UNIVERSITÄT KAISERSLAUTERN
Zentrum für Computeralgebra

REPORTS ON COMPUTER ALGEBRA
NO. 26

Solving One-Sided Equations in Integer Monoid Rings

by

B. Reinert

Jan 2000

The Zentrum für Computeralgebra (Centre for Computer Algebra) at the University of Kaiserslautern was founded in June 1993 by the Ministerium für Wissenschaft und Weiterbildung in Rheinland-Pfalz (Ministry of Science and Education of the state of Rheinland-Pfalz). The centre is a scientific institution of the departments of **Mathematics, Computer Science, and Electrical Engineering** at the University of Kaiserslautern.
The goals of the centre are to advance and to support the use of Computer Algebra in industry, research, and teaching. More concrete goals of the centre include

- the development, integration, and use of software for Computer Algebra
- the development of curricula in Computer Algebra under special consideration of interdisciplinary aspects
- the realisation of seminars about Computer Algebra
- the cooperation with other centres and institutions which have similar goals

The present coordinator of the Reports on Computer Algebra is:
Olaf Bachmann (email: `obachman@mathematik.uni-kl.de`)

Zentrum für Computeralgebra
c/o Prof. Dr. G.-M. Greuel, FB Mathematik
Erwin-Schrödinger-Strasse
D-67663 Kaiserslautern; Germany
Phone: 49 - 631/205-2850 Fax: 49 - 631/205-5052
email: `greuel@mathematik.uni-kl.de`
URL: `http://www.mathematik.uni-kl.de/~zca/`

Solving One-Sided Equations in Integer Monoid Rings

Birgit Reinert
Fachbereich Informatik
Universität Kaiserslautern
67663 Kaiserslautern
Germany
reinert@informatik.uni-kl.de

Abstract

One of the applications of Gröbner bases in commutative polynomial rings is to solve linear equations. Here we show how similar results can be obtained for systems of one-sided linear equations in the more general setting of monoid and group rings.

1 Introduction

Let $\mathbb{Z}[\mathcal{M}]$ be a monoid ring over the integers $\mathbb{Z}$. Further let the monoid $\mathcal{M}$ have a presentation by a finite convergent string rewriting system (Σ, T), i.e. the representatives of the elements are words on Σ and the word problem is decidable by normal form computation.
We show that for $f_1, \ldots, f_k \in \mathbb{Z}[\mathcal{M}]$ the linear inhomogeneous equation $f_1 * X_1 + \ldots + f_m * X_m = f_0$ in the variables $X_1, \ldots, X_m$ has a finite generating set of solutions in case the reduced prefix Gröbner basis of the right ideal generated by $\{f_1, \ldots, f_m\}$ is finite and how a generating set for the solutions can be obtained. A solution for this problem in the case that $\mathcal{M}$ is a free monoid can be found in [1]. Starting from this approach a solution for other monoid rings is provided. While in the case of free monoids, finite prefix Gröbner bases for finitely generated right ideals always exist, this is no longer

the case for arbitrary monoid rings. Therefore, we stress that the approach presented here only applies to those cases, where a finite prefix Gröbner basis exists (in the conclusions we give an outlook to more general cases). Moreover, the set of generating solutions derived from the prefix Gröbner bases in the free monoid case is not sufficient for arbitrary monoid rings. We will show why and enlarge the generating set of solutions. These additional solutions correspond to the situations which are characterized by the concept of saturation when computing Gröbner bases in monoid rings. It is outlined how this approach extends to systems of linear equations. A similar result can be shown for systems of left homogeneous equations using suffix Gröbner bases. Of course prefix reduction is a very restricted reduction relation when studying a monoid ring. If for example the monoid ring is commutative in general no finite prefix Gröbner bases will exist and hence the approach outlined here will not work. Still for many classes of monoids and groups finite Gröbner bases can be computed when using appropriate reduction relations (see e.g. [5] for an overview). We show how for these cases the approach can be adopted yielding that finite generating sets for systems of inhomogeneous equations can be constructed for finitely generated commutative monoid rings and finitely generated group rings for the classes of free groups, plain groups, and polycyclic groups.
The paper is organized as follows: Since the results presented here involve the theory of prefix Gröbner bases in monoid rings, Section 5 provides a rough overview of this field for readers not familiar with the topic. More details and leads to additional literature can be found in [5]. In Section 2 we show how Baader's results from [1] for solving one inhomogeneous equation can be extended to arbitrary monoid rings fulfilling our assumptions. We outline why additional solutions have to be defined. In Section 3 we show how this approach can be applied to characterize solutions of systems of inhomogeneous equations. In Section 4 we outline how this approach also works for certain group rings where finite Gröbner bases exist with respect to appropriate reduction relations.

2 The Special Case of One Equation

Let $f_0, \ldots, f_k \in \mathbb{Z}[\mathcal{M}]$ and $f_1 * X_1 + \ldots + f_m * X_m = f_0$ be the equation we want to solve. In order to describe the generating set of solutions we have to find *one* solution of the inhomogeneous equation

$$f_1 * X_1 + \ldots + f_m * X_m \quad = \quad f_0. \tag{1}$$

and if possible a finite set of generators for the solutions of the homogeneous equation

$$f_1 * X_1 + \ldots + f_m * X_m \quad = \quad 0. \tag{2}$$

The set of solutions of equation 2 forms a right $\mathbb{Z}[\mathcal{M}]$-module $\mathbb{Z}[\mathcal{M}]^m$ which is called the right module of syzygies of $f_1, \ldots, f_k$ according to the term used for ordinary Gröbner bases in the literature (see e.g. [2]). To find a generating set for this right module we proceed as suggested in [1]:

1. Let $G = \{g_1, \ldots, g_n\}$ be a finite reduced prefix Gröbner basis of the right ideal generated by $\{f_1, \ldots, f_m\}$ in $\mathbb{Z}[\mathcal{M}]$, and $\mathbf{f} = (f_1, \ldots, f_m)$, $\mathbf{g} = (g_1, \ldots, g_n)$ corresponding vectors. There are two linear mappings given by matrices[1] $P \in \mathsf{M}_{m\times n}(\mathbb{Z}[\mathcal{M}])$, $Q \in \mathsf{M}_{n\times m}(\mathbb{Z}[\mathcal{M}])$ such that $\mathbf{f} \cdot P = \mathbf{g}$ and $\mathbf{g} \cdot Q = \mathbf{f}$.

2. Equation 1 is solvable if and only if $f_0 \in \mathsf{ideal}_r(\{f_1, \ldots, f_m\})$. This is equivalent to $f_0 \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$ and the reduction sequence gives rise to a representation $f_0 = \sum_{i=1}^{n} g_i * h_i = \mathbf{g} \cdot \mathbf{h}$ where $\mathbf{h} = (h_1, \ldots, h_n)$. Then, as $\mathbf{f} \cdot P = \mathbf{g}$, we get $\mathbf{g} \cdot \mathbf{h} = (\mathbf{f} \cdot P) \cdot \mathbf{h}$ and $P \cdot \mathbf{h}$ is such a solution of equation 1.

