Are Buchberger's criteria necessary for the chain condition?

Hoon Hong

North Carolina State University, Raleigh NC USA

John Perry

The University of Southern Mississippi, Hattiesburg MS USA

Abstract

Buchberger's Gröbner basis theory plays a fundamental role in symbolic computation. The resulting algorithms essentially carry out several S-polynomial reductions. In his PhD thesis and later publication Buchberger showed that sometimes one can skip S-polynomial reductions if the leading terms of polynomials satisfy certain criteria. A question naturally arises: Are Buchberger's criteria also *necessary* for skipping S-polynomial reductions? In this paper, after making the question more precise (in terms of a chain condition), we show the answer to be "*almost, but not quite*": necessary when there are four or more polynomials, but not necessary when there are exactly three polynomials. For that case, we found an extension to Buchberger's criteria that is necessary as well as sufficient.

Key words: Gröbner bases, S-polynomials, Buchberger criteria

1991 MSC: 13P10

1. Introduction

Buchberger's theory and algorithm for Gröbner bases (Buchberger, 1965) play a fundamental role in computer algebra and symbolic computation. The algorithm essentially carries out several S-polynomial reductions. In (Buchberger, 1965) and (Buchberger, 1979), Buchberger showed that sometimes one can skip S-polynomial reductions if the leading terms of the polynomials satisfy certain criteria. A number of researchers have

⋆ This research was partly supported by US National Science Foundation Grant NSF-0097976.
Email addresses: hong@math.ncsu.edu (Hoon Hong), john.perry@usm.edu (John Perry).
URLs: www.math.ncsu.edu/~hong (Hoon Hong), www.math.usm.edu/perry (John Perry).

since studied how to apply these criteria to Buchberger's algorithm (Buchberger, 1985; Gebauer and Möller, 1988; Caboara et al., 2002). A question naturally arises: Are Buchberger's criteria also *necessary* for skipping S-polynomial reductions? In this paper, we show the answer to be "*almost, but not quite*".

In order to explain the meaning and the scope of the answer, let us make the question a bit more precise (also a bit more narrow). For this, we recall the notion of a *chain condition*. We say that three terms t_1, t_2 and t_3 satisfy the *chain condition* when for all polynomials $f_1, \ldots, f_m$ (where f_1, f_2 and f_3 have t_1, t_2 and t_3 as leading terms)

if the S-polynomial of f_1 and f_2 has a representation over $f_1, \ldots, f_m$, and
the S-polynomial of f_2 and f_3 has a representation over $f_1, \ldots, f_m$,
then the S-polynomial of f_1 and f_3 has a representation over $f_1, \ldots, f_m$.

(We review the definition of representation in the following section.) Buchberger showed that if t_1 and t_3 are relatively prime (the first criterion) or t_2 divides the lcm of t_1 and t_3 (the second criterion), then t_1, t_2 and t_3 satisfy the chain condition. Now the question can be stated more precisely: *Are Buchberger's two criteria also necessary for the chain condition?*

As mentioned above, we found the answer to be *almost, but not quite*. Buchberger's criteria are necessary when there are four or more polynomials ($m \geq 4$). However, when there are exactly three polynomials ($m = 3$), Buchberger's criteria are *not* necessary. For that case ($m = 3$), we found an extension to Buchberger's criteria that is necessary as well.

We assume that the reader is acquainted with the basic notions and terminology associated with Gröbner basis theory, that can be found in many excellent textbooks, such as (Becker et al., 1993; Adams and Loustaunau, 1994; Cox et al., 1997; Fröberg, 1997; Cox et al., 1998; Kreuzer and Robbiano, 2000).

The paper is structured as follows. In Section 2, we give precise statements of the question and the answer (two main theorems, one stating "*Almost*" and the other stating "*But not quite*"). We also illustrate the answer graphically in the hope of providing intuitive understanding. In Section 3, we provide proofs for the answer (two theorems). Finally, in Section 4, we discuss and clarify the result's relationship to several other works, and indicate some further questions.

2. Main Theorems

In this section, we state the question and the answer precisely. We begin by recalling the definitions of several basic notions. We work in a polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$. Let $\succ$ denote an admissible term ordering. For a polynomial f, we write $\mathrm{lt}(f)$ for the leading term of f, $\mathrm{lm}(f)$ for the leading monomial of f, and $\mathrm{lc}(f)$ for the leading coefficient of f, where we follow the convention that a monomial includes a coefficient, while a term does not. The *S-polynomial* of two polynomials f_i and f_j, written as S_{f_i,f_j} is defined by

$$S_{f_i,f_j} := \sigma_{f_i,f_j} \cdot f_i - \sigma_{f_j,f_i} \cdot f_j$$

where

$$\sigma_{f_i,f_j} := \frac{\mathrm{lcm}\left(\mathrm{lt}\left(f_i\right), \mathrm{lt}\left(f_j\right)\right)}{\mathrm{lm}\left(f_i\right)}.$$

We say that an S-polynomial S_{f_i,f_j} has a *representation* modulo $F = (f_1, \ldots, f_m)$ and write

$$\mathrm{Rep}\left(S_{f_i,f_j}, F\right)$$

if there exists $(h_1, \ldots, h_m)$ such that

$$S_{f_i,f_j} = h_1 \cdot f_1 + \cdots + h_m \cdot f_m$$

and for $k = 1, \ldots, m$ either $h_k = 0$ or

$$\mathrm{lt}(h_k) \cdot \mathrm{lt}(f_k) \prec \mathrm{lcm}(\mathrm{lt}(f_i), \mathrm{lt}(f_j)).$$

We call $(h_1, \ldots, h_m)$ a representation of S_{f_i,f_j} modulo F.[1]

Definition 1 (Chain Condition)**.** We say that terms t_1, t_2, t_3 satisfy the *m-chain condition* and write

$$\mathrm{Chain\_Condition}(t_1, t_2, t_3; m)$$

if for all $F = (f_1, \ldots, f_m)$ such that $t_1 = \mathrm{lt}(f_1), t_2 = \mathrm{lt}(f_2), t_3 = \mathrm{lt}(f_3)$ we have

$$\mathrm{Rep}(S_{f_1,f_2}, F) \text{ and } \mathrm{Rep}(S_{f_2,f_3}, F) \implies \mathrm{Rep}(S_{f_1,f_3}, F).\diamond$$

It is important to note that the chain condition is over *terms*, not over polynomials. In fact, the polynomials are universally quantified. Thus, if the condition holds on some terms, then the implication "$\Longrightarrow$" holds for all polynomials having those terms as leading terms. Since the notion makes sense only when $m \geq 3$, from now on we will assume that $m \geq 3$. In (Buchberger, 1965) and (Buchberger, 1979), Buchberger introduced the following criteria on terms and then proved the subsequent theorem.[2]

Definition 2 (Buchberger's Criteria)**.** We say that terms t_1, t_2, t_3 satisfy *Buchberger's criteria* and write

$$\mathrm{Buchberger\_Criteria}(t_1, t_2, t_3)$$

if $\gcd(t_1, t_3) = 1$ or t_2 divides $\mathrm{lcm}(t_1, t_3)$. $\diamond$

Theorem 3 (Buchberger 1965, 1979)**.** *For all t_1, t_2, t_3 and m we have*

$$\mathrm{Chain\_Condition}(t_1, t_2, t_3; m) \Longleftarrow \mathrm{Buchberger\_Criteria}(t_1, t_2, t_3).\diamond$$

Buchberger's Criteria consists of a disjunction of two criteria: the first part is called the first (or gcd) criteria and the second part is called the second (or lcm) criteria. The theorem states that Buchberger's criteria are *sufficient* for the chain condition. A question naturally arises: Are Buchberger's criteria also *necessary* for the chain condition (hence making them *equivalent*)?

