A NEW COMBINATORIAL CRITERION FOR GRÖBNER BASES

HOON HONG AND JOHN PERRY

ABSTRACT. An awesome abstract will go here.

1. INTRODUCTION

Bruno Buchberger introduced Gröbner bases in his 1965 PhD thesis [2]. Computation of Gröbner bases requires one to check whether S-polynomials reduce to zero. Reduction is a computationally expensive process, so one would like to avoid it whenever possible. If we know *a priori* that the S-polynomial reduces to zero, then of course we can skip its reduction.

Starting with Bruno Buchberger, several investigators [1, 2, 3, 5, 6] have discovered important *a priori* criteria or methods for skipping S-polynomial reduction. These criteria (and methods) can be divided into two kinds. One kind [5] uses both the exponents and the coefficients, while the other [1, 2, 3, 6] uses only the exponents (in fact, only the leading exponents, that is, the exponents of the leading terms). Since the exponents are natural numbers, we will refer to these criteria as *combinatorial*. Obviously, combinatorial criteria might not detect some S-polynomial reductions that could have been skipped if we also considered the coefficients. However, we can check combinatorial criteria with an ease and a speed that makes them appealling.

The question arises naturally:

Are the known combinatorial criteria "complete"?

By "complete", we mean that the criterion makes maximal use of the information from the leading exponents. In other words, if some exponents do not satisfy the criteria, then there is at least one polynomial system with those leading exponents where one cannot skip S-polynomial reduction.

The answer to the question is *no*. We show that Buchberger's two criteria are *not* complete: they miss cases where the information from the leading terms allows us to skip an S-polynomial reduction. We provide a new combinatorial criterion for skipping an S-polynomial reduction, and we show that this new criterion *is* complete for a system of three polynomials. The complete criterion for four or more polynomials remains an open problem.

2. MAIN THEOREM

All polynomials and monomials are from a ring $\mathbb{F}[x_1, \ldots, x_n]$, where $\mathbb{F}$ is a field. We follow the convention of Cox, Little and O'Shea in [4] that a **"monomial"** includes a coefficient, while a **"term"** does not. For any fixed term ordering $\succ$, and for polynomials p, f, r, and $f_1, \ldots, f_m$, we write $\mathrm{lt}_\succ(f)$ for the leading term of f, $\mathrm{lm}_\succ(f)$ for the leading monomial of f, and $\mathrm{lc}_\succ(f)$ for the leading coefficient of f. Observe that $\mathrm{lm}_\succ(f) = \mathrm{lc}_\succ(f) \cdot \mathrm{lt}_\succ(f)$.

We call the **S-polynomial** of f_i and f_j

$$S(f_i, f_j) := \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_i), \mathrm{lt}_\succ(f_j))}{\mathrm{lm}_\succ(f_i)} \cdot f_i - \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_i), \mathrm{lt}_\succ(f_j))}{\mathrm{lm}_\succ(f_j)} \cdot f_j$$

For the sake of convenience, we write S_{ij} for $S(f_i, f_j)$ (only if the polynomials are in fact f_i, f_j) and

$$\sigma_{ij} := \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_i), \mathrm{lt}_\succ(f_j))}{\mathrm{lm}_\succ(f_i)}$$

Hence $S_{ij} = \sigma_{ij} \cdot f_i - \sigma_{ji} \cdot f_j$.

The first results in skipping S-polynomial reduction are Buchberger's two combinatorial criteria:

2000 *Mathematics Subject Classification.* Primary: 68W30; Secondary: 13P10.

Key words and phrases. Gröbner bases, leading terms, Buchberger criteria, combinatorial criteria.

Research was supported in part by NSF grant 53344.

$$\begin{aligned} \mathrm{BC1}\left(t_i, t_j\right) &:= \gcd\left(t_i, t_j\right) = 1 \\ \mathrm{BC2}\left(t_i, t_j, t_k\right) &:= t_j \mid \mathrm{lcm}\left(t_i, t_k\right) \end{aligned}$$

We have the following two well-known lemmas. A proof of the first is in [2]; a proof of the second is in [1].

Lemma 1 (Buchberger's First Criterion)**.** For all terms t_i, t_j (A)⇒(B) where
(A) $\mathrm{BC1}\left(t_i, t_j\right)$
(B) $S_{ij} \underset{(f_1,\ldots,f_m)}{\overset{*}{\longrightarrow}} 0 \qquad \forall \left(f_1, \ldots, f_m\right)$ such that $\mathrm{lt}_{\succ}\left(f_i\right) = t_i$, $\mathrm{lt}_{\succ}\left(f_j\right) = t_j$.

Lemma 2 (Buchberger's Second Criterion)**.** For all terms t_i, t_j, t_k (A)⇒(B) where
(A) $\mathrm{BC2}\left(t_1, t_2, t_3\right)$
(B) $S_{12} \underset{(f_1,\ldots,f_m)}{\overset{*}{\longrightarrow}} 0 \ \wedge\ S_{23} \underset{(f_1,\ldots,f_m)}{\overset{*}{\longrightarrow}} 0 \quad \Rightarrow \quad S_{13} \underset{(f_1,\ldots,f_m)}{\overset{*}{\longrightarrow}} 0 \qquad \forall \left(f_1, f_2, f_3\right) : \forall k\ \mathrm{lt}_{\succ}\left(f_k\right) = t_k$

To our knowledge, the only other *combinatorial* criteria that allow us to skip S-polynomial reduction are Buchberger's two combinatorial criteria. We recall the question, *Are the known combinatorial criteria complete?* The answer to this question is no, as theorem 1 demonstrates.

Let us consider a "weaker version" of BC1 and BC2:

$$\begin{aligned} \mathrm{VB1}_x\left(t_1, t_3\right) &:= \deg_x t_1 = 0 \text{ or } \deg_x t_3 = 0 \\ \mathrm{VB2}_x\left(t_1, t_2, t_3\right) &:= \deg_x t_2 \leq \max\left(\deg_x t_1, \deg_x t_3\right) \end{aligned}$$

Observe that VB1 and VB2 define conditions that we can call "variable-wise" BC1 and "variable-wise" BC2, respectively.

Now we can define the complete criterion for skipping one S-polynomial reduction in a system of three polynomials:

Theorem 1 (A new combinatorial criterion)**.** (A) $\quad\Leftrightarrow\quad$ [(B) ∧ (C)] where
(A) $\mathrm{CC}\left(t_1, t_2, t_3, \succ, \left\{(1,2), (2,3)\right\}\right)$
(B) $\gcd\left(t_1, t_3\right) \mid t_2 \vee \mathrm{BC2}\left(t_1, t_2, t_3\right)$
(C) $\mathrm{VB1}_x\left(t_1, t_3\right) \vee \mathrm{VB2}_x\left(t_1, t_2, t_3\right)\ \forall x \in \left\{x_1, \ldots, x_m\right\}$

The theorem shows that we can skip the reduction of S_{13} even when the previously known combinatorial criteria fail: see example 1 of section 4.1 for a concrete example. However, one has to pay close attention to the quantifiers: see example 2 of section 4.2 for an example of how easily this can be misunderstood.

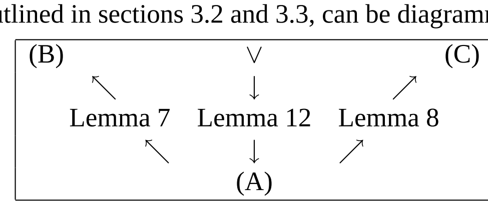
Of course, this new criterion is consistent with the previous criteria; part (B) of any one of lemmas 1 or 2 will imply (B) ∧ (C) of theorem 1.

3. Proof of main theorem

For convenience, we write CC for (B) ∨ (C) of theorem 1; that is,

$$\mathrm{CC} = \begin{cases} \gcd\left(t_1, t_3\right) \mid t_2 \ \vee\ \mathrm{BC2}\left(t_1, t_2, t_3\right) \\ \\ \mathrm{VB1}_x\left(t_1, t_3\right) \ \vee\ \mathrm{VB2}_x\left(t_1, t_2, t_3\right) \quad \forall x \in \left\{x_1, \ldots, x_m\right\} \end{cases}$$

The structure of the proof, as outlined in sections 3.2 and 3.3, can be diagrammed as follows.



