SCIENCE CHINA
Mathematics

• ARTICLES •

April 2013 Vol. 56 No. 4: 745–756
doi: 10.1007/s11425-012-4480-1

A new proof for the correctness of the F5 algorithm

SUN Yao[1,2] & WANG DingKang[2,*]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190*, China*
Email: sunyao@iie.ac.cn, dwang@mmrc.iss.ac.cn

Received July 22, 2011; accepted April 17, 2012; published online October 19, 2012

Abstract In 2002, Faugère presented the famous F5 algorithm for computing Gröbner basis where two criteria, syzygy criterion and rewritten criterion, were proposed to avoid redundant computations. He proved the correctness of the syzygy criterion, but the proof for the correctness of the rewritten criterion was left. Since then, F5 has been studied extensively. Some proofs for the correctness of F5 were proposed, but these proofs are valid only under some extra assumptions. In this paper, we give a proof for the correctness of F5B, an equivalent version of F5 in Buchberger's style. The proof is valid for both homogeneous and non-homogeneous polynomial systems. Since this proof does not depend on the computing order of the S-pairs, any strategy of selecting S-pairs could be used in F5B or F5. Furthermore, we propose a natural and non-incremental variant of F5 where two revised criteria can be used to remove almost all redundant S-pairs.

Keywords Gröbner basis, F5, F5B, correctness of F5

MSC(2010) 13B25, 13N10, 13P10

Citation: Sun Y, Wang D K. A new proof for the correctness of the F5 algorithm. Sci China Math, 2013, 56: 745–756, doi: 10.1007/s11425-012-4480-1

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, Gröbner basis is one of the most efficient approaches. Since Gröbner basis was proposed in 1965 in [3], many algorithms and improvements have been presented for computing Gröbner basis, including [4, 8, 9, 13, 14, 17, 18]. Currently, F5 is one of the most efficient algorithms.

Since the F5 algorithm was proposed, it has been widely investigated. For example, Bardet et al. [1] studied the complexity of this algorithm. Faugère and Ars [10] used the F5 algorithm to attack multivariable systems. Stegers [25] revisited the F5 algorithm in his master thesis. Eder discussed the two criteria of the F5 algorithm in [5] and proposed a variant of the F5 algorithm in [6]. Hashemi and Ars [15] presented two variants of criteria. Gao et al. gave a new algorithm to compute Gröbner basis in [11, 12]. The current authors discussed the F5 algorithm over Boolean ring and presented a branch F5 algorithm in [19, 20]. We also discussed the F5 algorithm in Buchberger's style in [21]. Recently, criteria and some other variants of F5 have been studied in [7, 16, 22–24, 26].

Currently, available proofs for the correctness of the F5 algorithm can be found in [5, 6, 9, 25]. However, these proofs are somewhat not as general as possible, particularly for non-homogeneous systems.

*Corresponding author

The main purpose of the current paper is to present a proof for the correctness of the F5 algorithm. As we have shown in [21] that F5B, the F5 algorithm in Buchberger's style, is equivalent to the original F5 algorithm, and F5B may deduce various F5-like algorithms. Therefore, we will focus on proving the correctness of the F5B algorithm in this paper. The proposed new proof is **not** limited to homogeneous systems and does **not** depend on the strategy of selecting S-pairs, so the correctness of all the variants of the F5 algorithm mentioned in [21] can be proved at the same time. The correctness of the variant of the F5 algorithm in [15], which is quite similar to the variant of the F5 algorithm in this paper, can also be proved by a slight modification.

Meanwhile, according to the new proposed proof, we find that F5-reduction plays a key role in the F5 and F5-like algorithms. F5-reduction, which is a one-direction reduction process, ensures the correctness of syzygy criterion and rewritten criterion in F5. Many variants of the F5 algorithm become available whenever maintaining the one-direction reduction. We also propose a non-incremental variant of the F5 algorithm. This variant can avoid computing Gröbner basis incrementally such that the Gröbner bases for subsets of input polynomials are not necessarily computed. Besides, the two revised criteria in this variant are able to remove almost all unnecessary reductions as shown in the experimental data.

This paper is organized as follows. We revisit the F5B algorithm after introducing some basic notations in Section 2. Some results on labeled polynomias are given in Section 3. The complete proof for the correctness of the F5B algorithm is presented in Section 4. A non-incremental variant of F5 is proposed in Section 5. This paper is concluded in Section 6.

2 Basic notation

Let K be a field and $R = K[x_1, \ldots, x_n]$ 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 $\{x_1, \ldots, x_n\}$, i.e., $PP(X) := \{x^\alpha \mid x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \alpha_i \in \mathbb{N}, i = 1, \ldots, n\}$.

Let $\succ$ 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 $0 \neq f \in K[x_1, \ldots, x_n]$, 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 $\mathrm{lpp}(f) := \max_\succ\{x^\alpha : c_\alpha \neq 0\}$. If $\mathrm{lpp}(f) = x^\alpha$, then the leading coefficient and leading monomial of f are defined to be $\mathrm{lc}(f) := c_\alpha$ and $\mathrm{lm}(f) := c_\alpha x^\alpha$ respectively.

Consider a polynomial system $\{w_1, \ldots, w_m\} \subset \mathbb{R}$ and $(w_1, \ldots, w_m)$ a polynomial m-tuple in $\mathbb{R}^m$. We call the w_i's initial polynomials, as they are initial generators of the ideal $\langle w_1, \ldots, w_m\rangle \subset \mathbb{R}$.

Let $\mathbf{e}_i$ be the canonical i-th unit vector in $\mathbb{R}^m$, 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 module $\mathbb{R}^m$:

$$\begin{aligned}&\sigma : \mathbb{R}^m \longrightarrow \langle w_1, \ldots, w_m\rangle,\\ &(f_1, \ldots, f_m) \longmapsto f_1 w_1 + \cdots + f_m w_m.\end{aligned}$$

Then $\sigma(\mathbf{e}_i) = w_i$. More generally, if $\mathbf{f} = f_1\mathbf{e}_1 + \cdots + f_m\mathbf{e}_m$, where $f_i \in \mathbb{R}$ for $1 \leqslant i \leqslant m$, then $\sigma(\mathbf{f}) = f_1 w_1 + \cdots + f_m w_m$.

The admissible order $\succ$ on $PP(X)$ extends to the free module $\mathbb{R}^m$ naturally in a POT (position over term) fashion.

$$x^\alpha\mathbf{e}_i \succ x^\beta\mathbf{e}_j \text{ iff } \begin{cases} i < j,\\ \text{ or}\\ i = j \text{ and } x^\alpha \succ x^\beta.\end{cases}$$

Thus we have $\mathbf{e}_1 \succ \mathbf{e}_2 \succ \cdots \succ \mathbf{e}_m$.

This order was introduced by Faugère [9]. We will introduce another order of signatures to deduce a natural variant of the F5 algorithm.

