Left and right Gröbner bases in Ore extensions of polynomial rings

Michael Pesch
Universität Passau
D-94030 Passau
pesch@alice.fmi.uni-passau.de

5th February 1996

MIP-9601

Abstract

We show, that Gröbner bases can be computed for left and right ideals of certain Ore extensions of polynomial rings.

Consider an Ore extension $K[X_1, \ldots, X_m][Y; \alpha, \delta]$ of a polynomial ring over a field, where

$$\alpha(X_i) = X_i^{e_i} + f_i$$

for some $f_i \in K[X_1, \ldots, X_m]$, $f_i \prec X_i^{e_i}$ for some admissible term order $\prec$, $e_i \in \mathbb{N} \setminus \{0\}$ and $\alpha|K = \mathrm{id}$. This rings are in general neither right nor left Noetherian. Nevertheless finite left and right Gröbner bases for finitely generated left and right ideals do exist for special term orders. Using this Gröbner bases the ideal membership problem can be solved.

For other term orders no finite Gröbner bases exist in general.

Finite left and right Gröbner bases can be computed using left/right reduction and s-polynomials (based on right/left divisibility and left/right least common multiples) in Buchbergers algorithm. Termination can be proven by a modified Dickson lemma, using the special term order.

Contents

1 Introduction **1**

2 Ore extensions of polynomial rings **2**

3 Ore extensions with one substitution operator **3**
3.1 Properties of terms 4
3.2 Admissible term orders 9
3.3 Left and right polynomial reduction 12
3.4 Left and right Gröbner bases 13

4 A modified Dickson lemma **17**

5 Finite Gröbner bases of left and right ideals **18**

6 Gröbner bases for iterated Ore extensions **26**

7 Concluding remarks and outlook **27**

1 Introduction

Non-commutative Gröbner bases for left, right and two sided ideals in several classes of rings have been studied during the last years. Examples of such are non-commutative algebras over fields (Mora, [6]) and solvable polynomial rings (Kandry-Rody and Weispfenning, [3], Kredel, [4]). For the latter class the left, right and two sided ideal membership problem can be solved algorithmically by Gröbner basis methods.

One problem concerning this rings is that Dickson's lemma does not hold, i.e. there is, in general, an infinite sequence of terms where no term is divided (on the left resp. on the right) by any term occuring earlier in the sequence. This implies termination of a Buchberger algorithm—if given at all—must be proven by different means.

A new feature occurs in the class of rings subject of the present paper, a special case of which has been considered in [11] by Weispfenning and by the author in [9]. Though left and right ideals are not finitely generated in general there is a finite Gröbner basis for any finitely generated left and right ideal provided a special term order is used. This Gröbner basis can be computed by a Buchberger algorithm.

For other admissible term orders only infinite Gröbner bases exist in general even for finitely generated ideals and will be enumerated by a Buchberger algorithm. If (for a special case) a finite Gröbner basis exists the algorithm will terminate and return such a basis.

In general for iterated Ore extensions (with more than one iteration) there are no finite left or right Gröbner bases wrt. any given admissible term order.

The plan of the paper is as follows. The second section gives the basic properties of Ore extensions. We consider polynomial rings with an added substitution operator in the third section. It is shown that no finite Gröbner bases exist in general for most term orders, but if one exists, it can be computed.

A modification of Dickson's lemma, which allows to prove termination of a Buchberger algorithm wrt. a special term order is proven in section four.

Using the results of the preceding sections we show in the fifth section that finite left and right Gröbner bases in more general Ore extensions can be computed by a Buchberger algorithm.

Subject of the sixth section is the general non-existence of finite left and right Gröbner bases in iterated Ore extensions for any given admissible term order.

2 Ore extensions of polynomial rings

Ore extensions of a ring R are noncommutative polynomial rings where each polynomial has a representation as "commutative" polynomial. We will give the basic definitions and properties in the following. Noether and Schmeidler [7] were the first to consider this extensions which then were systematically studied by Ore [8]. More on this subject can be found in [2] and [5].

2.1 Theorem *Let R be a ring. Let $\alpha\colon R \to R$ be a homomorphism and $\delta\colon R \to R$ be an α-derivation, i.e. for all $r, r' \in R$ we have*

$$\delta(r+r') = \delta(r) + \delta(r')$$

and

$$\delta(rr') = \alpha(r)\delta(r') + \delta(r)r'.$$

Then there exists a ring $R' \supseteq R$ and $Y \in R'$ such that

- *R' is a free left R-module with basis $\{1, Y, Y^2, \dots\}$.*
- *for all $r \in R$ we have $Yr = \alpha(r)Y + \delta(r)$.*

Proof See [2] □

The ring R' is called the *Ore extension* of R by α and δ or *skew polynomial ring* and denoted by $R[Y;\, \alpha, \delta]$. The multiplication in R' will be denoted by $*$. We will identify $R[Y;\, \alpha, \delta]$ and the commutative polynomial ring $R[Y]$ as free left R-modules and denote the product in $R[Y]$ by $\cdot$.

We will call a ring of the form

$$R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$$

an *iterated Ore extension* of R.

3 Ore extensions with one substitution operator

Before investigating the more general Ore extensions subject of this paper, we will consider Ore extensions with a substitution operator. This is are Ore extensions

$$K[X_1,\dots,X_m][Y;\,\alpha,\delta]$$

of a polynomial ring $K[X_1,\dots,X_m]$ over a field K where

$$\alpha(X_i) = X_i^{e_i}$$

for $e_i \in \mathbb{N} \setminus \{0\}$,

$$\alpha|K = \mathrm{id}$$

and

$$\delta = 0.$$

In this case the endomorphism α is injective.

This rings are generally neither right nor left Noetherian, as shown by the following example.

3.1 Example Let $\alpha(X_1) := X_1^{e_1}$ for some $e_1 \in \mathbb{N} \setminus \{0,1\}$.

1. The left ideal
$$\mathrm{I}_\ell\left(\left\{ X_1Y^d \;\middle|\; d \in \mathbb{N} \right\}\right)$$
is not finitely generated.

2. The right ideal
$$\mathrm{I}_r\left(\left\{ X_1^{e_1^d}Y^{d+1} \;\middle|\; d \in \mathbb{N} \right\}\right)$$
is not finitely generated.

See [2] and [11] for similar examples.

We will frequently use "tuple-notation" e.g. use X^c instead of $X_1^{c_1}\cdots X_m^{c_m}$ where $c \in \mathbb{N}^m$. All operations on $\mathbb{N}^m$ are then meant to be componentwise.

 ©1996 M. Pesch

3.1 Properties of terms

We will now investigate divisibility of terms and the existence of least common multiples. The set of terms will be denoted by

$$T := \mathrm{T}(K[X_1,\ldots,X_m][Y;\,\alpha,\delta])$$

and the set of monomials by

$$M := \mathrm{M}(K[X_1,\ldots,X_m][Y;\,\alpha,\delta]).$$

The product of two terms is

$$X^cY^d * X^{c'}Y^{d'} = X^{c+c'e^d}Y^{d+d'}$$

Terms have the following cancellation property.

3.2 Lemma • $X^{c'}Y^{d'} * X^cY^d = X^{c''}Y^{d''} * X^cY^d \Longrightarrow X^{c'}Y^{d'} = X^{c''}Y^{d''}$

• $X^cY^d * X^{c'}Y^{d'} = X^cY^d * X^{c''}Y^{d''} \Longrightarrow X^{c'}Y^{d'} = X^{c''}Y^{d''}$

Proof • We have

$$X^{c'}Y^{d'} * X^cY^d = X^{c'+ce^{d'}}Y^{d'+d} = X^{c''+ce^{d''}}Y^{d''+d} = X^{c''}Y^{d''} * X^cY^d$$

and therefore $d' = d''$ and $c' = c''$.