3.1. **Useful facts.** We begin the proof with a brief review of what we mean by *reduction*:

- $p \underset{f}{\longrightarrow} r$ if there exists a monomial q and a monomial d of p such that $q \cdot \mathrm{lm}_{\succ}\left(f\right) = d$ and $r = p - qf$
- $p \underset{f}{\not\rightarrow}$ if $\neg\exists r$ such that $p \underset{f}{\longrightarrow} r$

- $p \underset{(f_1,\ldots,f_m)}{\overset{*}{\longrightarrow}} r$ if $\exists \mu \in \mathbb{N}$, $\exists i_1, \ldots i_\mu \in \{1, \ldots, m\}$, and there exist polynomials $p_0, \ldots, p_\mu$ such that
$$p = p_0 \underset{f_{i_1}}{\longrightarrow} p_1 \underset{f_{i_2}}{\longrightarrow} p_2 \cdots \underset{f_{i_\mu}}{\longrightarrow} p_\mu = r$$
In this case, we say p **reduces to** r modulo $(f_1, \ldots, f_m)$.

A proof of lemma 3 is found in [7], at the website of the second author. We use it to create counterexamples. The application of lemma 3 usually requires a permutation on the indices of the polynomials $f_1, \ldots, f_m$. We do not write this out explicitly, but it is usually evident.

Lemma 3. Let τ be a nonzero monomial, and $F = (f_1, \ldots, f_m)$ a system of polynomials. Then (A)⇒(B) where

(A) $\exists \mu$ with $1 \le \mu \le m$ such that (A1)∧(A2) where

(A1) $\forall \ell = 1, \ldots, \mu\ \exists \lambda_1, \ldots, \lambda_\mu$ such that
$\deg_{x_{\lambda_\ell}} \operatorname{lm}_\succ(f_\ell) > \deg_{x_{\lambda_\ell}} \tau$

(A2) $\forall \ell = \mu + 1, \ldots, m$
$f_\ell = t_\ell + u_\ell$
$t_\ell \succ u_\ell$
$\deg_{x_{\lambda_i}} t_\ell \ge \deg_{x_{\lambda_i}} u_\ell\ \forall i = 1, \ldots, \mu$

(B) $\tau \underset{F}{\overset{*}{\not\to}} 0$.

We also resort to the following facts. Their proofs are not difficult, so we omit them.

Remark 1. The following are equivalent for all terms t_1, t_2, t_3:
(a) $\gcd(t_1, t_3) \mid t_2$
(b) $\gcd(t_1, t_3) \mid \gcd(t_1, t_2)$
(c) $\gcd(t_1, t_3) \mid \gcd(t_2, t_3)$

Remark 2. For all polynomials f, g we have the following:
- $\operatorname{lt}_\succ(f \pm g) \preceq \max_\succ(\operatorname{lt}_\succ(f), \operatorname{lt}_\succ(g))$
- $\operatorname{lt}_\succ(f \cdot g) = \operatorname{lt}_\succ(f) \cdot \operatorname{lt}_\succ(g)$

Remark 3. For all polynomials f_i, f_j with $i \ne j$, the leading monomials of $\sigma_{ij} f_i$ and $\sigma_{ji} f_j$ cancel, so that $\operatorname{lt}_\succ(S_{ij}) \prec \operatorname{lcm}(\operatorname{lt}_\succ(f_i), \operatorname{lt}_\succ(f_j))$.

Remark 4. For any fixed term ordering $\succ$, consider a reduction chain
$$p = p_0 \underset{f_{i_1}}{\longrightarrow} p_1 \underset{f_{i_2}}{\longrightarrow} p_2 \cdots \underset{f_{i_\mu}}{\longrightarrow} p_\mu = r$$
For this chain, we collect
$$h_k = \sum_{p_{j+1} = p_j - u f_k} u$$
Then
$$p - r = \sum_{k=1}^{m} h_k f_k \tag{3.1}$$
Note that $\forall k = 1, \ldots, m$, if $h_k \ne 0$, then from remark 3 we have $\operatorname{lt}_\succ(h_k f_k) \preceq \operatorname{lt}_\succ(p)$. In the case where $p = S_{ij}$, this implies that
$$\forall k \quad h_k \ne 0 \qquad \Rightarrow \qquad \operatorname{lt}_\succ(h_k f_k) \preceq \operatorname{lt}_\succ(S_{ij}) \prec \operatorname{lcm}(\operatorname{lt}_\succ(f_i), \operatorname{lt}_\succ(f_j)) \tag{3.2}$$
However, it is not always the case that if we can satisfy 3.1 for two polynomials p, r, then $p \underset{F}{\overset{*}{\longrightarrow}} r$. An example of where it *is* true is provided in lemma 5.

Remark 5. For all f_i and f_j where $\operatorname{BC1}(\operatorname{lt}_\succ(f_i), \operatorname{lt}_\succ(f_j))$,
$$S_{ij} = \mathcal{H}_i c_i + \mathcal{H}_j c_j$$
where
$$\mathcal{H}_i = -(c_j - \operatorname{lm}_\succ(c_j)) \qquad \mathcal{H}_j = c_i - \operatorname{lm}_\succ(c_i)$$

Lemma 4. For all $i \neq j$ (A)⇒(B) where
(A) $S_{ij} = h_1 f_1 + \cdots + h_m f_m$ such that $\forall k = 1, \ldots, m$ $\mathrm{lt}_\succ (h_k f_k) \preceq \mathrm{lt}_\succ (S_{ij})$
(B) $\mathrm{lt}_\succ ((\sigma_{ij} \pm h_i)) = \mathrm{lt}_\succ (\sigma_{ij})$ and $\mathrm{lt}_\succ ((\sigma_{ji} \pm h_j)) = \mathrm{lt}_\succ (\sigma_{ji})$

Proof. Let $i \neq j$ be arbitrary, but fixed.
Assume (A).
The statement of (B) is equivalent to $\mathrm{lt}_\succ (\sigma_{ij}) \succ \mathrm{lt}_\succ (h_i)$ and $\mathrm{lt}_\succ (\sigma_{ji}) \succ \mathrm{lt}_\succ (h_j)$.
By way of contradiction, assume

$$\mathrm{lt}_\succ (\sigma_{ij}) \preceq \mathrm{lt}_\succ (h_i)$$

Then

$$\begin{aligned}
\frac{\mathrm{lcm}\left(\mathrm{lt}_\succ (f_i), \mathrm{lt}_\succ (f_j)\right)}{\mathrm{lt}_\succ (f_i)} &\preceq \mathrm{lt}_\succ (h_i) \\
\mathrm{lcm}\left(\mathrm{lt}_\succ (f_i), \mathrm{lt}_\succ (f_j)\right) &\preceq \mathrm{lt}_\succ (h_i)\, \mathrm{lt}_\succ (f_i) = \mathrm{lt}_\succ (h_i f_i)
\end{aligned}$$

This contradicts (A) (see (3.2)).
Hence $\mathrm{lt}_\succ (\sigma_{ij}) \succ \mathrm{lt}_\succ (h_i)$.
That $\mathrm{lt}_\succ (\sigma_{ji}) \succ \mathrm{lt}_\succ (h_j)$, is proved similarly. □

The proof of lemma 5 below is somewhat tedious, so we do not reproduce it here. A key ingredient of the proof is that every syzygy of the leading terms can be written in terms of S-polynomials. This lemma is crucial for lemma 12.

Lemma 5. For all f_i, f_j, (A)⇔(B) where
(A) $S_{ij} = h_i f_i + h_j f_j$ $\exists h_i, h_j$, and $\forall k = i, j$

$$h_k \neq 0 \quad \Rightarrow \quad \mathrm{lt}_\succ (h_k f_k) \prec \mathrm{lcm}\left(\mathrm{lt}_\succ (f_i), \mathrm{lt}_\succ (f_j)\right)$$

(B) $S_{ij} \underset{(f_i, f_j)}{\longrightarrow} 0$

Lemma 6 will allow us to draw a connection between the reduction of an S-polynomial for polynomials f_1, f_2, f_3 and the reduction of the corresponding S-polynomials c_1, c_2, c_3, which are cofactors of the greatest common divisor of f_1, f_2, f_3. This lemma is crucial for lemma 12.

