Tutorial on Gröbner Bases in Monoid and Group Rings

Birgit Reinert
Universität Kaiserslautern

Abstract

The concept of algebraic simplification is of great importance for the field of symbolic computation in computer algebra. In this tutorial we review some fundamental concepts concerning reduction. The techniques for presenting monoids or groups by string rewriting systems are used to define several types of reduction in monoid and group rings. Gröbner bases in this setting arise naturally as generalizations of the corresponding known notions in the commutative and some non-commutative cases. The concepts of saturation and completion are introduced for monoid rings having a finite convergent presentation by a semi-Thue system. They are specialized for cases where the monoid and group presentations provide additional information.

1 Introduction

One of the amazing features of computers is the ability to discover new mathematical results due to extensive computations impossible to be done by hand. Besides incredible numerical calculations, symbolical mathematical manipulations are substantial to many fields in mathematics and physics. Hence the idea of using a computer to do such manipulations led to open up whole new areas of mathematics and computer science. One important contribution to the field of computer algebra is Buchberger's algorithm for manipulating systems of polynomial equations. In 1965 Buchberger introduced the theory of Gröbner bases for polynomial ideals in commutative polynomial rings over fields. It established a rewriting approach to the theory of polynomial ideals. Polynomials can be used as rules by giving an admissible ordering on the terms and using the largest monomial according to this ordering as a left hand side of a rule. "Reduction" then can be compared to division of one polynomial by a set of finitely many polynomials. A Gröbner basis G is a set of polynomials such that every polynomial in the polynomial ring has a unique normal form with respect to reduction using the polynomials in G as rules (especially the polynomials in the ideal generated by G reduce to zero using G). Buchberger developed a terminating procedure to transform a finite generating set of a polynomial ideal into a finite Gröbner basis of the same ideal.

In the last years, the method of Gröbner bases and its applications have been extended from commutative polynomial rings over fields to various types of algebras. Here we want to focus on their generalization to monoid and group rings. There in general admissible well-founded orderings on the set of terms (i.e. monoid elements) will not exist. Still by incorporating the idea of saturation, Gröbner bases can be characterized by s-polynomials and completion procedures can be developed, although they will not terminate in general.

Since our approach combines rewriting for the presentation of the monoid or group and polynomial rewriting in monoid and group rings, let us first introduce a special kind of term rewriting systems, the so called string rewriting systems, which are strongly related to the idea of presenting monoids or groups in terms of generators and defining relations: A string rewriting system consists of an alphabet Σ and a set of rules $T \subseteq \Sigma^* \times \Sigma^*$. We write $u \longrightarrow_T v$ if and only if $u \equiv xly$ and $v \equiv xry$ for some $(l, r) \in T$, $x, y \in \Sigma^*$. $\stackrel{*}{\longrightarrow}_T$ is the reflexive and transitive closure of $\longrightarrow_T$. Every monoid $\mathcal{M}$ can be presented by a string rewriting system (Σ, T), where Σ is an alphabet and T a set of rules. One only has to choose $\Sigma = \mathcal{M}$ and T the multiplication table of the monoid, but this presentation might be infinite or even non-recursive. We will restrict ourselves to presentations of monoids and groups, where Σ is finite and T is finite, confluent and Noetherian, i.e., each word in Σ^* has a unique normal form with respect to T. Furthermore, we require the existence of a total, well-founded ordering $\succeq$ which is admissible on Σ^* such that for all $(l, r) \in T$, $l \succ r$ holds. The monoid $\mathcal{M}$ then is isomorphic to the set of words irreducible with respect to T. The empty word $\lambda \in \Sigma^*$ represents the identity of $\mathcal{M}$. The word problem is decidable, which is essential for computation in $\mathbb{K}[\mathcal{M}]$. Multiplication of two terms $u, v \in \mathcal{M}$ is defined by $u \circ v = (uv){\downarrow_T}$ where $w{\downarrow_T}$ denotes the T-normal form of w. The ordering $\succeq$ on Σ^* induces an ordering $\succeq$ on $\mathcal{M}$ such that for $u, v \in \mathcal{M}$ we get $u \succeq \lambda$ and $uv \succeq u \circ v$.

