J. Symbolic Computation (1998) **25**, 643–662

Groebner Basis Under Composition I

HOON HONG[†]

Research Institute for Symbolic Computation,
Johannes Kepler University, A-4040 Linz, Austria

Composition is the operation of replacing variables in a polynomial with other polynomials. The main question of this paper is: *When does composition commute with Groebner basis computation?* We prove that this happens iff the composition is 'compatible' with the term ordering and the nondivisibility. This has a natural application in the computation of Groebner bases of composed polynomials which often arises in real-life problems.

1. Introduction

The main question of this paper is: *When does Groebner basis computation (Buchberger, 1965, 1985) commute with composition?*

More precisely, let F be a finite set of polynomials in the variables $x_1, \ldots, x_n$, and let G be a Groebner basis of the ideal generated by F under some term ordering. Let $\Theta = (\theta_1, \ldots, \theta_n)$ be a list of n polynomials in the variables $x_1, \ldots, x_n$. Let F^* be the set obtained from F by replacing x_i by θ_i and likewise let G^* be the set obtained from G by replacing x_i by θ_i. One ponders whether G^* is also a Groebner basis of F^* (under the same term ordering). It is *not*. One can easily construct counterexamples (for instance, just permute the variables) but one can also find numerous positive examples. Thus, the following question naturally arises: When is G^* a Groebner basis of F^*? In other words, when does Groebner basis computation commute with composition?

The main contribution of this paper is to show that Groebner basis computation commutes with composition *iff the composition is 'compatible' with the term ordering and the nondivisibility.*

Apart from satisfying curiosity, the answer to such a question has a natural application in the computation of a Groebner basis of the ideal generated by composed polynomials. In order to compute a Groebner basis of F^*, we first compute a Groebner basis G of F and carry out the composition on G, obtaining a Groebner basis of F^*. This should be more efficient than computing a Groebner basis of F^* directly (ignoring the structural information).

Composed objects (polynomials) often occur in real-life problem-solving because the

[†] E-mail: hhong@risc.uni-linz.ac.at; http://www.risc.uni-linz.ac.at/people/hhong

0747–7171/98/050643 + 21 $25.00/0 sy970192

underlying mathematical models are usually hierarchically structured. For instance, numerous physical quantities (such as work, torque, etc.) are defined in terms of other more basic quantifies (such as length, time, etc.). Thus, we often need to deal with a set of polynomials in which the variables are defined in terms of other variables.

On the other hand, if inputs are already given in expanded forms, one can first try to de-compose them and then apply the method described here. For several efficient methods for polynomial decomposition, see Barton and Zippel (1985); Kozen and Landau (1989); Von zur Gathen (1990a,b) and Binder (1996).

This paper is the first of two related papers. The second paper will provide an extension of the result given here. Namely, it will tackle the following more general question: Let G be a Groebner basis of F under the term ordering $>$. When is G^* a Groebner basis of F^* under *some* term ordering (possibly different from $>$)?

The reader might also be interested in the related works (McKay and Wang, 1989; Cheng *et al.*, 1995; Hong, 1995; Hong, 1997) which studied how other fundamental operations (resultants, subresultants and multivariate resultants) behave under composition.

The structure of this paper is as follows. In Section 2, we briefly review the terminology and results from Groebner basis theory that will be used throughout the subsequent sections. In Section 3, we give a precise statement of the main theorem of this paper. In Sections 4 and 5, we prove the sufficiency and necessity of the compatibility condition in the main theorem. In Section 6, we give several examples of compatible compositions. Finally in Section 7, we list several new questions/problems arising from this work.

2. Review of Groebner Basis Theory

In this section, we will review some basic terminology and results from Groebner basis theory that will be used in the subsequent sections. The reader who is familiar with the theory is still encouraged to skim through this section in order to become familiar with the notational convention. The details (and proofs) can be found in the original papers (Buchberger, 1965, 1985) or the textbooks (Cox *et al.*, 1992; Becker and Weispfenning, 1993).

Notation/Definitions 2.1.

K	*a field.*
a, b, c	*an element of* K.
p, q, r	*a term, that is,* $x_1^{e_1}, \ldots, x_n^{e_n}$ *for some* $e_1, \ldots, e_n \in \mathbf{N}$.[†]
f, g	*a non-zero polynomial in* $K[x_1, \ldots, x_n]$.
h	*a (possibly zero) polynomial in* $K[x_1, \ldots, x_n]$.
F, G	*a non-empty finite set of non-zero polynomials in* $K[x_1, \ldots, x_n]$.
H	*a non-empty (possibly infinite) set of (possibly zero) polynomials in* $K[x_1, \ldots, x_n]$.
$\mid$	*the divisibility relation over terms, that is,* $p \mid q$ *iff* p *divides* q.

[†] Caution. In the literature, there are two contradicting definitions of *term* and *monomial*. Some, such as Cox *et al.* (1992), define a monomial as a term with coefficient 1, while others, such as Buchberger (1985) and Becker and Weispfenning (1993), define a term as a monomial with coefficient 1. I follow Buchberger (1985).

$>$	*an admissible term ordering, that is, a linear ordering on terms such that* ◇ $\forall p \forall q \forall r\ [\ p > q \Longrightarrow pr > qr\ ]$, ◇ $\forall p\ [\ p \neq 1 \Longrightarrow p > 1\ ]$.
$\mathrm{lt}(f)$	*the leading term of* f *under* $>$.
$\mathrm{lc}(f)$	*the leading coefficient of* f *under* $>$.
$\mathrm{lm}(h)$	*the leading monomial of* h *under* $>$, *that is,* $\mathrm{lm}(h) = \mathrm{lc}(h)\mathrm{lt}(h)$ *for* $h \neq 0$, $\mathrm{lm}(0) = 0$.
$\mathrm{lm}(H)$	*the set* $\{\mathrm{lm}(h) \mid h \in H\}$.
$\mathrm{Ideal}(H)$	*the ideal generated by* H, *that is, the set* $\left\{\sum_i \hat{h}_i h_i \mid h_i \in H\right\}$.
$\mathrm{GB}(G)$	*the predicate stating that* G *is a Groebner basis, that is,* ◇ $\mathrm{Ideal}(\mathrm{lm}(G)) = \mathrm{Ideal}(\mathrm{lm}(\mathrm{Ideal}(G)))$.
$\mathrm{GB}(G, F)$	*the predicate stating that* G *is a Groebner basis of* $\mathrm{Ideal}(F)$, *that is,* ◇ $\mathrm{GB}(G)$, ◇ $\mathrm{Ideal}(G) = \mathrm{Ideal}(F)$.
$\mathrm{lcm}(p, q)$	*the least common multiple of* p *and* q.
$\sigma(f, g)$	$\mathrm{lcm}\left(\mathrm{lt}(f), \mathrm{lt}(g)\right)/\mathrm{lm}(f)$.
$\mathrm{S}(f, g)$	*the S-polynomial of* f *and* g, *that is,* $\sigma(f, g)f - \sigma(g, f)g$.

PROPOSITION 2.1. *The following are equivalent:*

(A) $\mathrm{GB}(G)$.

(B) $\forall f \in \mathrm{Ideal}(G)\ \exists\, g \in G\ \ [\ \mathrm{lt}(g) \mid \mathrm{lt}(f)\ ]$.

This follows immediately from the definition of a Groebner basis given above.

THEOREM 2.1. *(Buchberger, 1965) The following are equivalent:*

(A) $\mathrm{GB}(G)$.

(B) *For all* g_i *and* $g_j \in G = \{g_1, \ldots, g_t\}$, $i \neq j$, *there exist* $h_1, \ldots, h_t$ *such that*

  (a) $\mathrm{S}(g_i, g_j) = h_1 g_1 + \cdots + h_t g_t$,

  (b) *for every* k, *either* $h_k = 0$ *or* $\mathrm{lt}(h_k)\mathrm{lt}(g_k) < \mathrm{lcm}(\mathrm{lt}(g_i), \mathrm{lt}(g_j))$.

This is one of the key theorems in Groebner basis theory. Note that the statement of the theorem, in particular condition (b), is slightly different from the one usually found in the literature, Buchberger (1965, 1985); Cox *et al.* (1992); Becker and Weispfenning (1993), in that $\mathrm{lt}(\mathrm{S}(g_i, g_j))$ is usually used in place of $\mathrm{lcm}(\mathrm{lt}(h_k)\mathrm{lt}(g_k))$ and $\leq$ in place of $<$. However, the proofs for both are essentially the same. In the subsequent sections, we will make *essential* use of the formulation given above.[†]

COROLLARY 2.1. *The following are equivalent:*

(A) $\mathrm{GB}(G)$.

(B) *For all* g_i *and* $g_j \in G = \{g_1, \ldots, g_t\}$, $i \neq j$, *there exist* $h_1, \ldots, h_t$ *such that*

[†] I have made many attempts, without success, to find a simple proof for the main theorem of this paper using the usual formulation. I would be happy to know whether anyone has done it.