• We have

$$X^cY^d * X^{c'}Y^{d'} = X^{c+c'e^d}Y^{d+d'} = X^{c+c''e^d}Y^{d+d''} = X^cY^d * X^{c''}Y^{d''}$$

and therefore $d' = d''$ and $c' = c''$.

□

Since the ring is non-commutative there are left and right divisors.

3.3 Definition *Let* $X^{c'}Y^{d'} * X^{c''}Y^{d''} = X^cY^d$.

- $X^{c'}Y^{d'}$ *is a* left divisor *of* X^cY^d, $X^{c'}Y^{d'} \mid_\ell X^cY^d$ *and* X^cY^d *is a* right multiple *of* $X^{c'}Y^{d'}$.
- $X^{c''}Y^{d''}$ *is a* right divisor *of* X^cY^d, $X^{c''}Y^{d''} \mid_r X^cY^d$ *and* X^cY^d *is a* left multiple *of* $X^{c''}Y^{d''}$.

Divisibility of terms can be characterized by their exponents.

3.4 Lemma *For terms* $X^cY^d, X^{c'}Y^{d'} \in T$ *we have*

- $X^{c'}Y^{d'} \mid_\ell X^cY^d \iff d' \leqslant d, c' \leqslant c, e^{d'} \mid c - c'$. *In this case*

$$X^cY^d = X^{c'}Y^{d'} * X^{\frac{c-c'}{e^{d'}}}Y^{d-d'}.$$

- $X^{c'}Y^{d'} \mid_r X^cY^d \iff d' \leqslant d, c'e^{d-d'} \leqslant c$. *In this case*

$$X^cY^d = X^{c-c'e^{d-d'}}Y^{d-d'} * X^{c'}Y^{d'}.$$

Proof

$$\begin{aligned}
X^{c'}Y^{d'} \mid_\ell X^cY^d &\iff \exists c'', d'' : X^{c'}Y^{d'} * X^{c''}Y^{d''} = X^cY^d \\
&\iff \exists c'', d'' : X^{c'+c''e^{d'}}Y^{d'+d''} = X^cY^d \\
&\iff d' \leqslant d \wedge \exists c'' : \frac{c-c'}{e^d} = c'' \\
&\iff d' \leqslant d \wedge c > c' \wedge e^d \mid c - c'
\end{aligned}$$

$$\begin{aligned}
X^{c'}Y^{d'} \mid_r X^cY^d &\iff \exists c'', d'' : X^{c''}Y^{d''} * X^{c'}Y^{d'} = X^cY^d \\
&\iff \exists c'', d'' : X^{c''+c'e^{d''}}Y^{d''+d'} = X^cY^d \\
&\iff d' \leqslant d \wedge c'e^{d-d'} \leqslant c
\end{aligned}$$

□

This leads to the definition of right and left division.

3.5 Definition • *Let* $X^{c'}Y^{d'} \mid_\ell X^cY^d$.

$$X^cY^d /_\ell X^{c'}Y^{d'} := \frac{X^cY^d}{X^{c'}Y^{d'}}\ell := X^{\frac{c-c'}{e^{d'}}}Y^{d-d'}.$$

• *Let* $X^{c'}Y^{d'} \mid_r X^cY^d$.

$$X^cY^d /_r X^{c'}Y^{d'} := \frac{X^cY^d}{X^{c'}Y^{d'}}r := X^{c-c'e^{d-d'}}Y^{d-d'}.$$

3.6 Lemma *The relations* $\mid_\ell$ *and* $\mid_r$ *are orders on* T.

Proof • From lemma 3.4 it is obvious that $\mid_\ell$ is reflexive and antisymmetric. We show transitivity. Let $X^{c''}Y^{d''} \mid_\ell X^{c'}Y^{d'} \mid_\ell X^cY^d$. From lemma 3.4 we get

$$d'' \leqslant d' \leqslant d, c'' \leqslant c' \leqslant c, e^{d''} \mid c'-c'', e^{d'} \mid c-c'.$$

Since $d'' \leqslant d'$ we have

$$e^{d''} \mid e^{d'} \mid c-c'$$

and therefore

$$e^{d'} \mid c'-c''+c-c' = c-c'.$$

• From lemma 3.4 it is obvious that $\mid_\ell$ is reflexive and antisymmetric. We show transitivity. Let $X^{c''}Y^{d''} \mid_r X^{c'}Y^{d'} \mid_r X^cY^d$. From lemma 3.4 we get $d'' \leqslant d' \leqslant d$ and

$$c''e^{d'-d''} \leqslant c' \leqslant c'e^{d-d'} \leqslant c.$$

□

Left and right divisibility are compatible with multiplication from the right or left, respectively.

3.7 Lemma *For* $X^cY^d, X^{c'}Y^{d'}, X^{c''}Y^{d''} \in T$ *we have*

• $X^cY^d \mid_\ell X^{c'}Y^{d'} \Longrightarrow X^cY^d \mid_\ell X^{c'}Y^{d'} * X^{c''}Y^{d''}$

- $X^cY^d \mid_r X^{c'}Y^{d'} \Longrightarrow X^cY^d \mid_r X^{c''}Y^{d''} * X^{c'}Y^{d'}$

Proof
- From lemma 3.4 we know that $c \leqslant c'$, $d \leqslant d'$ and $e^d \mid c'-c$. This implies $d \leqslant d'+d''$ and $c \leqslant c'+c''e^{d'}$. Since $d \leqslant d' \Longrightarrow e^d \mid e^{d'}$ we also get $e^d \mid c'+c''e^{d'}-c$. By lemma 3.4 this means $X^cY^d \mid_\ell X^{c'+c''e^{d'}}Y^{d'+d''}$.
- From lemma 3.4 we know that $d \leqslant d'$ and $ce^{d'-d} \leqslant c'$. This implies $d \leqslant d''+d'$ and $ce^{d''+d'-d} \leqslant c''+c'e^{d''}$ which by lemma 3.4 means $X^cY^d \mid_r X^{c''+c'e^{d''}}Y^{d''+d'}$.

□

The next theorem claims the existence of least common left multiples. Let $\vee$ denote the componentwise maximum on $\mathbb{N}^k$ and $a \dot{-} b := (a-b) \vee 0$.

3.8 Theorem *Let $X^cY^d, X^{c'}Y^{d'} \in T$.*

$$\begin{aligned}\operatorname{llcm}\left(X^cY^d, X^{c'}Y^{d'}\right) &:= X^{(ce^{d'\dot{-}d})\vee(c'e^{d\dot{-}d'})}Y^{d\vee d'} \\ &= X^{c'e^{d\dot{-}d'}\dot{-}ce^{d'\dot{-}d}}Y^{d'\dot{-}d} * X^cY^d \\ &= X^{ce^{d'\dot{-}d}\dot{-}c'e^{d\dot{-}d'}}Y^{d\dot{-}d'} * X^{c'}Y^{d'}\end{aligned}$$

is the least common left multiple of X^cY^d and $X^{c'}Y^{d'}$.

Proof We first show that $\operatorname{llcm}\left(X^cY^d, X^{c'}Y^{d'}\right)$ is a common left multiple of X^cY^d and $X^{c'}Y^{d'}$.

$$\begin{aligned}X^{c'e^{d\dot{-}d'}\dot{-}ce^{d'\dot{-}d}}Y^{d'\dot{-}d} * X^cY^d &= X^{(c'e^{d\dot{-}d'}\dot{-}ce^{d'\dot{-}d})+ce^{d'\dot{-}d}}Y^{(d'\dot{-}d)+d} \\ &= X^{(ce^{d'\dot{-}d})\vee(c'e^{d\dot{-}d'})}Y^{d\vee d'}\end{aligned}$$

The same holds for $X^{c'}Y^{d'}$.

