Groebner Basis Under Composition II

Hoon Hong
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria
e-mail: hhong@risc.uni-linz.ac.at

Abstract

Composition is an 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 (possibly under different term orderings)?* We prove that this happens if the leading terms of the composition polynomials form "permuted powering". This is a sequel to another paper where we dealt with a more restricted question (that required same term ordering).

1 Introduction

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

This paper is a sequel to another paper (Hong 1995a) where we already gave a complete answer to the more restricted question: When does Groebner basis computation commute with composition under the *same* term ordering?.

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.

In the previous paper, we gave a complete answer to the question: When is G^* a Groebner basis of F^* under the *same* term ordering $>$? In this paper, we investigate a more general question: When is G^* a Groebner basis of F^* under *some* term ordering (possibly different from $>$)?

The main contribution of this paper is to provide a sufficient condition for the question: G^* is a Groebner basis of F^* under certain term ordering *if the leading terms of Θ are "permuted powering".*

This result could be applied in various ways. One natural application is in the computation of 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) occur often in real-life problem solving because the underlying mathematical models are usually hierarchically structured.

The reader might be also interested in related paper (Hong 1995c, Hong 1995b) where we study how other fundamental operations such as subresultants and multivariate resultants (Macaulay) behave under composition.

There are also some related works by Faugere, Gianni, Lazard, and Mora (Gianni and Mora 1987, Faugere *et al.* 1993), where an efficient method for computing zero-dimensional Groebner bases is described. Since the method works by change of term orderings, there might be some internal connection between their findings and ours. This needs more careful investigation.

The structure of the paper is as follows. In Section 2, we briefly review the terminology and the results of 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, we prove the main theorem. In Section 5, we illustrate the use of the main theorem by several examples.

2 Review of Groebner Basis Theory

In this section, we will review some basic terminology and results of 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 get familiar with the notational convention. The details (and proofs) can be found in the original papers (Buchberger 1965, Buchberger 1985) or the textbooks (Cox *et al.* 1992, Becker and Weispfenning 1993, Mishra 1993).

Notations/Definitions 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* $e_1, \ldots, e_n \in \mathbf{N}$.[1]
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.
$>$	*an admissible term ordering, that is, a binary relation over terms such that* ⋄ $\forall p \forall q \forall r\ [\ p > q \Longrightarrow pr > qr\ ]$, ⋄ $\forall p\ [\ p \neq 1 \Longrightarrow p > 1\ ]$, ⋄ $>$ *is a linear ordering.*
$\mathrm{lt}_>(f)$	*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 under* $>$, *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* $\mathrm{Ideal}(F)$ *under* $>$, *that is,* ⋄ $GB(G)$, ⋄ $\mathrm{Ideal}(G) = \mathrm{Ideal}(F)$.
$\mathrm{lcm}(p, q)$	*the least common multiple of* p *and* q.
$\sigma_>(f, g)$	$\mathrm{lcm}\,(\mathrm{lt}_>(f), \mathrm{lt}_>(g))\ /\ \mathrm{lm}_>(f)$.
$\mathrm{S}_>(f, g)$	*the S-polynomial of* f *and* g *under* $>$, *that is,* $\sigma_>(f, g)f - \sigma_>(g, f)g$.

[1]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, Becker and Weispfenning 1993)) define a term as a monomial with coefficient 1. We follow (Buchberger 1985).

Theorem 1 (Buchberger 1965) *The followings 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 of the Groebner basis theory. Note that the statement of the theorem, in particular the condition (b), is slightly different from the usual one found in (Buchberger 1965, Buchberger 1985, Cox *et al.* 1992, Becker and Weispfenning 1993), in that the usual one has $\mathrm{lt}_>(\mathrm{S}_>(g_i, g_j))$ in place of $\mathrm{lcm}(\mathrm{lt}_>(h_k)\mathrm{lt}_>(g_k))$ and $\leq$ in place of $<$. But the proofs for both are essentially the same. In the subsequent sections, we will make an *essential* use of the formulation given above.

3 Main Result

In this section, we make precise the main result described in the introduction. For this, we fix some notations and notions. These will be used throughout the paper.

Notations 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* $(\ \mathrm{lm}_>(\theta_1), \ldots, \mathrm{lm}_>(\theta_n)\ )$.
$\mathrm{Mat}(\mathrm{lt}_>(\Theta))$	*the exponent matrix of* $\mathrm{lt}_>(\Theta)$, *that is, the* n *by* n *matrix whose* (i, j)*-th entry is* $\deg_{x_i}(\mathrm{lt}_>(\Theta_j))$. *In other words, the* j*-th column of the matrix consists of the exponents of the leading term of* θ_j.