(a) $\mathrm{S}(g_i, g_j) = h_1 g_1 + \cdots + h_t g_t$,
(b) *for every k, either $h_k = 0$ or $\mathrm{lt}(h_k)\mathrm{lt}(g_k) < \mathrm{lcm}(\mathrm{lt}(g_i), \mathrm{lt}(g_j))$.*
(c) *for every $k < \ell$, no term in $h_\ell \mathrm{lt}(g_\ell)$ is divisible by $\mathrm{lt}(g_k)$.*

This is almost the same as in the previous theorem, except that we have one more condition (c). The implication from (B) to (A) is immediate from the previous theorem. The implication from (A) to (B), in particular (c), follows immediately from the characterization of the generalized division described in Cox *et al.* (1992, p. 68).

3. Main Result

In this section, we crystallize the question and answer described in the introduction. For this, we fix some notation and notions.

Notation 3.1.

Θ	*a list $(\theta_1, \ldots, \theta_n)$ of n non-zero polynomials in $K[x_1, \ldots, x_n]$.*
$\mathrm{lt}(\Theta)$	*the list ($\mathrm{lt}(\theta_1), \ldots, \mathrm{lt}(\theta_n)$).*
$\mathrm{lm}(\Theta)$	*the list ($\mathrm{lm}(\theta_1), \ldots, \mathrm{lm}(\theta_n)$).*

Definition 3.1. (Composition) *The* composition *of h by Θ, written as $h{\circ}\Theta$, is the polynomial obtained from h by replacing each x_i in it with θ_i. Likewise, $H{\circ}\Theta$ is the set $\{\ h{\circ}\Theta \mid h \in H\ \}$.*

One might consider the possibility of defining composition as the "function composition", namely,

$$\forall (x_1, \ldots, x_n) \in K^n\ \ [\ \ (h{\circ}\Theta)(x_1, \ldots, x_n) = h(\theta_1(x_1, \ldots, x_n), \ldots, \theta_n(x_1, \ldots, x_n)).\ \ ]$$

But this is not suitable since $h{\circ}\Theta$ is *not* uniquely determined when K is a finite field.

Definition 3.2. (Commutativity with Composition) *We say that composition by Θ* commutes *with Groebner basis computation iff the following formula is true for Θ:*

$$\forall F\ \forall G\ [\ \ \mathrm{GB}(G, F) \ \Longrightarrow\ \mathrm{GB}(G{\circ}\Theta, F{\circ}\Theta)\ \ ].$$

The main question of this paper is when a composition commutes with Groebner basis computation and the main contribution of this paper is to provide a simple answer to this question. In order to describe the answer we need to introduce a few new notions.

Definition 3.3. (Compatibility with term ordering) *We say that composition by Θ is* compatible *with a term ordering $>$ iff for all terms p and q, we have*

$$p\ >\ q \quad \Longrightarrow \quad p{\circ}\mathrm{lt}(\Theta)\ >\ q{\circ}\mathrm{lt}(\Theta).$$

Definition 3.4. (Compatibility with nondivisibility) *We say that composition by Θ is* compatible *with nondivisibility iff for all terms p and q, we have*

$$p\ \not|\ q \quad \Longrightarrow \quad p{\circ}\mathrm{lt}(\Theta)\ \not|\ q{\circ}\mathrm{lt}(\Theta).$$

The reader might wonder whether divisibility might be a more natural condition than *un*-divisibility; but divisibility is compatible with *every* composition. Thus, compatibility with divisibility is not a useful condition.

Theorem 3.1. (Main Theorem) *The following are equivalent.*

(A) *Composition by Θ commutes with Groebner basis computation.*

(B) *Composition by Θ is*

  (a) *compatible with term ordering $>$ and*

  (b) *compatible with nondivisibility.*

4. Proof of Sufficiency

In this section, we prove the sufficiency of the compatibility condition for commutativity, that is, we prove that (B) of the main theorem implies (A). We begin by stating some basic properties/facts about compositions and leading terms/monomials. These will be used throughout the paper, often *without* explicit reference to them.

Proposition 4.1.

(a) $(fg)\circ\Theta = f\circ\Theta \;\; g\circ\Theta$.

(b) $(f+g)\circ\Theta = f\circ\Theta + g\circ\Theta$.

(c) $\mathrm{lm}(fg) = \mathrm{lm}(f)\,\mathrm{lm}(g)$.

(d) $\mathrm{lt}(fg) = \mathrm{lt}(f)\,\mathrm{lt}(g)$.

(e) *If* $\mathrm{lt}(f) > \mathrm{lt}(g)$, *then* $\mathrm{lm}(f+g) = \mathrm{lm}(f)$.

(f) *If* $\mathrm{lt}(f) > \mathrm{lt}(g)$, *then* $\mathrm{lt}(f+g) = \mathrm{lt}(f)$.

(g) $\mathrm{lm}(p\circ\Theta) = p\circ\mathrm{lm}(\Theta)$.

(h) $\mathrm{lt}(p\circ\Theta) = p\circ\mathrm{lt}(\Theta)$. □

Proof. This follows immediately from their definitions. □

The following lemma states that a composition operation commutes with the leading monomial (term) extraction if it is compatible with the term ordering.

Lemma 4.1. *Let*

(A) *the composition by Θ be compatible with the term ordering $>$.*

(B) *For every f, we have*

  (a) $\mathrm{lm}(f\circ\Theta) = \mathrm{lm}(f)\circ\mathrm{lm}(\Theta)$.

  (b) $\mathrm{lt}(f\circ\Theta) = \mathrm{lt}(f)\circ\mathrm{lt}(\Theta)$.

Then (A) $\Longrightarrow$ (B).

Proof. Assume (A). We need to show (B). Let f be arbitrary but fixed. It can[†] be written as $f = c_1p_1+\cdots+c_tp_t$ where $c_i \neq 0$ and $p_1 > p_2 > \cdots > p_t$. Thus, we have $f\circ\Theta = c_1p_1\circ\Theta + \cdots + c_tp_t\circ\Theta$. From Proposition 4.1 (d) and (h), we have $\mathrm{lt}(c_ip_i\circ\Theta) = p_i\circ\mathrm{lt}(\Theta)$. From (A) we have $p_1\circ\mathrm{lt}(\Theta) > p_2\circ\mathrm{lt}(\Theta) > \cdots > p_t\circ\mathrm{lt}(\Theta)$. Thus, we have $\mathrm{lt}(c_1p_1\circ\Theta) >$

[†] Recall that our notational convention (Notation/Definition 2.1) dictates that f is a non-zero polynomial.

$\mathrm{lt}(c_2p_2\circ\Theta) > \cdots > \mathrm{lt}(c_tp_t\circ\Theta)$. Hence, from Proposition 4.1 (c)–(h) we conclude that $\mathrm{lm}(f\circ\Theta) = \mathrm{lm}(c_1p_1\circ\Theta) = \mathrm{lm}(f)\circ\mathrm{lm}(\Theta)$ and $\mathrm{lt}(f\circ\Theta) = \mathrm{lt}(c_1p_1\circ\Theta) = \mathrm{lt}(f)\circ\mathrm{lt}(\Theta)$. □

The following lemma completely characterizes the condition of compatibility with the nondivisibility. It will also be used in the next section while proving the necessity of the main theorem.

Lemma 4.2. *Let*

(A) *the composition by Θ be compatible with the nondivisibility; and*

(B) *the list* $\mathrm{lt}(\Theta)$ *be a 'permuted powering', that is,* $\mathrm{lt}(\Theta) = (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n})$ *for some permutation π of $(1,\ldots,n)$ and some $\lambda_1,\ldots,\lambda_n > 0$.*

Then (A) $\Longleftrightarrow$ (B).

Proof.
(A) $\Longleftarrow$ (B):

Assume (B). We need to show (A). Let p and q be arbitrary but fixed. Assume that $p\circ\mathrm{lt}(\Theta) \mid q\circ\mathrm{lt}(\Theta)$. We need to show that $p \mid q$.

Let $p = x_1^{\mu_1}\cdots x_n^{\mu_n}$ and $q = x_1^{\nu_1}\cdots x_n^{\nu_n}$. Then, we have

$$p\circ\mathrm{lt}(\Theta) = x_{\pi_1}^{\lambda_1\mu_1}\cdots x_{\pi_n}^{\lambda_n\mu_n},$$
$$q\circ\mathrm{lt}(\Theta) = x_{\pi_1}^{\lambda_1\nu_1}\cdots x_{\pi_n}^{\lambda_n\nu_n}.$$

Thus, for every i, we have $\lambda_i\mu_i \le \lambda_i\nu_i$. Since $\lambda_i > 0$, we have $\mu_i \le \nu_i$. Hence, $p \mid q$.

(A) $\Longrightarrow$ (B):

Assume (A). We need to show (B). Let $\mathrm{lt}(\theta_j) = x_1^{e_{1j}}\cdots x_n^{e_{nj}}$ and let $e = [e_{ij}]$ be the associated matrix. Let

$$(\mathrm{A}') \equiv \forall\alpha \in \mathbf{Z}^n\ [\ e\alpha \ge 0 \Longrightarrow \alpha \ge 0\ ]$$
$$(\mathrm{B}') \equiv \forall j\ \exists i\ [\ e_{ij} > 0\ \wedge\ \forall j' \ne j\ [e_{ij'} = 0\ ]\ ]$$

where $e\alpha$ is a matrix–vector multiplication and $\ge$ is applied component-wise. We will prove that

$$(\mathrm{A}) \Longrightarrow (\mathrm{A}') \Longrightarrow (\mathrm{B}') \Longrightarrow (\mathrm{B}).$$

Claim 1: (A) $\Longrightarrow$ (A$'$).