Next we show $\operatorname{llcm}\left(X^cY^d, X^{c'}Y^{d'}\right)$ is the *least* common left multiple of X^cY^d and $X^{c'}Y^{d'}$. Assume that $X^aY^b * X^cY^d = X^{a'}Y^{b'} * X^{c'}Y^{d'}$. This means

$$X^{a+ce^b}Y^{b+d} = X^{a'+c'e^{b'}}Y^{b'+d'}.$$

We show that

$$\operatorname{llcm}\left(X^cY^d, X^{c'}Y^{d'}\right) \mid_r X^aY^b * X^cY^d$$

using lemma 3.4. Obviously $b+d = b'+d' \geqslant d \vee d'$, $b \geqslant (d \vee d') - d = d' \dot{-} d$ and $b' \geqslant (d' \vee d - d') = d \dot{-} d'$. Therefore

$$a + ce^b = a' + c'e^{b'} \geqslant ce^b \vee c'e^{b'} \geqslant ce^{d' \dot{-} d} \vee c'e^{d \dot{-} d'}.$$

□

Least common right multiples are a bit more difficult. They do not always exist. Fortunately they do exist if some common multiple exists.

3.9 Theorem *Let $X^cY^d, X^{c'}Y^{d'} \in T$ and $d' \leqslant d$. Then the following holds:*

- *There is a common right multiple of X^cY^d and $X^{c'}Y^{d'}$ iff $e^{d'} \mid c - c'$.*
- *If $e^{d'} \mid c - c'$ then*

$$\begin{aligned}\operatorname{rlcm}\left(X^cY^d, X^{c'}Y^{d'}\right) &:= X^{e^d\left\lceil \frac{c' \dot{-} c}{e^d}\right\rceil + c}Y^d \\ &= X^cY^d * X^{\left\lceil \frac{c' \dot{-} c}{e^d}\right\rceil} \\ &= X^{c'}Y^{d'} * X^{\left\lceil \frac{c' \dot{-} c}{e^d}\right\rceil e^{d-d'} + \frac{c-c'}{e^{d'}}}Y^{d-d'}\end{aligned}$$

is the least common right multiple of X^cY^d and $X^{c'}Y^{d'}$.

Proof • **"$\Longrightarrow$":**

$$\begin{aligned} & X^cY^d * X^aY^b = X^{c'}Y^{d'} * X^{a'}Y^{b'} \\ \Longrightarrow\quad & X^{c+ae^d}Y^{d+b} = X^{c'+a'e^{d'}}Y^{d'+b'} \\ \Longrightarrow\quad & \frac{c-c'}{e^{d'}} = a' - ae^{d-d'} \in \mathbb{Z} \\ \Longrightarrow\quad & e^{d'} \mid c - c' \end{aligned}$$

"$\Longleftarrow$": Is a consequence of the second claim.

- First we show that rlcm $\left(X^cY^d, X^{c'}Y^{d'}\right)$ is a common right multiple of X^cY^d and $X^{c'}Y^{d'}$. Obviously

$$X^cY^d * X^{\left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil} = X^{e^d \left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil + c} Y^d$$

and

$$\begin{aligned} X^{c'}Y^{d'} * X^{\left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil e^{d-d'} + \frac{c-c'}{e^{d'}}} Y^{d-d'} & \\ = \quad X^{c' + \left(\left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil e^{d-d'} + \frac{c-c'}{e^{d'}} \right) e^{d'}} Y^{d-d'+d'} & \\ = \quad X^{c' + \left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil e^d + c - c'} Y^d & \\ = \quad X^{e^d \left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil + c} Y^d & \end{aligned}$$

Next we show that rlcm $\left(X^cY^d, X^{c'}Y^{d'}\right)$ is the *least* common right multiple of X^cY^d and $X^{c'}Y^{d'}$. Assume that $X^cY^d * X^aY^b = X^{c'}Y^{d'} * X^{a'}Y^{b'}$, i.e.

$$X^{c+ae^d}Y^{d+b} = X^{c'+a'e^{d'}}Y^{d'+b'}.$$

Obviously then $d \leqslant d+b$ and

$$e^d \left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil + c \leqslant c + ae^d.$$

Moreover

$$e^d \mid c + ae^d - \left(e^d \left\lceil \frac{c' \dot{-} c}{e^d} \right\rceil + c \right).$$

So by lemma 3.4 rlcm $\left(X^cY^d, X^{c'}Y^{d'}\right) \mid_\ell X^cY^d * X^aY^b$.

□

3.2 Admissible term orders

Admissible term orders are term orders compatible with multiplication.

3.10 Definition *1. We call an order $\prec$ on T a* left admissible term order *on T iff for all $X^cY^d, X^{c'}Y^{d'}, X^{c''}Y^{d''} \in T$*

- $1 \preccurlyeq X^cY^d$,
- $X^cY^d \preccurlyeq X^{c'}Y^{d'} \Longrightarrow X^{c''}Y^{d''} * X^cY^d \preccurlyeq X^{c''}Y^{d''} * X^{c'}Y^{d'}$.

2. We call an order $\prec$ on T a right admissible term order *on T iff for all X^cY^d, $X^{c'}Y^{d'}, X^{c''}Y^{d''} \in T$*

- $1 \preccurlyeq X^cY^d$,
- $X^cY^d \preccurlyeq X^{c'}Y^{d'} \Longrightarrow X^cY^d * X^{c''}Y^{d''} \preccurlyeq X^{c'}Y^{d'} * X^{c''}Y^{d''}$.

3. An admissible term order *is a left and right admissible term order.*

For a characterization of admissible term orders we need the following facts about orders.

3.11 Lemma *1. Let $A\colon \mathbb{R}^{m+1} \to \mathbb{R}^k$, $k \geqslant m+1$ be an injective $\mathbb{R}$-linear mapping where for all $x, y > 0$ we have $A((x,y)) > 0$ and there is some i such that for $j \neq i$*

$$(A((x,0)))_i = 0, \qquad (A((0,y)))_j = 0$$

Let

$$\gamma\colon \mathbb{R}^{m+1} \to \mathbb{R},\ x \mapsto x_{\min\{\, i \,|\, x_i \neq 0\}}.$$

The relation

$$X^cY^d \prec X^{c'}Y^{d'} \quad :\Longleftrightarrow \quad \gamma\big(A((c'-c, d'-d))\big) > 0$$

on T is a left admissible term order.

2. The inverse lexicographical term order on T is a left and right admissible term order.

3. The lexicographical term order on T is a left admissible term order.

4. Generally, there is no right admissible term order where $X_i \succ Y$ for some i.

Proof 1. It is well known that $\preccurlyeq$ is a term order. We show that it is left admissible. Let $X^cY^d \prec X^{c'}Y^{d'}$. Recall that

$$X^{c''}Y^{d''} * X^cY^d = X^{c''+ce^{d''}}Y^{d''+d}$$

and

$$X^{c''}Y^{d''} * X^{c'}Y^{d'} = X^{c''+c'e^{d''}}Y^{d''+d'}.$$

Since

$$(c''+c'e^{d''}, d''+d) - (c''+ce^{d''}, d''+d) = (e^{d''}(c'-c), d'-d)$$

we conclude

$$X^{c''}Y^{d''} * X^cY^d \prec X^{c''}Y^{d''} * X^{c'}Y^{d'}.$$

2. Let $\preccurlyeq$ be the inverse lexicographical order on T. Obviously it is left admissible. We show it is right admissible. Let $X^cY^d, X^{c'}Y^{d'}, X^{c''}Y^{d''} \in T$. Obviously $1 \preccurlyeq X^cY^d$. Let $X^cY^d \prec X^{c'}Y^{d'}$. If $d < d'$ then $d''+d < d''+d'$ and therefore $X^{c+c''e^d}Y^{d+d''} \preccurlyeq X^{c'+c''e^{d'}}Y^{d'+d''}$.