Definition 1 (Composition on Polynomials) *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* $\{\ h \circ \Theta \mid h \in H\ \}$. □

Definition 2 (Composition on Orderings) *The* composition *of* $>$ *by* Θ, *written as* $>\circ\Theta$, *is the binary relation over the terms defined by*

$$\forall p \forall q\, [\, p >\circ\Theta\, q \iff p\circ \mathrm{lt}_>(\Theta) > q\circ \mathrm{lt}_>(\Theta)\,].\ \square$$

Note that the relation $>\circ\Theta$ is not necessarily an admissible term ordering. As a simple counter example, consider a univariate case where $\Theta = (1)$. Obviously $x_1\circ\mathrm{lt}_>(\Theta) = 1 = 1\circ\mathrm{lt}_>(\Theta)$, and thus it *not* true that $x_1 >\circ\Theta 1$, which violates one of the conditions of an admissible term ordering (Notation/Definition 1). But in Lemma 4, we will show that the relation $>\circ\Theta$ is indeed an admissible term ordering iff the exponent matrix $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ is non-singular.

Definition 3 (Permuted Powering) *A list* $\mathrm{lt}_>(\Theta)$ *is called a* permuted powering *iff* $\mathrm{lt}_>(\Theta) = (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n})$ *for some permutation* π *of* $(1, \ldots, n)$ *and some* $\lambda_1, \ldots, \lambda_n > 0$. *In other words, the exponent matrix* $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ *is a permutation of a diagonal matrix with all positive diagonal entries.* $\square$

Let $\mathrm{lt}_>(\Theta)$ be a permuted powering. Then its exponent matrix is obviously non-singular, and thus, the binary relation $>\circ\Theta$ is an admissible term ordering. Now we are ready to state the main theorem of this paper.

Theorem 2 (Main Theorem) *If* $\mathrm{lt}_>(\Theta)$ *be a permuted powering then we have*

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

The following section is devoted to proving this theorem.

4 Proof

In this section, we prove the main theorem of this paper (Theorem 2). The proof is divided into several lemmas, which are interesting on their own. 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 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) $\mathrm{lt}_>(p\circ\Theta) = p\circ\mathrm{lt}_>(\Theta)$. $\square$

Proof. Immediate from their definitions. $\square$

Now we prove that the relation $>\circ\Theta$ is an admissible term ordering iff its exponent matrix is non-singular. I know of two different approaches for proving this. One is to recall the characterizations of admissible term orderings by one or more orthogonal vectors (Robbiano 1986, Weispfenning 1987). The other is to reason directly with the definition of admissible term ordering. Below, I will give the one based directly on the definition, since it is more elementary and self-contained.

We will need to refer to $>\circ\Theta$ numerous times. For notational simplicity, we will use the following short hand.

Notations 2 (Short-hand)

$>'$ *the binary relation* $>\circ\Theta$. $\square$

Lemma 1 $\forall p \forall q \forall r\, [\, p >' q \Rightarrow pr >' qr\,]$ *is true for arbitrary* Θ. $\square$

Proof. Let Θ, p, q, and r be arbitrary but fixed such that $p >' q$. Then we have $p\circ\mathrm{lt}_>(\Theta) > q\circ\mathrm{lt}_>(\Theta)$. Since $>$ is an admissible term ordering, we have $p\circ\mathrm{lt}_>(\Theta) r\circ\mathrm{lt}_>(\Theta) > q\circ\mathrm{lt}_>(\Theta) r\circ\mathrm{lt}_>(\Theta)$. Hence, $(pr)\circ\mathrm{lt}_>(\Theta) > (qr)\circ\mathrm{lt}_>(\Theta)$, which is equivalent to $pr >' qr$. $\square$

Lemma 2 *Let*

(A) *Every column of the exponent matrix* $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ *has at least one non-zero entry.*

(B) $\forall p\, [\, p \neq 1 \Rightarrow p >' 1\,]$

Then **(A)** $\iff$ **(B)**. $\square$

Proof. Let Θ be arbitrary but fixed and let e be its exponent matrix $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$. Note

$$\begin{array}{ll} & \forall p\, [\, p \neq 1 \Rightarrow p >' 1\,] \\ \text{iff} & \forall p\, [\, p \neq 1 \Rightarrow p\circ\mathrm{lt}_>(\Theta) > 1\circ\mathrm{lt}_>(\Theta)\,] \\ \text{iff} & \forall p\, [\, p \neq 1 \Rightarrow p\circ\mathrm{lt}_>(\Theta) > 1\,] \\ \text{iff} & \forall p\, [\, p \neq 1 \Rightarrow p\circ\mathrm{lt}_>(\Theta) \neq 1\,] \\ \text{iff} & \forall \mu \in \mathbf{N}^n\, [\, \mu \neq 0 \Rightarrow e\mu \neq 0\,] \end{array}$$

where $\mu = (\mu_1, \ldots, \mu_n)$ stands for the column vector of the exponents of the term p, that is, $p = x_1^{\mu_1} \cdots x_n^{\mu_n}$. The lemma follows immediately from the following two claims.