The elements of a monoid ring $\mathbb{K}[\mathcal{M}]$ over a field $\mathbb{K}$ can be presented as "polynomials" $f = \sum_{m \in \mathcal{M}} \alpha_m \cdot m$ where only finitely many coefficients are non-zero. Addition and multiplication for two polynomials $f = \sum_{m \in \mathcal{M}} \alpha_m \cdot m$ and $h = \sum_{m \in \mathcal{M}} \beta_m \cdot m$ is defined as $f + h = \sum_{m \in \mathcal{M}} (\alpha_m + \beta_m) \cdot m$ and $f * h = \sum_{m \in \mathcal{M}} \gamma_m \cdot m$ with $\gamma_m = \sum_{x \circ y = m \in \mathcal{M}} \alpha_x \cdot \beta_y$. For a subset F of $\mathbb{K}[\mathcal{M}]$ we call the set $\mathsf{ideal}_r(F) = \{\sum_{i=1}^n \alpha_i \cdot f_i * w_i \mid n \in \mathbb{N}, \alpha_i \in \mathbb{K}, f_i \in F, w_i \in \mathcal{M}\}$ the **right ideal** generated by F and this is the structure we are interested in describing by reduction. We will henceforth always assume that the field $\mathbb{K}$ is computable and the monoid $\mathcal{M}$ is presented by a finite convergent string rewriting system (Σ, T) with $\succeq$ a well-founded ordering as described above.

2 Defining Reduction in $\mathbb{K}[\mathcal{M}]$

Given a non-zero polynomial p in $\mathbb{K}[\mathcal{M}]$, the **head term** $\mathsf{HT}(p)$ is the largest term in p with respect to $\succ$, $\mathsf{HC}(p)$ is the coefficient of this term and $\mathsf{HM}(p) = \mathsf{HC}(p) \cdot \mathsf{HT}(p)$ the **head monomial**. The ordering on $\mathcal{M}$ can be extended to a partial ordering on $\mathbb{K}[\mathcal{M}]$ by setting $p > q$ if and only if $\mathsf{HT}(p) \succ \mathsf{HT}(q)$ or $(\mathsf{HM}(p) = \mathsf{HM}(q)$ and $p - \mathsf{HM}(p) > q - \mathsf{HM}(q))$, and this ordering is Noetherian. Frequently in polynomial rings reduction is defined by using the head monomial of a polynomial as a left hand side of a rule in case the head term of the polynomial is a divisor of the term of the monomial to be reduced. But defining reduction in this way for monoid rings need not be Noetherian as the following example shows.

Example 2.1 *Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow \lambda, ba \longrightarrow \lambda\}$ be a presentation of a group $\mathcal{G}$ with a length-lexicographical ordering induced by $a \succ b$. Suppose we simply require divisibility*[1] *of the head term to allow reduction. Then we could reduce the polynomial $b^2 + 1 \in \mathbb{Q}[\mathcal{G}]$ at the monomial b^2 by the polynomial $a + b$ as $b^2 = a \circ b^3$. This would give us:*

$$b^2 + 1 \longrightarrow_{a+b} b^2 + 1 - (a + b) * b^3 = -b^4 + 1$$

and the polynomial $-b^4 + 1$ likewise would be reducible by $a + b$ at the monomial $-b^4$ causing an infinite reduction sequence.

Hence additional restrictions are necessary to prevent that a monomial is replaced by a larger polynomial.

Definition 2.2 *Let p, f be two non-zero polynomials in $\mathbb{K}[\mathcal{M}]$. We say f* **strongly right reduces** *p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{s}}_f q$, if*

(a) $\mathsf{HT}(f * w) = t$ for some $w \in \mathcal{M}$, and

(b) $q = p - \alpha \cdot \mathsf{HC}(f * w)^{-1} \cdot f * w$.

Strong right reduction is indeed Noetherian and we have $\overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_F = \equiv_{\mathsf{ideal}_r(F)}$ for $F \subseteq \mathbb{K}[\mathcal{M}]$.

While it is possible to characterize Gröbner bases of right ideals by s-polynomials with respect to strong right reduction, in general infinitely many such s-polynomials have to be tested and hence there is no "nice" procedure.