Let $p = x_1^{\mu_1}\cdots x_n^{\mu_n}$ and $q = x_1^{\nu_1}\cdots x_n^{\nu_n}$. Then

$$p\circ\mathrm{lt}(\Theta) = x_1^{\mu_1'}\cdots x_n^{\mu_n'}$$
$$q\circ\mathrm{lt}(\Theta) = x_1^{\nu_1'}\cdots x_n^{\nu_n'}$$

where $\mu_i' = \sum_{j=1}^n e_{ij}\mu_j$ and $\nu_i' = \sum_{j=1}^n e_{ij}\nu_j$. Let $\mu = (\mu_1,\ldots,\mu_n)$, $\nu = (\nu_1,\ldots,\nu_n)$, $\mu' = (\mu_1',\ldots,\mu_n')$ and $\nu' = (\nu_1',\ldots,\nu_n')$ be column vectors. Then we have $\mu' = e\mu$ and $\nu' = e\nu$. Hence

$$p \mid q \Longleftrightarrow \mu_1 \le \nu_1 \wedge \cdots \wedge \mu_n \le \nu_n$$
$$\Longleftrightarrow \mu \le \nu$$

$$\begin{aligned} p{\circ}\mathrm{lt}(\Theta) \mid q{\circ}\mathrm{lt}(\Theta) &\Longleftrightarrow \mu_1' \le \nu_1' \wedge \cdots \wedge \mu_n' \le \nu_n' \\ &\Longleftrightarrow \mu' \le \nu' \\ &\Longleftrightarrow e\mu \le e\nu. \end{aligned}$$

So we have the following

$$\begin{aligned} (\mathrm{A}) &\Longleftrightarrow \forall \mu \in \mathbf{N}^n\ \forall \nu \in \mathbf{N}^n\ [\ \neg \mu \le \nu \Longrightarrow \neg e\mu \le e\nu\ ] \\ &\Longleftrightarrow \forall \mu \in \mathbf{N}^n\ \forall \nu \in \mathbf{N}^n\ [\ e\mu \le e\nu \Longrightarrow \mu \le \nu\ ] \\ &\Longleftrightarrow \forall \mu \in \mathbf{N}^n\ \forall \nu \in \mathbf{N}^n\ [\ e(\nu - \mu) \ge 0 \Longrightarrow \nu - \mu \ge 0\ ] \\ &\Longleftrightarrow \forall \alpha \in \mathbf{Z}^n\ [\ e\alpha \ge 0 \Longrightarrow \alpha \ge 0\ ] \\ &\Longleftrightarrow (\mathrm{A}'). \end{aligned}$$

Claim 2: (A′) $\Longrightarrow$ (B′).

We will prove the contrapositive. Thus, assume ¬(B′). Then, there exists, say j^*, such that for every i we have

$$e_{ij^*} = 0 \vee \exists j' \ne j^*\ [e_{ij'} \ne 0\ ].$$

We need to show ¬(A′), that is, we need to find an $\alpha \in \mathbf{Z}^n$ such that $e\alpha \ge 0$ but not $\alpha \ge 0$. We claim that the following α does the job:

$$\alpha_j = \begin{cases} -1 & \text{if } j = j^* \\ \max_k e_{kj^*} & \text{else.} \end{cases}$$

Clearly it is not that $\alpha \ge 0$. Thus, we only need to show that $e\alpha \ge 0$. Observe

$$\begin{aligned} (e\alpha)_i &= \sum_j e_{ij}\alpha_j \\ &= \left(\sum_{j \ne j^*} e_{ij} \max_k e_{kj^*} \right) - e_{ij^*} \\ &= \max_k e_{kj^*} \left(\sum_{j \ne j^*} e_{ij} \right) - e_{ij^*}. \end{aligned}$$

If $e_{ij^*} = 0$ then obviously $(e\alpha)_i \ge 0$. If $e_{ij^*} \ne 0$ then there exists $j' \ne j^*$ such that $e_{ij'} \ne 0$, and thus $\sum_{j \ne j^*} e_{ij} \ge 1$, and hence $(e\alpha)_i \ge 0$. Thus, we see that $(e\alpha)_i \ge 0$ in both cases. Hence, $(e\alpha) \ge 0$.

Claim 3: (B′) $\Longrightarrow$ (B).

Assume (B′). Then there are $\pi_1, \dots, \pi_n$ such that

$$\begin{array}{lcl} e_{\pi_1,1} > 0 & \wedge & \forall j' \ne 1\ [\ e_{\pi_1,j'} = 0\ ] \\ e_{\pi_2,2} > 0 & \wedge & \forall j' \ne 2\ [\ e_{\pi_2,j'} = 0\ ] \\ \vdots & & \vdots \\ e_{\pi_n,n} > 0 & \wedge & \forall j' \ne n\ [\ e_{\pi_n,j'} = 0\ ]. \end{array}$$

Note that $\pi_\ell \ne \pi_m$ for $\ell \ne m$ since $e_{\pi_\ell,\ell} > 0$ and $e_{\pi_m,\ell} = 0$. Thus $(\pi_1, \dots, \pi_n)$ is a permutation of $(1, \dots, n)$. Hence $e_{ij} = \lambda_j \delta_{i\pi_j}$ for some $\lambda_1, \dots, \lambda_n > 0$. Thus, $\mathrm{lt}(\theta_j) = x_{\pi_j}^{\lambda_j}$. So we have (B). □

The following lemma states that the composition operation commutes with the least common multiple computation if it is compatible with the nondivisibility.

Lemma 4.3. *Let*

(A) *the composition by* Θ *be compatible with the nondivisibility; and*

(B) $\forall p \forall q\ [\,\mathrm{lcm}(p\circ \mathrm{lt}(\Theta), q\circ \mathrm{lt}(\Theta)) = \mathrm{lcm}(p,q)\circ \mathrm{lt}(\Theta)\,]$.

Then (A) $\Longrightarrow$ (B).

Proof. Assume (A). We need to show (B). Let p and q be arbitrary but fixed. We need to show that $\mathrm{lcm}(p\circ \mathrm{lt}(\Theta), q\circ \mathrm{lt}(\Theta)) = \mathrm{lcm}(p,q)\circ \mathrm{lt}(\Theta)$.

From (A) and Lemma 4.2, we see that $\mathrm{lt}(\Theta) = (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n})$ for some permutation π of $(1,\ldots,n)$ and some λ_is. Let $p = x_1^{\mu_1}\cdots x_n^{\mu_n}$ and $q = x_1^{\nu_1}\cdots x_n^{\nu_n}$. Then, we have

$$\begin{aligned} p\circ \mathrm{lt}(\Theta) &= x_{\pi_1}^{\lambda_1\mu_1}\cdots x_{\pi_n}^{\lambda_n\mu_n},\\ q\circ \mathrm{lt}(\Theta) &= x_{\pi_1}^{\lambda_1\nu_1}\cdots x_{\pi_n}^{\lambda_n\nu_n}. \end{aligned}$$

Thus, we have

$$\begin{aligned} \mathrm{lcm}(p\circ \mathrm{lt}(\Theta), q\circ \mathrm{lt}(\Theta)) &= x_{\pi_1}^{\max(\lambda_1\mu_1,\lambda_1\nu_1)}\cdots x_{\pi_n}^{\max(\lambda_n\mu_n,\lambda_n\nu_n)}\\ &= x_{\pi_1}^{\lambda_1\max(\mu_1,\nu_1)}\cdots x_{\pi_n}^{\lambda_n\max(\mu_n,\nu_n)}\\ &= \left(x_1^{\max(\mu_1,\nu_1)}\cdots x_n^{\max(\mu_n,\nu_n)}\right)\circ \mathrm{lt}(\Theta)\\ &= \mathrm{lcm}(p,q)\circ \mathrm{lt}(\Theta). \qquad \square \end{aligned}$$

Lemma 4.4. $\mathrm{Ideal}(G) = \mathrm{Ideal}(F) \implies \mathrm{Ideal}(G\circ\Theta) = \mathrm{Ideal}(F\circ\Theta)$.

Proof. Assume $\mathrm{Ideal}(G) = \mathrm{Ideal}(F)$. We need to show that $\mathrm{Ideal}(G\circ\Theta) = \mathrm{Ideal}(F\circ\Theta)$.