3. Let $\{\mathbf{z}_1, \ldots, \mathbf{z}_r\}$ be a generating set for the solutions of the homogeneous equation

$$g_1 * X_1 + \ldots + g_n * X_n \quad = \quad 0. \tag{3}$$

and let I_m be the $m \times m$ identity matrix. Further let $\mathbf{w}_1, \ldots, \mathbf{w}_m$ be the columns of the matrix $P \cdot Q - I_m$. Since $\mathbf{f} \cdot (P \cdot Q - I_m) = \mathbf{f} \cdot P \cdot Q - \mathbf{f} \cdot I_m = \mathbf{g} \cdot Q - \mathbf{f} = 0$ these are solutions of the homogeneous equation 2 as well. We can even show that the set $\{P \cdot \mathbf{z}_1, \ldots, P \cdot \mathbf{z}_r, \mathbf{w}_1, \ldots, \mathbf{w}_m\}$ generates *all* solutions of 2:
Let $\mathbf{q} = (q_1, \ldots, q_m)$ be an arbitrary solution of equation 2, i.e. $\mathbf{f} \cdot \mathbf{q} = 0$. Then $Q \cdot \mathbf{q}$ is a solution of equation 3 as $\mathbf{f} = \mathbf{g} \cdot Q$. Hence there are

[1] These matrices can be computed during the Gröbner basis computation.

$h_1, \ldots, h_r \in \mathbb{Z}[\mathcal{M}]$ such that $Q \cdot \mathbf{q} = \mathbf{z}_1 * h_1 + \ldots \mathbf{z}_r * h_r$. Further we find

$$\begin{aligned} \mathbf{q} &= P \cdot Q \cdot \mathbf{q} - (P \cdot Q - I_m) \cdot \mathbf{q} \\ &= P \cdot \mathbf{z}_1 * h_1 + \ldots + P \cdot \mathbf{z}_r * h_r \\ &\quad + \mathbf{w}_1 * q_1 + \ldots + \mathbf{w}_m * q_m \end{aligned}$$

and hence $\mathbf{q}$ is a right linear combination of elements in $\{P \cdot \mathbf{z}_1, \ldots, P \cdot \mathbf{z}_r, \mathbf{w}_1, \ldots, \mathbf{w}_m\}$.

Now the important part is to find a generating set for the solutions of the homogeneous equation 3. Let $G = \{g_1, \ldots, g_n\}$ be a finite reduced prefix Gröbner basis of the right ideal generated by $\{f_1, \ldots, f_m\}$ and let $\mathsf{HT}(g_i) = t_i$, $\mathsf{HC}(g_i) > 0$ for $1 \leq i \leq n$. In [1] the following situations define a set of generating zeros:
For every $g_i, g_j \in G$ such that $\mathsf{HT}(g_i)$ is a prefix (as a word) of $\mathsf{HT}(g_j)$, i.e. $\mathsf{HT}(g_j) \equiv \mathsf{HT}(g_i)u$ for some $1 \neq u \in \mathcal{M}$, by Lemma 8 (see Section 5) we know $\mathsf{HC}(g_i) = \mathsf{HC}(g_j) \cdot b$ for some $b \in \mathbb{N} \backslash \{0, 1\}$. We determine vectors $\mathbf{a}_{ij}$ as follows:

$$\mathsf{spol}_p(g_i, g_j) = b \cdot g_j - g_i * u = \sum_{l=1}^{n} g_l * h_l,$$

where the polynomials $h_l \in \mathbb{Z}[\mathcal{M}]$ are due to the reduction sequence $\mathsf{spol}_p(g_i, g_j) \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$.
Then $\mathbf{a}_{ij} = (\alpha_1, \ldots, \alpha_n)$, where

$$\begin{aligned} \alpha_i &= h_i + u, \\ \alpha_j &= h_j - b, \\ \alpha_l &= h_l, \end{aligned}$$

$l \neq i, j$, is a solution of 3 as $\sum_{l=1}^{n} g_l * h_l - b \cdot g_j + g_i * u = 0$.
If no such polynomials exist in G, Baader concluded that the homogeneous equation 3 in the free monoid ring had no solution. This is no longer true for arbitrary monoid rings.

Example 1 *Let $\mathbb{Z}[\mathcal{M}]$ be a monoid ring where $\mathcal{M}$ is presented by the string rewriting system $\Sigma = \{a, b\}$, $T = \{ab \longrightarrow 1\}$. Then for the homogeneous equation*

$$(a + 1) * X_1 + (b + 1) * X_2 = 0$$

we find that the set $\{a+1, b+1\}$ is a reduced prefix Gröbner basis of the right ideal it generates. Moreover neither of the head terms of the polynomials in this basis is prefix of the other. Still the equation can be solved: $(b, -1)$ is a solution since $(a+1) * b - (b+1) = b + 1 - (b+1) = 0$.

This phenomenon is due to the fact that in most monoid rings s-polynomials are not sufficient for a Gröbner basis test. In [6] such a test for monoid rings as described here is presented. Besides testing s-polynomials the following test set has to be considered[2]:
For $t \in \mathcal{M}$ let $C(t) = \{w \in \Sigma^* \mid tw \equiv u_1 u_2 w \equiv u_1 l, u_2 \neq 1$ for some $(l, r) \in T\}$. Additionally, we define vectors $\mathbf{b}_{i,\ell} = (\beta_1, \ldots, \beta_n)$ for g_i and $1 \leq \ell \leq |C(\mathsf{HT}(g_i))|$ as follows: Let $C(\mathsf{HT}(g_i)) = \{w_1, \ldots, w_s\}$. For every $g_i * w_\ell$ we know $g_i * w_\ell = \sum_{l=1}^{n} g_l * h_l$ as G is a prefix Gröbner basis. Then $\mathbf{b}_{i,\ell} = (\beta_1, \ldots, \beta_n)$, where

$$\begin{aligned} \beta_i &= h_i - w_\ell, \\ \beta_l &= h_l, \end{aligned}$$

$l \neq i$, is a solution of equation 3 as $\sum_{l=1}^{n} g_l * h_l - g_i * w_\ell = 0$.

Lemma 2 *The finitely many vectors $\mathbf{a}_{i,j}, \mathbf{b}_{i,\ell}$, $1 \leq i, j \leq n$, $1 \leq \ell \leq |C(\mathsf{HT}(g_i))|$ form a right generating set for all solutions of equation 3.*

Proof :
Let $\mathbf{p} = (p_1, \ldots, p_n)$ be an arbitrary (non-trivial) solution of 3. Let $t_p = \max\{\mathsf{HT}(g_1)\mathsf{HT}(p_1), \ldots, \mathsf{HT}(g_n)\mathsf{HT}(p_n)\}$ be the maximal term when concatenating the head terms of the multiples in the sum $\sum_{i=1}^{n} g_i * p_i = 0$ and K_p the number of multiples $g_i * p_i$ with $\mathsf{HT}(g_i)\mathsf{HT}(p_i) \equiv t_p$. A solution $\mathbf{q}$ is called smaller than $\mathbf{p}$ if either $t_q < t_p$ or $t_q = t_p$ and $K_q < K_p$. We will prove our claim by induction on t_p and K_p[3]. Since we assume $\mathbf{p}$ to be a non-trivial solution, we know $K_p > 1$. Then we can distinguish two cases:

1. If there is $1 \leq i \leq n$ such that $t_p \equiv \mathsf{HT}(g_i)\mathsf{HT}(p_i) \not\equiv \mathsf{HT}(g_i * p_i)$, then $\mathsf{HT}(g_i) \equiv u_1 u_2$, $\mathsf{HT}(p_i) \equiv w_\ell v$, $u_2 \neq 1 \neq w_\ell$ and $u_2 w_\ell \equiv l$ for some

[2] In fact this test set is related to the technique called saturation and explained more precisely in [5].