With the admissible order on $\mathbb{R}^m$, we can define the leading power product, leading coefficient and leading monomial of an m-tuple vector $\mathbf{f} \in \mathbb{R}^m$ in a similar way. For example, let

$$\mathbf{f} = (2x^2 + y^2, 3xy) \in (\mathbb{Q}[x, y])^2$$

or equivalently $\mathbf{f} = (2x^2 + y^2)\mathbf{e}_1 + 3xy\mathbf{e}_2$. According to the Lex order $\succ$ on $PP(x, y)$ where $x \succ y$, we have $\mathrm{lpp}(\mathbf{f}) = x^2\mathbf{e}_1$, $\mathrm{lc}(\mathbf{f}) = 2$ and $\mathrm{lm}(\mathbf{f}) = 2x^2\mathbf{e}_1$.

The following are the definitions of labeled polynomial and its signature.

Definition 2.1. Let $f \in \langle w_1, \ldots, w_m\rangle$ be a polynomial and $\mathbf{f} \in \mathbb{R}^m$ an m-tuple vector such that $\sigma(\mathbf{f}) = f$, then we call $\mathcal{F} = (\mathbf{f}, f)$ a labeled polynomial. For a labeled polynomial $\mathcal{F}$, we define

1. the signature $\mathrm{sign}(\mathcal{F}) := \mathrm{lpp}(\mathbf{f})$, and
2. the polynomial part $\mathrm{poly}(\mathcal{F}) := f$.

Suppose $\mathcal{F} = (\mathbf{f}, f)$ and $\mathcal{G} = (\mathbf{g}, g)$ are labeled polynomials and u is a non-zero monomial. We define scaler multiplication and addition for labeled polynomials as follows,

$$u \cdot \mathcal{F} = u\mathcal{F} = (u\mathbf{f}, uf), \quad \mathcal{F} + \mathcal{G} = (\mathbf{f} + \mathbf{g}, f + g).$$

Let B be a list of labeled polynomials and $\mathcal{F}$ be an element in B. The *index* of $\mathcal{F}$ w.r.t B is defined to be the location of $\mathcal{F}$ in B, denoted by $\mathrm{index}(\mathcal{F}, B)$. For example, if $B = [\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_m]$, then $\mathrm{index}(\mathcal{F}_i, B) = i$.

Let B be a list of labeled polynomials, p, q be two polynomials in R and $\mathcal{F}, \mathcal{G}$ be two labeled polynomials in B, we define $(p, \mathcal{F}) \succ (q, \mathcal{G})$ (or $p\mathcal{F} \succ q\mathcal{G}$) if either $\mathrm{sign}(p\mathcal{F}) \succ \mathrm{sign}(q\mathcal{G})$, or $\mathrm{sign}(p\mathcal{F}) = \mathrm{sign}(q\mathcal{G})$ and $\mathrm{index}(\mathcal{F}, B) < \mathrm{index}(\mathcal{G}, B)$.

We also can define S-pairs and S-polynomials of labeled polynomials.

Definition 2.2. Let B be a list of labeled polynomials, $\mathcal{F}, \mathcal{G}$ be two labeled polynomials in B, $[\mathcal{F}, \mathcal{G}] := (u, \mathcal{F}, v, \mathcal{G})$ is called an S-pair of $\mathcal{F}$ and $\mathcal{G}$ if

$$u = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathrm{poly}(\mathcal{F})), \mathrm{lpp}(\mathrm{poly}(\mathcal{G})))}{\mathrm{lm}(\mathrm{poly}(\mathcal{F}))} \quad \text{and} \quad v = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathrm{poly}(\mathcal{F})), \mathrm{lpp}(\mathrm{poly}(\mathcal{G})))}{\mathrm{lm}(\mathrm{poly}(\mathcal{G}))}.$$

The corresponding S-polynomial of $[\mathcal{F}, \mathcal{G}]$ is denoted by $\mathrm{spoly}(\mathcal{F}, \mathcal{G}) := u\mathcal{F} - v\mathcal{G}$.

Let $\mathcal{F}$, $\mathcal{G}$ be two different labeled polynomials in B, for the S-pair $[\mathcal{F}, \mathcal{G}] = (u, \mathcal{F}, v, \mathcal{G})$, we always assume $u\mathcal{F} \succ v\mathcal{G}$.

For two S-pairs, $[F, G] = (u, \mathcal{F}, v, \mathcal{G})$ and $[F', G'] = (u', \mathcal{F}', v', \mathcal{G}')$, we define $[F, G] \succ [F', G']$ if one of the following two conditions holds,

1. $u\mathcal{F} \succ u'\mathcal{F}'$.
2. $u\mathcal{F} = u'\mathcal{F}'$ and $v\mathcal{G} \succ v'\mathcal{G}'$.

Before giving the algorithm F5B, we still need several definitions: F5-divisible, F5-rewritable and F5-reducible.

Definition 2.3 (F5-divisible, Syzygy criterion)**.** Let B be a list of labeled polynomials, u a monomial and $\mathcal{F}$ a labeled polynomial with $\mathrm{sign}(\mathcal{F}) = x^\alpha\mathbf{e}_i$ in B. A pair $(u, \mathcal{F})$ is said to be F5-divisible by B, if there exists a labeled polynomial $\mathcal{G}$ with $\mathrm{sign}(\mathcal{G}) = x^\beta\mathbf{e}_j$ in B such that

1. $\mathrm{lpp}(\mathrm{poly}(\mathcal{G})) \mid ux^\alpha$, and
2. $i < j$.

Definition 2.4 (F5-rewritable, Rewritten criterion)**.** Let B be a list of labeled polynomials, u a monomial and $\mathcal{F}$ a labeled polynomial in B. A pair $(u, \mathcal{F})$ is said to be F5-rewritable by B, if there exists a labeled polynomial $\mathcal{G}$ in B such that $\mathrm{sign}(\mathcal{G}) \mid \mathrm{sign}(u\mathcal{F})$ and $\mathrm{index}(\mathcal{F}, B) < \mathrm{index}(\mathcal{G}, B)$.

An S-pair $[\mathcal{F}, \mathcal{G}] = (u, \mathcal{F}, v, \mathcal{G})$ is said to be F5-divisible/F5-rewritable by B if $(u, \mathcal{F})$ or $(v, \mathcal{G})$ is F5-divisible/F5-rewritable by B.

The concept of signatures itself is not sufficient to ensure the correctness of the above two new criteria. It is the F5-reduction procedure that guarantees the S-pairs detected by criteria are really useless. The same is true for other F5-like algorithms. Let us give the definition of F5-reduction.

Definition 2.5 (F5-reducible)**.** Let $\mathcal{F} = (\mathbf{f}, f)$ be a labeled polynomial and B a list of labeled polynomials. $\mathcal{F}$ is said to be F5-reducible by B if there exists $\mathcal{G} = (\mathbf{g}, g)$ in B such that

1. $\mathrm{lpp}(g) \mid \mathrm{lpp}(f)$, denote $u = \mathrm{lpp}(f)/\mathrm{lpp}(g)$ and $c = \mathrm{lc}(f)/\mathrm{lc}(g)$,
2. $\mathrm{sign}(\mathcal{F}) \succ \mathrm{sign}(u\mathcal{G})$, and
3. $(u, \mathcal{G})$ is neither F5-divisible nor F5-rewritable by B.