Claim 1: $\forall \mu \in \mathbf{N}^n [\mu \neq 0 \Rightarrow e\mu \neq 0]$ if $\forall j \exists i [e_{ij} \neq 0]$.

Assume that $\forall j \exists i\, [e_{ij} \neq 0]$. Let μ be arbitrary but fixed such that $\mu \neq 0$. We need to show that $e\mu \neq 0$. Since $\mu \neq 0$, we have $\mu_{j'} \neq 0$ for some j', Since $\forall j \exists i\, [e_{ij} \neq 0]$, we have $e_{i'j'} \neq 0$ for some i'. Thus, we have $e_{i'j'}\mu_{j'} \neq 0$. Hence, the i'-th element of $e\mu$ is non-zero, and thus $e\mu \neq 0$.

Claim 2: $\forall j \exists i[e_{ij} \neq 0]$ if $\forall \mu \in \mathbf{N}^n[\mu \neq 0 \Rightarrow e\mu \neq 0]$.

Assume $\forall \mu \in \mathbf{N}^n[\mu \neq 0 \Rightarrow e\mu \neq 0]$. Let j be arbitrary but fixed. We need to show that $\exists i[e_{ij} \neq 0]$. Let $\mu = (0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 is at the j-th position. Since $\mu \neq 0$, we have $e\mu \neq 0$. Thus for some i', we have $(e\mu)_{i'} \neq 0$. Since $(e\mu)_{i'} = \sum_{k=1}^n e_{i'k}\mu_k = e_{i'j}$, we have $e_{i'j} \neq 0$, and thus $\exists i[e_{ij} \neq 0]$. □

Lemma 3 *Let*

(A) *The exponent matrix* $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ *is non-singular.*

(B) *The binary relation* $>'$ *is a linear ordering.*

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

Proof. The lemma follows from the three claims below.

Claim 1: $>'$ is transitive for arbitrary Θ.

Immediate from the transitivity of $>$.

Claim 2: For every p and q at most one of the following holds: $p>'q$, $q>'p$, and $p = q$, for arbitrary Θ.

Immediate from the fact that $>$ is a trichotomy.

Claim 3: For every p and q at least one of the following holds: $p>'q$, $q>'p$, and $p = q$, iff the exponent matrix $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ is non-singular.

We will prove the contrapositive of this. Note that

$$\begin{array}{ll} & \exists p, q[p \not>' q \wedge q \not>' p \wedge p \neq q] \\ \text{iff} & \exists p, q[p \circ \mathrm{lt}_>(\Theta) \not> q \circ \mathrm{lt}_>(\Theta) \wedge q \circ \mathrm{lt}_>(\Theta) \not> p \circ \mathrm{lt}_>(\Theta) \\ & \quad \wedge p \neq q] \\ \text{iff} & \exists p, q[p \circ \mathrm{lt}_>(\Theta) = q \circ \mathrm{lt}_>(\Theta) \wedge p \neq q] \\ \text{iff} & \exists \mu, \nu \in \mathbf{N}^n[e\mu = e\nu \wedge \mu \neq \nu] \\ \text{iff} & \exists \mu, \nu \in \mathbf{N}^n[e(\mu - \nu) = 0 \wedge \mu - \nu \neq 0] \\ \text{iff} & \exists \alpha \in \mathbf{Z}^n[e\alpha = 0 \wedge \alpha \neq 0] \\ \text{iff} & \exists \alpha \in \mathbf{Q}^n[e\alpha = 0 \wedge \alpha \neq 0] \\ \text{iff} & \det(e) = 0 \end{array}$$

where e is the exponent matrix $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$, and where μ and ν are the column vectors of the exponents of p and q. □

Now we put together the previous three lemmas.