[3] Note that this ordering is well-founded since we have a well-founded ordering on Σ^* and $K_p \in \mathbb{N}$.

$l \longrightarrow r \in T$, $w_\ell \in C(\mathsf{HT}(g_i))$. Then $\mathbf{q} = \mathbf{p} + \mathsf{HC}(p_i) \cdot \mathbf{b}_{i,\ell} * v$ with

$$\begin{aligned} q_i &= p_i + \mathsf{HC}(p_i) \cdot (h_i - w_\ell) * v \\ q_l &= p_l + \mathsf{HC}(p_i) \cdot h_l * v \end{aligned}$$

$l \neq i$, is again a solution of 3. It remains to show that it is a smaller one. To see this we have to examine the multiples $g_l * q_l$ for all $1 \leq l \leq n$. Remember that since $t_p \equiv \mathsf{HT}(g_i)\mathsf{HT}(p_i) \equiv \mathsf{HT}(g_i)w_l v > \mathsf{HT}(g_i * w_i)v$ we get $\mathsf{HT}(g_l)\mathsf{HT}(h_l)v \leq \mathsf{HT}(g_i * w_l)v < t_p$ as the h_l arise from the reduction sequence $g_i * w_l \overset{*}{\longrightarrow}^{\mathrm{p}}_{G} 0$.

(a) For $l = i$ we get $g_i * q_i = g_i * (p_i + \mathsf{HC}(p_i) \cdot (h_i - w_\ell) * v) = g_i * p_i + \mathsf{HC}(p_i) \cdot g_i * h_i * v - \mathsf{HC}(p_i) \cdot g_i * w_\ell * v$ and as $\mathsf{HT}(g_i)\mathsf{HT}(p_i) \equiv \mathsf{HT}(g_i)w_\ell v$ and the resulting monomials add up to zero we get $\mathsf{HT}(g_i)\mathsf{HT}(q_i) < t_p$.

(b) For $l \neq i$ we get $g_l * q_l = g_l * (p_l + \mathsf{HC}(p_i) \cdot h_l * v) = g_l * p_l + \mathsf{HC}(p_i) \cdot g_l * h_l * v$ and either $\mathsf{HT}(g_l)\mathsf{HT}(q_l) \equiv t_p$ if $\mathsf{HT}(g_l)\mathsf{HT}(p_l) \equiv t_p$ or else $\mathsf{HT}(g_l)\mathsf{HT}(q_l) < t_p$.

Hence either $t_q < t_p$ or K_p is decreased.

2. Let us now assume there are $1 \leq i, j \leq n$ such that $\mathsf{HT}(g_i * p_i) \equiv \mathsf{HT}(g_i)\mathsf{HT}(p_i) \equiv t_p \equiv \mathsf{HT}(g_j)\mathsf{HT}(p_j) \equiv \mathsf{HT}(g_j * p_j)$. Without loss of generality we can assume that $\mathsf{HT}(g_j) \equiv \mathsf{HT}(g_i)u$ for some $u \in \mathcal{M}$. Then by Lemma 8 we know that $\mathsf{HC}(g_i) = \mathsf{HC}(g_j) \cdot b$ for some $b \in \mathbb{Z}$. For the corresponding s-polynomial $g_i * u - g_j \cdot b$ we have a vector $\mathbf{a}_{ij}$ and we can define $\mathbf{q} = \mathbf{p} + \mathsf{HC}(p_i) \cdot \mathbf{a}_{i,j} * v$ where $v = \mathsf{HT}(p_j)$ with

$$\begin{aligned} q_i &= p_i + \mathsf{HC}(p_i) \cdot (h_i - u) * v \\ q_j &= p_j + \mathsf{HC}(p_i) \cdot (h_j + b) * v \\ q_l &= p_l + \mathsf{HC}(p_i) \cdot h_l * v \end{aligned}$$

$l \neq i, j$. It remains to show that this solution indeed is smaller. To do this we examine the multiples $g_l * q_l$ for all $1 \leq l \leq n$.

(a) For $l \neq i, j$ we get $g_l * q_l = g_l * p_l + \mathsf{HC}(p_i) \cdot g_l * h_l * v$ and by Lemma 8 $\mathsf{HT}(g_l * h_l) < \mathsf{HT}(g_i)u$. Hence $\mathsf{HT}(\mathsf{HC}(p_i) \cdot g_l * h_l *$

$v) < \mathsf{HT}(g_i)\mathsf{HT}(p_i) \equiv t_p$ implying either $\mathsf{HT}(g_l)\mathsf{HT}(q_l) \equiv t_p$ if $\mathsf{HT}(g_l)\mathsf{HT}(p_l) \equiv t_p$ or else $\mathsf{HT}(g_l)\mathsf{HT}(q_l) < t_p$.

(b) For $l = i$ we get $g_i * q_i = g_i * p_i + \mathsf{HC}(p_i) \cdot g_i * h_i * v - \mathsf{HC}(p_i) \cdot g_i * u * v$. Since $\mathsf{HM}(g_i * p_i) = \mathsf{HM}(\mathsf{HC}(p_i) \cdot g_i * u * v)$ we find $\mathsf{HT}(g_i)\mathsf{HT}(q_i) < t_p$.

(c) For $l = j$ we get $g_j * q_j = g_j * p_j + \mathsf{HC}(p_i) \cdot g_j * h_j * v + \mathsf{HC}(p_i) \cdot g_j * b * v$. Hence either $\mathsf{HT}(g_j * q_j) = t_p$ if $\mathsf{HM}(g_j * p_j) \neq -\mathsf{HM}(\mathsf{HC}(p_i) \cdot b \cdot g_j * v)$ or $\mathsf{HT}(g_j * q_j) < t_p$.

Hence we find that either $t_q < t_p$ or in case $t_q = t_p$, $K_q < K_p$. Therefore, in all cases the solution $\mathbf{q}$ derived from $\mathbf{p}$ is smaller and we can show our claim by induction.

3 The General Case

Let $f_{i,j} \in \mathbb{Z}[\mathcal{M}]$, $1 \leq i \leq m$, $0 \leq j \leq k$ and

$$\begin{array}{rcl} f_{1,1} * X_1 + \ldots + f_{1,m} * X_m & = & f_{1,0} \\ f_{2,1} * X_1 + \ldots + f_{2,m} * X_m & = & f_{2,0} \\ \vdots & & \vdots \\ f_{k,1} * X_1 + \ldots + f_{k,m} * X_m & = & f_{k,0} \end{array}$$

be the system of equations we want to solve in $\mathbb{Z}[\mathcal{M}]$. Let $\mathbf{f}_i = (f_{1,i}, f_{2,i}, \ldots, f_{k,i})$, $0 \leq i \leq m$ be vectors in the right $\mathbb{Z}[\mathcal{M}]$-module $\mathbb{Z}[\mathcal{M}]^k$. Hence we can abbreviate the system of inhomogeneous equations by

$$\mathbf{f}_1 \cdot X_1 + \ldots + \mathbf{f}_m \cdot X_m = \mathbf{f}_0. \tag{4}$$

In order to describe the generating set of solutions we have to find *one* solution of the inhomogeneous system 4 and if possible a finite set of generators for the solutions of the homogeneous system

$$\mathbf{f}_1 \cdot X_1 + \ldots + \mathbf{f}_m \cdot X_m = \mathbf{0}. \tag{5}$$

We can proceed as described in the previous section. Of course now the prefix Gröbner bases are bases of submodules in the right $\mathbb{Z}[\mathcal{M}]$-module $\mathbb{Z}[\mathcal{M}]^k$, i.e., their elements are vectors $\mathbf{g}_i = (g_{1,i}, g_{2,i}, \ldots, g_{k,i})$ in $\mathbb{Z}[\mathcal{M}]^k$.