One way to reduce the set of critical situations that have to be considered to ensure confluence is to weaken the reduction relation while preserving the generated equivalence relation. The key idea is that for two reduction relations $\longrightarrow^1$ and $\longrightarrow^2$ on a set $\mathcal{E}$ such that $\longrightarrow^1 \subseteq \longrightarrow^2$ and $\overset{*}{\longleftrightarrow}{}^1 = \overset{*}{\longleftrightarrow}{}^2$, the confluence of $\longrightarrow^1$ on $\mathcal{E}$ implies the confluence of $\longrightarrow^2$ on $\mathcal{E}$.

One natural weakening of strong right reduction is right reduction. Instead of using all right multiples of a polynomial by monomials as rules we restrict ourselves to those right multiples of a polynomial which allow the head term of the polynomial to keep its head position.

Definition 2.3 *Let p, f be two non-zero polynomials in $\mathbb{K}[\mathcal{M}]$. We say f* **right reduces** *p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{r}}_f q$, if*

(a) $\mathsf{HT}(f * w) = \mathsf{HT}(f) \circ w = t$ for some $w \in \mathcal{M}$, and

[1] We call a term t (right) divisible by a term x in case there exists a term z such that $t = x \circ z$.

(b) $q = p - \alpha \cdot \mathsf{HC}(f * w)^{-1} \cdot f * w$.

Again right reduction is Noetherian and let us continue to state some of the properties right reduction satisfies.

Lemma 2.4 *(Translation Lemma) Let F be a set of polynomials in $\mathbb{K}[\mathcal{M}]$ and $p, q, h \in \mathbb{K}[\mathcal{M}]$ some polynomials. Then the following statements hold:*

1. *Let $p - q \longrightarrow^{\mathrm{r}}_{F} h$. Then there are polynomials $p', q' \in \mathbb{K}[\mathcal{M}]$ such that we have $p \stackrel{*}{\longrightarrow}^{\mathrm{r}}_{F} p'$, $q \stackrel{*}{\longrightarrow}^{\mathrm{r}}_{F} q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{r}}_{F}$. Then there exists a polynomial $g \in \mathbb{K}[\mathcal{M}]$ such that $p \stackrel{*}{\longrightarrow}^{\mathrm{r}}_{F} g$ and $q \stackrel{*}{\longrightarrow}^{\mathrm{r}}_{F} g$.*

Unfortunately, right reduction is not as strong as strong right reduction.

Lemma 2.5 *Let $p, q \in \mathbb{K}[\mathcal{M}]$ and $F \subseteq \mathbb{K}[\mathcal{M}]$. Then $p \stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{F} q$ implies $p - q \in \mathsf{ideal}_r(F)$ but not vice versa.*

Example 2.6 *Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be a presentation of a group $\mathcal{G}$ with a length-lexicographical ordering induced by $a \succ b \succ c$. Inspecting the polynomials $p = a + b + c, q = b - \lambda \in \mathbb{Q}[\mathcal{G}]$ and the set $F = \{a + b + c\} \subseteq \mathbb{Q}[\mathcal{G}]$ we get $p - q = a + c + \lambda = (a + b + c) * b \in \mathsf{ideal}_r(F)$, but $a + b + c \not\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{F} b - \lambda$.*

Obviously for a set of polynomials $F \subseteq \mathbb{K}[\mathcal{M}]$ we have $\longrightarrow^{\mathrm{r}}_{F} \subseteq \longrightarrow^{\mathrm{s}}_{F}$, but in general we cannot expect $\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{F} = \stackrel{*}{\longleftrightarrow}^{\mathrm{s}}_{F}$. This can be gained by enriching the set F to a set F' such that $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(F')$ and $\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{F'} = \stackrel{*}{\longleftrightarrow}^{\mathrm{s}}_{F}$. This will be achieved by a process called saturation.

Definition 2.7
1. *A set of polynomials $S \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbb{K}^*, w \in \mathcal{M}\}$ is called a* **saturating set** *for a non-zero polynomial $p \in \mathbb{K}[\mathcal{M}]$, if for all $w \in \mathcal{M}$, in case $p * w \neq 0$ then $p * w \longrightarrow^{\mathrm{r}}_{S} 0$ holds.*
2. *We call a set $F \subseteq \mathbb{K}[\mathcal{M}]$* **saturated**, *if for all $f \in F$ and all $w \in \mathcal{M}$, $f * w \longrightarrow^{\mathrm{r}}_{F} 0$ holds in case $f * w \neq 0$.*

Note that in defining saturating sets we demand right reducibility to 0 in *one* step. This is done to have some equivalent for $p * w \longrightarrow_{p} 0$ in Buchberger's approach. The polynomial $a+b+c$ in Example 2.6 has the saturating set $S = \{a+b+c, a+c+\lambda, bc+c^2+b\}$. However, the following example shows that saturating sets need not be finite.