Lemma 4 (Composed term ordering) *Let*

(A) *The exponent matrix* $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ *is non-singular.*

(B) *The binary relation* $>\circ\Theta$ *is an admissible term ordering.*

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

Proof. Immediate from the last three lemmas (Lemmas 1, 2, and 3). □

From now on, the main strategy of the proof is similar to the one used in (Hong 1995a) where we investigated a more restricted problem. In fact, the proof given here is a careful generalization/adjustment of the one given in (Hong 1995a). For the reader who might want to compare the two proofs (in order to find out where the proofs differ), I tried my best to keep the structure and the notations as close as possible to those in (Hong 1995a). But one should be careful to notice numerous subtle and essential differences. In particular, one should pay attention to the places where $>'$ is used instead of $>$.

Lemma 5 *Let*

(A) $>'$ *is an admissible 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 $p_1 >' p_2 >' \cdots >' p_t$. (Note that $f \neq 0$ by the convention in Notation/Definition 1). Thus, we have $f \circ \Theta = c_1p_1 \circ \Theta + \cdots + c_tp_t \circ \Theta$. From Proposition 1 (d) and (h), we have $\mathrm{lt}_>(c_ip_i \circ \Theta) = p_i \circ \mathrm{lt}_>(\Theta)$. Recalling the definition of $>'$, $p_1 \circ \mathrm{lt}_>(\Theta) > p_2 \circ \mathrm{lt}_>(\Theta) > \cdots > p_t \circ \mathrm{lt}_>(\Theta)$. Thus, we have $\mathrm{lt}_>(c_1p_1 \circ \Theta) > \mathrm{lt}_>(c_2p_2 \circ \Theta) > \cdots > \mathrm{lt}_>(c_tp_t \circ \Theta)$. Hence, from Proposition 1 (c)–(h) we conclude that $\mathrm{lm}_>(f \circ \Theta) = \mathrm{lm}_>(c_1p_1 \circ \Theta) = c_1p_1 \circ \mathrm{lm}_>(\Theta) = \mathrm{lm}_{>'}(f) \circ \mathrm{lm}_>(\Theta)$ and $\mathrm{lt}_>(f \circ \Theta) = \mathrm{lt}_>(c_1p_1 \circ \Theta) = p_1 \circ \mathrm{lt}_>(\Theta) = \mathrm{lt}_{>'}(f) \circ \mathrm{lt}_>(\Theta)$. □

Lemma 6 *Let*

(A) *Every row of the exponent matrix* $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ *has at most one non-zero element.*

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

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

Proof. Let us first translate the condition **(B)** into more convenient form. For this, let

$$\begin{array}{rcl} e & = & \mathrm{Mat}(\mathrm{lt}_>(\Theta)) \\ p & = & x_1^{\mu_1} \cdots x_n^{\mu_n} \\ q & = & x_1^{\nu_1} \cdots x_n^{\nu_n} \\ r & = & x_1^{\lambda_1} \cdots x_n^{\lambda_n} = \mathrm{lcm}(p \circ \mathrm{lt}_>(\Theta), q \circ \mathrm{lt}_>(\Theta)) \\ s & = & x_1^{\eta_1} \cdots x_n^{\eta_n} = \mathrm{lcm}(p, q) \circ \mathrm{lt}_>(\Theta). \end{array}$$

After some simple calculation, one sees that

$$\begin{array}{rcl} \lambda_i & = & \max\left(\sum_{j=1}^n e_{ij}\mu_j, \sum_{j=1}^n e_{ij}\nu_j\right) \\ \eta_i & = & \sum_{j=1}^n e_{ij} \max(\mu_j, \nu_j). \end{array}$$

Thus the condition **(B)** is equivalent to

(B') $\forall \mu, \nu \in \mathbf{N}^n \forall i [\lambda_i = \eta_i]$.
Hence it sufficient to prove that **(A)** $\Longleftrightarrow$ **(B')**.

$\Longrightarrow$. Assume **(A)**. We need to show **(B')**. Let μ, ν, and i be arbitrary but fixed. We need to show that $\lambda_i = \eta_i$.
Case 1: The i-th row of e does not have non-zero entry.
Then trivially $\lambda_i = 0 = \eta_i$.
Case 2: The i-th row of e has exactly one non-zero entry.
Let $e_{ij} \neq 0$. Then $\lambda_i = \max(e_{ij}\mu_j, e_{ij}\nu_j) = e_{ij}\max(\mu_j, \nu_j) = \eta_i$.

