# Computing Gröbner Bases in Monoid and Group Rings


Klaus Madlener
Birgit Reinert
Fachbereich Informatik, Universität Kaiserslautern
W–6750 Kaiserslautern, Germany
email: madlener@informatik.uni-kl.de, reinert@informatik.uni-kl.de



## Abstract

Following Buchberger's approach to computing a Gröbner basis of a polynomial ideal in polynomial rings, a completion procedure for finitely generated right ideals in $\mathbf{Z}[\mathcal{H}]$ is given, where $\mathcal{H}$ is an ordered monoid presented by a finite, convergent semi–Thue system $(\Sigma, T)$. Taking a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ we get a (possibly infinite) basis of the right ideal generated by $F$, such that using this basis we have unique normal forms for all $p \in \mathbf{Z}[\mathcal{H}]$ (especially the normal form is zero in case $p$ is an element of the right ideal generated by $F$). As the ordering and multiplication on $\mathcal{H}$ need not be compatible, reduction has to be defined carefully in order to make it Noetherian. Further we no longer have $p \cdot x \longrightarrow_p 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$. Similar to Buchberger's s–polynomials, confluence criteria are developed and a completion procedure is given. In case $T = \emptyset$ or $(\Sigma, T)$ is a convergent, 2–monadic presentation of a group with inverses of length 1, termination can be shown. An application to the subgroup problem is discussed.


## 1 Introduction

The theory of Gröbner bases for polynomial ideals in commutative polynomial rings over fields $K[x_1, \ldots, x_n]$ was introduced by Buchberger in 1965 [Bu85]. It established a rewriting approach to the theory of polynomial ideals. A Gröbner basis $G$ is a generating set of a polynomial ideal such that every polynomial has a unique normal form using the polynomials in $G$ as rules (especially the polynomials in the ideal reduce to zero). Buchberger gave a terminating procedure to transform a generating set of polynomials into a Gröbner basis of the same ideal. In case we have a finite Gröbner basis many algebraic questions concerning polynomial ideals become solvable, e.g. the membership problem or the congruence problem. Authors as Kandri–Rody, Kapur, Lauer and Weispfenning extended this theory to other coefficient rings as the integers, Euclidean rings or regular rings [Bu85, KaKa84, KaKa88, La76, We87]. Recently there have been some attempts to expand these ideas to non–commutative polynomial rings, which are in general non–Noetherian. Take for example $\mathbf{Z}[\mathcal{H}]$ where $\mathcal{H}$ is the free monoid presented by $\Sigma = \{a, b, c\}, T = \emptyset$. Then the corresponding (right–, left–) ideals generated by $\{ab^ic - b^i \mid i \in \mathbf{N}\}$ do not have a finite basis. Authors as Mora, Baader, Kandri–Rody and Weispfenning have investigated the situation for special non–commutative polynomial rings, e.g. the ring $R\langle x_1, \ldots, x_n \rangle$, where $R$ denotes a field in [Mo85] or the integers in [Ba89], and algebras of solvable type as introduced in [KaWe90] or skew polynomial rings as introduced in [We92]. They have shown that in these cases finitely generated right ideals (or even ideals) admit finite Gröbner bases. These approaches have in common that their orderings are monotone with respect to multiplication on the respective structure: if $t_1 > t_2$ then $t_1 \cdot x > t_2 \cdot x$. The results of Baader and Mora can be described using the ring $R[\mathcal{H}]$, where $\mathcal{H}$ is the free monoid presented by $\Sigma = \{x_1, \ldots, x_n\}, T = \emptyset$. The main idea of this paper is to generalize these approaches to monoid rings $R[\mathcal{H}]$, where $\mathcal{H}$ is an ordered monoid presented by a finite, convergent semi–Thue system $(\Sigma, T)$.

In the next section the basic definitions of monoid rings $R[\mathcal{H}]$ and some examples are given. Section 3 discusses how polynomials can be used as rules. Two different definitions of reduction together with their properties and (dis–) advantages are given. Since ordering and multiplication on $\mathcal{H}$ need not be monotone, one main lack of our reduction is that $p \cdot x$, where $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$, need not be reducible to zero by $p$. In section 4 the concept of saturation is introduced, which gives a solution to this problem. Section 5 gives an algorithmic approach to this concept. We end up with a (possibly infinite) set $\textsc{Sat}(p)$ of polynomials, which allows us to reduce $p \cdot x$ to



ACM-ISSAC '93-7/93/Kiev, Ukraine
© 1993 ACM 0-89791-604-2/93/0007/0254...$1.50

zero. Saturating sets in general are no Gröbner bases, i.e. the reduction induced by them need not be confluent. In section 6 a confluence test is developed using a concept similar to Buchberger's s–polynomials. A procedure is provided, which takes a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ and produces a (possibly infinite) Gröbner basis of the right ideal generated by $F$, such that using this basis we have unique normal forms for all $p \in \mathbf{Z}[\mathcal{H}]$, and the normal form is zero in case $p$ lies in the right ideal generated by $F$. The procedure can be shown to terminate in case $T = \emptyset$ or $(\Sigma, T)$ is a convergent, 2–monadic presentation of a group with inverses of length 1, so in this case finitely generated right ideals admit finite Gröbner bases, even if the monoid ring is non–Noetherian. The class of groups presented by convergent, 2–monadic presentations with inverses of length 1 is the class of plain groups, i.e. free products of free and finitely many finite groups [MaOt89]. Further we give a short outline how this approach can be successfully applied to other special presentations $(\Sigma, T)$ of $\mathcal{H}$, where $T$ contains a commutative system for all letters in $\Sigma$. In this case all finitely generated ideals admit finite Gröbner bases. Finally a brief application to the subgroup problem is given, i.e. given a subgroup $S$ of a group $\mathcal{G}$ and an element $g \in \mathcal{G}$, decide whether $g \in S$. The proofs of the theorems of this paper can be found in [MaRe].

## 2 Basic Definitions

Let $R$ be a ring and let $\mathcal{H}$ be a monoid. Then $R[\mathcal{H}]$ denotes the set of all mappings $f : \mathcal{H} \to R$ where the set $\{m \in \mathcal{H} \mid f(m) \neq 0\}$ is finite. Abbreviating $f(m)$ by $a_m \in R$ we can express $f$ by the "polynomial" $f = \sum_{m \in \mathcal{H}} a_m \cdot m$. Further we define *addition* and *multiplication* in $R[\mathcal{H}]$ as follows: Let $f = \sum_{m \in \mathcal{H}} a_m \cdot m$ and $g = \sum_{m \in \mathcal{H}} b_m \cdot m$ denote two elements of $R[\mathcal{H}]$. Then the sum of $f$ and $g$ is denoted by $f + g$, where $(f+g)(m) = f(m) + g(m)$ or expressed in terms of polynomials $f + g = \sum_{m \in \mathcal{H}} (a_m + b_m) \cdot m$. The product of $f$ and $g$ is denoted by $f \cdot g$, where $(f \cdot g)(m) = \sum_{x \cdot y = m \in \mathcal{H}} f(x) \cdot g(y)$ or expressed in terms of polynomials $f \cdot g = \sum_{m \in \mathcal{H}} c_m \cdot m$ with $c_m = \sum_{x \cdot y = m \in \mathcal{H}} a_x \cdot b_y$. It is easily seen that $R[\mathcal{H}]$ is indeed a ring [1] and we call $R[\mathcal{H}]$ the *monoid ring* of $\mathcal{H}$ over $R$ or in case $\mathcal{H}$ is a group the *group ring* of $\mathcal{H}$ over $R$.