If $\mathcal{F}$ is F5-reducible by B, let $\mathcal{F}' = \mathcal{F} - cu\mathcal{G}$. 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 it is not F5-reducible by B any more. We denote the final $\mathcal{F}'$ as $\mathcal{F}^*$, i.e. $\mathcal{F} \Longrightarrow_B^* \mathcal{F}^*$.

Remark. Condition 3 does not affect the correctness of the F5 or F5B algorithm. It only makes the algorithm more efficient by avoiding some redundant computations/reductions.

The condition 2 implies that $\mathcal{F}$ and $\mathcal{F}^*$ should have same signatures, and this property plays a crucial role in the main proof for the correctness of F5B. For convenience of reference, we describe this property by the following proposition.

Proposition 2.6 (F5-reduction property)**.** *If labeled polynomial $\mathcal{F} = (\mathbf{f}, f)$ is* F5*-reduced to $\mathcal{F}^*$ by B, i.e., $\mathcal{F} \Longrightarrow_B^* \mathcal{F}^*$, then there exist polynomials $p_1, \ldots, p_s$ and labeled polynomials $\mathcal{G}_1 = (\mathbf{g}_1, g_1), \ldots, \mathcal{G}_s = (\mathbf{g}_s, g_s)$ in B such that*

$$\mathcal{F} = \mathcal{F}^* + p_1\mathcal{G}_1 + \cdots + p_s\mathcal{G}_s,$$

where $\mathrm{lpp}(\mathrm{poly}(\mathcal{F})) \succeq \mathrm{lpp}(p_i\mathrm{poly}(\mathcal{G}_i))$ *and* $\mathrm{lpp}(\mathbf{f}) \succ \mathrm{lpp}(p_i\mathbf{g}_i)$ *for* $1 \leqslant i \leqslant s$. *Moreover,* $\mathrm{sign}(\mathcal{F}) = \mathrm{sign}(\mathcal{F}^*)$.

With the definitions of F5-divisible, F5-rewrittable and F5-reducible, we can simplify the F5 algorithm in Buchberger's style — F5B as following. We have shown that F5B algorithm is equivalent to the original F5 algorithm in [21].

The F5 algorithm in Buchberger's style (F5B)

Input: a polynomial set $\{w_1, \ldots, w_m\} \subset R$, and an admissible order $\succ$ for the power products in R.

Output: A Gröbner basis of the ideal $\langle w_1, \ldots, w_m\rangle \subset R$ w.r.t. the order $\succ$.

begin

$\mathcal{F}_i \longleftarrow (\mathbf{e}_i, w_i)$ for $i = 1, \ldots, m$
$B \longleftarrow [\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_m]$
RedundantSPairs$\longleftarrow \emptyset$
Todo$\longleftarrow$ {S-pair $[\mathcal{F}_i, \mathcal{F}_j] \mid 1 \leqslant i < j \leqslant m$}
while *Todo* $\neq \emptyset$ **do**
  $[\mathcal{F}, \mathcal{G}] \longleftarrow$ select an S-pair from *Todo*
  Todo $\longleftarrow$ *Todo* $\setminus$ $\{[\mathcal{F}, \mathcal{G}]\}$
  if $[\mathcal{F}, \mathcal{G}]$ is **either** F5-Divisible **or** F5-Rewritable
    then
      RedundantSPairs$\longleftarrow$ RedundantSPairs$\cup\{[\mathcal{F}, \mathcal{G}]\}$
    else
      $\mathcal{P} \longleftarrow$F5-reduction(spoly$(\mathcal{F}, \mathcal{G}), B)$
      # spoly$(\mathcal{F}, \mathcal{G}) \Longrightarrow_B^* \mathcal{P}$
      if poly$(\mathcal{P}) \neq 0$
        then
          Todo$\longleftarrow$ *Todo* $\cup$ $\{[\mathcal{P}, \mathcal{Q}] \mid \mathcal{Q} \in B\}$
      end if
      # no matter whether poly$(\mathcal{P}) \neq 0$
      $B \longleftarrow$ append $\mathcal{P}$ to the **end** of B

end if
end while
return $\{\text{poly}(\mathcal{Q}) \mid \mathcal{Q} \in B\}$
end

Notice that B is a list which records all the labeled polynomials generated during the computation. According to the above algorithm, the *index* of $\mathcal{P}$ w.r.t. B is its position in B. The bigger index$(\mathcal{P}, B)$ is, the later $\mathcal{P}$ is generated. Notice that the indexes of the labeled polynomials in B are distinct from each other.

Notice that *Todo* records all the generated S-pairs during the computation which remain to be treated. We have shown in [21] that the only difference between F5 and F5B is that the original F5 algorithm always selects a minimal S-pair for some order to compute from the set *Todo* while F5B does not specify any computing order for the S-pairs. In fact, it is not necessary to specify any strategy of selecting S-pair. This is because our proof given in this paper for the correctness of F5B does not depend on the computing order of the S-pairs. Obviously, the proof for F5B is still valid for F5. In the following of this paper, we focus on proving the correctness of the F5B algorithm.

3 Some results on labeled polynomials

In this section, we will introduce the concepts of t-representation and strict lower representation for labeled polynomials.

We start this section by introducing the concept of t-representation for labeled polynomials.

Definition 3.1 (t-representation)**.** Let B be a list of labeled polynomials, $\mathcal{F}, \mathcal{G}$ labeled polynomials in B and t a power product. We say the S-pair $[\mathcal{F}, \mathcal{G}] = (u, \mathcal{F}, v, \mathcal{G})$ has a t-representation w.r.t. B, if there exist polynomials $p_1, \ldots, p_s$ and labeled polynomials $\mathcal{G}_1, \ldots, \mathcal{G}_s$ in B such that

$$\text{poly}(\text{spoly}(\mathcal{F}, \mathcal{G})) = p_1\text{poly}(\mathcal{G}_1) + \cdots + p_s\text{poly}(\mathcal{G}_s),$$

where $u\mathcal{F} \succeq p_i\mathcal{G}_i$ and $t = \text{lpp}(u\text{poly}(\mathcal{F})) = \text{lpp}(v\text{poly}(\mathcal{G})) \succ \text{lpp}(p_i\text{poly}(\mathcal{G}_i))$ for $i = 1, \ldots, s$.

The following theorem is the main result on t-representation for labeled polynomials. Its proof is straight from its polynomial version, so we omit the detailed proof here. The interested readers are referred to [2].