$\Longleftarrow$. Assume **(B')**. We need to show **(A)**. Let i be arbitrary but fixed. We need to show that there is at most one non-zero entry in the i-th row of e. We will show this by contradiction, thus assume that there are at least two non-zero entries in the i-th row of e, say e_{ij_1} and e_{ij_2}. Let $\mu = (0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 is at the j_1-th position. Let $\nu = (0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 is at the j_2-th position. A simple calculation shows that $\lambda_i = \max(e_{ij_1}, e_{ij_2})$ and $\eta_i = e_{ij_1} + e_{j_2}$. Since $e_{ij_1} \neq 0$ and $e_{ij_2} \neq 0$, we have $\lambda_i \neq \eta_i$. Contradiction to **(B')**. $\square$

We "bundle" all the previous lemmas into the following lemma (under some restriction). It will be used frequently and essentially in proving the next lemma (Lemma 8, which forms the core of the proof of the main theorem).

Lemma 7 *Let*
(A) *The list* $\mathrm{lt}_>(\Theta)$ *is a permuted powering.*
(B) (a) $>'$ *is an admissible term ordering.*
(b) *For all* p *and* q, $\mathrm{lcm}(p \circ \mathrm{lt}_>(\Theta), q \circ \mathrm{lt}_>(\Theta)) = \mathrm{lcm}(p, q) \circ \mathrm{lt}_>(\Theta)$.
(c) $\mathrm{lm}_>(f \circ \Theta) = \mathrm{lm}_{>'}(f) \circ \mathrm{lm}_>(\Theta)$.
(d) $\mathrm{lt}_>(f \circ \Theta) = \mathrm{lt}_{>'}(f) \circ \mathrm{lt}_>(\Theta)$.
Then **(A)** $\Longleftrightarrow$ **(B)**. $\square$

Proof. Assume **(A)**. We need to show **(B)**. Since $\mathrm{lt}_>(\Theta)$ is a permuted powering, $\det(\mathrm{Mat}(\mathrm{lt}_>(\Theta))) \neq 0$. Thus from Lemma 4, we have **(B)**(a). Since $\mathrm{lt}_>(\Theta)$ is a permuted powering, each row of $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ has at most one (in fact exactly one) non-zero entry. Thus from Lemma 6, we have **(B)**(b). From **(B)**(a) and Lemma 5, we also have **(B)**(c) and **(B)**(d).

Assume **(B)**. We need to show **(A)**. From **(B)**(a) and Lemma 4, we see that $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ is non-singular. From **(B)**(b) and Lemma 6, we see that each row of $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ has at most one non-zero entry. Thus, $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ must be a permuted diagonal matrix. $\square$

Lemma 8 *Let*
(A) $\mathrm{lt}_>(\Theta)$ *is a permuted powering.*
(B) $\forall G\, [\, \mathrm{GB}_{>'}(G) \implies \mathrm{GB}_>(G \circ \Theta)\,]$.
Then **(A)** $\Longrightarrow$ **(B)**. $\square$

Proof. Assume that $\mathrm{lt}_>(\Theta))$ is a permuted powering. 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 $\mathrm{GB}_{>'}(G)$, by Theorem 1, there exist $h_1, \ldots, h_t$ such that

$$\mathrm{S}_{>'}(g_i, g_j) = \sum_{k=1}^{t} h_k g_k \tag{1}$$

and

$$\forall k \;\, [\, h_k = 0 \,\vee\, \mathrm{lt}_{>'}(h_k g_k) <' \mathrm{lcm}(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j))\,]. \tag{2}$$

From (1) 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

$$\begin{aligned}
& \mathrm{S}_>(g_i \circ \Theta, g_j \circ \Theta) \\
= \;& \mathrm{S}_>(g_i \circ \Theta, g_j \circ \Theta) - c\mathrm{S}_{>'}(g_i, g_j) \circ \Theta + c\mathrm{S}_{>'}(g_i, g_j) \circ \Theta \\
= \;& \sigma_>(g_i \circ \Theta, g_j \circ \Theta) g_i \circ \Theta - \sigma_>(g_j \circ \Theta, g_i \circ \Theta) g_j \circ \Theta \\
& -c \left(\sigma_{>'}(g_i, g_j) g_i - \sigma_{>'}(g_j, g_i) g_j \right) \circ \Theta \\
& +c \sum_{k=1}^{t} h_k \circ \Theta \;\; g_k \circ \Theta \\
= \;& \sigma_>(g_i \circ \Theta, g_j \circ \Theta) g_i \circ \Theta - \sigma_>(g_j \circ \Theta, g_i \circ \Theta) g_j \circ \Theta \\
& -c\sigma_{>'}(g_i, g_j) \circ \Theta g_i \circ \Theta + c\sigma_{>'}(g_j, g_i) \circ \Theta g_j \circ \Theta \\
& +c \sum_{k=1}^{t} h_k \circ \Theta \;\; g_k \circ \Theta \\
= \;& \sum_{k=1}^{t} \hat{h}_k g_k \circ \Theta
\end{aligned}$$