Lemma 6. For all $F = (f_1, f_2, f_3)$ if $\exists g, c_k$ such that $\forall k$ $f_k = g c_k$, then $\forall h_1, h_2, h_3$ the following are equivalent:
(A) $S(f_i, f_j) = h_1 f_1 + h_2 f_2 + h_3 f_3$ and $h_k \neq 0$ implies $\mathrm{lt}_\succ (h_k f_k) \prec \mathrm{lcm}\left(\mathrm{lt}_\succ (f_i), \mathrm{lt}_\succ (f_j)\right)$
(B) $S(c_i, c_j) = \mathcal{H}_1 c_1 + \mathcal{H}_2 c_2 + \mathcal{H}_3 c_3$ where $\mathcal{H}_k = \mathrm{lc}_\succ (g) \cdot h_k$ and $\mathcal{H}_k \neq 0$ implies $\mathrm{lt}_\succ (\mathcal{H}_k c_k) \prec \mathrm{lcm}\left(\mathrm{lt}_\succ (c_j), \mathrm{lt}_\succ (c_j)\right)$

Proof. Let $\succ$ be arbitrary, but fixed.
Let F be arbitrary, but fixed.
Assume that $\forall k$ $\exists g, c_k$ such that $f_k = g c_k$.
Let $i \neq j$ be arbitrary, but fixed.
Then $\forall h_1, h_2, h_3$

$$\begin{aligned}
S(f_i, f_j) &= h_1 f_1 + h_2 f_2 + h_3 f_3 \\
&\Updownarrow \\
\frac{\mathrm{lcm}\left(\mathrm{lt}_\succ (f_i), \mathrm{lt}_\succ (f_j)\right)}{\mathrm{lm}_\succ (f_i)} \cdot f_i - \frac{\mathrm{lcm}\left(\mathrm{lt}_\succ (f_i), \mathrm{lt}_\succ (f_j)\right)}{\mathrm{lm}_\succ (f_j)} \cdot f_j &= h_1 f_1 + h_2 f_2 + h_3 f_3 \\
&\Updownarrow \\
g \cdot \left(\frac{\mathrm{lcm}\left(\mathrm{lt}_\succ (g c_i), \mathrm{lt}_\succ (g c_j)\right)}{\mathrm{lm}_\succ (g c_i)} \cdot c_i - \frac{\mathrm{lcm}\left(\mathrm{lt}_\succ (g c_i), \mathrm{lt}_\succ (g c_j)\right)}{\mathrm{lm}_\succ (g c_j)} c_j \right) &= g \cdot (h_1 c_1 + h_2 c_2 + h_3 c_3) \\
&\Updownarrow \\
\frac{\mathrm{lt}_\succ (g) \cdot \mathrm{lcm}\left(\mathrm{lt}_\succ (c_i), \mathrm{lt}_\succ (c_j)\right)}{\mathrm{lm}_\succ (g) \cdot \mathrm{lm}_\succ (c_i)} \cdot c_i - \frac{\mathrm{lt}_\succ (g) \cdot \mathrm{lcm}\left(\mathrm{lt}_\succ (c_i), \mathrm{lt}_\succ (c_j)\right)}{\mathrm{lm}_\succ (g) \cdot \mathrm{lm}_\succ (c_j)} c_j &= h_1 c_1 + h_2 c_2 + h_3 c_3 \\
&\Updownarrow \\
\frac{1}{\mathrm{lc}_\succ (g)} \cdot \left(\frac{\mathrm{lcm}\left(\mathrm{lt}_\succ (c_i), \mathrm{lt}_\succ (c_j)\right)}{\mathrm{lm}_\succ (c_i)} \cdot c_i - \frac{\mathrm{lcm}\left(\mathrm{lt}_\succ (c_i), \mathrm{lt}_\succ (c_j)\right)}{\mathrm{lm}_\succ (c_j)} c_j \right) &= h_1 c_1 + h_2 c_2 + h_3 c_3 \\
&\Updownarrow \\
S(c_i, c_j) &= \mathcal{H}_1 c_1 + \mathcal{H}_2 c_2 + \mathcal{H}_3 c_3
\end{aligned}$$

Moreover, for any k, if $h_k \neq 0$ then

$$\begin{array}{rcl} \mathrm{lt}_{\succ}(f_k h_k) & \prec & \mathrm{lcm}(\mathrm{lt}_{\succ}(f_i), \mathrm{lt}_{\succ}(f_j)) \\ & \Updownarrow & \\ \mathrm{lt}_{\succ}(f_k)\,\mathrm{lt}_{\succ}(h_k) & \prec & \mathrm{lcm}(\mathrm{lt}_{\succ}(f_i), \mathrm{lt}_{\succ}(f_j)) \\ & \Updownarrow & \\ \mathrm{lt}_{\succ}(gc_k)\,\mathrm{lt}_{\succ}(h_k) & \prec & \mathrm{lcm}(\mathrm{lt}_{\succ}(gc_i), \mathrm{lt}_{\succ}(gc_j)) \\ & \Updownarrow & \\ \mathrm{lt}_{\succ}(g)\,\mathrm{lt}_{\succ}(c_k)\,\mathrm{lt}_{\succ}(h_k) & \prec & \mathrm{lt}_{\succ}(g)\cdot\mathrm{lcm}(\mathrm{lt}_{\succ}(c_i), \mathrm{lt}_{\succ}(c_j)) \\ & \Updownarrow & \\ \mathrm{lt}_{\succ}(c_k h_k) & \prec & \mathrm{lcm}(\mathrm{lt}_{\succ}(c_i), \mathrm{lt}_{\succ}(c_j)) \end{array}$$

Clearly $\mathrm{lt}_{\succ}(h_k) = \mathrm{lt}_{\succ}(\mathcal{H}_k)$, so

$$\mathrm{lt}_{\succ}(c_k \mathcal{H}_k) \prec \mathrm{lcm}(\mathrm{lt}_{\succ}(c_i), \mathrm{lt}_{\succ}(c_j))$$

From the preceding, we have the equivalence

$$\begin{array}{rcl} S(f_i, f_j) & = & h_1 f_1 + h_2 f_2 + h_3 f_3 \\ & \Updownarrow & \\ S(c_i, c_j) & = & \mathcal{H}_1 c_1 + \mathcal{H}_2 c_2 + \mathcal{H}_3 c_3 \end{array}$$

and for each $k = 1, 2, 3$ we have the equivalence

$$\begin{array}{rcl} \mathrm{lt}_{\succ}(f_k h_k) & \prec & \mathrm{lcm}(\mathrm{lt}_{\succ}(f_i), \mathrm{lt}_{\succ}(f_j)) \\ & \Updownarrow & \\ \mathrm{lt}_{\succ}(c_k \mathcal{H}_k) & \prec & \mathrm{lcm}(\mathrm{lt}_{\succ}(c_i), \mathrm{lt}_{\succ}(c_j)) \end{array}$$

The statement of the lemma follows from these two equivalences. □

Three final remarks useful in the proof:

Remark 6. For all polynomials f_i, f_j with $i \neq j$

$$\sigma_{ij} = \frac{\mathrm{lcm}(\mathrm{lt}_{\succ}(f_i), \mathrm{lt}_{\succ}(f_j))}{\mathrm{lm}_{\succ}(f_i)} = \frac{\mathrm{lt}_{\succ}(f_i)\cdot\mathrm{lt}_{\succ}(f_j)}{\mathrm{lm}_{\succ}(f_i)\gcd(\mathrm{lt}_{\succ}(f_i), \mathrm{lt}_{\succ}(f_j))} = \frac{\mathrm{lt}_{\succ}(f_j)}{\mathrm{lc}_{\succ}(f_i)\gcd(\mathrm{lt}_{\succ}(f_i), \mathrm{lt}_{\succ}(f_j))}$$

Remark 7. $\forall i \neq j \; \gcd(\mathrm{lt}_{\succ}(\sigma_{ij}), \mathrm{lt}_{\succ}(\sigma_{ji})) = 1$

Remark 8. For any term ordering $\succ$ and for any two polynomials f_i, f_j, if $g \mid f_i$ and $g \mid f_j$, then $\mathrm{lt}_{\succ}(g) \mid \mathrm{lt}_{\succ}(f_i)$ and $\mathrm{lt}_{\succ}(g) \mid \mathrm{lt}_{\succ}(f_j)$. So if $\mathrm{lt}_{\succ}(f_i)$ and $\mathrm{lt}_{\succ}(f_j)$ are relatively prime, f_i and f_j have no nontrivial common factors.