The main contribution of this paper is to show that the answer is "*almost, but not quite*"; it depends on the number m of polynomials. For $m \geq 4$, it is indeed necessary, but for $m = 3$, it is not. We first state the "*almost*" case precisely.

---

[1] The notion of representation is taken from (Becker et al., 1993). One might wonder why we talk about *representation* instead of *reduction to zero*. It is because representations also can be used for characterizing Gröbner bases: a system is a Gröbner basis iff all the S-polynomials have representations (Becker et al., 1993; Cox et al., 1997). Furthermore, it turns out that using representation makes it easy to state and prove our main results. Nowadays Buchberger's criteria are also stated and proved in terms of representation, due to its simplicity (Becker et al., 1993; Cox et al., 1997).

[2] Buchberger presented the theorem in a slightly different way, but it is essentially the same as the one given here. We present it in this way because it is more convenient for describing the results of this paper. Buchberger also considered the possibility of longer chains, but in this paper, we restrict our discussions to chains of length three, because they still capture the essential idea.

Theorem 4 (Almost)**.** *For all* t_1, t_2, t_3 *and* $m \geq 4$*, we have*

$$\text{Chain\_Condition}\,(t_1, t_2, t_3; m) \Longleftrightarrow \text{Buchberger\_Criteria}\,(t_1, t_2, t_3)\,. \diamond$$

Before we state the "*but not quite*" case, we introduce an extension of Buchberger's criteria.

Definition 5 (Extended Criteria)**.** We say that terms t_1, t_2, t_3 satisfy the *extended criteria* and write

$$\text{Extended\_Criteria}\,(t_1, t_2, t_3)$$

if the terms satisfy the two conditions (EC_div) and (EC_var), where

(EC_div) gcd (t_1, t_3) divides t_2 or t_2 divides lcm (t_1, t_3)

(EC_var) $\text{VBG}_x\,(t_1, t_3)$ or (for every variable x $\text{VBL}_x\,(t_1, t_2, t_3)$), where

$$\begin{aligned} \text{VBG}_x\,(t_1, t_3) &:= \min(\deg_x t_1, \deg_x t_3) = 0 \\ \text{VBL}_x\,(t_1, t_2, t_3) &:= \deg_x t_2 \leq \max\,(\deg_x t_1, \deg_x t_3)\,. \diamond \end{aligned}$$

In the above, VBG stands for "Variable-wise Buchberger Gcd criterion" and VBL stands for "Variable-wise Buchberger Lcm criterion".

Theorem 6 (But not quite)**.** *For all* t_1, t_2, t_3 *and* $m = 3$*, we have*

$$\text{Chain\_Condition}\,(t_1, t_2, t_3; m) \Longleftrightarrow \text{Extended\_Criteria}\,(t_1, t_2, t_3)\,. \diamond$$

It is easy to see that the Buchberger's Criteria imply the Extended Criteria, but the Extended Criteria do *not* imply Buchberger's Criteria. Hence, the above theorem (Theorem "*But not quite*") tells us that there are terms that do not satisfy Buchberger's criteria, but still satisfy the chain condition.

Figure 1 illustrates Theorem "*But not quite*" graphically for two variable cases (first row) and three variable cases (second row). For several chosen terms t_1 and t_3 (colored black) all possible terms t_2 satisfying the chain condition are shaded. Observe that when t_1 and t_3 share *all* variables (Cases 2a and 3a), the condition $\text{VBG}_x\,(t_1, t_3)$ is false for all variables x, and thus the extended criteria is equivalent to Buchberger's lcm criterion. When t_1 and t_3 share *no* variables (Cases 2d and 3d), the condition $\text{VBG}_x\,(t_1, t_3)$ is true for all variables x, and thus the extended criteria is equivalent to Buchberger's gcd criterion. When t_1 and t_3 share *some* variables but not all (Cases 2b, 2c, 3b, 3c), the extended criteria is *not* equivalent to Buchberger's criteria, providing more general criteria than Buchberger's.

Note that applying Buchberger's criteria to Cases 2b, 2c and 3b, 3c would have given the same shaded regions as those shown in Cases 2a and 3a. Hence the segments in Cases 2b, 2c, 3b, 3c that "stick out" beyond the pictures for Cases 2a and 3a are additional terms t_2 satisfying the chain condition.

We conclude this section with two concrete examples of when the new criterion does and does not help.

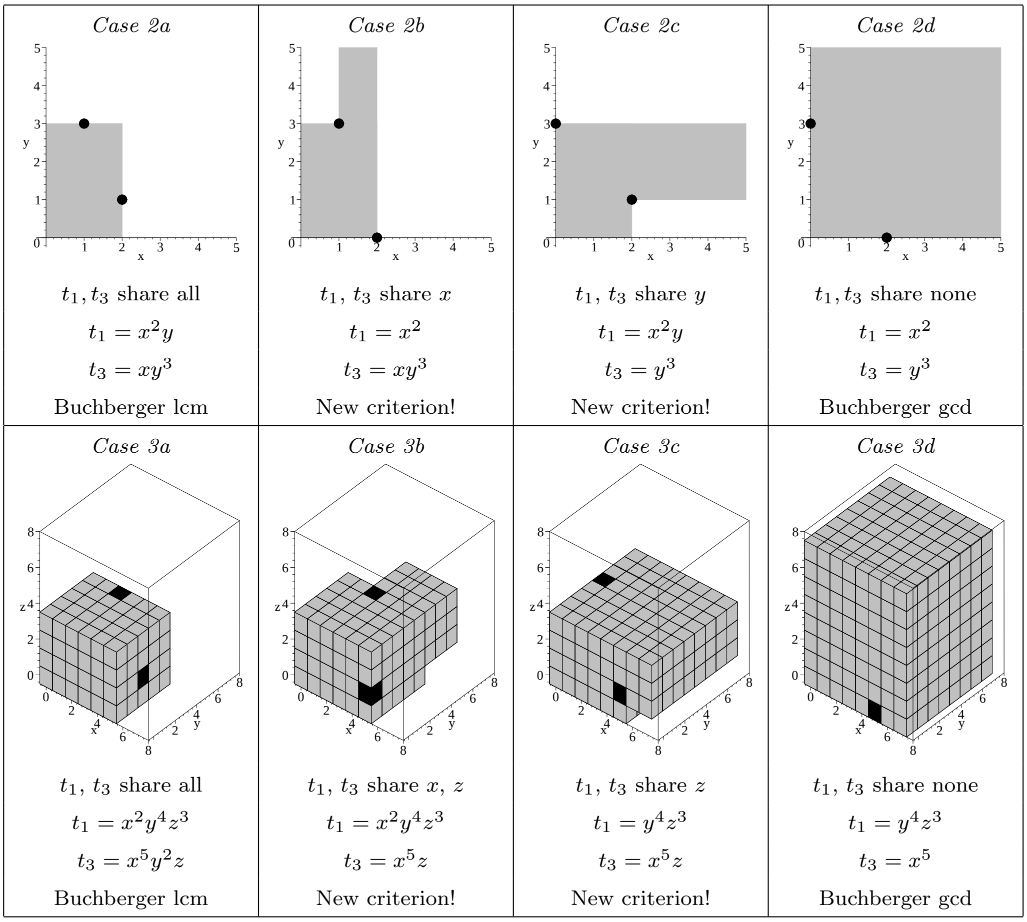

Figure 1. Illustration of Theorem "*But not quite*"