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 1, it will be sufficient to show that

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

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 $\mathrm{lt}_>(ch_k \circ \Theta g_k \circ \Theta) < \mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right)$. 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 **(A)** and Lemma 7 we have

$$\mathrm{lt}_>(ch_k \circ \Theta g_k \circ \Theta) = \mathrm{lt}_{>'}(h_k g_k) \circ \mathrm{lt}_>(\Theta). \tag{3}$$

From (2) and the definition of $>'$ we have

$$\mathrm{lt}_{>'}(h_k g_k) \circ \mathrm{lt}_>(\Theta) < \mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right) \circ \mathrm{lt}_>(\Theta). \tag{4}$$

From **(A)** and Lemma 7 we have

$$\begin{aligned} & \mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right) \circ \mathrm{lt}_>(\Theta) \\ = \; & \mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i) \circ \mathrm{lt}_>(\Theta), \mathrm{lt}_{>'}(g_j) \circ \mathrm{lt}_>(\Theta)\right) \\ = \; & \mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right). \end{aligned} \tag{5}$$

From (3), (4) and (5), the claim immediately follows.

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

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

$$\begin{aligned} & \mathrm{lm}_> \left(\sigma_>(g_i \circ \Theta, g_j \circ \Theta) g_i \circ \Theta\right) \\ = \; & \mathrm{lm}_> \left(\frac{\mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right)}{\mathrm{lm}_>(g_i \circ \Theta)} g_i \circ \Theta\right) \\ = \; & \mathrm{lm}_> \left(\frac{\mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right)}{\mathrm{lm}_>(g_i \circ \Theta)}\right) \mathrm{lm}_>(g_i \circ \Theta) \\ = \; & \frac{\mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right)}{\mathrm{lm}_>(g_i \circ \Theta)} \mathrm{lm}_>(g_i \circ \Theta) \\ = \; & \mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right). \end{aligned}$$

Note also

$$\begin{aligned} & \mathrm{lm}_> \left(c\sigma_{>'}(g_i, g_j) \circ \Theta g_i \circ \Theta\right) \\ = \; & c \, \mathrm{lm}_> \left[\left(\frac{\mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right)}{\mathrm{lm}_{>'}(g_i)}\right) \circ \Theta g_i \circ \Theta\right] \\ = \; & c \, \mathrm{lm}_> \left[\left(\frac{\mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right)}{\mathrm{lm}_{>'}(g_i)}\right) \circ \Theta\right] \mathrm{lm}_>(g_i \circ \Theta) \\ = \; & c \left(\frac{\mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right)}{\mathrm{lm}_{>'}(g_i)}\right) \circ \mathrm{lm}_>(\Theta) \, \mathrm{lm}_>(g_i \circ \Theta) \\ = \; & c \, \frac{\mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right) \circ \mathrm{lm}_>(\Theta)}{\mathrm{lm}_{>'}(g_i) \circ \mathrm{lm}_>(\Theta)} \mathrm{lm}_>(g_i \circ \Theta) \\ & \qquad \text{From } \mathbf{(A)} \text{ and Lemma 7} \\ = \; & c \, \frac{\mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right) \circ \mathrm{lm}_>(\Theta)}{\mathrm{lm}_{>'}(g_i) \circ \mathrm{lm}_>(\Theta)} \mathrm{lm}_{>'}(g_i) \circ \mathrm{lm}_>(\Theta) \\ = \; & c \, \mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right) \circ \mathrm{lm}_>(\Theta) \\ = \; & \mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i), \mathrm{lt}_{>'}(g_j)\right) \circ \mathrm{lt}_>(\Theta) \\ & \qquad \text{From } \mathbf{(A)} \text{ and Lemma 7} \\ = \; & \mathrm{lcm}\left(\mathrm{lt}_{>'}(g_i) \circ \mathrm{lt}_>(\Theta), \mathrm{lt}_{>'}(g_j) \circ \mathrm{lt}_>(\Theta)\right) \\ = \; & \mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right). \end{aligned}$$

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 with respect to $<$, namely $\mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right)$. Hence, we have

$$\mathrm{lt}_>(\bar{g}_{ij} g_i \circ \Theta) < \mathrm{lcm}\left(\mathrm{lt}_>(g_i \circ \Theta), \mathrm{lt}_>(g_j \circ \Theta)\right).$$