   Otherwise $d = d'$ and there exists a maximal $1 \leqslant i \leqslant m$ with $c_i < c'_i$ and $(c_{i+1}, \ldots, c_m) = (c'_{i+1}, \ldots, c'_m)$. We then have

$$c_i + c''_i e_i^d < c'_i + c''_i e_i^d = c'_i + c''_i e_i^{d'}.$$

3. Obvious.

4. If $\preccurlyeq$ were such an admissible term order, and $e_i \geqslant 2$ then since $Y \prec X_i$ we would have $Y * X_i = X_i^{e_i}Y \prec X_i^2$. But this contradicts the fact $X_i^2 \preccurlyeq X_i^{e_i} \prec X_i^{e_i}Y$.

□

Wrt. a term order we denote the head term of a polynomial f (or a finite set of polynomials F) by $\mathrm{HT}(f)$ ($\mathrm{HT}(F)$) its head coefficient by $\mathrm{HC}(f)$ and its head monomial by $\mathrm{HM}(f)$.

3.3 Left and right polynomial reduction

As in the case of commutative Gröbner bases we can now define a reduction relation and state some of its properties. We will omit the proofs since they do not differ significantly from the corresponding proofs in the well known commutative case (see e.g. [1]).

3.12 Definition *Let* $f, p \in K[X_1, \ldots, X_m][Y; \alpha, \delta]$ *and* $as \in \mathrm{M}(f)$*, where* $a \in K$ *and* $s \in \mathrm{T}(f)$*.*

- *Let* $\mathrm{HT}(p) \mid_r s$*. Define* reduction with a left multiple *of* p *(wrt.* as*) by*

$$f \xrightarrow{\ell}_p f' :\Longleftrightarrow f' = f - \frac{as}{\mathrm{HM}(p)} r * p.$$

- *Let* $\mathrm{HT}(p) \mid_\ell s$*. Define* reduction with a right multiple *of* p *(wrt.* as*) by*

$$f \xrightarrow{r}_p f' :\Longleftrightarrow f' = f - p * \frac{as}{\mathrm{HM}(p)} \ell.$$

Reduction with a set of polynomials is defined as usual.

3.13 Lemma *Let* $P \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$*.*

- $f \xrightarrow{\ell}{}^*_P f' \Longrightarrow f \succ f'$
- $f \xrightarrow{r}{}^*_P f' \Longrightarrow f \succ f'$
- $\xrightarrow{\ell}{}^*_P$ *and* $\xrightarrow{r}{}^*_P$ *are Noetherian.*

3.14 Lemma *Let* $P \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$*.*

- $f \xrightarrow{\ell}{}^*_P 0 \Longrightarrow f \in I_\ell(P)$
- $f \xrightarrow{r}{}^*_P 0 \Longrightarrow f \in I_r(P)$

3.15 Lemma (Translation lemma) *Let* $f, g, h \in K[X_1, \ldots, X_m][Y; \alpha, \delta]$ *and let* $P \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$*.*

- *If* $f - g \overset{*}{\underset{\ell}{\longrightarrow}}_P h'$ *then there exist* $f', g' \in K[X_1, \ldots, X_m][Y; \alpha, \delta]$ *such that* $f' - g' = h'$, $f \overset{*}{\underset{\ell}{\longrightarrow}}_P f'$ *and* $g \overset{*}{\underset{\ell}{\longrightarrow}}_P g'$.

- *If* $f - g \overset{*}{\underset{r}{\longrightarrow}}_P h'$ *then there exist* $f', g' \in K[X_1, \ldots, X_m][Y; \alpha, \delta]$ *such that* $f' - g' = h'$, $f \overset{*}{\underset{r}{\longrightarrow}}_P f'$ *and* $g \overset{*}{\underset{r}{\longrightarrow}}_P g'$.

3.16 Lemma *Let* $f, f' \in K[X_1, \ldots, X_m][Y; \alpha, \delta]$, $F \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$ *and* m *be a monomial in* $K[X_1, \ldots, X_m][Y; \alpha, \delta]$.

- $f \underset{\ell}{\longrightarrow}_F f' \Longrightarrow m * f \underset{\ell}{\longrightarrow}_F m * f'$

- $f \underset{r}{\longrightarrow}_F f' \Longrightarrow f * m \underset{r}{\longrightarrow}_F f' * m$

3.17 Lemma *Let* $f, f' \in K[X_1, \ldots, X_m][Y; \alpha, \delta]$, $F \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$.

- $f - f' \in I_\ell(F) \iff f \overset{*}{\underset{\ell}{\longleftrightarrow}}_F f'$

- $f - f' \in I_r(F) \iff f \overset{*}{\underset{r}{\longleftrightarrow}}_F f'$

3.4 Left and right Gröbner bases

Finite left Gröbner bases do not exist for every admissible term order. If finite left/right Gröbner bases exist, they can be computed.

For this section let $\prec$ be a left respectively right admissible term order.

3.18 Definition *1. A* left Gröbner basis *of a left ideal* I *is a subset* $G \subseteq I$ *such that* $I_\ell(G) = I$ *and* $\mathrm{HT}(I) = T * \mathrm{HT}(G)$.

2. A right Gröbner basis *of a right ideal* I *is a subset* $G \subseteq I$ *such that* $I_r(G) = I$ *and* $\mathrm{HT}(I) = \mathrm{HT}(G) * T$.

Note that we do not require a Gröbner basis to be finite.

Finite left Gröbner bases do not exist for every left admissible term order.

3.19 Example Let $\alpha(X_i) := X_i^{e_i}$ for some $e_i \in \mathbb{N} \setminus \{0,1\}$ and and $m \geqslant 2$. Assume a left admissible term order where $X_2 \succ Y$. We have

$$\mathrm{HT}(\mathrm{I}_\ell(\{X_2+Y, X_1Y\})) = T * \left\{ X_2, X_1Y^d \;\middle|\; d \in \mathbb{N} \setminus \{0\} \right\}.$$

By example 3.1 we already know there is no finite basis for the head term ideal and therefore no finite Gröbner basis.

3.20 Theorem (First characterization theorem) *Let $G \subseteq K[X_1, \ldots, X_m][Y;\ \alpha, \delta]$.*

- *The following are equivalent.*
  - *G is a left Gröbner basis.*
  - *$\ell \xrightarrow{*}_G$ is confluent.*
  - *For all $f \in \mathrm{I}_\ell(G) : f \,\ell\xrightarrow{*}_G 0$.*
  - *All $f \in \mathrm{I}_\ell(G) \setminus \{0\}$ are left reducible wrt. G.*
- *The following are equivalent.*
  - *G is a right Gröbner basis.*
  - *$r \xrightarrow{*}_G$ is confluent.*
  - *For all $f \in \mathrm{I}_r(G) : f \,r\xrightarrow{*}_G 0$.*
  - *All $f \in \mathrm{I}_r(G) \setminus \{0\}$ are f right reducible wrt. G.*

To give an algorithmic characterization of Gröbner bases we need the notion of s-polynomials.