Example 7. Let $F = (f_1, f_2, f_3, f_4)$ where

$$f_1 = x_0^{10}x_1^{12} + x_0^{10} + 2x_0^8x_1^{12} + 2x_0^8 - 21x_0^4x_1^{12} - 21x_0^4 + 12x_0^3x_1^{12} + 12x_0^3 + 2x_1^{12} + 2$$
$$f_2 = x_1^{12}x_2^{10} + x_2^7 - 3x_2^4 + 2x_2^3 + x_2^2 - 8x_2 - 1$$
$$f_3 = x_0^{10}x_3^8 + x_0^{10} + 2x_0^8x_3^8 + 2x_0^8 - 21x_0^4x_3^8 - 21x_04 + 12x_0^3x_3^8 + 12x_0^3 + 2x_3^8 + 2$$
$$f_4 = x_3^8x_4^{10} + x_4^8 + 1$$

Let $\prec$ be a lexicographic ordering where $x_0 \prec x_1 \prec x_2 \prec x_3 \prec x_4$. Then $\operatorname{lt}(f_1) = x_0^{10}x_1^{12}$, $\operatorname{lt}(f_2) = x_1^{12}x_2^{10}$, $\operatorname{lt}(f_3) = x_0^{10}x_3^8$, and $\operatorname{lt}(f_4) = x_3^8x_4^{10}$. We trace Buchberger's algorithm, using the normal strategy for selecting critical pairs.

The normal strategy sorts the list of critical pairs as

$$\mathcal{B} = ((1,2), (1,3), (2,3), (3,4), (1,4), (2,4)),$$

so the first S-polynomial to be considered is S_{f_1,f_2}, which does not have a representation modulo F. After reducing S_{f_1,f_2} modulo F, we append to F the resulting polynomial f_5, whose leading term is $x_0^{10}x_2^{10}$. We add the requisite critical pairs to $\mathcal{B}$, and sort the list, obtaining

$$\mathcal{B} = ((1,5),(2,5),(1,3),(3,5),(2,3),(3,4),(1,4),(4,5),(2,4)).$$

The next S-polynomials to be considered are S_{f_1,f_5}, S_{f_2,f_5}, and S_{f_1,f_3}, which all have representations modulo F. In fact, Buchberger's second criterion implies that S_{f_2,f_5} has a representation by a chain with f_1. Note that one can find representations of S_{f_1,f_5} and S_{f_1,f_3} modulo (f_1, f_5) and (f_1, f_3), respectively.

This brings us to S_{f_3,f_5}. Inspection shows that the leading terms of f_3 and f_5 satisfy the Extended Criteria, and moreover that none of the other leading terms divides their lcm ($x_0^{10}x_2^{10}x_3^8$). Because we can find representations of S_{f_1,f_3} and S_{f_1,f_5} modulo (f_1, f_3, f_5) only, Theorem "But not quite" implies that S_{f_3,f_5} has a representation modulo (f_1, f_3, f_5); there is no need to compute it explicitly. This shows that the Extended Criteria are not equivalent to Buchberger's criteria.

The next S-polynomial to be considered is S_{f_2,f_3}, which by Buchberger's first criterion has a representation modulo F.

Since S_{f_3,f_4} does not have a representation modulo F, we reduce it modulo F and append to F the resulting polynomial f_6, which has leading term $x_0^{10}x_4^{10}$. We add the requisite critical pairs to $\mathcal{B}$ and sort the list, obtaining

$$\mathcal{B} = ((1,6),(5,6),(2,6),(3,4),(3,6),(4,6),(1,4),(4,5),(2,4)).$$

The S-polynomial S_{f_1,f_6} has a representation modulo F. In fact, one can find a representation modulo (f_1, f_6).

We come to S_{f_5,f_6}. As with S_{f_3,f_5}, the leading terms satisfy the Extended criteria, and we can build a chain with f_1, since S_{f_1,f_5} and S_{f_1,f_6} have representations modulo (f_1, f_5, f_6). By Theorem "But not quite," S_{f_5,f_6} has a representation modulo (f_1, f_5, f_6).

By Buchberger's first criterion, S_{f_2,f_6} has a representation. By the Extended Criteria, S_{f_3,f_6} has a representation, building a chain with f_1. By Buchberger's second criterion, S_{f_4,f_6} has a representation, building a chain with f_3. By Buchberger's first criterion, S_{f_1,f_4}, S_{f_4,f_5}, and S_{f_2,f_4} have representations.

The algorithm now concludes. Out of fifteen S-polynomials, we computed a representation for six. (Phrased another way, we carried out six S-polynomial reductions.) Had we not used the Extended Criteria, we would have computed nine.

Example 8. Let $F = (f_1, f_2, f_3, f_4)$ where

$$\begin{aligned} f_1 &= x_0x_1 + x_2 \\ f_2 &= x_0x_2 + x_1 \\ f_3 &= x_0x_3 + x_3 \end{aligned}$$

and let $\prec$ be a lexicographic term ordering where $x_3 \prec x_2 \prec x_1 \prec x_0$.

The first S-polynomial considered is S_{f_2,f_3}. This does not have a representation modulo F, so we append $f_4 = x_1x_3 - x_2x_3$. After this, we consider S_{f_3,f_4}, S_{f_1,f_4}, and S_{f_1,f_3}, all of which have representations. Indeed, Buchberger's second criterion detects a representation for S_{f_1,f_3}, building a chain with f_4.

This brings us to S_{f_1,f_2}. The leading terms of f_1, f_2, and f_3 satisfy the Extended Criteria, and both S_{f_1,f_3} and S_{f_2,f_3} have representations modulo F, so one might naïvely expect that S_{f_1,f_2} has a representation modulo F. To the contrary, *no such representation* *exists*. We must append $f_5 = x_1^2 - x_2^2$ to F. It is easily verified that the remaining S-polynomials have representations, and $F = (f_1, f_2, f_3, f_4, f_5)$ is a Gröbner basis.

What happened with S_{f_1,f_2}? A careful reading of Theorem "*But not quite*" shows that in order to apply the Extended Criteria the representations of S_{f_1,f_3} and S_{f_2,f_3} can only be over (f_1, f_2, f_3). This is why we took pains to note such details in the previous example! In this example, the representations of the latter two S-polynomials depend on f_4, which lies outside the triplet of leading terms of f_1, f_2, and f_3, so Theorem "*But not quite*" does not apply.

The examples show that the Extended Criteria are sometimes useful, and other times not. A full statistical analysis of their benefit is desirable, but lies beyond the scope of the current paper. See Section 4 for related questions.

3. Proof

In this section, we prove the two main theorems "*Almost*" and "*But not quite*". Since Buchberger has proved the sufficiency side of Theorem "*Almost*", that is, (Chain_Condition) $\Longleftarrow$ (Buchberger_Criteria), it remains to show

- the necessity side of Theorem "*Almost*": that is,
  (Chain_Condition) $\Longrightarrow$ (Buchberger's_Criteria);
- the necessity side of Theorem "*But not quite*": that is,
  (Chain_Condition) $\Longrightarrow$ (Extended_Criteria);
- the sufficiency side of Theorem "*But not quite*": that is,
  (Chain_Condition) $\Longleftarrow$ (Extended_Criteria).