Example 2.8 *Let $\Sigma = \{a, b, c, d, e, f\}$ and $T = \{abc \longrightarrow ba, fbc \longrightarrow bf, bad \longrightarrow e\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by*

$a \succ b \succ c \succ d \succ e \succ f$. Then the polynomial $p = a + f \in \mathbb{Q}[\mathcal{M}]$ will allow no finite saturating sets:

$$\begin{array}{ccc}
\underline{a} + f & & \\
\Big| \, bc & & \\
\underline{ba} + bf & \overline{}_{d} & e + \underline{bfd} \\
\Big| \, bc & & \\
\underline{b^2 a} + b^2 f & \overline{}_{d} & be + \underline{b^2 fd} \\
\Big| \, bc & & \\
\vdots & &
\end{array}$$

In analogy to Buchberger we will call bases of right ideals which induce a confluent right reduction describing the right ideal congruence right Gröbner bases.

Definition 2.9 *A set $G \subseteq \mathbb{K}[\mathcal{M}]$ is called a* **right Gröbner basis** *of $\mathsf{ideal}_r(G)$, if $\overset{*}{\longleftrightarrow}{}^{\mathrm{r}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$ and $\longrightarrow^{\mathrm{r}}_{G}$ is confluent.*

In accordance with the terminology used in Buchberger's approach to give a confluence test for sets of polynomials, we define critical pairs of polynomials with respect to right reduction as situations were both polynomials can be applied for right reduction.

Definition 2.10 *Given two non-zero polynomials $p_1, p_2 \in \mathbb{K}[\mathcal{M}]$, every pair of elements $w_1, w_2 \in \mathcal{M}$ such that $\mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_1) \circ w_1 = \mathsf{HT}(p_2) \circ w_2 = \mathsf{HT}(p_2 * w_2)$, defines a* **right s-polynomial**

$$\mathsf{spol}_r(p_1, p_2, w_1, w_2) = \mathsf{HC}(p_1 * w_1)^{-1} \cdot p_1 * w_1 - \mathsf{HC}(p_2 * w_2)^{-1} \cdot p_2 * w_2.$$

Let $U_{p_1,p_2} \subseteq \mathcal{M} \times \mathcal{M}$ be the set containing all *such pairs $w_1, w_2 \in \mathcal{M}$.*

A right s-polynomial will be called non-trivial in case it is non-zero. Obviously the saturating set $S = \{a + b + c, a + c + \lambda, bc + c^2 + b\}$ of the polynomial $a + b + c$ from Example 2.6 is no right Gröbner basis as the polynomials $a + b + c$ and $a + c + \lambda$ give rise to the non-trivial s-polynomial $b - \lambda$ which cannot be right reduced to 0 using S.

Theorem 2.11 *For a saturated set F of polynomials in $\mathbb{K}[\mathcal{M}]$, the following statements are equivalent:*

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} 0$.*
2. *For all not necessarily different polynomials $f_k, f_l \in F$ and every corresponding pair $(w_k, w_l) \in U_{f_k,f_l}$ we have $\mathsf{spol}_r(f_k, f_l, w_k, w_l) \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} 0$.*

Notice that this theorem, although characterizing a right Gröbner basis by right s-polynomials, in general does not provide a finite test. This can be gained by introducing a further weakenings of right reduction e.g. by defining a right divisibility based on prefixes for Σ^*. Such prefixes are divisors with respect to word concatenation and hence easy to determine.

Definition 2.12 *Let p, f be two non-zero polynomials in $\mathbb{K}[\mathcal{M}]$. We say f* **prefix reduces** *p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{p}}_{f} q$, if*

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

(b) $q = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot f * w$.

