Two-sided Gröbner bases in iterated Ore extensions

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

5th February 1996

MIP-9602

Abstract

We show, how Gröbner bases can be computed for two-sided ideals of iterated Ore extensions with commuting variables.

Given a ring R consider an iterated Ore extension with commuting variables.

Identifying the iterated Ore extension of R and the polynomial ring over R (in the same number of variables) as free left R-Modules all two-sided ideals of the iterated Ore extension are left ideals of the polynomial ring.

We therefore define a Gröbner basis of a two-sided ideal of the iterated Ore extension as a Gröbner basis of this two-sided ideal seen as a left ideal of the corresponding polynomial ring. This, of course, requires that left Gröbner bases exist in the polynomial ring.

If there is an algorithm for computing a left Gröbner basis for any given finite subset of the polynomial ring this algorithm can be extended to compute two-sided Gröbner bases in the iterated Ore extension.

Examples of ground rings R meeting this requirement are polynomial rings over fields or over PID's and solvable polynomial rings.

Contents

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.

The two-sided ideal membership problem in free K-algebras with two or more generators is undecidable, since it comprises the word problem for monoids [3].

In this paper we consider two-sided ideals in iterated Ore extensions with commuting variables. This are skew polynomial rings where the variables commute with each other, but do not commute with the ground ring. A special case of this has been investigated by Weispfenning in [11] and by the author in [9].

As left modules over the ground ring, iterated Ore extensions of a ring can be identified with the (commutative) polynomial ring over this ring (in the same number of variables). Moreover every two-sided ideal of the iterated Ore extension is a left ideal of the polynomial ring.

Consequently, every two-sided ideal is finitely generated if it is finitely generated as a left ideal of the polynomial ring.

A Gröbner basis of a two-sided ideal can be defined as a left Gröbner basis of the two-sided ideal seen as a left ideal of the polynomial ring, provided such left Gröbner bases exist. They can be computed by a modification of the algorithm for computing left Gröbner bases of the corresponding polynomial ring, again, provided such an algorithm exists.

Ground rings which meet this requirement include polynomial rings over fields or over PID's (see e.g. [1]) and skew polynomial rings.

Applications are the algorithmic solution of the two-sided ideal membership problem and computing in residue class rings of the iterated Ore extension.

We will proceed with a short section containing basic facts about iterated Ore extension. In the third section we consider iterated Ore extensions with commuting variables, especially the connection between their two-sided ideals and the corresponding left ideals. We then define two-sided Gröbner bases as left Gröbner bases of the corresponding left ideal (if such exists) in the fourth section and give an algorithm to compute them.

2 Iterated Ore extensions

Iterated 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 were then 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 $Y r = \alpha(r)Y + \delta(r)$.*

Proof See [2] $\square$

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 the ground ring R. For ease of notation we extend α_i and δ_i to $R[Y_1;\ \alpha_1, \delta_1] \cdots [Y_n;\ \alpha_n, \delta_n]$ defining for all $1 \leqslant i \leqslant j \leqslant n$ $\alpha_i(Y_j) := Y_j$ and $\delta_i(Y_j) := 0$.

We will frequently use "tuple-notation", e.g. use Y^d instead of $Y_1^{d_1}, \dots, Y_n^{d_n}$ for $d \in \mathbb{N}^n$. All operations on elements of $\mathbb{N}^n$ are then meant bo be componentwise.

To give a representation of multiples of Y^k we define for $\ell, d \in \mathbb{Z}^n$

$$A_{\ell,d} := \begin{cases} \{\, \alpha_1^{a_{11}} \circ \delta_1^{d_{11}} \circ \cdots \circ \alpha_1^{a_{1j_1}} \circ \delta_1^{d_{1j_1}} \circ \cdots \circ \\ \alpha_n^{a_{n1}} \circ \delta_n^{d_{n1}} \circ \cdots \circ \alpha_n^{a_{nj_n}} \circ \delta_n^{d_{nj_n}} \mid \\ \sum\limits_{j=1}^{d} a_j = \ell,\ \sum\limits_{j=1}^{d} d_j = d - \ell,\ a_j, d_j \in \mathbb{N}^n \,\}, & 0 \leqslant \ell \leqslant d \\ \varnothing, & \text{else.} \end{cases}$$