Theorem 3.2. *Let B be a list of labeled polynomials. The polynomial set $\{\text{poly}(\mathcal{P}) \mid \mathcal{P} \in B\}$ is a Gröbner basis if for any two labeled polynomials $\mathcal{F}, \mathcal{G} \in B$, the S-pair $[\mathcal{F}, \mathcal{G}]$ has a t-representation w.r.t. B.*

Definition 3.3 (Strictly lower representation)**.** Let B be a list of labeled polynomials, u a monomial and $\mathcal{F}$ a labeled polynomial in B. Then a pair $(u, \mathcal{F})$ has a strictly lower representation w.r.t. B, if there exist polynomials $p_1, \ldots, p_s$ and labeled polynomials $\mathcal{G}_1, \ldots, \mathcal{G}_s \in B$, such that

$$u\text{poly}(\mathcal{F}) = p_1\text{poly}(\mathcal{G}_1) + \cdots + p_s\text{poly}(\mathcal{G}_s),$$

where $u\mathcal{F} \succ p_i\mathcal{G}_i$ for $i = 1, \ldots, s$.

The following key lemma builds a relation between *strictly lower representation* and *t-representation*.

Lemma 3.4. *Let B be a list of labeled polynomials, u a monomial, $\mathcal{F}$ a labeled polynomial in B. If*

1. *$(u, \mathcal{F})$ has a strictly lower representation w.r.t. B,*
2. *for each S-pair $[\mathcal{F}', \mathcal{G}'] = (u', \mathcal{F}', v', \mathcal{G}')$ where $\mathcal{F}', \mathcal{G}'$ in B, if $u\mathcal{F} \succ u'\mathcal{F}'$, then $[\mathcal{F}', \mathcal{G}']$ has a t-representation w.r.t. B,*

then there exist polynomials $p_1, \ldots, p_s$ and labeled polynomials $\mathcal{G}_1, \ldots, \mathcal{G}_s$ in B such that

$$u\text{poly}(\mathcal{F}) = p_1\text{poly}(\mathcal{G}_1) + \cdots + p_s\text{poly}(\mathcal{G}_s),$$

where $u\mathcal{F} \succ p_i\mathcal{G}_i$ *and* $\mathrm{lpp}(u\mathrm{poly}(\mathcal{F})) \succeq \mathrm{lpp}(p_i\mathrm{poly}(\mathcal{G}_i))$. *Hence, there exists a labeled polynomial* $\mathcal{H} = \mathcal{G}_i$ *for some* i *such that* $\mathrm{lpp}(\mathrm{poly}(\mathcal{H})) \mid \mathrm{lpp}(u\mathrm{poly}(\mathcal{F}))$ *and* $u\mathcal{F} \succ v\mathcal{H}$, *where* $v = \mathrm{lpp}(u\mathrm{poly}(\mathcal{F}))/\mathrm{lpp}(\mathcal{H})$.

Proof. Since $(u, \mathcal{F})$ has a strictly lower representation w.r.t. B, by the definition of strictly lower representation, there exist polynomials $p_1, \ldots, p_s$ in R and labeled polynomials $\mathcal{G}_1, \ldots, \mathcal{G}_s$ in B, such that: $u\mathrm{poly}(\mathcal{F}) = p_1\mathrm{poly}(\mathcal{G}_1) + \cdots + p_s\mathrm{poly}(\mathcal{G}_s)$, where $u\mathcal{F} \succ p_i\mathcal{G}_i$ for $i = 1, \ldots, s$.

Let

$$x^\delta = \max\nolimits_\succ\{\mathrm{lpp}(p_1\mathrm{poly}(\mathcal{G}_1)), \ldots, \mathrm{lpp}(p_s\mathrm{poly}(\mathcal{G}_s))\},$$

so $\mathrm{lpp}(u\mathrm{poly}(\mathcal{F})) \preceq x^\delta$ always holds. Now consider all possible strictly lower representations of $(u, \mathcal{F})$ w.r.t. B. For each such expression, we get a possibly different x^δ. Since a term order is well-ordering, we can select a strictly lower representation of $\mathcal{F}$ w.r.t. B such that power product x^δ is minimal. Assume this strictly lower representation is

$$u\mathrm{poly}(\mathcal{F}) = p_1\mathrm{poly}(\mathcal{G}_1) + \cdots + p_s\mathrm{poly}(\mathcal{G}_s), \tag{3.1}$$

where $p_i \in \mathbb{R}$, $\mathcal{G}_i \in B$ and $u\mathcal{F} \succ p_i\mathcal{G}_i$ for $i = 1, \ldots, s$. We will show that once the minimal x^δ is chosen, we have $\mathrm{lpp}(u\mathrm{poly}(\mathcal{F})) = x^\delta$ and hence the lemma is proved. We prove this by contradiction.

Equality fails only when $\mathrm{lpp}(u\mathrm{poly}(\mathcal{F})) \prec x^\delta$. Denote $\mathrm{m}(i) = \mathrm{lpp}(p_i\mathrm{poly}(\mathcal{G}_i))$, and then we can rewrite $u\mathrm{poly}(\mathcal{F})$ in the following form:

$$\begin{aligned} u\mathrm{poly}(\mathcal{F}) &= \sum_{\mathrm{m}(i)=x^\delta} p_i\mathrm{poly}(\mathcal{G}_i) + \sum_{\mathrm{m}(i)\prec x^\delta} p_i\mathrm{poly}(\mathcal{G}_i) \\ &= \sum_{\mathrm{m}(i)=x^\delta} \mathrm{lm}(p_i)\mathrm{poly}(\mathcal{G}_i) + \sum_{\mathrm{m}(i)=x^\delta} (p_i - \mathrm{lm}(p_i))\mathrm{poly}(\mathcal{G}_i) \\ &\quad + \sum_{\mathrm{m}(i)\prec x^\delta} p_i\mathrm{poly}(\mathcal{G}_i). \end{aligned} \tag{3.2}$$

The power products appearing in the second and third sums above are all less than x^δ. Thus, the assumption $\mathrm{lpp}(u\mathrm{poly}(\mathcal{F})) \prec x^\delta$ means that power products in the first sum are also less than x^δ. So the first sum must be a combination of S-polynomials, i.e.,

$$\sum_{\mathrm{m}(i)=x^\delta} \mathrm{lm}(p_i)\mathrm{poly}(\mathcal{G}_i) = \sum_{j,k} w_{jk}\mathrm{poly}(\mathrm{spoly}(\mathcal{G}_j, \mathcal{G}_k)), \tag{3.3}$$

where w_{jk}'s are monomials in R. For each S-pair $[\mathcal{G}_j, \mathcal{G}_k] = (u_{jk}, \mathcal{G}_j, v_{jk}, \mathcal{G}_k)$, we have $u\mathcal{F} \succ w_{jk}u_{jk}\mathcal{G}_j \succ w_{jk}v_{jk}\mathcal{G}_k$ for each j, k, since expression (3.1) is a strictly lower representation of $(u, \mathcal{F})$. And hence, by the hypothesis, each S-pair $[\mathcal{G}_j, \mathcal{G}_k]$ has a t-representation, i.e., there exist polynomials $g_1, \ldots, g_r \in \mathbb{R}$ and labeled polynomials $\mathcal{R}_1, \ldots, \mathcal{R}_r \in B$, such that

$$\mathrm{poly}(\mathrm{spoly}(\mathcal{G}_j, \mathcal{G}_k)) = g_1\mathrm{poly}(\mathcal{R}_1) + \cdots + g_r\mathrm{poly}(\mathcal{R}_r),$$

where $u_{jk}\mathcal{G}_j \succ g_i\mathcal{R}_i$ and

$$\mathrm{lcm}(\mathrm{lpp}(u_{jk}\mathrm{poly}(\mathcal{G}_j)), \mathrm{lpp}(v_{jk}\mathrm{poly}(\mathcal{G}_k))) \succ \mathrm{lpp}(g_i\mathrm{poly}(\mathcal{R}_i))$$

for $i = 1, \ldots, r$.