Notice that in the above definition the equation in (a) has at most one solution and we then always have $\mathsf{HC}(f * w) = \mathsf{HC}(f)$. The results of Lemma 2.4 carry over as does Lemma 2.5 and Example 2.6. Again we cannot expect $\stackrel{*}{\longleftrightarrow}^{\mathrm{p}}_{F} \;=\; \stackrel{*}{\longleftrightarrow}^{\mathrm{s}}_{F}$, but something similar can be gained by enriching the set F to a set F' such that $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(F')$ and $\stackrel{*}{\longleftrightarrow}^{\mathrm{p}}_{F'} \;=\; \stackrel{*}{\longleftrightarrow}^{\mathrm{s}}_{F}$. This will be achieved by a process called prefix saturation.

Definition 2.13 *1. A set of polynomials $S \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbb{K}^*, w \in \mathcal{M}\}$ is called a* **prefix saturating set** *for a non-zero polynomial $p \in \mathbb{K}[\mathcal{M}]$, if for all $w \in \mathcal{M}$, in case $p * w \neq 0$ then $p * w \longrightarrow^{\mathrm{p}}_{S} 0$ holds.*

2. We call a set $F \subseteq \mathbb{K}[\mathcal{M}]$ **prefix saturated***, if for all $f \in F$ and all $w \in \mathcal{M}$, $f * w \longrightarrow^{\mathrm{p}}_{F} 0$ holds in case $f * w \neq 0$.*

To enumerate prefix saturating sets for a polynomial, we can make use of the fact that the elements of the monoid are represented by words which are irreducible with respect to a convergent string rewriting system (Σ, T). We do not have to compute all right monoid multiples of a polynomial but we can restrict ourselves to those which are overlaps between the respective head term of a polynomial multiple and the rules in T. The following procedure uses this idea.

Procedure: Prefix Saturation

Given: A polynomial $p \in \mathbb{K}[\mathcal{M}]$ and
(Σ, T) a convergent string rewriting system presenting $\mathcal{M}$.
Find: S a prefix saturating set for p.

$S := \{p\}$;
$H := \{p\}$;
while $H \neq \emptyset$ **do**
  $q :=$ remove(H);
  % Remove an element using a fair strategy, i.e., no element is left in H for ever
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda$ for some $(l, r) \in T\}$ **do**

% $C(t)$ contains special overlaps between t and left hand sides of rules in T
$q' := q * w$;
if $q' \not\longrightarrow^{\mathrm{p}}_{S} 0$ and $q' \neq 0$
then $S := S \cup \{q'\}$;
$H := H \cup \{q'\}$;
endif
endfor
endwhile

Similar to definition 2.9 we can define Gröbner bases with respect to prefix reduction.

Definition 2.14 *A set $G \subseteq \mathbb{K}[\mathcal{M}]$ is said to be a* **prefix Gröbner basis** *of* $\mathsf{ideal}_r(G)$, *if* $\overset{*}{\longleftrightarrow}{}^{\mathrm{p}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$ *and* $\longrightarrow^{\mathrm{p}}_{G}$ *is confluent.*

Notice that prefix saturating sets for a polynomial p satisfy the first statement of this definition, but in general need not be prefix Gröbner bases of $\mathsf{ideal}_r(p)$, i.e., the elements of $\mathsf{ideal}_r(p)$ do not necessarily prefix reduce to zero.

Example 2.15 *Reviewing Example 2.6, let $p = a + b + c$. Then $S = \{a + b + c, a + c + \lambda, bc + c^2 + b, ba + ca + \lambda, ca + a + \lambda, c^2 + b + c\}$ is a prefix saturating set for p, but $\longrightarrow^{\mathrm{p}}_{S}$ is not confluent on $\{p * w \mid w \in \mathcal{M}\}$. We have $a + b + c \longrightarrow^{\mathrm{p}}_{a+c+\lambda} b - \lambda$ and $a + b + c \longrightarrow^{\mathrm{p}}_{a+b+c} 0$ but $b - \lambda \overset{*}{\not\longrightarrow}{}^{\mathrm{p}}_{S} 0$.*

This example also shows that Gröbner bases via $\longrightarrow^{\mathrm{p}}$ are Gröbner bases via $\longrightarrow^{\mathrm{s}}$ but not vice versa. The set $F = \{a+b+c, b-\lambda\}$ is a strong Gröbner basis, but not a prefix Gröbner basis.