Subsections 3.1, 3.2, and 3.3 respectively provide the proofs of these three assertions.

Before we plunge into details, we first provide a rough overview of the strategy and structure for the proofs, and remark on where the difficulties lay, as well as how we overcame them.

In order to prove the necessity side of Theorem "*Almost*", that is, (Chain_Condition) $\Longrightarrow$ (Buchberger_Criteria), we construct suitable "witness" polynomials $f_1, \ldots, f_m$ such that the S-polynomial of f_1 and f_2 and the S-polynomial of f_2 and f_3 have representations. We assumed the Chain Condition, so the S-polynomial of f_1 and f_3 also has a representation, whose structure in turn implies Buchberger's Criteria. Of course, the difficulty lies in finding a suitable witness. We conjectured some witnesses without too much difficulty; however, proving that these were indeed witnesses was non-trivial, because many subtle details required careful attention.

We tackled the necessity side of Theorem "*But not quite*", that is, (Chain_Condition) $\Longrightarrow$ (Extended_Criteria), in a similar manner. However, the witness polynomials of Theorem "*Almost*" could not be reused here, and finding new witnesses proved to be non-trivial. This required detailed analysis of term structure and the behavior (or misbehavior) of S-polynomials.

In order to prove the sufficiency side of Theorem "*But not quite*", that is, (Chain_Condition) $\Longleftarrow$ (Extended_Criteria), we note that the polynomials are universally quantified in the Chain Condition. The Extended Criteria only provide information about the leading terms, so we had to construct a representation of the S-polynomial S_{f_1,f_3} without any information about the non-leading terms of f_1, f_2, f_3, about their coefficients, or about representations of S_{f_1,f_2} and S_{f_2,f_3}.

Of course, much more difficult than proving Theorem "*But not quite*" was forming, in the first place, a promising conjecture to prove. This required not merely months, but years! Initially, we conjectured that Buchberger's criteria were "*always*" necessary. After some time spent in fruitless pursuit of a proof for this conjecture, we discovered a counterexample. This counterexample generalized naturally to (EC_div); however, proving its sufficiency turned out to be difficult. We discovered the correct form of the conjecture involving (EC_var) also, along with the general idea of the proof, only after computing tens of thousands of sets of polynomials and carefully analyzing their structure. In retrospect, it is remarkable how much information about the polynomials one can glean from such a small amount of information: the structure of their leading terms, and the assumption that two S-polynomials have representations.

3.1. Necessity side of Theorem "Almost"

In this section, we show that (Chain_Condition) $\Longrightarrow$ (Buchberger_Criteria) for Theorem "*Almost;*" that is, one of Buchberger's criteria is necessary for skipping an S-polynomial reduction when $m \geq 4$ polynomials. We begin with a technical but crucial lemma, which we will also use in the next subsection.

Lemma 9. *Let $f_1, \ldots, f_m$ be such that*

$$\begin{aligned} f_1 &= t_1 + u \\ f_2 &= t_2 \\ &\vdots \\ f_m &= t_m \end{aligned}$$

where u is a term such that $u \prec t_1$. Let $j > 1$. Suppose that S_{f_1,f_j} has a representation $(h_1, \ldots, h_m)$ modulo $(f_1, \ldots, f_m)$. Let

$$\tau_k = \operatorname{lcm}(t_1, t_j) \left(\frac{u}{t_1}\right)^k.$$

Then there exists $k \geq 1$ such that τ_k appears in $h_2 f_2 + \cdots + h_m f_m$. $\diamond$

Proof. We proceed by contradiction. Assume, to the contrary, that there does not exist $k \geq 1$ such that τ_k appears in $h_2 f_2 + \cdots + h_m f_m$. We will derive a contradiction. Note that

$$S_{f_1,f_j} = h_1 t_1 + h_1 u + h_2 f_2 + \cdots + h_m f_m. \tag{1}$$

Note that $\tau_1 = S_{f_1,f_j}$. Since τ_1 is the term on the left-hand side of equation (1), the term τ_1 must also appear on the right-hand side. Suppose that τ_1 appears in $h_1 u$. Then τ_1/u would appear in h_1, so

$$\operatorname{lcm}(t_1, t_j) \succ \operatorname{lt}(h_1) \cdot \operatorname{lt}(f_1) \succeq \frac{\tau_1}{u} \cdot t_1 = \operatorname{lcm}(t_1, t_j),$$

which is a contradiction. Therefore, τ_1 cannot appear in $h_1 u$. Recall that we assumed that τ_1 does not appear in $h_2 f_2 + \cdots + h_m f_m$. Thus τ_1 appears in $h_1 t_1$.

Note that τ_1/t_1 appears in h_1. Thus $\tau_2 = \tau_1/t_1 \cdot u$ appears in $h_1 u$. Note also that $\tau_1 \succ \tau_2$. Hence τ_2 does not appear on the left hand side of (1). Therefore τ_2 must appear in $h_1 t_1$ or in $h_2 f_2 + \cdots + h_m f_m$. Recall that we assumed that τ_2 does not appear in $h_2 f_2 + \cdots + h_m f_m$. Thus τ_2 appears in $h_1 t_1$.

Note that τ_2 / t_1 appears in h_1. Thus $\tau_3 = \tau_2 / t_1 \cdot u$ appears in $h_1 u$. Note also that $\tau_2 \succ \tau_3$. Hence τ_3 does not appear on the left hand side of (1). Therefore τ_3 must appear in $h_1 t_1$ or in $h_2 f_2 + \cdots + h_m f_m$. Recall that we assumed that τ_3 does not appear in $h_2 f_2 + \cdots + h_m f_m$. Thus τ_3 appears in $h_1 t_1$.

Continuing in the same way, we obtain an infinite descending sequence of terms $\tau_1 \succ \tau_2 \succ \tau_3 \succ \cdots$ that appear in $h_1 t_1$, contradicting the fact that $h_1 t_1$ has only finitely many terms. □

Lemma 10. *For $m \geq 4$, (Chain_Condition) $\Longrightarrow$ (Buchberger_Criteria).* ◇

Proof. Let $m \geq 4$. Assume (Chain_Condition). If $t_1 = 1$, then t_1 and t_3 are relatively prime, so (Buchberger_Criteria) is satisfied. Thus we assume that $t_1 \neq 1$. Let

$$\begin{aligned} f_1 &= t_1 + 1 \\ f_2 &= t_2 \\ f_3 &= t_3 \end{aligned}$$

and put

$$f_4 = \cdots = f_m = S_{f_1, f_2}.$$

Note that $S_{f_2, f_3} = 0$. Thus it has the trivial representation $(0, 0, 0)$. Note also that S_{f_1, f_2} has a representation since

$$S_{f_1, f_2} = 1 \cdot f_4$$

and

$$\operatorname{lt}(1) \cdot \operatorname{lt}(f_4) = \frac{\operatorname{lcm}(t_1, t_2)}{t_1} \prec \operatorname{lcm}(t_1, t_2).$$

Recall that we assumed (Chain_Condition); thus we have a representation $(h_1, \ldots, h_m)$ for S_{f_1, f_3}. By Lemma 9, there exists $k \geq 1$ such that $\tau_k = \operatorname{lcm}(t_1, t_3) \left(\frac{1}{t_1}\right)^k$ appears in $h_2 f_2 + \cdots + h_m f_m$. We consider three cases:

Case 1: τ_k is a term of $h_2 f_2$.
Then $t_2 \mid \operatorname{lcm}(t_1, t_3) \left(\frac{1}{t_1}\right)^k$. Thus $t_1^k t_2 \mid \operatorname{lcm}(t_1, t_3)$. Hence $t_2 \mid \operatorname{lcm}(t_1, t_3)$.