We will first show that $\mathrm{Ideal}(G\circ\Theta) \subseteq \mathrm{Ideal}(F\circ\Theta)$. Let $h \in \mathrm{Ideal}(G\circ\Theta)$. Then

$$h = \sum_i \hat{h}_i\ \ g_i\circ\Theta \tag{4.1}$$

for some $\hat{h}_i$s. Since $g_i \in \mathrm{Ideal}(F)$, we also have

$$g_i = \sum_j \hat{g}_{ij} f_j \tag{4.2}$$

for some $\hat{g}_{ij}$s. Putting (4.1) and (4.2) together and repeatedly rewriting, we obtain

$$\begin{aligned} h &= \sum_i \hat{h}_i \left(\sum_j \hat{g}_{ij} f_j\right)\circ\Theta\\ &= \sum_i \hat{h}_i \sum_j \hat{g}_{ij}\circ\Theta\ \ f_j\circ\Theta\\ &= \sum_i\sum_j \hat{h}_i\ \ \hat{g}_{ij}\circ\Theta\ \ f_j\circ\Theta\\ &= \sum_j\sum_i \hat{h}_i\ \ \hat{g}_{ij}\circ\Theta\ \ f_j\circ\Theta \end{aligned}$$

$$= \sum_j \left(\sum_i \hat{h}_i \ \hat{g}_{ij} \circ \Theta \right) f_j \circ \Theta$$
$$\in \operatorname{Ideal}(F \circ \Theta).$$

Thus, we have that $\operatorname{Ideal}(G \circ \Theta) \subseteq \operatorname{Ideal}(F \circ \Theta)$.

In a similar way, we can show that $\operatorname{Ideal}(G \circ \Theta) \supseteq \operatorname{Ideal}(F \circ \Theta)$. For this, we only need to switch the roles of G and F. Thus, we conclude that $\operatorname{Ideal}(G \circ \Theta) = \operatorname{Ideal}(F \circ \Theta)$. □

Lemma 4.5. *Let*

(A) $\forall F \, \forall G \, [\ \mathrm{GB}(G, F) \implies \mathrm{GB}(G \circ \Theta, F \circ \Theta) \ ]$; *and*

(B) $\forall G \, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G \circ \Theta) \ ]$.

Then (B) $\implies$ (A).

Proof. Assume (B). We need to show (A). Let F and G be arbitrary but fixed such that $\mathrm{GB}(G, F)$. We need to show that $\mathrm{GB}(G \circ \Theta, F \circ \Theta)$. Since $\mathrm{GB}(G, F)$, we trivially have $\mathrm{GB}(G)$. Then from (B), we have

$$\mathrm{GB}(G \circ \Theta). \tag{4.3}$$

Since $\mathrm{GB}(G, F)$, we have that $\operatorname{Ideal}(G) = \operatorname{Ideal}(F)$. Then from Lemma 4.4, we have

$$\operatorname{Ideal}(G \circ \Theta) = \operatorname{Ideal}(F \circ \Theta). \tag{4.4}$$

Putting together (4.3) and (4.4), we conclude that $\mathrm{GB}(G \circ \Theta, F \circ \Theta)$. □

Now we have prepared enough machinery to formulate the *core* of the sufficiency proof of the main theorem.

Lemma 4.6. *Let*

(A) $\forall G \, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G \circ \Theta) \ ]$*; and*

(B) *the composition by* Θ *be*

  (a) *compatible with the term ordering* $>$ *and*

  (b) *compatible with the nondivisibility.*

Then (B) $\implies$ (A).

Proof. Assume (B). We need to show (A). Let $G = \{g_1, \ldots, g_t\}$ be arbitrary but fixed such that $\mathrm{GB}(G)$. We need to show that $\mathrm{GB}(G \circ \Theta)$.

Let $1 \leq i \neq j \leq t$ be arbitrary but fixed. Since G is a Groebner basis, by Theorem 2.1, there exist $h_1, \ldots, h_t$ such that

$$\mathrm{S}(g_i, g_j) = \sum_{k=1}^{t} h_k g_k \tag{4.5}$$

and

$$\forall k \ \ [\ h_k = 0 \ \vee \ \mathrm{lt}(h_k g_k) < \operatorname{lcm}(\mathrm{lt}(g_i), \mathrm{lt}(g_j)) \ ]. \tag{4.6}$$

From (4.5) we have

$$\mathrm{S}(g_i, g_j) \circ \Theta = \sum_{k=1}^{t} h_k \circ \Theta \ \ g_k \circ \Theta.$$

Let $c = \frac{1}{\mathrm{lc}(\,\mathrm{lcm}(\mathrm{lt}(g_i),\mathrm{lt}(g_j))\circ\mathrm{lm}(\Theta))}$. Note that

$$\begin{aligned}
\mathrm{S}(g_i\circ\Theta, g_j\circ\Theta) &= \mathrm{S}(g_i\circ\Theta, g_j\circ\Theta) - c\mathrm{S}(g_i, g_j)\circ\Theta + c\mathrm{S}(g_i, g_j)\circ\Theta \\
&= \sigma(g_i\circ\Theta, g_j\circ\Theta)g_i\circ\Theta - \sigma(g_j\circ\Theta, g_i\circ\Theta)g_j\circ\Theta \\
&\quad -c\,(\sigma(g_i, g_j)g_i - \sigma(g_j, g_i)g_j)\circ\Theta \\
&\quad +c\sum_{k=1}^{t} h_k\circ\Theta \;\; g_k\circ\Theta \\
&= \sigma(g_i\circ\Theta, g_j\circ\Theta)g_i\circ\Theta - \sigma(g_j\circ\Theta, g_i\circ\Theta)g_j\circ\Theta \\
&\quad -c\sigma(g_i, g_j)\circ\Theta g_i\circ\Theta + c\sigma(g_j, g_i)\circ\Theta g_j\circ\Theta \\
&\quad +c\sum_{k=1}^{t} h_k\circ\Theta \;\; g_k\circ\Theta \\
&= \sum_{k=1}^{t} \hat{h}_k g_k\circ\Theta
\end{aligned}$$

where

$$\hat{h}_k = \begin{cases} ch_k\circ\Theta + \bar{g}_{ij} & \text{if } k = i \\ ch_k\circ\Theta - \bar{g}_{ji} & \text{if } k = j \\ ch_k\circ\Theta & \text{otherwise} \end{cases}$$

where again

$$\begin{aligned}
\bar{g}_{ij} &= \sigma(g_i\circ\Theta, g_j\circ\Theta) - c\sigma(g_i, g_j)\circ\Theta \\
\bar{g}_{ji} &= \sigma(g_j\circ\Theta, g_i\circ\Theta) - c\sigma(g_j, g_i)\circ\Theta.
\end{aligned}$$

Recalling Theorem 2.1, it will be sufficient to show that

$$\hat{h}_k = 0 \quad \text{or} \quad \mathrm{lt}(\hat{h}_k g_k\circ\Theta) < \mathrm{lcm}\,(\mathrm{lt}(g_i\circ\Theta), \mathrm{lt}(g_j\circ\Theta))$$

is true for every k. This follows immediately from the following three claims.

Claim 1: For every k, $ch_k\circ\Theta = 0$ or $\mathrm{lt}(ch_k\circ\Theta g_k\circ\Theta) < \mathrm{lcm}\,(\mathrm{lt}(g_i\circ\Theta), \mathrm{lt}(g_j\circ\Theta))$.

Let k be arbitrary but fixed. We need to show that $ch_k\circ\Theta = 0$ or $\mathrm{lt}(ch_k\circ\Theta g_k\circ\Theta) < \mathrm{lcm}\,(\mathrm{lt}(g_i\circ\Theta), \mathrm{lt}(g_j\circ\Theta))$. If $ch_k\circ\Theta = 0$, then the claim is trivially true. Thus, from now on assume that $ch_k\circ\Theta \neq 0$. Thus $h_k \neq 0$.

From (B) and Lemma 4.1 we have

$$\mathrm{lt}(ch_k\circ\Theta g_k\circ\Theta) = \mathrm{lt}(h_k g_k)\circ\mathrm{lt}(\Theta). \tag{4.7}$$

From (B) and Lemmas 4.1 and 4.3 we have

$$\mathrm{lcm}\,(\mathrm{lt}(g_i\circ\Theta), \mathrm{lt}(g_j\circ\Theta)) = \mathrm{lcm}\,(\mathrm{lt}(g_i), \mathrm{lt}(g_j))\circ\mathrm{lt}(\Theta). \tag{4.8}$$

From (B) and (4.6) we have

$$\mathrm{lt}(h_k g_k)\circ\mathrm{lt}(\Theta) < \mathrm{lcm}\,(\mathrm{lt}(g_i), \mathrm{lt}(g_j))\circ\mathrm{lt}(\Theta). \tag{4.9}$$

From (4.7), (4.8) and (4.9), the claim immediately follows.

Claim 2: $\bar{g}_{ij} = 0$ or $\mathrm{lt}(\bar{g}_{ij} g_i\circ\Theta) < \mathrm{lcm}\,(\mathrm{lt}(g_i\circ\Theta), \mathrm{lt}(g_j\circ\Theta))$.