1. Let $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$ be a finite reduced prefix Gröbner basis of the right submodule generated by $\{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ in $\mathbb{Z}[\mathcal{M}]^k$, and $\mathbf{F} = (\mathbf{f}_1, \ldots, \mathbf{f}_m)$, $\mathbf{G} = (\mathbf{g}_1, \ldots, \mathbf{g}_n)$ the corresponding vectors of course now in $(\mathbb{Z}[\mathcal{M}]^k)^m$ respectively $(\mathbb{Z}[\mathcal{M}]^k)^n$. There are two linear mappings given by matrices $P \in \mathsf{M}_{m\times n}(\mathbb{Z}[\mathcal{M}])$, $Q \in \mathsf{M}_{n\times m}(\mathbb{Z}[\mathcal{M}])$ such that $\mathbf{F} \cdot P = \mathbf{G}$ and $\mathbf{G} \cdot Q = \mathbf{F}$.

2. Equation 4 is solvable if and only if $\mathbf{f}_0 \in \mathsf{submodule}_r(\{\mathbf{f}_1, \ldots, \mathbf{f}_m\})$ which is again decidable using prefix reduction with respect to G.

3. Let $\{\mathbf{z}_1, \ldots, \mathbf{z}_r\} \subseteq \mathbb{Z}[\mathcal{M}]^n$ be a generating set for the solutions of the homogeneous system

$$\mathbf{g}_1 * X_1 + \ldots + \mathbf{g}_n * X_n \quad = \quad \mathbf{0}. \tag{6}$$

and let I_m be the $m \times m$ identity matrix. Further let $\mathbf{w}_1, \ldots, \mathbf{w}_m \in \mathbb{Z}[\mathcal{M}]^m$ be the columns of the matrix $P \cdot Q - I_m$. Since $\mathbf{F} \cdot (P \cdot Q - I_m) = \mathbf{F} \cdot P \cdot Q - \mathbf{F} \cdot I_m = \mathbf{G} \cdot Q - \mathbf{F} = 0$ these are solutions of the homogeneous system 5 as well. We can even show that the set $\{P \cdot \mathbf{z}_1, \ldots, P \cdot \mathbf{z}_r, \mathbf{w}_1, \ldots, \mathbf{w}_m\}$ generates all solutions of 5:
Let $\mathbf{q} = (q_1, \ldots, q_m)$ be an arbitrary solution of system 5, i.e. $\mathbf{F} * \mathbf{q} = 0$. Then $Q \cdot \mathbf{q}$ is a solution of system 6 as $\mathbf{F} = \mathbf{G} \cdot Q$. Hence there are $h_1, \ldots, h_r \in \mathbb{Z}[\mathcal{M}]$ such that $Q \cdot \mathbf{q} = \mathbf{z}_1 * h_1 + \ldots \mathbf{z}_r * h_r$. Further we find

$$\begin{aligned} \mathbf{q} &= P \cdot Q \cdot \mathbf{q} - (P \cdot Q - I_m) \cdot \mathbf{q} \\ &= P \cdot \mathbf{z}_1 * h_1 + \ldots + P \cdot \mathbf{z}_r * h_r \\ &\quad + \mathbf{w}_1 \cdot q_1 + \ldots + \mathbf{w}_m \cdot q_m \end{aligned}$$

and hence $\mathbf{q}$ is a right linear combination of elements in $\{P \cdot \mathbf{z}_1, \ldots, P \cdot \mathbf{z}_r, \mathbf{w}_1, \ldots, \mathbf{w}_m\}$.

Now the important part is to find a generating set for the solutions of the homogeneous system 6. Let $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$ be a finite reduced prefix Gröbner basis of the right submodule generated by $\{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$. Notice that for vectors $\mathbf{f}$ the head term is defined to be the polynomial in the first non-zero component. We define $\mathsf{nz}(\mathbf{f}) = i$ where $f_j = 0$ for $1 \leq j < i$ and $f_i \neq 0$, $\mathsf{nz}(\mathbf{0}) = 0$. See Section 5 for details how to realize a reduction relation for the module case. Hence we get $\mathsf{HT}(\mathbf{f}) \in \mathbb{Z}[\mathcal{M}]$ and $\mathsf{HT}(\mathsf{HT}(\mathbf{f})) \in \mathcal{M}$. As before we have to distinguish two cases.

1. For every $\mathbf{g}_i, \mathbf{g}_j \in G$ with $\mathsf{nz}(\mathbf{g}_i) = \mathsf{nz}(\mathbf{g}_j)$ such that $\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i)) = \mathsf{HT}(g_{i,s}) = t_{i,s}$ is a prefix (as a word) of $\mathsf{HT}(\mathsf{HT}(\mathbf{g}_{j,s})) = t_{j,s}$, i.e. $t_{j,s} \equiv t_{i,s}u$ for some $1 \neq u \in \mathcal{M}$, by Lemma 8 we know $\mathsf{HC}(g_{i,s}) = \mathsf{HC}(g_{j,s}) \cdot b$ for some $b \in \mathbb{N}\backslash\{0,1\}$. We determine vectors $\mathbf{a}_{ij}$ as follows:

$$\mathsf{spol}(\mathbf{g}_i, \mathbf{g}_j) = b \cdot \mathbf{g}_j - \mathbf{g}_i * u = \sum_{l=1}^{n} \mathbf{g}_l * h_l,$$

   where the polynomials $h_l \in \mathbb{Z}[\mathcal{M}]$ are due to the reduction sequence $\mathsf{spol}(\mathbf{g}_i, \mathbf{g}_j) \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$.
   Then $\mathbf{a}_{ij} = (\alpha_1, \ldots, \alpha_n)$, where

$$\begin{aligned} \alpha_i &= h_i + u, \\ \alpha_j &= h_j - b, \\ \alpha_l &= h_l, \end{aligned}$$

   $l \neq i, j$, is a solution of 6 as $\sum_{l=1}^{n} \mathbf{g}_l * h_l - b \cdot \mathbf{g}_j + \mathbf{g}_i * u = 0$.

2. For $t \in \mathcal{M}$ let $C(t) = \{w \in \Sigma^* \mid tw \equiv u_1u_2w \equiv u_1l, u_2 \neq 1$ for some $(l, r) \in T\}$. Additionally, we define vectors $\mathbf{b}_{i,\ell} = (\beta_1, \ldots, \beta_n)$ for $\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i)) = \mathsf{HT}(g_{i,s}) = t_{i,s}$ and $1 \leq \ell \leq |C(t_{i,s})|$ as follows: Let $C(t_{i,s}) = \{w_1, \ldots, w_s\}$. For every $\mathbf{g}_i * w_\ell$ we know $\mathbf{g}_i * w_\ell = \sum_{l=1}^{n} \mathbf{g}_l * h_l$ as G is a prefix Gröbner basis. Then $\mathbf{b}_{i,\ell} = (\beta_1, \ldots, \beta_n)$, where

$$\begin{aligned} \beta_i &= h_i - w_\ell, \\ \beta_l &= h_l, \end{aligned}$$

   $l \neq i$, is a solution of system 6 as $\sum_{l=1}^{n} \mathbf{g}_l * h_l - \mathbf{g}_i * w_\ell = 0$.