**Example 1**

*(a) Let $\mathcal{G}$ be a group. Then $\mathbf{Z}[\mathcal{G}]$ denotes the group ring of $\mathcal{G}$ over the integers $\mathbf{Z}$.*

*(b) Let $\mathcal{H} = \langle x \rangle$ be the free monoid with one generator. Then $R[\mathcal{H}]$ is isomorphic to the well-known polynomial ring in one indeterminate $R[x]$.*

[1] All operations mainly involve the coefficients in the ring $R$.

We will restrict our considerations to right ideals only. For a subset $F \subseteq R[\mathcal{H}]$ we call $ideal_r(F) = \{\sum_{i=1}^{n} c_i \cdot p_i \cdot m_i \mid n \in \mathbf{N}, c_i \in R, p_i \in F, m_i \in \mathcal{H}\}$ the *right ideal* generated by $F$. Two elements $f, g \in R[\mathcal{H}]$ are said to be *congruent modulo $ideal_r(F)$* (we write $f \equiv_{ideal_r(F)} g$), if $f = g + h$, where $h \in ideal_r(F)$, i.e. $f - g \in ideal_r(F)$. As we are interested in methods of Gröbner basis calculations for right ideals in $R[\mathcal{H}]$, we need a presentation of our monoid $\mathcal{H}$. Every monoid $\mathcal{H}$ can be presented by a pair $(\Sigma, T)$, where $\Sigma$ is an alphabet and $T$ a semi–Thue system over $\Sigma$. One only has to choose $\Sigma = \mathcal{H}$ and $T$ the multiplication table of the monoid. Since this presentation might be infinite or even non–recursive, we are only interested in monoids, which allow "nice" presentations. Therefore, we will restrict ourselves to presentations, where $\Sigma$ is finite and $T$ is finite, confluent and Noetherian. We will call such presentations convergent. Then each word in $\Sigma^*$ has a unique normal form with respect to $T$ and the monoid $\mathcal{H}$ is isomorphic to the set $IRR(T)$. The empty word $\lambda \in \Sigma^*$ presents the identity of $\mathcal{H}$. If $\cdot$ denotes the binary operation on $\mathcal{H}$, given $x, y \in \mathcal{H}$ we define $x \cdot y = (xy)\downarrow_T$, where $w\downarrow_T$ denotes the normal form of $w$ with respect to $T$.

**Example 2**

*(a) Let $\Sigma = \{x_1, \ldots, x_n\}$ and $T_c = \{x_i x_j \longrightarrow x_j x_i \mid j < i,\ i, j \in \{1, \ldots n\}\}$. Then $\mathcal{H}$ is the free commutative monoid generated by $\Sigma$ and $R[\mathcal{H}]$ is isomorphic to $R[x_1, \ldots x_n]$, the polynomial ring in $n$ indeterminates.*

*(b) Let $\Sigma = \{x_1, \ldots, x_n, x_1^{-1}, \ldots x_n^{-1}\}$ and $T = \{x_i^{\delta} x_j^{\delta'} \longrightarrow x_j^{\delta'} x_i^{\delta} \mid j < i,\ i, j \in \{1, \ldots n\},\ \delta, \delta' \in \{1, -1\}\} \cup \{x_i x_i^{-1} \longrightarrow \lambda, x_i^{-1} x_i \longrightarrow \lambda \mid i \in \{1, \ldots n\}\}$. Then $\mathcal{G}$ is the free commutative group generated by $\Sigma$.*

## 3 Right Reduction in $R[\mathcal{H}]$

Throughout this section let $\mathcal{H}$ be a monoid with a convergent presentation $(\Sigma, T)$. In order to define a reduction in $R[\mathcal{H}]$ we have to use polynomials as rules. Therefore, we introduce an ordering on monomials and, as we are interested in Noetherian reductions, we need a well–founded ordering on the elements of $R[\mathcal{H}]$. If not stated otherwise our well–founded ordering on $\mathcal{H}$ is the ordering induced by the admissible, i.e. compatible with concatenation, well–founded total ordering on $\Sigma^*$ used for orienting $T$ — for example the length–lexicographic ordering in case $T$ is monadic and convergent — in particular $w \succ \lambda$ for all $w \in \Sigma^* - \{\lambda\}$. We will take $R$ to be $\mathbf{Z}$, the ring of the integers.

**Definition 1** *Let $\succ$ denote a well–founded total ordering on $\mathcal{H}$ and $>_{\mathbf{Z}}$ a well–founded ordering on $\mathbf{Z}$.*

(a) *Let $p \in \mathbf{Z}[\mathcal{H}]$.*
*Arranging the $w_i \in \mathcal{H}$ with $p(w_i) \neq 0$ according to $\succ$ we get $w_1 \succ \ldots \succ w_n$, where $w_i \neq w_j$ for $i \neq j$. Using this ordering we write $p = \sum_{i=1}^{n} a_i \cdot w_i$, where $a_i = p(w_i)$. We let $HM(p) = a_1 \cdot w_1$ denote the* head monomial, *$HT(p) = w_1$ the* head term *and $HC(p) = a_1$ the* head coefficient *of p. $RED(p) = p - HM(p)$ stands for the* reductum *of p. $T(p) = \{w_1, \ldots, w_n\}$ is the set of terms occurring in p.*

(b) *Let $p = \sum_{i=1}^{n} a_i \cdot w_i, q = \sum_{j=1}^{m} b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$. p is* greater *than q, i.e. $p > q$, if*

(i) *$HT(p) \succ HT(q)$ or*

(ii) *$HT(p) = HT(q)$ and $HC(p) >_Z HC(q)$ or*

(iii) *$HM(p) = HM(q)$ and $RED(p) > RED(q)$.*

Now we are able to use a polynomial $p \in \mathbf{Z}[\mathcal{H}]$ as a rewrite rule by splitting it into $HM(p) \longrightarrow -RED(p)$ and $HM(p) > -RED(p)$.
The following remark shows that in general a well-founded ordering $\succ$ on $\mathcal{H}$ or $\mathcal{G}$ will not be monotone.

**Remark 1** *Let $\mathcal{G} \neq \{1\}$ be a group with a monotone ordering $\succ$.*

1. *$\mathcal{G}$ cannot contain an element of finite order $g \neq 1$.* *Suppose $g \in \mathcal{G} - \{1\}$ is of finite order, i.e. there is $n \in \mathbf{N}$ minimal such that $g^n = 1$. Without loss of generality let us assume $g \succ 1$. Then (as $\succ$ is monotone and transitive) we get $g^{n-1} \succ 1$ giving us $1 \succ g$, contradicting our assumption.*

2. *The ordering $\succ$ is not well-founded.* *Without loss of generality let us assume $g \succ 1$ for some $g \in \mathcal{G} - \{1\}$. Then (as $\succ$ is monotone) we have $1 \succ g^{-1}$ and (as $\succ$ is transitive) $g \succ 1 \succ g^{-1} \succ \ldots \succ g^{-n}$ for all $n \in \mathbf{N}$* [2].

**Remark 2** *We now will specify a total well-founded ordering on $\mathbf{Z}$* [3]*:*

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

*and $a \leq_Z b$ iff $a = b$ or $a <_Z b$.*
*Let $c \in \mathbf{N}$. We call the positive numbers $0, \ldots, c-1$ the remainders of c. Then for each $d \in \mathbf{Z}$ there are unique $a, b \in \mathbf{Z}$ 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.*

[2] As no $g \in \mathcal{G} - \{1\}$ has finite order.
[3] If not stated otherwise $<$ is the usual ordering on $\mathbf{Z}$.

In defining right reductions in $\mathbf{Z}[\mathcal{H}]$ we have to be more cautious than in defining reductions in the polynomial ring $K[x_1, \ldots, x_n]$ (compare [Bu85]). We will give two possible definitions together with their advantages and disadvantages.