3.2. **Necessity of criterion for three polynomials.** In this section, we show that we can skip the reduction of S_{13} only if CC3 holds true. We do this by showing the contrapositive: if CC3 is false, then we have to check the reduction of S_{13} explicitly. We demonstrate this by producing an $F = (f_1, f_2, f_3)$ whose leading terms are t_1, t_2, t_3, and which has the property that $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$, but $S_{13} \overset{*}{\underset{F}{\not\to}} 0$.

We treat two different cases: one if the first clause of CC3 is false (lemma 7); the other, if its second clause is false (lemma 8).

We use a form suggested by lemma 3 where $f_1 = t_1 + u$, $f_2 = t_2$, and $f_3 = t_3$. In our first approach, we arrange for $S_{12} \xrightarrow[f_2]{} 0$. Per remark 6,

$$S_{12} \;=\; \frac{t_2}{\gcd(t_1, t_2)} \cdot u$$

The simplest way to get $S_{12} \xrightarrow[f_2]{} 0$ is if $u_1 = \gcd(t_1, t_2)$. That $S_{23} \xrightarrow[F]{*} 0$ is trivial.

How then will we ensure that $S_{13} \overset{*}{\underset{F}{\not\to}} 0$? This will depend on some “magical properties” of u. These properties exploit the facts that $t_2 \nmid \mathrm{lcm}(t_1, t_3)$ *and* $\gcd(t_1, t_3) \nmid t_2$ (hence $\gcd(t_1, t_3) \nmid \gcd(t_1, t_2)$).

Lemma 7. For all terms t_1, t_2, t_3 (A)$\Leftarrow$(B) where

(A) $\gcd(t_1, t_3) \mid t_2$ or $\mathrm{BC2}(t_1, t_2, t_3)$

(B) $\left[S_{12} \xrightarrow[F]{*} 0 \quad \wedge \quad S_{23} \xrightarrow[F]{*} 0\right] \quad \Rightarrow \quad S_{13} \xrightarrow[F]{*} 0 \qquad \forall F = (f_1, f_2, f_3) : \forall k \ \mathrm{lt}_{\succ}(f_k) = t_k$

Proof. We show (A)$\Leftarrow$(B) by proving its contrapositive.

Assume $\neg$(A): $\gcd(t_1, t_3) \nmid t_2$ and $\neg\mathrm{BC2}(t_1, t_2, t_3)$.

We will construct F to show $\neg$(B).

Let $F = (f_1, f_2, f_3)$ be such that

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

We need to show that f_1 is a binomial, and $\mathrm{lt}_{\succ}(f_1) = t_1$.

Since $\gcd(t_1, t_2) \mid t_1$, we have $\gcd(t_1, t_2) \preceq t_1$.

It remains to show that $\gcd(t_1, t_2) \neq t_1$. By way of contradiction:

$\gcd(t_1, t_2) = t_1 \quad \Rightarrow \quad t_1 \mid t_2 \quad \Rightarrow \quad \gcd(t_1, t_3) \mid t_2$

But $\neg$(A) has $\gcd(t_1, t_3) \nmid t_2$.

So $\gcd(t_1, t_2) \neq t_1$.

Hence $\gcd(t_1, t_2) \prec t_1$.

Hence f_1 is a binomial, and $\mathrm{lt}_{\succ}(f_1) = t_1$.

We claim $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$ but $S_{13} \not\xrightarrow[F]{*} 0$.

From the construction of F

$$S_{23} = 0$$

Also

$$\begin{aligned} S_{12} &= \frac{\mathrm{lcm}(t_1, t_2)}{t_1} \cdot (t_1 + u) - \frac{\mathrm{lcm}(t_1, t_2)}{t_2} \cdot t_2 \\ &= \frac{t_2}{\gcd(t_1, t_2)} \cdot \gcd(t_1, t_2) \\ &= f_2 \end{aligned}$$

So $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$.

Consider

$$\begin{aligned} S_{13} &= \frac{\mathrm{lcm}(t_1, t_3)}{t_1} \cdot (t_1 + u) - \frac{\mathrm{lcm}(t_1, t_3)}{t_3} \cdot t_3 \\ &= \frac{t_3}{\gcd(t_1, t_3)} \cdot u \end{aligned}$$

We claim that $t_2 \nmid S_{13}$.

Assume by way of contradiction that $t_2 \mid S_{13}$.

Then

$$t_2 \mid \frac{t_3}{\gcd(t_1, t_3)} \cdot \gcd(t_1, t_2)$$

This implies that

$$t_2 \mid \frac{t_3}{\gcd(t_1, t_3)} \cdot t_1$$

Then

$$t_2 \mid \mathrm{lcm}(t_1, t_3)$$

This contradicts $t_2 \nmid \mathrm{lcm}(t_1, t_3)$.

Hence $t_2 \nmid S_{13}$.

We further claim that $t_3 \nmid S_{13}$.

Assume by way of contradiction that $t_3 \mid S_{13}$.

Then $\gcd(t_1, t_3) \mid u$.

Since $u = \gcd(t_1, t_2)$, we have $\gcd(t_1, t_3) \mid \gcd(t_1, t_2)$.

This contradicts $\gcd(t_1, t_3) \nmid t_2$.

Hence $t_3 \nmid S_{13}$.
So $\exists y_2, y_3$ such that $\deg_{y_2} t_2 > \deg_{y_2} S_{13}$ and $\deg_{y_3} t_3 > \deg_{y_3} S_{13}$.
By lemma 3, $S_{13} \overset{*}{\underset{F}{\not\rightarrow}} 0$. □

For the other clause of CC3, we employ a similar approach. As before, we build $F = (f_1, f_2, f_3)$ "as simple as possible": f_2 and f_3 will be monomials, and $f_1 = t_1 + u$ where u will have the "magical properties" that $S_{12} \underset{F}{\longrightarrow} 0$ but $S_{13} \overset{*}{\underset{F}{\not\rightarrow}} 0$. We find the "magical properties" by exploiting the failure of CC3: in this case, the existence of an indeterminate $y \in \{x_1, \dots, x_m\}$ such that $\neg\mathrm{VB1}_y(t_1, t_3)$ and $\neg\mathrm{VB2}_y(t_1, t_2, t_3)$. More precisely, we exploit $\deg_y \sigma_{12} > \deg_y \sigma_{13}$: then

$$\deg_y S_{12} = \deg_y(\sigma_{12} u) > \deg_y(\sigma_{13} u) = \deg_y S_{13}$$

This is the key: a sufficiently small choice for $\deg_y u$ gives $S_{12} \underset{f_3}{\longrightarrow} 0$ while $S_{13} \overset{*}{\underset{F}{\not\rightarrow}} 0$.