Substitute the above representations back into the equation (3.3) and hence into the equation (3.2). All the power products in the new expression of (3.2) will be less than x^δ. Then a new strictly lower representation of $(u, \mathcal{F})$ w.r.t. B appears with all power products less than x^δ, which contradicts with the minimality of x^δ. So we must have $\mathrm{lpp}(u\mathrm{poly}(\mathcal{F})) = x^\delta$. The lemma is proved. □

The following proposition provides a criterion to detect if an S-pair has a t-representation.

Proposition 3.5. *Let B be a list of labeled polynomials, $\mathcal{F},\mathcal{G}$ be labeled polynomials in B. Then S-pair $[\mathcal{F},\mathcal{G}]=(u,\mathcal{F},v,\mathcal{G})$ has a t-representation w.r.t. B, if*

1. *$(u,\mathcal{F})$ or $(v,\mathcal{G})$ has a strictly lower representation w.r.t. B, and*
2. *for each S-pair $[\mathcal{F}',\mathcal{G}']=(u',\mathcal{F}',v',\mathcal{G}')$ where $\mathcal{F}',\mathcal{G}'$ in B, if $[\mathcal{F}',\mathcal{G}']\prec[\mathcal{F},\mathcal{G}]$, then $[\mathcal{F}',\mathcal{G}']$ has a t-representation w.r.t. B.*

Proof. (1) First, we assume that $(u,\mathcal{F})$ has a strictly lower representation w.r.t. B. Then there exist polynomials $p_1,\ldots,p_s\in\mathbb{R}$ and labeled polynomials $\mathcal{G}_1,\ldots,\mathcal{G}_r\in B$, such that

$$\mathrm{poly}(u\mathcal{F})=p_1\mathrm{poly}(\mathcal{G}_1)+\cdots+p_r\mathrm{poly}(\mathcal{G}_r),$$

where $u\mathcal{F}\succ p_i\mathcal{G}_i$ for $i=1,\ldots,r$. Since $[\mathcal{F},\mathcal{G}]=(u,\mathcal{F},v,\mathcal{G})$ is an S-pair, we have $u\mathcal{F}\succ v\mathcal{G}$. Hence

$$\begin{aligned}\mathrm{poly}(u\mathcal{F}-v\mathcal{G})&=\mathrm{poly}(u\mathcal{F})-\mathrm{poly}(v\mathcal{G})\\&=p_1\mathrm{poly}(\mathcal{G}_1)+\cdots+p_r\mathrm{poly}(\mathcal{G}_r)-v\mathrm{poly}(\mathcal{G}).\end{aligned}$$

With the same proving method as the one used in Lemma 3.4, we can prove that the S-pair $[\mathcal{F},\mathcal{G}]$ has a t-representation, where

$$t=\mathrm{lcm}(\mathrm{lpp}(\mathrm{poly}(\mathcal{F})),\mathrm{lpp}(\mathrm{poly}(\mathcal{G})))\succ\mathrm{lpp}(\mathrm{poly}(\mathrm{spoly}(\mathcal{F},\mathcal{G}))).$$

(2) Second, we assume that $(v,\mathcal{G})$ has a strictly lower representation. For each S-pair $[\mathcal{F}',\mathcal{G}']=(u',\mathcal{F}',v',\mathcal{G}')$, if $u'\mathcal{F}'\prec v\mathcal{G}$, then $u'\mathcal{F}'\prec u\mathcal{F}$ since $v\mathcal{G}\prec u\mathcal{F}$. The hypothesis implies that $[\mathcal{F}',\mathcal{G}']$ has a t-representation w.r.t. B. By the key lemma, we know that there exists a labeled polynomial $\mathcal{H}\in B$ such that $\mathrm{lpp}(\mathrm{poly}(\mathcal{H}))\mid\mathrm{lpp}(v\mathrm{poly}(\mathcal{G}))$ and $v\mathcal{G}\succ w\mathcal{H}$, where $w=\mathrm{lm}(u\mathrm{poly}(\mathcal{F}))/\mathrm{lm}(\mathrm{poly}(\mathcal{H}))$.

Notice that $\mathrm{lpp}(u\mathrm{poly}(\mathcal{F}))=\mathrm{lpp}(v\mathrm{poly}(\mathcal{G}))=\mathrm{lpp}(w\mathrm{poly}(\mathcal{H}))$ and $u\mathcal{F}\succ v\mathcal{G}\succ w\mathcal{H}$.

$$\begin{aligned}\mathrm{poly}(\mathrm{spoly}(\mathcal{F},\mathcal{G}))&=u\mathrm{poly}(\mathcal{F})-v\mathrm{poly}(\mathcal{G})\\&=(u\mathrm{poly}(\mathcal{F})-w\mathrm{poly}(\mathcal{H}))-(v\mathrm{poly}(\mathcal{G})-w\mathrm{poly}(\mathcal{H}))\\&=\gcd(u,w)\mathrm{poly}(\mathrm{spoly}(\mathcal{F},\mathcal{H}))-\gcd(v,w)\mathrm{poly}(\mathrm{spoly}(\mathcal{G},\mathcal{H})).\end{aligned}$$

Since $[\mathcal{F},\mathcal{G}]\succ[\mathcal{F},\mathcal{H}]$ and $[\mathcal{F},\mathcal{G}]\succ[\mathcal{G},\mathcal{H}]$, both $[\mathcal{F},\mathcal{H}]$ and $[\mathcal{G},\mathcal{H}]$ should have a t-representation. Hence $[\mathcal{F},\mathcal{G}]$ also has a t-representation, where $t\prec\mathrm{lcm}(\mathrm{lpp}(\mathrm{poly}(\mathcal{F})),\mathrm{lpp}(\mathrm{poly}(\mathcal{H})))$. □

4 A proof for the correctness of F5B

For an ideal $I=\langle w_1,\ldots,w_m\rangle$ in $\mathbb{R}$, F5 or F5B computes the Gröbner basis of I. The following propositions show that if a labeled polynomial is either F5-*divisible* or F5-*rewritable* by B, then this labeled polynomial has a *strictly lower representation* w.r.t. B.