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

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

Lemma 9 $\mathrm{Ideal}(G) = \mathrm{Ideal}(F) \implies \mathrm{Ideal}(G \circ \Theta) = \mathrm{Ideal}(F \circ \Theta)$. □

Proof. Easy. □

Lemma 10 *Let*
(A) $\forall F \, \forall G \, [\; \mathrm{GB}_{>'}(G, F) \implies \mathrm{GB}_>(G \circ \Theta, F \circ \Theta) \;]$.
(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

$$\mathrm{GB}_>(G \circ \Theta). \tag{6}$$

Since $\mathrm{GB}_{>'}(G, F)$, we have that $\mathrm{Ideal}(G) = \mathrm{Ideal}(F)$. Then from Lemma 9, we have

$$\mathrm{Ideal}(G \circ \Theta) = \mathrm{Ideal}(F \circ \Theta). \tag{7}$$

Putting together (6) and (7), we conclude that $\mathrm{GB}_>(G \circ \Theta, F \circ \Theta)$. □

Finally we are ready to state the main theorem.

Theorem 3 (Main Theorem) *If* $\mathrm{lt}_>(\Theta)$ *is a permuted powering then we have*

$$\forall F \forall G \, [\, GB_{> \circ \Theta}(G, F) \implies \mathrm{GB}_>(G \circ \Theta, F \circ \Theta) \,]. \; \square$$

Proof. Immediate from Lemmas 8 and 10. □

5 Examples

In this section we illustrate the use of the main theorem by several examples. First let us list some examples of compositions Θ which satisfy the condition in the main theorem, that is, $\mathrm{lt}_>(\Theta)$ is a permuted powering. The list shows that the class of permuted powering covers many naturally arising compositions.

Example 1 (Compositions)

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, $\Theta = (x_1 - 2, x_2 + 3)$.
Permutation	$\theta_i = x_{\pi_i}$ for some permutation π of $(1, \ldots, n)$. For example, $\Theta = (x_2, x_1)$.
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 $\mathrm{lt}_>(\theta_i) = x_{\pi_i}^{\lambda_i}$ for some permutation π of $(1, \ldots, n)$ and $\lambda_i > 0$. For example, $\Theta = (x_2^2 - 2x_2x_1^2 + x_1^5 + 3, 2x_1^4 - 2x_1^2 + 1)$ for $x_2 > x_1$.

□

Now we give two examples illustrating the algorithmic use of the main theorem of this paper. At this point, we do not yet have a stable implementation of Groebner basis algorithm that allows "arbitrary" term ordering. Thus the examples given here are a bit contrived in order to fit the problem to the capabilities of the implementation available to us. (the implementation in the computer algebra system Maple (Char *et al.* 1985)).

Example 2 Let

$$\begin{aligned} F &= \{x_1x_2x_3 - 1, x_1x_2 + x_1x_3 + x_2x_3, x_1 + x_2 + x_3\} \\ \Theta &= ((x_1^2 + x_2 + x_3)^3, (x_1 + x_2^2 + x_3)^3, (x_1 + x_2 + x_3^2)^3) \end{aligned}$$

We would like to compute a Groebner basis of $F \circ \Theta$ under the graded reverse lexicographic ordering where $x_1 > x_2 > x_3$.

A brute-force way is to input $F \circ \Theta$ to a Groebner basis algorithm. As far I am aware, any existing algorithm/implementations will expand $F \circ \Theta$ into a distributed form (a sum of monomials). The expanded form is huge. Maple takes about 330 seconds on IBMPC 486 to compute a Groebner basis, which is too huge to put in here.

A better way is to see if we can use the theorem of this paper. First, we trivially see that $\mathrm{lt}_>(\Theta)$ is a permuted powering. Thus the main theorem of this paper applies. Next one easily finds that $>' = >\circ\Theta$ is the same as $>$. (In general, whenever $\mathrm{Mat}(\mathrm{lt}_>(\Theta))$ is a diagonal matrix with the same diagonal entries, we have $>'=>$.) Hence we first compute a Groebner basis G of F under the graded reverse lexicographic ordering, obtaining

$$G = \{x_2x_3 + x_2^2 + x_3^2, x_1 + x_2 + x_3, -1 + x_3^3\}$$

in about 0.7 seconds. It takes about 0.1 seconds to compose G by Θ and to expand it, obtaining a Groebner basis of $F \circ \Theta$ under the graded reverse lexicographic ordering.