3.21 Definition *Let $f_1, f_2 \in K[X_1, \ldots, X_m][Y;\ \alpha, \delta]$.* Left and right s-polynomials *of f_1, f_2 are defined as follows.*

$$\begin{aligned} &\mathrm{lSPol}(f_1, f_2) \\ &:= \quad \mathrm{HC}(f_2)\, \frac{\mathrm{llcm}\,(\mathrm{HT}(f_1), \mathrm{HT}(f_2))}{\mathrm{HT}(f_1)}\, r * f_1 - \mathrm{HC}(f_1)\, \frac{\mathrm{llcm}\,(\mathrm{HT}(f_1), \mathrm{HT}(f_2))}{\mathrm{HT}(f_2)}\, r * f_2 \end{aligned}$$

 © 1996 M. Pesch

$$\begin{aligned}&\mathrm{rSPol}(f_1,f_2)\\ &:= \quad \mathrm{HC}(f_2)f_1 * \frac{\mathrm{rlcm}\,(\mathrm{HT}(f_1),\mathrm{HT}(f_2))}{\mathrm{HT}(f_1)}\ell - \mathrm{HC}(f_1)f_2 * \frac{\mathrm{rlcm}\,(\mathrm{HT}(f_1),\mathrm{HT}(f_2))}{\mathrm{HT}(f_2)}\ell\end{aligned}$$

Note that since right common multiples do not always exist right s-polynomials do not always exist either. But since they are needed only in case some right common multiple exists this causes no further problems.

Left and right Gröbner bases can be characterized in terms of left and right s-polynomials.

3.22 Theorem (Second characterization theorem) *Let* $G \subseteq K[X_1,\ldots,X_m][Y;\,\alpha,\delta]$.

- *G is a left Gröbner basis iff for all* $f,f' \in G$, $f \neq f'$ *implies* $\mathrm{lSPol}(f,f')\,\ell\xrightarrow{*}_G 0$
- *G is a right Gröbner basis iff for all* $f,f' \in G$, $f \neq f'$ *implies if* $\mathrm{rSPol}(f,f')$ *exists then* $\mathrm{rSPol}(f,f')\,r\xrightarrow{*}_G 0$

Note that the right s-polynomial exists in the critical case.

3.23 Corollary *Let* $F \subseteq K[X_1,\ldots,X_m][Y;\,\alpha,\delta]$.

- *Define recursively*

$$\begin{aligned}F_0 &:= F\\ F_{i+1} &:= F_i \cup \{\,\mathrm{lSPol}(f_1,f_2) \mid f_1,f_2 \in F_i\,\}.\end{aligned}$$

  Then $\bigcup_i F_i$ *is a left Gröbner basis.*

- *Define recursively*

$$\begin{aligned}F_0 &:= F\\ F_{i+1} &:= F_i \cup \{\,\mathrm{rSPol}(f_1,f_2) \mid f_1,f_2 \in F_i\,\}.\end{aligned}$$

  Then $\bigcup_i F_i$ *is a right Gröbner basis.*

3.24 Definition *For a polynomial f and a set of polynomials F let $NF(f,F)$ be a normal form of f wrt. a Noetherian reduction relation $\longrightarrow_F$.*

The Buchberger algorithm *(for a reduction $\longrightarrow$ and s-polynomials* SPol*) is*

funct $GB(F) \equiv$
$\lceil G := F;$
$S := F^2 \setminus \triangle F;$
while $S \neq \varnothing$ **do**
some $(g_1, g_2) \in S$; $S := S \setminus \{(g_1, g_2)\}$;
$h := NF(\mathrm{SPol}(g_1, g_2), G)$;
if $h \neq 0$ **then**
$S := S \cup (G \times \{h\})$;
$G := G \cup \{h\}$;
fi;
od;
$G \rfloor$
tcnuf

3.25 Corollary *Let $F \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$ be finite.*

1. *The Buchberger algorithm (with left (right) reduction and left (right) s-polynomials) enumerates a Gröbner basis for $I_\ell(F)$ (or $I_r(F)$).*

2. *If there is a finite Gröbner basis for $I_\ell(F)$ (or $I_r(F)$) wrt. some admissible term order the Buchberger algorithm will terminate, and return such a Gröbner basis.*

Proof 1. Obvious.

2. If there is a finite Gröbner basis, $\mathrm{HT}(\mathrm{I}_\ell(F))$ (resp. $\mathrm{HT}(\mathrm{I}_r(F))$) is finitely generated. The possibly infinite Gröbner basis enumerated by Buchbergers algorithm then contains for each generating term a polynomial whose head term divides the generating term. These finitely many polynomials already are a

Gröbner basis. Therefore the algorithm terminates after producing this polynomials.

□

4 A modified Dickson lemma

Unfortunately Dickson's lemma does not hold in this rings, i.e. there is, in general, an infinite sequence of terms where no term is divided (on the left resp. on the right) by any term occuring earlier in the sequence. Examples are the sequences from 3.1.

We have already seen that we can not expect the Buchberger algorithm to terminate for any given input.

But using the following lemma we will be able to prove termination of such an algorithm (for some term order) anyway.

4.1 Lemma *Let $(c_i)_{i\in\mathbb{N}}$, $c_i, e \in \mathbb{N}^m$, $m \in \mathbb{N}$. Then there exist $j, j' \in \mathbb{N}, j \leqslant j'$ such that $c_j \leqslant c_{j'}$ and $e \mid c_{j'} - c_j$.*

Proof If there are $j < j'$ such that $c_j = c_{j'}$ we are done. Otherwise there is a strictly monotone subsequence $(c_{i_\ell})_{\ell\in\mathbb{N}}$ of $(c_i)_{i\in\mathbb{N}}$. To prove this note that a Dickson basis of an infinite set contains at least one element with an infinite number of successors. Define recursively

$$\begin{aligned} c_{i_\ell} &:= \text{some element of } D_\ell \text{ with infinitely many successors} \\ D_0 &:= \text{Dickson basis of } \{\, c_i \mid i \in \mathbb{N} \,\} \\ D_\ell + 1 &:= \text{Dickson basis of } \left\{\, c_i \mid i_\ell < i, c_{i_\ell} < k_i \,\right\}. \end{aligned}$$

Then we have $c_{i_\ell} < D_{l+1}$ and therefore $c_{i_\ell} < c_{i_\ell+1}$. This proves the existence of a strictly monotone subsequence. Since there are only finitely (namely $\prod_{i=1}^{m} e_i$) remainders modulo e there exist $j < j'$ such that $c_j \equiv c_{j'} \bmod e$, i.e. $e \mid c_{j'} - c_j$. □

4.2 Theorem (Modified Dickson lemma) *Let $(c_i, d_i)_{i\in\mathbb{N}}$, $c_i \in \mathbb{N}^m$ and $d_i \in \mathbb{N}$, with bounded $(d_i)_{i\in\mathbb{N}}$. Then the following hold:*

- *There exist* j, j', $j \leqslant j'$ *such that* $X^{c_j}Y^{d_j} \mid_\ell X^{c_{j'}}Y^{d_{j'}}$
- *There exist* j, j', $j \leqslant j'$ *such that* $X^{c_j}Y^{d_j} \mid_r X^{c_{j'}}{}^{d_{j'}}$

Proof Since $(d_i)_{i\in\mathbb{N}}$ is bounded there exists some d and an infinite subsequence $(h_i,d)_{i\in\mathbb{N}}$ of $(c_i,d_i)_{i\in\mathbb{N}}$. The claim for $\mid_r$ follows from Dickson's lemma for $(h_i)_{i\in\mathbb{N}}$. Applying lemma 4.1 on $(h_i)_{i\in\mathbb{N}}$ yields the claim for $\mid_\ell$. □

5 Finite Gröbner bases of left and right ideals

As shown above we can not expect to get finite Gröbner bases wrt. arbitrary admissible term orders. We therefore use the inverse lexicographical term order $\prec$ (which we recall to be right and left admissible) for this section.