Lemma 8. For all terms t_1, t_2, t_3 (A)⇐(B) where
(A) $\mathrm{VB1}_x(t_1, t_3)$ or $\mathrm{VB2}_x(t_1, t_2, t_3)$ $\forall x \in \{x_1, \dots, x_n\}$
(B) $\left[S_{12} \overset{*}{\underset{F}{\longrightarrow}} 0 \quad \wedge \quad S_{23} \overset{*}{\underset{F}{\longrightarrow}} 0\right] \quad \Rightarrow \quad S_{13} \overset{*}{\underset{F}{\longrightarrow}} 0 \; \forall F = (f_1, f_2, f_3) : \forall k \; \mathrm{lt}_\succ(f_k) = t_k$

Proof. We show (A)⇐(B) by proving its contrapositive.
Assume ¬(A); then $\exists y \in \{x_1, \dots, x_n\}$ such that $\neg\mathrm{VB1}_y(t_1, t_3)$ and $\neg\mathrm{VB2}_y(t_1, t_2, t_3)$.
Equivalently, $\exists y$ such that

$$0 < \deg_y t_1, \deg_y t_3 < \deg_y t_2$$

We need to find F such that $S_{12} \overset{*}{\underset{F}{\longrightarrow}} 0$ and $S_{23} \overset{*}{\underset{F}{\longrightarrow}} 0$ but $S_{13} \overset{*}{\underset{F}{\not\rightarrow}} 0$.
Without loss of generality, we may assume $\deg_y t_1 \leq \deg_y t_3$.
Case 1: $t_1 \succeq t_3$
Define u as

$$\forall x \in \{x_1, \dots, x_n\} \quad \deg_x u = \begin{cases} \deg_x t_3 & x \neq y \\ \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) & x = y \end{cases}$$

Let $F = (f_1, f_2, f_3)$ be such that

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

Note that $u \mid t_3$ and $u \neq t_3$; hence $u \prec t_3 \preceq t_1$.
Hence f_1 is a binomial with $\mathrm{lt}_\succ(f_1) = t_1$.
We claim that $S_{12} \overset{*}{\underset{F}{\longrightarrow}} 0$ and $S_{23} \overset{*}{\underset{F}{\longrightarrow}} 0$ but $S_{13} \overset{*}{\underset{F}{\not\rightarrow}} 0$.
Immediately we have $S_{23} = 0$.
Next,

$$S_{12} = \frac{\mathrm{lcm}(t_1, t_2)}{t_1} \cdot u$$

We see that

$$\forall x \neq y \;\; \deg_x S_{12} \quad \geq \quad \deg_x u = \deg_x t_3$$

whereas

$$\deg_y S_{12} = \max\left(\deg_y t_1, \deg_y t_2\right) - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right)$$

Recall $\deg_y t_2 > \deg_y t_1$. Then

$$\begin{aligned} \deg_y S_{12} &= \deg_y t_2 - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) \\ &= \max\left(\deg_y t_2 - \deg_y t_1, \deg_y t_3\right) \\ &\geq \deg_y t_3 \end{aligned}$$

So $S_{12} \underset{f_3}{\longrightarrow} 0$, as desired.

Next, consider

$$S_{13} = \frac{\operatorname{lcm}(t_1, t_3)}{t_1} \cdot u$$

We claim $\deg_y S_{13} < \deg_y t_3 < \deg_y t_2$.

We have

$$\deg_y S_{13} = \max\left(\deg_y t_1, \deg_y t_3\right) - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right)$$

Recall $\deg_y t_1 \leq \deg_y t_3$.

Then

$$\begin{aligned} \deg_y S_{13} &= \deg_y t_3 - \deg_y t_1 + \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) \\ &= \max\left(\deg_y t_3 - \deg_y t_1, 2\deg_y t_3 - \deg_y t_2\right) \end{aligned}$$

Recall $\deg_y t_3 < \deg_y t_2$ and $0 < \deg_y t_1$.

Then

$$\deg_y S_{13} < \deg_y t_3 < \deg_y t_2$$

Observe that $\deg_y t_1 > \deg_y u$.

By lemma 3, $S_{13} \underset{F}{\overset{*}{\not\to}} 0$.

<u>Case 2</u>: $t_1 \prec t_3$

We sketch the proof; it is similar to that for case 1.

Let $F = (f_1, f_2, f_3)$ be such that

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

where v is defined as

$$\forall x \in \{x_1, \ldots, x_n\} \quad \deg_x v = \begin{cases} \deg_x t_1 & x \neq y \\ \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) & x = y \end{cases}$$

We see that $v \mid t_1$ and $v \neq t_1$, so $v \prec t_1 \prec t_3$. Hence $\operatorname{lt}_{\succ}(f_3) \mid t_3$.

Again, we claim $S_{12} \xrightarrow[F]{*} 0$, $S_{23} \xrightarrow[F]{*} 0$, but $S_{13} \underset{F}{\overset{*}{\not\to}} 0$.

We have $S_{12} \xrightarrow[F]{*} 0$ trivially.

As for S_{23}:

$$S_{23} = -\frac{\operatorname{lcm}(t_2, t_3)}{t_3} \cdot v$$

Inspection shows $S_{23} \xrightarrow[f_1]{*} 0$.

We turn to S_{13}. We have

$$\begin{aligned} \deg_y S_{13} &= \max\left(0, \deg_y t_1 + \deg_y t_3 - \deg_y t_2\right) \\ &< \deg_y t_1 < \deg_y t_2 \end{aligned}$$

As in case 1, $\deg_y t_3 > \deg_y u$ and by lemma 3, $S_{13} \underset{F}{\overset{*}{\not\to}}$. □

We can now set *a strict boundary* on triplets of terms that eliminate the need to check whether $S_{13} \xrightarrow[F]{*} 0$.

Lemma 9. For all terms t_1, t_2, t_3 (A)⇐(B) where

(A) $\mathrm{CC3}(t_1, t_2, t_3)$

(B) $\left[S_{12} \xrightarrow[F]{*} 0 \ \wedge \ S_{23} \xrightarrow[F]{*} 0\right] \Rightarrow S_{13} \xrightarrow[F]{*} 0 \ \forall F = (f_1, f_2, f_3) : \forall k \ \operatorname{lt}_{\succ}(f_k) = t_k$

Proof. Assume (B). From lemmas 7 and 8, we have (A). □

3.3. **Sufficience of criterion for three polynomials.** Now we turn our attention to proving that CC3 eliminates the need to check the reduction of an *S*-polynomial.

We need the following observation, proved easily by inspection. Note the subtle difference between remark 7, which is true in all cases, and remark 9, which is true only if $\gcd(t_1, t_3) \mid t_2$.

Remark 9. If $\gcd(t_1, t_3) \mid t_2$, then $\gcd(\mathrm{lt}_\succ(\sigma_{21}), \mathrm{lt}_\succ(\sigma_{23})) = 1$.

Now we begin to delve into the meat of the proof. We proceed by factoring the common divisor of f_1, f_3. Lemma 10 shows that when the new criterion is satisfied, we have the surprising result that $\gcd(f_1, f_3) \mid f_2$.

Lemma 10. For all t_1, t_2, t_3 (A)⇒(B) where

(A) $\gcd(t_1, t_3) \mid t_2$

(B) $\forall F = (f_1, f_2, f_3) : \forall k\ \mathrm{lt}_\succ(f_k) = t_k$ and for $g_{13} = \gcd(f_1, f_3)$,

$$S_{12} \xrightarrow[F]{*} 0 \wedge S_{23} \xrightarrow[F]{*} 0 \quad \Rightarrow \quad g_{13} \mid f_2$$

Proof. Assume (A). Then $\gcd(t_1, t_3) \mid t_2$.

Assume $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$.

We need to show $g_{13} \mid f_2$.

From $S_{12} \xrightarrow[F]{*} 0$, we know $\exists h_1, h_2, h_3$ such that

$$S_{12} = h_1 f_1 + h_2 f_2 + h_3 f_3 \tag{3.3}$$

and $\forall k = 1, 2, 3$, $h_k \neq 0$ implies $\mathrm{lt}_\succ(h_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2))$.

Likewise, from $S_{23} \xrightarrow[F]{*} 0$, we know $\exists H_1, H_2, H_3$ such that

$$S_{23} = H_1 f_1 + H_2 f_2 + H_3 f_3 \tag{3.4}$$

and $\forall k = 1, 2, 3$, $H_k \neq 0$ implies $\mathrm{lt}_\succ(H_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_2), \mathrm{lt}_\succ(f_3))$.