Case 2: τ_k is a term of $h_3 f_3$.
Then $t_3 \mid \operatorname{lcm}(t_1, t_3) \left(\frac{1}{t_1}\right)^k$. Thus $t_1^k t_3 \mid \operatorname{lcm}(t_1, t_3)$. Hence $\gcd(t_1, t_3) = 1$.

Case 3: τ_k is a term of $h_k f_k$ for $4 \leq k \leq m$.
Then $S_{f_1, f_2} \mid \operatorname{lcm}(t_1, t_3) \left(\frac{1}{t_1}\right)^k$. Therefore, $\frac{\operatorname{lcm}(t_1, t_2)}{t_1}$ divides $\operatorname{lcm}(t_1, t_3) \left(\frac{1}{t_1}\right)^k$.
Thus $\operatorname{lcm}(t_1, t_2)\, t_1^{k-1} \mid \operatorname{lcm}(t_1, t_3)$. Hence $t_2 \mid \operatorname{lcm}(t_1, t_3)$.

In each of the three cases, we have (Buchberger_Criteria). Thus, the necessity side of Theorem "*Almost*" has been proved. □

3.2. Necessity side of Theorem "But not quite"

In this section, we show (Chain_Condition) $\Longrightarrow$ (Extended_Criteria) for Theorem "*But not quite.*" We prove a separate lemma for each part of the conjunction: Lemma 11 for (EC_div), and Lemma 12 for (EC_var).

Lemma 11. *For $m = 3$, (Chain_Condition) $\Longrightarrow$ (EC_div).* $\diamond$

Proof. Assume (Chain_Condition). If $t_1 \mid t_2$, then $\gcd(t_1, t_3) \mid t_2$. The lemma follows immediately. Thus we assume that $t_1 \nmid t_2$. Let

$$\begin{aligned} f_1 &= t_1 + \gcd(t_1, t_2) \\ f_2 &= t_2 \\ f_3 &= t_3. \end{aligned}$$

Since $t_1 \nmid t_2$, the term $\gcd(t_1, t_2)$ is a proper factor of t_1. Hence f_1 is a binomial with $\text{lt}(f_1) = t_1$.

Note that $S_{f_2,f_3} = 0$. Thus it has the trivial representation $(0, 0, 0)$. In addition,

$$S_{f_1,f_2} = \frac{\text{lcm}(t_1, t_2)}{t_1} \cdot \gcd(t_1, t_2) = \frac{t_2}{\gcd(t_1, t_2)} \cdot \gcd(t_1, t_2) = f_2$$

so $S_{f_1,f_2} = 1 \cdot f_2$. Note that $(0, 1, 0)$ is a representation of S_{f_1,f_2} because

$$\text{lt}(1) \cdot \text{lt}(f_2) = 1 \cdot \text{lt}(f_2) \prec \text{lcm}(\text{lt}(f_1), \text{lt}(f_2)).$$

Since S_{f_1,f_2} and S_{f_2,f_3} both have representations modulo F, it follows from the chain condition that S_{f_1,f_3} also has a representation (h_1, h_2, h_3) modulo F such that

$$S_{f_1,f_3} = h_1 f_1 + h_2 f_2 + h_3 f_3.$$

By Lemma 9, there exists $k \geq 1$ such that $\tau_k = \text{lcm}(t_1, t_3)\left(\frac{\gcd(t_1,t_2)}{t_1}\right)^k$ appears in $h_2 f_2 + h_3 f_3$. We consider two cases.

Case 1: τ_k appears in $h_2 f_2$.

Then $t_2 \mid \text{lcm}(t_1, t_3)\left(\frac{\gcd(t_1,t_2)}{t_1}\right)^k$. Thus $\left(\frac{t_1}{\gcd(t_1,t_2)}\right)^k t_2 \mid \text{lcm}(t_1, t_3)$. Hence $t_2 \mid \text{lcm}(t_1, t_3)$.

Case 2: τ_k appears in $h_3 f_3$.

Then $t_3 \mid \text{lcm}(t_1, t_3)\left(\frac{\gcd(t_1,t_2)}{t_1}\right)^k$. Thus $\left(\frac{t_1}{\gcd(t_1,t_2)}\right)^k t_3 \mid \text{lcm}(t_1, t_3)$. Thus

$$\begin{aligned} \left(\frac{t_1}{\gcd(t_1, t_2)}\right)^k \frac{t_3 t_2}{\text{lcm}(t_1, t_3)} &\mid t_2 \\ \left(\frac{t_1}{\gcd(t_1, t_2)}\right)^k \frac{t_3 t_2 \gcd(t_1, t_3)}{t_1 t_3} &\mid t_2 \\ \left(\frac{t_1}{\gcd(t_1, t_2)}\right)^{k-1} \frac{t_1}{\gcd(t_1, t_2)} \frac{t_2}{t_1} \gcd(t_1, t_3) &\mid t_2 \\ \left(\frac{t_1}{\gcd(t_1, t_2)}\right)^{k-1} \frac{t_2}{\gcd(t_1, t_2)} \gcd(t_1, t_3) &\mid t_2. \end{aligned}$$

Hence $\gcd(t_1, t_3) \mid t_2$.

Thus, in each of the two cases, we have (EC_div). $\square$

Lemma 12. *For $m = 3$, (Chain_Condition) $\Longrightarrow$ (EC_var).* $\diamond$

Proof. Since (Chain_Condition) and (EC_var) are symmetric in t_1 and t_3, we may assume that $t_1 \succeq t_3$ without loss of generality. We proceed by contradiction, that is, we assume (Chain_Condition) and $\neg$(EC_var), and show that it will lead to a contradiction.

Let $F = (f_1, f_2, f_3)$ where

$$\begin{aligned} f_1 &= t_1 + u \\ f_2 &= t_2 \\ f_3 &= t_3 \end{aligned}$$

where u is the term such that for every variable x

$$\deg_x u = \begin{cases} \deg_x t_3 & \text{if } \deg_x t_2 \le \max(\deg_x t_1, \deg_x t_3); \\ \max(\deg_x t_1 + \deg_x t_3, \deg_x t_2) & \text{otherwise.} \\ \quad - \deg_x t_2 & \end{cases}$$

Note that $u \mid t_3$. Since we assumed $\neg$(EC_var), there is a variable x such that $\deg_x t_2 > \max(\deg_x t_1, \deg_x t_3)$ and $\min(\deg_x t_1, \deg_x t_3) > 0$. Thus $u \neq t_3$. It follows $u \prec t_3 \preceq t_1$, and f_1 is a binomial with $\operatorname{lt}(f_1) = t_1$.

Note that $S_{f_2,f_3} = 0$. Thus it has the trivial representation $(0, 0, 0)$. Note

$$S_{f_1,f_2} = \frac{\operatorname{lcm}(t_1, t_2)}{t_1} \cdot u = \frac{\operatorname{lcm}(t_1, t_2)}{t_1 t_3} \cdot u \cdot f_3 = q \cdot f_3.$$

where

$$q = \frac{\operatorname{lcm}(t_1, t_2)}{t_1 t_3} \cdot u.$$

We show that $(0, 0, q)$ is a representation of S_{f_1,f_2}.

Claim 1: q is a term.