We will now consider extensions $K[X_1,\ldots,X_m][Y;\alpha,\delta]$ of a polynomial ring $K[X_1,\ldots,X_m]$ over a field K where

$$\alpha(X_i) = X_i^{e_i} + f_i$$

for some $f_i \in K[X_1,\ldots,X_m]$, $f_i \prec X_i^{e_i}$, $e_i \in \mathbb{N} \setminus \{0\}$ and

$$\alpha|K = \mathrm{id}.$$

Further we define an endomorphism α' of $K[X_1,\ldots,X_m]$ as

$$\alpha'(X_i) := \mathrm{HT}(\alpha(X_i))$$

and let $\delta' := 0$.

The endomorphism α is injective and moreover it is injective wrt. the head terms.

5.1 Lemma *1.* α *is injective.*

2. α' *is injective.*

3. $\mathrm{HT}\circ\alpha\mid_{\mathrm{T}(X_1,\ldots,X_m)}$ *is injective.*

The product of two terms is (generally) not a term.

We have the following variation of the cancellation property for terms.

5.2 Lemma *Let $t,t',t'' \in T$. Then the following hold:*

1. $\mathrm{HT}(t * t') = \mathrm{HT}(t * t'') \Longrightarrow t' = t''$,
2. $\mathrm{HT}(t' * t) = \mathrm{HT}(t'' * t) \Longrightarrow t' = t''$.

Proof Setting $t = X^c Y^d$, $t' = X^{c'} Y^{d'}$ and $t'' = X^{c''} Y^{d''}$ we have

- $X^c \,\mathrm{HT}(\alpha^d(X^{c'}))Y^{d+d'} = X^c \,\mathrm{HT}(\alpha^d(X^{c''}))Y^{d+d''}$. This implies $d' = d''$. By injectivity of $\mathrm{HT} \circ \alpha^d$ we then have $c' = c''$.
- $X^{c'} \,\mathrm{HT}(\alpha^{d'}(X^c))Y^{d'+d} = X^{c''} \,\mathrm{HT}(\alpha^{d''}(X^c))Y^{d''+d}$. This implies $d' = d''$. We then have $c' = c''$.

□

We therefore define a "divisibility" relation on the set of terms T as follows.

5.3 Definition *Let $t,t',t'' \in T$ and $\mathrm{HT}(t' * t'') = t$. We define*

$$t' \mid_\ell t, \qquad t'' \mid_r t, \qquad \frac{t}{t'}\ell := t'', \qquad \frac{t}{t''}r := t'.$$

Note that the quotients are well defined by lemma 5.2.

5.4 Lemma *For $X^c Y^d, X^{c'} Y^{d'} \in T$ we have*

$$X^c Y^d * X^{c'} Y^{d'} = X^c \sum_{\ell=0}^{d} \left(\sum_{\sigma \in A_{\ell,d}} \sigma(X^{c'}) \right) Y^{\ell + d'}$$

where

$$A_{\ell,d} := \begin{cases} \left\{ \alpha^{a_1} \circ \delta^{d_1} \circ \cdots \circ \alpha^{a_j} \circ \delta^{d_j} \;\middle|\; \sum_{j=1}^{d} a_j = \ell,\ \sum_{j=1}^{d} d_j = d - \ell \right\}, & 0 \leqslant \ell \leqslant d \\ \varnothing, & \text{else.} \end{cases}$$

Further we have

$$\mathrm{HT}(X^c Y^d * X^{c'} Y^{d'}) = X^c \,\mathrm{HT}(\alpha^d(X^{c'}))Y^{d+d'}.$$

 ©1996 M. Pesch

Divisibility in $K[X_1,\ldots,X_m][Y;\ \alpha,\delta]$ ist essentially the same, as divisibility in the Ore extension $K[X_1,\ldots,X_m][Y;\ \alpha',\delta']$ with a substitution operator, denoted by $|'_\ell$ resp. $|'_r$ which was considered earlier. More precisely we have the following.

5.5 Lemma *For all $t,t' \in T$ we have*

$$t' \mid_\ell t \iff t' \mid'_\ell t$$

and

$$t' \mid_r t \iff t' \mid'_r t$$

The lemmas on $|'_\ell$ and $|'_r$ from the preceding section, expecially the existence of least common multiples therefore hold for $|_\ell$ and $|_r$, too.

We define reduction and s-polynomials as in the preceding section. Up to the translation lemma all properties still hold. The characterization of Gröbner bases by s-polynomials however must be done by different means, considering that the product of two terms is no longer a term necessarily.

A standard representation of a polynomial wrt. a given basis is a representation without cancellation of terms above the head term.

5.6 Definition *Let $F \subseteq K[X_1,\ldots,X_m][Y;\ \alpha,\delta]$, $f \in K[X_1,\ldots,X_m][Y;\ \alpha,\delta]$ and $t \in T$.*

- *f has a* left *t*-representation wrt. *F iff there exist $f_1, \ldots, f_q \in F$ and $m_1, \ldots, m_q \in M$ such that*

$$f = \sum_{i=1}^{q} m_i * f_i \ \text{ and } \ \forall\, 1 \leqslant i \leqslant q : \mathrm{HT}(m_i * f_i) \preccurlyeq t.$$

- *f has a* right *t*-representation wrt. *F iff there exist $f_1, \ldots, f_q \in F$ and $m_1, \ldots, m_q \in M$ such that*

$$f = \sum_{i=1}^{q} f_i * m_i \ \text{ and } \ \forall\, 1 \leqslant i \leqslant q : \mathrm{HT}(f_i * m_i) \preccurlyeq t.$$

- *f has a* left standard representation wrt. *F iff it has a left $\mathrm{HT}(f)$-representation wrt. F.*

- *f has a* right standard representation wrt. *F iff it has a right* $\mathrm{HT}(f)$*-representation wrt. F.*

5.7 Lemma *Let $F \subseteq K[X_1,\ldots,X_m][Y;\ \alpha,\delta]$ be finite and $f \in K[X_1,\ldots,X_m][Y;\ \alpha,\delta]$.*

- *If f has a left standard representation wrt. F then $f \in I_\ell(F)$.*
- *If f has a right standard representation wrt. F then $f \in I_r(F)$.*

5.8 Lemma *Let $F \subseteq K[X_1,\ldots,X_m][Y;\ \alpha,\delta]$.*

- *If $f \overset{*}{\longrightarrow}_{\ell F} 0$ then f has a left standard representation wrt. F.*
- *If $f \overset{*}{\longrightarrow}_{r F} 0$ then f has a right standard representation wrt. F.*

Proof

- Since $f \overset{*}{\longrightarrow}_{\ell F} 0$ there are $p_1,\ldots,p_q \in F$ and

$$f_1,\ldots,f_{q-1} \in K[X_1,\ldots,X_m][Y;\ \alpha,\delta]$$

such that

$$f \longrightarrow_{\ell p_1} f_1 \longrightarrow_{\ell p_2} \cdots \longrightarrow_{\ell p_{q-1}} f_{q-1} \longrightarrow_{\ell p_q} 0.$$

Therefore we have monomials $m_1,\ldots,m_{q-1} \in \mathrm{M}(K[X_1,\ldots,X_m][Y;\ \alpha,\delta])$ such that

$$f - m_1 * p_1 = f_1,\ f_1 - m_2 * p_2 = f_2,\ldots,f_{q-1} - m_q * p_q = 0,$$

$$\mathrm{HT}(f) \succcurlyeq \mathrm{HT}(m_1 * p_1),\ \mathrm{HT}(f_1) \succcurlyeq \mathrm{HT}(m_2 * p_2),\ldots,\ \mathrm{HT}(f_{q-1}) \succcurlyeq \mathrm{HT}(m_q * p_q)$$

and

$$\mathrm{HT}(f) \succcurlyeq \mathrm{HT}(f_1),\ \mathrm{HT}(f_1) \succcurlyeq \mathrm{HT}(f_2),\ldots,\ \mathrm{HT}(f_{q-2}) \succcurlyeq \mathrm{HT}(f_{q-1}).$$