Consider (3.3). We have

$$\begin{aligned} \sigma_{12} f_1 - \sigma_{21} f_2 &= h_1 f_1 + h_2 f_2 + h_3 f_3 \\ (\sigma_{12} - h_1) f_1 - h_3 f_3 &= (\sigma_{21} + h_2) f_2 \end{aligned} \tag{3.5}$$

Likewise (3.4) gives us

$$H_1 f_1 + (\sigma_{32} + H_3) f_3 = (\sigma_{23} - H_2) f_2 \tag{3.6}$$

Let $g_{13} = \gcd(f_1, f_3)$.

Let c_1, c_3 be such that $f_1 = c_1 g_{13}$ and $f_3 = c_3 g_{13}$.

From (3.5), we have

$$g_{13} [(\sigma_{12} - h_1) c_1 - h_3 c_3] = (\sigma_{21} + h_2) f_2 \tag{3.7}$$

From (3.6), we have

$$g_{13} [H_1 c_1 + (\sigma_{32} - H_3) c_3] = (\sigma_{23} - H_2) f_2 \tag{3.8}$$

Note $g_{13} \mid (\sigma_{21} + h_2) f_2$ and $g_{13} \mid (\sigma_{23} - H_2) f_2$.

So g_{13} divides the greatest common divisor of the right-hand sides of (3.7) and (3.8).

Using lemma 4,

$$\mathrm{lt}_\succ(\sigma_{21} + h_2) = \mathrm{lt}_\succ(\sigma_{21})$$

and

$$\mathrm{lt}_\succ(\sigma_{23} - H_2) = \mathrm{lt}_\succ(\sigma_{23})$$

From remark 9, we know $\gcd(\mathrm{lt}_\succ(\sigma_{21}), \mathrm{lt}_\succ(\sigma_{23})) = 1$.

As a consequence, $\sigma_{21} + h_2$ and $\sigma_{23} + H_2$ are relatively prime.

Thus f_2 is the greatest common divisor of the right-hand side for both (3.7) and (3.8).

Hence $g_{13} \mid f_2$. □

We use lemma 11 on the *cofactors* of the gcd of f_1, f_2, f_3 in lemma 12.

Lemma 11. For all t_1, t_2, t_3 (A)⇒(B) where
(A) $\gcd(t_1, t_3) \mid t_2$ and $[\mathrm{VB1}_x(t_1, t_3) \ \vee\ \mathrm{VB2}_x(t_1, t_2, t_3)]\ \forall x \in \{x_1, \ldots, x_n\}$
(B) $\forall F = (f_1, f_2, f_3) : \forall k\ \mathrm{lt}_\succ(f_k) = t_k$ and $\gcd(f_1, f_3) = 1$,
if $\exists h_1, h_2, h_3$ such that $S_{12} = h_1 f_1 + h_2 f_2 + h_3 f_3$ and $h_k \neq 0$ implies $\mathrm{lt}_\succ(h_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2))$
and $\exists H_1, H_2, H_3$ such that $S_{23} = H_1 f_1 + H_2 f_2 + H_3 f_3$ and $H_k \neq 0$ implies $\mathrm{lt}_\succ(H_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_2), \mathrm{lt}_\succ(f_3))$
then

$$\gcd(t_1, t_3) = 1$$

Proof. Assume (A).
Let F be arbitrary but fixed.
Choose h_1, h_2, h_3 such that

$$S_{12} = h_1 f_1 + h_2 f_2 + h_3 f_3 \quad \wedge \quad \forall k\ h_k \neq 0 \Rightarrow \mathrm{lt}_\succ(h_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2)) \tag{3.9}$$

and H_1, H_2, H_3 such that

$$S_{23} = H_1 f_1 + H_2 f_2 + H_3 f_3 \quad \wedge \quad \forall k\ H_k \neq 0 \Rightarrow \mathrm{lt}_\succ(H_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_2), \mathrm{lt}_\succ(f_3)) \tag{3.10}$$

From (3.9),

$$\begin{aligned} \sigma_{12} f_1 - \sigma_{21} f_2 &= h_1 f_1 + h_2 f_2 + h_3 f_3 \\ (\sigma_{12} - h_1) f_1 - h_3 f_3 &= (\sigma_{21} + h_2) f_2 \\ \frac{(\sigma_{12} - h_1) f_1 - h_3 f_3}{\sigma_{21} + h_2} &= f_2 \end{aligned} \tag{3.11}$$

Likewise from (3.10),

$$\frac{H_1 f_1 + (\sigma_{32} + H_3) f_3}{\sigma_{23} - H_2} = f_2 \tag{3.12}$$

From (3.11) and (3.12),

$$\begin{aligned} \frac{(\sigma_{12} - h_1) f_1 - h_3 f_3}{\sigma_{21} + h_2} &= \frac{H_1 f_1 + (\sigma_{32} + H_3) f_3}{\sigma_{23} - H_2} \\ (\sigma_{23} - H_2)\left[(\sigma_{12} - h_1) f_1 - h_3 f_3\right] &= (\sigma_{21} + h_2)\left[H_1 f_1 + (\sigma_{32} + H_3) f_3\right] \end{aligned}$$

Collect expressions with f_1 and f_3 on opposite sides:

$$\left[(\sigma_{23} - H_2)(\sigma_{12} - h_1) - H_1(\sigma_{21} + h_2)\right] f_1 = \left[h_3(\sigma_{23} - H_2) + (\sigma_{21} + h_2)(\sigma_{32} + H_3)\right] f_3 \tag{3.13}$$

Let

$$P = h_3(\sigma_{23} - H_2) + (\sigma_{21} + h_2)(\sigma_{32} + H_3)$$

We claim $\mathrm{lt}_\succ(P) = \mathrm{lt}_\succ(\sigma_{21})\,\mathrm{lt}_\succ(\sigma_{32})$.
As per lemma 4,
* $\mathrm{lt}_\succ(\sigma_{23}) \succ \mathrm{lt}_\succ(H_2)$
* $\mathrm{lt}_\succ(\sigma_{21}) \succ \mathrm{lt}_\succ(h_2)$
* $\mathrm{lt}_\succ(\sigma_{32}) \succ \mathrm{lt}_\succ(H_3)$.

So the only possible leading terms of P are $\mathrm{lt}_\succ(\sigma_{21})\,\mathrm{lt}_\succ(\sigma_{32})$ and $\mathrm{lt}_\succ(\sigma_{23})\,\mathrm{lt}_\succ(h_3)$.
Assume by way of contradiction that

$$\mathrm{lt}_\succ(\sigma_{23})\,\mathrm{lt}_\succ(h_3) \quad \succ \quad \mathrm{lt}_\succ(\sigma_{21})\,\mathrm{lt}_\succ(\sigma_{32})$$

Then

$$\frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_2), \mathrm{lt}_\succ(f_3))}{\mathrm{lt}_\succ(f_2)} \cdot \mathrm{lt}_\succ(h_3) \quad \succ \quad \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2))}{\mathrm{lt}_\succ(f_2)} \cdot \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_2), \mathrm{lt}_\succ(f_3))}{\mathrm{lt}_\succ(f_3)}$$

Canceling, we find that this implies

$$\begin{aligned} \mathrm{lt}_\succ(h_3) &\succ \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2))}{\mathrm{lt}_\succ(f_3)} \\ \mathrm{lt}_\succ(f_3)\,\mathrm{lt}_\succ(h_3) &\succ \mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2)) \\ \mathrm{lt}_\succ(f_3 h_3) &\succ \mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2)) \end{aligned}$$

This clearly contradicts (3.9).
Hence $\mathrm{lt}_\succ(P) = \mathrm{lt}_\succ(\sigma_{21})\,\mathrm{lt}_\succ(\sigma_{32})$.