Lemma 3 *The finitely many vectors $\mathbf{a}_{i,j}, \mathbf{b}_{i,\ell}$, $1 \leq i, j \leq n$, $1 \leq \ell \leq |C(\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i)))|$ form a right generating set for all solutions of system 6.*

Proof :
Let $\mathbf{p} = (p_1, \ldots, p_n)$ be an arbitrary (non-trivial) solution of 6. We proceed by showing for all $1 \leq s \leq k$ as follows: Let $t_p = \max\{\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i))\mathsf{HT}(p_i) \mid \mathsf{nz}(\mathbf{g}_i) = s\}$ be the maximal term when concatenating the head terms of the multiples in the sum $\sum_{i=1}^{n} \mathbf{g}_i * p_i = 0$ and K_p the number of multiples $\mathbf{g}_i * p_i$ with $\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i))\mathsf{HT}(p_i) \equiv t_p$ and $\mathsf{nz}(\mathbf{g}_i) = s$. A solution $\mathbf{q}$ is called smaller than $\mathbf{p}$ if either $t_q < t_p$ or $t_q = t_p$ and $K_q < K_p$. We will prove our claim by induction on t_p and K_p[4]. Since we assume $\mathbf{p}$ to be a non-trivial solution, we know $K_p > 1$. Then following the lines of the proof of Lemma 2 we can distinguish two cases:

1. If there is $1 \leq i \leq n$ such that $t_p \equiv \mathsf{HT}(\mathsf{HT}(\mathbf{g}_i))\mathsf{HT}(p_i) \not\equiv \mathsf{HT}(\mathsf{HT}(\mathbf{g}_i) * p_i)$, then $\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i)) \equiv u_1 u_2$, $\mathsf{HT}(p_i) \equiv w_\ell v$, $u_2 \neq 1 \neq w_\ell$ and $u_2 w_\ell \equiv l$ for some $l \longrightarrow r \in T$, $w_\ell \in C(\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i)))$. Then $\mathbf{q} = \mathbf{p} + \mathsf{HC}(p_i) \cdot \mathbf{b}_{i,\ell} * v$ with

$$\begin{aligned} q_i &= p_i + \mathsf{HC}(p_i) \cdot (h_i - w_\ell) * v \\ q_l &= p_l + \mathsf{HC}(p_i) \cdot h_l * v \end{aligned}$$

$l \neq i$, is again a solution of 6. It remains to show that it is a smaller one. To see this we have to examine the multiples $g_{l,s} * q_l$ for all $1 \leq l \leq n$ where $\mathsf{nz}(\mathbf{g}_l) = s$ and $g_{l,s} = \mathsf{HT}(\mathbf{g}_l)$:

   (a) For $l = i$ we get $g_{i,s} * q_i = g_{i,s} * (p_i + \mathsf{HC}(p_i) \cdot (h_i - w_\ell) * v) = g_{i,s} * p_i + \mathsf{HC}(p_i) \cdot g_{i,s} * h_i * v - \mathsf{HC}(p_i) \cdot g_{i,s} * w_\ell * v$ and as $\mathsf{HT}(g_{i,s})\mathsf{HT}(p_i) \equiv \mathsf{HT}(g_{i,s)} w_\ell v$ and the resulting monomials add up to zero we get $\mathsf{HT}(g_{i,s})\mathsf{HT}(q_i) < t_p$[5].

   (b) For $l \neq i$ we get $g_{l,s} * q_l = g_{l,s} * (p_l + \mathsf{HC}(p_i) \cdot h_l * v) = g_{l,s} * p_l + \mathsf{HC}(p_i) \cdot g_{l,s} * h_l * v$ and either $\mathsf{HT}(g_{l,s})\mathsf{HT}(q_l) \equiv t_p$ if $\mathsf{HT}(g_{l,s})\mathsf{HT}(p_l) \equiv t_p$ or else $\mathsf{HT}(g_{l,s})\mathsf{HT}(q_l) < t_p$

   Hence either $t_q < t_p$ or K_p is decreased.

[4] Note that this ordering is well-founded since we have a well-founded ordering on Σ^* and $K_p \in \mathbb{N}$.

[5] Remember that $\mathsf{HT}(g_{i,s})\mathsf{HT}(h_i)v \leq \mathsf{HT}(g_{i,s} * w_l)v < t_p$.

2. Let us now assume there are $1 \leq i, j \leq n$ such that $\mathsf{nz}(\mathbf{g}_i) = \mathsf{nz}(\mathbf{g}_j = s$ and $\mathsf{HT}(\mathsf{HT}(\mathbf{g}_i)) = t_{i,s}$, $\mathsf{HT}(\mathsf{HT}(\mathbf{g}_j)) = t_{j,s}$ with $\mathsf{HT}(t_{i,s} * p_i) \equiv t_{i,s}\mathsf{HT}(p_i) \equiv t_p \equiv t_{j,s}\mathsf{HT}(p_j) \equiv \mathsf{HT}(t_{j,s} * p_j)$. Without loss of generality we can assume that $t_{j,s} \equiv t_{i,s}u$ for some $1 \neq u \in \mathcal{M}$. Then by Lemma 8 we know that $\mathsf{HC}(g_{i,s}) = \mathsf{HC}(g_{j,s}) \cdot b$ for some $b \in \mathbb{Z}$. For the corresponding s-polynomial $\mathbf{g}_i * u - \mathbf{g}_j \cdot b$ we have a vector $\mathbf{a}_{ij}$ and we can define $\mathbf{q} = \mathbf{p} + \mathsf{HC}(p_i) \cdot \mathbf{a}_{i,j} * v$ where $v = \mathsf{HT}(p_j)$ with

$$\begin{aligned} q_i &= p_i + \mathsf{HC}(p_i) \cdot (h_i - u) * v \\ q_j &= p_j + \mathsf{HC}(p_i) \cdot (h_j + b) * v \\ q_l &= p_l + \mathsf{HC}(p_i) \cdot h_l * v \end{aligned}$$

$l \neq i, j$. It remains to show that this solution indeed is smaller. To do this we examine the multiples $g_{l,s} * q_l$ for all $1 \leq l \leq n$ where $\mathsf{nz}(\mathbf{g}_l) = s$ and $g_{l,s} = \mathsf{HT}(\mathbf{g}_l)$.

   (a) For $l \neq i, j$ we get $g_{l,s} * q_l = g_{l,s} * p_l + \mathsf{HC}(p_i) \cdot g_{l,s} * h_l * v$ and by Lemma 8 $\mathsf{HT}(g_{l,s} * h_l) < \mathsf{HT}(g_{i,s})u$. Hence $\mathsf{HT}(\mathsf{HC}(p_i) \cdot g_{l,s} * h_l * v) < \mathsf{HT}(g_{i,s})\mathsf{HT}(p_i) \equiv t_p$ implying either $\mathsf{HT}(g_{l,s})\mathsf{HT}(q_l) \equiv t_p$ if $\mathsf{HT}(g_{l,s})\mathsf{HT}(p_l) \equiv t_p$ or else $\mathsf{HT}(g_{l,s})\mathsf{HT}(q_l) < t_p$.

   (b) For $l = i$ we get $g_{i,s} * q_i = g_{i,s} * p_i + \mathsf{HC}(p_i) \cdot g_{i,s} * h_i * v - \mathsf{HC}(p_i) \cdot g_{i,s} * u * v$. Since $\mathsf{HM}(g_{i,s} * p_i) = \mathsf{HM}(\mathsf{HC}(p_i) \cdot g_{i,s} * u * v)$ we find $\mathsf{HT}(g_{i,s})\mathsf{HT}(q_i) < t_p$.