Thus

$$f = \sum_{i=0}^{q} m_i * p_i$$

and for all $1 \leqslant i \leqslant q$

$$\mathrm{HT}(f) \succcurlyeq \mathrm{HT}(m_i * p_i).$$

- Since $f \xrightarrow{r,*}_F 0$ there are $p_1, \ldots, p_q \in F$ and

$$f_1, \ldots, f_{q-1} \in K[X_1, \ldots, X_m][Y; \alpha, \delta]$$

such that

$$f \xrightarrow{r}_{p_1} f_1 \xrightarrow{r}_{p_2} \cdots \xrightarrow{r}_{p_{q-1}} f_{q-1} \xrightarrow{r}_{p_q} 0.$$

Therefore we have monomials $m_1, \ldots, m_{q-1} \in \mathrm{M}(K[X_1, \ldots, X_m][Y; \alpha, \delta])$ such that

$$f - p_1 * m_1 = f_1,\ f_1 - p_2 * m_2 = f_2, \ldots, f_{q-1} - p_q * m_q = 0,$$

$$\mathrm{HT}(f) \succcurlyeq \mathrm{HT}(p_1 * m_1), \mathrm{HT}(f_1) \succcurlyeq \mathrm{HT}(p_2 * m_2), \ldots, \mathrm{HT}(f_{q-1}) \succcurlyeq \mathrm{HT}(p_q * m_q)$$

and

$$\mathrm{HT}(f) \succcurlyeq \mathrm{HT}(f_1), \mathrm{HT}(f_1) \succcurlyeq \mathrm{HT}(f_2), \ldots, \mathrm{HT}(f_{q-2}) \succcurlyeq \mathrm{HT}(f_{q-1}).$$

Thus

$$f = \sum_{i=0}^{q} p_i * m_i$$

and for all $1 \leqslant i \leqslant q$

$$\mathrm{HT}(f) \succcurlyeq \mathrm{HT}(p_i * m_i).$$

□

5.9 Lemma *Let $F \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$, $f_i, f_i' \in F$ and $m, m_i, m_i' \in M$.*

- *Let $\sum m_i * f_i$ be a left t-representation and $\sum m_i' * f_i'$ be a left t'-representation where $t \succ t'$. Then*
  1. *$\sum m_i * f_i + \sum m_i' * f_i'$ is a left t-representation wrt. F and*
  2. *$m * \sum m_i * f_i$ has a left $m * t$-representation wrt. $\{f_i\}$.*
- *Let $\sum f_i * m_i$ be a right t-representation and $\sum f_i' * m_i'$ be a right t'-representation where $t \succ t'$. Then*
  1. *$\sum f_i * m_i + \sum f_i' * m_i'$ is a right t-representation wrt. F and*

2. $(\sum f_i * m_i) * m$ *has a right* $t * m$*-representation wrt.* $\{f_i\}$.

5.10 Lemma *Let* $f \in K[X_1,\ldots,X_m][Y;\,\alpha,\delta] \setminus \{0\}$ *and* $F \subseteq K[X_1,\ldots,X_m][Y;\,\alpha,\delta]$.

- *If* f *has a left standard representation wrt.* F *then* f *is left reducible wrt.* F.
- *If* f *has a right standard representation wrt.* F *then* f *is right reducible wrt.* F.

Proof • Let $f = \sum m_i * f_i$ be the left standard representation. Then there is a j such that

$$\mathrm{HT}(f) = \mathrm{HT}(m_j * f_j)\,\big(= \mathrm{HT}(m_j * \mathrm{HT}(f_j))\big)\,.$$

So $\mathrm{HT}(f_j) \mid_r \mathrm{HT}(f)$ meaning f is left reducible.

- Similarly.

□

5.11 Lemma *Let* $F \subseteq K[X_1,\ldots,X_m][Y;\,\alpha,\delta]$, $f_1,\ldots,f_s \in F$ *and* $m_1,\ldots,m_s \in M$.

- *Assume for all* $f_1, f_2 \in F$ *we have* $\mathrm{lSPol}(f_1,f_2) = 0$ *or* $\mathrm{lSPol}(f_1,f_2)$ *has a left* t*-representation wrt.* F *where* $t \prec \mathrm{llcm}(\mathrm{HT}(f_1),\mathrm{HT}(f_2))$. *Let*

$$f = \sum_{i=1}^{s} m_i * f_i \in I_\ell(F)$$

If $\mathrm{HT}(\{\, m_i * f_i \mid 1 \leqslant i \leqslant s \,\}) \succ \mathrm{HT}(f)$ *then* f *has a left* t*-representation wrt.* F *with* $t \prec \mathrm{HT}(\{\, m_i * f_i \mid 1 \leqslant i \leqslant s \,\})$.

- *Assume for all* $f_1, f_2 \in F$ *we have* $\mathrm{rSPol}(f_1,f_2) = 0$ *or* $\mathrm{rSPol}(f_1,f_2)$ *has a right* t *representation wrt.* F *where* $t \prec \mathrm{rlcm}(\mathrm{HT}(f_1),\mathrm{HT}(f_2))$. *Let*

$$f = \sum_{i=1}^{s} f_i * m_i \in I_\ell(F)$$

If $\mathrm{HT}(\{\, f_i * m_i \mid 1 \leqslant i \leqslant s \,\}) \succ \mathrm{HT}(f)$ *then* f *has a right* t*-representation wrt.* F *with* $t \prec \mathrm{HT}(\{\, f_i * m_i \mid 1 \leqslant i \leqslant s \,\})$.

Proof • We prove this by induction on s.

$s = 1$: Obvious.

$s+1$: Let w.l.o.g.

$$\mathrm{HT}(\{\, m_i * f_i \mid 1 \leqslant i \leqslant s \,\}) = \mathrm{HT}(m_1 * f_1) = \mathrm{HT}(m_2 * f_2)$$

and define $a := \frac{a_1}{a_2}$ where a_1 and a_2 are the coefficients of m_1 and m_2, respectively. We have

$$f = \underbrace{\sum_{i=3}^{s} m_i * f_i + (1+a)m_2 * f_2}_{g} + m_1 * f_1 - am_2 * f_2.$$

By induction hypothesis g has a left t-representation where

$$t \prec \mathrm{HT}(\{\, m_i * f_i \mid 1 \leqslant i \leqslant s \,\}).$$

Using lemma 5.9 we now need to show only that there is a t-representation with $t \prec \mathrm{HT}(\{\, m_i * f_i \mid 1 \leqslant i \leqslant s \,\})$ for $m_1 * f_1 - am_2 * f_2$.