For $d \in \mathbb{Z}^n$ let

$$A_d := \bigcup_{\ell \in \mathbb{Z}^n} A_{\ell,d}.$$

For $d \in \mathbb{N}$ let

$$A_d^* := \bigcup_{\ell \in \mathbb{Z}^n,\ \sum\limits_{i=1}^{n} \ell_i \leqslant d} A_\ell$$

and

$$A_\infty^* := \bigcup_{\ell \in \mathbb{N}^n} A_\ell.$$

2.2 Lemma *Let $R' := R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ be an iterated Ore extension. Let $f \in R$. Then for $d \in \mathbb{N}^n$:*

$$Y^d * f = \sum_{0 \leqslant \ell \leqslant d} Y^\ell \sum_{\sigma \in A_{\ell,d}} \sigma(f).$$

Proof By induction on $d' := \sum\limits_{i=1}^{n} d_i$.

$d' = 1$**:** $Y * f = \alpha(f) Y + \delta(f)$.

$d' + 1$**:** Let $m = \min\left\{\, j \mid d_j \neq 0 \,\right\}$ and $e \in \mathbb{N}^n$ be such that

$$e_i = \begin{cases} 1, & i = m \\ 0, & \text{else.} \end{cases}$$

For all $\ell \in \mathbb{Z}^n$ we have

$$\alpha_m \circ A_{\ell-e,d} \cup \delta_m \circ A_{\ell,d} = A_{\ell,d+e}.$$

Therefore

$$\begin{aligned}
Y^{d+e} * f &= Y^e * \sum_{0 \leqslant \ell \leqslant d} Y^\ell \sum_{\sigma \in A_{\ell,d}} \sigma(f) \\
&= \sum_{0 \leqslant \ell \leqslant d} Y^\ell \sum_{\sigma \in A_{\ell,d}} Y^e * \sigma(f) \\
&= \sum_{0 \leqslant \ell \leqslant d} Y^\ell \sum_{\sigma \in A_{\ell,d}} \alpha_m(\sigma(f)) Y^e + \delta_m(\sigma(f)) \\
&= \left(\sum_{e \leqslant \ell \leqslant d+e} Y^\ell \sum_{\sigma \in A_{\ell-e,d}} \alpha_m(\sigma(f)) \right) + \left(\sum_{0 \leqslant \ell \leqslant d} Y^\ell \sum_{\sigma \in A_{\ell,d}} \delta_m(\sigma(f)) \right) \\
&= \sum_{0 \leqslant \ell \leqslant d+e} Y^\ell \left(\sum_{\sigma \in A_{\ell-e,d}} \alpha_m(\sigma(f)) + \sum_{\sigma \in A_{\ell,d}} \delta_m(\sigma(f)) \right) \\
&= \sum_{0 \leqslant \ell \leqslant d+e} Y^\ell \sum_{\sigma \in A_{\ell,d+e}} \sigma(f)
\end{aligned}$$

□

3 Iterated Ore extensions with commuting variables

Let R be a ring and

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

be an iterated Ore extension with the additional property that for all $1 \leqslant j, j' \leqslant n$ we have

$$Y_j * Y_{j'} = Y_{j'} * Y_j \quad \left(= Y_j Y_{j'}\right).$$

where, again, $*$ denotes the multiplication in the iterated Ore extension.

It has the following properties: For all $r, r' \in R$ and all $1 \leqslant j \leqslant n$:

- $r * Y_j = rY_j$
- $Y_j * r = \alpha_j(r)Y_j + \delta_j(r)$
- $r * r' = rr'$

3.1 Definition *Let* $I, F \subseteq R[Y_1;\ \alpha_1, \delta_1]\cdots[Y_n;\ \alpha_n, \delta_n]$.

- I *is a* two-sided ideal *of* $R[Y_1;\ \alpha_1, \delta_1]\cdots[Y_n;\ \alpha_n, \delta_n]$ *iff*

$$I + I \subseteq I$$

and

$$R[Y_1;\ \alpha_1, \delta_1]\cdots[Y_n;\ \alpha_n, \delta_n] * I * R[Y_1;\ \alpha_1, \delta_1]\cdots[Y_n;\ \alpha_n, \delta_n] \subseteq I.$$

- $I_{t\,R[Y_1;\ \alpha_1, \delta_1]\cdots[Y_n;\ \alpha_n, \delta_n]}(F) := \bigcap \{\ I \supseteq F \mid I \text{ two-sided ideal}\}.$

Two-sided ideals are related to left ideals in $R[Y_1, \ldots, Y_n]$ in the following way.