   (c) For $l = j$ we get $g_{j,s} * q_j = g_{j,s} * p_j + \mathsf{HC}(p_i) \cdot g_{j,s} * h_j * v + \mathsf{HC}(p_i) \cdot g_{j,s} * b * v$. Hence either $\mathsf{HT}(g_{j,s} * q_j) = t_p$ if $\mathsf{HM}(g_{j,s} * p_j) \neq -\mathsf{HM}(\mathsf{HC}(p_i) \cdot b \cdot g_{j,s} * v)$ or $\mathsf{HT}(g_{j,s} * q_j) < t_p$ else.

   Hence we find that either $t_q < t_p$ or in case $t_q = t_p$, $K_q < K_p$.

4 Conclusions

So far we have derived a generating set of solutions for a system of inhomogeneous equations using prefix Gröbner bases. Now in many monoid or group rings, e.g. when the respective structure is commutative, such prefix

Gröbner bases cannot be expected to be finite in general. On the other hand there are examples where finite Gröbner bases exist for finitely generated one or even two-sided ideals in monoid or group rings with respect to reduction relations other than prefix reduction. In general monoid and group rings (one and two-sided) Gröbner bases can be characterized in terms of two kinds of test sets

- $\mathsf{SPOL}(F)$ corresponding to critical polynomials of the generating set F called s-, g-, or m-polynomials depending on the context,
- $\mathsf{SAT}(F)$ corresponding to critical polynomial multiples of the generating set F (compare the saturation techniques described e.g. in [5]).

Both sets are dependent on the reduction relation chosen for the monoid or group ring. Now for those cases where a set G is a Gröbner basis and these two test sets $\mathsf{SPOL}(G)$ and $\mathsf{SAT}(G)$ are finite, a finite set of solutions for the homogeneous equation $g_1 * X_1 + \ldots + g_s * X_s = 0$ where $G = \{g_1, \ldots, g_s\}$ can be derived as described in Section 2. Examples where these ideas are applicable since the test sets are finite and finite respective one-sided Gröbner bases exist are free and plain group rings. Even two-sided finite Gröbner bases and finite test sets exist for commutative monoid rings and polycyclic group rings. A similar extension can be done to treat systems of inhomogeneous equations as described in Section 3. The details are subject of an extended version of this paper.

5 Prefix Gröbner Bases in $\mathbb{Z}[\mathcal{M}]$ and $\mathbb{Z}[\mathcal{M}]^k$

In [3] it was shown how to characterize and compute prefix Gröbner bases in monoid rings $\mathbb{Z}[\mathcal{M}]$ where $\mathcal{M}$ is presented by a finite convergent string rewriting system. Here we want to show that if a finite prefix Gröbner basis exists for a right ideal, then there is also a finite reduced prefix Gröbner basis and we want to list two important properties of such a basis needed to characterize the solutions of the homogeneous equations in the previous section. Further we outline how the technique of Gröbner bases extends to right $\mathbb{Z}[\mathcal{M}]$-modules $\mathbb{Z}[\mathcal{M}]^k$.

In order to use elements of $\mathbb{Z}[\mathcal{M}]$ as rules for reduction we need an ordering on $\mathbb{Z}$ and one on $\mathcal{M}$: We will first specify a total well–founded ordering on $\mathbb{Z}$ [6]:

$$a <_Z b \text{ iff } \begin{cases} a \geq 0 \text{ and } b < 0 \\ a \geq 0, b > 0 \text{ and } a < b \\ a < 0, b < 0 \text{ and } a > b \end{cases}$$

and $a \leq_Z b$ iff $a = b$ or $a <_Z b$[7].
As ordering on $\mathcal{M}$ we take the one induced by the completion ordering on Σ^* of the string rewriting system. This ordering has the advantage that it is admissible with respect to concatenation and we have $uv > u * v$ where $u, v \in \mathcal{M}$ and the multiplication $*$ on $\mathcal{M}$ is realized by normal form computation with respect to the string rewriting system presenting $\mathcal{M}$.
Then for any $p \in \mathbb{Z}[\mathcal{M}]$ we can characterize its largest term as head term $\mathsf{HT}(p)$, the coefficient of this term as $\mathsf{HC}(p)$, $\mathsf{HM}(p) = \mathsf{HC}(p) \cdot \mathsf{HT}(p)$ and $\mathsf{RED}(p) = p - \mathsf{HM}(p)$.
Let us briefly recall the reduction relation used for $\mathbb{Z}[\mathcal{M}]$ in [3].

Definition 4 *Let p, f be two non-zero polynomials in $\mathbb{Z}[\mathcal{M}]$.*
We say f prefix reduces *p to q at $a \cdot t$ in one step, i.e. $p \longrightarrow^{\mathrm{p}}_{g} q$, if*

(a) $t \equiv \mathsf{HT}(f)u$ *for some* $u \in \mathcal{M}$, *i.e.* $\mathsf{HT}(f)$ *is a prefix of* t *as a word.*

(b) $\mathsf{HC}(f) > 0$ *and* $a = \mathsf{HC}(f) \cdot b + d$ *with* $b, d \in \mathbb{Z}$, $b \neq 0$, *and* $0 \leq d < \mathsf{HC}(f)$.

(c) $q = p - f * (b \cdot u)$.

Prefix Gröbner bases with respect to this reduction relation then can be characterized using the concept of prefix s-polynomials combined with some extra polynomials which are necessary to describe the whole right ideal congruence by prefix reduction.

[6]If not stated otherwise $<$ is the usual ordering on $\mathbb{Z}$ where $\ldots < -2 < -1 < 0 < 1 < 2 < \ldots$.

[7]Let $c \in \mathbb{N}$. We call the positive numbers $0, \ldots, c-1$ the remainders of c. Then for each $d \in \mathbb{Z}$ there are unique $a, b \in \mathbb{Z}$ such that $d = a \cdot c + b$ and b is a remainder of c. We get $b < c$ and in case $d > 0$ and $a \neq 0$ even $c \leq d$. Further c does not divide $b_1 - b_2$, if b_1, b_2 are different remainders of c.

Definition 5 *Given two polynomials* $p_1, p_2 \in \mathbb{Z}[\mathcal{M}]$ *with* $HC(p_i) = c_i > 0, HT(p_i) = t_i, RED(p_i) = r_i$ *for* $i = 1, 2$*. If there is* $u \in \mathcal{M}$ *with* $t_1 \equiv t_2 u$ *we have to distinguish:*

1. *If* $c_1 \geq c_2$, $c_1 = a \cdot c_2 + b$*, where* $a, b \in \mathbb{Z}$, $0 \leq b < c_2$*, we get the following superposition causing a critical pair:*

$$\begin{array}{ccc} & a \cdot c_2 \cdot t_2 u + b \cdot t_2 u = c_1 \cdot t_1 & \\ \swarrow & & \searrow \\ -a \cdot r_2 * u + b \cdot t_2 u & & -r_1 \end{array}$$

   This gives us the prefix s–polynomial

$$\mathsf{spol}_p(p_1, p_2) = a \cdot r_2 * u - b \cdot t_2 u - r_1 = a \cdot p_2 * u - p_1.$$