If $\bar{g}_{ij} = 0$, the claim is trivially true. Thus from now on assume that $\bar{g}_{ij} \neq 0$. Note

$$\begin{aligned}
\operatorname{lm}(\sigma(g_i\circ\Theta, g_j\circ\Theta)g_i\circ\Theta) &= \operatorname{lm}\left(\frac{\operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta))}{\operatorname{lm}(g_i\circ\Theta)} g_i\circ\Theta\right) \\
&= \operatorname{lm}\left(\frac{\operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta))}{\operatorname{lm}(g_i\circ\Theta)}\right) \operatorname{lm}(g_i\circ\Theta) \\
&= \frac{\operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta))}{\operatorname{lm}(g_i\circ\Theta)} \operatorname{lm}(g_i\circ\Theta) \\
&= \operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta)).
\end{aligned}$$

Note also

$$\begin{aligned}
\operatorname{lm}(c\sigma(g_i, g_j)\circ\Theta g_i\circ\Theta) &= c \operatorname{lm}\left[\left(\frac{\operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))}{\operatorname{lm}(g_i)}\right)\circ\Theta g_i\circ\Theta\right] \\
&= c \operatorname{lm}\left[\left(\frac{\operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))}{\operatorname{lm}(g_i)}\right)\circ\Theta\right] \operatorname{lm}(g_i\circ\Theta) \\
&= c \left(\frac{\operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))}{\operatorname{lm}(g_i)}\right)\circ\operatorname{lm}(\Theta) \operatorname{lm}(g_i\circ\Theta) \\
&= c \frac{\operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))\circ\operatorname{lm}(\Theta)}{\operatorname{lm}(g_i)\circ\operatorname{lm}(\Theta)} \operatorname{lm}(g_i\circ\Theta) \ \square \\
&\qquad \text{from (B) and Lemma 4.1} \\
&= c\frac{\operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))\circ\operatorname{lm}(\Theta)}{\operatorname{lm}(g_i)\circ\operatorname{lm}(\Theta)} \operatorname{lm}(g_i)\circ\operatorname{lm}(\Theta) \\
&= c \operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))\circ\operatorname{lm}(\Theta) \\
&= \operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))\circ\operatorname{lt}(\Theta) \ \square \\
&\qquad \text{from (B) and Lemmas 4.3 and 4.1} \\
&= \operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta)).
\end{aligned}$$

Thus, the two polynomials $\sigma(g_i\circ\Theta, g_j\circ\Theta)g_i\circ\Theta$ and $c\sigma(g_i, g_j)\circ\Theta g_i\circ\Theta$ have the same leading monomial, namely $\operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta))$. Hence, we have

$$\operatorname{lt}(\bar{g}_{ij} g_i\circ\Theta) < \operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta)).$$

Claim 3: $\bar{g}_{ji} = 0$ or $\operatorname{lt}(\bar{g}_{ji} g_j\circ\Theta) < \operatorname{lcm}(\operatorname{lt}(g_i\circ\Theta), \operatorname{lt}(g_j\circ\Theta))$.

The proof is essentially the same as that for *Claim 2*. We only need to switch i and j. □

Finally we are ready to state the sufficiency side of the main theorem.

Theorem 4.1. (Sufficiency) *Let*

(A) *the composition by* Θ *commutes with Groebner basis computation; and*

(B) *the composition by* Θ *be*

  (a) *compatible with the term ordering* $>$ *and*

  (b) *compatible with the nondivisibility.*

Then (B) $\Longrightarrow$ (A).

Proof. Assume (B). By Lemma 4.6, we have

$$\forall G \, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G \circ \Theta)\ ].$$

By Lemma 4.5, we have

$$\forall F\, \forall G \, [\ \mathrm{GB}(G, F) \implies \mathrm{GB}(G \circ \Theta, F \circ \Theta)\ ].$$

By Definition 3.2, it is exactly the condition (A). □

5. Proof of Necessity

In this section, we prove the necessity of the compatibility condition for commutativity, that is, we prove that (A) of the main theorem implies (B).

Before plunging into the detail of the 'long' proof, we describe the overall strategy. Mostly the proof is by proving contrapositive. Thus, it goes like this. Assume that (B) is not true. Then find G such that $\mathrm{GB}(G)$ but not $\mathrm{GB}(G \circ \Theta)$. Obviously the main difficulty in this process lies in finding such G. I had to spend numerous days (experimenting with computer algebra systems, making conjectures, disproving them to my dismay, dreaming about them in my sleep, etc., as usual) to find the ones presented here. Once they have been found, it was easy to write down the 'straight-line forward' proof. Lemmas 5.4 and 5.5 are the cores of the proof, that is, they contain such Gs as those mentioned above.

Lemma 5.1. *Let*

(A) $\forall F\, \forall G \, [\ \mathrm{GB}(G, F) \implies \mathrm{GB}(G \circ \Theta, F \circ \Theta)\ ]$*; and*

(B) $\forall G \, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G \circ \Theta)\ ]$.

Then (A) $\implies$ (B).

Proof. Assume (A). We need to prove (B). Let G be arbitrary but fixed such that $\mathrm{GB}(G)$. We need to show that $\mathrm{GB}(G \circ \Theta)$. Since $\mathrm{GB}(G)$, we trivially have $\mathrm{GB}(G, G)$. Then from (A), we have $\mathrm{GB}(G \circ \Theta, G \circ \Theta)$. Thus, we have $\mathrm{GB}(G \circ \Theta)$. □

Lemma 5.2. *Let*

(A) $\forall G \, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G \circ \Theta)\ ]$.

(B) $\forall p \forall q \forall a \forall b\ [\, p > q \wedge a \neq 0 \wedge b \neq 0 \implies ap \circ \Theta \neq bq \circ \Theta\,]$.

Then (A) $\implies$ (B).

Proof. Assume (A). We need to show (B). Let p, q, a, and b be arbitrary but fixed such that $p > q, a \neq 0$ and $b \neq 0$. We need to show that $ap \circ \Theta \neq bq \circ \Theta$.

Let $G = \{ap - bq\}$. Since $p > q, a \neq 0$ and $b \neq 0$, we have $ap \neq bq$. Thus we have $\mathrm{GB}(G)$. From (A), we have $\mathrm{GB}(G \circ \Theta)$, and thus $\mathrm{GB}(\{ap \circ \Theta - bq \circ \Theta\})$. Since a Groebner basis must not have a zero polynomial, we conclude that $ap \circ \Theta \neq bq \circ \Theta$. □

Lemma 5.3. *Let*

(A) $\forall G \, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G \circ \Theta)\ ]$*; and*

(B) $\forall p \forall q \, [\ p > q \implies p \circ \mathrm{lt}(\Theta) \neq q \circ \mathrm{lt}(\Theta)\,]$.

Then (A) $\implies$ (B).

Proof. Assume (A). We need to show (B). Let p and q be arbitrary but fixed such that $p > q$. We need to show that $p{\circ}\mathrm{lt}(\Theta) \neq q{\circ}\mathrm{lt}(\Theta)$. We will prove this by contradiction. Thus assume that $p{\circ}\mathrm{lt}(\Theta) = q{\circ}\mathrm{lt}(\Theta)$.

Let

$$a = \frac{1}{\mathrm{lc}(p{\circ}\mathrm{lm}(\Theta))}$$
$$b = \frac{1}{\mathrm{lc}(q{\circ}\mathrm{lm}(\Theta))}.$$

Obviously $a \neq 0$ and $b \neq 0$.

Let $G = \{ap, bq\}$. Clearly $\mathrm{GB}(G)$. Thus, from (A), we have $\mathrm{GB}(G{\circ}\Theta)$, and therefore $\mathrm{GB}(\{ap{\circ}\Theta, bq{\circ}\Theta\})$. Let $f = ap{\circ}\Theta - bq{\circ}\Theta$. Clearly $f \in \mathrm{Ideal}(G{\circ}\Theta)$. From Lemma 5.2, we have $f \neq 0$. Note

$$\mathrm{lm}(ap{\circ}\Theta) = ap{\circ}\mathrm{lm}(\Theta) = p{\circ}\mathrm{lt}(\Theta)$$
$$\mathrm{lm}(bq{\circ}\Theta) = bq{\circ}\mathrm{lm}(\Theta) = q{\circ}\mathrm{lt}(\Theta).$$

Since $p{\circ}\mathrm{lt}(\Theta) = q{\circ}\mathrm{lt}(\Theta)$, we have $\mathrm{lm}(ap{\circ}\Theta) = \mathrm{lm}(bq{\circ}\Theta)$. Thus we have

$$\mathrm{lt}(f) < \mathrm{lt}(ap{\circ}\Theta)$$
$$\mathrm{lt}(f) < \mathrm{lt}(bq{\circ}\Theta).$$

So

$$\mathrm{lt}(ap{\circ}\Theta) \not| \, \mathrm{lt}(f)$$
$$\mathrm{lt}(bq{\circ}\Theta) \not| \, \mathrm{lt}(f).$$

Thus, by Proposition 2.1, $G{\circ}\Theta$ is not a Groebner basis. Contradiction. □

Lemma 5.4. *Let*

(A) $\forall G\, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G{\circ}\Theta)\ ]$; *and*

(B) $\forall p \forall q\, [\ p > q \implies p{\circ}\mathrm{lt}(\Theta) > q{\circ}\mathrm{lt}(\Theta)\ ]$.

Then (A) $\implies$ (B).

Proof. Assume (A). We need to show (B). Let p and q be arbitrary but fixed such that $p > q$. We need to show that $p{\circ}\mathrm{lt}(\Theta) > q{\circ}\mathrm{lt}(\Theta)$.