Definition 2.16 *Given two non-zero polynomials $p_1, p_2 \in \mathbb{K}[\mathcal{M}]$, if there is $w \in \mathcal{M}$ such that $\mathsf{HT}(p_1) \equiv \mathsf{HT}(p_2)w$ the* **prefix s-polynomial** *is defined as*

$$\mathsf{spol}_p(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot p_1 - \mathsf{HC}(p_2)^{-1} \cdot p_2 * w.$$

Now two polynomials give rise to at most one s-polynomial and a finite test for being a prefix Gröbner basis can be achieved for prefix saturated sets.

Theorem 2.17 *For a prefix saturated set F of polynomials in $\mathbb{K}[\mathcal{M}]$, the following statements are equivalent:*

(1) For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{p}}_{F} 0$.

(2) For all polynomials $f_k, f_l \in F$ we have $\mathsf{spol}_p(f_k, f_l) \overset{*}{\longrightarrow}{}^{\mathrm{p}}_{F} 0$.

Now Theorem 2.17 gives rise to the following procedure, which can be modified to enumerate a Gröbner basis with respect to $\longrightarrow^{\mathrm{p}}$ for a finitely generated right ideal.

Procedure: PREFIX GRÖBNER BASES

Given: A finite set of polynomials $F \subseteq \mathbb{K}[\mathcal{M}]$, and
(Σ, T) a convergent string rewriting system presenting $\mathcal{M}$.
Find: $\textsc{Gb}(F)$ a prefix Gröbner basis of F.
Using: $\textsc{Sat}_p$ a prefix saturating procedure for polynomials.

$G := \bigcup_{f \in F} \textsc{Sat}_p(f)$; % G is prefix saturated
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ **do** % Test if statement 2 of theorem 2.17 is valid
  $(q_1, q_2) :=$ remove(B); % Remove an element using a fair strategy
  if $\mathsf{spol}_p(q_1, q_2)$ exists % The s-polynomial is not trivial
    then $h :=$ normal form$(\mathsf{spol}_p(q_1, q_2), \longrightarrow^{\mathrm{p}}_{G})$;
      if $h \neq 0$
        then $G := G \cup \textsc{Sat}_p(h)$; % G is prefix saturated
          $B := B \cup \{(f, \tilde{h}), (\tilde{h}, f) \mid f \in G, \tilde{h} \in \textsc{Sat}_p(h)\}$;
      endif
  endif
endwhile
$\textsc{Gb}(F) := G$

There are two crucial points, why procedure PREFIX GRÖBNER BASES might not terminate: prefix saturation of a polynomial need not terminate and the set B need not become empty. Notice that in case prefix saturation does not terminate it is possible to modify this procedure in order to enumerate a prefix Gröbner basis by using fair enumerations of the prefix saturating sets needed.

In the following example we want to illustrate how procedure PREFIX GRÖBNER BASES works by computing a prefix Gröbner basis of the right ideal specified in Example 2.6.

Example 2.18 *Let* $\Sigma = \{a, b, c\}$ *and* $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ *with a length-lexicographical ordering induced by* $a \succ b \succ c$. *We want to compute a prefix Gröbner basis of* $\mathsf{ideal}_r(a + b + c)$.
On initializing G *we get* $G = \{a+b+c, a+c+\lambda, bc+c^2+b, ba+ca+\lambda, ca+a+\lambda, c^2+b+c\}$. *Now inspecting this set we see that only one prefix s-polynomial has to be considered, namely*

$$\mathsf{spol}_p(a + b + c, a + c + \lambda) = b - \lambda.$$

Since $\{b - \lambda\}$ *is a saturating set for the polynomial* $b - \lambda$ *we get* $G = G \cup \{b - \lambda\}$.
Now there are two possible prefix s-polynomials to consider and we find

$$\mathsf{spol}_p(bc + c^2 + b, b - \lambda) = c^2 + b + c \longrightarrow^{\mathrm{p}}_{G} 0$$

respectively

$$\mathsf{spol}_p(ba + ca + \lambda, b - \lambda) = ca + a + \lambda \longrightarrow^{\mathrm{p}}_{G} 0$$

and hence $\{a + b + c, a + c + \lambda, bc + c^2 + b, ba + ca + \lambda, ca + a + \lambda, c^2 + b + c, b - \lambda\}$ *is a prefix Gröbner basis of* $\mathsf{ideal}_r(a + b + c)$.