Let x be any variable. If $\deg_x t_2 > \max(\deg_x t_1, \deg_x t_3)$, then

$$\begin{aligned} \deg_x q &= \deg_x t_2 - (\deg_x t_1 + \deg_x t_3) \\ &\quad + \max(\deg_x t_1 + \deg_x t_3, \deg_x t_2) - \deg_x t_2 \\ &\ge 0. \end{aligned}$$

If however $\deg_x t_2 \le \max(\deg_x t_1, \deg_x t_3)$, then

$$\begin{aligned} \deg_x q &= \max(\deg_x t_1, \deg_x t_2) - (\deg_x t_1 + \deg_x t_3) \\ &\quad + \deg_x t_3 \\ &\ge 0; \end{aligned}$$

Claim 2: $(0, 0, q)$ is a representation of S_{f_1,f_2}.

We only need to note

$$\operatorname{lt}(q) \cdot \operatorname{lt}(f_3) = \frac{\operatorname{lcm}(t_1, t_2)}{t_1 t_3} u t_3 \prec \frac{\operatorname{lcm}(t_1, t_2)}{t_1} \cdot t_1 = \operatorname{lcm}(t_1, t_2).$$

By the chain condition, S_{f_1,f_3} has a representation modulo F such that

$$S_{f_1,f_3} = h_1 f_1 + h_2 f_2 + h_3 f_3.$$

By Lemma 9, there exists $k \geq 1$ such that $\tau_k = \mathrm{lcm}\,(t_1, t_3) \left(\frac{u}{t_1}\right)^k$ appears in $h_2 f_2 + h_3 f_3$.

From now on let x stand for a variable such that $\deg_x t_2 > \max(\deg_x t_1, \deg_x t_3)$ and $\min(\deg_x t_1, \deg_x t_3) > 0$. Note that $\deg_x u = \max(\deg_x t_1 + \deg_x t_3, \deg_x t_2) - \deg_x t_2$. It is easy to verify that $\deg_x u < \min(\deg_x t_1, \deg_x t_3)$. Now we consider two cases.

Case 1: τ_k appears in $h_2 f_2$.

Then $t_2 \mid \mathrm{lcm}\,(t_1, t_3) \left(\frac{u}{t_1}\right)^k$. Thus we have

$$\deg_x t_2 \leq \max(\deg_x t_1, \deg_x t_3) + k(\deg_x u - \deg_x t_1) < \max(\deg_x t_1, \deg_x t_3),$$

which contradicts the fact that $\deg_x t_2 > \max(\deg_x t_1, \deg_x t_3)$.

Case 2: τ_k appears in $h_3 f_3$.

Then $t_3 \mid \mathrm{lcm}\,(t_1, t_3) \left(\frac{u}{t_1}\right)^k$. Thus we have

$$\deg_x t_3 \leq \max(\deg_x t_1, \deg_x t_3) + k(\deg_x u - \deg_x t_1).$$

When $\deg_x t_1 \leq \deg_x t_3$, we have $\deg_x t_3 \leq \deg_x t_3 + k(\deg_x u - \deg_x t_1)$. Thus

$$0 \leq k(\deg_x u - \deg_x t_1),$$

which contradicts the fact that $\deg_x u < \deg_x t_1$.

When $\deg_x t_1 > \deg_x t_3$, we have $\deg_x t_3 \leq \deg_x t_1 + k(\deg_x u - \deg_x t_1)$. Thus $\deg_x t_3 - \deg_x t_1 \leq k(\deg_x u - \deg_x t_1)$. Hence

$$\deg_x u - \deg_x t_1 < k(\deg_x u - \deg_x t_1),$$

which contradicts the fact that $\deg_x u < \deg_x t_1$.

We assumed (Chain_Condition) and ¬(EC_var), and found that this led to a contradiction. Hence (Chain_Condition) $\Longrightarrow$ (EC_var). □

Lemmas 11 and 12 show that (EC_div) and (EC_var) of Theorem "*But not quite*" are both necessary for the Chain Condition. Thus, the necessity side of Theorem "*But not quite*" has been proved.

3.3. Sufficiency side of Theorem "But not quite"

In this section, we show that (Chain_Condition) $\Longleftarrow$ (Extended_Criteria) for Theorem "*But not quite.*" We begin by listing two propositions about some elementary properties of leading terms under polynomial addition and multiplication. We will use them frequently without explicitly referring to them. The proofs are easy, so we omit them.

Proposition 13. *For all non-zero polynomials f, g, we have (A) and (B) and (C) where*
(A) If $f \pm g \neq 0$, then $\mathrm{lt}\,(f \pm g) \preceq \max_{\succ}\,(\mathrm{lt}\,(f)\,, \mathrm{lt}\,(g))$.
(B) $\mathrm{lt}\,(f \cdot g) = \mathrm{lt}\,(f) \cdot \mathrm{lt}\,(g)$.
(C) If $f \mid g$, then $\mathrm{lt}\,(f) \mid \mathrm{lt}\,(g)$. ◇

Proposition 14. *For all polynomials f_i, f_j such that $i \neq j$: (A)$\Longrightarrow$(B) where*
(A) S_{f_i,f_j} has the representation $(h_1, \ldots, h_m)$ modulo $(f_1, \ldots, f_m)$.
(B) $\operatorname{lm}\left(\sigma_{f_i,f_j} \pm h_i\right) = \sigma_{f_i,f_j}$ and $\operatorname{lm}\left(\sigma_{f_j,f_i} \pm h_j\right) = \sigma_{f_j,f_i}$. $\diamond$

Lemma 15 is a technical but crucial lemma, that will play an essential role in proving the sufficiency side of Theorem "*But not quite.*".

Lemma 15. *We have (A)$\Longleftarrow$(B) where*
(A) For every f_1, f_2, f_3 with $\operatorname{lt}(f_1) = t_1, \operatorname{lt}(f_2) = t_2, \operatorname{lt}(f_3) = t_3$:
if S_{f_1,f_2} and S_{f_2,f_3} have representations modulo (f_1, f_2, f_3),
then $\gcd(\operatorname{lt}(f_1), \operatorname{lt}(f_3)) = \operatorname{lt}(\gcd(f_1, f_3))$.
(B) (Extended_Criteria) and $t_2 \nmid \operatorname{lcm}(t_1, t_3)$ $\diamond$.

Proof. Assume (B). Let f_1, f_2, f_3 be arbitrary, but fixed. Assume S_{f_1,f_2} has the representation (h_1, h_2, h_3), and S_{f_2,f_3} has the representation (H_1, H_2, H_3), that is,

$$\sigma_{f_1,f_2} \cdot f_1 - \sigma_{f_2,f_1} \cdot f_2 = h_1 f_1 + h_2 f_2 + h_3 f_3$$
$$\sigma_{f_2,f_3} \cdot f_2 - \sigma_{f_3,f_2} \cdot f_3 = H_1 f_1 + H_2 f_2 + H_3 f_3$$

By eliminating f_2 from the above two equations and collecting expressions with f_1 and f_3 on opposite sides, we obtain

$$P \cdot f_1 = Q \cdot f_3$$

where

$$P = (\sigma_{f_2,f_3} - H_2) \cdot (\sigma_{f_1,f_2} - h_1) - (\sigma_{f_2,f_1} + h_2) \cdot H_1$$
$$Q = (\sigma_{f_2,f_1} + h_2) \cdot (\sigma_{f_3,f_2} + H_3) + (\sigma_{f_2,f_3} - H_2) \cdot h_3$$

Let $g = \gcd(f_1, f_3)$, $c_1 = f_1/g$, and $c_3 = f_3/g$. Then we have

$$P \cdot c_1 = Q \cdot c_3$$

Note that c_1 and c_3 are relatively prime. Thus $c_1 \mid Q$. Hence $\operatorname{lm}(c_1) \mid \operatorname{lm}(Q)$.