3.2 Lemma *Every two-sided ideal of* $R[Y_1;\ \alpha_1, \delta_1]\cdots[Y_n;\ \alpha_n, \delta_n]$ *is a left ideal of* $R[Y_1, \ldots, Y_n]$.

Proof Let $I \subseteq R[Y_1;\ \alpha_1, \delta_1]\cdots[Y_n;\ \alpha_n, \delta_n]$ be a two-sided ideal. Obviously $I + I \subseteq I$. We show

$$R[Y_1, \ldots, Y_n]I \subseteq I.$$

Let

$$f := \sum_i r_i Y^i \in I$$

and $r \in R$. Then

$$rf = r * f \in I$$

and

$$Y_j f = Y_j \sum_i r_i Y^i = \sum_i r_i Y_j Y^i = \left(\sum_i r_i Y^i\right) * Y_j \in I.$$

□

3.3 Lemma *Let $F \subseteq R[Y_1, \dots, Y_n]$. If the left ideal generated by F (denoted by $I_{\ell R[Y_1,\dots,Y_n]}(F)$) is a two-sided ideal of $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ then*

$$I_{\ell R[Y_1,\dots,Y_n]}(F) = I_{t R[Y_1;\, \alpha_1,\delta_1]\cdots[Y_n;\, \alpha_n,\delta_n]}(F).$$

Proof

- $\mathrm{I}_{t R[Y_1;\, \alpha_1,\delta_1]\cdots[Y_n;\, \alpha_n,\delta_n]}(F) \subseteq \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F)$ since it is the minimal two-sided ideal containing F.
- $\mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) \subseteq \mathrm{I}_{t R[Y_1;\, \alpha_1,\delta_1]\cdots[Y_n;\, \alpha_n,\delta_n]}(F)$ since it is the minimal left ideal containing F.

□

3.4 Theorem *If R is left Noetherian then $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ is two-sided Noetherian.*

Proof Let $I \subseteq R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ be a two-sided ideal. Then I is a left ideal of $R[Y_1, \dots, Y_n]$ by lemma 3.2. Since R and therefore $R[Y_1, \dots, Y_n]$ is left Noetherian by the Hilbert basis theorem (see [2]) there is a finite $F \subseteq R[Y_1, \dots, Y_n]$ with $\mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) = I$. By lemma 3.3 we have $\mathrm{I}_{t R[Y_1;\, \alpha_1,\delta_1]\cdots[Y_n;\, \alpha_n,\delta_n]}(F) = I$. □

We now give a condition for left ideals to be two-sided ideals.

3.5 Lemma *Let $F \subseteq R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ be finite. If for all $\sigma \in A^*_\infty$, all $f \in F$, all $r \in R$, and all $1 \leqslant j \leqslant n$ holds:*

- $Y_j * f \in I_{\ell R[Y_1,\dots,Y_n]}(F)$
- $f * \sigma(r) \in I_{\ell R[Y_1,\dots,Y_n]}(F)$

then

$$I_{\ell R[Y_1,\dots,Y_n]}(F) = I_{t R[Y_1;\, \alpha_1,\delta_1]\cdots[Y_n;\, \alpha_n,\delta_n]}(F).$$

Proof Obviously $\mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) \subseteq \mathrm{I}_{t R[Y_1;\, \alpha_1,\delta_1]\cdots[Y_n;\, \alpha_n,\delta_n]}(F)$. We show that it is a two-sided ideal. Since $\mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F)$ is closed under $\cdot$ and $+$ we only need to show that

$Y_j * \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) \subseteq \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F)$ and $\mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) * r \subseteq \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F)$ for $r \in R$. Let for $r_s \in R$ and $f_s \in F$

$$f = \sum_s r_s Y^{d_s} f_s = \sum_s r_s * f_s * Y^{d_s} \in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F).$$

Then

$$\begin{aligned} Y_j * f &= \sum_s (Y_j * r_s * f_s) Y^{d_s} \\ &= \sum_s \big(\alpha_j(r_s) Y_j + \delta_j(r_s)\big) * f_s Y^{d_s} \\ &= \sum_s Y^{d_s} (\alpha_j(r_s) \underbrace{(Y_j * f_s)}_{\in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F)} + \delta_j(r_s) f_s) \in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) \end{aligned}$$

by our premise. Further we have

$$\begin{aligned} f * r &= \sum_s r_s * f_s * Y^{d_s} * r \\ &= \sum_s r_s \sum_{0 \leqslant j \leqslant d_s} Y^j \sum_{\sigma \in A_{j,d_s}} \underbrace{f_s * \sigma(r)}_{\in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F)} \in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) \end{aligned}$$

□

4 Two-sided Gröbner bases

For this section let $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ be an Ore extension of a ring R with commuting variables.