Observe that f_1 divides the left-hand side of (3.13).
So f_1 must also divide the right-hand side of (3.13).
Recall that f_1 and f_3 are relatively prime. Thus

$$f_1 \mid P$$

Then $\mathrm{lt}_\succ(f_1) \mid \mathrm{lt}_\succ(P)$.
That is,

$$\begin{aligned} t_1 &\mid \mathrm{lt}_\succ(\sigma_{21})\,\mathrm{lt}_\succ(\sigma_{32}) \\ t_1 &\mid \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_1),\mathrm{lt}_\succ(f_2))}{\mathrm{lt}_\succ(f_2)} \cdot \frac{\mathrm{lcm}(\mathrm{lt}_\succ(f_2),\mathrm{lt}_\succ(f_3))}{\mathrm{lt}_\succ(f_3)} \\ t_1 &\mid \frac{\mathrm{lcm}(t_1,t_2)}{t_2}\cdot\frac{\mathrm{lcm}(t_2,t_3)}{t_3} \\ t_1 &\mid \frac{t_1t_2}{\gcd(t_1,t_2)\cdot t_2}\cdot\frac{t_2t_3}{\gcd(t_2,t_3)\cdot t_3} \end{aligned}$$

$$\gcd(t_1,t_2)\cdot\gcd(t_2,t_3) \mid t_2 \tag{3.14}$$

We claim this proves $\gcd(t_1,t_3)=1$.
Let x be an arbitrary, but fixed indeterminate.
Recall from (A): $\gcd(t_1,t_3) \mid t_2$ and $\mathrm{VB1}_x(t_1,t_3)$ or $\mathrm{VB2}_x(t_1,t_2,t_3)$.
It will suffice to show that, in our circumstances, $\mathrm{VB2}_x(t_1,t_2,t_3)$ implies $\mathrm{VB1}_x(t_1,t_3)$.
Assume $\mathrm{VB2}_x(t_1,t_2,t_3)$.
Assume $\deg_x t_1 \le \deg_x t_3$
Then $\deg_x t_1 \le \deg_x t_2 \le \deg_x t_3$.
From (3.14),

$$\deg_x t_1 + \deg_x t_2 \le \deg_x t_2$$

So $\deg_x t_1 = 0$.
Hence $\mathrm{VB1}_x(t_1,t_3)$.
The case where $\deg_x t_1 > \deg_x t_3$ is shown similarly.
Hence $\mathrm{VB2}_x(t_1,t_2,t_3)$ implies $\mathrm{VB1}_x(t_1,t_3)$.
Since x was arbitrary, we have for all indeterminates x, $\deg_x t_1 = 0$ or $\deg_x t_3 = 0$.
Thus $\gcd(t_1,t_3)=1$. □

Lemma 12 completes the proof of the main theorem, by showing that the new criterion suffices to skip the reduction of one S-polynomial.

Lemma 12. For all terms t_1,t_2,t_3 (A)⇒(B) where
(A) $\mathrm{CC3}(t_1,t_2,t_3)$
(B) $\left[S_{12} \xrightarrow[F]{*} 0 \quad\wedge\quad S_{23} \xrightarrow[F]{*} 0\right] \Rightarrow S_{13} \xrightarrow[F]{*} 0\ \forall F=(f_1,f_2,f_3) : \forall k\ \mathrm{lt}_\succ(f_k)=t_k$

Proof. Assume (A). Thus $\mathrm{CC3}(t_1,t_2,t_3)$.
Let F be arbitrary, but fixed.
Assume $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$.
We have two cases.
Case 1: $\mathrm{BC2}(t_1,t_2,t_3)$
From lemma 2, we have (B).
Case 2: $\neg\mathrm{BC2}(t_1,t_2,t_3)$
From (A), we have

$$\gcd(t_1,t_3) \mid t_2 \ \wedge\ [\mathrm{VB1}_x(t_1,t_3)\ \vee\ \mathrm{VB2}_x(t_1,t_2,t_3)\ \forall x\in\{x_1,\ldots,x_n\}]$$

Let $g=\gcd(f_1,f_3)$, with $\mathrm{lc}_\succ(g)=1$.
Recall $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$.
From lemma 10, $g \mid f_2$.
Let c_1,c_3 be such that $f_k = gc_k$.
So c_1 and c_3 are relatively prime.

Let c_2 be such that $f_2 = gc_2$.
By inspection,

$$\gcd(\mathrm{lt}_\succ(c_1), \mathrm{lt}_\succ(c_3)) \mid \mathrm{lt}_\succ(c_2) \ \wedge\ \forall x\, [\mathrm{VB1}_x(\mathrm{lt}_\succ(c_1), \mathrm{lt}_\succ(c_3)) \ \vee\ \mathrm{VB2}_x(\mathrm{lt}_\succ(c_1), \mathrm{lt}_\succ(c_2), \mathrm{lt}_\succ(c_3))]$$

Since $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$, there exist h_1, h_2, h_3 and H_1, H_2, H_3 to satisfy

$$S_{12} = h_1 f_1 + h_2 f_2 + h_3 f_3$$

and

$$S_{23} = H_1 f_1 + H_2 f_2 + H_3 f_3$$

Also,

$$\forall k = 1,2,3 \quad h_K \neq 0 \qquad \Rightarrow \qquad \mathrm{lt}_\succ(h_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2))$$

and

$$\forall k = 1,2,3 \quad H_K \neq 0 \qquad \Rightarrow \qquad \mathrm{lt}_\succ(H_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_2), \mathrm{lt}_\succ(f_3))$$

By lemma 6, we have

$$S(c_1, c_2) = h_1 c_1 + h_2 c_2 + h_3 c_3$$

and

$$S(c_2, c_3) = H_1 c_1 + H_2 c_2 + H_3 c_3$$

Also,

$$\forall k = 1,2,3 \quad h_k \neq 0 \Rightarrow \mathrm{lt}_\succ(h_k c_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(c_1), \mathrm{lt}_\succ(c_2))$$

and

$$\forall k = 1,2,3 \quad H_k \neq 0 \Rightarrow \mathrm{lt}_\succ(H_k c_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(c_2), \mathrm{lt}_\succ(c_3))$$

By lemma 11, $\mathrm{lt}_\succ(c_1)$ and $\mathrm{lt}_\succ(c_3)$ are relatively prime.
Thus $\mathrm{BC1}(\mathrm{lt}_\succ(c_1), \mathrm{lt}_\succ(c_3))$.
As per remark 5,

$$S(c_1, c_3) = \mathcal{H}_1 c_1 + \mathcal{H}_3 c_3$$

where

$$\mathcal{H}_1 = \mathrm{lm}_\succ(c_3) - c_3 \quad \mathcal{H}_3 = c_1 - \mathrm{lm}_\succ(c_1)$$

Observe that $\forall k = 1,3\ \mathcal{H}_k \neq 0$ implies $\mathrm{lt}_\succ(\mathcal{H}_k c_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(c_1), \mathrm{lt}_\succ(c_3))$
Re-applying lemma 6, we obtain

$$S(f_1, f_3) = \mathcal{H}_1 \cdot f_1 + \mathcal{H}_3 \cdot f_3$$

where $\forall k = 1,3$, if $\mathcal{H}_k \neq 0$ then $\mathrm{lt}_\succ(\mathcal{H}_k f_k) \prec \mathrm{lcm}(\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_3))$.
By lemma 5, $S_{13} \xrightarrow[F]{} 0$. □

4. Observations and conclusion

4.1. **What's new?** We start with a very simple example of where the new criterion applies, that Buchberger's Criteria do not.

Example 1. Let $F = (f_1, f_2, f_3)$ where $\mathrm{lt}_\succ(f_1) = x_0 x_1$, $\mathrm{lt}_\succ(f_2) = x_0 x_2$, and $\mathrm{lt}_\succ(f_3) = x_0 x_3$. It is clear that Buchberger's criteria do not apply to any pair. Upon inspection, however, we see that the new criterion *does* apply: if $S_{12} \xrightarrow[F]{*} 0$ and $S_{23} \xrightarrow[F]{*} 0$, it follows from theorem 1 that $S_{13} \xrightarrow[F]{*} 0$.

As in case 2 of lemma 12, we can formally isolate the new combinatorial criterion from the theorem as follows:

$$\mathrm{NC}\ (t_1, t_2, t_3) := \ \gcd(t_1, t_3) \mid t_2 \quad \wedge \quad \forall x\ \mathrm{VB1}_x(t_1, t_3) \ \text{or}\ \mathrm{VB2}_x(t_1, t_2, t_3)$$

This is a generalization of the first criterion: $\mathrm{BC1}(t_1, t_3)$ implies $\mathrm{NC}(t_1, t_2, t_3)$, while the converse does not hold.