Let $G = \{p + q, q\}$. We claim that $\mathrm{GB}(G)$. For this, let $f \in \mathrm{Ideal}(G)$. It suffices to show that $\mathrm{lt}(p + q) \mid \mathrm{lt}(f)$ or $\mathrm{lt}(q) \mid \mathrm{lt}(f)$. Note that $\{p, q\}$ is a Groebner basis and that $\mathrm{Ideal}(\{p, q\}) = \mathrm{Ideal}(\{p+q, q\}) = \mathrm{Ideal}(G)$. Thus, $\{p, q\}$ is a Groebner basis of $\mathrm{Ideal}(G)$. From Proposition 2.1, we have

$$\mathrm{lt}(p) = p|\mathrm{lt}(f) \quad \text{or} \quad \mathrm{lt}(q) = q|\mathrm{lt}(f).$$

Since $p > q$, we also have

$$\mathrm{lt}(p + q) = p \quad \mathrm{lt}(q) = q.$$

Thus

$$\mathrm{lt}(p + q)|\mathrm{lt}(f) \quad \text{or} \quad \mathrm{lt}(q)|\mathrm{lt}(f).$$

By Proposition 2.1, we conclude that G is a Groebner basis.

Thus from (A), we have $\mathrm{GB}(G{\circ}\Theta)$. Now we will prove that $p{\circ}\mathrm{lt}(\Theta) > q{\circ}\mathrm{lt}(\Theta)$, by contradiction. Thus assume $p{\circ}\mathrm{lt}(\Theta) \leq q{\circ}\mathrm{lt}(\Theta)$.

From Lemma 5.3, we have $p \circ \mathrm{lt}(\Theta) \neq q \circ \mathrm{lt}(\Theta)$. Thus $p \circ \mathrm{lt}(\Theta) < q \circ \mathrm{lt}(\Theta)$. Note $G \circ \Theta = \{p \circ \Theta + q \circ \Theta, q \circ \Theta\}$. Thus, $p \circ \Theta = (p \circ \Theta + q \circ \Theta) - q \circ \Theta \in \mathrm{Ideal}(G \circ \Theta)$. Note

$$\begin{aligned} \mathrm{lt}(p \circ \Theta) &= p \circ \mathrm{lt}(\Theta) \\ \mathrm{lt}(q \circ \Theta) &= q \circ \mathrm{lt}(\Theta). \end{aligned}$$

Since $p \circ \mathrm{lt}(\Theta) < q \circ \mathrm{lt}(\Theta)$, we have that $\mathrm{lt}(p \circ \Theta + q \circ \Theta) = q \circ \mathrm{lt}(\Theta)$. We also have that $q \circ \mathrm{lt}(\Theta) \not| p \circ \mathrm{lt}(\Theta)$. Thus, we have

$$\begin{aligned} \mathrm{lt}(q \circ \Theta) &\not| \mathrm{lt}(p \circ \Theta) \\ \mathrm{lt}(p \circ \Theta + q \circ \Theta) &\not| \mathrm{lt}(p \circ \Theta). \end{aligned}$$

Thus, by Proposition 2.1, $G \circ \Theta$ is not a Groebner basis. Contradiction. □

Thus, we have proved one half: the commutativity implies the compatibility with the term ordering. Now, let us work on the other half: the commutativity implies the compatibility with the nondivisibility.

Lemma 5.5. *Let f and g be two non-zero polynomials in $K[x_1, \ldots, x_n]$ and let $\mathrm{lt}(f) = x_1^{\mu_1} \cdots x_n^{\mu_n}$ and $\mathrm{lt}(g) = x_1^{\nu_1} \cdots x_n^{\nu_n}$. Assume that $\mu_k \geq \nu_k > 0$ for some k. Then we have*
 (a) *$\{f, g\}$ is not a Groebner basis, or*
 (b) *$\{f + 1, g\}$ is not a Groebner basis.*

Proof. We will prove by contradiction. Thus, assume that both $\{f, g\}$ and $\{f + 1, g\}$ are Groebner bases. Since $\{f, g\}$ is a Groebner basis, by Corollary 2.1, there exists $\bar{f}$ and $\bar{g}$ such that
 (a1) $\mathrm{S}(f, g) = \bar{f} f + \bar{g} g$,
 (a2) $\bar{f} = 0$ or $\mathrm{lt}(\bar{f})\mathrm{lt}(f) < \mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))$,
 (a3) $\bar{g} = 0$ or $\mathrm{lt}(\bar{g})\mathrm{lt}(g) < \mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))$,
 (a4) none of the terms in $\bar{g}\mathrm{lt}(g)$ is divisible by $\mathrm{lt}(f)$.
Since $\mu_k > 0$, we have that $f + 1 \neq 0$ and that $\mathrm{lt}(f + 1) = \mathrm{lt}(f)$. Since $\{f + 1, g\}$ is a Groebner basis, by Corollary 2.1, there exists $\hat{f}$ and $\hat{g}$ such that
 (b1) $\mathrm{S}(f + 1, g) = \hat{f}(f + 1) + \hat{g} g$,
 (b2) $\hat{f} = 0$ or $\mathrm{lt}(\hat{f})\mathrm{lt}(f) < \mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))$,
 (b3) $\hat{g} = 0$ or $\mathrm{lt}(\hat{g})\mathrm{lt}(g) < \mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))$,
 (b4) none of the terms in $\hat{g}\mathrm{lt}(g)$ is divisible by $\mathrm{lt}(f)$.
Note

$$\begin{aligned} \mathrm{S}(f+1, g) &= \frac{\mathrm{lcm}(\mathrm{lt}(f+1), \mathrm{lt}(g))}{\mathrm{lm}(f+1)}(f+1) - \frac{\mathrm{lcm}(\mathrm{lt}(f+1), \mathrm{lt}(g))}{\mathrm{lm}(g)} g \\ &= \frac{\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))}{\mathrm{lm}(f)}(f+1) - \frac{\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))}{\mathrm{lm}(g)} g \\ &= \frac{\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))}{\mathrm{lm}(f)} f - \frac{\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))}{\mathrm{lm}(g)} g + \frac{\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))}{\mathrm{lm}(f)} \\ &= \mathrm{S}(f, g) + \frac{\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))}{\mathrm{lm}(f)}. \end{aligned}$$

Thus, from (a1) and (b1), we obtain that

$$\hat{f}(f+1)+\hat{g}g=\bar{f}f+\bar{g}g+\frac{\operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g))}{\operatorname{lm}(f)}.$$

Rewriting this, we obtain

$$\frac{\operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g))}{\operatorname{lm}(f)}-\hat{f}=(\hat{f}-\bar{f})f+(\hat{g}-\bar{g})g.$$

By multiplying out $\operatorname{lm}(f)$, we obtain that

$$\text{r.h.s} = \text{l.h.s}$$

where

$$\begin{aligned}\text{l.h.s} &= \operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g))-\hat{f}\operatorname{lm}(f),\\ \text{r.h.s} &= (\hat{f}-\bar{f})f\operatorname{lm}(f)+(\hat{g}-\bar{g})g\operatorname{lm}(f).\end{aligned}$$

Recalling (b2), we have $\hat{f}=0$ or $\operatorname{lt}(\hat{f})\operatorname{lt}(f)<\operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g))$. Thus, we have

$$\operatorname{lt}(\text{l.h.s}) = \operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g)).$$

From now on, we will show that $\operatorname{lt}(\text{r.h.s}) \neq \operatorname{lt}(\text{l.h.s})$. This will give us the desired contradiction.

Case 1: $\hat{f}=\bar{f}$ and $\hat{g}=\bar{g}$.

Obviously the r.h.s $=0$. Thus $\operatorname{lt}(\text{r.h.s}) \neq \operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g)) = \operatorname{lt}(\text{l.h.s})$.

Case 2: $\hat{f}=\bar{f}$ and $\hat{g}\neq\bar{g}$.

We have r.h.s $=(\hat{g}-\bar{g})g\operatorname{lm}(f)$. Thus

$$\begin{aligned}\operatorname{lt}(\text{r.h.s}) &= \operatorname{lt}(\hat{g}-\bar{g})\operatorname{lt}(g)\operatorname{lt}(f)\\ &\geq \operatorname{lt}(g)\operatorname{lt}(f)\\ &= \gcd(\operatorname{lt}(f),\operatorname{lt}(g))\operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g))\\ &> \operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g))\end{aligned}$$

since $\mu_k \geq \nu_k > 0$. Thus, $\operatorname{lt}(\text{r.h.s}) \neq \operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g)) = \operatorname{lt}(\text{l.h.s})$.

Case 3: $\hat{f}\neq\bar{f}$ and $\hat{g}=\bar{g}$.

We have r.h.s $=(\hat{f}-\bar{f})f\operatorname{lm}(f)$. Thus $\operatorname{lt}(\text{r.h.s})=\operatorname{lt}(\hat{f}-\bar{f})\operatorname{lt}(f)\operatorname{lt}(f)$. Hence

$$\deg_{x_k}(\operatorname{lt}(\text{r.h.s})) \geq 2\mu_k.$$

But we know that $\mu_k \geq \nu_k > 0$. Thus,

$$\deg_{x_k}(\operatorname{lt}(\text{l.h.s})) = \deg_{x_k}(\operatorname{lcm}(\operatorname{lt}(f),\operatorname{lt}(g))) = \max(\mu_k,\nu_k) = \mu_k.$$

Since $\mu_k > 0$, we have $\deg_{x_k}(\operatorname{lt}(\text{r.h.s})) \neq \deg_{x_k}(\operatorname{lt}(\text{l.h.s}))$. Thus $\operatorname{lt}(\text{r.h.s}) \neq \operatorname{lt}(\text{l.h.s}))$.