The correspondence between two-sided ideals of an iterated Ore extension with commuting variables and left ideals of the corresponding polynomial ring motivates a definition of two-sided Gröbner bases in $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ bases using left Gröbner bases in $R[Y_1, \dots, Y_n]$, if existent.

4.1 Definition *An order* $\preccurlyeq$ *on the set of terms* $T \subseteq R[Y_1,\ldots,Y_n]$ *is called a* (left) admissible term order *iff for all* $t,t',t'' \in T$

- $1 \preccurlyeq t$ *and*
- $t \preccurlyeq t' \Longrightarrow t''t \preccurlyeq t'$.

Wrt. a left admissible term order we denote the head term of a polynomial by HT, *the head monomial by* HM *and the head coefficient by* HC.

The main tool here is standard representation.

4.2 Definition *Let* $f \in R[Y_1,\ldots,Y_n]$, $F \subseteq R[Y_1,\ldots,Y_n]$, $r_s \in R$ *and* $f_s \in F$. *We call*

$$f = \sum r_s Y^{d_s} f_s \left(= \sum_s r_s * f_s * Y^{d_s} \right)$$

a left standard representation *of* f *wrt.* F *iff for all* s *holds*

$$\mathrm{HT}(Y^{d_s} * f_s) \preccurlyeq \mathrm{HT}(f).$$

Since two-sided ideals are left ideals the question is how to complete a given basis of a two-sided ideal to a basis of the corresponding left ideal.

4.3 Theorem *Let* $X_1,\ldots,X_m \in R$ *and let* $\rho\colon \mathcal{P}_{\mathit{fin}}(R[Y_1,\ldots,Y_n]) \to \mathbb{N}$ *and*

$$B\colon \mathcal{P}_{\mathit{fin}}(R[Y_1,\ldots,Y_n]) \to \mathcal{P}_{\mathit{fin}}(R[Y_1,\ldots,Y_n])$$

be computable functions.

Assume for all finite $F, F_i \subseteq R[Y_1,\ldots,Y_n]$:

1. $I_{\ell R[Y_1,\ldots,Y_n]}(F) = I_{\ell R[Y_1,\ldots,Y_n]}(B(F))$,
2. *if for all* $i \in \mathbb{N}$ *we have* $I_{\ell R[Y_1,\ldots,Y_n]}(F_i) \subseteq I_{\ell R[Y_1,\ldots,Y_n]}(F_{i+1})$ *then there is some* $j \in \mathbb{N}$ *such that* $B(F_j) = B(F_{j+1})$,

3. *if for all* $\sigma \in A^*_{\rho(F)}$, *all* $f \in F$ *and all* $1 \leqslant i \leqslant m$ *we have*

$$f * \sigma(X_i) \in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F)$$

then for all $f \in F$ *and* $r \in R$ *we have*

$$f * r \in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F).$$

Then for every finite $F \subseteq R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ *the following algorithm computes a finite basis of* $\mathrm{I}_{t\,R[Y_1;\,\alpha_1,\delta_1]\cdots[Y_n;\,\alpha_n,\delta_n]}(F)$ *as a left ideal of* $R[Y_1,\dots,Y_n]$.

funct $TB(F) \equiv$

$$\ulcorner\textbf{while } B\left(F \cup \bigcup_{j=1}^{n} Y_j * F \cup \bigcup_{j=1}^{m} \bigcup_{\sigma\in A^*_{\rho(F)}} F * \sigma(X_j)\right) \neq F \textbf{ do}$$

$$F := B\left(F \cup \bigcup_{j=1}^{n} Y_j * F \cup \bigcup_{j=1}^{m} \bigcup_{\sigma\in A^*_{\rho(F)}} F * \sigma(X_j)\right)$$

od;

$F \lrcorner$

tcnuf

Proof Note that the set $A^*_{\rho(F)}$ is finite by definition.