While Theorem 2.17 characterizes *prefix saturated* prefix Gröbner bases it is also possible to drop this restriction e.g. by introducing the concept of interreduction to the theory. So one can show that for $\mathsf{ideal}_r(a+b+c)$ in Example 2.18 the set $\{a+c+\lambda, ca-c, c^2+c+\lambda, b-\lambda\}$ is a reduced prefix Gröbner basis.

3 Further Generalizations

Of course prefix reduction is not the appropriate weakening for every structure. There are cases were finitely generated strong Gröbner bases exist but no finite prefix ones, e.g. in commutative structures. Nevertheless they can be used to compute a strong Gröbner basis, since such a basis is always contained in the weaker one. Other ways of weakening strong right reduction for special structures have been developed and studied for special monoids and groups. The key idea used is as follows:

(1) Define a weakening of strong reduction, say w-reduction, appropriate to the respective structure in the following sense:
If for some polynomials $p, g \in \mathbb{K}[\mathcal{M}]$ and a set of polynomials $F \subseteq \mathbb{K}[\mathcal{M}]$ we have $p \longrightarrow_g^{\mathrm{w}} 0$ and $g \xrightarrow{*}_F^{\mathrm{w}} 0$, then there exists a representation of p in terms of F such that one term in this representation equals the head term of p and all other terms are smaller with respect to the ordering on $\mathcal{M}$.

(2) Define saturation with respect to w-reduction.

(3) Define s-polynomials with respect to w-reduction.

Then in case the translation lemma holds for w-reduction, a characterization of w-Gröbner bases of right ideals as follows is possible:

For a w-saturated set $F \subseteq \mathbb{K}[\mathcal{M}]$ the following statements are equivalent:

(1) For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}_F^{\mathrm{w}} 0$.

(2) For all polynomials $f_k, f_l \in F$ we have $\mathsf{spol}_w(f_k, f_l) \xrightarrow{*}_F^{\mathrm{w}} 0$.

In order to get an effective procedure from this characterization some finiteness and computability conditions have to be satisfied.

This approach has been successfully applied to commutative monoid rings and rings over special groups which are summarized in the following table listing the reductions which – again using appropriate presentations for the groups – ensure the construction of the respective finite Gröbner basis of ideals. Note that $\longrightarrow^{\mathrm{su}}$ stands for suffix, $\longrightarrow^{\mathrm{p}}$ for prefix, $\longrightarrow^{\mathrm{qc}}$ for quasi-commutative, $\longrightarrow^{\mathrm{lpc}}$ for left-polycyclic reduction and $\longrightarrow^{\mathrm{rpc}}$ for right-polycyclic reduction.

Group	*left ideals*	*right ideals*	*two-sided ideals*
free	$\longrightarrow^{\mathrm{su}}$	$\longrightarrow^{\mathrm{p}}$	none[2]
plain	$\longrightarrow^{\mathrm{su}}$	$\longrightarrow^{\mathrm{p}}$	none
context-free	$\longrightarrow^{\mathrm{su}}$	$\longrightarrow^{\mathrm{p}}$	none
nilpotent	$\longrightarrow^{\mathrm{lpc}}$	$\longrightarrow^{\mathrm{qc}}$	$\longrightarrow^{\mathrm{qc}}$ $\longrightarrow^{\mathrm{lpc}}$
polycyclic	$\longrightarrow^{\mathrm{lpc}}$	$\longrightarrow^{\mathrm{rpc}}$	$\longrightarrow^{\mathrm{lpc}}$ $\longrightarrow^{\mathrm{rpc}}$

As mentioned above, the different reductions require special forms of presentations for the respective groups.

More details on Gröbner bases in monoid and group rings and a survey of the literature can be found in

- *Relating Rewriting Techniques on Monoids and Rings: Congruences on Monoids and Ideals in Monoid Rings.*
  (K. Madlener, B. Reinert) Theoretical Computer Science, 208 (1998).

- *String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings.*
  (K. Madlener, B. Reinert) Proceedings of the 1995 Conference on Symbolic Rewriting Techniques. Monte Verita. (Birkhäuser 1998).

- MRC – *Data Structures and Procedures for Computing in Monoid and Group Rings.*
  (B. Reinert, D. Zeckzer) to appear in Applicable Algebra in Engineering, Communications and Computing