2. *If* $c_2 > c_1$, $c_2 = a \cdot c_1 + b$*, where* $a, b \in \mathbb{Z}$, $0 \leq b < c_1$*, we get the following superposition causing a critical pair:*

$$\begin{array}{ccc} & c_2 \cdot t_2 u = a \cdot c_1 \cdot t_1 + b \cdot t_1 & \\ \swarrow & & \searrow \\ -r_2 * u & & -a \cdot r_1 + b \cdot t_1 \end{array}$$

   This gives us the prefix s–polynomial

$$spol_p(p_1, p_2) = a \cdot r_1 - r_2 * u - b \cdot t_1 = a \cdot p_1 - p_2 * u.$$

Prefix Gröbner bases then can be characterized by the following theorem from [6]:

Theorem 6 *Equivalent are:*

1. $ideal_r(G) \overset{*}{\longrightarrow}{}^{\mathrm{p}}_{G} 0.$
2.
   - *For all* $g_k, g_l \in G$ *we have* $\mathsf{spol}_p(g_k, g_l) \overset{*}{\longrightarrow}{}^{\mathrm{p}}_{G} 0.$
   - *For all* $g \in G$, $w \in C(\mathsf{HT}(g)) = \{w \in \Sigma^* \mid \mathsf{HT}(g)w \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq 1, (l, r) \in T\}$ *we have* $g * w \overset{*}{\longrightarrow}{}^{\mathrm{p}}_{G} 0.$

The set G then is called a prefix Gröbner basis of the right ideal it generates. Notice that without loss of generality we can always assume that all head coefficients of its polynomials are greater than zero.

Lemma 7 *Let G be a finite prefix Gröbner basis and $g \in G$ such that $g \longrightarrow^{\mathrm{p}}_{G\backslash\{g\}} g'$. Then $G\backslash\{g\} \cup \{canon(g')\}$[8] is again a prefix Gröbner basis of the same right ideal.*

Proof :
This follows as $\mathbb{Z}[\mathcal{M}]$ can be shown to be a ring with a reduction relation fulfilling the axioms (A1) - (A4) for reduction rings as presented in [4]. It is easy to see that the reduction relation is terminating (A1), preserves the right ideal congruence (A2) and for any non-zero polynomial $p \longrightarrow^{\mathrm{p}}_{p} 0$ holds (A3). The important axiom allowing to reduce prefix Gröbner bases without losing the prefix Gröbner basis property[9] (A4) holds if for any $h, p, f, q \in \mathbb{Z}[\mathcal{M}]$, $h \longrightarrow^{\mathrm{p}}_{p}$ and $p \longrightarrow^{\mathrm{p}}_{f} q$ imply $h \longrightarrow^{\mathrm{p}}_{\{f,q\}}$.
Let $h \longrightarrow^{\mathrm{p}}_{p}$ at some monomial $a \cdot t$, i.e. $t \equiv \mathsf{HT}(p)u$ for some $u \in \mathcal{M}$, $a = \mathsf{HC}(p) \cdot b + d$, $b, d \in \mathbb{Z}$, $b \neq 0$ and $0 \leq d < \mathsf{HC}(p)$. Moreover, let $p \longrightarrow^{\mathrm{p}}_{f} q$ at some monomial $c \cdot s$, i.e. $s \equiv \mathsf{HT}(f)v$ for some $v \in \mathcal{M}$, $c = \mathsf{HC}(f) \cdot b' + d'$, $b', d' \in \mathbb{Z}$, $b' \neq 0$ and $0 \leq d' < \mathsf{HC}(f)$. We have to distinguish the following cases:

1. If $t \neq s$ then we are done at once, since $\mathsf{HM}(q) = \mathsf{HM}(p)$ and hence $h \longrightarrow^{\mathrm{p}}_{q}$.

2. If $t = s$ we have to be more careful as $c \cdot s = \mathsf{HM}(p)$, i.e. the reduction step took place at the head monomial of p and $c = \mathsf{HC}(p)$, $s = \mathsf{HT}(p)$.

   (a) If $d' \neq 0$ then $\mathsf{HM}(q) = d' \cdot \mathsf{HT}(p)$. We get $a = \mathsf{HC}(p) \cdot b + d = (\mathsf{HC}(f) \cdot b' + d') \cdot b + d = \mathsf{HC}(f) \cdot (b' \cdot b) + d' \cdot b + d$. Now either $0 \leq d' \cdot b + d < \mathsf{HC}(f)$ or there exist $b'', d'' \in \mathbb{Z}$ such that $d' \cdot b + d = \mathsf{HC}(f) \cdot b'' + d''$ with $0 \leq d'' < \mathsf{HC}(f)$. In either case h then can be prefix reduced using f.

[8] $canon(p) = p$ if $HC(p) > 0$ and $canon(p) = -p$ otherwise.

[9] By Theorem 6 a set can be characterized as a prefix Gröbner basis if any element in its right ideal can be prefix reduced to zero using the set.

(b) If $d' = 0$ then $\mathsf{HC}(p) = \mathsf{HC}(f) \cdot b'$ and hence $a = \mathsf{HC}(f) \cdot b' \cdot b$ and $t \equiv \mathsf{HT}(p)u \equiv \mathsf{HT}(f)vu$ imply that h is prefix reducible by f.

Now it is easy to see that $G' = G\backslash\{g\} \cup \{canon(g')\}$ is again a prefix Gröbner basis of the same right ideal. If some polynomial $h \in \mathsf{ideal}_r(G)$ is reducible by G it will also be reducible by G'. q.e.d.

Now a prefix Gröbner basis G is called **reduced** if no $g \in G$ is prefix reducible by $G\backslash\{g\}$.

Lemma 8 *Let G be a reduced prefix Gröbner basis. Further let $g_1, g_2 \in G$ such that $\mathsf{HC}(g_i) = c_i > 0$ and $\mathsf{HT}(g_2) \equiv \mathsf{HT}(g_1)u$ for some $u \in \mathcal{M}$. Then $c_1 = c_2 \cdot b$ for some $b \in \mathbb{N}\backslash\{0, 1\}$ and $u \neq 1$.*

Proof :
We show that the other cases are not possible.

1. Assume that $u = 1$.
   Then without loss of generality we can also assume $c_1 > c_2$ and hence $c_1 = c_2 \cdot b + d$, $b, d \in \mathbb{N}$, $b \neq 0$ and $0 \leq d < c_2$. Therefore, $g_1 \longrightarrow^{\mathrm{p}}_{g_2} g_1 - g_2 \cdot b$ contradicting the assumption that G is supposed to be reduced.

2. Now let $u \neq 1$. We have to distinguish two cases:

   (a) If $c_1 > c_2$ again we have $c_1 = c_2 \cdot b + d$, $b, d \in \mathbb{N}$, $b \neq 0$ and $0 < d < c_2$. This situation now gives rise to an s-polynomial $\mathsf{spol}_p(g_1, g_2) = g_1 * u - g_2 \cdot b$. Notice that this s-polynomial has head monomial $d \cdot \mathsf{HT}(g_2)$ and hence is neither reducible by g_1 nor by g_2. On the other hand, as G is a prefix Gröbner basis, the s-polynomial must be reducible to zero using elements of G. Additionally we know that g_2 is reducible by this s-polynomial which implies that then g_2 must also be reducible by some element in G contradicting our assumption of G being reduced.

   (b) If $c_2 > c_1$ we get $c_2 = c_1 \cdot b + d$, $b, d \in \mathbb{N}$, $b \neq 0$ and $0 \leq d < c_1$. Then $g_2 \longrightarrow^{\mathrm{p}}_{g_1} g_2 - g_1 \cdot (b \cdot u)$ as before contradicting the assumption that G is supposed to be reduced.