**Definition 2 (Right reduction)**
*Let $p = \sum_{i=1}^{n} a_i \cdot w_i, g = \sum_{j=1}^{m} b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$. We say g* right reduces *p to q at $a_k \cdot w_k$ in one step, i.e. $p \longrightarrow_g^r q$, if*

(a) *$HT(g \cdot x) = v_1 \cdot x = w_k$ for some $x \in \mathcal{H}$.*

(b) *$HC(g \cdot x) > 0$ and $a_k = a \cdot HC(g \cdot x) + b$ for $a, b \in \mathbf{Z}$, $a \neq 0$, b a remainder of $HC(g \cdot x)$.*

(c) *$q = p - a \cdot g \cdot x$.*

*We write $p \longrightarrow_g^r$ if there is a polynomial q as defined above.*
*We can define $\overset{*}{\longrightarrow}^r$, $\overset{+}{\longrightarrow}^r$, $\overset{n}{\longrightarrow}^r$ and right reduction by a set $F \subseteq \mathbf{Z}[\mathcal{H}]$ as usual.*

In order to decide, whether a polynomial $g$ right reduces a polynomial $p$ at a monomial $a_k \cdot w_k$, the equation in (a) must be solvable in $(\Sigma, T)$. Note that if this is possible, there can be no, one or even (infinitely) many solutions depending on $\mathcal{H}$. In case $\mathcal{H}$ is left–cancellative we have at most one solution. In case $\mathcal{H}$ is right–cancellative we get $HC(g \cdot x) = HC(g)$.

**Example 3** *Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{ab \longrightarrow a, cb \longrightarrow a\}$. Then $p = b^2$ is not right reducible by $g = a + b - c$, as $HT(g \cdot b) = b^2 \neq a \cdot b$. On the other hand $p = a + c$ is right reducible by $g = 2a - c + \lambda$, as $g \cdot b = a + b$ and $HT(g \cdot b) = a \cdot b = a$.*

Note that we use $HM(g \cdot x) \longrightarrow -RED(g \cdot x)$ as a rule only in case $HC(g \cdot x) > 0$ and $HT(g \cdot x) = HT(g) \cdot x$. We do not use $HM(g) \longrightarrow -RED(g)$, since then $\longrightarrow^r$ would no longer be Noetherian, i.e. infinite reduction sequences could arise. This is due to the unfortunate fact that our ordering $\succ$ on $\mathcal{H}$ is not necessarily monotone (admissible) in the sense that $m_1 \succ m_2$ does not imply $m_1 \cdot x \succ m_2 \cdot x$.

**Example 4** *Let $\Sigma = \{x, x^{-1}\}$, $x^{-1} \succ x$ and $T = \{xx^{-1} \longrightarrow \lambda, x^{-1}x \longrightarrow \lambda\}$ be a presentation of the free group generated by $\{x\}$. If we use $HM(g) \longrightarrow -RED(g)$ as a rule in definition 2 we can right reduce $x^2 + 1$ by $x^{-1} + x$ in the following manner:*

$$x^2 + 1 \longrightarrow_{x^{-1}+x}^r x^2 + 1 - (x^{-1} + x) \cdot x^3 = -x^4 + 1$$

*and $-x^4 + 1$ again is right reducible by $x^{-1} + x$ causing an infinite reduction sequence.*

**Definition 3 (Prefix right reduction)**
*Let $p = \sum_{i=1}^{n} a_i \cdot w_i, g = \sum_{j=1}^{m} b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$. We say $g$* prefix right reduces *$p$ to $q$ at $a_k \cdot w_k$ in one step, i.e. $p \longrightarrow_g^p q$, if*

(a) *$v_1 x = w_k$ for some $x \in \mathcal{H}$, i.e. $v_1$ is a prefix of $w_k$.*

(b) *$b_1 > 0$ and $a_k = a \cdot b_1 + b$ for $a, b \in \mathbf{Z}, a \neq 0$, $b$ a remainder of $b_1$.*

(c) *$q = p - a \cdot g \cdot x$.*

*We can define $p \longrightarrow_g^p$, $\xrightarrow{*}{}^p$, $\xrightarrow{+}{}^p$, $\xrightarrow{n}{}^p$ and right reduction by a set $F \subseteq \mathbf{Z}[\mathcal{H}]$ as usual.*

Notice that in this case (a) has at most one solution and we always have $HC(g \cdot x) = HC(g)$. We now can use $HM(g) \longrightarrow -RED(g)$ as a rule in case $b_1 > 0$ and $w_k = HT(g)x$. Without this trick of using a restricted multiplication on $\mathcal{H}$ it is very hard to say how a polynomial will "behave".
The following statements hold for both definitions of reduction:

**Lemma 1** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$.*

1. *For all $p, q \in \mathbf{Z}[\mathcal{H}]$, $p \longrightarrow_F q$ implies $p > q$.*
2. *$\longrightarrow_F$ is Noetherian.*
3. *$p \longrightarrow_q 0$ and $q \longrightarrow_w 0$ imply $p \longrightarrow_{\{w,-w\}} 0$.*

**Lemma 2** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, $p, q, h \in \mathbf{Z}[\mathcal{H}]$.*

1. *Let $p - q \longrightarrow_F h$, where the reduction takes place at the monomial $d \cdot t$, and let $t \notin T(h)$. Then there are $p', q' \in \mathbf{Z}[\mathcal{H}]$ such that $p \xrightarrow{*}_F p', q \xrightarrow{*}_F q'$ and $h = p' - q'$.*
2. *Let 0 be the unique normal form of $p \neq 0$ with respect to $F$, and $t = HT(p)$. Then there is a polynomial $f \in F$ such that $p \longrightarrow_f p'$ and $t \notin T(p')$.*
3. *Let 0 be the unique normal form of $p - q$ with respect to $F$. Then there exists a polynomial $g \in \mathbf{Z}[\mathcal{H}]$ such that $p \xrightarrow{*}_F g$ and $q \xrightarrow{*}_F g$.*
4. *$p \xleftrightarrow{*}_F q$ implies $p - q \in ideal_r(F)$.*

Unfortunately, reduction as defined above does lack some of the nice properties that reductions in general have, as e.g. $p \cdot x \longrightarrow_p 0$ or transitivity in the sense that $p \longrightarrow_q$ and $q \longrightarrow_w q_1$ imply $p \longrightarrow_w$ or $p \longrightarrow_{q_1}$.

**Remark 3** 1. *Looking at right reduction as defined in definition 2 we get*

(a) *We no longer have $p \cdot x \xrightarrow{*}{}_p^r 0$ for $p \in \mathbf{Z}[\mathcal{H}]$, $x \in \mathcal{H}$.*
*Taking $\mathcal{H}$ to be the free group generated by $\Sigma = \{x\}$ we find that $(x^{-1} + x) \cdot x = x^2 + 1$ is not right reducible by $x^{-1} + x$. (Compare example 4)*

(b) *Right reduction is not transitive.*
*Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be the presentation of a group. Looking at $p = ba + b, q = a + \lambda$ and $w = c^2 + b$ we get $p \longrightarrow_q^r p - q \cdot ca = -ca + b$ and $q \longrightarrow_w^r q - w \cdot bc = -c + \lambda =: q_1$. Further $p$ is neither right reducible at $ba$ by $w$ or $q_1$, as $w \cdot bc^2 a = ba + c^2 a$ and $q_1 \cdot bca = -ba + bca$ both violate condition (a) of definition 2, nor at $b$, as $w \cdot bc^2 = b + c^2$ and $q_1 \cdot bc = -b + bc$.*

2. *Looking at prefix right reduction as defined in definition 3 we get*

(a) *We no longer have $p \cdot x \xrightarrow{*}{}_p^p 0$ for $p \in \mathbf{Z}[\mathcal{H}]$, $x \in \mathcal{H}$.*
*Taking $\mathcal{H}$ to be the free group generated by $\Sigma = \{x\}$ we find that $(x^{-2} + \lambda) \cdot x = x^{-1} + x$ is not prefix right reducible by $x^{-2} + \lambda$.*

(b) *Prefix right reduction is transitive.*
*Let $p \longrightarrow_q^p$ and $q \longrightarrow_w^p q_1$. In case $HM(q) = HM(q_1)$ we immediately get $p \longrightarrow_{q_1}^p$. Otherwise $HT(q) = HT(w)y$, for some $y \in \mathcal{H}$, and $0 < HC(w) \leq HC(q)$ together imply $p \longrightarrow_w^p$.*

Unfortunately the reflexive, symmetric and transitive closure of (prefix) right reduction with respect to a set of polynomials need not capture the congruence induced by the right ideal generated by these polynomials.