In fact, it is not necessary to actually carry out the composition of G and Θ. In most cases, it is more useful to keep the output in the decomposed form. For instance, one might want to apply a similar idea again on this de-composed form for some other operations, in a 'pipe-lined' fashion. □

Example 3 Let

$$\begin{aligned} F &= \{x_1x_2x_3 - 1, x_1x_2 + x_1x_3 + x_2x_3, x_1 + x_2 + x_3\} \\ \Theta &= ((x_1^3 + x_2 + x_3)^3, (x_1 + x_2^2 + x_3)^3, (x_1 + x_2 + x_3)^3) \end{aligned}$$

We would like to compute a Groebner basis of $F \circ \Theta$ under the following term ordering $>$ (weighted reverse lexicographic)

$$x_1^{\mu_1} x_2^{\mu_2} x_3^{\mu_3} > x_1^{\nu_1} x_2^{\nu_2} x_3^{\nu_3}$$

if

$$2\mu_1 + 3\mu_2 + 6\mu_3 > 2\nu_1 + 3\nu_2 + 6\nu_3.$$

We break the tie by the reverse lexicographic ordering where $x_1 > x_2 > x_3$. Following the notation of (Robbiano 1986), the term ordering corresponds to the matrix T:

$$\begin{bmatrix} 2 & 3 & 6 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

We first check that $\mathrm{lt}_>(\Theta) = (x_1^9, x_2^6, x_3^3)$ is a permuted powering. Thus the main theorem of this paper applies.

Next we determine the term ordering $>' = >\circ\Theta$, by multiplying the matrix T by the exponent matrix of $\mathrm{lt}_>(\Theta)$

$$\begin{bmatrix} 9 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

obtaining a matrix for $>'$

$$\begin{bmatrix} 18 & 18 & 18 \\ 0 & 0 & -3 \\ 0 & -6 & 0 \end{bmatrix}$$

This corresponds to the graded reverse lexicographic ordering.

Thus, we compute a Groebner basis G of F under the graded reverse lexicographic ordering, obtaining

$$G = \{x_2x_3 + x_2^2 + x_3^2, x_1 + x_2 + x_3, -1 + x_3^3\}$$

From this, we obtain a Groebner basis of $F \circ \Theta$ under the weighted reverse lexicographic ordering, simply by composing G with Θ. □

Acknowledgment: This research was done in the framework of the European project ACCLAIM sponsored by Austrian Science Foundation. Thanks for Bruno Buchberger for several interesting remarks on the draft of this paper.

References

[Becker and Weispfenning 1993] Becker, T., Weispfenning, V. (1993). *Gröbner bases - a computational approach to commutative algebra.* Graduate Texts in Mathematics. Springer Verlag, New York, Berlin, Heidelberg.

[Buchberger 1965] 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. German.

[Buchberger 1985] Buchberger, B. (1985). Groebner bases: An algorithmic method in polynomial ideal theory. In Bose, N. K., editor, *Recent Trends in Multidimensional Systems Theory*, chapter 6. D. Riedel Publ. Comp.

[Char *et al.* 1985] Char, B. W., Geddes, K. O., Gonnet, G. H., Watt, S. M. (1985). *Maple User's Guide.* WATCOM Publications Limited, 4th edition.

[Cox *et al.* 1992] Cox, D., Little, J., ÓShea, D. (1992). *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer Verlag, New York, Berlin, Heidelberg.

[Faugere *et al.* 1993] Faugere, J.C., Gianni, P., Lazard, D., Mora, T. (1993). Efficient Computation of Zero-dimensional Groebner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16:329–344.

[Gianni and Mora 1987] Gianni, P., Mora, T. (1987). Algebraic Solution of Systems of Polynomial Equations Using Groebner Bases. In *Proceedings of AAECC-5*, pages 247–257. Springer. Lecture Notes in Computer Science 356.

[Hong 1995a] Hong, H. (1995). Groebner basis Under Composition. Technical Report 95-55, Research Institute for Symbolic Computation, Johannes Kepler University A-4040 Linz, Austria. Submitted for publication.

[Hong 1995b] 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 1995c] Hong, H. (1995). Subresultant Under Composition. Technical Report 95-47, Research Institute for Symbolic Computation, Johannes Kepler University A-4040 Linz, Austria. Submitted for publication.

[Mishra 1993] Mishra, B. (1993). *Algorithmic Algebra.* Springer-Verlag, New York.

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

[Weispfenning 1987] Weispfenning, V. (1987). Admissible Orderings and Linear Forms. *SIGSAM Bulletin*, 21(2):16–18.