Proposition 4.1. *Suppose that B is a list of labeled polynomials and every $\mathcal{F}_i$ is an element of B where $\mathcal{F}_i=(\mathbf{e}_i,w_i)$ for $i=1,\ldots,m$. Let u be a monomial and $\mathcal{F}$ be a labeled polynomial in B. If $(u,\mathcal{F})$ is* **F5-divisible** *by B, then $(u,\mathcal{F})$ has a strictly lower representation w.r.t. B.*

Proof. Suppose $\mathcal{F}=(\mathbf{f},f)$ and $\mathrm{lm}(\mathbf{f})=cx^\alpha\mathbf{e}_i$, since $(u,\mathcal{F})$ is F5-divisible by B, then there exists $\mathcal{G}=(\mathbf{g},g)$ in B such that $\mathrm{sign}(\mathcal{G})=\mathrm{lpp}(\mathbf{g})\mathbf{e}_j$ with $i<j$ and $\mathrm{lm}(g)$ divides ux^α, i.e., there exists a monomial v such that $cux^\alpha=v\mathrm{lm}(g)$. Suppose $\mathbf{w}=(w_1,\ldots,w_m)$. We have $\mathbf{e}_i\cdot\mathbf{w}=w_i$. Then

$$\begin{aligned}\mathrm{poly}(u\mathcal{F})&=u\mathbf{f}\cdot\mathbf{w}\\&=u\mathrm{lm}(\mathbf{f})\cdot\mathbf{w}+u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&=cux^\alpha\mathbf{e}_i\cdot\mathbf{w}+u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&=v\mathrm{lm}(g)\mathbf{e}_i\cdot\mathbf{w}+u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&=v\mathrm{lm}(g)w_i+u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\end{aligned}$$

$$\begin{aligned}&= v(g-(g-\mathrm{lm}(g)))w_i + u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&= vw_i\mathbf{g}\cdot\mathbf{w} - v(g-\mathrm{lm}(g))\mathbf{e}_i\cdot\mathbf{w} + u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}.\end{aligned}$$

Clearly,

$$\mathrm{lpp}(u\mathbf{f}) \succ \mathrm{lpp}(vw_i\mathbf{g}),\quad \mathrm{lpp}(u\mathbf{f}) \succ \mathrm{lpp}(v(g-\mathrm{lm}(g))\mathbf{e}_i),\quad \mathrm{lpp}(u\mathbf{f}) \succ \mathrm{lpp}(u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))).$$

This shows that $(u,\mathcal{F})$ has a strictly lower representation. □

Proposition 4.2. *Suppose that B is a list of labeled polynomials and every $\mathcal{F}_i$ is an element of B where $\mathcal{F}_i = (\mathbf{e}_i, w_i)$ for $i = 1,\ldots,m$. Let u be a monomial and $\mathcal{F}$ be a labeled polynomial in B. If $(u,\mathcal{F})$ is* **F5-rewritable** *by B, then $(u,\mathcal{F})$ has a strictly lower representation w.r.t. B.*

Proof. Suppose that $\mathcal{F} = (\mathbf{f}, f)$, since $(u,\mathcal{F})$ is rewritable by B, there exists a labeled polynomial $\mathcal{G} = (\mathbf{g}, g) \in B$ such that $\mathrm{sign}(\mathcal{G}) \mid \mathrm{sign}(u\mathcal{F})$, i.e., $\mathrm{lm}(\mathbf{g}) \mid u\mathrm{lm}(\mathbf{f})$, and $\mathrm{index}(\mathcal{F},B) < \mathrm{index}(\mathcal{G},B)$. Let $u\mathrm{lm}(\mathbf{f}) = v\mathrm{lm}(\mathbf{g})$. We have

$$\begin{aligned}\mathrm{poly}(u\mathcal{F}) &= u\mathbf{f}\cdot\mathbf{w}\\&= u\mathrm{lm}(\mathbf{f})\cdot\mathbf{w} + u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&= v\mathrm{lm}(\mathbf{g})\cdot\mathbf{w} + u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&= v(\mathbf{g}-(\mathbf{g}-\mathrm{lm}(\mathbf{g})))\cdot\mathbf{w} + u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&= v\mathbf{g}\cdot\mathbf{w} - v(\mathbf{g}-\mathrm{lm}(\mathbf{g}))\cdot\mathbf{w} + u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}\\&= v\mathrm{poly}(\mathcal{G}) - v(\mathbf{g}-\mathrm{lm}(\mathbf{g}))\cdot\mathbf{w} + u(\mathbf{f}-\mathrm{lm}(\mathbf{f}))\cdot\mathbf{w}.\end{aligned}$$

In the above formula, $u\mathcal{F}$ and $v\mathcal{G}$ have same signatures, but $\mathrm{index}(\mathcal{F},B) < \mathrm{index}(\mathcal{G},B)$. This shows that $u\mathcal{F} \succ v\mathcal{G}$. Clearly, $\mathrm{lpp}(u\mathbf{f}) \succ \mathrm{lpp}(v(\mathbf{g}-\mathrm{lm}(\mathbf{g})))$ and $\mathrm{lpp}(u\mathbf{f}) \succ \mathrm{lpp}(u(\mathbf{f}-\mathrm{lm}(\mathbf{f})))$, therefore, $(u,\mathcal{F})$ has a strictly lower representation w.r.t. B. □

Now, we are able to prove the correctness of the F5B algorithm.

Theorem 4.3. *If* F5B *terminates in finite steps, the algorithm computes a Gröbner basis* $\{\mathrm{poly}(\mathcal{Q}) \mid \mathcal{Q} \in B\}$ *of the ideal generated by the input polynomial set* $\{w_1,\ldots,w_m\}$.

Proof. To prove the F5B algorithm computing a Gröbner of the ideal $\langle w_1,\ldots,w_m\rangle$, it suffices to show that for every $\mathcal{F},\mathcal{G}$ in B, the S-pair $[\mathcal{F},\mathcal{G}]$ has a t-representation. All these S-pairs can be divided into two sets SP_1 and SP_2 as follows:

$$\begin{aligned}SP_1 = \{&[\mathcal{F},\mathcal{G}] \mid \mathcal{F}\in B, \mathcal{G}\in B, [\mathcal{F},\mathcal{G}] \text{ is neither F5-divisible}\\&\text{nor F5-rewritable by } B\},\ \text{and}\\SP_2 = \{&[\mathcal{F},\mathcal{G}] \mid \mathcal{F}\in B, \mathcal{G}\in B, [\mathcal{F},\mathcal{G}] \text{ is either F5-divisible}\\&\text{or F5-rewritable by } B\}.\end{aligned}$$