**Remark 4** *$p - q \in ideal_r(F)$ does in general not imply $p \xleftrightarrow{*}{}_F^{(r,p)} q$. Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$. Taking $p = a + b + c, q = b - \lambda$ and $F = \{a + b + c\}$ we get $p - q = a + c + \lambda = (a + b + c) \cdot b \in ideal_r(F)$ but $a + b + c \not\xleftrightarrow{*}{}_F^{(r,p)} b - \lambda$.*

Next we define Gröbner bases for right ideals.

**Definition 4** *A set $G \subseteq \mathbf{Z}[\mathcal{H}]$ is called a* Gröbner basis (with respect to right reduction) *of a set $F \subseteq \mathbf{Z}[\mathcal{H}]$, if*

(i) *$\xleftrightarrow{*}{}_G^r = \equiv_{ideal_r(F)}$*

(ii) *$\xrightarrow{*}{}_G^r$ is confluent.*

As remark 4 shows both reductions in general violate condition (i) of this definition.

# 4 Saturation of a Polynomial $p \in \mathbf{Z}[\mathcal{H}]$

As stated in the previous section, reduction as defined in definition 2 and 3 does not have the property $p \cdot x \xrightarrow{*}{}_p^{(r,p)} 0$ and the reflexive, symmetric, transitive closure need not capture the right ideal congruence relation. The main purpose of this section is to find sets of polynomials in $\mathbf{Z}[\mathcal{H}]$, which allow us to (prefix) right reduce all $a \cdot p \cdot x$ to zero, where $a \in \mathbf{Z}, x \in \mathcal{H}$.

**Definition 5** *Let $p \in \mathbf{Z}[\mathcal{H}]$ and $F \subseteq \{p \cdot x, -p \cdot x \mid x \in \mathcal{H}\}$. $F$ is called a* saturating set *for $p$, if for all $x \in \mathcal{H}$, $p \cdot x \longrightarrow_F^r 0$ holds. $F$ is called a* prefix saturating set *for $p$, if for all $x \in \mathcal{H}$, $p \cdot x \longrightarrow_F^p 0$ holds. $\mathcal{SAT}(p)$ respectively $\mathcal{SAT}_p(p)$ are the families of saturating respectively prefix saturating sets for $p$.*

**Remark 5** *1. Note that in defining (prefix) saturating sets we demand (prefix) right reducibility to* 0 *in* one *step.*

*2. To learn more about (prefix) saturating sets for polynomials, we will take a more constructive look at them.*
*Let $p = \sum_{i=1}^{k} c_i \cdot t_i$, where $c_i \in \mathbf{Z}, t_i \in \mathcal{H}$.*
*Let $X_{t_i} = \{x \in \mathcal{H} \mid HT(p \cdot x) = t_i \cdot x\}$, i.e. the set of all elements, which put $t_i$ in head position*[4].
*Let $Y_{t_i} = \{canon(p \cdot x) \mid x \in X_{t_i}\}$, where $canon(p \cdot x) = p \cdot x$ if $HC(p \cdot x) > 0$ and $canon(p \cdot x) = -p \cdot x$ otherwise.*

*(a) Choosing $B_{t_i} \subseteq Y_{t_i}$ such that for all $p_j \in Y_{t_i}$ we have $p_j \longrightarrow_{B_{t_i}}^r 0$, $\bigcup_{i=1}^{k} B_{t_i} \in \mathcal{SAT}(p)$.*

*(b) Choosing $B_{t_i} \subseteq Y_{t_i}$ such that for all $p_j \in Y_{t_i}$ we have $p_j \longrightarrow_{B_{t_i}}^p 0$, $\bigcup_{i=1}^{k} B_{t_i} \in \mathcal{SAT}_p(p)$.*

*3. In 2 we do not specify how to choose the $B_{t_i}$ and, therefore, (prefix) saturating sets might not be unique. Choosing $B_{t_i} = Y_{t_i}$ we always get saturating sets, which are in general infinite.*

*4. $Y_{t_1}$ must at least contain $canon(p)$, but all other $Y_{t_i}$ can be empty. In case the ordering on $\mathcal{H}$ is monotone, we get $Y_{t_1} = \{canon(p \cdot x) \mid x \in \mathcal{H}\}, Y_{t_i} = \emptyset$ for $i \neq 1$, and $B_{t_1} = \{canon(p)\}$ is a finite saturating set for $p$.*

*5. The right ideal generated by $p$ is the same as the right ideal generated by a (prefix) saturating set for $p$.*

*6. $\mathcal{SAT}(p)$ and $\mathcal{SAT}_p(p)$ need not contain finite sets. Take $\Sigma = \{a, b, c, d, e, f\}$ with $a \succ b \succ c \succ d \succ e \succ f$ and $T = \{abc \longrightarrow ba, bad \longrightarrow e, fbc \longrightarrow bf\}$. Then $(\Sigma, T)$ is a convergent presentation of a cancellative monoid. Now look at $p = a + f$:*
*Then $X_f = \{(bc)^i dw \mid i \in \mathbf{N}, w \in IRR(T)\}$, and $Y_f = \{b^{i+1} f dw + b^i ew \mid i \in \mathbf{N}, w \in IRR\}$ has no finite basis in either sense. Since if it had a finite basis $B_f$, we could choose $k \in \mathbf{N}$ such that $b^{k+1} fd + b^k e \notin B_f$. But then we get $b^{k+1} fd + b^k e \not\longrightarrow_{B_f}^{(r,p)} 0$ as $b^{i+1} fdw \cdot x = b^{k+1} fd$ has no solution in $\mathcal{H}$ unless $w = \lambda$ and $i = k$*[5].

*7. If $q = p \cdot x$ then a (prefix) saturating set for $p$ is also a (prefix) saturating set for $q$ but not vice versa. Take for instance $\Sigma = \{a, b, c\}, a \succ b \succ c, T = \{ab \longrightarrow c\}$ and $p = a + 1, q = p \cdot b = b + c$.*

**Definition 6** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$. We call $F$* (prefix) saturated, *if for all $f \in F$, $x \in \mathcal{H}$ there is $g \in F$ such that $f \cdot x \longrightarrow_g 0$ using the corresponding reduction.*

Note that saturating sets for a polynomial $p$ are saturated and prefix saturating sets are prefix saturated. Further prefix saturated sets are saturated sets and unions of (prefix) saturated sets are again (prefix) saturated. The next lemma gives some insight in the reflexive, symmetric, transitive closure of reduction induced by (prefix) saturated sets.