We have

$$\mathrm{llcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2)) \mid_r \mathrm{HT}(m_1 * f_1) = \mathrm{HT}(am_2 * f_2).$$

Let $m \in M$ be such that

$$\mathrm{HT}(m * \mathrm{llcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2))) = \mathrm{HT}(m_1 * f_1) = \mathrm{HT}(am_2 * f_2).$$

By our assumption on s-polynomials and lemma 5.9 we get a t-representation for $m * \mathrm{lSPol}(f_1, f_2)$, where

$$t \prec m * \mathrm{llcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2)) \preccurlyeq \mathrm{HT}(m_1 * f_1) = \mathrm{HT}(\{\, m_i * f_i \mid 1 \leqslant i \leqslant s \,\}).$$

By definition we have

$$\begin{aligned} m * \mathrm{lSPol}(f_1, f_2) = & \\ & \mathrm{HC}(f_2) \underbrace{m * \frac{\mathrm{llcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2))}{\mathrm{HT}(f_1)}}_{p_1} r * f_1 \\ - \quad & \mathrm{HC}(f_1) \underbrace{m * \frac{\mathrm{llcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2))}{\mathrm{HT}(f_2)}}_{p_2} r * f_2 \end{aligned}$$

where $\mathrm{HM}(p_1) = m_1$ and $\mathrm{HM}(p_2) = m_2$.
We find that

$$m * \mathrm{lSPol}(f_1, f_2) - (m_1 * f_1 - am_2 * f_2) = \underbrace{(p_1 - m_1) * f_1}_{\prec \mathrm{HT}(m_1 * f_1)} \underbrace{- (p_2 - am_2) * f_2}_{\substack{\prec \mathrm{HT}(m_1 * f_1) = \\ \mathrm{HT}(am_2 * f_2)}}$$

and so

$$m_1 * f_1 - am_2 * f_2 = m * \mathrm{lSPol}(f_1 * f_2) - (p_1 - m_1) * f_1 + (p_2 - am_2) * f_2$$

which is a t-representation where $t \prec \mathrm{HT}(\{ m_i * f_i \mid 1 \leqslant i \leqslant s \})$.

- Analogously.

□

5.12 Corollary *Let $F \subseteq K[X_1, \ldots, X_m][Y; \alpha, \delta]$.*

- *If for all $f_1, f_2 \in F$ we have $\mathrm{lSPol}(f_1, f_2) = 0$ or $l\mathrm{SPol}(f_1, f_2)$ has a left t representation wrt. F where $t \prec \mathrm{llcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2))$ then all $f \in I_\ell(F)$ have a left standard representation wrt. F.*

- *If for all $f_1, f_2 \in F$ we have $\mathrm{rSPol}(f_1, f_2) = 0$ or $\mathrm{rSPol}(f_1, f_2)$ has a right t representation wrt. F where $t \prec \mathrm{rlcm}(\mathrm{HT}(f_1), \mathrm{HT}(f_2))$ then all $f \in I_r(F)$ have a left standard representation wrt. F.*

This enables us to characterize Gröbner bases using s-polynomials.

5.13 Corollary *Let* $F \subseteq K[X_1,\ldots,X_m][Y;\,\alpha,\delta]$.

- *If for all* $f_1, f_2 \in F$ *we have* $\mathrm{lSPol}(f_1,f_2) \xrightarrow[\ell]{*}_F 0$ *then for all* $f \in I_\ell(F) \setminus \{0\}$ *we have* $f \xrightarrow[\ell]{*}_F 0$.
- *If for all* $f_1, f_2 \in F$ *we have* $\mathrm{rSPol}(f_1,f_2) \xrightarrow{*}_F 0$ *then for all* $f \in I_r(F) \setminus \{0\}$ *we have* $f \xrightarrow[r]{*}_F 0$.

For a finite $F \subseteq K[X_1,\ldots,X_m][Y;\,\alpha,\delta]$ we can compute a finite left/right Gröbner basis using the Buchberger algorithm. Partial correctness follows from corollary 5.13. The proof of termination uses the fact that construction of s-polynomials and polynomial reduction do not increase the degree in Y of the polynomials in question. This allows to apply the modified Dickson lemma 4.2.

Membership in finitely generated left and right ideals can therefore be decided.

6 Gröbner bases for iterated Ore extensions

Left and right Gröbner bases for (at least twice) iterated Ore extension do generally not exist for any given admissible term order.

6.1 Example Consider an iterated Ore extension

$$K[X_1,\ldots,X_m][Y_1;\,\alpha_1,\delta_1]\cdots[Y_n;\,\alpha_n,\delta_n]$$

where $\alpha_j(X_i) := X_i^{e_{ij}}$ for $e_{ij} \in \mathbb{N} \setminus \{0\}$, $e_{1,1} \geqslant 2$, $\delta_j(X_i) := 0$ and $n \geqslant 2$. W.l.o.g. assume an admissible term order, where $Y_1 \prec Y_2$.

1. We have
$$\mathrm{HT}(\mathrm{I}_\ell(\{Y_2+Y_1, X_1Y_1\})) = T * \left\{ Y_2, X_1Y_1^d \;\middle|\; d \in \mathbb{N} \setminus \{0\} \right\}.$$
2. Additionally let $\alpha_1(X_2) := X_2$. We have
$$\mathrm{HT}(\mathrm{I}_r(\{Y_2+Y_1, X_1Y_1\})) = \left\{ Y_2, X_1^{e_1^d}Y_1^{d+1} \;\middle|\; d \in \mathbb{N} \setminus \{0\} \right\} * T.$$

By example 3.1 we already know there is no finite basis for the respective head term ideals and therefore no finite Gröbner basis.

7 Concluding remarks and outlook

We proved that left and right Gröbner bases of finitely generated left and right ideals in polynomial rings with an added substitution operator can be computed for a special term order in spite of the fact that this rings are generally neither right nor left Noetherian. This solves the ideal membership problem for such ideals.

Applications include deciding the submodule membership problem for finitely generated left or right $K[X_1, \ldots, X_m][Y; \alpha, \delta]$-modules.

In iterated Ore extensions there are generally no finite Gröbner bases for any admissible term order.

Two sided Gröbner bases in iterated Ore extensions with commuting Y_i can also be computed, see ([10]).

References

[1] Th. Becker and V. Weispfenning. *Gröbner Bases, A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, Berlin, Heidelberg, 1993. ISBN 0-387-97971-0, 3-540-97971-9.

[2] K.R. Goodearl and R.B. Warfield. *An Introduction to Non-Commutative Noetherian Rings*, volume 16 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1989.

[3] A. Kandry-Rody and V. Weispfennning. Non-commutative Gröbner bases in algebras of solvable type. *Journal of Symbolic Computation*, 9(1):1–26, January 1990.

[4] H. Kredel. *Solvable Polynomial Rings*. Dissertation, Universität Passau, Passau, 1992.

[5] J.C. McConnel and J.C. Robson. *Non-Commutative Noetherian Rings*. Pure and Applied Mathematics. John Wiley&Sons, Chichester, 1987. ISBN 0 471 91550 5.

[6] Teo Mora. Gröbner bases in non-commutative algebras. In P. Gianni, editor, *Symbolic and Algebraic Computation, International Symposium ISSAC '88, Rome, Italy, July 4–8, 1988, Proceedings*, volume 358 of *Lecture Notes in Computer Science*, pages 150–161, Berlin-Heidelberg-New York, 1989. Springer-Verlag. ISBN 3-540-51084-2, 0-387-51084-2.

[7] Emmy Noether and Werner Schmeidler. Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzausdrücken. *Mathematische Zeitschrift*, pages 1–35, 1920.

[8] Oystein Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34:480–508, 1933.

[9] Michael Pesch. Gröbner bases in rings of substitution operators. In Jacques Calmet, editor, *The Rhine Workshop on Computer Algebra, Karlsruhe March 22-24, 1994, Proceedings*, pages 138–143. Universität Karlsruhe, Institut für Algorithmen und kognitive Systeme, April 1994.

[10] Michael Pesch. Two-sided Gröbner bases in iterated Ore extensions. Technical Report MIP-9602, Universität Passau, Fakultät für Mathematik und Informatik, D-94030 Passau, February 1996.

[11] V. Weispfenning. Finite Gröbner bases in non-Noetherian skew polynomial rings. In P.S. Wang, editor, *ISSAC '92, International Symposium on Symbolic and Algebraic Computation, Berkeley, California*, pages 329–334, New York, 1992. ACM.

 © 1996 M. Pesch