
- J. C. Faugère, A new efficient algorithm for computing Gröbner bases (f4), Journal of Pure and Applied Algebra, 1999, 139(1): 61–88.
- [3] J. C. Faugère, A new efficient algorithm for computing Grönber bases without reduction to zero (F5), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ISSAC'02, 2002.

- [4] R. Gebauer and H. M. Moller, Buchberger's algorithm and staggered linear bases, Proceedings of the 1986 Symposium on Symbolic and Algebraic computation, Waterloo, Ontario, Canada, 1986.
- [5] A. Giovini, T. Mora, G. Niesi, L. Robbiano and C. Traverso, One sugar cube, please, or Selection strategies in the Buchberger Algorithm, S. M. Watt, editor, *Proceedings of the 1991 International* Symposium on Symbolic and Algebraic Computation, ISSAC'91, ACM Press, Bonn, West Germany, 1991.
- [6] D. Lazard, Gaussian elimination and resolution of systems of algebraic equations, Proc. EUROCAL 83, Lect. Notes in Comp. Sci., Springer Verlag, 1983, 162: 146–157.
- T. Mora, H. M. Möller and C. Traverso, Gröbner Bases computation using syzygies, Proceedings of the 1992 International Symposium on Symbolic and Algebraic Computation, ISSAC'92 (ed. by P. S. Wang), ACM Press, Berkeley, California, United States, 1992.
- [8] M. Bardet and J. C. Faugère, B. Salvy, Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over F₂ with solutions in F₂, *Proceedings of International Conference* on Polynomial System Solving Paris, November 24–26, 2004, in honor of Daniel Lazard.
- [9] J. C. Faugère and G. Ars, An Algebraic Cryptanalysis of Nonlinear Filter Generators Using Gröbner Bases, TR No. 4739, INRIA, 2003.
- [10] T. Stegers, Faugère's F5 Algorithm Revisited, Thesis for the degree of Diplom-Mathematiker, 2005.
- [11] C. Eder, On the criteria of the F5 algorithm, ArXiv: 0804.2033v1, 2008.
- [12] C. Eder and J. Perry, F5C: A variant of Faugère's F5 algorithm with reduced Gröbner bases, ArXiv: 0906.2967v5, 2009.
- [13] G. Ars and A. Hashemi, Extended F5 criteria, MEGA, Barcelona, 2009.
- [14] S. H. Gao, Y. H. Guan, and F. Volny, A new incremental algorithm for computing Gröbner Bases, Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ISSAC 10, Munchen, 2010.
- [15] Y. Sun and D. K. Wang, Branch Groebner Bases Algorithm over Boolean Ring (in Chinese), Journal of Systems Science and Mathematical Sciences, 2009, 29(9): 1266–1277.
- [16] Y. Sun and D. K. Wang, The implementation and complexity analysis of the branch Groebner bases algorithm over boolean ring, ASCM 2009 (ed. by M. Suzuki etc.), ISSN 1881-4042, 2009.
- [17] Y. Sun and D. K. Wang, A new proof for the correctness of F5 algorithm, ArXiv: 1004.0084, 2010.
- [18] B. Buchberger, A criterion for detecting unnecessary reductions in the construction of Gröbner basis, Proceedings of EUROCAL 79, Lect. Notes in Comp. Sci., Springer-Verlag, 1979, 72: 3–21.