**Lemma 3** *Let $p \in \mathbf{Z}[\mathcal{H}]$.*

*1. Let $S_1, S_2 \in \mathcal{SAT}(p)$. Then $\xleftrightarrow{*}{}_{S_1}^r = \xleftrightarrow{*}{}_{S_2}^r$.*

*2. Let $S \in \mathcal{SAT}(p)$ and $S_p \in \mathcal{SAT}_p(p)$. Then $\xleftrightarrow{*}{}_S^r = \xleftrightarrow{*}{}_{S_p}^r$.*

*3. Let $S \in \mathcal{SAT}(p), S_p \in \mathcal{SAT}_p(p)$, $f, g \in \mathbf{Z}[\mathcal{H}]$. Then $f \longrightarrow_S^r g$ if and only if $f \longrightarrow_{S_p}^p g$.*

Right now we know that (prefix) saturating sets for a polynomial $p$ (prefix) right reduce the set $\{a \cdot p \cdot x \mid a \in \mathbf{Z}, x \in \mathcal{H}\}$ to zero in one step. However, (prefix) saturated sets allow special representations of the elements belonging to their right ideal and, therefore, enable us to capture their right ideal congruence.

**Lemma 4** *1. Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be a saturated set. Every $g \in ideal_r(F)$ has a representation $g = \sum_{i=1}^{k} c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$, and $HT(f_i \cdot x_i) = HT(f_i) \cdot x_i, HC(f_i \cdot x_i) > 0$.*

*2. Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be a prefix saturated set. Every $g \in ideal_r(F)$ has a representation $g = \sum_{i=1}^{k} c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$, and $HT(f_i \cdot x_i) = HT(f_i) x_i, HC(f_i) > 0$.*

[4] Note that if $\mathcal{H}$ is not right–cancellative one $x$ may belong to different sets.

[5] Every $S \in \mathcal{SAT}(p)$ or $S \in \mathcal{SAT}_p(p)$ must (prefix) right reduce the set $X_f$ to zero in one step.

**Theorem 1** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be a saturated set and $F_p \subseteq \mathbf{Z}[\mathcal{H}]$ be a prefix saturated set, $p, q \in \mathbf{Z}[\mathcal{H}]$.*

1. *Then $p \overset{*}{\leftrightarrow}{}^r_F\, q$ if and only if $p - q \in ideal_r(F)$.*
2. *Then $p \overset{*}{\leftrightarrow}{}^p_{F_p}\, q$ if and only if $p - q \in ideal_r(F_p)$.*

**Corollary 1** *Let $p \in \mathbf{Z}[\mathcal{H}], S \in \mathcal{SAT}(p)$. Then we get*

$$\overset{*}{\leftrightarrow}{}^r_S \;= \equiv_{ideal_r(S)} = \equiv_{ideal_r(p)} .$$

**Corollary 2** *Let $p_1, \ldots p_n \in \mathbf{Z}[\mathcal{H}]$ and $S_1 \in \mathcal{SAT}(p_1)$, $\ldots, S_n \in \mathcal{SAT}(p_n)$. Then*

$$\overset{*}{\leftrightarrow}{}^r_{S_1 \cup \ldots \cup S_n} \;= \equiv_{ideal_r(S_1 \cup \ldots \cup S_n)} = \equiv_{ideal_r(p_1, \ldots, p_n)} .$$

Notice that (prefix) saturating sets for a polynomial $p$ satisfy (i) of definition 4 but in general are no Gröbner bases of $ideal_r(\{p\})$, i.e. the Noetherian relation $\overset{*}{\longrightarrow}{}^r$ induced by them need not be confluent, even restricted to $\{a \cdot p \cdot x \mid a \in \mathbf{Z}, x \in \mathcal{H}\}$ as the following example shows.

**Example 5** *Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$, $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$, and $p = a + b + c$. Then $S = \{a+b+c, a+c+\lambda, bc+c^2+b\} \in \mathcal{SAT}(p)$, $S_p = \{a+b+c, bc+c^2+b, a+c+\lambda, ba+ca+\lambda, ca+a+\lambda, c^2+b+c\} \in \mathcal{SAT}_p(p)$. Neither $\longrightarrow^r_S$ nor $\longrightarrow^r_{S_p}$ are confluent on $\{k \cdot p \cdot x \mid k \in \mathbf{Z}, x \in \mathcal{H}\}$ as the following example shows:*
*We have $a + b + c \longrightarrow^r_{a+c+\lambda} b - \lambda$ and $a + b + c \longrightarrow^r_{a+b+c} 0$ but $b - \lambda \not\overset{*}{\longrightarrow}{}^r_S 0$ and $b - \lambda \not\overset{*}{\longrightarrow}{}^r_{S_p} 0$.*

Even (prefix) saturated sets $F$ do not guarantee that $p \overset{*}{\longrightarrow}{}^r_F 0$ implies $p \cdot x \overset{*}{\longrightarrow}{}^r_F 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$.

**Example 6** *Let $\Sigma = \{a, b, c, d\}$ with $a \succ b \succ c \succ d$ and $T = \{abc \longrightarrow ba, dbc \longrightarrow bd\}$.*
*Then the set $F = \{a - c, cbc - ba, c + d\}$ is (prefix) saturated.*
*Looking at $p = a + d$ we get $p \overset{2}{\longrightarrow}{}^r_F 0$. But $p \cdot bc = ba + bd$ is $F$-irreducible.*

## 5 Prefix Saturation for Monoids with Convergent Presentations

We will give a procedure, which enumerates a prefix saturating set for a polynomial in $\mathbf{Z}[\mathcal{H}]$.

**Procedure Prefix Saturation**

input: $p = \sum_{i=1}^{k} c_i \cdot t_i \in \mathbf{Z}[\mathcal{H}]$,
$(\Sigma, T)$ a convergent presentation of $\mathcal{H}$.
output: $\mathrm{SAT}_p(p) \in \mathcal{SAT}(p)$.

$\mathrm{SAT}_p(p) := \{\mathrm{canon}(p)\}$;
$H := \{\mathrm{canon}(p)\}$;
while $H \neq \emptyset$ do
  $q := \mathrm{remove}(H)$;
  $t := HT(q)$;
  for all $x \in C(t)$ do
    $q' := \mathrm{canon}(q \cdot x)$
    if $q' \not\longrightarrow^p_{\mathrm{SAT}_p(p)} 0$
    then $\mathrm{SAT}_p(p) := \mathrm{SAT}_p(p) \cup \{q'\}$;
      $H := H \cup \{q'\}$
  endfor
endwhile

where $C(t) = \{x \in \mathcal{H} \mid tx = t_1 t_2 x = t_1 l, t_2 \neq \lambda$ for some $(l, r) \in T\}$, *remove* removes a polynomial from a set and *canon* canonizes a polynomial, i.e. multiplies it by $-1$ in case its head coefficient is not positive.
The procedure is illustrated by the following example.