Case 4: $\hat{f}\neq\bar{f}$ and $\hat{g}\neq\bar{g}$.

We have r.h.s $=(\hat{f}-\bar{f})f\operatorname{lm}(f)+(\hat{g}-\bar{g})g\operatorname{lm}(f)$. Let

$$\begin{aligned}p &= \operatorname{lt}((\hat{f}-\bar{f})f\operatorname{lm}(f))\\ q &= \operatorname{lt}((\hat{g}-\bar{g})g\operatorname{lm}(f)).\end{aligned}$$

We will show that $p \neq q$, by contradiction. Thus assume $p=q$. Then we have

$$p=\operatorname{lt}(\hat{f}-\bar{f})\operatorname{lt}(f)\operatorname{lt}(f)=\operatorname{lt}(\hat{g}-\bar{g})\operatorname{lt}(g)\operatorname{lt}(f)=q.$$

So we have

$$\mathrm{lt}(\hat{f}-\bar{f})\mathrm{lt}(f)=\mathrm{lt}(\hat{g}-\bar{g})\mathrm{lt}(g).$$

Thus we have

$$\mathrm{lt}(f) \mid \mathrm{lt}(\hat{g}-\bar{g})\mathrm{lt}(g).$$

Hence we have

$$\mathrm{lt}(f) \mid r\,\mathrm{lt}(g)$$

for some term r in $\hat{g}$ or $\bar{g}$. This contradicts (a4) and (b4). Thus we conclude that $p \neq q$.

From this, we see that $\mathrm{lt}(\mathrm{r.h.s}) = p$ or $\mathrm{lt}(\mathrm{r.h.s}) = q$. However in the proofs of *Case 2* and *Case 3*, we have already shown that $q \neq \mathrm{lt}(\mathrm{l.h.s})$ and $p \neq \mathrm{lt}(\mathrm{l.h.s})$. Thus we conclude $\mathrm{lt}(\mathrm{r.h.s}) \neq \mathrm{lt}(\mathrm{l.h.s})$. □

LEMMA 5.6. *Let f and g be two non-zero polynomials in $K[x_1,\ldots,x_n]$ and let $\mathrm{lt}(f) = x_1^{\mu_1}\cdots x_n^{\mu_n}$ and $\mathrm{lt}(g) = x_1^{\nu_1}\cdots x_n^{\nu_n}$. Assume that the leading terms are* not *relatively prime, that is, $\mu_k > 0$ and $\nu_k > 0$ for some k. Then there exists $\lambda > 0$ such that*
(a) *$\{f^\lambda, g\}$ is not a Groebner basis, or*
(b) *$\{f^\lambda + 1, g\}$ is not a Groebner basis.*

PROOF. Let λ be such that $\lambda\mu_k \geq \nu_k$. Let $\hat{f} = f^\lambda$ and let $\mathrm{lt}(\hat{f}) = x_1^{\hat{\mu}_1}\cdots x_n^{\hat{\mu}_n}$. Then, we have $\hat{\mu}_k = \lambda\mu_k \geq \nu_k > 0$. The lemma follows immediately after applying Lemma 5.5 on $\hat{f}$ and g. □

LEMMA 5.7. *Let*
(A) $\forall G\ [\ \mathrm{GB}(G) \implies \mathrm{GB}(G\circ\Theta)\ ]$*; and*
(B) *the terms $\mathrm{lt}(\theta_1),\ldots,\mathrm{lt}(\theta_n)$ be pair-wise relatively prime.*
Then (A) $\implies$ (B).

PROOF. Assume (A). We need to show (B). We will show (B) by contradiction, thus assume that there exists a pair, say $\mathrm{lt}(\theta_i)$ and $\mathrm{lt}(\theta_j)$, $(i \neq j)$, that are *not* relatively prime.

By Lemma 5.6, for some $\lambda > 0$ we have that $\{\theta_i^\lambda, \theta_j\}$ is *not* a Groebner basis or $\{\theta_i^\lambda + 1, \theta_j\}$ is *not* a Groebner basis.

Case 1: $\{\theta_i^\lambda, \theta_j\}$ is *not* a Groebner basis.

Let $G = \{x_i^\lambda, x_j\}$. Clearly $\mathrm{GB}(G)$. But $G\circ\Theta = \{\theta_i^\lambda, \theta_j\}$ is not a Groebner basis. Contradiction to (A).

Case 2: $\{\theta_i^\lambda + 1, \theta_j\}$ is *not* a Groebner basis.

Let $G = \{x_i^\lambda + 1, x_j\}$. Clearly $\mathrm{GB}(G)$, since the leading terms are relatively prime. But $G\circ\Theta = \{\theta_i^\lambda + 1, \theta_j\}$ is not a Groebner basis. Contradiction to (A). □

LEMMA 5.8. *Let*
(A) $\forall G\ [\ \mathrm{GB}(G) \implies \mathrm{GB}(G\circ\Theta)\ ]$.
(B) $\forall j\ \ \mathrm{lt}(\theta_j) \neq 1$.
Then (A) $\implies$ (B).

PROOF. Assume (A). We need to prove (B). Let j be arbitrary but fixed. We need to show that $\text{lt}(\theta_j) \neq 1$. Note that $x_j > 1$ in any term ordering. Thus, from (A) and Lemma 5.4, we have

$$x_j \circ \text{lt}(\Theta) > 1 \circ \text{lt}(\Theta).$$

Hence

$$\text{lt}(\theta_j) > 1. \qquad \square$$

Lemma 5.9. *Let*

(A) $\forall G\ [\ \text{GB}(G) \implies \text{GB}(G \circ \Theta)\ ]$*; and*

(B) *the list* $\text{lt}(\Theta)$ *be a 'permuted powering', that is,* $\text{lt}(\Theta) = (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n})$ *for some permutation* π *of* $(1, \ldots, n)$ *and some* $\lambda_1, \ldots, \lambda_n > 0$.

Then (A) $\implies$ (B).

Proof. Assume (A). We need to show (B). Let $e = [e_{ij}]$ be the matrix where $e_{ij} = \deg_{x_i}(\text{lt}(\theta_j))$.

From Lemma 5.7, we know that the terms $\text{lt}(\theta_i)$ and $\text{lt}(\theta_j)$, $i \neq j$, are relatively prime. Therefore there exists at most one non-zero element in each row of e. From Lemma 5.8, we also know that $\forall j\ \ \text{lt}(\theta_j) \neq 1$. Therefore there exists at least one non-zero element in each column of e.

Thus, we see that there is exactly one non-zero element in each row and each column of e. Hence e is a permuted diagonal matrix, which is equivalent to (B). $\square$

Lemma 5.10. *Let*

(A) $\forall G\ [\ \text{GB}(G) \implies \text{GB}(G \circ \Theta)\ ]$.

(B) $\forall p \forall q\ [\ p \not| q \implies p \circ \text{lt}(\Theta) \not| q \circ \text{lt}(\Theta)\ ]$.

Then (A) $\implies$ (B).

Proof. Immediate from Lemma 5.9 and Lemma 4.2. $\square$

Lemma 5.11. *Let*

(A) $\forall G\ [\ \text{GB}(G) \implies \text{GB}(G \circ \Theta)\ ]$*; and*

(B) *the composition by* Θ *be*

  (a) *compatible with the term ordering* $>$ *and*

  (b) *compatible with the nondivisibility.*

Then (A) $\implies$ (B).

Proof. Follows immediately from Lemmas 5.4 and 5.10. $\square$

Finally, we are ready to state the necessity side of the main theorem.

Theorem 5.1. (Necessity) *Let*

(A) *the composition by* Θ *commute with Groebner basis computation; and*

(B) *the composition by* Θ *be*

  (a) *compatible with the term ordering* $>$ *and*

  (b) *compatible with the nondivisibility.*

Then (A) $\implies$ (B). $\square$

Proof. Assume (A). Recalling Definition 3.2, we have

$$\forall F\, \forall G\, [\ \mathrm{GB}(G, F) \implies \mathrm{GB}(G \circ \Theta, F \circ \Theta)\ ].$$

By Lemma 5.1, we have

$$\forall G\, [\ \mathrm{GB}(G) \implies \mathrm{GB}(G \circ \Theta)\ ].$$

By Lemma 5.11, we have (B). □

6. Examples of Compatible Compositions

In this section we give several examples of compatible compositions. Let us first recall the compatibility condition:

(a) The composition by Θ is compatible with the term ordering $>$.

(b) The composition by Θ is compatible with the nondivisibility.

By Lemma 4.2, we know that condition (b) is equivalent to the simpler condition:

(b′) The list $\mathrm{lt}(\Theta)$ is a 'permuted powering', that is, $\mathrm{lt}(\Theta) = (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n})$ for some permutation π of $(1, \ldots, n)$ and some $\lambda_1, \ldots, \lambda_n > 0$.