We claim that $\operatorname{lm}(Q) = \sigma_{f_2,f_1} \cdot \sigma_{f_3,f_2}$. In order to prove the claim, first observe that $Q = Q_1 + Q_2$ where

$$Q_1 = (\sigma_{f_2,f_1} + h_2) \cdot (\sigma_{f_3,f_2} + H_3)$$
$$Q_2 = (\sigma_{f_2,f_3} - H_2) \cdot h_3$$

and that

$$\operatorname{lm}(Q_1) = \sigma_{f_2,f_1} \cdot \sigma_{f_3,f_2}$$
$$\operatorname{lm}(Q_2) = \sigma_{f_2,f_3} \cdot \operatorname{lm}(h_3)$$

Note that

$$\operatorname{lm}(f_3) \operatorname{lm}(h_3) \prec \operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_2))$$
$$\frac{\operatorname{lcm}(\operatorname{lt}(f_2), \operatorname{lt}(f_3))}{\operatorname{lm}(f_2)} \cdot \operatorname{lm}(h_3) \prec \frac{\operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_2))}{\operatorname{lm}(f_2)} \cdot \frac{\operatorname{lcm}(\operatorname{lt}(f_2), \operatorname{lt}(f_3))}{\operatorname{lm}(f_3)}$$
$$\sigma_{f_2,f_3} \cdot \operatorname{lm}(h_3) \prec \sigma_{f_2,f_1} \cdot \sigma_{f_3,f_2}$$
$$\operatorname{lm}(Q_2) \prec \operatorname{lm}(Q_1)$$

Thus $\text{lm}(Q) = \text{lm}(Q_1 + Q_2) = \text{lm}(Q_1)$. We have proven the claim.

Recall that $\text{lm}(c_1) \mid \text{lm}(Q)$, so

$$\frac{\text{lm}(f_1)}{\text{lm}(g)} \mid \sigma_{f_2,f_1} \cdot \sigma_{f_3,f_2}.$$

From this, for every variable x, we have

$$\deg_x t_1 - \deg_x \text{lt}(g) \leq \max(\deg_x t_2, \deg_x t_1) - \deg_x t_2 + \max(\deg_x t_3, \deg_x t_2) - \deg_x t_3.$$

From condition (B)'s (EC_div), for every variable x, we have

$$\min(\deg_x t_1, \deg_x t_3) \leq \deg_x t_2.$$

From condition (B)'s (EC_var), for every variable x, we have

$$\deg_x t_1 = 0 \quad \text{or} \quad \deg_x t_3 = 0 \quad \text{or} \quad \deg_x t_2 \leq \max(\deg_x t_1, \deg_x t_3).$$

We claim that the above conditions imply that $\min(\deg_x t_1, \deg_x t_3) \leq \deg_x \text{lt}(g)$. If $\deg_x t_1 = 0$ or $\deg_x t_3 = 0$, then the claim is trivially true. Thus, assume that $\deg_x t_1 > 0$ and $\deg_x t_3 > 0$. Then we have

$$\min(\deg_x t_1, \deg_x t_3) \leq \deg_x t_2 \leq \max(\deg_x t_1, \deg_x t_3).$$

We consider two cases:

Case 1: $\deg_x t_1 \leq \deg_x t_3$.
Then we have $\deg_x t_1 \leq \deg_x t_2 \leq \deg_x t_3$, and thus

$$\deg_x t_1 - \deg_x \text{lt}(g) \leq \deg_x t_2 - \deg_x t_2 + \deg_x t_3 - \deg_x t_3.$$

Thus we have $\min(\deg_x t_1, \deg_x t_3) = \deg_x t_1 \leq \deg_x \text{lt}(g)$.

Case 2: $\deg_x t_3 \leq \deg_x t_1$.
Then we have $\deg_x t_3 \leq \deg_x t_2 \leq \deg_x t_1$, and thus

$$\deg_x t_1 - \deg_x \text{lt}(g) \leq \deg_x t_1 - \deg_x t_2 + \deg_x t_2 - \deg_x t_3$$

Thus we have $\min(\deg_x t_1, \deg_x t_3) = \deg_x t_3 \leq \deg_x \text{lt}(g)$.

Thus we have shown that $\min(\deg_x t_1, \deg_x t_3) \leq \deg_x \text{lt}(g)$ for every variable x, that is, $\gcd(t_1, t_3) \mid \text{lt}(g)$. It is trivial that $\text{lt}(g) \mid \gcd(t_1, t_3)$. Hence $\gcd(t_1, t_3) = \text{lt}(g)$. The Lemma has been proved. □

We now complete the proof of the sufficiency of the extended criteria.

Lemma 16. *For $m = 3$, (Chain_Condition) $\Longleftarrow$ (Extended_Criteria).* ◇

Proof. If $t_2 \mid \text{lcm}(t_1, t_3)$, then (Chain_Condition) follows immediately from Buchberger's theorem. Thus, from now on, assume that $t_2 \nmid \text{lcm}(t_1, t_3)$.

Let t_1, t_2, t_3 be arbitrary, but fixed. Assume that t_1, t_2, t_3 satisfy the Extended Criteria. Let f_1, f_2, f_3 be arbitrary, but fixed such that $\text{lt}(f_1) = t_1$, $\text{lt}(f_2) = t_2$, $\text{lt}(f_3) = t_3$. Assume that S_{f_1,f_2} and S_{f_2,f_3} have representations modulo (f_1, f_2, f_3). It remains to show that S_{f_1,f_3} has a representation modulo (f_1, f_2, f_3).

From Lemma 15,

$$\gcd(\text{lt}(f_1), \text{lt}(f_3)) = \text{lt}(\gcd(f_1, f_3)).$$

Note that

$$S_{f_1,f_3} = \frac{\operatorname{lcm}(t_1,t_3)}{\operatorname{lm}(f_1)} \cdot f_1 - \frac{\operatorname{lcm}(t_1,t_3)}{\operatorname{lm}(f_3)} \cdot f_3.$$

Let $g = \gcd(f_1, f_3)$, $c_1 = f_1/g$, and $c_3 = f_3/g$. Note that

$$\frac{\operatorname{lcm}(t_1,t_3)}{\operatorname{lm}(f_1)} = \frac{t_1t_3}{\operatorname{lm}(f_1)\gcd(t_1,t_3)} = \frac{t_1t_3}{\operatorname{lm}(f_1)\operatorname{lt}(g)} = \frac{\operatorname{lt}(c_3)}{\operatorname{lc}(f_1)} = \frac{\operatorname{lm}(c_3)}{\operatorname{lc}(c_3)\operatorname{lc}(c_1)\operatorname{lc}(g)}$$

$$\frac{\operatorname{lcm}(t_1,t_3)}{\operatorname{lm}(f_3)} = \frac{t_1t_3}{\operatorname{lm}(f_3)\gcd(t_1,t_3)} = \frac{t_1t_3}{\operatorname{lm}(f_3)\operatorname{lt}(g)} = \frac{\operatorname{lt}(c_1)}{\operatorname{lc}(f_3)} = \frac{\operatorname{lm}(c_1)}{\operatorname{lc}(c_1)\operatorname{lc}(c_3)\operatorname{lc}(g)}.$$