4.2. **Pitfalls.** These results apply only to triplets of polynomials (f_1, f_2, f_3). The fact that the criterion requires the reduction to be over f_1, f_2, f_3 *only* means that one has to remain wary of pitfalls such as the following:

Example 2. Let $F = (f_1, f_2, f_3, f_4)$ where

- $f_1 = x_0x_1 + x_2$
- $f_2 = x_0x_2$
- $f_3 = x_0x_3$
- $f_4 = x_2^2$

Let $\succ$ be any term ordering such that $\mathrm{lt}_\succ(f_1) = x_0x_1$; for example, a total-degree term ordering. Observe that $\mathrm{lt}_\succ(f_1), \mathrm{lt}_\succ(f_2), \mathrm{lt}_\succ(f_3)$ are the same as those of example 1; hence, they satisfy CC3. However,

$$\begin{aligned} S_{12} &= x_2^2 \underset{F}{\longrightarrow} 0 \\ S_{23} &= 0 \\ S_{13} &= x_2x_3 \underset{F}{\not\rightarrow} 0 \end{aligned}$$

The natural question to ask is, how do we generalize the new criterion to $m \geq 4$? At present, we do not know the answer.

4.3. **Another way of defining BC1 and BC2.** The new criteria provide alternate definitions for BC1 and BC2: for all terms t_1, t_2, t_3

$$\begin{aligned} \mathrm{BC1}(t_1, t_3) &\Leftrightarrow (\forall x\ \mathrm{VB1}_x(t_1, t_3)) \\ \mathrm{BC2}(t_1, t_2, t_3) &\Leftrightarrow (\forall x\ \mathrm{VB2}_x(t_1, t_2, t_3)) \end{aligned}$$

Observe that

$$\mathrm{BC1}(t_1, t_3) \ \vee\ \mathrm{BC2}(t_1, t_2, t_3) \Rightarrow \forall x\,[\mathrm{VB1}_x(t_1, t_3) \text{ or } \mathrm{VB2}_x(t_1, t_2, t_3)]$$

However, as we see from example 1,

$$\mathrm{BC1}(t_1, t_3) \ \vee\ \mathrm{BC2}(t_1, t_2, t_3) \not\Leftarrow \forall x\,[\mathrm{VB1}_x(t_1, t_3) \text{ or } \mathrm{VB2}_x(t_1, t_2, t_3)]$$

4.4. **Geometric classification.** If we plot all possible terms t_2 that allow us to skip the reduction of S_{13}, we observe the following pattern.

At the one extreme, t_1 and t_3 are relatively prime. Here $\mathrm{BC1}(t_1, t_3)$ applies; there is *no restriction at all* on t_2 (see figure one).

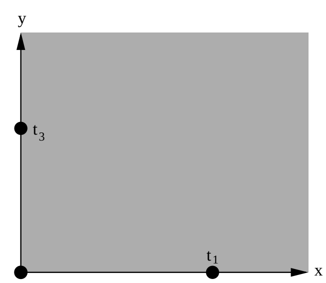


Figure 1

At the other extreme, t_1 and t_3 share all their variables. In this case, as lemma 8 shows, only $\mathrm{BC2}(t_1, t_2, t_3)$ applies: t_2 is constrained to the finite region bounded by $\mathrm{lcm}(t_1, t_3)$ (see figure two).

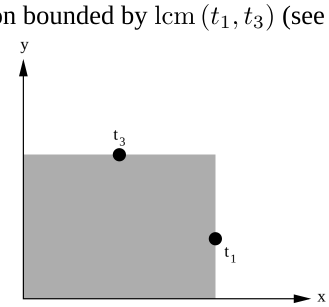


Figure 2

Between these two extremes, we have terms t_1 and t_3 where $\exists x, y \in \{x_1, \dots, x_n\}$ such that $\deg_x t_1 \neq 0$ and $\deg_x t_3 = 0$, and $\deg_y t_1 = 0$ and $\deg_y t_3 \neq 0$. In this case the new theorem applies: with each indeterminate removed from t_1 or t_3, we can pick t_2 from larger sets of additional regions of the space of terms, *unbounded on the variables that t_1, t_3 do not share.*

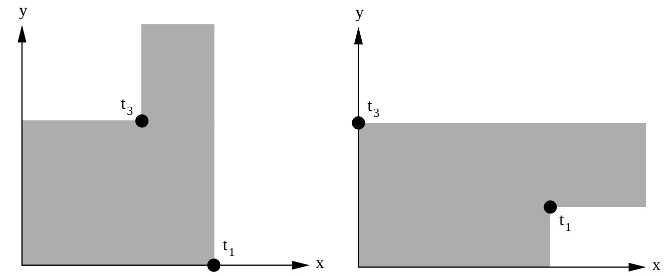


Figure 3(a) **Figure 3(b)**

We observe the following lattice structure from one extreme (BC1) to the other (BC2):

$$\begin{array}{ccccc} & & \text{Only } x_1 \text{ shared} & & \\ & \nearrow & & \searrow & \\ \text{No indeterminates shared (BC1)} & & & & \text{All indeterminates shared (BC2)} \\ & \searrow & & \nearrow & \\ & & \text{Only } x_2 \text{ shared} & & \end{array}$$

4.5. **Directions for future research.** We have already mentioned the question of how to generalize the result to four polynomials. There are different options for which S-polynomials to skip, and which to check:

- We have the option of one straightline path:

$$S_{12} \xrightarrow[F]{*} 0 \wedge S_{23} \xrightarrow[F]{*} 0 \wedge S_{34} \xrightarrow[F]{*} 0 \Rightarrow S_{14} \xrightarrow[F]{*} 0?$$

- There are also possibilities for lattice-style paths; for example,

$$S_{12} \xrightarrow[F]{*} 0 \wedge S_{13} \xrightarrow[F]{*} 0 \wedge S_{23} \xrightarrow[F]{*} 0 \wedge S_{34} \xrightarrow[F]{*} 0 \Rightarrow S_{14} \xrightarrow[F]{*} 0$$

Dr. Bruno Buchberger has suggested a statistical analysis of the results, and we have carried out a limited analysis. [insert results here]

REFERENCES

[1] B. Buchberger, *A Criterion for Detecting Unnecessary Reductions in the Construction of Groebner Bases.* Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation, Marseille, June 26-28, 1979, Lecture Notes in Computer Science, Vol. 72 E. W. Ng (ed) Springer, Berlin - Heidelberg - New York, 1979, pp. 3-21.

[2] B. Buchberger, *Ein Algorithmus sum 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).* PhD Thesis, Mathematical Insitute, University of Innsbruck, Austria, 1965. (English translation to appear in Journal of Symbolic Computation, 2004).

[3] M. Caboara, M. Kreuzer and L. Robbiano, *Minimal Sets of Critical Pairs*. Proceedings of the First Congress of Mathematical Software, 2002, B. Cohen, X. Gao and N. Takayama, eds., World Scientific, pp. 390-404.

[4] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms* (2nd ed.) 1997, Springer-Verlag New York, Inc.

[5] J. Faugere, *A new efficient algorithm for computing Gröbner bases without reduction to zero*. Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, 2002, Marc Giusti (chair); pp. .

[6] R. Gebauer and H. Möller, *On an Installation of Buchberger's Algorithm*, Journal of Symbolic Computation, vol. 6 pp. 275-286, 1988.

[7] H. Hong and J. Perry, *Buchberger's Combinatorial Criteria Applied to Gröbner Bases*, in preparation.

NORTH CAROLINA STATE UNIVERSITY, BOX 8205, DEPARTMENT OF MATHEMATICS, RALEIGH, NC 27695-8205
E-mail address: hong@math.ncsu.edu
URL: http://www4.ncsu.edu/ hong/

NORTH CAROLINA STATE UNIVERSITY, BOX 8205, DEPARTMENT OF MATHEMATICS, RALEIGH, NC 27695-8205
E-mail address: jeperry@ncsu.edu
URL: http://www4.ncsu.edu/ jeperry/