**Example 7** *Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$. Saturating $p = a + b + c$ we get:*
*Initialization: $H := \{a + b + c\}, \mathrm{SAT}_p(p) := \{a + b + c\}$.*
*1. Taking $a + b + c \in H$ and $x \in \{a, b, c\}$ we get $ba + ca + \lambda, a + c + \lambda, bc + c^2 + b$, which are all added to $H$ and $\mathrm{SAT}_p(p)$.*
*2. Taking $ba + ca + \lambda \in H$ and $x \in \{a, b, c\}$ we get $a + b + c, bc + c^2 + b, a + c + \lambda$, which prefix right reduce to zero by $\mathrm{SAT}_p(p)$.*
*3. Taking $a + c + \lambda \in H$ and $x \in \{a, b, c\}$ we get $ca + a + \lambda, a + b + c, c^2 + b + c$ and $ca + a + \lambda, c^2 + b + c$ are added to $H$ and $\mathrm{SAT}_p(p)$.*
*4. Taking $bc + c^2 + b \in H$ and $x \in \{b\}$ we get $ba + ca + \lambda$, which prefix right reduces to zero by $\mathrm{SAT}_p(p)$.*
*5. Taking $ca + a + \lambda \in H$ and $x \in \{a, b, c\}$ we get $a + c + \lambda, c^2 + b + c, a + b + c$, which prefix right reduce to zero by $\mathrm{SAT}_p(p)$.*
*6. Taking $c^2 + b + c \in H$ and $x \in \{b\}$ we get $ca + a + \lambda$, which prefix right reduces to zero by $\mathrm{SAT}_p(p)$.*
*7. As $H = \emptyset$ we get $\mathrm{SAT}_p(p) = \{a+b+c, bc+c^2+b, a+c+\lambda, ba+ca+\lambda, ca+a+\lambda, c^2+b+c\}$.*

**Theorem 2** *The procedure is correct, i.e. for all $p \in \mathbf{Z}[\mathcal{H}]$, $x \in \mathcal{H}$ the polynomial $p \cdot x$ is prefix right reducible to zero by $\mathrm{SAT}_p(p)$.*

**Theorem 3** *The procedure terminates for left-cancellative monoids with a finite convergent monadic presentation.*

## 6 Completion in $\mathbf{Z}[\mathcal{H}]$

As we are interested in Gröbner bases of right ideals we are looking for a finite test for checking, whether the reduction relation induced by a finite set of polynomials is confluent, using the concepts of superpositions, critical pairs and s–polynomials, as introduced by Buchberger. First we consider a general definition of superpositions, which does not correspond to the usual critical situations in reduction systems, but nevertheless provides a criterion for confluence.

**Definition 7** *Given two polynomials $p_1, p_2 \in \mathbf{Z}[\mathcal{H}]$ with $HT(p_i) = t_i$ for $i = 1, 2$. If there are $x_1, x_2 \in \mathcal{H}$ with $t_1 \cdot x_1 = t_2 \cdot x_2 = t$, let $c_1, c_2$ be the coefficients of $t$ in $p_1 \cdot x_1$ respectively $p_2 \cdot x_2$. If $c_2 \geq c_1 > 0$ and $c_2 = a \cdot c_1 + b$, where $a, b \in \mathbf{Z}, b$ a remainder of $c_1$, we get the following s-polynomial*

$$spol(p_1, p_2, x_1, x_2) = a \cdot p_1 \cdot x_1 - p_2 \cdot x_2.$$

*Let $U_{HM(p_1),HM(p_2)} \subseteq \mathcal{H}^2$ be the set containing all pairs $x_1, x_2 \in \mathcal{H}$ as above.*

Notice that $p_1 = p_2$ is possible. The set $U_{HM(p_1),HM(p_2)}$ can be empty, finite or even infinite depending on $\mathcal{H}$, i.e. given a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ the set of critical situations belonging to the polynomials in $F$ can be infinite.

**Theorem 4** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, $F$ saturated. Equivalent are:*

1. *$F$ is a Gröbner basis.*
2. *$ideal_r(F) \xrightarrow{*}{}^{r}_{F} 0$.*
3. *For all not necessarily different $f_k, f_l \in F$, $(x_k, x_l) \in U_{HM(f_k),HM(f_l)}$ we have:*

$$spol(f_k, f_l, x_k, x_l) \xrightarrow{*}{}^{r}_{F} 0.$$

Unfortunately theorem 4 is only of theoretical interest as in general it only provides an infinite test for verifying that a set is a Gröbner basis. Trying to localize this test severe problems arise, as our reduction relation is not transitive (compare remark 3).
In ordinary polynomial rings as $\mathbf{Z}[x_1, \ldots x_n]$ one can select a "smallest" critical pair by taking the least common multiply of $t_1$ and $t_2$ and it is sufficient to examine this case [KaKa84, KaKa88]. In $\mathbf{Z}[\mathcal{H}]$ the situation is more complicated. Reviewing definition 7 we see that it is important to solve the equation $t_1 \cdot x = t_2 \cdot y$.
Therefore, we are looking for a suitable basis of a set

$$U_{t_1,t_2} = \{(x_1, x_2) \mid t_1 \cdot x_1 = t_2 \cdot x_2\}.$$

One idea might be to look at a basis $B_{t_1,t_2} \subseteq U_{t_1,t_2}$ such that for all $(x_1, x_2) \in U_{t_1,t_2}$ we have $(b_1, b_2) \in B_{t_1,t_2}, m \in \mathcal{H}$ fulfilling $x_1 = b_1 \cdot m, x_2 = b_2 \cdot m$. But this is not sufficient as the following example shows:

**Example 8** *Let $\Sigma = \{a, b, c, d, e, f\}$ with $d \succ a \succ b \succ c \succ e \succ f$ and $T = \{abc \longrightarrow d^2, b^2ce \longrightarrow d^2f\}$. Take $F = \{a + b, b^2c + d^2, d^2e + d^2f, d + \lambda\}$. Looking at $a + b$ and $d + \lambda$ we get a critical situation in $d^2$ which leads to $b^2c - d$ and $b^2c - d \xrightarrow{*}{}^{r}_{F} 0$. But $d^2e$ gives us $d^2f - de$, which does not reduce to zero by $F$. The clue is that $d^2$ is no real critical situation, i.e. $a + b$ cannot be applied to reduce $d^2$, but $d^2e$ can be reduced by both, $a + b$ and $d + \lambda$.*

Example 8 is due to the fact that we have an s–polynomial $spol(p_1, p_2, x_1, x_2)$, where $RED(p_1) \cdot x_1 > HM(p_1) \cdot x_1$ or $RED(p_2) \cdot x_2 > HMp_2) \cdot x_2$, which can be reduced to zero by saturating sets of $p_1$ and $p_2$, while $spol(p_1, p_2, x_1, x_2) \cdot z$ with $z \in \mathcal{H}$ is not trivial according to them. Even taking a saturated set of polynomials into account does not guarantee the Gröbner basis property, as the set $F$ in our example is a (prefix) saturated set.
Another approach might be to look for a suitable basis of a set $U_{p_1,p_2} = \{(x_1, x_2) \mid HT(p_1 \cdot x_1) = t_1 \cdot x_1 = t_2 \cdot x_2 = HT(p_2 \cdot x_2), HC(p_1 \cdot x_1), HC(p_2 \cdot x_2) > 0\}$, which describes real critical situations in the sense that $t_1 \cdot x_1 = t_2 \cdot x_2$ is an overlap, where both $p_1$ and $p_2$ can be applied for reduction. But even a basis for such a set is not sufficient.

**Example 9** *Let $\Sigma = \{a, b, c, d, e, f, g\}$ with $a \succ b \succ c \succ d \succ e \succ f \succ g$ and $T = \{ac \longrightarrow d, bc \longrightarrow e, dg \longrightarrow b, eg \longrightarrow f\}$. Take $F = \{a + b, d + e, b + f, fc + e, d + \lambda, b + g, gc + e, e + g, g^2 + f, g + \lambda\}$. Looking at $a + b$ and $d + \lambda$ we get a real critical situation in $d$, which leads to $e - \lambda \longrightarrow^{r}_{e+g} - g - \lambda \longrightarrow^{r}_{g+\lambda} 0$, but $(e - \lambda) \cdot g = f - g$ is $F$–irreducible.*

As seen in example 6 even (prefix) saturated sets do not guarantee that $p \xrightarrow{*}{}^{r}_{F} 0$ implies $p \cdot x \xrightarrow{*}{}^{r}_{F} 0$ for $p \in \mathbf{Z}[\mathcal{H}]$, $x \in \mathcal{H}$. Now prefix right reduction is transitive and gives enough information to cope with this defect. It will enable us to formulate another characterization of Gröbner bases.