Hence the only possible case remains to be $c_1 = c_2 \cdot b$ for some $b \in \mathbb{N}\backslash\{0,1\}$ and $u \neq 1$. As before this gives rise to an s-polynomial, but now we cannot conclude that one of the polynomials g_1, g_2 is reducible by it hence since we get no contradiction to G being reduced, this case is possible. q.e.d.

If we want to compute prefix Gröbner bases of submodules in a right $\mathbb{Z}[\mathcal{M}]$-module $\mathbb{Z}[\mathcal{M}]^k$ this can be done by introducing a reduction relation and completing it. Provided a finite basis $\mathbf{e}_1 = (1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$ of $\mathbb{Z}[\mathcal{M}]^k$ its elements can be represented by polynomials $\mathbf{f} = \sum_{i=1}^{k} \mathbf{e}_i \cdot f_i$. A reduction relation now can be defined as follows:

Definition 9 *Let* $\mathbf{f} = \sum_{i=1}^{k} \mathbf{e}_i * f_i$, $\mathbf{p} = \sum_{i=1}^{k} \mathbf{e}_i * p_i \in \mathbb{Z}[\mathcal{M}]^k$. *We say that* **f prefix reduces p** *to* **q** *at* $\mathbf{e}_s * p_s$ *in one step, denoted by* $\mathbf{p} \longrightarrow_{\mathbf{f}} \mathbf{q}$, *if*

(a) $p_j = 0$ *for* $1 \leq j \leq s$,

(b) $p_s \longrightarrow^{\mathrm{p}}_{f_s} q_s$ *with* $q_s = p_s - a \cdot f_s * w$, *and*

(c) $\mathbf{q} = \mathbf{p} - a \cdot \mathbf{f} * w = (p_1, \ldots, p_{s-1}, q_s, p_{s+1} - a \cdot f_{s+1} * w, \ldots, p_k - a \cdot f_k * w)$.

Hence prefix reduction in $\mathbb{Z}[\mathcal{M}]^k$ reduces to prefix reduction in $\mathbb{Z}[\mathcal{M}]$. One can show that $\mathbb{Z}[\mathcal{M}]^k$ together with this reduction relation fulfills (A1) – (A4) for reduction rings as specified in [4] and Gröbner bases can be characterized using g- and m-polynomials. The basic idea is to compute a prefix Gröbner basis of a right $\mathbb{Z}[\mathcal{M}]$-module generated by a set of vectors F by modifying the set F according to the following steps:

1. initialize a counter $i = 1$,

2. compute a prefix Gröbner basis of the right ideal generated by the head terms of those vectors $\mathbf{f} \in F$ with $\mathsf{nz}(\mathbf{f}) = i$ which is in fact a prefix Gröbner basis computation in $\mathbb{Z}[\mathcal{M}]$ which also affects the components of the vectors involved "below" the i-th component,

3. compute a set of solutions for the homogeneous equation related to those vectors $\mathbf{f} \in F$ with $\mathsf{nz}(\mathbf{f}) = i$ hence generating new generators for the submodule with non-zero component larger than i,

4. continue for $i = i + 1$ until all components have been handled.

References

[1] F. Baader. *Unification in commutative theories, Hilbert's basis theorem and Gröbner bases.* In *Proc. UNIF'89*, 1989.

[2] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer, 1992.

[3] K. Madlener and B. Reinert. *On Gröbner bases in monoid and group rings.* SEKI Report SR-93-08, Universität Kaiserslautern, 1993. http://www-madlener.informatik.uni-kl.de/ag-madlener/staff/reinert/publications_en.html

[4] K. Madlener and B. Reinert. *Gröbner bases in non-commutative reduction rings.* In B. Buchberger and F. Winkler, editors, *Gröbner Bases and Applications (Proc. of the Conference 33 Years of Gröbner Bases)*, volume 251 of *London Mathematical Society Lecture Notes Series*, pages 408–420. Cambridge University Press, 1998.

[5] K. Madlener and B. Reinert. *String rewriting and Gröbner bases – a general approach to monoid and group rings.* In M. Bronstein, J. Grabmeier, and V. Weispfenning, editors, *Proceedings of the Workshop on Symbolic Rewriting Techniques, Monte Verita, 1995*, volume 15 of *Progress in Computer Science and Applied Logic*, pages 127–180. Birkhäuser, 1998.

[6] B. Reinert. *On Gröbner Bases in Monoid and Group Rings.* PhD thesis, Universität Kaiserslautern, 1995. http://www-madlener.informatik.uni-kl.de/ag-madlener/staff/reinert/publications_en.html

List of papers published in the Reports on Computer Algebra series

[RCA:29] Greuel, G.-M. Computer Algebra and Algebraic Geometry – Achievements and Perspectives. Feb 2000.

[RCA:28] Siebert, T. Recursive Computation of Free Resolutions and a Generalized Koszul Complex. Jan 2000.

[RCA:27] Bachmann, O. and Gräbe, H.-G. The SymbolicData Project: Towards an Electronic Repository of Tools and Data for Benchmarks of Computer Algebra Software. Jan 2000.

[RCA:26] B. Reinert. Solving One-Sided Equations in Integer Monoid Rings. Jan 2000.

[RCA:25] B. Reinert and D. Zeckzer. Coset Enumeration using Prefix Gröbner Bases in Mrc – An Experimental Approach. Nov 1999.

[RCA:23] Birgit Reinert. Observations on coset enumeration. Nov 1998.

[RCA:22] K. Madlener and F. Otto. Some Applications Of Prefix-Rewriting In Monoids, Groups, And Rings. November 1998.

[RCA:21] G.-M. Greuel, G. Pfister, and H. Schönemann. Singular version 1.2 user manual. June 1998.

[RCA:20] B. Reinert and D. Zeckzer. MRC – A System for Computing Gröbner Bases in Monoid and Group Rings. July 1998.

[RCA:19] B. Reinert, K. Madlener, and T. Mora. A note on nielsen reduction and coset enumeration. February 1998.

[RCA:18] O. Bachmann and H. Schönemann. Monomial Representations for Gröbner Bases Computations. January 1998.

[RCA:17] Thomas Siebert. An algorithm for constructing isomorphisms of modules. January 1998.

[RCA:16] K. Madlener and B. Reinert. String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings. October 1997.

[RCA:15] B. Martin and T. Siebert. Splitting Algorithm for vector bundles. September 1997.

[RCA:14] K. Madlener and B. Reinert. Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings. September 1997.

[RCA:12] O. Bachmann, S. Gray, and H. Schönemann. MP Prototype Specification. Dec 1997.

[RCA:11] O. Bachmann. Effective simplification of cr expressions. January 1997.

[RCA:10] O. Bachmann, S. Gray, and H. Schönemann. A proposal for syntactic data integration for math protocols. January 1997.

[RCA:09] B. Reinert. Introducing reduction to polycyclic group rings – a comparison of methods. October 1996.

[RCA:08] T. Siebert. On strategies and implementations for computations of free resolutions. September 1996.

[RCA:02] H. Schönemann. Algorithms in singular. June 1996.

[RCA:01] H. Grassmann, G.-M. Greuel, B. Martin, W. Neumann, G. Pfister, W. Pohl, H. Schönemann, and T. Siebert. Standard bases, syzygies and their implementation in singular. July 1996.