Proposition 6.1. *Every composition of the form*

$$\mathrm{lt}(\theta_i) = x_i^{\lambda}$$

where $\lambda > 0$ is a compatible composition, and thus commutes with Groebner basis computation.

Proof. Note that $\mathrm{lt}(\theta_i) = x_i^{\lambda}$. Thus it trivially satisfies the two compatibility conditions. □

Example 6.1. The above mentioned class of composition covers many naturally arising compositions. We list some of them, starting with the simple ones.

Scaling	$\theta_i = a_i x_i, a_i \neq 0$. For example, $\Theta = (2x_1, 3x_2)$.
Translation	$\theta_i = x_i - c_i$. For example, $\Theta = (x_1 - 2, x_2 + 3)$.
Powering	$\theta_i = x_i^{\lambda}, \lambda > 0$. For example, $\Theta = (x_1^2, x_2^2)$.
Univariate	$\theta_i \in K[x_i]$ of degree $\lambda > 0$. For example, $\Theta = (2x_1^4 - x_1^3 + 3x_1^2 - 2x_1 + 4, x_2^4 + 3x_2^3 - 2x_2^2 + x_2 - 3)$.
General	$\theta_i \in K[x_1, \ldots, x_n]$ such that $\mathrm{lt}(\theta_i) = x_i^{\lambda}, \lambda > 0$. For example, $\Theta = (2x_1^4 - 2x_1 x_2^2 + 4x_2^3 - 1, x_2^4 - 2x_2^2 x_1^2 + x_2 x_1^2 + 3)$ for the graded lexicographic ordering $(x_2 > x_1)$.□

Proposition 6.2. *Let $>$ be a lexicographic ordering. Then, every composition of the form*

$$\mathrm{lt}(\theta_i) = x_i^{\lambda_i}$$

where $\lambda_i > 0$ is a compatible composition, and thus commutes with Groebner basis computation. Note that we now allow different λ_i for different x_i.

Proof. Note that $\mathrm{lt}(\theta_i) = x_i^{\lambda_i}$. Thus it trivially satisfies the condition (b$'$). One can also easily verify that it satisfies condition (a) also. □

Example 6.2. We list several compatible compositions for the lexicographic term ordering.

Powering	$\theta_i = x_i^{\lambda_i}, \lambda_i > 0$. For example, $\Theta = (x_1^2, x_2^3)$.
Univariate	$\theta_i \in K[x_i]$ of degree $\lambda_i > 0$. For example, $\Theta = (2x_1^3 - x_1^2 + 3x_1 + 4, x_2^4 + 3x_2^3 - 2x_2^2 + x_2 - 3)$.
General	$\theta_i \in K[x_1, \ldots, x_n]$ such that $\mathrm{lt}(\theta_i) = x_i^{\lambda_i}, \lambda_i > 0$. For example, $\Theta = (2x_1^4 - 2x_1^2 + 1, x_2^2 - 2x_2x_1^2 + x_1^5 + 3)$ for $x_2 > x_1$.□

So far, all the examples have one thing in common: $\mathrm{lt}(\theta_i)$ involves x_i, that is, no permutation of variables. Now we consider an example with a permutation.

Example 6.3. Let $p = x_1^{\mu_1} x_2^{\mu_2}$ and $q = x_1^{\nu_1} x_2^{\nu_2}$ be two terms in $K[x_1, x_2]$. Consider the term ordering defined by:

$$p < q \iff \mu_1 + \sqrt{2}\mu_2 < \nu_1 + \sqrt{2}\nu_2.$$

We claim that the composition by $\Theta = (x_2 + x_1, x_1^2 + x_2)$ is a compatible composition. Let us verify this. Note that $\mathrm{lt}(\Theta) = (x_2, x_1^2)$. Note that the variables permute. One can easily check that condition (b$'$) is satisfied. In order to check condition (a), let $p < q$, we need to show that $p \circ \mathrm{lt}(\Theta) < q \circ \mathrm{lt}(\Theta)$. For this, note

$$\begin{aligned} p \circ \mathrm{lt}(\Theta) &= x_2^{\mu_1} x_1^{2\mu_2} = x_1^{\mu_1'} x_2^{\mu_2'} \\ q \circ \mathrm{lt}(\Theta) &= x_2^{\nu_1} x_1^{2\nu_2} = x_1^{\nu_1'} x_2^{\nu_2'}. \end{aligned}$$

Thus

$$\begin{aligned} \mu_1' + \sqrt{2}\mu_2' &= 2\mu_2 + \sqrt{2}\mu_1 = \sqrt{2}(\mu_1 + \sqrt{2}\mu_2) \\ \nu_1' + \sqrt{2}\nu_2' &= 2\nu_2 + \sqrt{2}\nu_1 = \sqrt{2}(\nu_1 + \sqrt{2}\nu_2). \end{aligned}$$

Hence, one sees immediately that $\mu_1' + \sqrt{2}\mu_2' < \nu_1 + \sqrt{2}\nu_2'$. Thus $p \circ \mathrm{lt}(\Theta) < q \circ \mathrm{lt}(\Theta)$. □

7. Related Questions and Problems

In this paper, we have answered the question: When does a composition commute with Groebner basis computation? The answer is: *iff it is compatible with the term ordering and the nondivisibility.* However, this is not the end as it raises many new questions/problems. We list a few of them.

(Q1) Does there exist a decision procedure that will determine whether a given composition is compatible with a given term ordering. If so, find one.

In order to answer this question, the question itself will have to be made precise. In particular, one will have to clarify the meaning of the phrase 'a given term ordering', that is, one will have to find suitable finite representations of term orderings. For instance, it could be given as an oracle that tells whether a given term is greater than another given term. It could also be given as a collection of orthogonal vectors (Robbiano, 1986), or a single vector (Weispfenning, 1987; Ritter and Weispfenning, 1991), etc.

(Q2) When does a composition commute with the *reduced* Groebner basis computation?

One can easily construct an example that shows that the two conditions given in this paper are not sufficient. An answer to this question will shed new light on the notion of 'reduced'.

(Q3) Let G be a Groebner basis of F with respect to $>$. When is $G \circ \Theta$ a Groebner basis of $F \circ \Theta$ (possibly with respect to *another* term ordering $>'$)?

In order to answer this question, one could carefully analyze the proof given in this paper, and generalize it. In fact, the author has already followed this approach and found some answer, which is reported in another paper (Hong, 1996), but it might be interesting to find a completely new approach.

Acknowledgements

This research was done in the framework of the European Union project ACCLAIM sponsored by Austrian Science Foundation.

References

Barton, D., Zippel, R. (1985). Polynomial decomposition algorithms. *J. Symb. Comput.* **1**, 159–168.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases - A Computational Approach to Commutative Algebra, Graduate Texts in Mathematics.* New York: Springer.

Binder, F. (1996). Fast computations in the lattice of polynomial rational function fields. In *ISSAC-96*, pp. 43–48. New York: ACM Press.

Buchberger, B. (1965). *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal* . PhD thesis, Universitat Innsbruck, Institut fur Mathematik. In German.

Buchberger, B. (1985). Groebner bases: an algorithmic method in polynomial ideal theory. In Bose, N.K. ed., *Recent Trends in Multidimensional Systems Theory*, Chapter 6. Dordrecht: D. Riedel.

Cheng, C., McKay, J. H., Wang, S. (1995). A chain rule for multivariate resultants. *Proc. Amer. Math. Soc.* **123**, 1037–1047.

Cox, D., Little, J., ÓShea, D. (1992). *Ideals, Varieties, and Algorithms, Undergraduate Texts in Mathematics.* New York: Springer.

Hong, H. (1995). Multivariate resultants under composition. Technical Report 95-56, Research Institute for Symbolic Computation, Johannes Kepler University A-4040 Linz, Austria. Submitted for publication.

Hong, H. (1996). Groebner basis under composition II. In *Proceedings of ISSAC 96 (International Symposium on Symbolic and Algebraic Computation)*, pp. 79–85. New York: ACM Press.

Hong, H. (1997). Subresultant under composition. *J. Symb. Comput.* **23**, 355–365.

Kozen, D., Landau, S. (1989). Polynomial decomposition algorithms. *J. Symb. Comput.* **7**, 445–456.

McKay, J., Wang, S. (1989). A chain rule for the resultant of two polynomials. *Arch. Math.* **53**, 347–351.

Ritter, G., Weispfenning, V. (1991). On the number of term orders. *Applic. Algeb. Eng. Comm. Comput.* **2**, 55–79.

Robbiano, L. (1986). On the theory of graded structures. *J. Symb. Comput.* **2**, 139–170.

Von zur Gathen, J. (1990a). Functional decomposition of polynomials: the tame case. *J. Symb. Comput.* **9**, 281–300.

Von zur Gathen, J. (1990b). Functional decomposition of polynomials: the wild case. *J. Symb. Comput.* **10**, 437–452.

Weispfenning, V. (1987). Admissible orderings and linear forms. *SIGSAM Bulletin* **21**, 16–18.

Originally received 28 December 1995
Accepted 15 August 1996