**Lemma 5** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ and $p, q \in \mathbf{Z}[\mathcal{H}]$. Let $p \longrightarrow^{p}_{q} 0$ and $q \xrightarrow{*}{}^{r}_{F} 0$. From these reduction sequences we get the representations $p = d \cdot q \cdot x$ and $q = \sum_{i=1}^{k} d_i \cdot g_i \cdot x_i$, for $d, d_i \in \mathbf{Z}, g_i \in F, x, x_i \in \mathcal{H}$, where the following statements hold:*

1. *$HM(p) \geq d_i \cdot g_i \cdot x_i \cdot x$ for all $i \in \{1, \ldots k\}$.*
2. *If $HT(p) = HT(g_i \cdot x_i \cdot x)$ then $HT(g_i \cdot x_i \cdot x) = HT(g_i \cdot x_i)x$ and $HC(g_i \cdot x_i \cdot x) \leq |HC(p)|$.*

We can even restrict ourselves to special s–polynomials to localize our confluence test.

**Definition 8 (Prefix s–polynomials)** *Given two polynomials $p_1, p_2 \in \mathbf{Z}[\mathcal{H}]$ with $HC(p_i) = c_i > 0$, $HT(p_i) = t_i$, $RED(p_i) = r_i$ for $i = 1, 2$. If there is $x \in \mathcal{H}$ with $t_1 = t_2 x$ we have to distinguish:*

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

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

*This gives us the prefix s–polynomial*

$$spol_p(p_1, p_2) = a \cdot r_2 \cdot x - b \cdot t_2 x - r_1 = a \cdot p_2 \cdot x - p_1.$$

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

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

*This gives us the prefix s–polynomial*

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

Notice that a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ only gives us finitely many prefix s–polynomials.

**Theorem 5** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, $F$ prefix saturated. Equivalent are:*

1. *$F$ is a Gröbner basis.*
2. *$ideal_r(F) \xrightarrow{*}{}_F^r 0$*
3. *For all $f_k, f_l \in F$ we have $S_p \xrightarrow{*}{}_F^r 0$, where $S_p \in \mathcal{SAT}_p(spol_p(f_k, f_l))$.*

This theorem gives rise to the following procedure.

**Procedure Completion with respect to Prefix Saturation**

input: $F \subseteq \mathbf{Z}[\mathcal{H}]$, $F = \{f_1, \ldots f_n\}$ and
$(\Sigma, T)$ a convergent presentation of $\mathcal{H}$.
output: $\text{GB}(F)$, a Gröbner basis of $F$.

$G := \bigcup_{i=1}^n \text{SAT}_p(f_i)$;
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ do
  $(q_1, q_2) :=$ remove$(B)$;
  if $h := spol_p(q_1, q_2)$ exists then;
    $S := \text{SAT}_p(h)$;
    while $S \neq \emptyset$ do
      $g :=$ remove$(S)$;
      $g' :=$ hnf$(g, G)$;
      if $g' \neq 0$ then
        $B := B \cup \{(f, \tilde{g}) \mid f \in G, \tilde{g} \in \text{SAT}_p(g')\}$;
        $G := G \cup \text{SAT}_p(g')$;
endwhile
$\text{GB}(F) := G$

where $\text{SAT}_p$ denotes the output of our prefix saturation procedure, *remove* removes an element from a set and $hnf(g, G)$ computes a "canonized normal form" of $g$ with respect to $G$, where only right reduction at the head monomial is allowed.
There are two critical points, why this procedure might not terminate: prefix saturation of a polynomial need not terminate and the set $B$ need not become empty.

**Theorem 6** *In case the procedure terminates the output is a Gröbner basis.*

Note that in general monoid rings are not (right–, left–) Noetherian, i.e. not every ideal can be finitely generated. We can show that in special cases finitely generated right ideals allow finite Gröbner bases, even when the corresponding monoid ring is not right–Noetherian.

**Theorem 7** *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be finite.*

1. *The procedure terminates when $\mathcal{H}$ is a free monoid presented by finite $\Sigma$ and $T = \emptyset$.*
2. *The procedure terminates when $\mathcal{H}$ is a group presented by a finite convergent 2–monadic system providing inverses of length 1 for the generators.*

# 7 Relations to Other Work and Applications

In our approach to generalize the concept of Gröbner bases to monoid rings, we find that in order to give a criteria for a set to be a Gröbner basis (in our case of a right ideal), there are two main problems to solve. They arise from the fact that in general the ordering and multiplication on our monoid are not compatible, i.e. $m_1 \succ m_2$ need not imply $m_1 \cdot x \succ m_2 \cdot x$. Let $\rightarrow$ be a computable reduction on our monoid ring $R[\mathcal{H}]$ (e.g. as described in definition 2). Trying to characterize a set $F \subseteq R[\mathcal{H}]$ as a Gröbner basis of a (right, left) ideal by means of s–polynomials and their reducibility as in Buchberger's work, we have to solve the following problems:

1. We have to localize our critical situations.

2. We have to guarantee that $p \longrightarrow_q 0$ and $q \xrightarrow{*}_F 0$ implies the existence of a representation of $p$ as $p = \sum_{i=1}^{k} d_i \cdot g_i \cdot x_i$, $d_i \in \mathbf{Z}, g_i \in F, x_i \in \mathcal{H}$ such that $HM(p) \geq d_i \cdot g_i \cdot x_i$ for all $i \in \{1, \ldots k\}$. Note that this is weaker than demanding $p \xrightarrow{*}_F 0$.

In case these problems are solved we immediately get: $F \subseteq R[\mathcal{H}]$ is a Gröbner basis for the (right, left) ideal generated by $F$ if and only if for all $f, g \in F$ the "appropriate" s–polynomials reduce to zero by $\xrightarrow{*}_F$.
In the previous sections we have solved these problems by introducing prefix right reduction, prefix saturation and prefix s–polynomials. Unfortunately prefix saturation need not be finite in general. For example take $T = \{ba \longrightarrow ab\}$ and $p = b + \lambda$. Then a prefix saturating set of $p$ must prefix right reduce the set $\{a^n b + a^n | n \in \mathbf{N}\}$ to zero. It is obvious that no such finite prefix saturating sets of $p$ exist.
In case $T$ contains the commutator set of $\Sigma$, $T_c = \{a_2 a_1 \longrightarrow a_1 a_2 | a_1, a_2 \in \Sigma, a_1 \prec a_2\}$ the two problems can be solved in a similar way by introducing commutative right reduction, commutative saturation and commutative s–polynomials. Due to Dickson's lemma we always get finite Gröbner bases (in this case even of ideals)([MaRe]).
Now we want to sketch, how the results of Buchberger [Bu85], Kandri–Rody, Kapur [KaKa84, KaKa88], Mora [Mo85], Baader [Ba89] and Weispfenning [We92] can be seen in this context. Note that the approach can easily be modified for $K[\mathcal{H}]$, where $K$ is a field.