First, we consider the S-pairs in SP_1. Suppose that $[\mathcal{F},\mathcal{G}] = (u,\mathcal{F},v,\mathcal{G})$ is an S-pair in SP_1. During the computation in F5B, its S-polynomials $\mathrm{spoly}(\mathcal{F},\mathcal{G})$ will be F5-reduced by the current B, i.e., $\mathrm{spoly}(\mathcal{F},\mathcal{G}) \Longrightarrow_B^* \mathcal{P}$. By Proposition 2.6, there exist polynomials p_i in R and labeled polynomials $\mathcal{G}_i$, such that

$$\mathrm{spoly}(\mathcal{F},\mathcal{G}) = \mathcal{P} + p_1\mathcal{G}_1 + \cdots + p_s\mathcal{G}_s,$$

where

$$\begin{aligned}&\mathrm{lpp}(\mathrm{poly}(\mathrm{spoly}(\mathcal{F},\mathcal{G}))) \succeq \mathrm{lpp}(\mathrm{poly}(\mathcal{P})),\\&\mathrm{lpp}(\mathrm{poly}(\mathrm{spoly}(\mathcal{F},\mathcal{G}))) \succeq \mathrm{lpp}(p_i\mathrm{poly}(\mathcal{G}_i))\end{aligned}$$

and $\mathrm{sign}(u\mathcal{F}) \succ \mathrm{sign}(p_i\mathcal{G}_i)$ for $i = 1, \ldots, s$. Moreover, $\mathrm{sign}(u\mathcal{F}) = \mathrm{sign}(\mathcal{P})$. In F5B, the labeled polynomial $\mathcal{P}$ is appended to the *end* of the current B. After B is updated, we have $\mathrm{index}(\mathcal{F}, B) < \mathrm{index}(\mathcal{P}, B)$. It follows that the S-pair $[\mathcal{F}, \mathcal{G}]$ has a t-representation w.r.t. this updated B, and hence has a t-representation w.r.t. the final B.

Second, we consider the S-pairs in SP_2. Notice that SP_2 is just the set RedundantSPairs in F5B. We will prove that all the S-pairs in SP_2 also have t-representations. Now, let us take the minimal S-pair $[\mathcal{F}, \mathcal{G}]$ from SP_2. Since all the S-pairs smaller than $[\mathcal{F}, \mathcal{G}]$ are elements of SP_1, they should have t-representations. It is because we have already shown every S-pair in SP_1 had a t-representation. For this minimal S-pair $[\mathcal{F}, \mathcal{G}] = (u, \mathcal{F}, v, \mathcal{G})$, $[\mathcal{F}, \mathcal{G}]$ is either F5-divisible or F5-rewritable. This implies that $(u, \mathcal{F})$ or $(v, \mathcal{G})$ is either F5-divisible or F5-rewritable. Propositions 4.1, 4.2 and 3.5 show that $[\mathcal{F}, \mathcal{G}]$ has a t-representation. Next, we move the S-pair $[\mathcal{F}, \mathcal{G}]$ from SP_2 to SP_1, select another minimal S-pair from SP_2, and repeat the above procedures. After all, we can prove that all the S-pairs in the original SP_2 have t-representations, and the theorem is proved. □

5 Available variants of F5

5.1 Available variants

Generally speaking, F5 or F5B introduces a special reduction (F5-reduction) and provides two criteria (syzygy criterion and rewritten criterion) to avoid unnecessary computations or reductions.

From the proofs in last section, Lemma 3.4 plays a crucial role in the whole proofs. This key lemma is based on the property of F5-reduction (Proposition 2.6). So *the* F5*-reduction is the key of the whole* F5 *or* F5B *algorithm, and it ensures the correctness of the whole algorithm.*

Therefore, various variants of the F5 algorithm become available if we maintain the F5-reduction. For example,

1. using various strategies of selecting S-pairs, such as incremental F5 algorithm in [9] and the F5 algorithm (reported by Faugère in INSCRYPT 2008);

2. using matrix techniques while processing reductions, such as *matrix*-F5 algorithm mentioned in [1];

3. adding some new initial polynomials during computation, such as branch Gröbner basis algorithm over Boolean ring [19, 20];

4. choosing different order for signatures, such as Gröbner basis algorithms in [15, 19, 20].

Next, we introduce a natural variant of the F5 algorithm by giving a new order for signatures. This natural variant has been reported in [19, 20], and it is also quite similar as the variant in [15].

5.2 A natural variant

In fact, the original F5 algorithm is always an incremental algorithm no matter which strategy of selecting S-pair is used. Specifically, the outputs of the F5 algorithm not only contain the Gröbner basis of the ideal $\langle w_1, \ldots, w_m\rangle$, but also include the Gröbner bases of the ideals $\langle w_i, \ldots, w_m\rangle$ for $1 < i < m$. However, there are some disadvantages for this kind of incremental algorithms.

1. Generally, the ideals $\langle w_i, \ldots, w_m\rangle$ for $1 < i < m$ usually have higher dimensions than the ideal $\langle w_1, \ldots, w_m\rangle$, so their Gröbner bases may be expensive to compute.

2. The Gröbner bases of the ideals $\langle w_i, \ldots, w_m\rangle$ for $1 < i < m$ are not necessary, since the Gröbner of ideal $\langle w_1, \ldots, w_m\rangle$ is what we really need.

3. The order of initial polynomials influences the efficiency of algorithm significantly.

If we investigate the algorithm carefully, we would find that *it is the order of signatures that makes the* F5 *algorithm incremental*. The original F5 algorithm uses a POT (position over term) order for signatures on monomials of $\mathbb{R}^m$. Thus, a natural idea is to change the POT order to the TOP (term over position) order. When using a TOP order for signatures, the F5 algorithm becomes a non-incremental algorithm.

We extend the admissible order $\succ$ on monomials of $\mathbb{R}$ to an order on monomials of $\mathbb{R}^m$ in the TOP fashion as follows:

$$x^\alpha \mathbf{e}_i \succ' x^\beta \mathbf{e}_j \quad \text{iff} \begin{cases} x^\alpha \mathrm{lpp}(w_i) \succ x^\beta \mathrm{lpp}(w_j), & \text{or} \\ x^\alpha \mathrm{lpp}(w_i) = x^\beta \mathrm{lpp}(w_j) \text{ and } i < j. \end{cases}$$

All the definitions and conclusions under this new ordering remain unchanged except the following.

Definition 5.1. Let B be a list of labeled polynomials, u a monomial and $\mathcal{F}$ a labeled polynomial in B. A pair $(u, \mathcal{F})$ is said to be F5-divisible by B, if there exists a labeled polynomial $\mathcal{G}$ in B such that if

$$\mathrm{sign}(\mathcal{F}) = x^\alpha \mathbf{e}_i, \quad \mathrm{sign}(\mathcal{G}) = x^\beta \mathbf{e}_j$$

and $i < j$, we have

1. $\mathrm{lpp}(\mathrm{poly}(\mathcal{G})) \mid ux^\alpha$, and
2. $ux^\alpha \mathbf{e}_i \succ' v\mathrm{lpp}(w_i)x^\beta \mathbf{e}_j$, where

$$v = \frac{ux^\alpha}{\mathrm{lpp}(\mathrm{poly}(\mathcal{G}))}.$$

From the definition, we know that this new syzygy criterion only utilizes the principle syzygies of the initial polynomials, i.e. $w_i w_j - w_j w_i = 0$, which is the same as the criteria in [15]. The syzygy criterion in Hashemi and Ars [15] can also be proved in a same way. In order to use more possible syzygies on initial polynomials, we introduced the following technique in [19, 20].