Observe that $-c_3f_1 + c_1f_3 = -\operatorname{lcm}(f_1,f_3) + \operatorname{lcm}(f_1,f_3) = 0$. Thus

$$\begin{aligned} S_{f_1,f_3} &= +\frac{\operatorname{lm}(c_3)}{\operatorname{lc}(c_3)\operatorname{lc}(c_1)\operatorname{lc}(g)} \cdot f_1 - \frac{\operatorname{lm}(c_1)}{\operatorname{lc}(c_1)\operatorname{lc}(c_3)\operatorname{lc}(g)} \cdot f_3 \\ &= -\frac{c_3 - \operatorname{lm}(c_3)}{\operatorname{lc}(c_3)\operatorname{lc}(c_1)\operatorname{lc}(g)} \cdot f_1 + \frac{c_1 - \operatorname{lm}(c_1)}{\operatorname{lc}(c_1)\operatorname{lc}(c_3)\operatorname{lc}(g)} \cdot f_3 \\ &= h_1f_1 + h_2f_2 + h_3f_3 \end{aligned}$$

where $h_1 = -\frac{c_3-\operatorname{lm}(c_3)}{\operatorname{lc}(c_3)\operatorname{lc}(c_1)\operatorname{lc}(g)}$ and $h_2 = 0$ and $h_3 = +\frac{c_1-\operatorname{lm}(c_1)}{\operatorname{lc}(c_1)\operatorname{lc}(c_3)\operatorname{lc}(g)}$. Note

$$\operatorname{lt}(h_1)\cdot\operatorname{lt}(f_1) \prec \operatorname{lt}(c_3)\cdot\operatorname{lt}(f_1) = \frac{t_3}{\operatorname{lt}(g)} \cdot t_1 = \frac{t_1t_3}{\gcd(t_1,t_3)} = \operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_3))$$

$$\operatorname{lt}(h_3)\cdot\operatorname{lt}(f_3) \prec \operatorname{lt}(c_1)\cdot\operatorname{lt}(f_3) = \frac{t_1}{\operatorname{lt}(g)} \cdot t_3 = \frac{t_1t_3}{\gcd(t_1,t_3)} = \operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_3)).$$

Thus (h_1, h_2, h_3) is a representation of S_{f_1,f_3}. Hence we have (Chain_Condition). Thus, the sufficiency side of Theorem "*But not quite*" has been proved. □

4. Remarks

4.1. Comparison with minimal generating sets of syzygy modules

It is well-known that the set of all S-polynomials (critical pairs) can be viewed essentially as a generating set of the syzygy module of the leading terms. Furthermore, it is also well-known that Buchberger's criteria essentially tell us that sometimes a proper subset of the set of all critical pairs generates the syzygy module, allowing us to skip the reduction of the remaining S-polynomials.

Since Theorem "*But not quite*" shows that we can sometimes skip an additional S-polynomial reduction, one wonders whether this new criterion corresponds to minimal generating sets of syzygy modules, where by "minimal" we mean that no proper subset generates the module (Caboara et al., 2002).

The answer is, not always, as the following example illustrates. Consider the following three terms:

$$x_0x_1,\ x_0x_2,\ x_0x_3.$$

Obviously, the syzygy module of the terms is generated by the following syzygies corresponding to the S-polynomials

$$\Sigma_{12} = \begin{pmatrix} x_2 \\ -x_1 \\ 0 \end{pmatrix},\ \Sigma_{23} = \begin{pmatrix} 0 \\ x_3 \\ -x_2 \end{pmatrix},\ \Sigma_{13} = \begin{pmatrix} x_3 \\ 0 \\ -x_1 \end{pmatrix}.$$

Inspection shows that the set $\mathcal{S} = \{\Sigma_{12}, \Sigma_{23}, \Sigma_{13}\}$ is a minimal set of generators. However, Theorem "*But not quite*" shows that the terms satisfy the chain condition. Thus, we could skip an S-polynomial reduction that would not be discovered by computing a minimal set of generators of the sygyzy module.

4.2. New questions

Theorems "*Almost*" and "*But not quite*" fix the number of leading terms at three. We saw in Example 8 that this makes it difficult to apply Theorem "*But not quite*" in many situations. It is well-known that Buchberger's lcm criterion can be generalized to more than three leading terms. Do Theorems "*Almost*" and "*But not quite*" generalize to more than three leading terms? If so, how? It turns out that Theorem "*Almost*" has a natural generalization. We do not yet know how Theorem "*But not quite*" generalizes, and are currently pursuing the solution to this problem.

Other questions follow from asking how the additional criterion presented in this paper could help an algorithm to compute a Gröbner basis. First, does the new criterion suggest a different strategy for selecting critical pairs while computing a Gröbner basis? Second, how many additional S-polynomial reductions could we expect to skip on average? At this time, we have only preliminary answers to these questions.

Acknowledgements

The authors would like to thank Bruno Buchberger, Erich Kaltofen, and Volker Weispfenning and his colleagues at the University of Passau for interesting and helpful discussions related to this problem, especially regarding the second and third questions in section 4.2. We also wish to thank the anonymous reviewers for their comments.

References

Adams, W., Loustaunau, P., 1994. An Introduction to Gröbner Bases. Vol. 3 of Graduate studies in mathematics. American Mathematical Society, Providence, R.I.

Becker, T., Weispfenning, V., Kredel, H., 1993. Gröbner Bases: a Computational Approach to Commutative Algebra. Springer-Verlag New York, Inc., New York.

Buchberger, B., 1965. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (an algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal). Ph.D. thesis, Mathematical Insitute, University of Innsbruck, Austria, English translation to appear in the Journal of Symbolic Computation.

Buchberger, B., 1979. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In: Ng, E. W. (Ed.), Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation, Marseille, June 26-28, 1979. Vol. 72 of Lecture Notes in Computer Science. Springer, Berlin - Heidelberg - New York, pp. 3–21.

Buchberger, B., 1985. Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. In: Bose, N. K. (Ed.), Multidimensional Systems Theorey - Progress, Directions and Open Problems in Multidimensional Systems, 1985. Reidel Publishing Company, Dotrecht, pp. 184–232.

Caboara, M., Kreuzer, M., Robbiano, L., 2002. Minimal sets of critical pairs. In: Cohen, B., Gao, X., Takayama, N. (Eds.), Proceedings of the First Congress of Mathematical Software. World Scientific, pp. 390–404.

Cox, D., Little, J., O'Shea, D., 1997. Ideals, Varieties, and Algorithms, 2nd Edition. Springer-Verlag New York, Inc., New York.

Cox, D., Little, J., O'Shea, D., 1998. Using Algebraic Geometry. Springer-Verlag New York, Inc., New York.

Fröberg, R., 1997. An Introduction to Gröbner Bases. John Wiley & Sons, Chichester, New York.

Gebauer, R., Möller, H. On an Installation of Buchberger's Algorithm. Journal of Symbolic Computation vol. 6, 1988, pp. 275–286.

Kollreider, C., Buchberger, B., 1978. An Improved Algorithmic Construction of Gröbner Bases for Polynomial Ideals. ACM SIGSAM Bulletin vol. 12 no. 2, May 1978, pp. 27–36.

Kreuzer, M., Robbiano, L., 2000. Computational Commutative Algebra I. Springer-Verlag, Heidelberg.

Perry, J., 2005. Combinatorial criteria for Gröbner bases. Ph.D. thesis, North Carolina State University at Raleigh, United States.