1. Gröbner bases for $R[x_1, \ldots x_n]$, where $R$ is a field or $\mathbf{Z}$, as described in [Bu85, KaKa84, KaKa88]:
   We can view $R[x_1, \ldots x_n]$ as the monoid ring over the free commutative monoid $\mathcal{H}$ generated by $\{x_1, \ldots, x_n\}$ and for instance the lexicographic–degree ordering is monotone on $\mathcal{H}$. Therefore, $p$ itself is (commutatively) saturated and we can take the usual definition of s–polynomials as a basis for our set of s–polynomials. Such s–polynomials are for example in case $R = \mathbf{Z}$ defined as follows: Given two polynomials $p_1, p_2$ with $HC(p_2) = c_2 \geq HC(p_1) = c_1 > 0$, $HT(p_i) = t_i, RED(p_i) = r_i$ for $i = 1, 2$. Let $x_1, x_2$ such that $t_1 \cdot x_1 = t_2 \cdot x_2$ is the least common multiple of $t_1, t_2$ and $a, b \in \mathbf{Z}$, $b$ a remainder of $c_1$ with $c_2 = a \cdot c_1 + b$. We get the following $spol(p_1, p_2) = a \cdot p_1 \cdot x_1 - p_2 \cdot x_2$.
   Equivalent are:
   (a) $ideal_r(F) \xrightarrow{*}_F 0$
   (b) For all $f_k, f_l \in F$ we have: $spol(f_k, f_l) \xrightarrow{*}_F 0$.

2. Gröbner bases for $R\langle x_1, \ldots x_n\rangle$, where $R$ is a field or $\mathbf{Z}$, as described in [Mo85, Ba89]:
   We can view $R\langle x_1, \ldots x_n\rangle$ as the monoid ring over the free monoid $\mathcal{H}$ generated by $\{x_1, \ldots, x_n\}$. We know that $p$ itself is (prefix) saturated since $T = \emptyset$ and we can take prefix s–polynomials as described in definition 8.
   Equivalent are:
   (a) $ideal_r(F) \xrightarrow{*}_F 0$
   (b) For all $f_k, f_l \in F$ we have: $spol_p(f_k, f_l) \xrightarrow{*}_F 0$.

3. Gröbner bases for skew polynomials rings $K\langle X, Y\rangle$ as described in [We92]:
   We can view the skew polynomial ring $K\langle X, Y\rangle$ as a monoid ring over a monoid $\mathcal{H}$ presented by $\Sigma = \{X, Y\}, T = \{YX \longrightarrow X^e Y\}$, where $e \in \mathbf{N}^+$. Since the ordering used by Weispfenning is monotone, $p$ itself is saturated and taking his s–polynomials as a basis for our set of s–polynomials we are done. Weispfenning's s–polynomials are defined as follows: Given two polynomials $p_1, p_2$ with $HC(p_i) = c_i$, $HT(p_i) = t_i, RED(p_i) = r_i$ for $i = 1, 2$. Let $x_1, x_2$ such that $t_1 \cdot x_1 = t_2 \cdot x_2$ is the "least common multiple" of $t_1, t_2$ according to the "modified" multiplication. We get the following $spol(p_1, p_2) = c_2 \cdot p_1 \cdot x_1 - c_1 \cdot p_2 \cdot x_2$.
   Equivalent are:
   (a) $ideal_r(F) \xrightarrow{*}_F 0$
   (b) For all $f_k, f_l \in F$ we have: $spol(f_k, f_l) \xrightarrow{*}_F 0$.

Now we want to discuss an application to the subgroup problem.

**Definition 9** *Let $\mathcal{G}$ be a group, $S \subseteq \mathcal{G}$ and $\langle S\rangle$ denote the subgroup generated by $S$. The subgroup problem is to determine, given $w \in \mathcal{G}$, whether $w \in \langle S\rangle$.*

Let $(\Sigma, T)$ be a convergent presentation of a group $\mathcal{G}$. Further let $S = \{u_1, \ldots, u_n\}$ be a subset of $\mathcal{G}$ (we will identify $\mathcal{G}$ and $IRR(T)$ throughout this section), $P_S = \{u_i - 1 \mid u_i \in S\}$ and $\textsc{Gb}(P_S)$ the output of our procedure.

**Lemma 6** *Let $S \subseteq \mathcal{G}$. Then the following statements are equivalent:*

*1.* $w \in \langle S\rangle$

*2.* $w - 1 \in ideal_r(P_S)$

*3.* $w - 1 \xrightarrow{*}{}^{r}_{\textsc{Gb}(P_S)} 0$

**Example 10** *Let $\Sigma = \{a, b, c\}, T = \{a^4 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, a^3 c \longrightarrow b, cb \longrightarrow a\}$ denote a group $\mathcal{G}$ and $S = \{ca, a^2 ca^3, b\}$ a subset of $\mathcal{G}$. Then $\{b - 1, ca - 1, c^2 - b, a^2 c - a, a^3 - c\}$ is a right Gröbner basis of $P_S$ with respect to $\longrightarrow^r$.*

A word of caution: This cannot be generalized to the submonoid problem as the following example shows:

**Example 11** *Let $\Sigma = \{a,b\}, T = \{ab \rightarrow \lambda\}$ denote a monoid $\mathcal{H}$. Let $U = \{a^n \mid n \in \mathbf{N}\}$ be the submonoid of $\mathcal{H}$ generated by $S = \{a\}$. Then we have $b - 1 \in ideal_r(P_S)$ since $b - 1 = -1(a-1) \cdot b$ but $b \notin U$.*

Further research is done on the termination of the prefix completion procedure in case e.g. $(\Sigma, T)$ is a monadic presentation of a group or a monoid. We will investigate if and how the approach described in this paper can be extended to Gröbner bases of ideals and to other structures, as e.g. polycyclic groups.

## Acknowledgements
We would like to thank Thomas Deiß for valuable discussion on a preliminary version of this paper.

# References

[Ba89] F. Baader. *Unification in Commutative Theories, Hilbert's Basis Theorem and Gröbner Bases.* Proc. 3rd UNIF'89.

[Bu85] B. Buchberger. *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory.* N. K. Bose (ed). Multidimensional Systems Theory. Chapter 6. 1985. Dordrecht: Reidel. pp 184–232.

[KaKa84] A. Kandri–Rody and D. Kapur. *An Algorithm for Computing the Gröbner Basis of a Polynomial Ideal over an Euclidean Ring.* Technical Information Series General Electric Company Corporate Research and Development Schenectady. NY 12345. Dec. 1984.

[KaKa88] A. Kandri–Rody and D. Kapur. *Computing a Gröbner Basis of a Polynomial Ideal over an Euclidean domain.* Journal of Symbolic Computation 6(1988). pp 37–57.

[KaWe90] A. Kandri–Rody and V. Weispfenning. *Non–Commutative Gröbner Bases in Algebras of Solvable Type.* Journal of Symbolic Computation 9(1990). pp 1–26.

[KuMa89] N. Kuhn, K. Madlener. *A Method for Enumerating Cosets of a Group Presented by a Canonical System.* Proc. ISSAC'89. pp 338–350.

[La76] M. Lauer. *Kanonische Repräsentanten für die Restklassen nach einem Polynomideal.* Diplomarbeit. Universität Kaiserslautern. 1976.

[MaOt89] K. Madlener, F. Otto. *About the Descriptive Power of Certain Classes of Finite String–Rewriting Systems.* Theoretical Computer Science 67(1989). pp 143–172.

[MaRe] K. Madlener, B. Reinert. *On Gröbner Bases in Monoid Rings.* Internal Report (to appear 1993).

[Mo85] F. Mora. *Gröbner Bases for Non–Commutative Polynomial Rings.* Proc. AAECC–3(1985). Springer LNCS 229. pp 353–362

[NaOD89] P. Narendran and C. Ó'Dúnlaing. *Cancellativity in Finitely Presented Semigroups.* Journal of Symbolic Computation 7(1989). pp 457–472.

[We87] V. Weispfenning. *Gröbner Basis for Polynomial Ideals over Commutative Regular Rings.* Proc. EUROCAL'87. Springer LNCS 378. pp 336–347.

[We92] V. Weispfenning. *Finite Gröbner Bases in Non-Noetherian Skew Polynomial Rings.* Proc. ISSAC'92. pp 329–334.