Suppose the ideal is generated by the initial polynomials $w_1, \ldots, w_m$. Let B be a list of labeled polynomials in F5B. When a labeled polynomial $\mathcal{P} = (\mathbf{p}, p)$ is generated during the computation. We can treat p as an initial polynomial, and assign p a new signature $\mathbf{e}_{m+1}$, i.e., we can rewrite $\mathcal{P}$ as $\mathcal{P}' = (\mathbf{e}_{m+1}, p)$. The list B will be updated by appending $\mathcal{P}'$, and the related S-pairs should be updated also.

5.3 Experimental results for Boolean polynomial systems

Although only the principle syzygies of initial polynomials are used, the new syzygy criterion also performs pretty good in experiments. We have implemented this natural variant of the F5 algorithm over Boolean ring [19, 20]. The data structure ZDD (zero-suppressed binary decision diagrams) is used to express Boolean polynomials.

The following is a table of experimental results for computing Gröbner basis of Boolean polynomial system. In the experiments, Boolean polynomials are randomly generated and the number of initial polynomials m equals to the number of variables n. The timings are obtained on a computer (OS Linux, CPU Xion 4*3.0 GHz, 16.0 GB RAM). In the table, the rows F2-*divisible, divisible* and *rewritable* indicate the number of S-pairs which meet the corresponding criteria. For F2-divsible, please see [19, 20]. Besides, the row *useful S-pairs* indicates the number of S-pairs which are really operated during computation. The row 0-*polys* indicates the number of S-pairs which are not removed by the revised criteria but reduced to 0 by F5-reduction.

From Table 1, we can see that all the redundant S-pairs have been rejected. Our experiences also

Table 1 Experiments for the revised criteria

$m = n$	12	14	16	18	20
divisible	898	72189	68337	99058	136404
F2-divisible	114	7770	6763	9374	11749
rewritable	136	6908	4786	6293	8536
useful S-pairs	305	841	3480	4469	5672
0-polys	0	0	0	0	0
Time(sec.)	0.107	0.778	14.586	77.197	344.875

show that almost all redundant S-pairs can be removed by the new criteria, especially for large systems.

6 Conclusions

We introduce a concept of t-representation for labeled polynomials, and we also show that an S-pair should have a t-representation if it is F5-divisible or F5-rewritable. Based on this fact, the correctness of the F5 algorithm is not affected if discarding the S-pairs which are F5-divisible or F5-rewritable. Hence, we prove the correctness of the F5B algorithm which has been shown to be equivalent to F5. This new proof is not limited to homogeneous systems and does not depend on the strategies of selecting S-pairs, so it can be extended to other variants of the F5 algorithm. From the proof, we find that the F5-reduction is the key of the whole algorithm and it ensures the correctness of two criteria. With these insights, various variants of the F5 algorithm become available by maintaining the F5-reduction. We also present a natural and non-incremental variant of the F5 algorithm, and the experimental results show that this variant also can reject almost all the redundant S-pairs. Other possible variants of the F5 algorithm will be studied in the future.

Acknowledgements This work was supported by National Key Basic Research Project of China (Grant No. 2011CB302400) and National Natural Science Foundation of China (Grant Nos. 10971217 and 61121062). We would also like to thank Xiaoshan Gao, Shuhong Gao, Deepak Kapur and Christian Eder for their constructive suggestions.

References

1 Bardet M, Faugère J-C, Salvy B. Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$. Inria Research Report, n 5049, 2003
2 Becker T, Weispfenning V, Kredel H. Gröbner Bases. New York: Springer-Verlag, 1993
3 Buchberger B. Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. PhD Thesis, Innsbruck, 1965
4 Buchberger B. A criterion for detecting unnecessary reductions in the construction of Gröbner basis. In: Proc EUROCAL'79, Lecture Notes in Computer Science, vol. 72. New York: Springer-Verlag, 1979, 3–21
5 Eder C. On the criteria of the F5 algorithm. ArXiv:0804.2033, 2008
6 Eder C, Perry J. F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases. ArXiv:0906.2967, 2009
7 Eder C, Perry J. Signature-based algorithms to compute Gröbner bases. In: Proc ISSAC'11. New York: ACM Press, 2011, 99–106
8 Faugère J-C. A new efficient algorithm for computing gröbner bases (F4). J Pure Appl Algebra, 1999, 139: 61–88
9 Faugère J-C. A new efficient algorithm for computing Grönber bases without reduction to zero (F5). In: Porc ISSAC'2002. New York: ACM Press, 2002, 75–83
10 Faugère J-C, Ars G. An algebraic cryptanalysis of nonlinear filter generators using Gröbner bases. Inria Research Report, n 4739, 2003
11 Gao S H, Guan Y H, Volny F. A new incremental algorithm for computing Gröbner bases. In: Proc ISSAC'10. New York: ACM Press, 2010, 13–19
12 Gao S H, Volny F, Wang M S. A new algorithm for computing Gröbner bases. Cryptology ePrint Archive: Report 2010/641, 2010
13 Gebauer R, Moller H M. Buchberger's algorithm and staggered linear bases. In: Proc ISSAC'86. Ontario: Waterloo, 1986, 218–221
14 Giovini A, Mora T, Niesi G, et al. One sugar cube, please, or selection strategies in the Buchberger algorithm. In: Proc ISSAC'91. Bonn: ACM Press, 1991, 49–54
15 Hashemi A, Ars G. Extended F5 criteria. J Symb Comput, 2010, 45: 1330–1340
16 Huang L. A new conception for computing Gröbner basis and its applications. ArXiv:1012.5425, 2010
17 Lazard D. Gaussian elimination and resolution of systems of algebraic equations. In: Proc EUROCAL'83, Lecture Notes in Computer Science, vol. 162. New York: Springer-Verlag, 1983, 146–157
18 Mora T, Möller H M, Traverso C. Gröbner bases computation using syzygies. In: Proc ISSAC'92. New York: ACM Press, 1992, 320–328
19 Sun Y, Wang D K. Branch Gröbner bases algorithm over Boolean ring (in Chinese). J Syst Sci Math Sci, 2009, 29: 1266–1277

20 Sun Y, Wang D K. The implementation and complexity analysis of the branch Gröbner bases algorithm over Boolean ring. In: Proc ASCM'09, 2009, 191–200
21 Sun Y, Wang D K. The F5 algorithm in Buchberger's style. J Syst Sci Complex, 2011, 24: 1218–1231
22 Sun Y, Wang D K. A generalized criterion for signature related Gröbner basis algorithms. In: Proc ISSAC'11. New York: ACM Press, 2011, 337–344
23 Sun Y, Wang D K. Solving detachability problem for the polynomial ring by signature-based Gröbner basis algorithms. Preprint, 2011
24 Sun Y, Wang D K, Ma X D, et al. A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras. In: Proc ISSAC'12. New York: ACM Press, 2012, 351–358
25 Stegers T. Faugère's F5 algorithm revisited. Thesis for the degree of Diplom-Mathematiker, 2005
26 Zobnin A. Generalization of the F5 algorithm for calculating Gröbner bases for polynomial ideals. Program Comput Softw, 2010, 36: 75–82