Termination follows from the second assumption since the sequence F_i of values of F in the ith iteration of the while-loop has the property that

$$\begin{aligned}
\mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F_i) &\subseteq \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}\left(F_i \cup \bigcup_{j=1}^{n} Y_j * F_i \cup \bigcup_{j=1}^{m} \bigcup_{\sigma\in A^*_{\rho(F_i)}} F_i * \sigma(X_j)\right) \\
&= \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}\left(B\left(F_i \cup \bigcup_{j=1}^{n} Y_j * F_i \cup \bigcup_{j=1}^{m} \bigcup_{\sigma\in A^*_{\rho(F_i)}} F_i * \sigma(X_j)\right)\right) \\
&= \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F_{i+1})
\end{aligned}$$

Partial correctness can be shown as follows. A loop invariant is

$$I = \mathrm{I}_{t\,R[Y_1;\,\alpha_1,\delta_1]\cdots[Y_n;\,\alpha_n,\delta_n]}(F),$$

i.e. if $I = \mathrm{I}_{t\,R[Y_1;\,\alpha_1,\delta_1]\cdots[Y_n;\,\alpha_n,\delta_n]}(F)$ holds before entering the while-loop it holds after execution of the while loop. At this point we further have

$$F = B\left(F \cup \bigcup_{j=1}^{n} Y_j * F \cup \bigcup_{j=1}^{m} \bigcup_{\sigma \in A^*_{\rho(F)}} F * \sigma(X_i)\right)$$

and therefore

$$\begin{aligned} \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(F) &= \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}\left(B\left(F \cup \bigcup_{j=1}^{n} Y_j * F \cup \bigcup_{j=1}^{m} \bigcup_{\sigma \in A^*_{\rho(F)}} F * \sigma(X_j)\right)\right) \\ &= \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}\left(F \cup \bigcup_{j=1}^{n} Y_j * F \cup \bigcup_{j=1}^{m} \bigcup_{\sigma \in A^*_{\rho(F)}} F * \sigma(X_j)\right). \end{aligned}$$

The claim now follows from the third premise and lemma 3.5. □

The following lemma enables us to find a function ρ as required above under certain conditions.

4.4 Lemma *Let $F \subseteq R[Y_1,\dots,Y_n]$ with bounded degree (i.e. there exists a d such that for all $f \in F$ we have $\deg(f) \leqslant d$). Further assume that R is a left R'-module, generated by $\mathrm{T}(X_1,\dots,X_m)$ for some $X_1,\dots,X_m \in R$ and $\alpha|R' = \mathrm{id}$.*

If for all $f \in F$, $r \in R$ and $1 \leqslant i \leqslant m$ and all $\sigma \in A^*_{\deg(F)}$ there is a standard representation for

$$f * \sigma(X_i)$$

wrt. F then for all $f \in F$ and all $r \in R$ there is a standard representation for

$$f * r$$

wrt. F.

Proof It clearly suffices to consider the case of a monomial r. Fixing a representation of r as a product of the $X_1,\dots,X_m$, we prove the lemma by induction on $\ell = \deg(r)$. Let $f \in F$.

$\ell = 0$: obvious.

$\ell > 0$: Let $X_i \in \{X_1,\dots,X_m\}$ a the generating element with maximal index i occuring in r.

By our induction hypothesis there exists a standard representation of $f * \frac{r}{X_i}$ wrt. F, namely

$$f * \frac{r}{X_i} = \sum_s r_s f_s Y^{d_s}$$

and therefore

$$\begin{aligned} f * r &= f * \frac{r}{X_i} * X_i \\ &= \sum_s (r_s f_s Y^{d_s}) * X_i \\ &= \sum_s r_s (f_s * Y^{d_s} * X_i) \\ &= \sum_s r_s \left(\sum_{0 \leqslant j \leqslant d_s} Y^j \left(\sum_{\sigma \in A_{j,d_s}} f_s * \sigma(X_i) \right) \right) \end{aligned}$$

Since for all s

$$\sum_k d_{sk} \leqslant \deg\left(\sum_s r_s f_s Y^{d_s}\right) = \deg(f * \frac{r}{X_i}) = \deg(f) \leqslant \deg(F)$$

we have by our premise for all s and all $0 \leqslant j \leqslant d_s$ a Y-standard representation for

$$\sum_{\sigma \in A_{j,d_s}} f_s * \sigma(X_i)$$

and thus for $f * r$.

□

We can now define two-sided Gröbner bases.

4.5 Definition *Let $G \subseteq R[Y_1, \dots, Y_n]$ be a left Gröbner basis in $R[Y_1, \dots, Y_n]$ in the following sense:*

- *there is a Noetherian, confluent reduction relation $\longrightarrow_G$ such that*

$$f \in I_{\ell R[Y_1,\dots,Y_n]}(G) \iff f \xrightarrow{*}_G 0$$

and

- *each $f \in I_{\ell R[Y_1,\dots,Y_n]}(G)$ has a left standard representation wrt. G.*

Then we call G a two-sided Gröbner basis *in $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$, iff*

$$I_{\ell R[Y_1,\dots,Y_n]}(G) = I_{t R[Y_1;\,\alpha_1,\delta_1]\cdots[Y_n;\,\alpha_n,\delta_n]}(G).$$

4.6 Theorem (Characterization of two-sided Gröbner bases) *Let G be a left Gröbner basis in $R[Y_1, \dots, Y_n]$. Further assume the ground ring R is a left R'-module generated by $\mathrm{T}(X_1, \dots, X_m)$, and $\alpha | R' = \mathrm{id}$.*

If

- *for all $1 \leqslant j \leqslant n$ we have $Y_j * g \xrightarrow{*}_G 0$*
- *for all $1 \leqslant i \leqslant m$ and all $\sigma \in A^*_{\deg(G)}$ we have $g * \sigma(X_i) \xrightarrow{*}_G 0$,*

then G is a two-sided Gröbner basis.

Proof We show that $\mathrm{I}_{t R[Y_1;\,\alpha_1,\delta_1]\cdots[Y_n;\,\alpha_n,\delta_n]}(G) = \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(G)$. By definition of a left Gröbner basis and applying lemma 4.4 we get for each $g \in G$ and $r \in R$ a standard representation of $g * r$ wrt. G. Especially we have $g * r \in \mathrm{I}_{\ell R[Y_1,\dots,Y_n]}(G)$. Since we also have $Y_j * g \in I(G)$ for each $g \in G$ by our premise, the claim follows from lemma 3.5. $\square$

This allows computation of two-sided Gröbner bases if the corresponding left Gröbner bases can be computed.

4.7 Theorem *Let G be a left Gröbner basis in $R[Y_1, \dots, Y_n]$. Further assume R is a left R'-module generated by $\mathrm{T}(X_1, \dots, X_m)$, and $\alpha|R' = \mathrm{id}$ and there is a computable function B which returns a left Gröbner basis for any given finite subset F of $R[Y_1, \dots, Y_n]$ where $I_{\ell R[Y_1,\dots,Y_n]}(F) = I_{\ell R[Y_1,\dots,Y_n]}(B(F))$ and if for all $i \in \mathbb{N}$ we have $I_{\ell R[Y_1,\dots,Y_n]}(F_i) \subseteq I_{\ell R[Y_1,\dots,Y_n]}(F_{i+1})$ then there is some $j \in \mathbb{N}$ such that $B(F_j) = B(F_{j+1})$.*

Then the function TB from theorem 4.3 with $\rho := \deg$ computes two-sided Gröbner bases for any given finite subset of $R[Y_1, \dots, Y_n]$.

Proof Using lemma 4.4 we see that all assumptions from theorem 4.3 are satisfied. Therefore *TB* returns a left ideal basis of the two-sided ideal which, since B computes left Gröbner bases, also is a left Gröbner basis. □

4.8 Corollary *Let R be*

- *a computable polynomial ring $K[X_1, \dots, X_m]$ over a field K,*
- *a computable polynomial ring $K[X_1, \dots, X_m]$ over a PID K or*
- *a computable solvable ring $K\{X_1, \dots, X_m\}$ (see [3]).*

Then two-sided Gröbner bases can be computed in $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$ where $\alpha|K = \mathrm{id}$ (using a term order where $Y_1, \dots, Y_n \succ X_1, \dots, X_m$).

In the cases of theorem 4.8 two-sided Gröbner bases can be computed more efficiently. Instead of repeatedly calling the Buchberger algorithm, it can be modified such that apart from adding normal forms of s-polynomials, their (finitely many) right and left multiples mentioned above (or their normal forms) are added.

5 Concluding remarks and outlook

We have shown that two-sided Gröbner bases in iterated Ore extensions with commuting variables of arbitrary rings R can be computed provided Gröbner bases can be computed for left ideals in the polynomial ring $R[Y_1, \dots, Y_n]$.

Applications include computing in residue class rings of the iterated Ore extension $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$. The ideal membership problem for such residue class rings can be solved by lifting the ideal to $R[Y_1;\, \alpha_1, \delta_1] \cdots [Y_n;\, \alpha_n, \delta_n]$.

Left and right Gröbner bases in Ore extensions of polynomial rings can be computed for certain term orders, as shown in [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. Left and right Gröbner bases in Ore extensions of polynomial rings. Technical Report MIP-9601, 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.